Meditaciones sobre la materia

Elementos de álgebra y de geometría

Versión ante-preliminar

Rosana V. Entizne

Universidad Nacional del Sur
Bahía Blanca
Argentina.

22 de enero de 2019

Elementos de álgebra y de geometría
Programa analítico

Unidad 1
Conjuntos. Subconjuntos. Unión. Intersección. Complemento. Diferencia. Leyes de De Morgan. Producto cartesiano de conjuntos.

Unidad 2
Relaciones binarias. Propiedades. Relaciones de equivalencia. Partición de un conjunto. Partición inducida por una relación de equivalencia. Clases de equivalencia. Conjunto cociente.

Unidad 3
Funciones. Imagen e imagen completa inversa. Funciones inyectivas, epiyectivas y biyectivas. Composición de funciones.

Unidad 4
Números naturales. Principio de inducción. Números enteros. Definición del conjunto $\mathbb{Q}$ de los números racionales. Propiedades. Orden. Irracionales. El conjunto $\mathbb{R}$ de los números reales: la recta real. Existencia de raíces en $\mathbb{R}$. Potenciación de exponente entero. Raíz aritmética. Potenciación de exponente racional.

Unidad 5
Divisibilidad de enteros. Máximo común divisor. Algoritmo de Euclides. Teorema fundamental de factorización. Aplicaciones. Sistemas de numeración en distintas bases.

Unidad 6
Números complejos. Operaciones. El plano complejo. Módulo y conjugado. Propiedades. Producto y cociente en forma polar. Potenciación de exponente entero: Fórmula de De Moivre. Radicación. Propiedades.

Unidad 7
Polinomios y ecuaciones algebraicas. Suma y Multiplicacicón. Divisivilidad. Máximo común divisor. Algoritmo de Euclides. Teorema de factorización. Raíces de un polinomio. Raíces múltiples. Teorema fundamental del álgebra. Raíces complejas. Polinomios irreducibles en $\mathbb{R}[X]$. Cálculo de raíces. Problemas de acotación, separación y cálculo de raíces reales. Regla de los signos de Descartes. Cálculo de las raíces racionales de ecuaciones con coeficientes racionales.

Unidad 8
Sistemas de ecuaciones lineales. Resolución por eliminación. Matrices. Operaciones. Propiedades. Traspuesta de una matriz. Determinantes. Definición y propiedades.

Desarrollo por los elementos de una fila o una columna. Determinante de un producto de matrices. Matrices inversibles. Matriz inversa. Regla de Cramer.

Unidad 9
Vectores. Operaciones con vectores. Bases de E^2 y E^3. Sistemas de coordenadas ortogonales. Componentes de un vector y cosenos directores. Proyección ortogonal. Producto escalar. Orientaciones del plano y del espacio. Producto vectorial. Producto mixto. Geometra del plano y del espacio: Ecuación de la recta en el plano y en el espacio. Ecuación del plano. Ángulos entre rectas y planos. Distancia de un punto a un plano y una recta. Distancia entre recta y plano. Distancia entre planos. Distancia entre rectas.

Unidad 10
Espacios vectoriales. Subespacios. Ejemplos. Subespacio generado. Dependencia lineal. Bases. Bases ortonormales. Dimensión. Teorema de la dimensión. Cambio de base. Cambio de coordenadas. Transformaciones lineales. Matriz asociada a una transformación lineal.

Unidad 11
Transformaciones lineales simétricas. Autovalores y autovectores. Polinomio característico. Reducción de una matriz simétrica a la forma diagonal.

Índice general

Estos apuntes para la materia Elementos de álgebra y de geometría no pretenden ser un libro de texto ni mucho menos.
El objetivo es escribir de la forma más clara posible las mismas cosas que digo en clase, haciendo posible la lectura de lo que diré (¿eh?) o bien de lo que he dicho (esta es una situación algo más real). A lo largo del texto se encontrarán muchas preguntas que pretenden motivar la curiosidad del lector. Algunas citas históricas para amenizar un poco y sobre todo rigor matemático "hasta ahí". Es decir: el objetivo principal es que los conceptos se comprendan y se aprehendan. Las formalizaciones vendrán después, leyendo, por ejemplo, un verdadero libro de texto, como los que figuran en la biblografía.

Si el lector saca provecho de estos apuntes, le sugiero tenga a bien mostrarse agradecido con los estudiantes que me pidieron en más de una oportunidad que los escriba y con quien enceró el cerámico dando lugar a un yeso que me mantuvo "inactiva" el tiempo suficiente.

Pequeñas indicaciones al lector:

Como dije hace un momento, estos apuntes son casi un “dictado” de mis clases, en las que además de los contenidos de la materia hago comentarios históricos y propuestas lúdicas, amén de ciertas explicaciones que escapan a la materia pero hacen al mejor entendimiento de la misma.

Todos estos “desvaríos” están señalados, según el siguiente código:

- ($\clubsuit$): comentario lúdico.
- (✠): comentario histórico.
- ©: escapa a la materia.
- ®: recomendación para el lector.
- ($\spadesuit$): ejercicio para final.

Del mismo modo, en los ejercicios de cada capítulo hay marcas con el siguiente significado:

- ®: resuelto en teoría.
- ($\diamond$): similar a los anteriores.
- ©: muy teórico
- ($\clubsuit$): lúdico

Capítulo 1

Teoría intuitiva de conjuntos

Conjuntos. Subconjuntos. Unión. Intersección. Complemento. Diferencia. Leyes de De Morgan.

1.1. Motivación

En el transcurso de estas clases querremos trabajar con conceptos matemáticos como relaciones y funciones y también con estructuras algebraicas que necesitan de una "noción base" que les proporcione un marco conceptual. Este "punto de partida" es la denominada *teoría de conjuntos* que nace de la mano del matemático alemán George Cantor (1845-1918) y que fue prohibida en 1967 por la dictadura griega y luego aquí en la Argentina. Aunque es difícil de entender, durante la dictadura de Videla (1976-1981) se quemaron libros y entre ellos también de teoría de conjuntos, por considerarlos subversivos. El 30 de agosto de 1980 comenzó una quema en un baldío de Sarandí que duró tres días.

1.2. Conceptos primitivos y notaciones

Llamamos *conceptos primitivos* de una teoría a aquellos que no podemos definir, pero sí, interpretar claramente a nivel intuitivo.

Cuando escuchamos la palabra *conjunto* dentro del lenguaje cotidiano la asociamos con la idea de agrupar objetos, por ejemplo un conjunto de discos, de libros..., es decir denota una colección de elementos que guardan alguna característica en común. Ya sean números, personas, figuras o conceptos.

No daremos una definición matemática de esta noción, así como tampoco definiremos lo que es un *elemento* ni la relación de *pertenencia* de un elemento a un conjunto. Simplemente daremos ejemplos que llevarán a aprehender el concepto. Notaremos (salvo excepciones especiales) a los conjuntos con letras mayúsculas de imprenta $(A, B, C, \ldots)$ y a los elementos con letras minúsculas $(a, b, c, \ldots)$.

La característica esencial de un conjunto es estar bien definido, es decir que dado un objeto particular, se puede determinar si pertenece o no al conjunto. Por ejemplo, si se considera el conjunto de los colores primarios, sabemos que el azul pertenece al conjunto, pero el verde no. Si quisiéramos considerar el conjunto de los números decentes, no podríamos hacerlo ya que nadie es capaz de discernir el grado de decencia de un número. Es decir, si el concepto no es claro, no se pueden "agrupar" los elementos "iguales" según ese concepto.

Una vez que tenemos claro el concepto que define a un conjunto, por ejemplo el de los colores primarios que mencionábamos hace un momento, podemos describirlo de dos formas posibles:

1. Por extensión:
   Para definir un conjunto por extensión basta escribir todos los elementos que pertenecen al conjunto entre llaves, así el conjunto de colores primarios, que podemos llamar P, queda definido:
   $$P = \{\textit{rojo, azul, amarillo}\}.$$
2. Por comprensión:
   Para definir un conjunto por comprensión debemos describir exactamente a sus miembros, decir algo así como "son los elementos que son colores primarios" y lo escribimos dentro de llaves, usando a la x como nuestro "elemento genérico", así el conjunto queda definido:
   $$P = \{x : x \text{ es un color primario}\}.$$
   y se lee "P es el conjunto de los x tal que x es un color primario".

Describimos la relación de pertenencia del siguiente modo:

"El azul pertenece al conjunto de colores primarios":	$\textit{azul} \in P$
"El verde no pertenece al conjunto de colores primarios":	$\textit{verde} \notin P$

En general, dada cualquier relación en matemática representaremos la negación de la relación simplemente cruzando el símbolo con una barra inclinada.

Definición 1.1 Dado un determinado conjunto es posible que puedan nombrarse todos sus miembros, como en el caso de los colores primarios, los estudiantes de una determinada promoción de un colegio o, aunque sean muchos, los habitantes de un país. Estos conjuntos se denominan *conjuntos finitos*. En contraposición a ellos existen los *conjuntos infinitos* que son aquellos cuyos elementos no se pueden mencionar en su totalidad, por ejemplo el conjunto de los números naturales o de los puntos de un plano. Si un conjunto es finito, llamamos *orden* a la cantidad de elementos que contiene. Notamos $|A|$ o bien $o(A)$ al orden del conjunto A.

Observación 1.1 Es posible "contar" la cantidad de elementos de un conjunto infinito A. En este caso lo llamamos *cardinal* de A y lo notamos $|A|$ o bien $\sharp A$. Es claro que en un conjunto finito ambas nociones coinciden.

Ejemplo 1.1 Daremos algunos ejemplos de conjuntos por comprensión y por extensión. Claramente sólo algunos conjuntos finitos admiten representación por extensión y algunos conjuntos finitos no admiten representación por comprensión.

1. $P = \{rojo, azul, amarillo\}, \; |P| = 3,$
2. $A = \{x : x \in \mathbb{Z}, -3 \leq x < 5\} = \{-3, \, -2, \, -1, \, 0, \, 1, \, 2, \, 3, \, 4\}, \; |A| = 7,$
3. $B = \{x : x \in \mathbb{R}, 2 < x \leq 6\} = (2, 6], \; |B| = c,$
4. $C = \{a, b, c, m, n, q\}, \quad |C| = 6.$

Es importante notar que dentro del conjunto los elementos no tienen un orden definido y si se repiten al nombrarlos, sólo se consideran una vez. Así, el conjunto V de todas las vocales se puede representar:

$$V = \{a, e, i, o, u\} \qquad V = \{a, e, o, i, u\} \qquad V = \{a, a, e, e, e, i, o, u\}$$
$$V = \{i, i, o, a, e, u\} \quad V = \{a, a, e, e, i, i, i, i, o, o, u\} \quad V = \{x : x \text{ es una vocal}\}$$

pero no de estas formas

$$V_1 = \{\{a\}, \{e\}, \{i\}, \{o\}, \{u\}\} \quad V_2 = \{aeiou\} \qquad V_3 = \{a, \{a\}, e, \{e\}, i, \{i\}, o, \{o\}, u, \{u\}\}$$
$$V_4 = \{\{x\} : x \text{ es una vocal}\} \qquad V_5 = \{vocales\} \quad V_6 = \{\text{vocales castellanas}\}$$

Los elementos que conforman un conjunto son los "dibujitos" diferentes que están separados por comas dentro de las llaves. O bien los que se ajustan a la descripción escrita después de "$x : x$ es" que se lee "*x tal que x es*".

Observación 1.2 La notación que estamos usando no es única. En otros textos se puede encontrar $x \setminus x$ o $x \ni x$ para representar "x tal que x".

La cantidad de elementos de V, o el orden de V es cinco. En símbolos: $|V| = o(V) = 5$. Vemos que:

$|V_1| = 5$: tiene cinco elementos, cada elemento es un conjuntito que contiene una vocal.

$|V_2| = 1$: hay una sola cosa adentro de las llaves: la concatenación de todas las vocales.

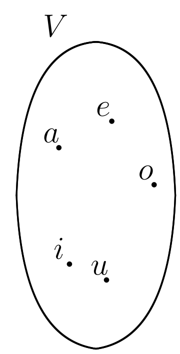
$|V_3| = 10$: dentro del conjunto hay 10 cosas separadas por comas.

$|V_4| = 5$: es la descripción por comprensión del conjunto V_1.

$|V_5| = 1$: sólo hay un elemento: la palabra vocales.

$|V_6| = 1$: igual que en el caso anterior, sólo tiene un elemento: la expresión "vocales castellanas".

1.2.1. Diagramas de Venn-Euler



Los conjuntos se pueden representar de una forma muy gráfica. Si la idea es que un conjunto es como una bolsita que contiene cosas, el diagrama de Venn no es más que una representación gráfica de este hecho: Una curva cerrada que no se corta a sí misma y encierra todos los elementos del conjunto.
Usualmente decimos diagrama de Venn y en verdad utilizamos el *diagrama de Euler* que es una generalización del anterior. Veremos más tarde en qué se diferencian.

1.2.2. Dos conjuntos distinguidos

En general, cuando hablamos, y me estoy refiriendo al lenguaje cotidiano, solemos tener un contexto, un referencial. Las palabras "los chicos" dichas dentro de una casa suele referirse a "los hijos que viven en esta casa"; si la dice una maestra estará resumiendo "los chicos que tengo por alumnos" y si lo dice una persona de mediana edad estará hablando seguramente de sus compañeros de aventuras. La misma idea de tener un contexto, un universo de referencia que ayude a simplificar las descripciones, también es válida en matemática y así definimos el *conjunto universal* o simplemente *Universo* que

representamos con $\mathcal{U}$.
En algunos textos se puede encontrar este conjunto representado por $\mathcal{I}$, pero he preferido la notación $\mathcal{U}$ porque se asocia más con la idea de universo.

La contrapartida de un conjunto que "lo contiene todo" es el conjunto que "no tiene nada" y, naturalmente, denominaremos *conjunto vacío* y lo notaremos $\emptyset$ o bien $\{\}$. La primera de estas notaciones es simplemente un diagrama de Venn tachado, indicando que dentro de la curva cerrada no puede haber ningún elemento. La segunda representación es claramente su descripción por extensión: están las dos llaves, y no hay nada entre ellas. El conjunto vacío también se puede representar por comprensión mediante la descripción de una situación imposible, por ejemplo "ser un humano con clorofila en las venas".

Ejemplo 1.2 $\emptyset = \{\} = \{x : x \in \mathbb{N}, x < 0\}$

1.3. Relaciones entre conjuntos

Definido un nuevo objeto matemático urge analizar la relación de igualdad. Para llegar a ello, comencemos con la siguiente definición:

Definición 1.2 Dados dos conjuntos A y B, claramente referidos al mismo universo, diremos que A *está incluído* en B o que A *está contenido* en B y escribiremos $A \subset B$ si todo elemento de A también es elemento de B. En símbolos:

$$A \subset B \text{ si } x \in A \text{ implica } x \in B.$$

Es claro que si $A \subset B$, entonces $|A| < |B|$, pero cuando escribimos $<$ entre números estamos asegurando que el de la izquierda es realmente más chico que el de la derecha del signo. En verdad entre conjuntos la idea es la misma. Al escribir $A \subset B$ estamos indicando que A está *incluido estrictamente* en B, es decir que todo elemento de A también está en B y existe algún elemento de B que no está en A. Cuando no se trata de inclusión estricta escribimos $A \subseteq B$.

Proposición 1.1 *(Propiedades de la relación de inclusión)*

$\subseteq_1$: $A \subseteq A$ *(propiedad reflexiva)*

$\subseteq_2$: *Si* $A \subseteq B$ *y* $B \subseteq C$ *entonces* $A \subseteq C$ *(propiedad transitiva)*

Demostración:

$\subseteq_1$: Para probar $A \subseteq A$ tenemos que ver que todo elemento x que esté en A también está en A, lo cual es trivial. □

$\subseteq_2$: Cada vez que tenemos que demostrar algo enunciado en la forma "si ... entonces ..." (*if ... then*) lo que está escrito entre ambas palabras ("si" y "entonces") es la *hipótesis*, es decir *lo que sabemos y tenemos que usar en la demostración* y lo que está escrito después del "entonces" es la *tesis* es decir, *lo que tenemos que probar*.

En este caso tenemos que probar que $A \subseteq C$ y sabemos:
$A \subseteq B$ que es lo mismo que: si $x \in A$ entonces $x \in B$, (1)
y $B \subseteq C$ que es lo mismo que: si $x \in B$ entonces $x \in C$. (2)
Tenemos que probar que todo elemento x de A es un elemento de C, entonces la demostración comienza:
Sea $x \in A$,
por (1) afirmamos que $x \in B$
y por (2) afirmamos que $x \in C$.

□

Definición 1.3 Dados dos conjuntos A y B decimos que $A = B$ si tienen exactamente los mismos elementos, es decir si todo elemento de A es elemento de B y todo elemento de B es elemento de A. En símbolos:

$$A = B \text{ si y sólo si } A \subseteq B \text{ y } B \subseteq A.$$

Ejemplo 1.3 Veamos algunos ejemplos de inclusiones entre conjuntos:

1. $A \subseteq \mathcal{U}$ cualquiera que sea el conjunto A, ya que por definición $\mathcal{U}$ es el conjunto marco o contexto, es nuestro universo.
2. $\emptyset \subseteq A$, cualquiera que sea el conjunto A. Para demostrar esto hay que probar que todo x que está en $\emptyset$ está en A, o, lo que es lo mismo (ley contrapositiva) los elementos que no están en A no están en $\emptyset$. Trivial.
3. $\mathbb{P} \subset \mathbb{N}$, donde $\mathbb{P}$ es el conjunto de los números naturales pares y $\mathbb{N}$ el conjunto de los números naturales.
4. $(-1, 1) \subset \mathbb{R}$, donde $\mathbb{R}$ es el conjunto de los número reales.
5. $\{a, e, o\} \subset \{x : x \text{ es una vocal castellana}\}$
6. $\{a, e, i, o, u\} \subseteq \{x : x \text{ es una vocal castellana}\}$

Definición 1.4 Dados dos conjuntos tales que $A \subseteq B$ decimos que A es un *subconjunto* de B. Si $A \subset B$ A se dice un *subconjunto propio*. Los *subconjuntos triviales* de B son $\emptyset$ y el propio B.

1.3.1. Partes de un conjunto

Definición 1.5 Dado un conjunto A definimos el conjunto de *partes de* A y lo notamos $\mathbb{P}(A)$ al conjunto de todos los subconjuntos posibles de A.
En símbolos:

$$\mathbb{P}(A) = \{X : X \subseteq A\}.$$

Ejemplo 1.4 Sea $A = \{1, 2\}$, como $|A| = 2$, es decir, tiene 2 elementos, sus subconjuntos tendrán 0, 1, o a lo sumo, 2 elementos.
Con 0 elemento: $\emptyset$,
con 1 elemento $\{1\}$, $\{2\}$
con 2 elementos, el propio A, entonces:

$$\text{Si } A = \{1, 2\} \text{ resulta } \mathbb{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}.$$

(♣) ¿Existe algún conjunto A para el que $|\mathbb{P}(A)| = 1$?

Observación 1.3 El conjunto de partes del conjunto A también se suele notar como $\mathbf{2}^A$. Por el momento podemos observar que $|\mathbb{P}(A)| = 2^{|A|}$, cuando hablemos de funciones veremos el por qué de esta notación y cuando trabajemos con números naturales, podremos demostrar la igualdad que por el momento nos parece una feliz coincidencia.

1.4. Operaciones entre conjuntos

1.4.1. Unión de conjuntos

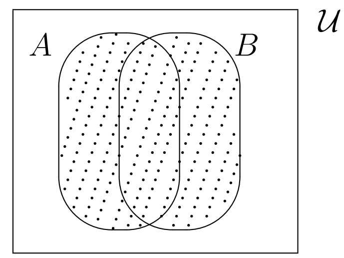
Definición 1.6 Dados dos conjuntos A y B en el mismo universo $\mathcal{U}$, se denomina A *unión* B y se nota $A \cup B$ al conjunto formado por todos los elementos que pertenecen a A o a B.
En símbolos:

$$A \cup B = \{x : x \in A \text{ ó } x \in B\}$$

Ejemplo 1.5 Dados los conjuntos $A = \{1, 2, 3, 4, 5, 10\}$ y $B = \{2, 4, 5, 6, 7, 8, 9\}$ resulta $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Observación 1.4 Ya hemos mencionado que los elementos repetidos en un conjunto cuentan como uno solo. La idea de esta unión es como cuando uno agrega varios archivos en una cierta carpeta. Si algún archivo en particular ya estaba, simplemente lo copia encima. (ahora pienso que en mi última versión en lugar de hacer esto me pone "copia de...", seguramente para no esta preguntando si lo quiero reescribir o no. Bueno, de cualquier modo, la idea es esa.)

El diagrama de Venn de dos conjuntos cualesquiera debe hacerse siempre posibilitando la superposición de parte de los mismos. En el diagrama que se encuentra a la derecha, vemos dos conjuntos A y B, contenidos en un universo $\mathcal{U}$ que usualmente graficamos como un rectángulo y hemos sombreado la unión de ambos.



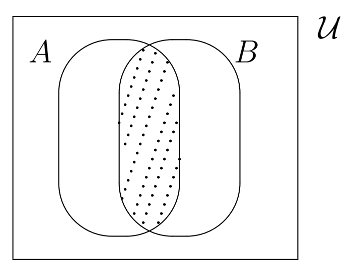
1.4.2. Intersección de conjuntos

Definición 1.7 Dados dos conjuntos A y B en el mismo universo $\mathcal{U}$, se denomina A *intersección* B y se nota $A \cap B$ al conjunto formado por todos los elementos que pertenecen a A y a B simultáneamente.
En símbolos:

$$A \cap B = \{x : x \in A \text{ y } x \in B\}$$

Ejemplo 1.6 Dados los conjuntos $A = \{1, 2, 3, 4, 5, 10\}$ y $B = \{2, 4, 5, 6, 7, 8, 9\}$ resulta $A \cap B = \{2, 4, 5\}$.

Hemos dicho que el diagrama de Venn de dos conjuntos cualesquiera debe hacerse siempre posibilitando la superposición de parte de los mismos, es decir, previendo la posibilidad de una intersección no vacía. En el diagrama que se encuentra a la derecha, vemos dos conjuntos A y B, contenidos en un universo $\mathcal{U}$ y hemos sombreado la intersección de ambos.



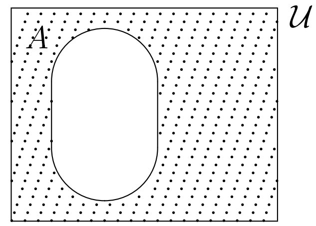
1.4.3. Complemento de un conjunto

Definición 1.8 Dado un conjunto A en el universo $\mathcal{U}$, se denomina *complemento* de A y se nota A' ó $\bar{A}$ al conjunto formado por todos los elementos

que no pertenecen a A.
En símbolos:

$$A' = \{x : x \notin A\}$$

Ejemplo 1.7 Dado el universo $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, sea $A = \{1, 2, 3, 4, 5, 10\}$; resulta entonces $A' = \{6, 7, 8, 9\}$.



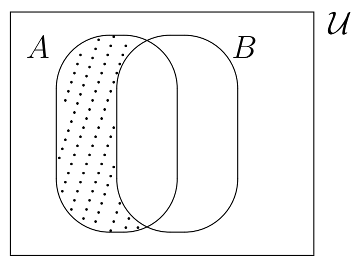
En el diagrama que se encuentra a la derecha, hemos sombreado el complemento del conjunto A.

1.4.4. Diferencia de conjuntos

Definición 1.9 Dados dos conjuntos A y B en el mismo universo $\mathcal{U}$, se denomina A *menos* B y se nota $A \setminus B$ al conjunto formado por todos los elementos que pertenecen a A y no pertenecen a B o, usando las definiciones dadas anteriormente: $A \setminus B = A \cap B'$.
En símbolos:

$$A \setminus B = \{x : x \in A \text{ y } x \notin B\}$$

Ejemplo 1.8 Dados los conjuntos $A = \{1, 2, 3, 4, 5, 10\}$ y $B = \{2, 4, 5, 6, 7, 8, 9\}$ resulta $A \setminus B = \{1, 3, 10\}$.



En el diagrama que se encuentra a la derecha, vemos dos conjuntos A y B, y hemos sombreado la diferencia $A \setminus B$.

Observación 1.5 Dada esta nueva definición podemos considerar $A' = \mathcal{U} \setminus A$. Esta relación hace que suela llamarse a la diferencia de conjuntos el *complemento relativo*. Más específicamente: $A \setminus B = C_A B = B' \cap A$.

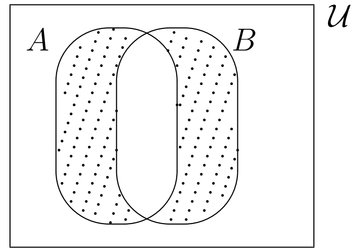
1.4.5. Diferencia simétrica de conjuntos

Definición 1.10 Dados dos conjuntos A y B en el mismo universo $\mathcal{U}$, se denomina *diferencia simétrica de* A *y* B y se nota $A \triangle B$ al conjunto formado por todos los elementos que pertenecen a A y no pertenecen a B o pertenecen a B y no pertenecen a A.
En símbolos:

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

Ejemplo 1.9 Dados los conjuntos $A = \{1, 2, 3, 4, 5, 10\}$ y $B = \{2, 4, 5, 6, 7, 8, 9\}$ resulta $A\triangle B = \{1, 3, 6, 7, 8, 9, 10\}$.

En el diagrama que se encuentra a la derecha, vemos dos conjuntos A y B, y hemos sombreado la diferencia simétrica $A\triangle B$.



1.4.6. Propiedades de las operaciones conjuntistas

Daremos a continuación una lista, claramente no exhaustiva, de las propiedades de las operaciones entre conjuntos. Demostraremos algunas de ellas y dejamos las demostraciones restantes a cargo del lector interesado.®
Antes de comenzar el listado aclaremos que todas las demostraciones deben hacerse usando la definición de igualdad, es decir, la doble inclusión. Entonces cada vez que querramos demostrar que $A = B$ debemos hacerlo en dos pasos: $A \subseteq B$ y $B \subseteq A$, sin importar el orden en que lo hagamos.
Hay ocasiones en que el segundo paso de la demostración es idéntico al primero, pero leído desde el final hacia el principio. Esto ocurre porque en realidad cada "entonces" escrito en la demostración es "si y sólo si", es decir, una equivalencia. En estos casos, se suele escribir al inicio de la demostración "son equivalentes", quitar todos los "entonces" y concluir la igualdad en un sólo paso. (Veremos un caso.)

1. $A \cap (B \cap C) = (A \cap B) \cap C$ propiedad asociativa de la intersección
2. $A \cap B = B \cap A$ propiedad conmutativa de la intersección
3. $A \cap A = A$ propiedad idempotente de la intersección
4. $A \cup (B \cup C) = (A \cup B) \cup C$ propiedad asociativa de la unión
5. $A \cup B = B \cup A$ propiedad conmutativa de la unión
6. $A \cup A = A$ propiedad idempotente de la unión
7. $A \cap (A \cup B) = A$ ley de absorción
8. $A \cup (A \cap B) = A$ ley de absorción
9. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ propiedad distributiva
10. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ propiedad distributiva
11. $A \cap \emptyset = \emptyset, \quad A \cup \emptyset = A$ leyes de $\emptyset$
12. $A \cap \mathcal{U} = A, \quad A \cup \mathcal{U} = \mathcal{U}$ leyes de $\mathcal{U}$

13. $A \cap A' = \emptyset, \quad A \cup A' = \mathcal{U}$ leyes de complemento
14. $(A')' = A$ ley de involución
15. $(A \cap B)' = A' \cup B', \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$ leyes de De Morgan
16. $A \triangle B = (A \cup B) \setminus (A \cap B)$

Demostración:

1. $A \cap (B \cap C) = (A \cap B) \cap C$

   a) $A \cap (B \cap C) \subseteq (A \cap B) \cap C$
   Sea $x \in A \cap (B \cap C)$, entonces $x \in A$ y $x \in B \cap C$, entonces $x \in A$ y $x \in B$ y $x \in C$, entonces $x \in A \cap B$ y $x \in C$, entonces $x \in (A \cap B) \cap C$.

   b) $(A \cap B) \cap C \subseteq A \cap (B \cap C)$
   Sea $x \in (A \cap B) \cap C$, entonces $x \in A \cap B$ y $x \in C$, entonces $x \in A$ y $x \in B$ y $x \in C$, entonces $x \in A$ y $x \in B \cap C$, entonces $x \in A \cap (B \cap C)$. $\square$

   Éste es un claro caso en que el paso 2 es el paso 1 "en reversa". Reescribamos la demostración:
   Son equivalentes:

   $x \in A \cap (B \cap C)$,
   $x \in A$ y $x \in B \cap C$,
   $x \in A$ y $x \in B$ y $x \in C$,
   $x \in A \cap B$ y $x \in C$,
   $x \in (A \cap B) \cap C$.

   De donde concluimos: $A \cap (B \cap C) = (A \cap B) \cap C$. $\square$

7. $A \cap (A \cup B) = A$

   a) $A \cap (A \cup B) \subseteq A$ se verifica por definición de intersección.

   b) $A \subseteq A \cap (A \cup B)$
   Sea $x \in A$, es claro que si x es un elemento de A, es también un elemento de A unido cualquier otro conjunto, en especial $x \in A \cup B$, por lo tanto $x \in A \cap (A \cup B)$. $\square$

11. $A \cap \emptyset = \emptyset$

   Cuando debemos probar que un determinado conjunto es vacío normalmente suponemos lo contrario y llegamos a un absurdo. Supongamos, entones que existe un elemento en $A \cap \emptyset$.
   Sea $x \in A \cap \emptyset$, entonces $x \in A$ y $x \in \emptyset$, lo cual es un absurdo, que provino de suponer que $A \cap \emptyset \neq \emptyset$, por lo tanto $A \cap \emptyset = \emptyset$. $\square$

12. $A \cup \mathcal{U} = \mathcal{U}$

    a) $A \cup \mathcal{U} \subseteq \mathcal{U}$ por la definición de conjunto universal.

    b) $\mathcal{U} \subseteq A \cup \mathcal{U}$ por la definición de unión. $\square$

13. $A \cap A' = \emptyset, \quad A \cup A' = \mathcal{U}$

    a) $A \cap A' = \emptyset$
    Como dijimos en el caso anterior, sea $x \in A \cap A'$, entonces $x \in A$ y $x \in A'$, es decir $x \in A$ y $x \notin A$, lo cual es un absurdo que provino de suponer que $A \cap A' \neq \emptyset$, entonces $A \cap A' = \emptyset$. $\square$

    b) $A \cup A' = \mathcal{U}$
    Sea $x \in \mathcal{U}$, existen dos posibilidades:

    caso 1: $x \in A$, entonces x pertenece a A unido cualquier otra cosa, en especial $x \in A \cup A'$.

    caso 2: $x \notin A$, entonces x pertenece a A' , entonces x pertenece a A' unido cualquier otra cosa, en especial $x \in A \cup A'$.

    En cualquier caso $x \in A \cup A'$, por lo tanto $A \cup A' = \mathcal{U}$. $\square$

15. $(A \cap B)' = A' \cup B'$

    a) $(A \cap B)' \subseteq A' \cup B'$
    Sea $x \in (A \cap B)'$, entonces $x \notin (A \cap B)$, entonces $x \notin A$ o $x \notin B$.

    caso 1: Si $x \notin A$ entonces $x \in A'$ y, en consecuencia $x \in A' \cup B'$.

    caso 2: Si $x \notin B$ entonces $x \in B'$ y por lo tanto $x \in A' \cup B'$.

    En cualquier caso, $x \in A' \cup B'$.

    b) $A' \cup B' \subseteq (A \cap B)'$
    Sea $x \in A' \cup B'$, entonces $x \in A'$ o $x \in B'$.

    caso 1: $x \in A'$, resulta $x \notin A$ entonces $x \notin A \cap B$, es decir $x \in (A \cap B)'$.

    caso 2: $x \in B'$, entonces $x \notin B$ entonces $x \notin (A \cap B)$ y por lo tanto $x \in (A \cap B)'$.

    En cualquier caso, $x \in (A \cap B)'$. $\square$

El resto de las demostraciones queda a cargo del estimado lector.®

1.5. Ejemplos de demostraciones

Hemos hecho demostraciones de propiedades de conjuntos sin utilizar hipótesis adicionales. Veamos cómo realizar demostraciones del tipo:

1. Si $A \subseteq C$ y $B \subseteq C$, entonces $A \cup B \subseteq C$.
   Dijimos que $A \subseteq C$ y $B \subseteq C$ son las hipótesis, es decir lo que sabemos y

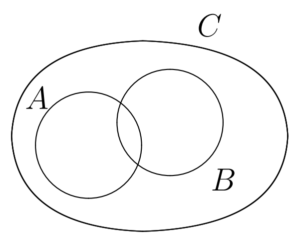
tenemos que usar dentro de la demostración. Lo que tenemos que probar es $A \cup B \subseteq C$, es decir que todo elemento de $A \cup B$ es también elemento de C.
Demostración: Sea $x \in A \cup B$. Puede ser que $x \in A$ o $x \in B$

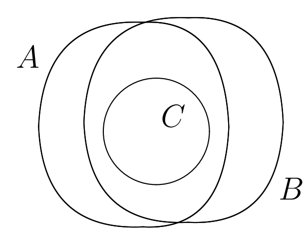
caso 1: Si $x \in A$, como $A \subseteq C$ resulta $x \in C$.
caso 2: Si $x \in B$, como $B \subseteq C$ resulta $x \in C$.

En cualquier caso $x \in C$. □

2. Si $A \subseteq B$ y $A \subseteq C$, entonces $A \subseteq (B \cap C)$.
$A \subseteq B$ y $A \subseteq C$ son las hipótesis, es decir lo que sabemos y tenemos que usar dentro de la demostración. Lo que tenemos que probar es $A \subseteq (B \cap C)$, es decir que todo elemento de A es también elemento de $B \cap C$.
Demostración: Sea $x \in A$. Como $A \subseteq B$ resulta $x \in B$ y como $A \subseteq C$ resulta $x \in C$, en consecuencia $x \in B \cap C$. □

Hemos mencionado los diagramas de Venn y de Venn-Euler. Esta es una oportunidad de mostrar la diferencia. En un diagrama de Venn se debe graficar de la forma más general posible. Es decir, si se pide el gráfico de dos conjuntos, debe hacerse como si la intersección fuera no vacía. En el caso de un diagrama de Euler, se grafica exactactamente la situación y se puede utilizar como demostración. (No en este curso.)
Veamos los diagramas de las demostraciones 1.5





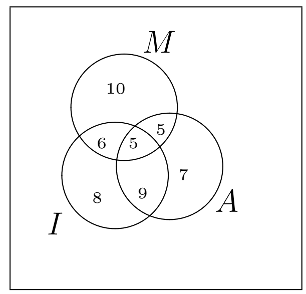
1.5.1. Demostraciones por cálculo directo

Una vez que hemos probado las propiedades básicas, muchas otras pueden ser demostradas haciendo uso de ellas, por un método llamado *cálculo directo*. Probemos, por ejemplo $(A \cup B)' = A' \cap B'$. Haciendo este tipo de demostraciones debemos partir de un lado del igual hasta llegar a otro, pero NUNCA llevar la igualdad. En general partimos del lado del igual "con más cosas" y escribimos sobre cada igualdad una referencia a la propiedad que utilizamos. En este caso, yo usaré el número que le corresponde en la lista anterior.

$A' \cap B' \overset{14}{=} ((A' \cap B')')' \overset{15}{=} ((A')' \cup (B')')' \overset{14}{=} (A \cup B)'$. □

1.6. Problemas de conteo

Vamos a analizar una situación real: En una institución educacional van dar becas para diferentes cursos. En total pueden becar a 50 personas y los cursos que brindan son: conversación en inglés, tácticas de mercadeo y asesoramiento legal. Seleccionan entre los interesados a las 50 personas de mayor rendimiento educacional y les entregan fichas para seleccionar los cursos. Una vez hecho el listado de los cursos, la secretaria del colegio encontró 28 anotados para el curso de inglés, 26 para el de mercadeo y también 26 para el de asesoramiento. Al sumar la cantidad de nombres dijo asustada a la directora: "Metimos la pata: 28+26+26 son 80. ¿Cómo fue que nos pasamos?". La directora le contestó: "Esperá, yo tengo una amiga matemática que me contó justo ayer cómo resolver esto."
Y ahora les voy a explicar a ustedes cómo hacerlo.
De los 50 estudiantes 5 se anotaron en los 3 cursos, 11 en inglés y mercadeo, 10 en mercadeo y asesoramiento y 14 en inglés y asesoramiento.
Claramente el conjunto de los que anotados en inglés y mercadeo incluye al conjunto de los anotados en los tres cursos, entonces la cantidad de estudiantes anotados inglés y mercadeo pero no en asesoramiento legal es: $11 - 5 = 6$. Con el mismo razonamiento los que están anotados solamente en mercadeo son 10.



Llamemos A al conjunto de estudiantes que harán el curso de asesoramiento, I al de los que estudiarán inglés y M a los de mercadeo. Si hacemos un diagrama de Venn de estos tres conjuntos, podemos colocar en cada zona la cantidad de estudiantes que corresponde. Finalmente, si sumamos todos los números, el universo tiene 50 estudiantes.

1.7. Ejercicios propuestos

Ejercicio 1.1 Expresar, en caso de ser posible, los siguientes conjuntos por extensión:

1. $A = \{x : x \in \mathbb{N},\ 2 \leq x < 3\}$
2. $A = \{x : x \in \mathbb{Z},\ \sqrt{x} \in \mathbb{Z} \text{ y } x \leq 100\}$
3. $A = \{x : x \in \mathbb{N},\ x = 2n + 1, n \in \mathbb{N}\}$
4. $A = \{x : x \in \mathbb{N},\ x \text{ divide a } 4\}$

5. $A = \{x : x \in \mathbb{Z},\, x \text{ divide a } 4\}$
6. $A = \{x : x \in \mathbb{R},\, x \text{ divide a } 4\}$

Ejercicio 1.2 Definir simbólicamente los siguientes conjuntos:
(es decir, expresarlos por comprensión).

1. Números reales de cuadrado par.
2. Números naturales impares mayores que 10.
3. Las raíces de la parábola $\mathcal{P} : x^2 - x - 6$.

Ejercicio 1.3 Dados los siguientes conjuntos, decidir si $A_i = A_j$

1. A_1: conjunto de las vocales
2. $A_2 = \{\, a,\, e,\, i,\, o,\, u\,\}$
3. $A_3 = \{\{\, a,\, e,\, i,\, o,\, u\,\}\}$
4. $A_4 = \{\, \emptyset,\, a,\, e,\, i,\, o,\, u\,\}$
5. $A_5 = \{x : x \text{ es una vocal}\}$
6. $A_6 = \{\text{el conjunto de las vocales}\}$
7. $A_7 = \{\, \{a\},\, \{e\},\, \{i\},\, \{o\},\, \{u\}\,\}$
8. $A_8 = \{\, a,\, a,\, e,\, e,\, i,\, i,\, i,\, o,\, u,\, u\,\}$
9. $A_9 = \{\, \{x\} : x \text{ es vocal del alfabeto castellano}\,\}$

Ejercicio 1.4 Dados los siguientes conjuntos analizar la cantidad de elementos (el orden) de cada uno:

1. $\emptyset$
2. $\{\,\}$
3. $\{\emptyset\}$
4. $\{\{\emptyset\}\}$
5. $\{\emptyset, \{\emptyset\}\}$
6. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

Ejercicio 1.5 Decidir si las siguientes proposiciones son verdaderas o falsas:

1. $x \in \{x\}$
2. $x \subseteq \{x\}$
3. $\{x\} \in \{x\}$
4. $\{x\} \subseteq \{x\}$
5. $\emptyset \in \{x\}$
6. $\emptyset \subseteq \{x\}$
7. $\{x\} \in \{x, \emptyset, \{x\}\}$
8. $x \in \{x, \emptyset, \{x\}\}$

Ejercicio 1.6 Hallar $\mathbb{P}(A)$ si:

1. $A = \{a, b, c\}$
2. $(\diamond)$ $A = \{a, b, c, d\}$

Ejercicio 1.7 Sean

$\mathcal{U} = \{x : x \in \mathbb{Z}, |x| < 8\}$,

$A = \{x : x \in \mathcal{U}, x \text{ es par }\}$,

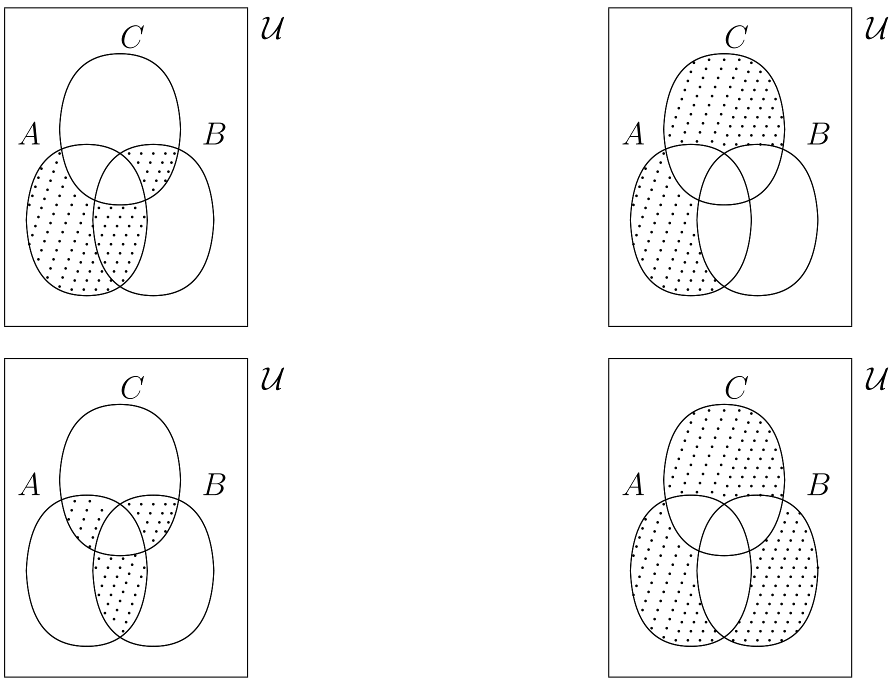
$B = \{x : x \in \mathcal{U}, x \text{ es múltiplo de } 4\}$,

$C = \{x : x \in \mathcal{U}, x \text{ es positivo y } x > 4\}$.

Hallar:

1. $A \cap (B \cup C)$
2. $B \setminus A, \ A \setminus B$
3. $A' \cap B', \ (A \cup B)'$

Ejercicio 1.8 Encontrar fórmulas que describan las partes rayadas de los diagramas de Venn-Euler, utilizando únicamente intersecciones, uniones y complementos:



Ejercicio 1.9 En una reunión de estudiantes de ciencias de la computación en la que participan 110 personas, se dictan tres seminarios de interés A : *La computadora como nuevo psicoanalista*, B : *De la máquina de Turing a la supercomutadora* y C : *Experiencias virtuales*. Al finalizar el encuentro, se hizo una encuesta, por la cual se averiguaron las siguientes cifras: 63 se inscribieron en A, 30 en B y 50 en C. Se sabe que 7 tomaron los tres seminarios, 30 sólo el A, 13 sólo el B y 25 sólo el C. Determinar:

1. ¿Cuántos estudiantes toman A y B, pero no C?
2. ¿Cuántos estudiantes toman B y C, pero no A?

3. ¿Cuántos estudiantes toman A y C, pero no B?
4. ¿Cuántos estudiantes no toman ningún seminario?
5. ¿Cuántos estudiantes toman exactamente un seminario?
6. ¿Cuántos estudiantes toman a lo sumo dos seminarios?
7. ¿Cuántos estudiantes toman exactamente dos seminarios?
8. ¿Cuántos estudiantes toman por lo menos dos seminarios?

Ejercicio 1.10 (♣) Sin tiempo para la escuela.
"Pero no tengo tiempo para la escuela"-explicaba Eddie-"Duermo 8 horas diarias, que, sumadas, dan 122 días por año, suponiendo que cada día es de 24 horas. No hay clases los sábados ni los domingos, que suman 104 días por año. Tenemos 60 días de vacaciones de verano. Necesito 3 horas diarias para comer. Esto es más de 45 días al año. Y necesito, al menos, 2 horas diarias de recreación... que suman más de 30 días al año." Mientras hablaba, Eddie sumó todas estas cifras: $122 + 104 + 60 + 56 + 30 = 361$ días. "Ya ve" -continuó Eddie- "Eso me deja tan sólo 4 días para estar enfermo y en cama y ni siquera he tomado en cuenta los 7 feriados escolares de cada año".
¿Dónde está el error en los cálculos de Eddie?

Ejercicio 1.11 (♣) Una fiesta familiar congregaba a 1 abuelo, 1 abuela, dos padres, 2 madres, 3 nietos, 1 hermano, 2 hermanas, 2 hijos varones, 2 hijas mujeres, 1 suegro 1 suegra y una nuera. ¿Veintitrés personas? No. Sólo había 7 presentes. ¿Cómo es posible?

Ejercicio 1.12 Demostrar por definición y por cálculo directo:

1. Si $A \subseteq C,\ B \subseteq C$, entonces $A \cup B \subseteq C$.
2. ($\diamond$) Si $C \subseteq A,\ C \subseteq B$, entonces $C \subseteq A \cap B$.
3. $A \subseteq B$ si y sólo si $A \cap B = A$.
4. ($\diamond$) $A \subseteq B$ si y sólo si $B' \subseteq A'$.

Ejercicio 1.13 (©) Sea $\mathcal{U}$ un conjunto universal y A, B, C tres subconjuntos. Demostrar las siguientes igualdades, por doble inclusión:

1. $A \cap (B \cap C) = (A \cap B) \cap C$ propiedad asociativa de la intersección
2. $A \cap B = B \cap A$ propiedad conmutativa de la intersección
3. $A \cap A = A$ propiedad idempotente de la intersección

4. $A \cup (B \cup C) = (A \cup B) \cup C$ — propiedad asociativa de la unión
5. $A \cup B = B \cup A$ — propiedad conmutativa de la unión
6. $A \cup A = A$ — propiedad idempotente de la unión
7. $A \cap (A \cup B) = A$ — ley de absorción
8. $A \cup (A \cap B) = A$ — ley de absorción
9. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ — propiedad distributiva
10. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ — propiedad distributiva
11. $A \cap \emptyset = \emptyset, \quad A \cup \emptyset = A$ — leyes de $\emptyset$
12. $A \cap \mathcal{U} = A, \quad A \cup \mathcal{U} = \mathcal{U}$ — leyes de $\mathcal{U}$
13. $A \cap A' = \emptyset, \quad A \cup A' = \mathcal{U}$ — leyes de complemento
14. $(A')' = A$ — ley de involución
15. $(A \cap B)' = A' \cup B', \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$ — leyes de De Morgan

Ejercicio 1.14 Sea $\mathcal{U}$ un conjunto universal y A, B, C tres subconjuntos. Demostrar por cálculo directo:

1. $A \setminus (A \cap B) = A \setminus B$
2. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
3. $(A \setminus B) \setminus (A \setminus C) = A \cap (C \setminus B)$

Ejercicio 1.15 ($\diamond$) Resolver por cálculo directo:

1. $A \subseteq B$, $C \subseteq D$, entonces $(A \cap C) \subseteq (B \cup D)$.
2. $A \subseteq C$, $B \subseteq C$, entonces $(A \cup B) \subseteq C$.

Capítulo 2

Relaciones binarias

Producto cartesiano de conjuntos. Relaciones binarias. Propiedades. Relaciones de equivalencia. Partición de un conjunto. Partición inducida por una relación de equivalencia. Clases de equivalencia. Conjunto cociente.

2.1. Motivación

En el quinto piso de un edificio de estudiantes hay dos departamentos. En el departamento A viven Agustín, Bernardo y Claudio y en el departamento B viven Ximena, Yamile y Zoe. Como cursan materias coincidentes suelen estudiar juntos: Agustín con Ximena, Agustín con Yamile, Bernardo con Yamile, Bernardo con Zoe y Claudio con Zoe.
Para describir esta situación de un modo más esquemático, digamos, podemos escribir cada pareja de estudio poniendo los nombres separados por comas y unidos por paréntesis, del siguiente modo:
(Agustín,Ximena), (Agustín,Yamile), (Bernardo,Yamile), (Bernardo,Zoe), (Claudio,Zoe).

El siguiente paso de minimización de escritura es considerar cada departamento como un conjunto, notar a cada habitante por su inicial minúscula y llamar $\mathcal{R}$ a la relación "estudia con". Resulta, entonces:

$$A = \{a, b, c\},\ B = \{x, y, z\},\ \mathcal{R} = \{(a, x), (a, y), (b, y), (b, z), (c, z)\}.$$

Esta situación motiva claramente las definiciones de *producto cartesiano de conjuntos* y *relaciones binarias*.

2.2. Producto cartesiano de conjuntos

Definición 2.1 Dados dos conjuntos A y B se denomina *producto cartesiano de* A y B y se nota $A \times B$ al conjunto:

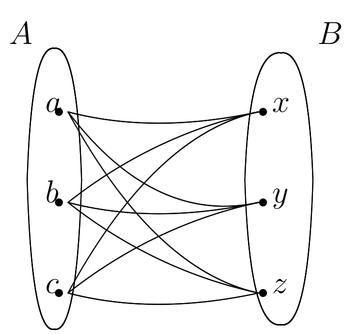
$$A \times B = \{(x, y) : x \in A, y \in B\}$$

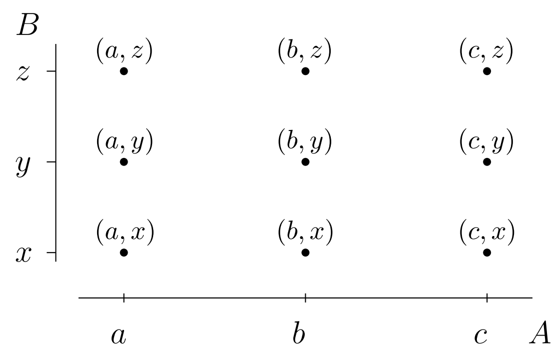
llamaremos *par ordenado* a cada $(x, y) \in A \times B$, *primera coordenada* a la x y *segunda coordenada* a la y. Dos pares ordenados (a, b), (c, d) son *iguales* si son iguales coordenada a coordenada, es decir si $a = c$, $b = d$.

Si tomamos los departamentos de la sección anterior como ejemplo, resulta:

$$A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\}$$

Una posible representación gráfica es utilizando diagramas de Venn y otra, tal vez más clara, que es la idea de la representación cartesiana del plano:





En el diagama de la derecha hemos graficado un “eje horizontal” en el que marcamos los elementos del conjunto A y un “eje vertical” donde marcamos los elementos del conjunto B. Como los elementos dentro de un conjunto no tienen un orden predeterminado, es muy importante en este tipo de representación marcar estos elementos.

El producto cartesiano de conjuntos puede combinarse con las operaciones que hemos visto hasta el momento y se verifican las siguiente propiedades distributivas:

Proposición 2.1 *Dados tres conjuntos no vacíos* A, B, C, *se verifica:*

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2. $A \cup (B \times C) = (A \cup B) \times (A \cup C)$

3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
4. $A \cap (B \times C) = (A \cap B) \times (A \cap C)$

Demostración: Ejercicio para el lector.®

2.3. Relaciones binarias

Definición 2.2 Dados dos conjuntos no vacíos A y B, una *relación binaria* $\mathcal{R}$ es cualquier subconjunto del producto $A \times B$. Si un elemento $a \in A$ está en relación con un elemento $b \in B$ podemos escribir $(a, b) \in \mathcal{R}$ o bien $a\mathcal{R}b$.

Observación 2.1 Acabamos de decir que si un elemento $a \in A$ está en relación con un elemento $b \in B$ podemos escribir $(a, b) \in \mathcal{R}$ o bien $a\mathcal{R}b$. Esta segunda forma, si bien parece más extraña es la que hemos usado desde siempre. Por ejemplo si queremos representar "3 es menor o igual que 4" escribimos $3 \leq 4$ mucho más naturalmente que $(3, 4) \in \leq$.

Llamamos *conjunto de salida* al conjunto A, *conjunto de llegada* o *rango* al conjunto B, *dominio* de la relación y lo notamos $Dom\mathcal{R}$ subcojunto del conjunto de salida conformado por las primeras coordenadas de la relación, análogamente llamamos *imagen* de la relación y notamos $Im\mathcal{R}$ al subconjunto del rango conformado por las segundas coordenadas. En símbolos:

$$Dom\mathcal{R} = \{x \in A : (x, y) \in \mathcal{R} \text{ para algún } y \in B\} \subseteq A$$

$$Im\mathcal{R} = \{y \in B : (x, y) \in \mathcal{R} \text{ para algún } x \in A\} \subseteq B$$

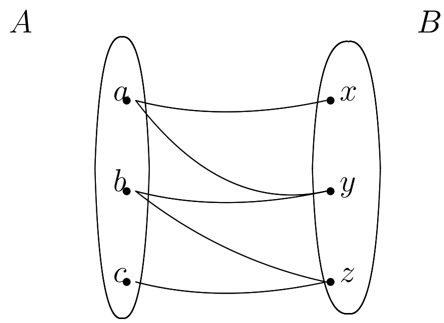
También podemos hablar de la *imagen* de $x \in A$ por $\mathcal{R}$, que notamos $\mathcal{R}(x)$ y la *preimagen* de $y \in B$ por $\mathcal{R}$ que notamos $\mathcal{R}^{-1}(y)$, descriptos por los siguientes conjuntos:

$$\mathcal{R}(x) = \{y \in B : (x, y) \in \mathcal{R}\}, \quad \mathcal{R}^{-1}(y) = \{x \in A : (x, y) \in \mathcal{R}\}$$

Si continuamos con nuestros amigos estudiantes, podemos escribir:

$$A = \{a, b, c\},\ B = \{x, y, z\},\ \mathcal{R} = \{(a, x), (a, y), (b, y), (b, z), (c, z)\}$$

$$Dom\mathcal{R} = \{a, b, c\} = A,\ Im\mathcal{R} = \{x, y, z\} = B$$



$$\begin{array}{ll} \mathcal{R}(a) = \{x, y\} & \mathcal{R}^{-1}(x) = \{a\} \\ \mathcal{R}(b) = \{y, z\} & \mathcal{R}^{-1}(y) = \{a, b\} \\ \mathcal{R}(c) = \{z\} & \mathcal{R}^{-1}(z) = \{c\} \end{array}$$

Veamos otro ejemplo:

Ejemplo 2.1 $A_1 = \{a, b, c, d\}, B_1 = \{1, 2, 3, 4, 5\},\ \mathcal{R}_1 = \{(a, 1), (a, 3), (a, 5), (c, 2)(c, 3)\}$

$$Dom\mathcal{R}_1 = \{a, c\} \subset A_1,\ Im\mathcal{R}_1 = \{1, 2, 3, 5\} \subset B_1$$

Definición 2.3 Dada una relación $\mathcal{R}$ definida de A en B, se define la *relación opuesta* y se nota $\mathcal{R}^{op}$ de B en A a la relación definida por

$$\mathcal{R}^{op} = \{(x, y) : (y, x) \in \mathcal{R}\}$$

Volviendo a nuestros amigos estudiantes:

$$\mathcal{R}^{op} = \{(x, a), (y, a), (y, b), (z, b), (z, c)\}$$

2.3.1. Operaciones entre relaciones

Dado que las relaciones son conjuntos, se puede efectuar entre relaciones todas las operaciones conjuntistas, si es que son factibles. Es decir, Si $\mathcal{R}$ y $\mathcal{S}$ son ambas relaciones de A en B podemos realizar la unión, intersección y el complemento relativo entre ellas.
Por ejemplo:
$A = \{1, 2, 3, 4\},\ B = \{a, e, i, o, u\},$
$\mathcal{R} = \{(1, a), (1, e), (3, o), (4, o)\},\ \mathcal{S} = \{(1, a), (2, e), (3, i), (4, o)\}$

$$\mathcal{R} \cup \mathcal{S} = \{(1, a), (1, e), (2, e), (3, i), (3, o), (4, o)\}$$
$$\mathcal{R} \cap \mathcal{S} = \{(1, a)(4, o)\}$$
$$\mathcal{R} \setminus \mathcal{S} = \{(1, e), (3, o)\}$$
$$\begin{aligned} \mathcal{R}' = \{&(1, i), (1, o), (1, u), (2, 1), (2, e), (2, i), (2, o), (2, u), \\ &(3, a), (3, e), (3, i), (3, u), (4, a), (4, e), (4, i), (4, u)\} \end{aligned}$$

Una nueva operación entre relaciones es la composición.

Definición 2.4 Si $\mathcal{R} \subseteq A \times B$ y $\mathcal{S} \subseteq B \times C$ se define la composición de $\mathcal{R}$ y $\mathcal{S}$ y se nota $\mathcal{S} \circ \mathcal{R}$ al conjunto:

$$\mathcal{S} \circ \mathcal{R} = \{(x, y) : \text{ existe } z \in B : (x, z) \in \mathcal{R},\ (z, y) \in \mathcal{S}\} \subseteq A \times C.$$

Es fácil ver que $Dom\mathcal{S} \circ \mathcal{R} \subseteq Dom\mathcal{R}$ y $Im\mathcal{S} \circ \mathcal{R} \subseteq Im\mathcal{S}$.
Demostremos la primera de estas afirmaciones: $Dom\mathcal{S} \circ \mathcal{R} \subseteq Dom\mathcal{R}$

Demostración:

$$Dom\mathcal{S} \circ \mathcal{R} \overset{def.Dom}{=} \{x \in A : \text{ existe } y \in C : (x, y) \in \mathcal{S} \circ \mathcal{R}\} \overset{def.\circ}{=}$$

$$\overset{def.\circ}{=} \{x \in A : \text{ existe } y \in C : \text{ existe } z \in B : (x, z) \in \mathcal{R}, (z, y) \in \mathcal{S}\} \subseteq$$

$$\subseteq \{x \in A : \text{ existe } z \in B : (x, z) \in \mathcal{R}\} \overset{def.Dom}{=} Dom\mathcal{R}. \qquad \square$$

La demostración de la segunda afirmación queda a cargo del lector.®

Veamos un ejemplo de composición de relaciones.

Ejemplo 2.2 Consideremos:

$$A = \{a, b, c\},\ B = \{x, y, z\},\ C = \{m, n, p\} \text{ y}$$

$\mathcal{R} = \{(a, y), (a, z), (b, x), (c, x)\} \subseteq A \times B,\ \mathcal{S} = \{(x, n), (x, p), (z, m)\} \subseteq B \times C,$

Entonces

$$\mathcal{S} \circ \mathcal{R} = \{(a, m), (b, n), (b, p), (c, n), (c, p)\} \subseteq A \times C$$

Analicemos este resultado:

$(a, m) \in \mathcal{S} \circ \mathcal{R}$ por el *link* $z \in B$ que hace $(a, z) \in \mathcal{R}$ y $(z, m) \in \mathcal{S}$,
$(b, n) \in \mathcal{S} \circ \mathcal{R}$ por el *link* $x \in B$ que hace $(b, x) \in \mathcal{R}$ y $(x, n) \in \mathcal{S}$,
$(b, p) \in \mathcal{S} \circ \mathcal{R}$ por el *link* $x \in B$ que hace $(b, x) \in \mathcal{R}$ y $(x, p) \in \mathcal{S}$,
$(c, n) \in \mathcal{S} \circ \mathcal{R}$ por el *link* $x \in B$ que hace $(c, x) \in \mathcal{R}$ y $(x, n) \in \mathcal{S}$.
$(c, p) \in \mathcal{S} \circ \mathcal{R}$ por el *link* $x \in B$ que hace $(c, x) \in \mathcal{R}$ y $(x, p) \in \mathcal{S}$.

Proposición 2.2 Dadas las relaciones $\mathcal{R}, \mathcal{S}$, toda vez que sea posible realizar las operaciones, se verifican las igualdades:

1. $(\mathcal{R}^{op})^{op} = \mathcal{R}$,
2. $(\mathcal{R} \cup \mathcal{S})^{op} = \mathcal{R}^{op} \cup \mathcal{S}^{op}$,
3. $(\mathcal{R} \cap \mathcal{S})^{op} = \mathcal{R}^{op} \cap \mathcal{S}^{op}$,
4. $(\mathcal{R} \circ \mathcal{S})^{op} = \mathcal{S}^{op} \circ \mathcal{R}^{op}$.

Demostración: La demostración queda a cargo del lector interesado.®

2.3.2. Relaciones en un conjunto

Si una relación $\mathcal{R} \subseteq A \times A$ se dice que $\mathcal{R}$ es una relación en A. Notamos $Rel(A)$ al conjunto de todas las relaciones en A y escribimos $\mathcal{R} \in Rel(A)$.
Se dice que $\mathcal{R} \in Rel(A)$ cumple con la propiedad:

1. *Reflexiva*: Si $x\mathcal{R}x$ para todo $x \in A$.
2. *Simétrica*: Si $x\mathcal{R}y$ entonces $y\mathcal{R}x$.
3. *Antisimétrica*: Si $x\mathcal{R}y$ e $y\mathcal{R}x$ implica $x = y$ ó Si $x \neq y$ y $x\mathcal{R}y$ entonces $y\not\mathcal{R}x$.
4. *Transitiva*: Si $x\mathcal{R}y$ e $y\mathcal{R}z$ entonces $x\mathcal{R}z$.

Es fácil ver que una relación es reflexiva si y solamente si contiene a la relación identidad. Es decir,

$$\mathcal{R} \in Rel(A),\ \mathcal{R} \text{ es reflexiva } \textit{sii } 1_A \subseteq \mathcal{R}.$$

Decir esto es afirmar que $1_A \subseteq \mathcal{R}$ caracteriza la propiedad reflexiva de $\mathcal{R}$.

Demostración:

($\Rightarrow$) Sabemos que $\mathcal{R}$ es reflexiva y queremos probar que $1_A \subseteq \mathcal{R}$. Sea $(x, x) \in 1_A$, como $x \in A$ y $\mathcal{R}$ reflexiva el par $(x, x) \in \mathcal{R}$. (Acabamos de ver que todo elemento de 1_A es elemento de $\mathcal{R}$.)

($\Leftarrow$) Sabemos que $1_A \subseteq \mathcal{R}$ y queremos probar que $\mathcal{R}$ es reflexiva. Sea $x \in A$, Por definición de identidad $(x, x) \in 1_A \subseteq \mathcal{R}$ y, en consecuencia $(x, x) \in \mathcal{R}$, por lo tanto $\mathcal{R}$ es reflexiva.

$\square$

La propiedad simétrica afirma que si $(x, y) \in \mathcal{R}$ entonces $(y, x) \in \mathcal{R}$, lo cual le da cierto parentesco con la relación opuesta. Intuitivamente vemos que si una relación es simétrica va a coincidir con su opuesta. En verdad no es necesario pedirle tanto, ya que para caracterizar la simetría de $\mathcal{R}$ alcanza con pedir $\mathcal{R} \subseteq \mathcal{R}^{op}$. En efecto, probemos

$$\mathcal{R} \in Rel(A),\ \mathcal{R} \text{ es simétrica } \textit{sii } \mathcal{R} \subseteq \mathcal{R}^{op}.$$

Demostración:

($\Rightarrow$) Sabemos que $\mathcal{R}$ es simétrica, veamos que $\mathcal{R} \subseteq \mathcal{R}^{op}$. Sea $(x, y) \in \mathcal{R}$, como $\mathcal{R}$ es simétrica y $(x, y) \in \mathcal{R}$ resulta que $(y, x) \in \mathcal{R}$ y en consecuencia $(x, y) \in \mathcal{R}^{op}$. Hemos probado que $\mathcal{R} \subseteq \mathcal{R}^{op}$.

($\Leftarrow$) Supongamos ahora que $\mathcal{R} \subseteq \mathcal{R}^{op}$ y probemos que $\mathcal{R}$ es simétrica. Sea $(x, y) \in \mathcal{R}$, como $\mathcal{R} \subseteq \mathcal{R}^{op}$ resulta $(x, y) \in \mathcal{R}^{op}$ y, en consecuencia, $(y, x) \in \mathcal{R}$. Por lo tanto afirmamos que $\mathcal{R}$ es simétrica.

$\square$

La propiedad antisimétrica afirma que si $(x, y) \in \mathcal{R}, x \neq y$ entonces $(y, x) \notin \mathcal{R}$, o bien $(x, y) \in \mathcal{R}$, $(y, x) \in \mathcal{R}$, entonces $x = y$. Esta segunda afirmación la podemos escribir como sigue: $(x, y) \in \mathcal{R}$, $(x, y) \in \mathcal{R}^{op}$, entonces $x = y$, o aún mejor: $(x, y) \in \mathcal{R} \cap \mathcal{R}^{op}$, entonces $x = y$. En base a esto probemos la caracterización de la antisimetría de una relación binaria:

$$\mathcal{R} \in Rel(A),\ \mathcal{R} \text{ es antisimétrica } \textit{sii } \mathcal{R} \cap \mathcal{R}^{op} \subseteq 1_A.$$

Demostración:

($\Rightarrow$) Sabemos que $\mathcal{R}$ es antisimétrica. Supongamos que $(x, y) \in (\mathcal{R} \cap \mathcal{R}^{op})$, esto quiere decir que $(x, y) \in \mathcal{R}$, y $(x, y) \in \mathcal{R}^{op}$, es decir $(x, y) \in \mathcal{R}$, y $(y, x) \in \mathcal{R}$. Como $\mathcal{R}$ es antisimétrica, necesariamente $x = y$ y $(x, y) \in 1_A$.

($\Leftarrow$) Supongamos ahora que $\mathcal{R} \cap \mathcal{R}^{op} \subseteq 1_A$ y probemos que $\mathcal{R}$ es antisimétrica. Sean $x, y \in A$ tales que $(x, y) \in \mathcal{R}$ e $(y, x) \in \mathcal{R}$, es decir $(x, y) \in \mathcal{R}$ y $(x, y) \in \mathcal{R}^{op}$, por lo tanto $(x, y) \in (\mathcal{R} \cap \mathcal{R}^{op}) \subseteq 1_A$, de donde resulta $(x, y) \in 1_A$ y, en consecuencia $x = y$, por lo tanto $\mathcal{R}$ es antisimétrica.

$\square$

La propiedad transitiva afirma que si $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$ entonces $(x, z) \in \mathcal{R}$. A partir de la definición de composición sabemos que si $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$ entonces $(x, z) \in \mathcal{R} \circ \mathcal{R} = \mathcal{R}^2$. En efecto, probemos

$$\mathcal{R} \in Rel(A),\ \mathcal{R} \text{ es transitiva } \textit{sii } \mathcal{R}^2 \subseteq \mathcal{R}.$$

Demostración:

($\Rightarrow$) Sabemos que $\mathcal{R}$ es transitiva, veamos que $\mathcal{R}^2 \subseteq \mathcal{R}$. Sea $(x, z) \in \mathcal{R}^2$. Por la definición de composición debe existir un $y \in A$ tal que $(x, y) \in \mathcal{R}$ y $(y, z) \in \mathcal{R}$, pero como $\mathcal{R}$ es transitiva, la existencia de este $y \in A$ implica que $(x, z) \in \mathcal{R}$.

($\Leftarrow$) Supongamos ahora que $\mathcal{R}^2 \subseteq \mathcal{R}$ y probemos que $\mathcal{R}$ es transitiva. Sean $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$ queremos ver que $(x, z) \in \mathcal{R}$. En virtud de la definición de composición $(x, z) \in \mathcal{R}^2 \subseteq \mathcal{R}$ y en consecuencia $(x, z) \in \mathcal{R}$.

□

Una relación $\mathcal{R} \in \mathcal{R}el(A)$ se dice de *equivalencia* si es reflexiva, simétrica y transitiva. Se dice de *orden* si es reflexiva, antisimétrica y transitiva. Un buen ejercicio para el lector interesado sería buscar la caracterización de una relación de orden y de una relación de equivalencia.(♠)

(♣) La propiedad transitiva puede usarse para hacer razonamientos fallidos. Raymond Smullyan suele preguntar a quien encuentre: "¿Qué vale más, un sándwich de jamón o la felicidad eterna?" El, por su parte, afirma que un sándwich de jamón vale más. Y no sólo lo afirma, sino que lo demuestra:
Un sándwich de jamón es mejor que nada.
Nada es mejor que la felicidad eterna.
Por propiedad transitiva: Un sándwich de jamón es mejor que la felicidad eterna.

® Ahora algo un poco más "en serio". El desafío es encontrar la falla en este razonamiento.
Proposición: Toda relación simétrica y transitiva es reflexiva.
Demostración: Debemos probar que nuestra relación cumple la propiedad reflexiva, sabiendo que cumple las propiedades simétrica y transitiva. Veamos: Sea $x \in A$, por la propiedad simétrica si $(x, y) \in \mathcal{R}$ resulta $(y, x) \in \mathcal{R}$ y por la propiedad transitiva como $(x, y) \in \mathcal{R}$ e $(y, x) \in \mathcal{R}$ tenemos que $(x, x) \in \mathcal{R}$ y se verifica la propiedad reflexiva.

En verdad las propiedades son independientes. Fácilmente podemos construir ejemplos de relaciones que verifiquen sólo una de estas propiedades.
En efecto: Sea $A = \{a, b, c, d\}$

$\mathcal{R}_1 = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (c, b)\}$ sólo cumple la propiedad reflexiva

$\mathcal{R}_2 = \{(a, b), (b, a)\}$ sólo cumple la propiedad simétrica

$\mathcal{R}_3 = \{(a, c), (c, b)\}$ sólo cumple la propiedad antisimétrica

$\mathcal{R}_4 = \{(a, a), (b, b), (a, b), (c, d), (b, a)\}$ sólo cumple la propiedad transitiva

2.4. Relaciones de equivalencia

Definición 2.5 Una relación $\mathcal{R} \in \mathcal{R}el(A)$ se dice *relación de equivalencia* si satisface las propiedades reflexiva, simétrica y transitiva.

Ejemplo 2.3 Ejemplos cotidianos de relaciones de equivalencia pueden ser "ser hijo de los mismos padres", "vivir en el mismo departamento", "tener las mismas iniciales", "tener el mismo signo del zodíaco", "calzar lo mismo", etc. En todos ellos encontramos la palabra "mismo", pariente cercano (por no decir gemelo idéntico) de "igual". Y en verdad podemos pensar las relaciones de quivalencia como "iguales gordos". Veamos un ejemplo matemático.

$A = \mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$, $x\mathcal{R}y$ si y sólo si $x \cdot y > 0$

Reflexiva: Sea $x \in \mathbb{Z}_0$, $x \cdot x = x^2 > 0$, en consecuencia $x\mathcal{R}x$.

Simétrica: Sea $x\mathcal{R}y$, entonces $x \cdot y > 0$, de donde afirmamos que $y \cdot x > 0$ y,

en consecuencia $y\mathcal{R}x$.

Transitiva: Sean $x\mathcal{R}y$, $y\mathcal{R}z$, entonces $x \cdot y > 0$ e $y \cdot z > 0$.

Sabemos que $y^2 > 0$, de allí que $x \cdot z = \dfrac{(x \cdot y)(y \cdot z)}{y^2} > 0$ y resulta $x\mathcal{R}z$.

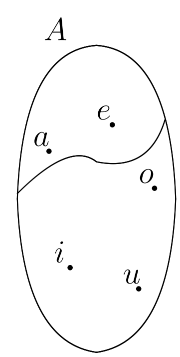
¿Qué ocurre si definimos esta relación en $\mathbb{Z}$? ®

Veamos un ejemplo finito para ver realmente qué ocurre cuando estamos en presencia de una equivalencia. Sean

$$A = \{a, b, c, d, e\}$$

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

Dejamos al lector aplicado verificar que se trata de una relación de equivalencia.®
Busquemos, por ejemplo, todos los elementos que forman par con a: sólo encontramos a a y e. Si buscamos los que se relacionan con b encontramos a b, c y d. El conjunto nos que quedado partido al mejor estilo rompecabezas. Esto no es una casualidad. Toda relación de equivalencia "guarda a cada habitante en su departamento".
Daremos algunas definiciones para poner estas ideas en un contexto matemático.



Definición 2.6 Dada una relación de equivalencia $\mathcal{R}$ definida en un conjunto no vacío A, para cada elemento $x \in A$ definimos la *clase de equivalencia* del elemento x y lo notamos $\overline{x}$ ó C_x o $[x]$ al conjunto de todos los elementos de A que están en relación con x. En símbolos:

$$[x] = \{y \in A : x\mathcal{R}y\}.$$

El conjunto de todas las clases de equivalencia se denomina *conjunto cociente* y se nota $A/\mathcal{R}$.

2.4.1. Partición de un conjunto

Acabamos de decir que hicimos de un conjunto un *puzzle*. Esta idea de partir un conjunto en pedacitos disjuntos se formaliza del siguiente modo:

Definición 2.7 Dado un conjunto A diremos que los subconjuntos $A_1, A_2, \ldots$, A_n constituyen una *partición* de A si satisfacen las siguientes condiciones:

P1) $A_i \neq \emptyset,\ 1 \leq i \leq n$,

P2) $A_i \cap A_j = \emptyset$ cada vez que $i \neq j$,

P3) $\displaystyle\bigcup_{i=1}^{n} A_1 = A_1 \cup A_2 \cup \ldots \cup A_n = A$.

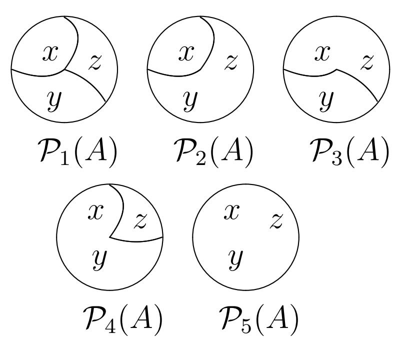
Observación 2.2 Esta definición puede ampliarse a una familia cualquiera de conjuntos, finita o no, contable o no, pero excede los límites de este curso.

Ejemplo 2.4 Si tomamos el conjunto A del ejemplo 2.3 vemos que hay dos subconjuntos $A_1 = \{a, e\}$ y $A_2 = \{b, c, d\}$. Claramente ambos son no vacíos, de intersección vacía y se cumple $A = A_1 \cup A_2$.
Podemos representar una partición de A de dos formas diferentes:

$$\mathcal{P}(A) = \{a, e\} \cup \{b, c, d\} \qquad \text{ó} \qquad \mathcal{P}(A) = \{\{a, e\},\ \{b, c, d\}\}$$

Podemos particionar el conjunto de números enteros en tres partes: los enteros negativos, el cero y los enteros positivos. La imagen es clara: es tomar el conjunto, cortarlo en pedacitos y rearmarlo. Cada conjunto se puede particionar de muchas formas, por ejemplo, si $A = \{x, y, z\}$ todas las particiones posibles son:

$$\begin{aligned}
\mathcal{P}_1 &= \{x\} \cup \{y\} \cup \{z\} \\
\mathcal{P}_2 &= \{x\} \cup \{y, z\} \\
\mathcal{P}_3 &= \{y\} \cup \{x, z\} \\
\mathcal{P}_4 &= \{z\} \cup \{x, y\} \\
\mathcal{P}_5 &= \{x, y, z\}
\end{aligned}$$



Entre las particiones que acabamos de ver hay dos que se denominan *particiones triviales* la $\mathcal{P}_1$, llamada *partición identidad* que separa a cada elemento y la $\mathcal{P}_5$, llamada *partición universal* que los deja a todos juntos. Veremos más adelante la razón de ser de estos nombres.

En general, dada cualquier relación de equivalencia $\mathcal{R}$ en A, el conjunto cociente $A/\mathcal{R}$ es una partición de A. Probemos las tres condiciones que definen una partición:

P1) $[x] \neq \emptyset$, ya que por la propiedad reflexiva $x\mathcal{R}x$ para todo $x \in A$.

P2) $[x] \cap [y] = \emptyset$ cada vez que $[x] \neq [y]$. Probemos que si $[x] \cap [y] \neq \emptyset$, entonces necesariamente $[x] = [y]$. Sea $z \in [x] \cap [y]$, entonces $z\mathcal{R}x$ y $z\mathcal{R}y$, y por las propiedades simétrica y transitiva resulta $x\mathcal{R}y$, es decir $x \in [y]$ e $y \in [x]$, por lo tanto, $[x] = [y]$

P3) $\displaystyle\bigcup_{x\in A}[x] = A$. Como $[x] \subseteq A$ para todo $x \in A$ es claro que $\displaystyle\bigcup_{x\in A}[x] \subseteq A$. Para ver que $A \subseteq \displaystyle\bigcup_{x\in A}[x]$ basta ver que todo $x \in A$ está considerado en la unión.

Habiendo hablado ya de relaciones de equivalencia y de particiones veamos qué las hace tan unidas, o, si se quiere, interdependientes.

Dar una partición de un conjunto es como poner paredes en el "Loft de Venn" y decidir qué elemento vive con cuál. Dada una partición cualquiera, entonces se puede definir la relación "vive con" que será claramente una relación de equivalencia ya que toda persona vive consigo misma, si alguien vive con otra persona es claro que no importa el orden al decir quién vive con quién y si una persona vive con otra que a su vez vive con una tercera, y no hay infidelidades extrañas, es claro que viven los tres juntos entonces el primero vive con el tercero.
Escribámoslo matemáticamente:

Sea $A = A_1 \cup A_2 \cup \ldots \cup A_n$ una partición de A y definamos la relación:

$$x\mathcal{R}y \text{ si y sólo si existe } A_i \text{ tal que } \{x, y\} \subseteq A_i \text{ para algún } 1 \leq i \leq n.$$

El primer paso es comprobar que se trata de una relación de equivalencia:

1. Propiedad reflexiva: Sea $x \in A$, claramente existe un $i \in \{1, 2, \ldots, n\}$ tal que $x \in A_i$ y, en consecuencia, $\{x, x\} = \{x\} \subseteq A_i$ y $x\mathcal{R}x$ para todo $x \in A$.

2. Propiedad simétrica: Sea $x\mathcal{R}y$, entonces $\{x, y\} \subseteq A_i$ para algún $1 \leq i \leq n$. Como $\{x, y\} = \{y, x\}$ resulta $\{y, x\} \subseteq A_i$ para algún $1 \leq i \leq n$, es decir $y\mathcal{R}x$.

3. Propiedad transitiva: Sean $x, y, z \in A$ tales que $x\mathcal{R}y$ e $y\mathcal{R}z$. Existen $i, j \in \{1, 2, \ldots, n\}$ tales que $\{x, y\} \subseteq A_i$, $\{y, z\} \subseteq A_j$, entonces $y \in A_i \cap A_j$ y como son mutuamente excluyentes, es decir $A_i \cap A_j = \emptyset$, para todo $i \neq j$ resulta $i = j$ y $\{x, y, z\} \subseteq A_i$ de donde, obviamente, $\{x, z\} \subseteq A_i$ y $x\mathcal{R}z$.

El segundo paso será construir las clases de equivalencia de esta relación:

$[x] = \{y \in A : x\mathcal{R}y\} = \{y \in A : \text{ existe } A_i \text{ tal que } \{x, y\} \subseteq A_i\} = A_i$ tal que $x \in A_i$.

En palabras lo que estamos diciendo es que la clase de equivalencia de cada elemento x es el "pedacito" de la partición en donde "vive" x. Probemos esto:

Para todo $x \in A$ existe $A_i \subseteq A$ tal que $x \in A_i$. Por la definición de la relación de equivalencia $y \in A_i$ si y sólo si $x\mathcal{R}y$ y queda demostrada la igualdad.

Es decir: dada una partición definimos una relación de equivalencia tal que las clases de equivalencia son exactamente los miembros de la partición. Podemos recorrer este mismo camino a la inversa. Es decir, dada una relación de equivalencia las clases determinan una partición y esa partición determina una relación de equivalencia que es exactamente la misma que teníamos al principio. Espero ansiosamente la construcción realizada por el lector interesado.®

A partir de esta conexión es fácil ver por qué se llaman partición identidad y partición universal respectivamente las $\mathcal{P}_1$ y $\mathcal{P}_5$ del ejemplo 2.4 ya que están indisolublemente unidas a las relaciones de equivalencia 1_A y U_A. Veamos la construcción de la relación de equivalencia que determina, por ejemplo, $\mathcal{P}_3 = \{\{x, z\}, \{y\}\}$.

$\mathcal{R}_{\mathcal{P}_3} = \{(x, x), (y, y), (z, z), (x, z), (z, x)\} = 1_A \cup \{(x, z), (z, x)\}$

No es necesario probar que esta en particular es una relación de equivalencia, porque ya lo hemos demostrado en general. Construyamos las clases:

$[x] = \{x, z\} = [z]$, $[y] = \{y\}$.

Y vemos que se cumple que las clases de equivalencia coinciden con los miembros de la partición.

2.5. Ejercicios propuestos

2.5.1. Producto cartesiano

Ejercicio 2.1 Dados los conjuntos $A = \{a, b, c\}$ y $B = \{1, 2\}$, escribir los conjuntos $A \times B$ y $B \times A$. ¿Es conmutativo el producto cartesiano de conjuntos?

Ejercicio 2.2 Probar que, cualesquiera que sean A, B, C tres conjuntos no vacíos, tales que $B \cap C \neq \emptyset$, se verifica:

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$

¿Se verifica $(A \times B)' = A' \times B'$?

Ejercicio 2.3 (♣) En una reunión hay más hombres que mujeres, más mujeres que beben que hombres que fuman, y más mujeres que fuman y no beben que hombres que ni beben ni fuman. Demostrar que hay menos mujeres que ni beben ni fuman que hombres que beben y no fuman.

2.5.2. Relaciones

Ejercicio 2.4 Sean $\mathcal{R} \subseteq A \times B$ y $\mathcal{S} \subseteq B \times C$

1. (®) Dada una relación $\mathcal{R} \subseteq A \times B$, se define el Dominio de $\mathcal{R}$ como los elementos del conjunto A que son primera coordenada de algún par en la relación, la Imagen de $\mathcal{R}$ como los elementos del conjunto B que son segunda coordenada de algún par en la relación. Describir los conjuntos $Dom\mathcal{R}$ y $Im\mathcal{R}$ por comprensión.
2. (®) Dada una relación $\mathcal{R} \subseteq A \times B$, se define la opuesta $\mathcal{R}^{op} \subseteq B \times A$ como el conjunto de los pares (x, y) tales que $y\mathcal{R}x$. Describir el conjunto $\mathcal{R}^{op}$ por comprensión.
3. (®) Un par (x, y) pertenece a la composición de $\mathcal{R}$ y $\mathcal{S}$, que se escribe $\mathcal{S} \circ \mathcal{R} \subseteq A \times C$ si existe un elemento $z \in B$ tal que $(x, z) \in \mathcal{R}$ y $(z, y) \in \mathcal{S}$. Describir el conjunto $\mathcal{S} \circ \mathcal{R}$ por comprensión.
4. Probar que (®) $Dom(\mathcal{S} \circ \mathcal{R}) \subseteq Dom(\mathcal{R})$.
5. Probar que $Im(\mathcal{S} \circ \mathcal{R}) \subseteq Im(\mathcal{S})$.

Ejercicio 2.5 Dadas las relaciones $\mathcal{R}$ y $\mathcal{S}$ Hallar $\mathcal{R}\circ\mathcal{S}$ y ($\diamond$) $\mathcal{S}\circ\mathcal{R}$, dando en cada caso el dominio y la imagen de cada una de las composiciones obtenidas.

$$\mathcal{R} = \{(1,2),\ (1,4),\ (2,3),\ (2,5),\ (3,2),\ (3,4),\ (6,9)\},$$

$$\mathcal{S} = \{(2,5),\ (4,1),\ (5,7),\ (6,9)\}$$

Ejercicio 2.6 ($\diamond$) Sean:
$A = \{x \in \mathbb{Z} : x \text{ es divisor positivo de } 20\}$, $B = \{x \in \mathbb{Z} : x \text{ es divisor positivo de } 18\}$, y $\mathcal{R}$ la relación binaria $\{(x,y) : x \text{ divide a } y\} \subseteq A \times B$.

Hallar, si es posible, (Sugerencia: realizar el diagrama de Venn)

1. $\mathcal{S} \subseteq B \times A$ tal que $\mathcal{T} = \mathcal{S}\circ\mathcal{R}$, siendo $\mathcal{T} = \{(1,1),\ (2,2)\}$.
2. $\mathcal{S} \subseteq B \times A$ tal que $\mathcal{T} = \mathcal{R}\circ\mathcal{S}$, siendo $\mathcal{T} = \{(9,2),\ (9,6),\ (9,18)\}$.

Ejercicio 2.7 (©) Si $\mathcal{R} \in Rel(A)$. Se dice que cumple con la propiedad:

1. *Reflexiva*: Si $x\mathcal{R}x$ para todo $x \in A$.
2. *Simétrica*: Si $x\mathcal{R}y$ entonces $y\mathcal{R}x$.
3. *Antisimétrica*: Si $x\mathcal{R}y$ e $y\mathcal{R}x$ implica $x = y$ ó Si $x\mathcal{R}y$ y $x \neq y$, entonces $y\not\mathcal{R}x$.
4. *Transitiva*: Si $x\mathcal{R}y$ e $y\mathcal{R}z$ entonces $x\mathcal{R}z$.

Demostrar que:

1. $\mathcal{R}$ es reflexiva si y sólo si $1_A \subseteq \mathcal{R}$,
2. $\mathcal{R}$ es simétrica si y sólo si $\mathcal{R}^{op} \subseteq \mathcal{R}$,
3. $\mathcal{R}$ es antisimétrica si y sólo si $\mathcal{R}^{op} \cap \mathcal{R} \subseteq 1_A$,
4. $\mathcal{R}$ es transitiva si y sólo si $\mathcal{R}^2 \subseteq \mathcal{R}$.

Ejercicio 2.8 Determinar qué propiedades verifican las siguientes relaciones en A:

1. $A = \{1,3,5,15\}$; $\mathcal{R} = \{(1,1),(1,3),(1,5),(1,15),(3,3),(3,15),(15,15)\}$.
2. $A = \{x,y,z\}$; $\mathcal{R} = \{(x,x),(z,z),(x,z),(z,x),(x,y),(y,x)\}$.
3. $A = \{x : x \in \mathbb{N},\ x < 25\}$; $\mathcal{R} = A \times A$.

Ejercicio 2.9 Sea el conjunto $A = \{a,e,i,o,u\}$, dar una relación $\mathcal{R} \in Rel(A)$ tal que:

1. sea reflexiva y simétrica, pero no transitiva.
2. sea antisiḿetrica y transitiva.
3. sea simétrica y antisimétrica.

Ejercicio 2.10 ($\diamond$) Sean $\mathcal{R}_1, \mathcal{R}_2 \in Rel(A)$. Determinar la veracidad o falsedad de las siguientes proposiciones:

1. Si $\mathcal{R}_1$ es reflexiva, entonces $\mathcal{R}_1 \cap \mathcal{R}_2$ es reflexiva.
2. Si $\mathcal{R}_1$ es reflexiva, entonces $\mathcal{R}_1 \cup \mathcal{R}_2$ es reflexiva.
3. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son simétricas, entonces $\mathcal{R}_1 \cap \mathcal{R}_2$ es simétrica.
4. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son simétricas, entonces $\mathcal{R}_1 \cup \mathcal{R}_2$ es simétrica.
5. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son antisimétricas, entonces $\mathcal{R}_1 \cap \mathcal{R}_2$ es antisimétrica.
6. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son antisimétricas, entonces $\mathcal{R}_1 \cup \mathcal{R}_2$ es antisimétrica.
7. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son transitivas, entonces $\mathcal{R}_1 \cap \mathcal{R}_2$ es transitiva.
8. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son transitivas, entonces $\mathcal{R}_1 \cup \mathcal{R}_2$ es transitiva.

2.5.3. Relaciones de equivalencia

Ejercicio 2.11 Determinar en cada caso si $\mathcal{R} \in EQ(A)$, siendo:

1. $A = \mathbb{N}$, $x\mathcal{R}y$ si y sólo si $x - y$ es un número impar.
2. $A = \{a, b, c, d, e\}$, $\mathcal{R} = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, e), (e, a), (a, c), (c, a), (c, e), (e, c)\}$

En caso afirmativo hallar las clases de equivalencia y el conjunto cociente.

Ejercicio 2.12 Hallar la relación de equivalencia asociada a la partición:

$$A = \{1\} \cup \{2, 3\} \cup \{4\} \cup \{5, 6\}.$$

Ejercicio 2.13 Hallar todas las relaciones de equivalencia posibles sobre un conjunto A con tres elementos

Capítulo 3

Funciones

Funciones. Imagen e imagen completa inversa. Funciones inyectivas, epiyectivas y biyectivas. Composición de funciones.

3.1. Motivación

Una *función* en términos cotidianos, es lo que "conecta" dos cosas. "Conecta" del mismo modo que un colectivo "conecta" Bahía Blanca con Buenos Aires, y ésta es la idea que intentaremos explicar.
Imaginemos una terminal de colectivos, todos y cada uno de los colectivos que están en la línea de salida, salen y tienen un destino final (tal vez en su recorrido se detengan, quizá más de una vez, pero su destino final en cada viaje es único).
Esto exactamente es la idea de función: un conjunto de salida, donde

(F1) todos salen, [1]

(F2) ninguno tiene dos destinos finales.

Vamos a formalizar este concepto con términos matemáticos. Hemos visto las nociones de conjunto, producto cartesiano de conjuntos y relaciones.
Consideremos los conjunto A y B definidos por: $A = \{1, 2, 3\}, \quad B = \{a, b, c, d\}$.
Su producto cartesiano es entonces:

$$A \times B = \{(1, a), (1, b), (1, c), (1, d), (2, a), (2, b), (2, c), (2, d), (3, a), (3, b), (3, c), (3, d)\}.$$

Defininamos las relaciones:

[1] podría considerarse la posibilidad de que no todos salgan-to be continued...

$\mathcal{R}_1 = \emptyset,$
$\mathcal{R}_2 = \{(1,a),(1,b),(1,c),(1,d)\},$
$\mathcal{R}_3 = \{(1,a),(2,a),(3,a)\},$
$\mathcal{R}_4 = \{(1,d),(2,b),(3,a)\},$
$\mathcal{R}_5 = \{(1,a),(1,d),(2,c),(3,b)\},$
$\mathcal{R}_6 = \{(1,a),(1,b),(1,c),(1,d),(2,a),(2,b),(2,c),(2,d),(3,a),(3,b),(3,c),(3,d)\}.$

De estas relaciones las menos interesantes son $\mathcal{R}_1$ y $\mathcal{R}_6$, que se llaman respectivamente *relación nula* y *relación universal*, $\mathcal{R}_2$ no cumple con las condiciones para ser función porque los "colectivos" 2 y 3 se quedan en la terminal, en $\mathcal{R}_3$ y $\mathcal{R}_4$ salen todos y cada uno tiene su destino, en $\mathcal{R}_5$ salen todos pero el "colectivo" 1 va a dos lugares diferentes.

Según la idea que hemos dado, las relaciones que son *funciones* (también llamadas *funciones totales*) son R_3 y R_4. Llamémoslas respectivamente, f_3 y f_4. Como cada elemento va a un único destino podemos decir que

$f_3(1) = a,\ f_3(2) = a,\ f_3(3) = a$
$f_4(1) = d,\ f_4(2) = b,\ f_4(3) = a$

Y describir las funciones mediante *tabla de valores:*

x	1	2	3
$f_3(x)$	a	a	a

x	1	2	3
$f_4(x)$	d	b	a

3.2. Definición

Escribamos ahora estos conceptos en términos matemáticos:

Definición 3.1 Dados dos conjuntos A y B, se dice que f es una *función* de A en B y se escribe $f : A \to B$ si:

(F0) $(x, f(x)) \in A \times B$ (sale de A y llega a B)

(F1) Para todo $x \in A$, existe $f(x) \in B$ (salen todos)

(F2) Si $f(x_1) \neq f(x_2)$, entonces $x_1 \neq x_2$ (cada uno tiene único destino)

Dado que una función es una relación que cumple determinadas propiedades, todos los conceptos vistos para relaciones se pueden aplicar a las funciones. Reescribamos, entonces, las definiciones más importantes:

Definición 3.2 Dada $f : A \to B$, A se llama el *dominio* de f, y se escribe $D(f)$. B es el *rango* (conjunto de llegada) de f. Dentro del rango distinguimos los puntos que provienen del conjunto A como la *imagen* de f y lo notamos $I(f)$.

$$D(f) = \{x \in A : f(x) \in B\} = A \qquad \text{dominio de } f$$
$$I(f) = \{y \in B : \text{ existe } x \in A : y = f(x)\} = A \qquad \text{imagen de } f$$

Observación 3.1 (Continuación de la nota al pie.) Si una relación cumple (F0) y (F2) pero no F(1) (es decir, hay elementos en A que no pertenecen al dominio) se suele llamar una *función parcial*. En este caso $f : D(f) \to B$ es función. Cada vez que se escribe $f : A \to B$ A debe ser el dominio de la función. En el caso de las llamadas funciones parciales si se quiere usar la notación de la flechita se escribe $A \xrightarrow{f} B$.

Observación 3.2 Las funciones se diferencian de las relaciones sobre todo en el hecho de tener cada elemento una única imagen, lo cual nos permite pensar cada función como una pequeña máquina que cuando se le introduce una determinada ficha que le "quepa en la ranura" (un valor que pertenezca al dominio), nos entrega un determinado producto en relación con la ficha. Por ejemplo, la "máquina" f_4 al introducirle la "ficha" 1 entrega una d, con la "ficha" 2 entrega una b y finalmente, con la 3, una a. Es decir, lo que entrega *depende* de lo que uno introduce que es una ficha absolutamente *libre*. Por esta razón al escribir $y = f(x)$ decimos que x es una variable libre e y una variable dependiente.

Observación 3.3 ¿Podemos pensar en definir entre funciones las mismas operaciones que entre relaciones? Claramente si pensamos que las funciones son relaciones, operamos y obtenemos relaciones. Pero... ¿Serán funciones? ¿Se puede definir la unión de funciones con el mismo dominio? ¿Y la intersección? ¿Y el complemento? Dejando estas preguntas a cargo del lector interesado, vamos a ver qué ocurre con la composición de funciones y la función opuesta.®

Definición 3.3 Dadas dos funciones $f : A \to B$ y $g : B \to C$ se define la *composición de f seguida de g* y se nota $g \circ f : A \to C$ a la función tal que $(g \circ f)(x) = g(f(x))$, para todo $x \in A$ tal que $f(x) \in D(g)$.

Aquí vemos que, a diferencia de las relaciones, la composición de funciones sólo existe para los elementos del dominio de la primera función cuya imagen pertenezca al dominio de la segunda función. En algunos textos se afirma que La composición $g \circ f$ sólo existe si $I(f) \subseteq D(g)$, lo cual restringe completamente la idea de composición. Nosotros asumimos que tal composición existe para los puntos en que sea posible y declararemos $g \circ f : D(g \circ f) \to C$. Aclararemos este concepto con un ejemplo sencillo.

Ejemplo 3.1 Sean $A = \{a, b, c, d, e, f\},\ B = \{m, n, p, q\},\ C = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ y las funciones definidas por las tablas:

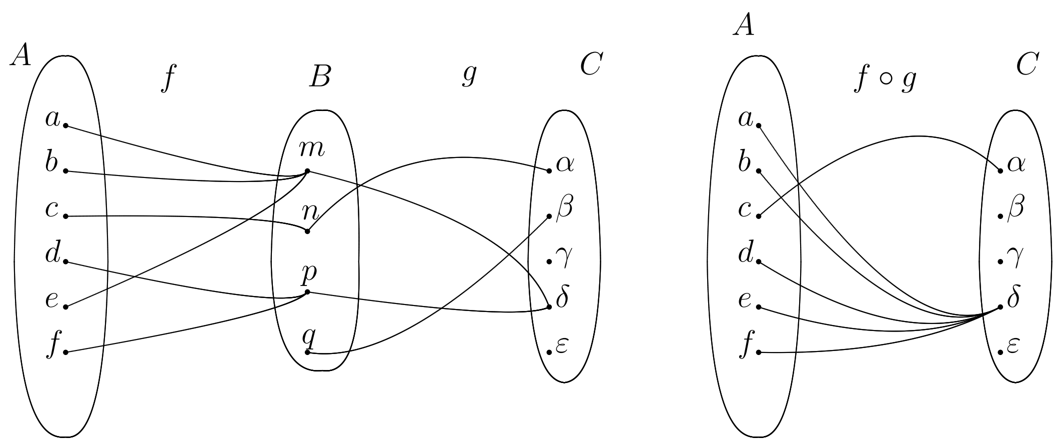
x	a	b	c	d	e	f
$f(x)$	m	m	n	p	m	p

x	m	n	p	q
$g(x)$	δ	α	δ	β

Entonces la composición está definida por:

x	a	b	c	d	e	f
$g \circ f(x)$	δ	δ	α	δ	δ	δ

Este hecho se ve mucho más claramente utilizando diagramas de Venn. Haremos los tres conjuntos en forma consecutiva y luego consideraremos todos los caminos de dos tramos, restringiendo el dominio.



En este caso el dominio de composición coincide con el de la primera función, pero aún podríamos considerar:

$A = \{a, b, c, d, e, f\},\ B = \{m, n, p, q\},\ B' = \{m, n, q\},\ C = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ y las funciones definidas por las tablas:

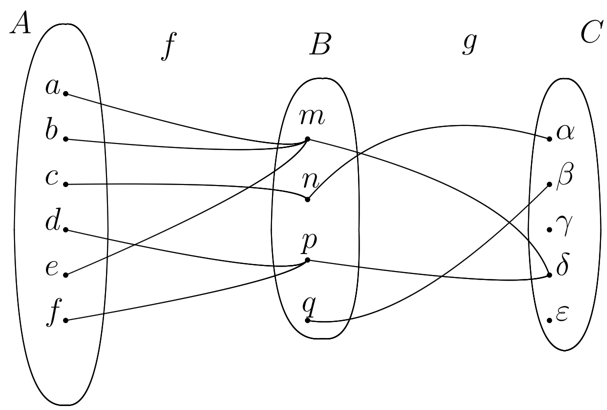
x	a	b	c	d	e	f
$f(x)$	m	m	n	p	m	p

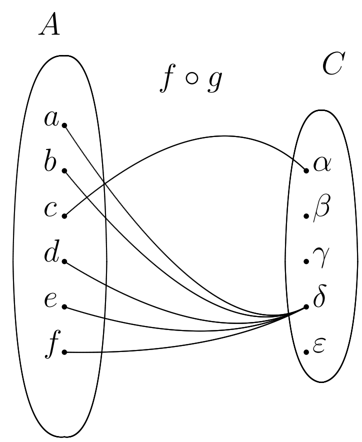
x	m	n	q
$g(x)$	δ	α	δ

Entonces la composición está definida por:

x	a	b	c	e
$g \circ f(x)$	δ	δ	α	δ

Que gráficamente es:





En este caso la composición no es función de A en C, pero sí de $\{a, b, c, e\} \to C$ y resulta $D(g \circ f) \subset D(f)$. Veremos muchos ejemplos numéricos más adelante.

Si pensamos en hacer la opuesta de una función es claro que siempre existe y es relación, pero ¿en qué condiciones la opuesta de una función es función?

Veamos: $f^{op} : B \to A$. En primer lugar dijimos que debe cumplirse "todos salen" que en términos matemáticos, para una aplicación f de A en B se convierte en:
"para todo $x \in A$ existe $y \in B$ tal que $f(x) = y$."
y para f^{op} resulta:
"para todo $y \in B$ existe $x \in A$ tal que $f^{op}(y) = x$", o bien:
"para todo $y \in B$ existe $x \in A$ tal que $f(x) = y$."
Al afirmar esto estamos diciendo que si pusiéramos un papelito $f(x)$ sobre cada $y = f(x)$ taparíamos todo B, lo cubriríamos, por eso decimos que la imagen de f está *sobre* el conjunto B y llamamos a una función que cumple esta propiedad función sobreyectiva, epiyectiva o suryectiva, porque respectivamente en griego y francés sobre es "epi" o "sur".

Definición 3.4 Una función $f : A \to B$ se dice *epiyectiva*, *suryectiva* o *sobreyectiva* si para cada $y \in B$ existe $x \in A$ tal que $y = f(x)$.

Observación 3.4 La definción precedente es equivalente a decir $Im(f) = B$, lo cual tiene lógica ya que el dominio de una relación es la imagen de su opuesta y estamos buscando que el dominio de $f^{op} = B$.

La siguiente condición pedida fue tener "destino único", es decir: "para cada $f(x_1) \neq f(x_2)$ debe ser $x_1 \neq x_2$." Si pedimos esto para f^{op} resulta:
"para cada $f^{op}(y_1) \neq f^{op}(y_2)$ debe ser $y_1 \neq y_2$." que llevado a la función f resulta:
"para cada $x_1 \neq x_2$ debe ser $f(x_1) \neq f(x_2)$."
Al afirmar esto estamos diciendo que cada elemento de A tiene una "copia exclusiva" en B, es decir, dentro de B podemos encontrar una "copia exacta" de A, es decir A se puede *inyectar* dentro de B y llamamos inyectiva a una función que cumple esta propiedad.

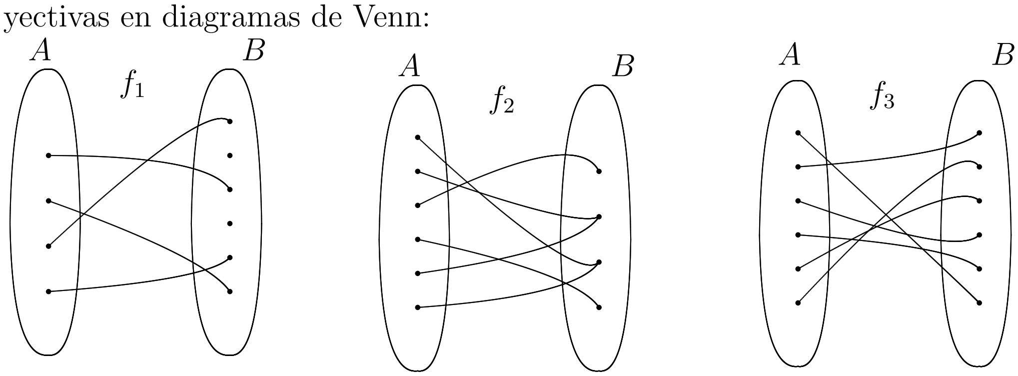
Definición 3.5 Una función $f : A \to B$ se dice *inyectiva* si para cada $x_1 \neq x_2$ en A resulta $f(x_1) \neq f(x_2)$ en B.

Observación 3.5 La definción precedente, en virtud de la *Ley contrapositiva* es equivalente a decir $f(x_1) = f(x_2)$ impica $x_1 = x_2$ lo cual es mucho más sencillo de demostrar, porque la igualdad es única.

Claramente, para que f^{op} sea función deben cumplirse ambas propiedades y como dos en griego es "bi", definimos:

Definición 3.6 Una función $f : A \to B$ se dice *biyectiva* si es simultáneamente inyectiva y epiyectiva.

Veamos el aspecto que presentan las funciones inyectivas, sobreyectivas o biyectivas en diagramas de Venn:



La primera, f_1, se trata de una función inyectiva, no sobreyectiva; la segunda, f_2 es sobreyectiva no inyectiva y finalmente f_3 es biyectiva.

Observación 3.6 Sea $f : A \to B$ y supongamos que A y B son conjuntos finitos, entonces $|A| = m$ y $|B| = n$, con m, n números naturales. ¿Se puede establecer alguna relación entre m y n sabiendo que la función f es inyectiva, sobreyectiva o biyectiva?®

Si f es una función biyectiva, existe f^{op} y es función. Es, en verdad, "el colectivo de vuelta" y por eso "ir y volver" nos debe "dejar en el mismo lugar". Escribamos todo esto matemáticamente:

Definición 3.7 Dada $f : A \to B$, si f es biyectiva se define la función inversa de f y se nota f^{-1} a la relación opuesta de f.

Proposición 3.1 *Si $f : A \to B$ es una función biyectiva, entonces existe f^{-1}. Aún más, $f^{-1} \circ f = 1_A$ y $f \circ f^{-1} = 1_B$.*

Demostración:
Debemos probar en primer lugar que f^{-1} es función. Dejamos esta demostración al lector porque la hemos hecho en forma encubierta al buscar su existencia.®
Hagamos las composiciones:

$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$, porque f es inyectiva (pensarlo). Como esto vale para todo $x \in A$, resulta $f^{-1} \circ f = 1_A$.

$(f \circ f^{-1})(y) = f(f^{-1}(y)) = y$, porque f es sobreyectiva e inyectiva (pensarlo). Como esto vale para todo $y \in B$, resulta $f \circ f^{-1} = 1_B$. □

En verdad otra definición de función biyectiva es justamente la existencia de función inversa, es decir:

Definición 3.8 Una función $f : A \to B$ se dice *inyectiva* si existe una aplicación $f^{op} : B \to A$ tal que $f^{op} \circ f = 1_A$.

Definición 3.9 Una función $f : A \to B$ se dice *epiyectiva* si existe una aplicación $f^{op} : B \to A$ tal que $f \circ f^{op} = 1_B$.

Definición 3.10 Una función $f : A \to B$ se dice *biyectiva* si existe una aplicación $f^{op} : B \to A$ tal que $f^{op} \circ f = 1_A$, y $f \circ f^{op} = 1_B$. En dicho caso $f^{op} = f^{-1}$.

Observación 3.7 El lector interesado puede demostrar la equivalencia entre las definiciones 3.4 y 3.9, entre 3.5 y 3.8 y en consecuencia habrá probado la equivalencia entre 3.6 y 3.10. ¿Estará probada esta última con las anteriores o faltará un "pequeño" detalle?®

Ejemplo 3.2 En general se cree que una función es una aplicación y ella en sí es inyectiva, sobreyectiva o biyectiva. En verdad una función es una aplicación que tiene un dominio y un codominio y esta terna es quien define si la función es o no inyectiva, epiyectiva o biyectiva. Veámoslo con $f(x) = |2x|$.

1. $f : \mathbb{R} \to \mathbb{Z}$: ni siquiera es función porque $\sqrt{2} \in \mathbb{R}$ y $|2\sqrt{2}| \notin \mathbb{Z}$.
2. $f : \mathbb{Z} \to \mathbb{Z}$: es función no inyectiva ya que $f(-2) = f(2)$, no epiyectiva ya que no existe $x \in \mathbb{Z} : f(x) = -1$.
3. $f : \mathbb{N} \to \mathbb{Z}$: es una función inyectiva, no epiyectiva.
4. $f : \mathbb{N} \to \mathbb{P}$: es una función biyectiva, donde $\mathbb{P}$ el conjunto de los números naturales pares.

Probemos algunas relaciones entre estas definciones y la composición:

Proposición 3.2 *Sean $f : A \to B$ y $g : B \to C$, se demuestra que:*

1. *Si f y g son inyectivas, entonces $g \circ f$ es inyectiva,*
2. *Si f y g son epiyectivas, entonces $g \circ f$ es epiyectiva.*

Demostración:
Para aclarar notaciones llamaremos x a los elementos que pertenecen al conjunto A, y a los del conjunto B y z a los del conjunto C.

1. Sabemos que f y g son inyectivas, es decir que $f(x_1) = f(x_2)$ implica $x_1 = x_2$ y $g(y_1) = g(y_2)$ implica $y_1 = y_2$. Probemos que $g \circ f$ lo es, es decir probemos que si $(g \circ f)(x_1) = (g \circ f)(x_2)$, entonces $x_1 = x_2$.

   $(g \circ f)(x_1) = (g \circ f)(x_2)$ implica $g(f(x_1)) = g(f(x_2))$, y como g es inyectiva implica $f(x_1) = f(x_2)$ y como f es inyectiva implica $x_1 = x_2$.
2. Sabemos que f y g son epiyectivas, es decir que para todo $z \in C$ existe $y \in B$ tal que $g(y) = z$ y para cada y en B existe $x \in A$ tal que $f(x) = y$. Veamos que $g \circ f$ es epiyectiva, es decir que para cada $z \in C$ existe $x \in A$ tal que $(g \circ f)(x) = z$.

   Sea $z \in C$, como g es epiyectiva existe $y \in B$ tal que $z = g(y)$, para ese y, como f es epiyectiva existe $x \in A$ tal que $f(x) = y$, entonces resulta $z = g(y) = g(f(x)) = (g \circ f)(x)$.

Corolario 3.1 *Si f y g son biyectivas, entonces $g \circ f$ es biyectiva. Además $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Demostración: A cargo del lector interesado.®

Observación 3.8 El lector interesado puede preguntarse ¿Y al revés? es decir: Si la composición es inyectiva lo son las funciones? ¿Qué pasa con la epiyectividad? Lector (dama o caballero) interesado: ¡Busque y encontrará! y si tiene dificultades en el camino... pregunte a la cátedra, que para eso estamos.®

Proposición 3.3 *Sean $f : A \to B,\ g : C \to D$. Si $h : A \times C \to B \times D$ está definida por : $h((x, y)) = (f(x), g(y))$, se verifican las siguientes afirmaciones:*

1. *Si f y g son inyectivas, h es inyectiva.*
2. *Si h es inyectiva, f y g son inyectivas.*
3. *Si f y g son sobreyectivas, h es sobreyectiva.*
4. *Si h es sobreyectiva, f y g son sobreyectivas.*

Demostración:

1. Veamos que si f y g son inyectivas, h es inyectiva. Supongamos que $h((x_1, y_1)) = h((x_2, y_2))$, es decir $(f(x_1), g(y_1)) = (f(x_2), g(y_2))$ por igualdad de pares ordenados resulta $f(x_1) = f(x_2)$ y $g(y_1) = g(y_2)$, pero como f y g son inyectivas, resulta $x_1 = x_2$ e $y_1 = y_2$, de donde $(x_1, y_1) = (x_2, y_2)$.
2. Supongamos ahora h es inyectiva. Queremos probar que f y g son inyectivas.
   Comencemos por la f: Sea $f(x_1) = f(x_2)$ consideremos cualquier elemento $y \in B$, entonces resulta $(x_1, y), (x_2, y) \in A \times C$ y $h((x_1, y)) = (f(x_1), g(y)) = (f(x_2), g(y)) = h((x_2, y))$, y como h es inyectiva resulta $(x_1, y) = (x_2, y)$ y por igualdad de pares, $x_1 = x_2$ y f inyectiva.
   Dejamos a cargo del lector la demostración de g inyectiva.®
   Podríamos haber hecho ambas demostraciones en simultáneo, y si el lector interesado desea intentarlo, cuenta con todo nuestro apoyo.

3. Probemos ahora que si f y g son sobreyectivas, h es sobreyectiva. debemos probar que todo elemento del conjunto $B \times D$ proviene, vía la función h de un elemento de $A \times C$. Sea, entonces $(z,t) \in B \times D$, como $z \in B$ y f es epiyectiva, existe $x \in A$ tal que $z = f(x)$, como $t \in D$ y g es epiyectiva, existe $y \in C$ tal que $t = g(y)$. Entonces $(x,y) \in A \times C$ y $h((x,y)) = (f(x), g(y)) = (z,t)$, como queríamos probar.
4. Si h es sobreyectiva, f y g son sobreyectivas. Nuevamente haremos esta demostración en dos partes, y, por usar otra función probaremos que g es epiyectiva:
   Sea $t \in D$ y consideremos cualquier $z \in B$, entonces el par $(z,t) \in B \times D$ y como h es epiyectiva existe un par $(x,y) \in A \times C$ tal que $h((x,y)) = (z,t)$, pero $h(x,y) = (f(x), g(y))$, entonces $f(x) = z$ y $g(y) = t$, es decir, hemos encontrado un $y \in C$ tal que $g(y) = t$.
   Nuevamente dejamos a cargo del lector la otra demostración y reiteramos la posibilidad de trabajar con ambas funciones a un tiempo.®

Corolario 3.2 *Si f y g son biyectivas, entonces h también lo es.*

3.3. $f : \mathbb{P}(A) \to \mathbb{P}(B)$

Dada una aplicación cualquiera $f : A \to B$ siempre es posible definir una aplicación de $\mathbb{P}(A)$ en $\mathbb{P}(B)$, usando la misma función f. Hay quien nota a esta función con mayúscula, es decir F, pero como en esencia se trata de la misma función usaremos la misma notación.

Definición 3.11 Si $f : A \to B$ se define el conjunto *imagen de X*, para cada $X \in \mathbb{P}(A)$, y se lo nota $f(X)$ a $f(X) = \{f(x) : x \in X\}$.

Ejemplo 3.3 Sean $A = \{a, b, c\},\ B = \{0, 1\}$ y $f : \mathcal{A} \to B$ por:

x	a	b	c
$f(x)$	0	1	1

$\mathbb{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, A\}$, $\qquad \mathbb{P}(B) = \{\emptyset, \{0\}, \{1\}, B\}$
Claramente, en este ejemplo, $f(\emptyset) = \emptyset$ y $f(A) = B$,

$f(\{a\}) = \{0\} = \{f(a)\}$, $f(\{b\}) = \{1\} = \{f(b)\}$, $f(\{c\}) = \{1\} = \{f(c)\}$,

$f(\{a,b\}) = \{0,1\} = \{f(a), f(b)\}$, $f(\{a,c\}) = \{0,1\} = \{f(a), f(c)\}$,

$f(\{b,c\}) = \{1\} = \{f(b), f(c)\}$, ya que $f(b) = f(c)$.

Proposición 3.4 *Sea* $f : A \to B$ *una función,* $X, X_1, X_2 \subseteq A$*,*

1. $X_1 \subseteq X_2 \Rightarrow f(X_1) \subseteq f(X_2)$*;*
2. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$*;*
3. $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$*.*
4. $f(X_1 \cap X_2) = f(X_1) \cap f(X_2) \Leftrightarrow f$ *es inyectiva.*
5. $f(X') = [f(X)]' \Leftrightarrow f$ *es biyectiva.*

Demostración: Sólo probaremos la primera a modo de ejemplo, dejando las restantes al lector.®
Sabemos que $X_1 \subseteq X_2$ y queremos probar que $f(X_1) \subseteq f(X_2)$, es decir, tenemos que ver que todo elemento que esté en $f(X_1)$ está también en $f(X_2)$. Lo más importante al comenzar una de estas demostraciones es considerar qué "aspecto" tiene ese elemento. Vamos a la definición de conjunto imagen y vemos que los elementos que están dentro del conjunto son de la forma $f(\text{algo})$. Tomemos esa forma y tendremos la mitad de la demostración resuelta. Sea $f(x) \in f(X_1)$, entonces, por la defini̇ción de $f(X_1)$ necesariamente $x \in X_1$ y $X_1 \subseteq X_2$, en consecuencia $x \in X_2$ y $f(x) \in f(X_2)$. Hemos probado que todo elemento de $f(X_1)$ es elemento de $f(X_2)$. $\square$

Del mismo modo es posible definir una aplicación de $\mathbb{P}(B)$ en $\mathbb{P}(A)$, usando la aplicación f^{op}, que notaremos f^{-1}.

Definición 3.12 Dada $f : A \to B$ se define el conjunto *preimagen de* Y para cada $Y \in \mathbb{P}(B)$, y se lo nota $f^{-1}(Y)$, a $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$.

Ejemplo 3.4 Consideremos el mismo caso que en ejemplo 3.3.

Claramente, en este ejemplo, $f^{-1}(\emptyset) = \emptyset$ y $f^{-1}(B) = A$,

$f^{-1}(\{0\}) = \{a\}$, porque $f(a) = 0$, $f^{-1}(\{1\}) = \{b, c\}$, porque $f(b) = f(c) = 1$.

Proposición 3.5 *Sea* $f : A \to B$ *una función,* $Y, Y_1, Y_2 \subseteq B$*.*

1. $Y_1 \subseteq Y_2 \Rightarrow f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$*;*
2. $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$*;*
3. $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$*;*
4. $f(f^{-1}(Y)) \subseteq Y$*.*
5. $X = f^{-1}(f(X)) \Leftrightarrow f$ *es inyectiva.*

Demostración:
Sólo probaremos la primera a modo de ejemplo, dejando las restantes al lector.®
Sabemos que $Y_1 \subseteq Y_2$ y queremos probar que $f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$, es decir, tenemos que ver que todo elemento que esté en $f^{-1}(Y_1)$ está también en $f^{-1}(Y_2)$. Repetimos que lo más importante al comenzar una de estas demostraciones es considerar qué "aspecto" tiene ese elemento. Vamos a la definición de conjunto preimagen y vemos que los elementos que están dentro del conjunto son de la forma x. Tomemos esa forma y tendremos la mitad de la demostración resuelta. Sea $x \in f^{-1}(Y_1)$, entonces, por la defineión de $f^{-1}(Y_1)$ necesariamente $f(x) \in Y_1$ y $Y_1 \subseteq Y_2$, en consecuencia $f(x) \in Y_2$ y $x \in f^{-1}(Y_2)$. Hemos probado que todo elemento de $f^{-1}(Y_1)$ es elemento de $f^{-1}(Y_2)$.

Observación 3.9 En general la definición de imagen de un conjunto les restulta bastante clara ya que es directa, es decir, $a \in X$ si y sólo si $f(a) \in f(X)$. El inconveniente se presenta con la preimagen, ya que $a \in f^{-1}(Y)$ si y sólo si $f(a) \in Y$.
Hagamos una pequeña comparación que tal vez sirva para recordar esta definición:

$$\begin{array}{c|c} 5 = x^{-1} \cdot 9 & a \in f^{-1}(Y) \\ \\ x \cdot 5 = x \cdot x^{-1} \cdot 9 & f(a) \in f(f^{-1}(Y)) \\ \\ x \cdot 5 = 9 & f(a) \in Y \end{array}$$

Observación 3.10 En la Unidad 1, observación 1.3 dijimos que el conjunto de partes de A se podía notar con 2^A, aclaremos esta notación a la luz del concepto de funciones. Dado un conjunto A se puede caracterizar a cada subconjunto $X \subseteq A$ con una función χ (denominada función característica) definida del siguiente modo:

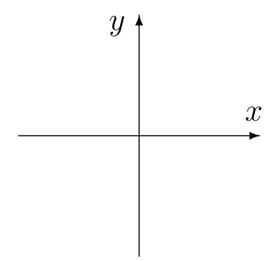
$$\chi(x) = \begin{cases} 1 & \text{si } x \in X \\ 0 & \text{si } x \notin X \end{cases}$$

Claramente $\chi : A \to \{0, 1\}$. Este conjunto se suele notar $\mathbf{2}$, entonces $\chi : A \to \mathbf{2}$. Dado que a cada subconjunto lo podemos identificar con su función característica, podemos identificar el conjunto de todos los subconjuntos de A como el conjunto de todas las funciones que van de A a $\mathbf{2}$, que se representa $\mathbf{2}^A$.

3.4. Funciones reales

En la sección anterior hablamos acerca de funciones de un conjunto A cualquiera en otro B. Cuando el dominio y la imagen son subconjuntos de los números reales, las funciones se denominan *funciones reales a variable real.* Se puede pensar que f mide cómo varía una cierta cantidad que depende de x, según la variación de x. Ya no podemos representarlas por diagramas de Venn, ni con tabla de valores porque los valores que puede llegar a tomar son infinitos.

Para representarlas por completo podemos usar las *coordenadas cartesianas*: dos rectas perpendiculares, que son representaciones de $\mathbb{R}$, en las mismas condiciones que representamos la recta. La horizontal se llama *eje de abscisas* y la vertical *eje de ordenadas*. Pese a que es frecuente usar la misma unidad de medida en ambos ejes, no es una condición necesaria. Es importante notar que la flecha, igual que en el caso de la recta real, marca el sentido positivo. (Hacia dónde va).



No ahondaremos más en funciones reales a variable real, porque los contenidos necesarios para este curso han sido vistos en el curso de nivelación. Sólo haremos mención, ya que hablamos de cómo se grafican las funciones reales, de la relación entre el gráfico y las propiedades de inyectividad o sobreyectividad.

Los valores de $f(x)$ se marcan en el eje de las ordenadas, es decir, en el eje y. Si una función no es epiyectiva quiere decir que hay alguna altura y por donde la función no pasa, es decir, una recta paralela al eje de las abscisas (x) a esa altura no corta a la función. Entonces:

f es *epiyectiva* si toda recta paralela al eje de las x *siempre* corta al gráfico de f.

Si la función no fuera inyectiva, para una cierta altura y existirán $x_1 \neq x_2$ tales que $f(x_1) = f(x_2) = y$. Es decir la recta paralela al eje de las abscisas que está a la altura y cortará al menos dos veces a la gráfica de la función.

f es *inyectiva* si toda recta paralela al eje x corta *a lo sumo* una vez al gráfico de f.

Entonces podemos afirmar:

f es *biyectiva* si toda recta paralela al eje x corta *exactamente* una vez al gráfico de f.

(✠) René Descartes, también llamado Renatus Cartesius (1596-1650), fue filósofo, matemático y físico, considerado como el padre de la geometría analítica y de la filosofía moderna. Hizo famoso el principio *cogito ergo sum*, (pienso, luego existo), pero ya existían formulaciones anteriores, alguna tan exacta a la suya como la de Gómez Pereira en 1554, por lo que ya en su siglo fue acusado de plagio. Escribió una parte de sus obras en latín, (la lengua internacional del conocimiento) y la otra en francés. Se lo asocia con los ejes cartesianos en geometría, con la iatromecánica y la fisiología mecanicista en medicina, con el principio de inercia en física, con el dualismo filosófico mente-cuerpo y el dualismo metafísico materia-espíritu. Su obra *Discurso del método* (1637), está caracterizada por su simplicidad y pretende romper con los interminables razonamientos escolásticos.

(♣) "Papar moscas" no siempre es improductivo: desde niño, debido a su mala salud, Descartes tuvo que pasar innumerables horas en cama. Aprovechaba para divagar e incluso se permitía perder el tiempo pensando en las musarañas. Teniendo su vista perdida en el techo una mosca se cruzó en su mirada, cosa que hizo que la siguiera con la vista durante un buen rato, mientras pensaba y se preguntaba si se podría determinar a cada instante la posición que tendría el insecto, por lo que pensó que si se conociese la distancia a dos superficies perpendiculares (en este caso la pared y el techo) se podría saber. Pensando en esto se levantó de la cama y agarrando un trozo de papel dibujó sobre él dos rectas perpendiculares: cualquier punto de la hoja quedaba determinado por su distancia a los dos ejes. A estas distancias las llamó *coordenadas del punto*: acababan de nacer las *Coordenadas Cartesianas.*

3.5. Ejercicios propuestos

3.5.1. Relaciones funcionales - Funciones

Ejercicio 3.1 Dada $\mathcal{R} = \{(1,3),\ (2,5),\ (3,3),\ (4,6),\ (5,6),\ (8,7)\} \subseteq \mathbb{N}\times\mathbb{N}$, hallar $\mathcal{R}^{op}$ y determinar, justificando la respuesta, si $\mathcal{R}$ y/o $\mathcal{R}^{op}$ son relaciones funcionales.

Ejercicio 3.2 Dadas las siguientes aplicaciones $f : A \to B$ decidir si son funciones, y en caso afirmativo si son inyectivas, epiyectivas y/o biyectivas.

1. $A = \mathbb{Q}$, $B = \{x : x \text{ es un cuadrado perfecto }\}$, $f(x) = x^2$.
2. $A = \mathbb{N}$, $B = \{x : x \text{ es un cuadrado perfecto }\}$, $f(x) = x^2$.

3. $A = \mathbb{N}$, $B = \mathbb{N}$, $f(x) = x^2$.
4. $A = \mathbb{Z}$, $B = \mathbb{N}$, $f(x) = x^2$.

Ejercicio 3.3 © Sea $f : A \longrightarrow B$ Probar que si f es una función biyectiva, entonces que $f^{-1} : B \longrightarrow A$ también lo es.

Ejercicio 3.4 Sea $f : A \longrightarrow B$, $g : B \longrightarrow C$.

1. Si f y g son inyectivas, entonces $g \circ f$ es inyectiva
2. Si f y g son epiyectivas, entonces $g \circ f$ es epiyectiva

Concluir que si Si f y g son biyectivas, entonces $g \circ f$ es biyectiva. Además $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. ¿Es necesario probarlo?

Ejercicio 3.5 ©© Sea $f, f_1, f_2 : A \longrightarrow B$, $g, g_1, g_2 : B \longrightarrow C$, $h_1, h_2 : C \longrightarrow D$. Probar las siguiente equivalencias:

1. g es inyectiva $\Leftrightarrow$ $g \circ f_1 = g \circ f_2$ entonces $f_1 = f_2$
2. g es epiyectiva $\Leftrightarrow$ $h_1 \circ g = h_2 \circ g$ entonces $h_1 = h_2$
3. g es biyectiva $\Leftrightarrow$ $g \circ f_1 = g \circ f_2$ entonces $f_1 = f_2$ y $h_1 \circ g = h_2 \circ g$ entonces $h_1 = h_2$

Ejercicio 3.6 Sea $f : A \longrightarrow B$, $g : B \longrightarrow C$ tal que $g \circ f$ es biyectiva. ¿Qu se puede afirmar acerca de f y g?

Ejercicio 3.7 Sea $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \longrightarrow D$ tal que $h \circ g \circ f$ es biyectiva. ¿Se puede afirmar algo acerca de f, g o h ?

Ejercicio 3.8 Sea $f : A \to B$ una función, $X, X_1, X_2 \subseteq A$, $Y, Y_1, Y_2 \subseteq B$. Considerando que

$$f(X) = \{f(a) : a \in X\} \subseteq B, \text{ y } f^{-1}(Y) = \{a \in A : f(a) \in Y\} \subseteq A,$$

Probar que:

1. (®) $X_1 \subseteq X_2 \;\Rightarrow\; f(X_1) \subseteq f(X_2)$; $\quad Y_1 \subseteq Y_2 \;\Rightarrow\; f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$.
2. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$; $\quad f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.
3. ($\diamond$) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$; $\quad f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.
4. © $f(X_1 \cap X_2) = f(X_1) \cap f(X_2) \;\Leftrightarrow\; f$ es inyectiva.

5. $f^{-1}(B \setminus Y) = A \setminus f^{-1}(Y)$.
6. © ($\diamond$) $f(X') = [f(X)]' \Leftrightarrow f$ es biyectiva.
7. ($\diamond$) $f(X) = \emptyset \Leftrightarrow X = \emptyset$; $f^{-1}(Y) = \emptyset \Leftrightarrow Y \cap f(X) = \emptyset$.
8. ($\diamond$) $X \subseteq f^{-1}(f(X))$; $f(f^{-1}(Y)) \subseteq Y$.

Ejercicio 3.9 Sean $f : A \to B$, $g : C \to D$. Se define $h : A \times C \to B \times D$ por : $h((x, y)) = (f(x), g(y))$. Probar que:

1. ($\diamond$) Si f y g son inyectivas, h es inyectiva.
2. © Si h es inyectiva, f y g son inyectivas.
3. ($\diamond$) Si f y g son sobreyectivas, h es sobreyectiva.
4. © Si h es sobreyectiva, f y g son sobreyectivas.

Concluir que f y g son biyectivas, si y sólo si h también lo es.

Capítulo 4

De los naturales a los reales

Números naturales. Principio de inducción. Números enteros.
Definición del conjunto $\mathbb{Q}$ de los números racionales.
Propiedades. Orden. Irracionales.
El conjunto $\mathbb{R}$ de los números reales: la recta real. Existencia de raíces en $\mathbb{R}$.
Potenciación de exponente entero.
Raíz aritmética. Potenciación de exponente racional.

Un número es una entidad abstracta que representa una cantidad. El símbolo de un número recibe el nombre de numeral. Los números se usan con mucha frecuencia en la vida diaria como etiquetas (números de teléfono, numeración de carreteras), como indicadores de orden (números de serie), como códigos (ISBN), etc. En matemática, la definición de número se extiende para incluir abstracciones tales como números fraccionarios, negativos, irracionales, trascendentales, complejos...

Los números más conocidos son los números naturales 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ..., que se usan para contar. Si añadimos los números negativos obtenemos los enteros. Cocientes de enteros generan los números racionales. Si incluimos todos los números que son expresables con decimales pero no con fracciones de enteros, obtenemos los números reales; si a éstos les añadimos los números complejos, tendremos todos los números necesarios para resolver cualquier ecuación algebraica. Podemos ampliar aún más los conjuntos de números, pero ya escapa a los contenidos de este curso. Entre los reales, existen números que no son soluciones de una ecuación polinomial o algebraica. Reciben el nombre de transcendentales. El ejemplo más famoso de estos números es π (Pi), otro ejemplo fundamental e igual de importante es e, base de los logaritmos naturales. Estos dos números están relacionados entre sí por la identidad de Euler, también llamada la fórmula más importante del mundo.

$$e^{i\pi} + 1 = 0$$

4.1. Números naturales

Un número natural es cualquiera de los números que se pueden usar para contar los elementos de un conjunto. Reciben ese nombre porque fueron los primeros que utilizó el ser humano para contar objetos de la naturaleza.

Pensemos un poco: ¿Cómo es el conjunto de los números que aparecen naturalmente al contar?

1. Cuando estoy contando, claramente, lo primero que noto es la diferencia entre "no tengo nada" y "tengo algo", entonces encuentro que existe un primer elemento en mi cuenta.
2. Nuestro universo es infinito, entonces sé que, tenga lo que tenga, siempre puedo agregar uno más.
3. El primer elemento, que por algo es el primero, no es el sucesor de ninguno.
4. Ese elemento que "le sigue" a otro es único.
5. Y no hay otra cosa. Es decir: cualquier conjunto numérico que satisfaga que tiene este primer elemento y dado cualquier elemento tiene el que sigue, es todo el conjunto.

Si escribimos estas ideas maás "matemáticamente" aparecen los axiomas de Peano o postulados de Peano que definen de manera exacta al conjunto de los números naturales. Fueron establecidos por el matemático italiano Giuseppe Peano (1858-1932), en el siglo XIX.

Definición 4.1 Axiomas de Peano Existe un conjunto, que notaremos $\mathbb{N}$, y llamaremos el *conjunto de los números naturales* que satisface las siguientes propiedades:

P1) Existe un primer elemento, sea p.

P2) Para todo $x \in \mathbb{N}$, existe un elemento x', llamado el *sucesor* de x.

P3) p no es el sucesor de ningún elemento de $\mathbb{N}$.

P4) Si $x' = y'$, entonces $x = y$.

P5) **Axioma de Inducción:** Si $M \subseteq \mathbb{N}$ satisface:

(i) $p \in M$

(ii) Si $x \in M$, entonces $x' \in M$

entonces, $M = \mathbb{N}$.

El hecho de considerar el 0 como natural, o no, es tema de controversia. Normalmente se considera que lo es según si se necesita o no. Algunos matemáticos (especialmente los que trabajan en teoría de números) prefieren no reconocer el cero como un número natural, mientras que otros, especialmente los que se dedican a teoría de conjuntos, lógica e informática, tienen la postura opuesta. En este curso tomaremos 0 como primer elemento de $\mathbb{N}$.

Notación 4.1 $0' = 1$, $1' = 2$, $2' = 3$ y así sucesivamente.

Proposición 4.1 *Todo número natural, distinto de cero, es el sucesor de otro número natural. En símbolos, si $x \in \mathbb{N}, x \neq 0$, entonces $x = y'$, para algún $y \in \mathbb{N}$.*

Demostración: Para esta demostración, igual que para toda demostración acerca de números naturales, usaremos el axioma de inducción. Es decir, definiremos un subconjunto M de $\mathbb{N}$ y probaremos que satisface las condiciones (i) e (ii) del principio de inducción de la definición 4.1, y concluiremos que $M = \mathbb{N}$.
Sea $M = \{0\} \cup \{x \in \mathbb{N} : \exists y \in \mathbb{N} : x = y'\}$
(i) $0 \in M$ por construcción
(ii) Supongamos que $x \in M$, entonces x' es el sucesor de un elemento natural y, por lo tanto, $x' \in M$. Por el principio de inducción, afirmamos que $M = \mathbb{N}$ y, en consecuencia, se verifica el teorema. $\square$

© Enunciaremos, a continuación, una serie de teoremas y propiedades, cuyas demostraciones son de lectura optativa y nos permitirán munir de una estructura algebraica y de orden al conjunto de los números naturales.

Teorema 4.1 Definición de suma *Dados dos números naturales x e y, es posible definir de única forma otro número natural llamado* suma*, que se nota $x + y$, de modo que se satisfagan las propiedades:*

(S_0) $x + 0 = x$ (0: elemento neutro para la suma)

(S_1) $x + y' = (x + y)'$

Demostración: Debemos demostrar la existencia y la unicidad de la operación. Veamos en primer lugar que es única. Para ello supongamos que existen dos formas de hacerlo y veamos que coinciden para todo número natural.
Sean $A_x(y) = x +_A y$, $B_x(y) = x +_B y$ dos formas de definir la suma que satisfacen (S_0) e (S_1) y M el subconjunto de $\mathbb{N}$ en que las dos formas coinciden, es decir: $M = \{y \in \mathbb{N} : A_x(y) = B_x(y)\}$. Usaremos el principio de inducción para verificar que $M = \mathbb{N}$
(i) $A_x(0) = x + 0 = x = B_x(0)$, entonces $0 \in M$
(ii) Supongamos que $y \in M$, es decir que $A_x(y) = B_x(y)$ y debemos probar que $y\,' \in M$, es decir que $A_x(y\,') = B_x(y\,')$. $A_x(y\,') = x + y\,' = (x + y)\,' = (A_x(y))\,' = (B_x(y))\,' = B_x(y\,')$.
Como se verifican (i) e (ii) del axioma de inducción, resulta que $M = \mathbb{N}$ y, en consecuencia, el modo de definir la suma es único.
Veamos ahora la existencia de esta operación. Nuevamente haremos uso del axioma de inducción: sea M el subconjunto de números naturales tales que la definición de suma satisfaciendo S_0 y S_1 es posible.
(i) $0 \in M$, ya que $0 + 0 = 0$ y $0 + y\,' = (0 + y)\,' = y\,'$.
(ii) Supongamos que $x \in M$ y definamos $x\,' + y = (x + y)\,'$.
Vemos que $x\,' + 0 = (x + 0)\,' = x\,'$ y $x' + y' = (x + y')' = (x + y)'' = (x' + y)'$, es decir se verifican S_0 y S_1. Entonces $x\,' \in M$ para todo $x \in M$ y aplicando el axioma de inducción afirmamos que1 $M = \mathbb{N}$. en consecuencia, la definición es posible para todo número natural. $\square$

Observación 4.1 En la demostración del teorema hemos visto las siguientes propiedades de la suma:

1. $x + 1 = 1 + x = x'$
2. $x + y' = (x + y)' = x' + y$

Proposición 4.2 *La suma de números naturales satisface las siguientes propiedades, para todo $x, y, z \in \mathbb{N}$:*

(S1) $x + (y + z) = (x + y) + z$ (propiedad asociativa de la suma)

(S2) $x + y = y + x$ (propiedad conmutativa de la suma)

Demostración:
Propiedad asociativa:
Dados $x, y \in \mathbb{N}$, consideremos el conjunto $M = \{z \in \mathbb{N} : (x + y) + z = x + (y + z)\}$. (i) $0 \in M$, ya que $(x + y) + 0 = x + y = x + (y + 0)$.
(ii) Supongamos que $z \in M$, es decir que $(x+y)+z = x+(y+z)$. Probaremos

$(x+y)+z' = x+(y+z')$. $(x+y)+z' = ((x+y)+z)' = (x+(y+z))' = x+(y+z)' = x+(y+z')$. De (i) y (ii) concluimos que $M = \mathbb{N}$.

Propiedad conmutativa:
Dado $x \in \mathbb{N}$, consideremos el conjunto $M = \{y \in \mathbb{N} : x+y = y+x\}$.
(i) $0 \in M$, ya que $y+0 = y = 0+y$.
(ii) Supongamos que $z \in M$, es decir que $(x+y)+z = x+(y+z)$. Probaremos $(x+y)+z\,' = x+(y+z\,')$. $(x+y)+z\,' = ((x+y)+z)\,' = (x+(y+z))\,' = x+(y+z)\,' = x+(y+z\,')$. De (i) y (ii) concluimos que $M = \mathbb{N}$. □

Teorema 4.2 Definición de producto *Dados dos números naturales x e y, es posible definir de única forma otro número natural llamado* producto, *que se nota $x \cdot y$, de modo que se satisfagan las propiedades:*

(P_0) $x \cdot 0 = 0$

(P_1) $x \cdot y\,'\,' = x \cdot y + x$

Demostración: Igual que en el caso de la suma, veamos primero que este modo es único. Para ello supongamos que existen dos formas de hacerlo y veamos que coinciden para todo número natural.
Sean $A_x(y) = x \cdot_A y$, $B_x(y) = x \cdot_B y$ dos formas de definir el producto que satisfacen P_0 y P_1 y M el subconjunto de $\mathbb{N}$ en que los dos coinciden: $M = \{y \in \mathbb{N} : A_x(y) = B_x(y)\}$.
(i) $A_x(0) = x \cdot 0 = 0 = B_x(0)$, entonces $0 \in M$
(ii) Supongamos que $y \in M$, es decir que $A_x(y) = B_x(y)$ y debemos probar que $y\,' \in M$, es decir que $A_x(y\,') = B_x(y\,')$. $A_x(y\,') = x \cdot y\,' = x \cdot y + x = (A_x(y)) + x = (B_x(y)) + x = B_x(y\,')$.
Aplicando el axioma de inducción aformamos que que $M = \mathbb{N}$ y, que el modo de definir el producto es único.
Veamos ahora la existencia de esta operación: sea M el subconjunto de números naturales tales que la definición de producto satisfaciendo P_0 y P_1 es posible.
(i) $0 \in M$, ya que $0 \cdot 0 = 0$ y $0 \cdot y\,' = 0 \cdot y + 0 = 0 + 0 = 0$.
(ii) Supongamos que $x \in M$ y definamos $x\,' \cdot y = x \cdot y + y$. De este modo se verifican P_0 y P_1 ya que $x\,' \cdot 0 = x \cdot 0 + x = x$ y $x\,' \cdot y\,' = x \cdot y\,' + y\,'$. Entonces $M = \mathbb{N}$ por el axioma de inducción y la definición es posible para todo número natural. □

Proposición 4.3 *El producto de números naturales satisface las siguientes propiedades:*

$(P1)$ $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (propiedad asociativa del producto)

$(P2)$ $x \cdot y = y \cdot x$ (propiedad conmutativa del producto)

$(P3)$ $x \cdot 1 = 1 \cdot x = x$ (1: elemento neutro para el producto)

Demostración: Las demostraciones son totalmente análogas a las vistas para la suma y quedan a cargo del lector. Ⓡ □

Proposición 4.4 *El producto y la suma de números naturales satisfacen la siguiente propiedad:*

$(D1)$ $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (propiedad distributiva)

Demostración: Sea $M = \{z \in \mathbb{N} : x \cdot (y + z) = (x \cdot y) + (x \cdot z)\}$
(i) $x \cdot (y + 0) = x \cdot y = (x \cdot y) + 0 = (x \cdot y) + (x \cdot 0)$, por lo tanto $0 \in M$
(ii) Supongamos que $z \in M$, queremos probar que $z' \in M$. Es decir, si $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ probemos que $x \cdot (y + z') = (x \cdot y) + (x \cdot z')$.
$x \cdot (y + z') = x \cdot (y + z)' = x \cdot (y + z) + x = ((x \cdot y) + (x \cdot z)) + x = (x \cdot y) + ((x \cdot z) + x) = (x \cdot y) + (x \cdot z')$.
De (i) e (ii) por el axioma de inducción afirmamos que $M = \mathbb{N}$ y, en consecuencia, la propiedad distributiva del producto con respecto a la suma es válida para toda terna de números naturales. □

Definición 4.2 Diremos que el número natural a es *menor* que b y escribiremos $a < b$, si existe un número natural $c \neq 0$ tal que $a + c = b$.

Teorema 4.3 *Dados $x, y \in \mathbb{N}$ se verifica una y sólo uno de los siguientes casos: $x < y$, $x = y$ ó $y < x$.*

Demostración: Sea $x \in \mathbb{N}$, fijo, cualquiera, $M = \{y : x < y \text{ ó } x = y \text{ ó } y < x\}$
(i) Veamos que $0 \in M$. Si $x = 0$, se verifica $x = y$. Si $x \neq 0$, entonces, como 0 es el primer elemento, necesariamente $0 < x$.
(ii) Supongamos que $y \in M$ y probemos que $y' \in \mathbb{N}$. Dado que $y \in M$ pueden ocurrir 3 casos: $x < y$, $x = y$, $y < x$. Como $y < y'$, por la propiedad transitiva, si $x < y$ ó $x = y$ resulta $x < y'$ e $y' \in M$. Si fuera $y < x$, entonces existe $z \in \mathbb{N}$, $z \neq 0$ tal que $y + z = x$. Como $z \neq 0$ resulta $z = w'$, para algún $w \in \mathbb{N}$ y $x = y + w' = (y + w)' = y' + w$, de donde, si $w = 0$ resulta $x = y'$ y si $w \neq 0$, $y' < x$. En cualquier caso $y' \in M$.
Por el axioma de inducción inferimos que $M = \mathbb{N}$.
Hemos demostrado que para un par de números naturales x, y se da al menos una de las posibilidades $x < y, x = y$ Ó $y < x$. Es inmediato ver que no es posible que se den simultáneamente. □

Definición 4.3 Un par $(A, \leq)$ tal que A es un conjunto no vacío y $\leq$ una relación de orden en A se dice un *conjunto ordenado*. Si dados $x, y \in A$ se verifica $x \leq y$ ó $y \leq x$, $(A, \leq)$ se dice un *conjunto totalmente ordenado* o *cadena.*

Proposición 4.5 *Sea $\leq$ la relación definida en $\mathbb{N}$ por: $x \leq y$ si y sólo si $x < y$ ó $x = y$, entonces $(\mathbb{N}, \leq)$ es una cadena.*

Demostración: Ejercicio para el lector.® □

Teorema 4.4 Leyes de monotonía

(M1) *Si $a < b$, entonces $a + c < b + c$,*

(M2) *Si $a < b$, $c \neq 0$, entonces $a \cdot c < b \cdot c$.*

Demostración: Ejercicio para el lector.® □

Teorema 4.5 Leyes de cancelación

(C1) *Si $a + x = a + y$, entonces $x = y$,*

(C2) *Si $a \cdot x = a \cdot y$, $a \neq 0$, entonces $x = y$.*

Demostración: Ejercicio para el lector.® □

Lema 4.1 *Entre un número natural y su sucesor no existe ningún número natural. En símbolos: si $x \leq y \leq x'$, entonces $x = y$ ó $x' = y$.*

Demostración: Sea $M = \{x : (x \leq y \leq x') \Rightarrow (x = y) \text{ ó } (x' = y)\}$
(i) Sea $0 \leq y \leq 0'$ Si $y = 0$ no hay nada que probar. Si $y \neq 0$, entonces $y = z'$ para algún $z \in \mathbb{N}$ y como $z' \leq 0'$ podemos decir $z' + c = 0'$ o, lo que es lo mismo, $(z + c)' = 0'$ y por P4 $z + c = 0$, es decir $z \leq 0$ y dado que 0 es el primer elemento, necesariamente, $z = 0$ e $y = 0'$. Entonces $0 \in M$.
(ii) Supongamos $x \in M$ y probemos $x' \in M$. Supongamos $x' \leq y \leq x''$. Por definición de $\leq$ es equivalente a que existen $z_1, z_2 \in \mathbb{N}$ tales que $x' + z_1 = y$, $y + z_2 = x''$. Como $(x + z)' = y$ es claro que $y \neq 0$ y puedo hallar $w \in \mathbb{N}$ tal que $w' = y$. Reemplazando obtengo $(x + z_1)' = w'$ y $w' + z_2 = x''$ o, lo que es lo mismo, $(w + z_2)' = x''$. Por P3 podemos afirmar que $x + z_1 = w$ y $w + z_2 = x'$, que es equivalente a $x \leq w \leq x'$. Por hipótesis inductiva, $x = w$ ó $w = x'$. Si $x = w$ resulta $x' = w' = y$, y si $x' = w$ resulta $x'' = w' = y$. En cualquier caso se verifica el lema.

□

© Fin de la "zona optativa".

4.1.1. Principio de inducción

A partir de la definición, todas las demostraciones referidas a número natural las hemos hecho haciendo uso del quinto axioma de Peano, conocido como el axioma de inducción. Este axioma nos proporciona un método de demostración llamado por inducción o recurrencia y suele enunciarse como *principio de inducción*.

Axioma de inducción: Si S es un subconjunto de $\mathbb{N}$ que satisface:

Ax_1: $0 \in S$,

Ax_2: Si $n \in S$, entonces $n' \in S$,

entonces,

Ax_3: $S = \mathbb{N}$.

Y equivalentemente:

Principio de inducción: Si $P(n)$ es una proposición relativa al número natural n y se verifica:

PI_1: $P(0)$ es verdadera,

PI_2: Si $P(k)$ es verdadera, entonces $P(k+1)$ es verdadera, para cualquier $k \in \mathbb{N}$,

entonces,

PI_3: $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Es decir, para demostrar una cierta propiedad acerca de números naturales debemos hacer:

(i) *caso inicial (o caso base)*,

(ii) *paso inductivo*

(iii) *conclusión*.

Observación 4.2 Hemos dicho que son equivalentes el axioma de inducción y el principio de inducción. Esta equivalencia está dada por lo que se llama el *conjunto de verdad asociado a una proposición*. Sea $S = \{n \in \mathbb{N} : P(n) \text{ es verdadera}\}$, entonces S es el conjunto de verdad asociado a la proposición P y es evidente que "$0 \in S$"$\Leftrightarrow$"$P(0)$ es verdadera", como también "Si $n \in S$, entonces $n' \in S$" es equivalente a "Si $P(k)$ es verdadera, entonces $P(k+1)$ es verdadera". Esto hace que las conclusiones sean equivalentes. Como $S = \mathbb{N}$ podemos afirmar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Otra cosa a considerar es que el principio de inducción se puede aplicar "a partir de...", es decir si nuestro caso base no se verifica para $n < 3$ y es verdadero para $n = 3$, y probamos el paso inductivo, entonces podemos afirmar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$, $n \geq 3$. Por ejemplo, podría ser el caso de una proposición que asocie n a la cantidad de lados de un polígono, que es imposible construir con menos de 3 lados.

Ejercicio 4.1 Probemos que $5^n \geq 2^n + 3^n$, para todo $n > 0$.
Caso inicial: Como debe ser $n > 0$, consideramos $n = 1$.
$5^1 = 5,\ \ 2^1 + 3^1 = 2 + 3 = 5$. Como $5 = 5$, se verifica.
Paso inductivo: supongamos que es válido para $n = k$ y lo probamos para $n = k+1$. Es decir, la hipótesis inductiva es: $5^k \geq 2^k + 3^k$. Queremos probar: $5^{k+1} \geq 2^{k+1} + 3^{k+1}$.
$5^{k+1} = 5 \cdot 5^k \geq 5 \cdot (2^k + 3^k) = 5 \cdot 2^k + 5 \cdot 3^k > 2 \cdot 2^k + 3 \cdot 3^k = 2^{k+1} + 3^{k+1}$.
Conclusión: Por lo tanto $5^n \geq 2^n + 3^n$, para todo $n > 0$.

Observación 4.3 Antes de avanzar más en este tema, dado que ya tenemos las herramientas para hacerlo, completemos la explicación propuesta en la Unidad 1, observación 1.3, con un esbozo de demostración.

Probemos que $|\mathbf{2}^A| = 2^{|A|}$, por inducción sobre el orden de A.

Caso base: $|A| = 0$, es decir $A = \emptyset$
¿Cuántos subconjuntos tiene $\emptyset$? sólo él mismo, es decir, $|\mathbf{2}^A| = 1 = 2^0 = 2^{|A|}$ y se verifica la proposición.

Paso inductivo: supongamos que es válido para $|A| = k$ y probémoslo para $|A| = k + 1$.
Sea A un conjunto con $k+1$ elementos que podemos pensarlo como la unión de dos conjuntos: $A = \{a_1, a_2, \ldots, a_k\} \cup \{a_{k+1}\}$.

Pensemos en los subconjuntos de A y el elemento a_{k+1}: Todos los subconjuntos de A pueden clasificarse en todos los subconjuntos de A a los que no pertenece a_{k+1} y todos los subconjuntos de A a los que pertenece a_{k+1}. La cantidad de subconjuntos de A a los que no pertenece a_{k+1} es 2^k, ya que son todos los subconjuntos de un conjunto con k elementos. Los subconjuntos de A a los que pertenece a_{k+1} son exactamente los mismos que los anteriores a los que se une este elemento, por lo tanto también son 2^k. Si sumamos todos los subconjuntos queda $2^k + 2^k = 2.2^k = 2^{k+1}$.

Conclusión, si $|A| = n$ entonces $|\mathbf{2}^A| = 2^n$, para todo $n \in \mathbb{N}$.

Definiciones por recursión:

Supongamos que tenemos una bolsa que contiene a los números naturales. Metemos la mano dentro y sacamos uno. ¿qué puede ocurrir? Puede ser que el número escogido sea el primero o no. Si es el primero, es el primero. Si no es el primero, como demostramos en la proposición 4.1 es el sucesor de otro. Este hecho nos permite hacer definiciones en forma recursiva del siguiente modo

R_1: Caso base: definimos cuánto vale en 0. (O en el primer elemento válido).

R_2: Paso recursivo: definimos cuánto vale en $n+1$ basándonos en lo que vale en n.

Tal vez la definición por recursión más conocida sea la de número factorial. Dado un número natural n, se llama factorial de n, y se nota $n!$, al número definido de la siguiente manera:

$$0! = 1$$
$$(n+1)! = (n+1) \cdot n!$$

Veamos cómo encontrar, por ejemplo, $5!$.
$5! = 5 \cdot 4! = 5 \cdot (4 \cdot 3!) = 5 \cdot (4 \cdot (3 \cdot 2!)) = 5 \cdot (4 \cdot (3 \cdot (2 \cdot 1!))) = 5 \cdot (4 \cdot (3 \cdot (2 \cdot (1 \cdot 0!)))) =$
$= 5 \cdot (4 \cdot (3 \cdot (2 \cdot (1 \cdot 1)))) = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

Ejercicio 4.2 Consideremos la sucesión definida inductivamente (o recursivamente) del siguiente modo: $a_0 = 3, a_{n+1} = 2a_n$. Buscamos un término general para esta sucesión.
Escribamos algunos términos:

$$a_0 = 3 = 3 \cdot 2^0$$
$$a_1 = 2 \cdot a_0 = 2 \cdot 3 \cdot 2^0 = 3 \cdot 2^1$$
$$a_2 = 2 \cdot a_1 = 2 \cdot 3 \cdot 2^1 = 3 \cdot 2^2$$
$$a_3 = 2 \cdot a_2 = 2 \cdot 3 \cdot 2^2 = 3 \cdot 2^3$$
$$\ldots$$

Parece ser que el término general es $a_n = 3 \cdot 2^n$. Verifiquémoslo usando el principio de inducción.
Caso inicial: $n = 0$. $a_0 = 3 \cdot 2^0 = 3 \cdot 1 = 3$. Se verifica.
Paso inductivo: Supongamos que $a_k = 3 \cdot 2^k$ y probemos que $a_{k+1} = 3 \cdot 2^{k+1}$.
$a_{k+1} = 2 \cdot a_k = 2 \cdot (3 \cdot 2^k) = 3 \cdot 2^{k+1}$.
Conclusión: Por el principio de inducción podemos afirmar que $a_n = 3 \cdot 2^n$, para todo $n \in \mathbb{N}$.

Otro enunciado para el principio de inducción es lo que llamamos el *principio fuerte de inducción* o *principio de inducción global*. Si $P(n)$ es una proposición relativa al número natural n y se verifica:

(i) $P(0)$ es verdadera,

(ii) Si $P(k)$ es verdadera para todo $k < n$, entonces $P(n)$ es verdadera,

entonces, $P(n)$ es verdadera para todo $n \in \mathbb{N}$.
Es un ejericicio interesante, y no demasiado complicado, probar la equivalencia entre ambas formas del principio de inducción. ®
Veamos un ejemplo de demostración con este procedimiento:

Ejercicio 4.3 Buscamos un término general para la sucesión definida recursivamente: $a_0 = 3, a_1 = 6, a_{n+1} = 2 \cdot a_n - a_{n-1} + 2^n, n > 2$. Comencemos escribiendo algunos términos:

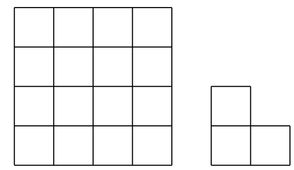
$$\begin{aligned}
&a_0 = 3\\
&a_1 = 6\\
&a_2 = 2 \cdot a_1 - a_0 + 2^1 = 3 + 2^3\\
&a_3 = 2 \cdot a_2 - a_1 + 2^2 = 4 + 2^4\\
&a_4 = 2 \cdot a_3 - a_2 + 2^3 = 5 + 2^5\\
&\ldots
\end{aligned}$$

El término general parece ser: $a_n = (n + 1) + 2^{(n+1)}$. Verifiquémoslo por inducción global:
Caso inicial: $n = 0$ $a_0 = (0 + 1) + 2^{(0+1)} = 1 + 2 = 3$. Se verifica.
Paso inductivo: Supongamos que la fórmula es válida para todo $k < n$ y probémosla para n.
$a_n = 2 \cdot a_{n-1} - a_{n-2} + 2^{n-2}$.
Claramente $n - 1 < n$ y $n - 2 < n$, entonces vale $a_{n-1} = n + 2^n$ y $a_{n-2} = (n - 1) + 2^{(n-1)}$ (es nuestra hipótesis inductiva) podemos reemplazar en la definición recursiva:
$a_{n-1} = n + 2^n$ y $a_{n-2} = (n - 1) + 2^{(n-1)}$, entonces obtenemos:
$a_n = 2 \cdot a_{n-1} - a_{n-2} + 2^{n-1} = 2 \cdot (n + 2^n) - ((n - 1) + 2^{(n-1)}) + 2^{(n-1)} = (n + 1) + 2^{(n+1)}$. Concluimos entonces que $a_n = (n + 1) + 2^{(n+1)}$ para todo $n \in \mathbb{N}$.

(♣) Pongamos un último desafío a demostrar por inducción:

Sea un cuadrado formado por $2^n \times 2^n$ cuadraditos como se muestra en la figura (hemos ilustrado el caso $n = 2$).

Supongamos que se suprime uno de los cuadraditos al azar. Demostrar que la superficie que queda, cualquiera que sea el cuadradito suprimido, siempre puede ser cubierta completamente con azulejos formados por tres cuadraditos en forma de L, como el que se muestra en la figura, sin que queden huecos ni se produzcan solapamientos.



(♣) La anécdota del modo de pago del juego de ajedrez, con que pretendía hacerse rico su creador es conocida. Tal vez no lo es tanto el ardid utilizado por el matemático de la corte para hacer que en verdad el inventor quede en deuda con el rey.
El pedido del inventor es que le dieran un grano de trigo por el primer cuadrado, dos por el segundo, cuatro por el tercero y así seguir sumando el duplo del anterior hasta el cuadradito 64. La propuesta del matemático de la corte es ofrecerle esta misma suma, pero hasta el infinito. Como el inventor aceptó, el matemático hizo la siguiente cuenta:

Llamemos S a la suma total que recibirá el inventor. Entonces
$S = 1 + 2 + 4 + 8 + 16 + \cdots$
$2 \cdot S = 2 + 4 + 8 + 16 + \cdots$, es decir
$2 \cdot S = S - 1$ y restando S a ambos miembros resulta $S = -1$.

En consecuencia el inventor debe un grano de trigo al rey. ¿Es esto cierto?

4.1.2. Principio de buena ordenación

Definición 4.4 Un conjunto ordenado $(A, \leq)$ es un *conjunto bien ordenado* si todo subconjunto no vacío de A tiene primer elemento. En símbolos: Si $\emptyset \subset \mathcal{H} \subseteq A$, existe $p \in \mathcal{H}$ tal que $p \leq h$, para todo $h \in \mathcal{H}$.

Teorema 4.6 Principio de buena ordenación $\mathbb{N}$ *es bien ordenado. O lo que es lo mismo: todo subconjunto no vacío de números naturales posee primer elemento.*

Demostración: Sea $\emptyset \subset \mathcal{H} \subseteq \mathbb{N}$, entonces $h \in \mathcal{H}$. Puede ser $h = 0$ ó $h \neq 0$.

Si $h = 0$, como $0 \leq n$ para todo $n \in \mathbb{N}$, claramente $0 \leq h$ para todo $h \in \mathcal{H} \subseteq \mathbb{N}$.

Vamos a continuar esta demostración por dos caminos diferentes, sólo para mostrar diferentes (muy diferentes) formas de demostrar una proposición:

(1) Usando inducción:

Si $0 \notin \mathcal{H}$, consideremos el conjunto $K = \{k \in \mathbb{N} : k < h, \text{ para todo } h \in \mathcal{H}\}$. Como $0 \notin \mathcal{H}$, es claro que $0 \in K$. Por el axioma de inducción existe un elemento $k \in K$ tal que $k + 1 \notin K$, ya que si así no fuera se cumplirían el caso base y el paso inductivo y por el axioma de inducción sería $K = \mathbb{N}$, lo cual es imposible ya que $\mathcal{H} \neq \emptyset$.

Como $k < h$ para todo $h \in \mathcal{H}$ resulta que $k + 1 = p \leq h$ para todo $h \in \mathcal{H}$ y p es el primer elemento de $\mathcal{H}$.

(2) Por descenso infinito:

Si $h \neq 0$, entonces $h = k_0 + 1$, si $k_0 \leq h$ para todo $h \in \mathcal{H}$ encontramos el primer elemento.
Si $k_0 \not\leq h$ para todo $h \in \mathcal{H}$, existe algún $k_1 \in \mathcal{H}$, $k_1 < k_0$, puede ser $k_1 \leq h$ para todo $h \in \mathcal{H}$ y encontramos el primer elemento.
Si $k_1 \not\leq h$ para todo $h \in \mathcal{H}$, existe algún $k_2 \in \mathcal{H}$, $k_2 < k_1$, puede ser $k_2 \leq h$ para todo $h \in \mathcal{H}$ y encontramos el primer elemento.
Si $k_2 \not\leq h$ para todo $h \in \mathcal{H}$, existe algún $k_3 \in \mathcal{H}$, $k_3 < k_1$, puede ser $k_3 \leq h$ para todo $h \in \mathcal{H}$ y encontramos el primer elemento.
Iterando el procedimiento construimos una sucesión decreciente $k_0 > k_1 > k_2 > ... \subseteq \mathcal{H}$ y como $|\mathcal{H}|$ es finito esta sucesión para en un cierto k_r que verifica $k_r \leq h$ para todo $h \in \mathcal{H}$, es decir, k_r es el primer elemento del conjunto $\mathcal{H}$. □

(♣) Los números naturales se caracterizan por tener siempre “el menor de ellos” pero ¿Existe un número natural mayor que todos? Sea **N** el más grande de todos los números naturales. Multipliquemos **N**$\times$ **N**. Claramente no puede ser mayor que **N** porque es el mayor de todos. Tampoco puede ser menor porque el producto de dos números naturales nunca es menor que ambos factores. La única posibilidad es que **N**$\times$**N**=**N** y el único número natural positivo que lo satisface es **N**= 1. Entonces 1 es el mayor de todos los números naturales positivos. ¿1 es el mayor número natural? ¿Dónde está el error?

4.2. Números enteros

Dados dos números naturales a, b, la ecuación $a + x = b$ tiene solución única $x = b - a$ para $a \leq b$. Para que esta ecuación tenga solución sin restricciones, hagamos la siguiente construcción:
Consideremos en $\mathbb{N} \times \mathbb{N}$ la relación $\mathcal{R}_1$ definida por: $(a, b)\mathcal{R}_1(c, d)$ si y sólo si $a + d = c + b$.

Observación 4.4 Sabemos que para $a, b, c, d \in \mathbb{N}$ cualesquiera está definida $a + d = c + b$, y en realidad lo que estamos pidiendo es que $a - b = c - d$, es decir, dos pares están relacionados si al restar el segundo del primero se obtiene el mismo resultado.

$\mathcal{R}_1$ es claramente una relación de equivalencia (Ⓡ ejercicio para el lector) y definimos $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\mathcal{R}_1$. En este conjunto cociente, para simplificar la notación la clase del par (a, b) la notamos simplemente $[a, b]$.
$\mathbb{Z}$ contiene una "copia" de $\mathbb{N}$ por la función $Incl_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ definida por: $f(x) = [x, 0]$.

Por la ley de tricotomía, dado el elemento $[a, b]$ pueden ocurrir tres casos:

$b < a$,	es decir: $a = b + x$	lo notamos x,	es un entero positivo.
$a = b$,		lo notamos 0,	es el elemento neutro.
$a < b$,	es decir: $b = a + x$;	lo notamos $-x$,	es un entero negativo.

Definamos ahora las operaciones "heredadas" en $\mathbb{Z}$: $[a, b] +_{\mathbb{Z}} [c, d]$ y $[a, b] \cdot_{\mathbb{Z}} [c, d]$.

Para que nos resulte "más natural" hagamos un poquito de "trampa".

$[a, b] +_{\mathbb{Z}} [c, d] = (a - b) +_{\mathbb{Z}} (c - d) = (a - b) + (c - d) = (a + c) - (b + d) = [a + c\, ,\, b + d]$.

$[a, b] \cdot_{\mathbb{Z}} [c, d] = (a - b) \cdot_{\mathbb{Z}} (c - d) = (a - b) \cdot (c - d) = a \cdot c - a \cdot d - b \cdot c + b \cdot d =$

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

Es decir:

$$[a, b] +_{\mathbb{Z}} [c, d] = [a + c\, ,\, b + d].$$

$$[a, b] \cdot_{\mathbb{Z}} [c, d] = [a \cdot c + b \cdot d\, ,\, b \cdot c + a \cdot d].$$

Estas operaciones, debido a que son una extensión de las definidas en $\mathbb{N}$, verifican las mismas propiedades enunciadas para $\mathbb{N}$ y además:

(S4) Para cada $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$, que satisface $x + (-x) = 0$ (elemento simétrico)

En efecto: $x \in \mathbb{Z}$, entonces $x = [a, b]$, es claro que $[b, a] \in \mathbb{Z}$ y se verifica $[a, b] + [b, a] = [a + b, a + b]$. Poniendo $-x = [b, a]$ obtenemos la propiedad.

Extendamos ahora la relación de orden: Sabemos que $[a, b] = [c, d]$ si y sólo si $a + d = b + c$, pongamos, entonces $[a, b] <_{\mathbb{Z}} [c, d]$ si y sólo si $a + d < b + c$. Esta

es nuevamente una relación de orden que, claramente, extiende a la dada en $\mathbb{N}$. (® ejercicio para el lector)
Esta relación satisface las siguientes propiedades:

Proposición 4.6 *Si $x, y, z \in \mathbb{Z}$:*

(O1) *Si $x < y$, entonces $x + z < y + z$.* (ley de monotonía)

(O2) *Si $x < y$, $0 < z$, entonces $x \cdot z < y \cdot z$.* (ley de monotonía)

(O3) *Si $x < y$, $z < 0$, entonces $y \cdot z < x \cdot z$.* (ley de monotonía)

(O4) *Si $0 < x, 0 < y$, entonces $0 < x \cdot y$.* (regla de los signos)

(O5) *Si $x < 0, y < 0$, entonces $0 < x \cdot y$.* (regla de los signos)

(O6) *Si $0 < x, y < 0$ ó $x < 0, 0 < y$, entonces $x \cdot y < 0$.* (regla de los signos)

(O7) *Si $x \cdot y = 0$, entonces $x = 0$ ó $y = 0$.* (dominio de integridad)

Demostración: Verifiquemos una propiedad cualquiera de la lista a modo de ejemplo:

$(O5)$ Si $x < 0, y < 0$, entonces $0 < x \cdot y$. (regla de los signos)

Sean $x = [a, b], y = [c, d]$. Dado que $x < 0, y < 0$ debe ser $a < b$ y $c < d$. Calculemos $x \cdot y = [a \cdot c + b \cdot d\,,\, a \cdot d + b \cdot c] > 0$ si $a \cdot c + b \cdot d > a \cdot d + b \cdot c$. Como $a < b$ podemos afirmar que $b - a \in \mathbb{N}$, y por la ley de monotonía para el producto $(b - a) \cdot d > (b - a) \cdot c$, sumando a ambos miembros $a \cdot d + a \cdot c$, por la ley de monotonía para la suma obtenemos la desigualdad buscada. □

Definición 4.5 Un conjunto A no vacío se dice *numerable* si existe una biyección (una aplicación biyectiva) f entre A y $\mathbb{N}$.

Observación 4.5 Pedimos una biyección "entre" A y $\mathbb{N}$, en lugar de decir una f biyectiva, $f : A \to \mathbb{N}$. Si encontramos la función $f : A \to \mathbb{N}$, como f es biyectiva existe $f^{-1} : \mathbb{N} \to A$. Del mismo modo si hubiéramos encontrado $g : \mathbb{N} \to A$, $g^{-1} : A \to \mathbb{N}$, entonces al decir en la definición "entre" damos libertad a hallar la función biyectiva con dominio o imagen en $\mathbb{N}$, según nos convenga en cada caso.

Teorema 4.7 *$\mathbb{Z}$ es numerable.*

Demostración: Sea $f : \mathbb{Z} \to \mathbb{N}$ definida por:

$$f(x) = \begin{cases} 2x & \text{si } x \geq 0\ ; \\ -2x - 1 & \text{en otro caso.} \end{cases}$$

Los detalles de la demostración quedan a cargo del lector. ® □

4.3. Números racionales

Dados dos números enteros a, b, la ecuación $a \cdot x = b$ no siempre tiene solución. En efecto, si consideramos $3 \cdot x = 15$, $x = (15/3) = 5$ lo satisface, pero $3 \cdot x = 2$ no. Para que esta ecuación tenga solución sin restricciones, hagamos la siguiente construcción:
Consideremos en $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ la relación $\mathcal{R}_2$ definida por: $(a, b)\mathcal{R}_2(c, d)$ si y sólo si $a \cdot d = c \cdot b$.

Observación 4.6 Sabemos que para $a, b, c, d \in \mathbb{Z}$ cualesquiera está definida $a \cdot d = c \cdot b$, y en realidad lo que estamos pidiendo es que $a/b = c/d$, es decir, dos pares están relacionados si al dividir el primero por el segundo se obtiene el mismo resultado.

$\mathcal{R}_2$ es claramente una relación de equivalencia (Ⓡ ejercicio para el lector) y definimos $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/R_2$. En este conjunto cociente, para simplificar la notación la clase del par $\langle a, b\rangle$ la notamos simplemente a/b.

Observación 4.7 Aunque la relación de equivalencia $\mathcal{R}_1$ usada para construir los números enteros no había sido vista anteriormente, $\mathcal{R}_2$ la conocimos en la escuela cuando vimos "fracciones equivalentes" o nos pedían "simplificar una fracción" hasta hallar lo que llamaban una *fracción simple*.
Por ejemplo, $\dfrac{18}{15} = \dfrac{6}{5}$, simplificando por 3 numerador y denominador.

$\mathbb{Q}$ contiene una "copia" de $\mathbb{Z}$ por la función $Incl_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}$ definida por: $f(x) = x/1$.

Definamos ahora las operaciones "heredadas" en $\mathbb{Q}$:
$a/b +_{\mathbb{Q}} c/d$ y $a/b \cdot_{\mathbb{Q}} c/d$ Para que nos resulte "más natural" hagamos un poquito de "trampa".

$a/b +_{\mathbb{Q}} c/d = \dfrac{a}{b} +_{\mathbb{Q}} \dfrac{c}{d} = \dfrac{a}{b} \cdot \dfrac{d}{d} + \dfrac{c}{d} \cdot \dfrac{b}{b} = \dfrac{a \cdot d}{b \cdot d} + \dfrac{c \cdot b}{b \cdot d} = \dfrac{a \cdot d + c \cdot b}{b \cdot d} = (a \cdot d + c \cdot b)/(b \cdot d)$.

$a/b \cdot_{\mathbb{Q}} c/d = \dfrac{a}{b} \cdot_{\mathbb{Q}} \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d} = (a \cdot c)/(b \cdot d)$.

Es decir:

$$a/b +_{\mathbb{Q}} c/d = \frac{a \cdot d + c \cdot b}{b \cdot d} = (a \cdot d + c \cdot b)/(b \cdot d).$$

$$a/b \cdot_{\mathbb{Q}} c/d = (a \cdot c)/(b \cdot d).$$

Estas operaciones, debido a que son una extensión de las definidas en $\mathbb{Z}$, verifican las mismas propiedades enunciadas para $\mathbb{Z}$ y además:

(P4) Si $x \neq 0$ existe $x^{-1} \in \mathbb{Q}$, que satisface $x \cdot (x^{-1}) = 1$ (elemento inverso)

En efecto: $x \in \mathbb{Q}$, entonces $x = a/b$, como $x \neq 0$ resulta $a \neq 0$ y $b/a \in \mathbb{Q}$ y se verifica $a/b \cdot b/a = (a \cdot b)/(b \cdot a) = 1$. Poniendo $x^{-1} = b/a$ obtenemos la propiedad.
$(\mathbb{Q}, +, \cdot, -, ^{-1}, 0, 1)$ es un *cuerpo conmutativo*.

Extendamos ahora la relación de orden: Sabemos que $a/b = c/d$ si y sólo si $a \cdot d = b \cdot c$, pongamos, entonces $a/b <_{\mathbb{Q}} c/d$ si y sólo si $a \cdot d = b \cdot c$. Esta es nuevamente una relación de orden que, claramente, extiende a la dada en $\mathbb{Z}$. (Ⓡ ejercicio para el lector)
Esta relación satisface (obligatoriamente) las mismas propiedades que en $\mathbb{Z}$ y además las siguientes:

Proposición 4.7 *El cuerpo ordenado $\mathbb{Q}$ satisface las siguientes propiedades:*

(D_1) *Dado un número racional a/b existe siempre otro mayor.*

(D_2) *Dado un número racional a/b existe siempre otro menor.*

(D_3) *Dados dos números racionales $a/b < c/d$ existe siempre otro e/f tal que $a/b < e/f < c/d$.*

Esta proposición indica que $\mathbb{Q}$ (al igual que $\mathbb{Z}$ no tiene primer ni último elemento. Además (D_3) afirma que $\mathbb{Q}$ es *denso*.
Es interesante verificar que si $\dfrac{a}{b} < \dfrac{c}{d}$, entonces $\dfrac{a}{b} < \dfrac{a+c}{b+d} < \dfrac{c}{d}$.
Con números: $\dfrac{1}{5} < \dfrac{2}{3}$, entonces $\dfrac{1}{5} < \dfrac{1+2}{5+3} = \dfrac{3}{8} < \dfrac{2}{3}$.

Enunciaremos a continuación un resultado muy interesante cuya demostración no veremos:

Teorema 4.8 *El cuerpo ordenado $\mathbb{Q}$ es el cuerpo ordenado mínimo que contiene a $\mathbb{N}$.*

Teorema 4.9 $\mathbb{Q}$ *es numerable.*

Demostración: Veremos que existe una inyección de $\mathbb{Q}^+$, el conjunto de los racionales positivos, en $\mathbb{N}$. Para ellos utilizaremos el llamado *primer método diagonal de Cantor*. Escribimos una primera línea que contenga a todos los números racionales positivos de denominador 1, la segunda tendrá a todos los números racionales positivos de denominador 2, la tercera los de denominador 3 y así sucesivamente, es decir, la n-ésima línea tendrá todos los números racionales positivos de denominador n. En este "cuadro infinito" aparecen todos los números racionales positivos, pero no escritos de forma única ni por única vez. Por ejemplo: el número 1 aparecerá en el lugar n de la columna n-ésima como $1/1$, $2/2$, $3/3$, etc. En términos simples "hay más" que los racionales positivos. Si logramos encontrar un primer elemento y asignarle a cada elemento un sucesor único habremos encontrado un conjunto numerable. (Cuidado: No es necesario que se conserve el orden natural de $\mathbb{Q}$). Si seguimos el recorrido de la flecha que propone Cantor, tachando los números que aparecen repetidos, habremos encontrado la correspondencia buscada.

$$
\begin{array}{ccccccccccccc}
\frac{1}{1} & \longrightarrow & \frac{2}{1} & & \frac{3}{1} & \longrightarrow & \frac{4}{1} & & \frac{5}{1} & \longrightarrow & \frac{6}{1} & & \frac{7}{1} \longrightarrow \cdots \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} & & \frac{6}{2} & & \frac{7}{2} \quad \cdots \\
\downarrow & & & & & & & & & & & & \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \frac{5}{3} & & \frac{6}{3} & & \frac{7}{3} \quad \cdots \\
\frac{1}{4} & & \frac{2}{4} & & \frac{3}{4} & & \frac{4}{4} & & \frac{5}{4} & & \frac{6}{4} & & \frac{7}{4} \quad \cdots \\
\downarrow & & & & & & & & & & & & \\
\frac{1}{5} & & \frac{2}{5} & & \frac{3}{5} & & \frac{4}{5} & & \frac{5}{5} & & \frac{6}{5} & & \frac{7}{5} \quad \cdots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

$f\left(\frac{1}{1}\right) = 1$, $f\left(\frac{2}{1}\right) = 2$, $f\left(\frac{1}{2}\right) = 3$, $f\left(\frac{1}{3}\right) = 4$, $f\left(\frac{3}{1}\right) = 5$, $\cdots$, donde hemos "salteado" $\frac{2}{2}$ porque es uno de los "repetidos".

En general $f\left(\frac{a}{b}\right) = n$. Definimos $f(0) = 0$ y $f\left(-\frac{a}{b}\right) = -f\left(\frac{a}{b}\right) = -n$.

Definida de este modo $f : \mathbb{Q} \to \mathbb{Z}$ es una biyección y como $\mathbb{Z}$ es numerable, existe una biyección $g : \mathbb{Z} \to \mathbb{N}$ y $g \circ f : \mathbb{Q} \to \mathbb{N}$ es una biyección. $\square$

4.4. Números reales

Hemos hallado un cuerpo denso, es decir un conjunto numérico en el que siempre es posible hallar solución única para las ecuaciones $a + x = b$ y $c \cdot x = d$, si $c \neq 0$, aparentemente "sin agujeros" (entre dos números racionales siempre hay un racional). Sin embargo, hay valores que no se pueden expresar como números racionales, tal es el caso de $\sqrt{2}$.
En efecto: supongamos que $\sqrt{2} = \dfrac{a}{b}$, como fracción irreducible, es decir, a y b no tienen factores comunes propios. Resulta entonces, $\dfrac{a^2}{b^2} = 2$, es decir, $a^2 = 2 \cdot b^2$. Si a^2 es par, necesariamente a es par (® verificarlo), entonces $a = 2 \cdot c$ y resulta $4 \cdot c^2 = 2 \cdot b^2$, de donde inferimos $2 \cdot c^2 = b^2$, b^2 es par, b es par. Lo que contradice la hipótesis de fracción irreducible.
Queda claro, entonces, que $\sqrt{2} \notin \mathbb{Q}$, y, sin embargo (por la densidad de $\mathbb{Q}$) se puede aproximar con números racionales tanto como se desee. Podemos entonces partir al conjunto de los números racionales en dos subconjuntos A y B del siguiente modo: $A = \{x : x \in \mathbb{Q}, x^2 \leq 2\}$, $B = \{x : x \in \mathbb{Q}, x^2 \geq 2\}$. $\mathbb{Q} = A \cup B$, es decir $B = \mathbb{Q} \setminus A$, donde A "no termina" y B "no empieza". Aquí nos encontamos con un a descomposición de $\mathbb{Q}$ que es lo que llamamos una *laguna*, pero los números reales no tienen lagunas, por lo tanto $A \cup \mathbb{R} \setminus A$ es la idea de una *cortadura de Dedekind*. Es posible demostrar que $\mathbb{R} \setminus A$ queda unívocamente definido por A, de esta manera la cortadura se reduce simplemente a A y todas las cortaduras determinan todos los números reales.

(✠) Julius Wilhelm Richard Dedekind (1831-1916) fue un matemático alemán nacido y fallecido en Braunschweig. Empezó su carrera en ciencias físicas, pero se desvió hacia la matemática, siendo alumno de Gauss. Su trabajo incluye los números irracionales, presentándolos de una manera lógica; introduciendo "cortes" Dedekind presenta el número real como una cortadura en el conjunto de los números racionales, dando al conjunto de los números reales una interpretación geométrica en forma de línea recta. La propiedad de continuidad de la recta, según Dedekind, consiste en que las cortaduras se encontrarán o en el punto más a la derecha o en el más a la izquierda de una clase. El conjunto de los racionales no tiene la propiedad de la continuidad. Al introducir estas cortaduras y llamarlas *números irracionales*, Dedekind crea un nuevo conjunto dotado de la propiedad de continuidad.

Una cortadura A es cortadura racional si y sólo si existe $r \in \mathbb{Q}$ tal que $r = sup(A)$. Es evidente que a todo número racional le corresponde una cortadura racional y sólo una. Podemos establecer así una aplicación inyectiva $Inc_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$ que al número racional r le asocie la cortadura racional $A_r = \{x : x \leq r\}$.
También es demostrable que el conjunto de todas las cortaduras cumple con los axiomas de los números racionales, más la idea de continuidad. Es decir: todo subconjunto acotado superiormente tiene supremo y todo subconjunto acotado inferiormente tiene ínfimo.
Resumiendo: hemos llegado a construir el cuerpo ordenado de los números reales, que es el cuerpo ordenado máximo que contiene a $\mathbb{N}$. En $\mathbb{R}$ se cumplen las siguientes propiedades:

(S1) $x + (y + z) = (x + y) + z$ (propiedad asociativa de la suma)

(S2) $x + y = y + x$ (propiedad conmutativa de la suma)

(S3) $x + 0 = 0 + x = x$ (0: elemento neutro para la suma)

(S4) Para cada x existe $-x$, que satisface
$x + (-x) = (-x) + x = 0$ (elemento simétrico)

(P1) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (propiedad asociativa del producto)

(P2) $x \cdot y = y \cdot x$ (propiedad conmutativa del producto)

(P3) $x \cdot 1 = 1 \cdot x = x$ (1: elemento neutro para el producto o unidad)

(P4) Para cada $x, x \neq 0$ existe x^{-1}, que satisface
$x \cdot (x^{-1}) = (x^{-1}) \cdot x = 1$ (elemento inverso)

(D1) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (propiedad distributiva)

(O0) Dados x, y, z, si $x < y$, $y < z$, entonces $x < z$ (ley transitiva)

(O1) Dados x, y, se verifica $x < y$, $x = y$ ó $y < x$, (ley de tricotomía)

(O2) Si $x < y$, entonces $x + z < y + z$, (ley de monotonía para la suma)

(O3) Si $x < y$, $z > 0$ entonces $x \cdot z < y \cdot z$. (ley de monotonía para el producto)

Definición 4.6 Si $x \in \mathbb{R}$ y $x \notin \mathbb{Q}$, entonces x se dice un *número irracional.* Notaremos $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.

Teorema 4.10 $\mathbb{R}$ *es no numerable.*

Corolario 4.1 *El conjunto de los números irracionales es no numerable.*

No veremos las demostraciones de estos teoremas pero analizaremos intuitivamente qué significan. Que $\mathbb{R}$ sea no numerable quiere decir que hay muchos más números reales que números naturales, lo cual suena bastante lógico. Ahora bien $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. $\mathbb{Q}$ es numerable, si $\mathbb{I}$ fuera numerable, $\mathbb{R}$ también lo sería. (Para ver que esto es posible podemos pensar a $\mathbb{N}$ como el conjunto de pares unido el conjunto de los impares, ambos subconjuntos tiene la misma cantidad de elementos que $\mathbb{N}$.) Conclusión: hay más irracionales que racionales. (Cualquier parecido con la sociedad es mera coincidencia.)

Observación 4.8 Dentro del programa de esta materia se incluyen algunos temas (El conjunto $\mathbb{R}$ de los números reales: la recta real, existencia de raíces en $\mathbb{R}$, potenciación de exponente entero, raíz aritmética y potenciación de exponente racional) que ya se han visto en el Curso de Nivelación y dado que es requisito para cursar esta materia haber aprobado el examen de nivelación, se suponen sabidos. De cualquier modo, agrego a este capítulo un estracto de mis apuntes para nivelación, recordando siempre que la cátedra está disponible para satisfacer todas las dudas que se presenten durante el cursado, aún cuando debieran haber sido resueltas previamente.

4.5. Anexo: Extracto del Curso de Nivelación

4.5.1. Algo de historias...

Hay, a grandes rasgos, dos formas de presentar a $\mathbb{R}$, el cuerpo de los números reales.
Una de ellas es la axiomática: $\mathbb{R}$ es un conjunto con dos operaciones binarias $(+, \cdot)$, dos unarias $(-, ^{-1})$, dos constantes, también llamadas operaciones ceroarias, (0,1) y una relación de orden $(\leq)$ que satisface los siguientes axiomas[1], cualesquiera que sean a, b, c números reales:

1. $a + (b + c) = (a + b) + c$ — propiedad asociativa de la suma
2. $a + b = b + a$ — propiedad conmutativa de la suma
3. Existe 0 tal que $a + 0 = 0 + a = a$ — elemento neutro de la suma
4. para todo a existe $b = -a$ tal que $a + b = 0$ — existencia de simétricos
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ — propiedad asociativa del producto
6. $a \cdot b = b \cdot a$ — propiedad conmutativa del producto
7. Existe 1 tal que $a \cdot 1 = 1 \cdot a = a$ — unidad del producto

[1] un axioma es algo que se tiene que cumplir, es verdadero porque ésas son las leyes del juego.

8. para todo $a \neq 0$ existe $b = a^{-1}$ tal que $a \cdot b = 1$ — existencia de inversos
9. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ — propiedad distributiva
10. $a \leq a$ — propiedad reflexiva
11. Si $a \leq b$ y $b \leq a$, entonces $a = b$ — propiedad antisimétrica
12. Si $a \leq b$ y $b \leq c$, entonces $a \leq c$ — propiedad transitiva

Decimos entonces que $\langle \mathbb{R}, +, \cdot, -, ^{-1}, 0, 1, \leq \rangle$ es un cuerpo ordenado.

La otra forma tiene mucho más que ver con la verdadera esencia de la matemática, que es encontrar un modelo abstracto que nos sirva a nuestra realidad.

En un principio el hombre supo si tenía algo o no tenía nada (conocía la existencia del número 1), luego distinguió entre “1” y “muchos”. Así *naturalmente* aparece la idea de los números 0, 1, 2, 3, 4, ... a la que denominaremos *números naturales* y los notaremos con $\mathbb{N}$. Nos damos cuenta de que si juntamos dos cantidades obtenemos una tercera (es decir, dos piedritas y tres piedritas son cinco piedritas), estamos en presencia de la *suma* y vemos que se cumplen las propiedades asociativa y conmutativa. Tenemos $\langle \mathbb{N}, +, 0 \rangle$ [2]

Nuestro hombre primitivo colecciona piedritas, que también sirven como modo de pago. Si este hombre tiene cuatro piedritas y para obtener lo que desea debe dar cinco piedritas nota que le *falta una* y a este nuevo número lo llama -1. Así, para cada número existente se crea su simétrico, es decir, para el 1, el -1; para el 2 el -2, para el 3 el -3 y así sucesivamente. Distingue lo que tiene de lo que le falta colocando un signo “+” delante de lo que tiene y un signo “−” delante de lo que le falta. Los números precedidos por “+” se llaman *enteros positivos* y no son otra cosa que los números naturales, los precedidos por “−” son los *enteros negativos*. Cree que ya tiene todos los números y los nota $\mathbb{Z}$ ¿Por qué una Z? porque es la inicial de Zahl: número en idioma alemán. Tenemos $\langle \mathbb{Z}, +, -, 0 \rangle$ [3].

Cuidado: suma $5 + (-2) = 3$ pero para ahorrar en signos y paréntesis, decide escribir $5 - 2 = 3$. Escribe sólo el “−” entre dos números lo hace por ahorrativo, lo llama *resta*, pero la resta no es una operación binaria asociativa ni conmutativa, no “funciona bien” como la suma.

Cuando tiene que sumar muchas veces el mismo número, por ejemplo, cuando tiene que hacer $3 + 3 + 3 + 3 + 3 + 3 = 18$ piensa que sumar tres piedritas seis veces puede escribirse con un nuevo signo $3 \times 6 = 18$. Si pone las tres

[2] llamamos a esta estructura *semigrupo conmutativo con unidad* o *monoide conmutativo*.

[3] llamamos a esta estructura *grupo conmutativo*, + es la operación binaria, − la unaria y 0 la cero-aria

piedritas en hilera, toma la primera de cada hilera y forma un montoncito, forma otro montoncito con la segunda de cada hilera y las que quedan forman un último montoncito. Ahora tiene tres montoncitos de seis piedritas, lo que en símbolos es $6 \times 3 = 18$. Crea una nueva operación que llama *multiplicación*, que se ve que es una operación conmutativa, como "resumen" de la suma. Por la propiedad asociativa de la suma sabemos que $(3+3+3+3)+(3+3) = (3\times 4)+(3\times 2) = 3\times(4+2)$ que es la propiedad distributiva de la multiplicación con respecto a la suma, que garantiza que la multiplicación es una "suma abreviada". Tenemos $\langle \mathbb{Z}, +, \times, -, 0\rangle$ [4].

Cuando multiplica un número a por 1, quiere decir que suma a una vez, es decir $a \times 1 = a$ y 1 es el *elemento neutro para el producto* o *unidad*. Tenemos $\langle \mathbb{Z}, +, \times, -, 0, 1\rangle$ [5].

Al momento de crearse la pizza se crea un nuevo problema: debemos partirla en trozos iguales, en cualquier pizzería una redonda de muzzarela sale en ocho pedacitos, si los amigos se comen tres, de los ocho quedan cinco, quedan 5 entre 8, que escribimos $\frac{5}{8}$. Todos los números que estén escritos en forma de fracción, razón o cociente forma el conjunto de los *números racionales* que notamos $\mathbb{Q}$ (del inglés, quotient: cociente).
Pensemos en un número entero, por ejemplo el 4, si tenemos 4 pizzas, cada una de ellas sin partir, tenemos 4 partidas en 1, 4 entre 1, que escribimos $\frac{4}{1}$, así todo número entero a puede escribirse como $\frac{a}{1}$. Hablamos entonces de *racionales enteros*.

Algo entero lo podemos partir en cualquier cantidad, entonces para cada número b, no cero, podemos escribir $b^{-1} = \frac{1}{b}$, que cumple $b^{-1} \times b = \frac{1}{b} \times b = 1$. Resulta además que $\frac{a}{b} \times \frac{b}{a} = 1$ y en consecuencia $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. Encontramos así los *inversos* y tenemos $\langle \mathbb{Q}, +, \times, -, ^{-1}, 0, 1\rangle$ [6].

Del mismo modo que llamamos "restar" a "sumar el simétrico" llamaremos *dividir* a "multiplicar por el inverso". Igual que antes, la división no es una operación asociativa ni conmutativa, no "funciona bien" como el producto (

[4]llamamos a esta estructura *anillo conmutativo*, $+$ y $\times$ son operaciones binarias, $-$ la unaria y 0 la cero-aria

[5]llamamos a esta estructura *anillo con unidad*, $+$ y $\times$ son las operaciones binarias, $-$ la unaria y 0 y 1 las cero-arias

[6]llamamos a esta estructura *cuerpo*, $+$,$\times$ son las operaciones binarias, $-$ y $^{-1}$ las unarias y 0 y 1 las cero-arias

o multiplicación).

Por sumas, productos, simétricos o inversos no va a crecer este conjunto, parece que hemos encontrado todos los números, pero... ¿qué ocurre si recortamos un cartón cuadrado de 1 *cm* de lado por la diagonal? ¿cuánto mide este nuevo lado? No podemos encontrar ningún número escrito en forma de fracción que represente exactamente esta medida, pero es un número *real*, en verdad existe, y llamamos al conjunto formado por todos esos número el conjunto de los *números reales* y lo notamos $\mathbb{R}$.

Los números reales, no racionales los llamamos *irracionales* y lo notamos $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.

Esta "historieta" simplemente muestra el proceso de extensión algebraico que hemos realizado hasta el momento, pero dista mucho de la verdadera historia de la matemática ya que $\sqrt{2}$ fue reconocida mucho antes que el 0 o los números negativos.

(✠) Hipaso de Metaponto fue un matemático, teórico de la música y filósofo presocrático, miembro de la Escuela pitagórica. (Estamos hablando del siglo V a.C.) Se le atribuyen tres importantes descubrimientos: La construcción de un dodecaedro inscripto en una esfera, el descubrimiento de la inconmensurabilidad y la determinación de las relaciones numéricas de las consonancias básicas a través de experimentos de sonido. Era miembro de la escuela pitagórica, que tenía la firme creencia que todo el universo podía ser explicado con números naturales y sus cocientes. Según cuenta la leyenda, Hipaso fue el "culpable" de plantear el problema de medir la diagonal de un cuadrado utilizando el lado como unidad de medida. No sólo halló un número irracional, sino que lo hizo utilizando el más famoso de todos los teoremas pitagóricos. Los documentos de la época dan versiones diferentes de su final: parece ser que murió en un naufragio en circunstancias misteriosas; algunos dicen que se suicidó como autocastigo, dejando así libertad a su alma para ir a buscar la purificación en otro cuerpo y finalmente otros afirman que un grupo de pitagóricos lo mataron.

(✠ Los números negativos ingresaron a la matemática como *números deudos* o *números absurdos*. Las primeras manifestaciones de su uso se remontan al siglo V, en oriente, y no llegan a occidente hasta el siglo XVI. Los chinos los usaban dentro del cálculo, sin embargo, no aceptaron la idea de que un número negativo pudiera ser solución de una ecuación. Brahmagupta, un indio contemporáneo de Bhaskara I (hacia el año 630 d.C), comenzó a usar el 0 para calcular e interpretó como créditos y débitos, respectivamente, a los números positivos y negativos. Gerolamo Cardano (lo vamos a encontrar hablando de números complejos), en el siglo XVI, llamaba a los números negativos "falsos", pero los estudió en su *Ars Magna* (1545), John Wallis (1616 - 1703), "demuestra" la imposibilidad de su existencia en su *Arithmetica Infinitorum* (1655) y Leonard Euler es el primero en darles estatuto legal, en *Anleitung zur Algebra* (1770).

Pero volviendo al tema que nos ocupa:

RESUMIENDO:

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}}$$

Todo número natural es entero, todo entero es racional, todo racional es real. Hay números reales que no son racionales (los irracionales), hay números racionales que no son enteros (los fraccionarios), hay números enteros que no son naturales (los negativos y tal vez el cero, según como definamos a los naturales).

Ejemplo 4.1 Son números naturales: 1, 3, 46, 325, 135709, etc.

Son números enteros: -10, 3 -425, -30, 5470, 0, etc.

Son números racionales: $\frac{3}{5}, -\frac{3}{9}, 0,3,45789, \frac{-2}{48}$, etc.

Son números irracionales: $\sqrt{2}, \pi, e, \phi$

Son números reales: 1, 3, 46,-425, -30, 5470, 0, $\frac{3}{5}, -\frac{3}{9}, 0,3,45789, \frac{-2}{48}, \sqrt{2}, \pi, e, \phi$

Observación 4.9 Dado un número racional $\frac{a}{b}$, a se dice el *numerador* y b el *denominador*.

Se define la *igualdad* de números racionales del siguiente modo:

$$\frac{a}{b} = \frac{c}{d} \text{ si y sólo si } a \times d = c \times b.$$

Siempre consideramos que el denominador es un número positivo, ya que

$$\frac{-a}{b} = \frac{a}{-b} = -\frac{a}{b}$$

Observación 4.10 Entre los ejemplos hemos escrito el número $-\frac{3}{9}$ que es una fracción, pero el numerador y el denominador tienen un divisor en común (ambos son divisibles por 3), por cuanto podemos simplificar y obtenemos $-\frac{1}{3}$ una fracción donde numerador y denominador no tienen factores en común, es decir, una *fracción irreducible*

Notación 4.2 Para la multiplicación o el producto hemos estado utilizando el signo $\times$, es frecuente que lo reemplacemos por $\cdot$, de mismo modo la división escrita con línea de fracción puede reemplazarse por : como se ve en el siguiente ejemplo:

Ejemplo 4.2 $3 \times 2 = 3 \cdot 2$ $\qquad \frac{3}{2} = 3 : 2$

Sabemos intuitivamente realizar las sumas de números naturales y su extensión a números enteros resulta sencilla. Tampoco tenemos inconvenientes en multiplicar ni números naturales, ni enteros. Recordemos cómo realizar estas operaciones para números racionales:

Dados $\frac{a}{b}$, $\frac{c}{d}$

$$\boxed{\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}}$$

Ejemplo 4.3

$$\frac{3}{5} + \frac{2}{3} = \frac{3 \cdot 3 + 2 \cdot 5}{5 \cdot 3} = \frac{19}{15} \qquad \frac{3}{5} \cdot \frac{2}{3} = \frac{3 \cdot 2}{5 \cdot 3} = \frac{2}{5}$$

$$\frac{3}{4} + \frac{5}{8} = \frac{3 \cdot 8 + 4 \cdot 5}{4 \cdot 8} = \frac{44}{32} = \frac{11}{8} \qquad \frac{3}{4} \cdot \frac{5}{8} = \frac{3 \cdot 5}{4 \cdot 8} = \frac{15}{32}$$

Propiedades de los números reales

Los números reales, definidos axiomáticamente o construídos a partir de los naturales, satisfacen muchas propiedades, a continuación daremos un listado de aquellas que son de uso más frecuente:

1. $-(-a) = a$
2. $a + b = a + c$, entonces $b = c$
3. $a \cdot 0 = 0$

4. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
5. $(-a) \cdot (-b) = a \cdot b$
6. $a \cdot b = 0$, entonces $a = 0$ ó $b = 0$
7. $a \cdot b = a \cdot c,\ c \neq 0$, entonces $b = c$
8. $(a^{-1})^{-1} = a$
9. $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$
10. Si $b \neq 0, d \neq 0$, $\dfrac{a}{b} = \dfrac{c}{d}$ si y sólo si $a \cdot d = b \cdot c$
11. Si $c \neq 0$, $\dfrac{a}{b} = \dfrac{a \cdot c}{b \cdot c}$
12. Si $b \neq 0, d \neq 0$, $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a \cdot d + b.c}{b \cdot d}$
13. Si $b \neq 0, d \neq 0$, $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$
14. Si $b \neq 0, c \neq 0, d \neq 0$, $\dfrac{a}{b} : \dfrac{c}{d} = \dfrac{a \cdot d}{b \cdot c}$
15. Si $b \neq 0$, $\dfrac{-a}{b} = \dfrac{a}{-b} = -\dfrac{a}{b}$
16. Si $a \neq 0, b \neq 0$, $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$

Ejercicios resueltos

1. Dar ejemplos de valores que deben ser números naturales, números enteros, números positivos, números negativos.
   - Naturales: Cantidad de asistentes a una reunión, Número de unidades móviles necesarias para hacer un tour.
   - Enteros: Cantidad de números que faltan para completar una colección.
   - Positivos: Distancia entre dos puntos,
   - Negativos: Altura bajo el nivel del mar, Temperatura bajo nivel de congelación.
2. Sumar $2 + (-3) + 7 + (-1) + 4$ de diferentes formas, explicando en cada caso qué propiedad se ha utilizado.
   - $(2+(-3))+(7+(-1))+4 = (-1)+6+4 = -1+(6+4) = -1+10 = 9$
     por propiedad asociativa
   - $((-3) + (-1)) + 4 + (7 + 2) = (-4) + 4 + (7 + 2)$
     por propiedad conmutativa y asociativa

$((-4)+4)+(7+2)=0+9=9$
por simétricos y elementos neutro

3. Dar ejemplos de operaciones donde se verifiquen la propiedad asociativa y la propiedad conmutativa y otros donde no se verifiquen.

    - La suma verifica la propiedad conmutativa

      $$\frac{3}{4}+\frac{2}{5}=\frac{3\cdot 5+2\cdot 4}{4\cdot 5}=\frac{23}{20},\qquad \frac{2}{5}+\frac{3}{4}=\frac{2\cdot 4+3\cdot 5}{5\cdot 4}=\frac{23}{20}$$

      entonces resulta: $\dfrac{3}{4}+\dfrac{2}{5}=\dfrac{2}{5}+\dfrac{3}{4}$

    - La resta no verifica la propiedad conmutativa

      $$\frac{3}{4}-\frac{2}{5}=\frac{3\cdot 5-2\cdot 4}{4\cdot 5}=\frac{7}{20},\qquad \frac{2}{5}-\frac{3}{4}=\frac{2\cdot 4-3\cdot 5}{5\cdot 4}=-\frac{7}{20}$$

      entonces resulta: $\dfrac{3}{4}-\dfrac{2}{5}\neq\dfrac{2}{5}-\dfrac{3}{4}$

    - La suma verifica la propiedad asociativa

      $$\left(\frac{3}{4}+\frac{2}{5}\right)+\frac{7}{2}=\frac{23}{20}+\frac{7}{2}=\frac{93}{20},\qquad \frac{3}{4}+\left(\frac{2}{5})+\frac{7}{2}\right)=\frac{3}{4}+\frac{39}{10}=\frac{93}{20}$$

      entonces resulta: $\left(\dfrac{3}{4}+\dfrac{2}{5}\right)+\dfrac{7}{2}=\dfrac{3}{4}+\left(\dfrac{2}{5}+\dfrac{7}{2}\right)$

    - El cociente (la división) no verifica la propiedad asociativa

      $$\left(\frac{3}{4}:\frac{2}{5}\right):\frac{7}{2}=\frac{15}{8}:\frac{7}{2}=\frac{15}{28},\qquad \frac{3}{4}:\left(\frac{2}{5}):\frac{7}{2}\right)=\frac{3}{4}:\frac{4}{35}=\frac{105}{16}$$

      entonces resulta: $\left(\dfrac{3}{4}:\dfrac{2}{5}\right):\dfrac{7}{2}\neq\dfrac{3}{4}:\left(\dfrac{2}{5}:\dfrac{7}{2}\right)$

4. Construyendo los dígitos con cuatro 3

   $0=(3-3)\cdot(3+3)$
   $1=(3:3)+3-3$
   $2=(3:3)+(3:3)$
   $3=3+3\cdot(3-3)$
   $4=(3\cdot 3+3):3$
   $5=((3+3):3)+3$
   $6=3+3+3-3$
   $7=3+3+(3:3)$
   $8=3\cdot 3-(3:3)$
   $9=(3\cdot 3\cdot 3):3$

Ejercicios propuestos

1. Dar ejemplos de cantidades que deben ser:
   a) naturales
   b) enteras
   c) positivas
2. Dar ejemplos donde se verifique la propiedad asociativa de la suma y del producto, un ejemplo de la propiedad distributiva del producto con respecto a la suma, y ejemplos donde no se verifique la propiedad asociativa de la resta y del cociente. ¿Es posible encontrar ejemplos donde se verifiquen las propiedades asociativa y/o conmutativa de la resta y el cociente? ¿Distribuye el cocienterespecto de la suma? Justificar.
3. En cada caso decir qué propiedad justifica la igualdad
   a) $3+5=5+3$
   b) $3-0=3$
   c) $5\cdot 3=5\cdot 2+5$
4. Si $a+b=12$, calcular $a+(b+10)$
5. Si $a\neq 0$, $b\neq 0$ indicar si es verdadero o falso:
   a) $a+b\neq 0$
   b) $a\cdot b\neq 0$
   c) $a+a\neq 0$
   d) $a^2\neq 0$
6. Calcular utilizando las propiedades del producto y la suma:
   a) $(3+2a)-(a+b)+(3-2a)-2\,(-2a+3b)$
   b) $\dfrac{(2+5a)-3\,(a+2b)+2\,(5-a)}{-3+2a-b+4(c+2)-2\,(2c+3)+5\,(b+3)}$
   c) $\dfrac{(3+2a)-(3-2a)}{a+b}$
   d) $\dfrac{3\,(a-b)+3\,(b-a)}{a+2b+3-7c}$
   e) ¿En cuánto aumenta la suma de tres sumandos si a cada uno de ellos se le suma 5?
   f) Construir los diez dígitos a partir de cuatro 4.
   Nota: Esto es posible hacerlo con cuatro dígitos cualesquiera.

Verdadero o Falso:

1. Los números naturales son enteros
2. Los números reales son racionales
3. La suma de números enteros es un número entero
4. La suma de números irracionales es un número irracional
5. El producto de números racionales es un número racional
6. El producto de números irracionales es un número irracional
7. El producto de un número racional por un número irracional es un número irracional
8. Si $a \cdot b = 0$, entonces $a = 0$ ó $b = 0$
9. $\frac{0}{a} = 0$
10. $\frac{a}{0} = 0$

4.5.2. Potenciación y radicación

Potenciación con exponentes enteros

Hemos visto cómo aparece la multiplicación como "resumen" de la suma ¿qué ocurre si tenemos que calcular $4 \times 4 \times 4 \times 4 \times 4 \times 4 \times 4 = 16384$? Vemos que es multiplicar el 4 siete veces, un modo abreviado de escribirlo es 4^7 y lo llamamos *potencia* 4^7 quiere decir que el factor 4 aparece 7 veces en mi cuenta y el resultado es: $4^7 = 16384$.

¿Qué propiedades tiene esta nueva operación? Las que hereda de quien proviene. No es el objetivo de este curso hacer una demostración de ellas, pero veamos cómo es que funcionan:

$$a^1 = a$$

¿Qué significa 4^1? Que el factor 4 aparece sólo una vez, entonces el resultado debe ser 4.

$$a^0 = 1$$

¿Qué significa 4^0? Que el factor 4 no aparece, que no estoy multiplicando por nada, que no hace ningún efecto el factor 4. ¿cuál es el número que no tiene efecto al multiplicar? El 1, entonces $4^0 = 1$

$$a^b \cdot a^c = a^{(b+c)}$$

¿Qué significa $4^3 \cdot 4^2$? 4 tres veces por 4 dos veces, es decir $(4 \cdot 4 \cdot 4) \cdot (4 \cdot 4)$ y por la propiedad asociativa sabemos que podemos agrupar los 4 como querramos, entonces, sacamos los paréntesis y ¿cuántos 4 hay? cinco 4, entonces $4^3 \cdot 4^2 = 4^5 = 4^{(3+2)}$

$$(a^b)^c = a^{b \cdot c}$$

¿Qué significa $(4^3)^2$? Que el factor 4^3 aparece dos veces, es decir $(4^3)^2 = 4^3 \cdot 4^3$ pero 4^3 quiere decir que el factor 4 aparece tres veces, entonces $(4^3)^2 = (4 \cdot 4 \cdot 4) \cdot (4 \cdot 4 \cdot 4)$, volvemos a sacar los paréntesis y contamos los 4. ¿Cuántos son? seis, $(4^3)^2 = 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 = 4^6 = 4^{2 \cdot 3}$

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

$4^3 \cdot 5^3 = (4 \cdot 4 \cdot 4) \cdot (5 \cdot 5 \cdot 5)$, por la propiedad asociativa del producto podemos sacar los paréntesis, y por la conmutativa, podemos cambiar el orden de los factores, entonces

$$4^3 \cdot 5^3 = (4 \cdot 4 \cdot 4) \cdot (5 \cdot 5 \cdot 5) = (4 \cdot 5) \cdot (4 \cdot 5) \cdot (4 \cdot 5) = (4 \cdot 5)^3$$

$$a^{-1} = \frac{1}{a}$$

Notamos a^{-1} al número que al multiplicarlo por a da 1. Veamos que tiene sentido.
$4 \cdot \frac{1}{4} = 1$. Si queremos escribir $\frac{1}{4} = 4^k$ como potencia de 4 resulta que $4 \cdot \frac{1}{4} = 4^1 \cdot 4^k = 4^{(k+1)}$

Entonces $4^{(k+1)} = 1 = 4^0$, para que $k + 1 = 0$ debe ser $k = -1$

$$a^{-c} = \frac{1}{a^c} = \left(\frac{1}{a}\right)^c$$

$$4^{-3} = 4^{(-1) \cdot 3} = (4^{-1})^3 = \left(\frac{1}{4}\right)^3$$

$$4^{-3} = 4^{3 \cdot (-1)} = (4^3)^{-1} = \frac{1}{4^3}$$

$$a^b : a^c = a^{(b-c)}$$

$$4^5 : 4^3 = 4^5 \cdot (4^3)^{-1} = 4^5 \cdot 4^{-3} = 4^{(5+(-3))} = 4^{(5-3)}$$

$$a^c : b^c = (a : b)^c$$

$3^5 : 4^5 = 3^5 \cdot (4^5)^{-1} = 3^5 \cdot (4^{-1})^5 = (3 \cdot 4^{-1})^5 = (3 : 4)^5$

Listando todas las propiedades enunciadas:

1. $a^1 = a$
2. $a^0 = 1$
3. $a^b \cdot a^c = a^{(b+c)}$
4. $a^c \cdot b^c = (a \cdot b)^c$
5. $(a^b)^c = a^{b \cdot c}$
6. $a^{-1} = \dfrac{1}{a}$
7. $a^{-c} = \dfrac{1}{a^c}$
8. $a^b : a^c = a^{(b-c)}$
9. $a^c : b^c = (a : b)^c$

Radicación

Conocimos la suma y, sabiendo que $3 + 10 = 13$ definimos la resta diciendo que $13 - 10 = 3$ ó $13 - 3 = 10$.

Conocimos el producto y, sabiendo que $7 \cdot 3 = 21$ definimos el cociente diciendo que $21 : 3 = 7$ ó $21 : 7 = 3$.

Conocemos la potenciación $4^3 = 64$, definimos ahora $\sqrt[3]{64} = 4$ y decimos la *raíz* cúbica de 64 es 3. Es decir:
La raíz n de a es igual a b, si y sólo si $b^n = a$.

Veamos qué relación tiene esta nueva operación con la potenciación.

Dijimos $\sqrt[3]{64} = 4$ si y sólo si $4^3 = 64$.

Escribamos $\sqrt[3]{64} = 64^k$ como potencia, entonces $\sqrt[3]{64} = 64^k$ si y sólo si $(64^k)^3 = 64$,

pero $(64^k)^3 = 64^{k \cdot 3}$ y $64^{k \cdot 3} = 64$ si $k \cdot 3 = 1$, de donde $k = \dfrac{1}{3}$.

Este razonamiento podemos hacerlo en forma general y afirmamos entonces que

$$\boxed{\sqrt[n]{a} = a^{\frac{1}{n}}.}$$

Podemos listar las propiedades de la radicación en base a las propiedades de la potenciación:

1. $\sqrt[1]{a} = a$ — $a^1 = a$
2. (No existe la “raíz cero-ésima”, ya que no existe $\frac{1}{0}$) — $a^0 = 1$
3. $\sqrt[b]{a} \cdot \sqrt[c]{a} = \sqrt[b\cdot c]{a^{(b+c)}}$ — $a^b \cdot a^c = a^{(b+c)}$[7]
4. $\sqrt[c]{a} \cdot \sqrt[c]{b} = \sqrt[c]{a \cdot b}$ — $a^c \cdot b^c = (a \cdot b)^c$
5. $\sqrt[c]{\sqrt[b]{a}} = \sqrt[b\cdot c]{a}$ — $(a^b)^c = a^{b\cdot c}$
6. (no se define) — $a^{-1} = \frac{1}{a}$
7. (no se define) — $a^{-c} = \frac{1}{a^c}$
8. $\sqrt[b]{a} : \sqrt[c]{a} = \sqrt[b\cdot c]{a^{(c-b)}}$ — $a^b : a^c = a^{(b-c)}$
9. $\sqrt[c]{a} : \sqrt[c]{b} = \sqrt[c]{a : b}$ — $a^c : b^c = (a : b)^c$

Las propiedades 3. y 8. parecen más complicadas que las correspondientes a la potenciación. Veamos un ejemplo de la propiedad 3.:

$$\sqrt[3]{8} \cdot \sqrt[5]{8} = 8^{\frac{1}{3}} \cdot 8^{\frac{1}{5}} = 8^{\frac{1}{3}+\frac{1}{5}} = 8^{\frac{1\cdot 5+1\cdot 3}{3\cdot 5}} = 8^{\frac{5+3}{3\cdot 5}} = 8^{\frac{3+5}{3\cdot 5}} = \sqrt[3\cdot 5]{8^{3+5}}$$

Analicemos lo que ocurre con las propiedades 6. y 7.:

> La propiedad 6.:
> No tiene sentido pensar en definir una $\sqrt[-1]{x}$ ya que sería $\sqrt[-1]{x} = x^{\frac{1}{-1}} = x^{\frac{-1}{1}} = x^{-1}$.
>
> La propiedad 7.:
> Quedaría como $\sqrt[-c]{a} = \frac{1}{\sqrt[c]{a}}$ y, nuevamente, no hemos definido raíces de exponente negativo, por lo cual **nunca** podemos dejar una raíz en el denominador de una fracción.

El proceso de eliminar las raíces del denominador se denomina *racionalización*.

Hagamos algunas consideraciones:

[7] $\sqrt[b]{a} \cdot \sqrt[c]{a} = a^{\frac{1}{b}} \cdot a^{\frac{1}{c}} = a^{\frac{1}{b}+\frac{1}{c}} = a^{\frac{c+b}{b\cdot c}} = \sqrt[b\cdot c]{a^{(b+c)}}$

$(\sqrt[n]{a})^n = a$

$\frac{a}{a} = 1$

$a \cdot 1 = a$

$\frac{x}{y} = \frac{x}{y} \cdot 1 = \frac{x}{y} \cdot \frac{a}{a} = \frac{x \cdot a}{y \cdot a}$

Igual que lo hicimos con las propiedades de la potenciación, veamos un ejemplo para comprender el mecanismo de la racionalización:

Ejemplo 4.4 1. $\frac{1}{\sqrt{3}}$

Sabemos que $(\sqrt{3})^2 = 3$, y en el denominador figura $\sqrt{3}$

entonces tenemos que multiplicar por $\sqrt{3}$.

$$\frac{1}{\sqrt{3}} = \frac{1}{\sqrt{3}}.\frac{\sqrt{3}}{\sqrt{3}} = \frac{1.\sqrt{3}}{(\sqrt{3})^2} = \frac{\sqrt{3}}{3}$$

2. $\frac{5}{\sqrt[3]{7}}$

Sabemos que $(\sqrt[3]{7})^3 = 7$, y en el denominador figura $\sqrt[3]{7}$

entonces tenemos que multiplicar por $(\sqrt[3]{7})^2$.

$$\frac{5}{\sqrt[3]{7}} = \frac{5}{\sqrt[3]{7}}.\frac{(\sqrt[3]{7})^2}{(\sqrt[3]{7})^2} = \frac{5.(\sqrt[3]{7})^2}{(\sqrt[3]{7})^2} = \frac{5.\sqrt[3]{7^2}}{(\sqrt[3]{7})^3} = \frac{5}{7}\sqrt[3]{49}$$

3. $\frac{\sqrt{3}}{\sqrt[3]{5}\sqrt[4]{3^3}}$

Sabemos que $(\sqrt[3]{5})^3 = 5$ y $(\sqrt[4]{3})^4 = 3$, y en el denominador figura $\sqrt[3]{5}$ y $(\sqrt[4]{3})^3$ entonces tenemos que multiplicar por $(\sqrt[3]{5})^2$ y $\sqrt[4]{3}$.

$$\frac{\sqrt{3}}{\sqrt[3]{5}\sqrt[4]{3^3}} = \frac{\sqrt{3}}{\sqrt[3]{5}\sqrt[4]{3^3}}.\frac{(\sqrt[3]{5})^2.\sqrt[4]{3}}{(\sqrt[3]{5})^2.\sqrt[4]{3}} = \frac{(\sqrt{3})((\sqrt[3]{5})^2.\sqrt[4]{3})}{(\sqrt[3]{5}\sqrt[4]{3^3})((\sqrt[3]{5})^2.\sqrt[4]{3})} =$$

$$= \frac{\sqrt{3}.(\sqrt[3]{5})^2.\sqrt[4]{3}}{\sqrt[3]{5^3}\sqrt[4]{3^4}} = \frac{\sqrt[4]{3^2}.\sqrt[3]{5^2}.\sqrt[4]{3}}{5{,}3} = \frac{1}{15}\sqrt[4]{27}\sqrt[3]{25}$$

De estos ejemplos y las consideraciones previas podemos deducir lo siguiente:

Dada una fracción con productos de raíces en el denominador, para racionalizar la expresión se debe multiplicar el denominador por la potencia de cada raíz que haga falta, y para no variar la fracción se multiplica el numerador por el mismo número.

En símbolos:

$$\frac{a}{\sqrt[n]{b^c}} = \frac{a}{\sqrt[n]{b^c}}.\frac{\sqrt[n]{b^{n-c}}}{\sqrt[n]{b^{n-c}}} = \frac{a.\sqrt[n]{b^{n-c}}}{\sqrt[n]{b^c}.\sqrt[n]{b^{n-c}}} = \frac{a.\sqrt[n]{b^{n-c}}}{\sqrt[n]{b^{n-c+c}}} = \frac{a.\sqrt[n]{b^{n-c}}}{b}$$

Si en el denominador, juntamente con las raíces aparecen sumas (o restas) no tenemos un "método general" para resolverlo, salvo los casos que puedan solucionarse por medio de diferencias de cuadrados

Ejemplo 4.5 1. $\frac{1}{\sqrt{3}-\sqrt{5}}$

Sabemos que $(\sqrt{3}-\sqrt{5})(\sqrt{3}+\sqrt{5}) = 3-5$, y en el denominador figura $\sqrt{3}-\sqrt{5}$

entonces tenemos que multiplicar por $\sqrt{3}+\sqrt{5}$

$$\frac{1}{\sqrt{3}-\sqrt{5}} = \frac{1}{\sqrt{3}-\sqrt{5}}.\frac{\sqrt{3}+\sqrt{5}}{\sqrt{3}+\sqrt{5}} = \frac{\sqrt{3}+\sqrt{5}}{(\sqrt{3}-\sqrt{5})(\sqrt{3}+\sqrt{5})} =$$

$$= \frac{\sqrt{3}+\sqrt{5}}{3-5} = -\frac{1}{2}(\sqrt{3}+\sqrt{5})$$

2. $\frac{\sqrt[4]{x}+2}{\sqrt[4]{x}-\sqrt[3]{8}}$

Sabemos que $\sqrt[4]{x}-\sqrt[3]{8} = \sqrt[4]{x}-2$ y $(\sqrt[4]{x}-2)(\sqrt[4]{x}+2) = \sqrt{x}-4$, además $(\sqrt{x}-4)(\sqrt{x}+4) = x-16$.
entonces tenemos que multiplicar por $\sqrt[4]{x}+2$ en primer lugar

$$\frac{\sqrt[4]{x}+2}{\sqrt[4]{x}-\sqrt[3]{8}} = \frac{\sqrt[4]{x}+2}{\sqrt[4]{x}-2}.\frac{\sqrt[4]{x}+2}{\sqrt[4]{x}+2} = \frac{(\sqrt[4]{x}+2)(\sqrt[4]{x}+2)}{\sqrt[4]{x}^2-2^2} = \frac{(\sqrt[4]{x}+2)(\sqrt[4]{x}+2)}{\sqrt{x}-4}$$

y luego por $\sqrt{x}+4$:

$$\frac{(\sqrt[4]{x}+2)(\sqrt[4]{x}+2)}{\sqrt{x}-4} = \frac{(\sqrt[4]{x}+2)^2}{\sqrt{x}-4}.\frac{\sqrt{x}+2}{\sqrt{x}+2} = \frac{(\sqrt[4]{x}+2)^2(\sqrt{x}+2)}{\sqrt{x}^2-4^2} = \frac{(\sqrt[4]{x}+2)^2(\sqrt{x}+2)}{x-16}$$

El hecho de pensar a las raíces como potencias nos permite hablar de potencias fraccionarias definiendo

$$\boxed{a^{\frac{b}{c}} = \sqrt[c]{a^b}}$$

Del mismo modo que al escribir fracciones buscamos expresiones irreducibles (es decir, preferimos escribir $\frac{2}{7}$ en lugar de $\frac{10}{35}$) al escribir expresiones con raíces, buscamos que sean irreducibles, es decir, preferimos 4 a $\sqrt{16}$ y $3\sqrt[4]{3}$ a $\sqrt[3]{729}$.

El procedimiento para reducir estas expresiones de llama *extracción de radicales* y se basa sencillamente en factorizar el número bajo la raíz y aplicar la propiedad 4. ó 9.

Ejemplo 4.6 1. $729 = 3^6$, por lo tanto $\sqrt[4]{729} = \sqrt[4]{3^6} = \sqrt[4]{3^6} \cdot \sqrt[4]{3} = 3 \cdot \sqrt[4]{3^2}$

2. $\sqrt[3]{864000} = \sqrt[3]{3^3 \cdot 4^4 \cdot 5^3} = \sqrt[3]{3^3} \cdot \sqrt[3]{4^4} \cdot \sqrt[3]{5^3} = 3 \cdot \sqrt[3]{4^3 \cdot 4} \cdot 5 = 3 \cdot \sqrt[3]{4^3} \cdot \sqrt[3]{4} \cdot 5 = 3 \cdot 4 \cdot \sqrt[3]{4} \cdot 5 = 3 \cdot 4 \cdot 5\sqrt[3]{4} = 60\sqrt[3]{4}$

Analicemos lo que ha ocurrido en el caso de $\sqrt[4]{729} = 3 \cdot \sqrt[4]{3^2}$.

Si hacemos la división entera 6 dividido 4 es 1 y da resto 2. Es decir, $6 = 4 \cdot 1 + 2$ y resulta

$\sqrt[4]{3^6} = \sqrt[4]{3^{4 \cdot 1 + 2}} = \sqrt[4]{(3^1)^4} \cdot \sqrt[4]{3^2} = 3 \cdot \sqrt[4]{3^2} = 3 \cdot \sqrt{3}.$

Otra forma es pensarlo como potencia fraccionaria:
$\sqrt[4]{3^6} = 3^{\frac{6}{4}} = 3^{1+\frac{2}{4}} = 3^{1+\frac{1}{2}} = 3^1 \cdot 3^{\frac{1}{2}} = 3 \cdot \sqrt{3}$

Esto se cumple en general: Si $a = q \cdot b + r$ resulta
$\sqrt[b]{x^a} = \sqrt[b]{x^{b \cdot 1 + r}} = \sqrt[b]{(x^q)^b} \cdot \sqrt[b]{x^r} = x^q \cdot \sqrt[b]{x^r}$

Ejercicios resueltos

1. $(2+1)^2 + 3^3 : (-3)^2 = 3^2 + 3^{(3-2)} = 9 + 1 = 10$
2. $\sqrt{60+4} = \sqrt{64} = \pm 8$
3. $\sqrt[3]{b} \cdot \sqrt[3]{b^5} = \sqrt[3]{b^{1+5}} = \sqrt[3]{b^6} = b^{\frac{6}{3}} = b^2$
4. $(\sqrt[5]{32} - \sqrt{\sqrt{625}}) : \sqrt[3]{3^3} = (2 - \sqrt[4]{625}) : 3 = (2-5) : 3 = -1$
5. $\sqrt[3]{20^3 x^6 y^9} = \sqrt[3]{20^3} \cdot \sqrt[3]{x^6} \cdot \sqrt[3]{y^9} = 20 \cdot x^2 \cdot y^3$
6. $\dfrac{1-\sqrt{3}}{\sqrt[4]{3}-1} =$

$$= \frac{1-\sqrt{3}}{\sqrt[4]{3}-1} \cdot \frac{\sqrt[4]{3}+1}{\sqrt[4]{3}+1} = \frac{(1-\sqrt{3})(\sqrt[4]{3}+1)}{(\sqrt[4]{3}-1)(\sqrt[4]{3}+1)} = \frac{(1-\sqrt{3})(\sqrt[4]{3}+1)}{(\sqrt[4]{3})^2-1^2}$$

$$= \frac{(1-\sqrt{3})(\sqrt[4]{3}+1)}{\sqrt{3}-1} = \frac{(1-\sqrt{3})(\sqrt[4]{3}+1)}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} =$$

$$= \frac{(1-\sqrt{3})(\sqrt[4]{3}+1)(\sqrt{3}+1)}{(\sqrt{3}-1)(\sqrt{3}+1)} = \frac{(1-\sqrt{3})(\sqrt[4]{3}+1)(\sqrt{3}+1)}{(\sqrt{3})^2-1^2} =$$

$$= \frac{1}{2}(1-\sqrt{3})(\sqrt[4]{3}+1)(\sqrt{3}+1).$$

4.5.3. Factorización

En esta sección trabajaremos con sumas algebraicas para convertirlas, en caso de ser posible, en productos. Igual que hasta ahora trabajaremos sobre ejemplos y deduciremos la regla general.

Ejemplo 4.7 $3a^2 + a^8 \cdot b - a^6 b^2 + a^4 c$

Los términos de esta suma algebraica son: $3a^2,\ a^8 \cdot b,\ -a^6 \cdot b^2,\ a^4 \cdot c$, en cada uno de estos términos aparece el factor a, en el primero con potencia 2, en el segundo 8, en el tercero 6 y en el cuarto 4, por lo tanto la mayor potencia que hay en todos (la menor potencia que aparece) es 2. Resulta que a^2 es un *factor común*.

¿Cómo transformamos esta suma en un producto? Dividimos cada término por el factor común y colocamos el resultado entre paréntesis.

Cálculos auxiliares:

$$\frac{3 \cdot a^2}{a^2} = 3 \quad \frac{a^8 \cdot b}{a^2} = a^6 \cdot b \quad \frac{-a^6 \cdot b^2}{a^2} = -a^4 \cdot b^2 \quad \frac{a^4 \cdot c}{a^2} = a^2 \cdot c$$

$$3a^2 + a^8 \cdot b - a^6 \cdot b^2 + a^4 c = a^2 \cdot (3 + a^6 \cdot b - a^4 \cdot b^2 + a^2 c).$$

Ejemplo 4.8 $a \cdot b - a \cdot c + 3 \cdot a + 2 \cdot b - 2 \cdot c + 6$

En este caso si analizamos los términos $a \cdot b,\ -a \cdot c,\ 3 \cdot a,\ 2 \cdot b,\ -2 \cdot c,\ 6$ no encontramos un factor que sea común a todos, pero entre el primero, segundo y tercero encontramos a a como factor común y en los tres últimos 2 es factor común, podemos hacer el mismo procedimiento de antes, por grupos, para obtener:

$a \cdot b - a \cdot c + 3 \cdot a + 2 \cdot b - 2 \cdot c + 6 = a \cdot (b - c + 3) + 2 \cdot (b - c = 3)$

Ahora tenemos dos términos y el factor común a ambos es $b-c+3$, entonces podemos escribir:

$a \cdot b - a \cdot c + 3 \cdot a + 2 \cdot b - 2 \cdot c + 6 = (a + 2)(b - c + 3)$

Hemos sacado *factor común por grupos.*

- $(a + b)^2 = (a + b) \cdot (a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b = a^2 + 2 \cdot a \cdot b + b^2$

Acabamos de elevar al cuadrado un *binomio* [8] Hemos obtenido un *trinomio cuadrado perfecto*, es decir, una expresión de tres términos que tiene dos cuadrados perfectos y el doble producto de las bases.

Ejemplo 4.9 1. $c^2 + 9 - 6c$

c^2 es un cuadrado perfecto que es tanto el cuadrado de c como el de $-c$, $9 = 3^2$ también; el término que falta debe ser $2 \cdot c \cdot 3$ ó $2 \cdot (-c) \cdot 3$. Como se cumple esta segunda posibilidad $c^2 + 9 - 6c = ((-c) + 3)^2 = (3 - c)^2$.

2. $a^2 + b^2$

No es el cuadrado de un binomio porque no tiene tres términos.

- $(a + b)^3 = (a + b)^2 \cdot (a + b) =$

$$= (a^2 + 2 \cdot a \cdot b + b^2) \cdot (a + b) =$$
$$= a^3 + 2 \cdot a^2 \cdot b + a \cdot b^2 + a^2 \cdot b + 3 \cdot a \cdot b^2 + b^3 =$$
$$= a^3 + 3 \cdot a^2 \cdot b + 3 \cdot a \cdot b^2 + b^3$$

Acabamos de elevar al cubo un binomio, obtuvimos un *cuatrinomio cubo perfecto*, es decir, una expresión de cuatro términos donde dos de ellos son cubos perfectos y los otros dos son el triplo del cuadrado de una base por la otra.

Ejemplo 4.10 1. $z^3 - 64 - 12 \cdot z^2 + 48 \cdot z$

z^3 es un cubo perfecto, $-64 = (-4)^3$, los otro dos términos deben ser

[8] bi: dos, nomio: parte, un *binomio* es una expresión que tiene dos términos. Así un *trinomio* tendrá tres términos, un *cuatrinomio*, cuatro y un *polinomio*, muchos.

$3 \cdot (-4)^2 \cdot z = 48 \cdot z$ y $3 \cdot (-4) \cdot z^2 = -12 \cdot z^2$, como estos términos aparecen, podemos afirmar:

$z^3 - 64 - 12 \cdot z^2 + 48 \cdot z = (z-4)^3$

2. $8 + 3a^2 + 3a + 27$

   $8 = 2^3$ y $27 = 3^3$ son cubos perfectos, pero no figura entre los términos $3 \cdot 2^2 \cdot 3$ ni $3 \cdot 2 \cdot 3^2$, por lo tanto no es un cuatrinomio cubo perfecto.

- $(a+b) \cdot (a-b) = a \cdot a - a \cdot b + a \cdot b + b \cdot b = a^2 - b^2$

Hemos encontrado una *diferencia de cuadrados* que provino de multiplicar un binomio por otro con el signo cambiado en uno (y sólo uno) de sus términos. Estos binomios se llaman *conjugados*. Son conjugados $2 + a$ y $2 - a$, $-3 + b$ y $3 + b$, pero no lo son $a + 4$ y $-a - 4$.

Ejemplo 4.11 1. $x^2 + 9$.

   Tanto x^2 como $9 = 3^2$ son cuadrados, pero el signo + hace que no sea una diferencia y no tiene solución.

2. $x^4 - 25$.

   $x^4 = (x^2)^2$ y $25 = 5^2$, entonces podemos afirmar que $x^4 - 25 = (x^2+5) \cdot (x^2-5)$.

En resumen: Hemos mencionado cinco casos de factoreo:

1. Factor común
2. Factor común por grupos
3. Trinomio cuadrado perfecto
4. Cuatrinomio cubo perfecto
5. Diferencia de cuadrados

Nos queda el "sexto caso" que veremos cuando hayamos visto la *regla de Ruffini*.

Ejercicios resueltos

1. $2\sqrt{3} - \sqrt{6} - 2\sqrt{5} + \sqrt{10} = 2\sqrt{3} - \sqrt{2 \cdot 3} - 2\sqrt{5} = \sqrt{2 \cdot 5} = 2\sqrt{3} - \sqrt{2}\sqrt{3} - 2\sqrt{5} + \sqrt{2}\sqrt{5} = 2(\sqrt{3} - \sqrt{5}) - \sqrt{2}(\sqrt{3} - \sqrt{5}) = (2 - \sqrt{2})(\sqrt{3} - \sqrt{5})$
2. $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$
3. $x\sqrt{x} + 6x + 12\sqrt{+}8 = (\sqrt{x})^3 + 3 \cdot \sqrt{x}^2 \cdot 2 + 3 \cdot \sqrt{x} \cdot 2^2 + 2^3 = (\sqrt{x} + 2)^3$

Ejercicios propuestos

1. Calcular:

   (a) $\dfrac{3\,(2+a)}{6+3a}$

   (b) $\dfrac{3a+6+2b+ab}{(5+6b)+a-(3+b)}$

   (c) $\dfrac{a^2-1}{3a+ab-3-b}$

   (d) $\dfrac{a^2+6a+9}{ab^2-2ab+a-3\,(-b^2+2b-1)}$

   (e) $\dfrac{a^3+3a^2b+3ab^2+b^3}{(a^2-b^2)(a^2+2ab+b^2)}$

2. Simplificar las siguientes expresiones:

   a) $\left(\dfrac{3x^{\frac{2}{3}}y^3}{2x^{\frac{5}{3}}z^{-3}}\right)\left(\dfrac{16x^4y^5}{x^2z^4}\right)^{\frac{1}{2}}$

   b) $\left(\dfrac{25x^{\frac{1}{5}}y^{\frac{4}{3}}}{x^{-\frac{2}{15}}x^{-\frac{1}{3}}}\right)^{-\frac{1}{3}}\left(\dfrac{125x^{-2}z}{y^2}\right)^{-\frac{1}{3}}$

   c) $\left(\dfrac{16a^5+6a^6-2a^5b}{-2a^2x^5-4a^2x^4-2a^2x^3}\right):\left(\dfrac{8+3a-b}{x^2+2x+1}\right)^{\frac{2}{3}}$

   d) $\dfrac{a^4b^2-c^2a^2}{a^3b+ca^2}$

   e) $\dfrac{2a^3+a^2-2ab-b}{a(2a+1)}$

   f) $\dfrac{x^2y-9z+zx^2-9y}{xy+zx+3y+3z}$

4.5.4. Ecuaciones

Una *ecuación* es una igualdad entre dos expresiones que contiene al menos una incógnita, a la que llamaremos *variable.*

Vamos a resolver ecuaciones en una variable. Hemos aprendido a resolver ecuaciones “pasando términos” (si está sumando, pasa restando, si está dividiendo pasa multiplicando, etc.) Si bien es cierto que éste es el resultado final la idea no es “pasar términos” en primer lugar porque si “pasamos sumando” (o restando) sí trabajamos con términos, pero si “pasamos multiplicando” (o dividiendo) estamos trabajando con factores.

Veamos un caso muy sencillo:

Ejemplo 4.12 $-9x - 4 = -4x + 6$

$-9x + 4x = 6 + 4$ “pasamos para un lado las x y los números para el otro”
$-5x = 10$ “hacemos las cuentas”
$x = \dfrac{10}{-5}$ “pasa el -5 dividiendo”
$x = -2$ “hacemos las cuentas”

En realidad lo que estamos haciendo es aplicar las reglas de monotonía de la suma y el producto y la existencia de simétricos e inversos. Es decir:

$-9x - 4 = -4x + 6$

$(-9x - 4) + 4 = (-4x + 6) + 4$ para eliminar el -4 sumamos su simétrico
$-9x = -4x + 10$ se resuelven las cuentas
$(-9x) + 4x = (-4x + 10) + 4x$ para eliminar el $-4x$ sumamos su simétrico
$-5x = 10$ se resuelven las cuentas
$-5x \cdot (-5)^{-1} = 10 \cdot (-5)^{-1}$ para eliminar el -5 se multilpica por su inverso
$x = -(10 \cdot 5^{-1})$ se resuelven las cuentas
$x = -2$ se resuelven las cuentas

Si bien en el caso de resolución de ecuaciones no tiene consecuencias insalvables, al momento de trabajar con inecuaciones es de vital importancia tener en claro qué es lo que se está haciendo al “pasar términos” ya que las desigualdades pueden llegar a cambiar.

Otro tema muy importante al momento de resolver una ecuación es encontrar los valores para los cuales no tiene sentido tal ecuación.

Ejemplo 4.13 $\dfrac{x^2 - 9}{x - 3} = 0$

Aquí tenemos una fracción, para que un cociente sea 0 debe ser nulo el numerador, pero **no** el denominador ya que **no se puede dividir por 0**

$x^2 - 9 = 0$ si y sólo si $x^2 = 9$, es decir, $x = 3$ ó $x = -3$. Si $x = -3$ no hay ningún problema, pero si $x = 3$ la cuenta no se puede hacer, por lo tanto la única solución de la ecuación es $x = -3$

Por último, pero no menos importante, se debe tener muy a mano todas las propiedades que nos ayuden a allanar el camino a la solución.

Ejemplo 4.14

Si tenemos que calcular $5(x-4)(x+2)(x-\sqrt{2}) = 0$, lo que tendemos a hacer es aplicar propiedad distributiva y hacer todos los productos. La ecuación queda:
$x^3 - (2+\sqrt{2})x^2 + (2\sqrt{2}-8)x + 8\sqrt{2} = 0,$

y encontrar la solución, al menos en esta instancia, es imposible. Sin embargo, si recordamos que un producto es igual a 0 si y sólo si uno de sus factores lo son, esta ecuación se verifica si:

$(x-4) = 0$ ó $\quad (x+2) = 0$ ó $\quad (x-\sqrt{2}) = 0,$
es decir si $\quad x = 4$ ó $\quad x = -2$ ó $\quad x = \sqrt{2}.$

Ejercicios resueltos

1. $9x - 4 = -4x + 6$

   $(9x-4) + 4 = (-4x+6) + 4$

   $9x = -4x + 10$

   $9x + 4x = (-4x+10) + 4x$

   $13x = 10, \qquad\qquad x = 10/13$

2. $\dfrac{2x-2}{3} - 2 = \dfrac{2x+4}{5} - 4$

   $\dfrac{2x-2}{3} - \dfrac{2x+4}{5} = -4 + 2$

   $\dfrac{5(2x-2) - 3(2x+4)}{3 \cdot 5} = -2$

   $\dfrac{10x - 10 - 6x - 12)}{15} = -2$

   $\dfrac{4x - 22)}{15} = -2$

   $4x - 22 = -30 \; 4x = -30 + 22, \qquad\qquad x = -8$

4.6. Ejercicios propuestos

Ejercicio 4.4 Encontrar el primer elemento de los siguientes subconjuntos de $\mathbb{N}$:

1. $A = \{n \in \mathbb{N} : n > 10\}$
2. $B = \{n \in \mathbb{N} : n \text{ divide a } 5\}$
3. $C = \{n \in \mathbb{N} : n^2 + n > 20\}$
4. $D = \{n \in \mathbb{N} : n \text{ no divide a } 5\}$

Ejercicio 4.5 Hallar los primeros cuatro términos de la sucesión definida recursivamente:

1. $a_0 = 2,\ a_{n+1} = 2 + a_n$
2. $(\diamond)$ $a_0 = 1,\ a_{n+1} = 1 + 2\,a_n$
3. $(\diamond)$ $a_0 = 1,\ a_1 = 1,\ a_{n+2} = a_n + a_{n+1}$

Ejercicio 4.6 Definir recursivamente:

1. $n!$
2. (®) $\displaystyle\bigcup_{i=0}^{n} A_i$
3. $(\diamond)$ $\displaystyle\bigcap_{i=0}^{n} A_i$
4. 3^n

Ejercicio 4.7 Usar el principio de inducción para probar:

1. $1 + r + r^2 + \cdots + r^n = \dfrac{1 - r^{n+1}}{1 - r},\ r \neq 1.$
2. $(\diamond)$ $1 + \dfrac{1}{2} + \dfrac{1}{4} + \cdots + \dfrac{1}{2^n} = 2 - \dfrac{1}{2^n}$
3. $(\diamond)$ $1 + 3 + 5 + \cdots + (2n - 1) = n^2,\ n > 0.$
4. $a + (a + d) + (a + 2\,d) + \cdots + (a + (n - 1)d) = \dfrac{n\,(2\,a + (n - 1)\,d\,)}{2}$
5. (®)$\displaystyle\sum_{k=1}^{n} k\,2^k = 2 + (n - 1)\,2^{n+1}$
6. $(\diamond)$ $\displaystyle\sum_{k=1}^{n} kk! = (n + 1)! - 1,\ n > 0.$
7. $\dfrac{1}{1\,.\,2} + \dfrac{1}{2\,.\,3} + \cdots + \dfrac{1}{n\,.\,(n + 1)} = \dfrac{n}{n + 1}$
8. $\dfrac{5^n - 1}{4}$ es un número entero.

9. ($\diamond$) $2^{2n+1}+1$ es divisible por 3.
10. $3^n \geq 1+2^n$.
11. ($\diamond$) $n^2 \geq n$.
12. ($\diamond$) $\left(\dfrac{1}{2}\right)^n \leq \dfrac{1}{n}$.
13. ($\diamond$) $\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$. Observación: $\overline{A} = A'$.
14. ($\diamond$) $|A_1 \times A_2 \times \cdots \times A_n| = |A_1|.|A_2|. \cdots .|A_n|$

    Observación: $|A|$ es el número de elementos de A, también llamado el orden de A.
15. ($\clubsuit$) La suma de las medidas de los ángulos internos de un polígono convexo de n lados es $(n-2)\cdot\pi$.
16. ($\clubsuit$) El número de diagonales de un polígono convexo de n lados $(n \geq 3)$ es $\dfrac{n(n-3)}{2}$.

Ejercicio 4.8 ($\clubsuit$) (Problema atribuído por Knuth a un libro de Pólya de 1954.)
Hallar el error en la siguiente "demostración"de que todos los caballos son del mismo color.
Como cualquier cantidad de caballos es un número natural, podemos reformular la proposición como: $P(n)$ En cualquier conjunto de n caballos, todos los caballos son del mismo color.
Caso base: Un solo caballo es claramente del mismo color que sí mismo.
Paso inductivo: Supongamos que $P(k)$ es verdadero y probemos $P(k+1)$.
Sea A un conjunto de $k+1$ caballos, podemos escribir $A = \{c_1, c_2, c_3 \cdots, c_k, c_{k+1}\}$.
Consideremos los conjuntos $A_1 = \{c_1, c_2, c_3 \cdots, c_k\}$ y $A_2 = \{c_2, c_3 \cdots, c_k, c_{k+1}\}$
Ambos conjuntos tienen k elementos y, por hipótesis inductiva, todos los caballos de A_1 y de A_2 son del mismo color. Como $A_1 \cap A_2 \neq \emptyset$, necesariamente se verifica $P(k+1)$.

Ejercicio 4.9 ¿Es posible la siguiente proposición?:
Todos los números naturales son iguales.
En efecto: Supongamos que vale para $k \in \mathbb{N}$ y probémoslo para $k+1$. Es decir, suponemos $k = k+1$ y queremos probar $k+1 = (k+1)+1$, lo cual se verifica simplemente sumando 1 a ambos miembros de la igualdad $k = k+1$.
Por lo tanto, $n = n+1$ para todo $n \in \mathbb{N}$, es decir, todos los números naturales son iguales.

Ejercicio 4.10 ¿Es válido el siguiente argumento?:
Al levantarme cierta maana, pude presenciar un espectacular amanecer. Deseé que todas las mañanas fueran como esa. Desde entonces, siempre me he despertado temprano para ver la salida del Sol, y he observado cómo cada nuevo amanecer sigue al anterior. De esta experiencia podemos concluir, por inducción, que el Sol saldrá mañana y que continuará saliendo en cada jornada sucesiva.

Ejercicio 4.11 Ejemplos claros de principio de inducción fuerte o segunda forma del principio de inducción:
Demostrar que todo número mayor que 13 puede escribirse como sumas de ochos y treses.
Veamos los primeros pasos: (casos base):

$$14 = 8 + 3 + 3$$
$$15 = 3 + 3 + 3 + 3 + 3$$
$$16 = 8 + 8$$

Paso inductivo fuerte:
Supongamos que todo número menor que k y mayor que 13 satisface esta proposición y probémoslo para $k > 16$. Claramente $k = (k - 3) + 3$, como $k - 3$ es menor que k y mayor que 13 satisface la proposición y sumando 3 a ambos miembros vemos que se verifica para k. Por lo tanto todo número natural mayor que trece puede escribirse como la suma de un múltiplo de tres más un múltiplo de 8.

1. $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_n = a_{n-1} + a_{n-2} + a_{n-3}$. Probar que $a_n < 3^n$, para todo $n \geq 2$.
2. ($\diamond$) $a_0 = 1$, $a_1 = 2$, $a_n = a_{n-1} + a_{n-2}$, si $n > 2$. Demostrar que $a_n \leq (7/4)^n$.
3. ($\diamond$) Sea $a_0 = 0$, $a_1 = 1$, $a_{n+2} = \dfrac{a_{n+1} + a_n}{2}$. Demostrar que $a_n = \dfrac{2}{3}\left(1 - \left(-\dfrac{1}{2}\right)^n\right)$.

($\clubsuit$) Después de transcurridos n meses en un experimento de invernadero, se ha observado el siguiente comportameinto en el número de plantas de un cierto tipo particular:
$p_0 = 3$,
$p_1 = 7$ y
$p_n = 3\,p_{n-1} - 2\,p_{n-2}$.
Demostrar que el número de plantas es $p_n = 2^{n+2} - 1$.

Ejercicio 4.12 Dadas las siguientes sucesiones, definirlas recursivamente, hallar un posible término n-ésimo y probar la veracidad inductivamente.

1. 3,5,7,9,11,13,...
2. $2, -1, \frac{1}{2}, -\frac{1}{4}, \frac{1}{8}, -\frac{1}{16}, \ldots$
3. $\frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \frac{1}{120}, \ldots$

Ejercicio 4.13 Dadas la función $f(x) = 2x + 1$ y las siguientes definiciones recursivas, hallar la forma general y demostrar su validez por inducción.

1. $\begin{cases} a_0 = f(x) \\ a_{n+1} = f \circ a_n \end{cases}$
2. $\begin{cases} b_0 = f(x) \\ b_{n+1} = f + b_n \end{cases}$
3. $\begin{cases} c_0 = f(x) \\ c_{n+1} = f \cdot c_n \end{cases}$

Ejercicio 4.14 ($\diamond$) Pasar las siguientes expresiones de forma recursiva a forma explícita:

1. $\begin{cases} a_0 = 1 \\ a_{n+1} = 2a_n + 1 \end{cases}$
2. $\begin{cases} a_0 = 2 \\ a_{n+1} = 3a_n + 1 \end{cases}$
3. $\begin{cases} a_0 = \frac{1}{2} \\ a_{n+1} = 5a_n - 3 \end{cases}$
4. $\begin{cases} a_0 = 1 \\ a_{n+1} = 2(n+1)a_n \end{cases}$

Ejercicio 4.15 Dada la expresión explícita $\frac{5^{n+1} - 1}{7}$, determinar una forma recursiva.

Ejercicio 4.16 ($\clubsuit$) Un número impar de gente se para en un parque de manera que la distancia entre ellos es mutuamente distinta. Cada persona lanza una torta a la persona que tiene más cerca. Demostrar usando inducción que siempre existe una persona a la que no le llega una torta en la cara.

Capítulo 5

Divisibilidad de enteros

Divisibilidad de enteros. Máximo común divisor. Algoritmo de Euclides. Teorema fundamental de factorización. Aplicaciones. Sistemas de numeración en distintas bases.

5.1. Divisibilidad

Hemos construido los números naturales a partir de los axiomas de Peano, los enteros para poder resolver la ecuación $a + x = b$ para todo par de números a, b y los racionales para poder resolver la ecuación $a \cdot x = b$ para todo par a, b.
Estas ecuaciones tienen solución para algunos pares de números. Así, si para el par de números naturales a, b tales que existe un x que solucione la ecuación $a + x = b$ decimos que $a < b$ y probamos que esta es una relación de orden para los números naturales. Luego extendimos esta relación a los enteros, racionales y reales.
En este capítulo trabajaremos con los pares de enteros a, b tales que existe un x que solucione la ecuación $a \cdot x = b$

Definición 5.1 Dados $a, b \in \mathbb{Z}$ se dice que a *divide* a b y se escribe $a \mid b$ si existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Si a no divide a b escribiremos $a \not| b$.

Ejemplo 5.1 Consideremos los enteros 6 y 3. Podemos ver que $6 = 2 \cdot 3$ y por lo tanto afirmar que $3 \mid 6$ y en verdad también $2 \mid 6$. $5 \not| 6$.

(✠) Hablamos de números enteros y el primer ejemplo lo dimos con números naturales. El tema es que históricamente, si bien los indios usaron desde el siglo VII los números negativos para indicar deudas, sólo fueron aceptados formalmente en la matemática hasta el siglo XVIII. Sabemos que la divisibilidad es conocida desde tiempos remotos, por ejemplo los indios conocían la divisibilidad por tres, siete y nueve, los egipcios distinguían números pares e impares, pero fue el matemático griego Euclides (c.325 - c.265 a.C.) quien demostró los teoremas básicos de divisibilidad. Finalmente, el matemático francés Pascal (1623-1662) propuso las reglas para conocer la divisibilidad de cualquier número.

Observación 5.1 Cuando hablamos de números naturales, dijimos que Peano los definió diciendo que tienen un primer elemento y que está discutido si es 1 o 0. Hasta este momento consideramos que $0 \in \mathbb{N}$, ya que en todo proceso debe considerarse el estado inicial, que es el "tiempo cero". En este capítulo, sin embargo, hablaremos de divisibilidad y es, justamente, en teoría de números cuando el 0 se convierte en un elementos indeseable. En consecuencia, cada vez que hablemos de números naturales, consideraremos que el 0 no está dentro del conjunto, salvo mención explícita.

Veamos algunas propiedades de la divisibilidad:

Es claro que $a = 1 \cdot a$ para cualquier número entero a, lo cual hace que afirmemos $1 \mid a$ y $a \mid a$ para todo entero a.

Si $a \mid b$ y $b \mid c$ resulta que existen $k_1, k_2 \in \mathbb{Z}$ tales que $b = a \cdot k_1$ y $c = b \cdot k_2$. Reemplazando b en la segunda ecuación queda $c = (a \cdot k_1) \cdot k_2 = a \cdot (k_1 \cdot k_2) = a \cdot k$, es decir $a \mid c$.

$0 = a \cdot 0$ para todo $a \in \mathbb{Z}$, entonces $a \mid 0$, cualquiera que sea $a \in \mathbb{Z}$ (¿También para a=0? ¿El 0 es divisor de alguien?)

Si $c \mid a$ y $c \mid b$ podemos escribir $a = c \cdot k_1$ y $b = c \cdot k_2$, entonces:

$$\begin{array}{lcl} a = c \cdot k_1 & & a \cdot x = c \cdot k_1 \cdot x \\ & + & \\ b = c \cdot k_2 & & b \cdot y = c \cdot k_2 \cdot y \end{array}$$

$$a \cdot x + b \cdot y = (k_1 \cdot x + k_2 \cdot y) \cdot c = k \cdot c$$

y resulta que $c \mid ax + by$, cualesquiera sean $x, y \in \mathbb{Z}$.

Además, si $a \mid b$ resulta que existe $k \in \mathbb{Z}$ tal que $b = a.k$. Si $a, b > 0$ entonces

$$b = \underbrace{a + a + \cdots + a}_{k \text{ veces}} \text{ y resulta } b \geq a.$$

Si fuera $b < 0, -b > 0$ y

$$-b = \underbrace{a + a + \cdots + a}_{k \text{ veces}} \text{ y resulta } -b \geq a.$$

Considerando ambas posibilidades $|b| \geq a$, si $b \neq 0$.

Hemos estado dando justificaciones para las siguientes propiedades de la división:

Proposición 5.1 *Para todo $a, b, c \in \mathbb{Z}$ se tiene:*

(D_1) $1 \mid a$,

(D_2) $a \mid a$, *(propiedad reflexiva)*

(D_3) *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$* *(propiedad transitiva)*

(D_4) $a \mid 0$,

(D_5) *Si $c \mid a$ y $c \mid b$ entonces $c \mid a. \cdot x + b \cdot y$, cualesquiera sean $x, y \in \mathbb{Z}$*[1]

(D_6) *Si $a \mid b$ entonces $a \mid -b$, $-a \mid b, -a \mid -b$ y $a \mid k \cdot b$, $k \in \mathbb{Z}$,*

(D_7) *Si $a \mid b$, entonces $a \cdot c \mid b \cdot c$,*

(D_8) *Si $a \mid b$, $b \neq 0$, entonces $|a| \leq |b|$,*

(D_9) *Si $a \mid b$ y $b \mid a$ entonces $|a| = |b|$.*

Demostración: Hemos hecho el esquema de la demostración de casi todas las propiedades, queda a cargo del lector (y es muy buen ejercicio) realizar todas las demostraciones.®

Observación 5.2 Luego de revisar las propiedades aparecen algunas meditaciones:

1. Escribimos $c \mid a$ y $c \mid b$ entonces $c \mid a + b$ ¿vale la recíproca?
   ¿Qué pasa si sabemos que c divide a alguno de ellos (lo es a que b)?

[1] Dados $a, b \in \mathbb{Z}$, $a \cdot x + b \cdot y$ se dice una *combinación lineal entera*. Es combinación porque combina sumas o restas con productos, es lineal porque todo lo que aparece está elevado "a la 1" y es entera porque son todos números enteros. A esta propiedad la llamaremos "la reina" o bien "la sierva" porque nos va a servir (o a mandar) desde aquí hasta el final de los apuntes.

2. La relación divide, ¿define un orden en $\mathbb{Z}$?

Ejercicio 5.1 (♠)Este es un ejercicio realmente interesante, porque se utilizan recursos de diferentes capítulos:
Sean $a, b \in \mathbb{Z}$. Demostrar que si $b \mid a$, entonces $b \mid a^n$ para todo $n \in \mathbb{N}$.

5.2. Algoritmo de la división entera

Hasta ahora hablamos de pares de enteros a, b tales que $a \mid b$. Dijimos que en este caso lo que ocurre es que $b = k \cdot a$. Podríamos pensar que es como tener b unidades y cajitas con capacidad para a unidades. Si $a \mid b$ puedo llenar exactamente k cajitas. ¿Qué ocurre cuando $a \not\mid b$? Comenzamos a llenar las cajitas de a unidades y de pronto las unidades que quedan no alcanzan para llenar una nueva cajita. Siempre la cantidad de unidades que "sobra" es estrictamente menor que la capacidad de las cajitas.

Escribamos esto más formalmente:

Teorema 5.1 *Dados dos enteros a y b, con $b \neq 0$ existen enteros q y r unívocamente determinados tales que*

$$a = b \cdot q + r \text{ y } 0 \leq r < |b|.$$

Este resultado lo conocemos desde la escuela primaria, donde aprendimos que a se llama *dividendo*, b *divisor*, q *cociente*, (q por quotient) y r el *resto.*
La demostración de este teorema, tiene dos partes porque debemos probar no sólo que existen los q y r, sino que son únicos.
Demostración:

- *Existencia*

Supongamos, en primer lugar que $b > 0$ (como hablamos de números enteros esto es lo mismo que decir $b \geq 1$)y consideremos el conjunto

$$R = \{x : x = a - q.b, x \geq 0, q \in \mathbb{Z}\}$$

Claramente $R \subseteq \mathbb{N}$ y si $q = -|a|$ resulta $a - qb = a + |a|b = (1 + b)|a| > 0$ y por lo tanto $a - q.b \in R$. Por el Principio de Buena Ordenación, ya que R es un subconjunto no vacío de $\mathbb{N}$ tiene primer elemento. Llamemos r a ese primer elemento y veamos que cumple lo pedido.
Claramente $r = a - q.b$ y entonces $a = q.b + r$, $r \in R$, en consecuencia $0 \leq r$.

Resta ver $r < |b| = b$.
Supongamos $b \leq r$, entonces $0 = b - b \leq r - b$ y $r - b = a - q \cdot b - b = a - (q+1) \cdot .b$.
Es decir, $r - b$ satisface las condiciones del conjunto R, pero es estrictamente menor que su primer elemento r. Absurdo, que provino de suponer que $b \leq r$, en consecuencia debe ser $r < b$.

Si $b < 0$, resulta $-b > 0$. Hemos probado que existen q, r tales que $a = q \cdot (-b) + r = (-q) \cdot b + r$, con $0 \leq r < -b = |b|$.

► *Unicidad*

Siguiendo el método más sencillo para demostrar unicidad, supongamos que hay dos.
El simple hecho de suponer que hay dos no significa que estemos haciendo una demostración por el absurdo. Sólo suponemos que hay dos (no dos distintos) y llegaremos a ver que son necesariamente iguales.
Sean q_1, r_1 y q_2, r_2 tales que $a = q_1 \cdot b + r_1$ y $a = q_2 \cdot b + r_2$. Entonces $q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ y resulta $(q_1 - q_2) \cdot b = r_2 - r_1$.
Las posibilidades son $r_2 = r_1$ o $r_2 \neq r_1$.
Si fuera $r_2 \neq r_1$ resultaría $r_2 - r_1 \neq 0$, es decir, $(q_1 - q_2) \cdot b \neq 0$ y, en consecuencia $|r_2 - r_1| = |(q_1 - q_2) \cdot b| = |q_1 - q_2| \cdot |b| \geq |b|$ (si $q_1 - q_2 \neq 0$, entonces $|q_1 - q_2| \geq 1$), lo cual es un absurdo.
Veamos explícitamente este absurdo: Ha quedado escrito $|r_2 - r_1| \geq |b|$. Los restos son “los que sobran” que siempre son menos que b, la diferencia entre dos cantidades menores que b jamás puede ser mayor o igual que b. $\square$

Ejemplo 5.2 Si pretendemos hoy en día que tomen lápiz y papel para hacer una división y encontrar el cociente y el resto no vamos a llegar a buen puerto. Las calculadoras hacen las divisiones con coma... ¿qué hacer? ¡La cuenta! Y no es nada difícil. Veamos: queremos hallar el cociente y el resto de dividir 356 por 43.

$$356 \div 43 = 8,2...$$

$$356 - 43.8 = 12$$

$$q = 8 \text{ y } r = 12.$$

Haciendo este ejemplo tuve una lamentable experiencia que justifica a muchos de los resultados erróneos en las cuentitas que se propoponen en las redes sociales. En un primer momento usé la “vista estándar” de la calculadora que ofrece Microsoft e hice la cuenta: $356 - 43 \cdot 8 = 2504$ ¿qué? ¡imposible! Repetí el proceso y vi que este tipo de calculadoras resuelve las operaciones en el orden en que ingresan, sin considerar la separación en términos. Busqué

la "vista científica" y obtuve el resultado correcto.
Moraleja: no se olviden que *todavía* el cerebro propio piensa mejor.

Juguemos un poquito con números negativos:

1. 356 y 43: $356 = 43 \cdot 8 + 12$
2. 356 y -43: $356 = (-43) \cdot (-8) + 12$ y podemos admitir cocientes negativos.
3. -356 y 43:$-356 = -(43 \cdot 8 + 12) = 43 \cdot (-8) - 12$, pero no admitimos restos negativos, entonces sumamos y restamos el divisor: $43 \cdot (-8) - 12 = 43 \cdot (-8) \underbrace{-12 + 43} - 43 = 43 \cdot (-8) + 31 - 43 = 43 \cdot (-9) + 31$
4. -356 y -43: $-356 = -(43 \cdot 8 + 12) = (-43) \cdot 8 - 12$, pero no admitimos restos negativos, entonces sumamos y restamos el divisor: $(-43) \cdot 8 - 12 = (-43) \cdot 8 \underbrace{-12 + 43} - 43 = (-43) \cdot (-8) + 31 - 43 = (-43) \cdot 9 + 31$

Veamos ejemplos más entretenidos:

Ejemplo 5.3 Si el resto de dividir a por 15 es 7, hallar el resto de dividir $a^2 - 6a + 10$ por 15.

Veamos: $a = 15 \cdot q + 7$, entonces:

$$a^2 = (15 \cdot q + 7)^2 = 15^2 \cdot q^2 + 2 \cdot 15 \cdot q \cdot 7 + 7^2 = 15 \cdot (15 \cdot q^2 + 2 \cdot q \cdot 7) + 49 = 15 \cdot q_1 + 49$$

$$6 \cdot a = 6 \cdot (15 \cdot q + 7) = 15 \cdot (6 \cdot q) + 42 = 15 \cdot q_2 + 42$$

$$a^2 - 6 \cdot a + 10 = 15 \cdot q_1 + 49 - (15 \cdot q_2 + 42) + 10 = 15 \cdot q_3 + 7 + 10 = 15 \cdot (q_3 + 1) + 2.$$

El resto de dividir $a^2 - 6a + 10$ por 15 es 2.

($\clubsuit_1$) Si el resto de dividir un entero a por 5 es 3, calcular el resto de la división por 5 de: $3a$, $-a$, $2a + 5$, $-a + 2$, $5a + 2$, a^2, a^3.

($\clubsuit_2$) El famoso cuento de la propina: Tres amigos toman algo en un bar. Al finalizar el mozo les trae la cuenta: son 30 dólares. Cada amigo aporta 10 dólares. Al rato el mozo vuelve diciendo que hubo un error, que eran solamente 25 dólares y trae 5 billetes de un dólar. Cada amigo toma un dólar y dejan 2 dólares de propina. Al día siguiente uno de los amigos razona:
-Hay algo que no entiendo. Cada uno puso 10 dólares, luego recuperó uno.

Entonces, cada uno puso 9 dólares por 3, ventisiete y dos que dejamos de propina son veintinueve ¿Dónde está el dólar que falta?

5.3. Máximo común divisor

En las propiedades de divisibilidad hemos visto que $1 \mid a$ y $a \mid a$ para todo $a \in \mathbb{Z}$, esto en parte nos anima a dar las siguientes definiciones:

Definición 5.2 Dado $a \in \mathbb{Z}$, definimos el conjunto de los *divisores de* a y lo notamos $D(a)$ al conjunto de todos los números enteros que dividen a a. En símbolos:

$$D(a) = \{k \in \mathbb{Z} : k \mid a\}$$

Comentamos antes de esta definición que $D(a) \neq \emptyset$ y también podemos afirmar que es acotado, ya que $k \mid a$, entonces $|k| \leq |a|$ y resulta ser $|a|$ el mayor divisor de a.

Ejemplo 5.4 $D(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\} = \{1, 2, 3, 6, \} \cup \{-1, -2, -3, -6\}$.

Y motiva la siguiente

Definición 5.3 Dado $a \in \mathbb{Z}$, definimos el conjunto de los *divisores positivos de* a y lo notamos $D^+(a)$ al conjunto de todos los números enteros positivos que dividen a a. Análogamente definimos el conjunto de los *divisores negativos de* a y lo notamos $D^-(a)$ al conjunto de todos los números enteros negativos que dividen a a. En símbolos:

$$D^+(a) = \{k \in \mathbb{Z} : k \mid a, k > 0\},\ D^-(a) = \{k \in \mathbb{Z} : k \mid a, k < 0\}$$

Claramente $D(a) = D^+(a) \cup D^-(a)$.

(♠) Otro lindo ejercicio “mezcla”: Probar $D(a) = D(-a)$, cualquiera sea $a \in \mathbb{Z}$.®

(♣) Hallar $D(0)$.

Definición 5.4 Sean $a, b \in \mathbb{Z}$. Se define el conjunto de *divisores comunes de a y b* y se nota $D(a, b)$ a la intersección de los conjuntos $D(a)$ y $D(b)$.

Ejemplo 5.5

$$D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$$

$$D(15) = \{\pm1, \pm3, \pm5, \pm15\}$$

$$D(12, 15) = D(12) \cap D(15) = \{\pm1, \pm3\}.$$

Claramente la intersección es no vacía ya que $1 \in D(a)$, para todo $a \in \mathbb{Z}$ y, además tiene un elemento mayor que todos , un máximo dentro del conjunto.

Definición 5.5 Dados dos enteros a y b llamamos *máximo común divisor de a y b* y lo notamos (a, b) al último elemento (o máximo) del conjunto $D(a, b)$.

Ejemplo 5.6 Si retomamos el ejemplo 5.5 vemos que $(12, 15) = 3$.

¿Puede ser $(a, b) < 0$ para algún par a, b? ¿Puede ser $(a, b) = 0$? ®

Ejercicio 5.2 $a, b \in \mathbb{Z}$ tales que $b \mid a, b \neq 0$, entonces $(a, b) = |b|$

Ejercicio 5.3 (con "trampita") Demostrar que para todo par de enteros a, b se verifica:

$(a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b)$.

Algoritmo de Euclides

El procedimiento para encontrar el máximo común divisor es, entonces, buscar todos los divisores comunes, que podemos buscar sólo los positivos, y luego el más grande entre todos ellos. Esta es una tarea relativamente sencilla si trabajamos con números pequeños, pero a la hora de buscar $(425, 2985)$ el procedimiento se hace algo más que tedioso. Veremos cómo alivianar el camino.

Lema 5.1 *Si $a, b \in \mathbb{Z}$, $b \neq 0$ y r es el resto de dividir a por b, entonces $D(a, b) = D(b, r)$.*

Demostración:
Para probar $D(a, b) = D(b, r)$ debemos probar una igualdad de conjuntos y lo haremos por su definición. Usaremos fuertemente el algoritmo de la división entera, ya que $a = q \cdot b + r$ ó $r = a - q \cdot b$

1. $D(a,b) \subseteq D(b,r)$
   Sea $d \in D(a,b)$, entonces $d \mid a$ y $d \mid b$ por la Proposisión5.1-D_5, afirmamos que $d \mid a - q \cdot b$, es decir $d \mid r$ y en consecuencia $d \in D(b,r)$.
2. $D(a,b) \supseteq D(b,r)$
   Sea ahora $d \in D(b,r)$. Con un argumento similar y considerando que $a = q \cdot b + r$ concluimos que $d \in D(a,b)$.

Corolario 5.1 *En las condiciones del Lema 5.1* $(a,b) = (b,r)$.

Demostración: : A cargo del lector.®

Ejemplo 5.7 Comencemos el camino para calcular $(425, 2985)$.
El primer paso será conmutar los números y luego hacer las divisiones:

$$(2985, 425) = (425, 10) = (10, 5) = (5, 0) = 5.$$

Sabemos que el cociente y el resto son únicos, por lo tanto el camino que recorremos también lo es. Resulta confuso escribir simplemente en un renglón el proceso y para clarificar el proceso lo haremos en una tabla del siguiente modo:

	7	42	2
2985	425	10	5
10	5	0	

Veamos cómo hemos calculado: Comenzamos escribiendo el número más grande a la izquierda y a su derecha el más pequeño. Sobre él escribimos el cociente y debajo del más grande el resto que luego trasladamos hacia la derecha:

	7 (q_1)	42 (q_2)	2 (q_3)
2985 (a)	524 (b)	10 (r_1)	5 (r_2)
10 (r_1)	5 (r_2)	0 (r_3)	

El último resto no nulo $(r_2 = 5)$ es el máximo común divisor.

Este procedimiento nos brinda otra herramienta más. Sabemos que el máximo común divisor es finalmente un resto y que los restos los podemos escribir como combinación lineal del divisor y el dividendo. Iterando este procedimiento llegaremos a escribir el máximo común divisor $d = (a,b)$ como combinación lineal de a y b. (No necesariamente de forma única.)
Vayamos a por ello en nuestro ejemplo:

(1) $5 = \underline{425} - 42 \cdot 10$

(2) $10 = \underline{2985} - \underline{425} \cdot 7$

Reemplazando (2) en (1): $5 = \underline{425} - 42 \cdot (\underline{2985} - \underline{425} \, . \, 7) =$

$$= -42 \cdot \underline{2985} + (1 - 42 \cdot 7) \cdot \underline{425} =$$

$$= -42 \cdot \underline{2985} + 295 \cdot \underline{425}.$$

De este modo hemos escrito al máximo común divisor, 5, como combinación lineal de los enteros 2985 y 425.

Observación 5.3 Dijimos que esta combinación no es única, veamos un ejemplo:
$(4, 5) = 1$ y podemos escribir 1=(-1).4+5.1 o bien 1= 4.4-5.3 o bien 1=(-6).4+5.5.

Ejemplo 5.8 Busquemos $(2137, -623)$

	3	2	3	12	2	3
2137	623	268	87	7	3	1
268	87	7	3	1	0	

(1) $1 = 7 - 2 \cdot 3$

(2) $3 = 87 - 12 \cdot 7$

(3) $7 = 268 - 3 \cdot 87$

(4) $87 = \underline{623} - 2 \cdot 268$

(5) $268 = \underline{2137} - \underline{623} \cdot 3$

(6) Reemplazando (2) en (1) $1 = 7 - 2 \cdot (87 - 12 \cdot 7) = 25 \cdot 7 - 2 \cdot 87$

(7) Reemplazando (3) en (6) $1 = 25 \cdot (268 - 3 \cdot 87) - 2 \cdot 87 = 25 \cdot 268 - 77 \cdot 87$

(8) Reemplazando (4) en (7) $1 = 25 \cdot 268 - 77 \cdot (\underline{623} - 2 \cdot 268) = 179 \cdot 268 - 7 \cdot \underline{623}$

(9) Reemplazando (5) en (8) $1 = 179 \cdot (\underline{2137} - \underline{623} \cdot 3) - 77 \cdot \underline{623} = 179 \cdot \underline{2137} - 614 \cdot \underline{623}$

Finalmente:

$$1 = 179 \cdot \underline{2137} + 614 \cdot (\underline{-623})$$

Hemos definido un divisor en base al orden natural, daremos a continuación otra definición del máximo común divisor usando solamente la divisibilidad.

Definición 5.6 Sean $a, b \in \mathbb{Z}$ Si d es un entero positivo que cumple

(d_1) $d \mid a$, $d \mid b$,

(d_2) Si $d' \mid a$ y $d' \mid b$ entonces $d' \mid d$,

decimos que d es el *máximo común divisor* de a y b.

Proposición 5.2 *Las definiciones 5.5 y 5.6 son equivalentes*

Demostración:

(Definición 5.5 $\Rightarrow$ Definición 5.6)

Supongamos que d es el último elemento del conjunto $D(a) \cap D(b)$, entonces es necesariamente $d > 0$. No es necesario probar (d_1) ya que es un divisor común de a y b. Para probar (d_2) recordemos que $d = (a, b)$ puede escribirse como combinación lineal de a y b, sea $d = a \cdot x + b \cdot y$. Supongamos que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d = a \cdot x + b \cdot y$ y se verifica (d_2).

(Definición 5.6 $\Rightarrow$ Definición 5.5)

Supongamos ahora que d verifica (d_1) y (d_2). Por (d_1) resulta que $d \in D(a) \cap D(b) = D(a, b)$. debemos probar que se trata del mayor entre todos. Sea entonces un $d' \in D(a, b)$, por (d_2) resulta $d' \mid d$, por la Proposición5.1(D_8) resulta $d' \leq d$. $\square$

Con esta nueva definición se demuestran fácilmente las siguientes proiedades de (a, b):

Proposición 5.3 *Sean $a, b, c, m, k \in \mathbb{Z}$, se verifican las siguiente propiedades:*

1. $(a, b) = (b, a)$ *Propiedad conmutativa*
2. $(m \cdot a, m \cdot b) = m \cdot (a, b)$ *Propiedad distributiva*
3. $((a, b), c) = (a, (b, c))$ *Propiedad asociativa*
4. $(a, (a, b)) = (a, b)$ *Ley de absorción*
5. $(a, b) = (a, b + k \cdot a)$
6. *Si* $b = a \cdot q + r$, *entonces* $(a, r) = (a, b)$

Demostración: : A cargo del lector interesado.®

Definición 5.7 Dos enteros a, b se dicen *relativamente primos* o *coprimos* si verifican $(a, b) = 1$.

Proposición 5.4 Euclides *Sean* $a, b, c \in \mathbb{Z}$. *Si* $c \mid a \cdot b$ *y* $(a, c) = 1$, *entonces* $c \mid b$.

Demostración: :
Como $(a, c) = 1$ existen $x, y \in \mathbb{Z}$ tales que $1 = a \cdot x + c \cdot y$, y multiplicando ambos miembros por b obtenemos $b = a \cdot b \cdot x + c \cdot b \cdot y$. $a \cdot b = c \cdot k_1$ porque $c \mid a \cdot b$ y reemplazando en la igualdad anterior obtenemos $b = c \cdot k_1 \cdot x + c \cdot b \cdot y = c \cdot (k_1 \cdot x + b \cdot y) = c \cdot k$, de donde $c \mid b$.

Proposición 5.5 *Si* $a \mid n$ *y* $b \mid n$, *con* $(a, b) = 1$, *entonces* $a \cdot b \mid n$

Demostración: :
Como $a \mid n$ resulta $n = k \cdot a$, pero como $b \mid n$ podemos decir $b \mid ka$, con $(a, b) = 1$. En virtud de la Proposición5.4 resulta $b \mid k$, en consecuencia, $k = k_1 \cdot b, k_1 \in \mathbb{Z}$ y de aquí $n = k_1 \cdot b \cdot a$, es decir $a \cdot b \mid n$.

Observación 5.4 Afirmamos que todas las hipótesis deben ser usadas en una demostración, porque si fueran superfluas no estarían en el enunciado. ¿Dónde usamos $(a, b) = 1$? ¿Valdría esta proposición sin esa hipótesis? Si la respuesta es afirmativa, habrá que demostrarlo; si es negativa, dar un contraejemplo.

Proposición 5.6 *Si* a *y* b *son enteros no simultáneamente nulos, se vertifican:*

1. $(0, b) = \mid b \mid$.
2. $(a, b) = \mid a \mid \Leftrightarrow a \mid b$.
3. *Si* $c \in \mathbb{Z}$, $c > 0$, *entonces* $(a \cdot c, b \cdot c) = (a, b) \cdot c$.
4. *Si* $d = (a, b)$, *entonces* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demostración:

1. $(0, b) = \mid b \mid$.
   $|b| \mid 0$ y $|b| \mid b$ y si $d' \mid 0$ y $d' \mid b$, claramente $d' \mid |b|$.
2. $(a, b) = \mid a \mid \Leftrightarrow\ a \mid b$.
   Ya hemos probado que si $a \mid b$ resulta $(a, b) = |a|$, la recíproca es casi evidente porque si $|a| \mid b$, claramente $a \mid b$.
3. Si $\ c \in \mathbb{Z},\ \ c > 0,\ $ entonces $\ (a \cdot c, b \cdot c) = (a, b) \cdot c$.
   Sea $d = (a.b)$ y probemos que $d \cdot c = (a \cdot c, b \cdot c)$. Como $c > 0$ resulta $d \cdot c > 0$ $d \mid a$ entonces $d \cdot c \mid a \cdot c$ y $d \mid b$ entonces $d \cdot c \mid b \cdot c$, lo que prueba (d_1). Para probar (d_2) debemos ver que si $d' \mid a \cdot c$ y $d' \mid b \cdot c$ entonces $d' \mid d \cdot c$, lo que se verifica por Propiedad 5.1D$_5$. En efecto: como $d = (a, b)$ existen $x, y \in \mathbb{Z}$ tales que $d = a \cdot x + b \cdot y$, entonces $d \cdot c = c \cdot x \cdot c + b \cdot y \cdot c$.
4. Si $\ d = (a, b),\ $ entonces $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.
   Sea $d' \in D\left(\dfrac{a}{d}\right) \cap D\left(\dfrac{b}{d}\right)$. Entonces $\dfrac{a}{d} = k_1 \cdot d'$ y $\dfrac{b}{d} = k_2 \cdot d'$, es decir: $a = k_1 \cdot d' \cdot d$ y $b = k_2 \cdot d' \cdot d$, es decir, $d \cdot d' \in D(a, b)$, pero $d = (a, b)$ entonces $d \cdot d' \mid d$ y resulta $|d'| = 1$, de donde se concluye $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

Proposición 5.7 *Sean* $\ a,\ b,\ c, \in \mathbb{Z},\ \ a\ \ y\ \ b\ $ *no simultáneamente nulos, entonces existen enteros* x, y *tales que*

$$a \cdot x + b \cdot y = c \ \Leftrightarrow\ (a, b) \mid c.$$

Demostración:
Llamemos $d = (a, b)$.

$$a \cdot x + b \cdot y = c \ \Rightarrow\ (a, b) \mid c.$$

Claramente $d \mid a$, $d \mid b$ y por la Proposición 5.1 D$_5$ resulta $d \mid a \cdot x + b \cdot y$.

$$ax + by = c \ \Leftarrow\ (a, b) \mid c.$$

Sabemos, por el algoritmo de Euclides, que existen enteros x_1, y_1 tales que $d = a \cdot x_1 + b \cdot y_1$. Como $d \mid c$ podemos escribir $c = k \cdot d = k \cdot (a \cdot x_1 + b \cdot y_1) = a \cdot k \cdot x_1 + b \cdot k \cdot y_1 = a \cdot x + b \cdot y$.

Ejercicio 5.4 En las condiciones de la Proposición 5.7

1. Deducir que: $\ (a, b) = 1 \ \Leftrightarrow\ a \cdot x + b \cdot y = 1$.
2. Si $\ a \cdot x + b \cdot y = 1$, ¿Qué se puede decir de $\ (a, y),\ \ (x, b),\ $ y $\ (x, y)$?

5.4. Ecuaciones Diofánticas

(✠) Diofanto de Alejandría fue un antiguo matemático griego considerado "el padre del álgebra". De él ha quedado un epitafio redactado en forma de problema y conservado en la antología griega.

> *Caminante, esta es la tumba de Diofanto: los números pueden mostrar, ¡oh maravilla! la duración de su vida. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte, de vello se cubrieron sus mejillas. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años.*

Según este epitafio podemos calcular a qué edad falleció Diofanto (un ejercicio demasiado sencillo para nuestro lector) pero no en qué siglo vivió. Sólo podemos afirmar que vio la luz después del año 150 a.C. y su vida se apagó antes del 270 d.C. La hipótesis más apoyada es que vivió en los tiempos del emperador Juliano, hacia 365.
Su renombre se debe a *Arithmetica*, una colección de trece libros de los que sólo sobrevivieron seis a los ataques moros a la biblioteca de Alejandría, en el siglo VII. Diofanto demostró increíble creatividad y destreza en la solución de problemas, sin embargo sólo consideraba las respuestas racionales no negativas. Revisemos un problema: (libro1, problema 28): Calcular dos números tales que su suma y la suma de sus cuadrados sean números dados.
Supongamos que la suma de los dos números es 20 y la de sus cuadrados es 208.
Estaríamos pensando el el sistema:

$$\begin{cases} x + y = 20 \\ x^2 + y^2 = 208 \end{cases}$$

Diofanto propone una única ecuación:

$$(10 + x)^2 + (10 - x)^2 = 208,$$

de modo tal que le queda $200 + 2x^2 = 208$ y restando 200 a ambos miembros: $2x^2 = 8$, $x^2 = 4$, $x = 2$ (ya dijimos que sólo considera números no negativos) y la respuesta al problema es 12 y 8.

Aritmethica deja más que claro que Diofanto sabía resolver ecuaciones cuadráticas en todas sus formas, pero actualmente se lo conoce más por la resolución de ecuaciones racionales con variables que tienen un valor racional. Hoy en día las llamamos *ecuaciones diofánticas*. La más famosa entre todas ellas, con toda seguridad, es $x^n + y^n = z^n$ que llamamos *el último teorema de Fermat*. Justamente, en el margen del segundo libro de *Artimethica* escribió Pierre de Fermat su famosa frase "Es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados, y en general, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente. He encontrado una demostración realmente admirable, pero el margen del libro es muy pequeño para ponerla." 356 años (y mucha agua bajo el puente) más tarde Andrew Wiles encontró una demostración que, con seguridad, no cabe en el margen del libro ni en la imaginación de Pierre de Fermat.

Hoy en día una ecuación diofántica escrita en su forma más general es $a \cdot x + b \cdot y = c$, con $a, b, c \in \mathbb{Z}$. La proposición 5.7 y el algoritmo de Euclides nos dan una solución a este tipo de ecuaciones.

Ejemplo 5.9 Busquemos una solución para $216 \cdot x - 25 \cdot y = 32$

	8	1	1	1	3	2
216	25	16	9	7	2	1
16	9	7	2	1	0	

El último resto no nulo es el mcd, entonces $(216, 25) = 1$

(1) $1 = 7 - 3 \cdot 2$

(2) $2 = 9 - 7 \cdot 1$

(3) $7 = 16 - 9 \cdot 1$

(4) $9 = \underline{25} - 16 \cdot 1$

(5) $16 = \underline{216} + 8 \cdot (\underline{-25})$

(6) Reemplazando (2) en (1):$1 = 7 - 3 \cdot (9 - 7 \cdot 1) = -3 \cdot 9 + 4 \cdot 7$

(7) Reemplazando (3) en (6):$1 = -3 \cdot 9 + 4 \cdot (16 - 9 \cdot 1) = -7 \cdot 9 + 4 \cdot 16$

(8) Reemplazando (4) en (7):$1 = -7 \cdot (\underline{25} - 16 \cdot 1) + 4 \cdot 16 = 11 \cdot 16 - \underline{25} \cdot 7$

(9) Reemplazando (5) en (8):$1 = 11 \cdot (\underline{216} + 8 \cdot (\underline{-25})) - \underline{25} \cdot 7 = 11 \cdot \underline{216} + 95 \cdot (\underline{-25})$

Como $1 = 11 \cdot \underline{216} + 95 \cdot (\underline{-25})$, multiplicando ambos miembros por 32 obtenemos:

$32 \cdot 1 = 32 \cdot (11 \cdot \underline{216} + 95 \cdot (\underline{-25})) = 352 \cdot \underline{216} - 3040 \cdot \underline{25}$.

**Una vez descartado lo imposible, lo que queda,
por improbable que parezca, debe ser la verdad.**

La Propiedad 5.7 sirve también para encontrar solución a los problemas que yo llamo "estilo Sherlock". Veamos un ejemplo:

Ejemplo 5.10 Decir cuál es el mcd de dos enteros a y b si se sabe que no son relativamente primos, que (b,27)=1 y $9 \cdot a + 48 \cdot b = 18$.
Veamos todas las posibilidades:

> Sabemos que (a, b) es un divisor positivo de 18,
> entonces todos los candidatos son: $1, 2, 3, 6, 9, 18$.
>
> Como $(b, 27) = 1$ y $27 = 3^3$, resulta $(b, 3) = 1$,
> esto descarta a $3, 6, 9, 18$.
>
> Es decir, sólo quedan $1, 2$.
>
> Pero como $(a, b) \neq 1$, necesariamente $(a, b) = 2$.

5.5. Mínimo común múltiplo

Un matemático cuando encuentra un objeto que le gusta lo mira detenidamente, lo da vuelta y lo vuelve a mirar. Lo que se diría "lo mira por arriba y por abajo".
Hemos dicho que a divide a b toda vez que exista un $k \in \mathbb{Z}$ tal que $b = k \cdot a$.

Definición 5.8 Dados dos enteros a y b se dice que b es *múltiplo* de a y se escribe $b = \dot{a}$ si existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$.

Ejemplo 5.11 $6 = \dot{2}$, $6 = \dot{3}$

Definición 5.9 Dado $a \in \mathbb{Z}$ se define el conjunto de todos los *múltiplos de* a y se nota $M(a)$ al conjunto:

$$M(a) = \{b \in \mathbb{Z} : b = k \cdot a,\ k \in \mathbb{Z}\}.$$

Claramente $0, a \in M(a)$, para todo $a \in \mathbb{Z}$. Hasta aquí venimos bien, pero ahora $M(a)$ está muy lejos de ser finito. Es más, tiene tantos elementos como todo $\mathbb{Z}$.
Igual que antes podemos definir

$$M^+(a) = \{b \in \mathbb{Z} : b = \dot{a}, b > 0\},\ M^-(a) = \{b \in \mathbb{Z} : b = \dot{a}, b < 0\}.$$

Ahora vemos que

$$M(a) = M^-(a) \cup \{0\} \cup M^+(a).$$

$M^+(a) \subseteq \mathbb{N}$, y por el Principio de Buena Ordenación tiene un primer elemento, el mínimo, que en este caso se ve claramente que es a. (¿En serio es claro? El lector que no lo vea, que pregunte.)

Definición 5.10 Dados dos enteros a y b se define el *conjunto de divisores comunes de a y b* y se nota $M(a, b)$ a la intersección de $M(a)$ y $M(b)$

$M^+(a, b) = M^+(a) \cap M^+(b) \subseteq \mathbb{N}$ y tiene un elemento mínimo.

Definición 5.11 Dados dos enteros no nulos a, b el *mínimo común múltiplo de a y b* que notamos $m = [a, b]$ es el primer elemento del conjunto $M^+(a, b) = M^+(a) \cap M^+(b) \subseteq \mathbb{N}$. Si $a = 0$ o $b = 0$, definimos $[a, b] = 0$.

Ejemplo 5.12 $[2, 3] = 6$, $[15, 9] = 45$.

Proposición 5.8 *Sean $a, b, c \in \mathbb{Z}$, se verifican las siguientes propiedades:*

1. $[\,a, b\,] = [\,b, a\,]$ *Propiedad conmutativa*
2. $[\,c \cdot a, c \cdot b\,] = c \cdot [\,a, b\,]$ *Propiedad distributiva*
3. $[\,[\,a, b\,], c\,] = [\,a, [\,b, c\,]\,]$ *Propiedad asociativa*
4. $[\,a, [\,a, b\,]\,] = [\,a, b\,]$ *Ley de absorción*
5. $[\,a, b\,] = \mid b \mid \Leftrightarrow\ a \mid b$.

Demostración: A cargo del lector interesado. ®

Veremos ahora un teorema que demuestra la existencia del el mínimo común múltiplo de a y b y además nos permitirá calcularlo fácilmente para cualquier par de enteros.
Recordemos la Definición 5.6: $d = (a, b) > 0$ debe cumplir:

(d1) $d \mid a$, $d \mid b$,

(d2) Si $d' \mid a$ y $d' \mid b$ entonces $d' \mid d$

Escribamos esto es términos de múltiplos:

(m1) $m = \dot{a}$, $m = \dot{b}$, $(m \in M(a, b))$

(m2) Si $m' = \dot{a}$ y $m' = \dot{b}$ (si $m' \in M(a,b)$) entonces $m' = \dot{m}$ (o $m \mid m'$).

decimos que m es el *mínimo común múltiplo* de a y b.

Teorema 5.2 *Dados $a, b \in \mathbb{Z}$ existe $m \in M(a,b) = M(a) \cap M(n)$ tal que $m \mid m'$, para todo $m' \in M(a,b)$.*

Demostración: Supongamos que $a > 0, b > 0$ y sea $d = (a,b)$. Resulta entonces:

$$a = d \cdot k_a \qquad\qquad b = d \cdot k_b$$

De la definición de máximo común divisor resulta que $(k_a, k_b) = 1$.
En efecto: si $t \in D(k_a, k_b)$ entonces $t \cdot d \in D(a,b)$.
Sea $m = d \cdot k_a \cdot k_b$. Es claro que $m \in M(a,b)$.
Sea $m' \in M(b) \cap M(a)$.
$m' = a \cdot t_a = d \cdot k_a \cdot t_a$. Además $m' = b \cdot t_b = d \cdot k_b \cdot t_b \quad (\diamond)$,
es decir $d \cdot k_a \cdot t_a = d \cdot k_b \cdot t_b$, de donde $k_a \cdot t_a = k_b \cdot t_b$, es decir $k_a \mid k_b \cdot t_b$.
Como $(k_a, k_b) = 1$ necesariamente $k_a \mid t_b$ y resulta $t_b = k_a \cdot k$, reemplazando en $(\diamond)$ resulta

$$m' = b \cdot t_b = d \cdot k_b \cdot t_b = d \cdot k_b \cdot k_a \cdot k = (d \cdot k_b \cdot k_a) \cdot k = m \cdot k$$

Si a ó b son nulos, $[\,a, b\,] = 0$ y si alguno de ellos fuera negativo, consideramos el valor absoluto.

Observación 5.5 Revisemos la definición del m.
Escribimos $m = d \cdot k_a \cdot k_b$, donde $a = d \cdot k_a$ y $b = d \cdot k_b$, entonces $a \cdot b = (d \cdot k_a) \cdot (d \cdot k_b) = d \cdot m$. Considerando la posibilidad de que alguno sea negativo o aún nulo, podemos escribir:

$$m = \frac{|a \cdot b|}{(a,b)} \qquad\qquad [\,a, b\,] = \frac{|a \cdot b|}{(a,b)}.$$

Ejemplo 5.13 Calculemos el mínimo común múltiplo de 36 y -243:

	6	1	3
243	36	27	9
27	9	0	

Entonces $(-243, 36) = 9$ y $[-243, 36] = \dfrac{36{,}243}{9} = 972$.

5.6. Números primos

Dijo Paul Erdös: *Un niño puede hacer preguntas acerca de los primos que ningún adulto es capaz de responder.*

Veremos como punto central de esta sección el teorema fundamental de la aritmética. Este teorema establece la importancia de los números primos. Éstos son los "ladrillos básicos" con los que se "construyen" los enteros, en el sentido de que todo entero puede construirse como producto de números primos de una única manera. Conocer la factorización en primos de un número permite encontrar todos sus divisores, primos o compuestos y determinar con sencillez el mcm y el mcd. Implica también que las funciones aritméticas aditivas y multiplicativas están completamente determinadas por sus valores en las potencias de los números primos.
El teorema fue prácticamente demostrado por primera vez por Euclides (c. 300 aC), pero la primera prueba completa apareció en las *Disquisitiones Arithmeticae* de Carl Friedrich Gauss (1808). Aunque a primera vista el teorema parezca "obvio", no vale en sistemas numéricos más generales, entre estos muchos anillos de enteros algebraicos. Ernst Kummer fue el primero en notar esto en 1843, en su trabajo sobre el último teorema de Fermat. El reconocimiento de este fallo es uno de los primeros avances de la teoría de números algebraicos.

Veamos qué es un número primo. Si $a \in \mathbb{Z}$, a es divisible por $a, -a, 1, -1$, que se denominan los *divisores triviales* de a. Si a posee otro divisor, éste se llama un *divisor propio.*

Definición 5.12 Un entero $p \neq 0, 1, -1$ se dice *primo* si sus únicos divisores son los triviales. De modo equivalente podemos decir que un entero es primo si posee *exactamente* 4 divisores.

Observación 5.6 Para definir un entero primo pusimos como condición que sea distinto de 0,1,-1 y que no tenga divisores no triviales. Luego, al poner como condición que posea exactamente cuatro divisores no se ha mencionado esta condición. ¿Un olvido? Ⓡ

Definición 5.13 Si un entero $a \neq 0, 1, -1$ no es primo, se dice *compuesto.*

Por cientos de años los matemáticos han estudiado los números primos y hoy en día hay más problemas abiertos referentes a ellos que los que nunca ha

habido. Tal vez el mayor misterio de ellos es que siendo tan sencillo definirlos tienen un comportamiento tan irregular. Diría acerca de ellos Hans Magnus Einzenberger "lo diabólico de los números es lo sencillos que son".
Uno de los primeros interesados en estos números, quizá más conocido por haber determinado el radio de la tierra utilizando las sombras de Alejandría al mediodía, es Eratóstenes de Cirene (276-194 a.C). Eratóstenes ideó un "cedazo" para separar los preciosos primos de los números compuestos, igual que un granjero separa el grano de la paja.
Pongamos en funcionamiento esta *criba de Eratóstenes*:
Escribamos, para comenzar, los números en filas de 10, hasta el 50.:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

El 1 sabemos que es elemento unidad y que, en consecuencia, no es primo. El primero que queda es 2 que sólo admite divisores propios. Dejamos el 2 y sacamos todos sus múltiplos:

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	

Nuevamente el que sigue, el 3, sólo admite divisores propios. Dejamos el 3 y sacamos todos sus múltiplos (algunos de ellos, los múltiplos de 6, ya han sido borrados):

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	

El 5 y el 7 sólo admiten divisores propios. Los dejamos y sacamos todos sus múltiplos (algunos de ellos, igual que antes, ya han sido borrados):

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			

Hasta aquí hemos determinado los primeros 15 números primos. ¿Por qué afirmamos que hemos hecho un trabajo exahustivo cuando sólo llegamos al número 7? La explicación es sencilla: Cada vez que hallamos un número primo anulamos todos sus múltiplos. Con el 2 anulamos en primer lugar el $4 = 2^2$, con el 3, ya habíamos anulado los múltiplos de 2, entonces el primer anulado fue el $9 = 3^2$, al considerar el 5, el primer múltiplo anulado fue el 25 y en el caso del 7, el 49. Es decir, cada vez que encontramos un primo p, comenzamos a anular los múltiplos a partir de p^2. En consecuencia, nuestro trabajo de “limpieza de números” ha sido exahustivo hasta el 50. En verdad, si hubiéramos hecho una criba hasta el número 100, ya tendríamos todos los primos entre 1 y 113. ¿Es cierto?

Esta criba nos impulsa a hacer algunas observaciones:

1. 2 y 3 son primos consecutivos ¿Existirá algún otro par de primos consecutivos? ®
2. 3 y 5 son primos de la forma $p, p+2$. Estos pares de primos se llaman *primos gemelos*. ¿Hay más? ®
3. 3 y 5 y 7 son primos de la forma $p-2, p, p+2$. Estos pares de primos se llaman *primos trillizos*. ¿Hay más? ®
4. Los primos de “forma capicúa” se denominan *primos hermanos*. En la criba hasta el 50 aparecen 13 y 31 ¿Hay más? ®
5. 4 es un número compuesto entre dos primos. Entre 13 y 17 hay tres compuestos consecutivos. ¿Podemos hallar cualquier cantidad de números compuestos consecutivos? ®
6. Hagamos la siguiente observación: 1, el elemento unidad, quien genera aditivamente los números enteros satisface:

   $1 + 1 = 2$, el primer número primo.
   $2 + 1 = 3$, el segundo número primo.
   $2 \cdot 3 + 1 = 7$, que es un número primo.
   $2 \cdot 3 \cdot 5 + 1 = 31$, que es un número primo.

   y el proceso continúa, pero:

   $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

($\clubsuit_1$) Sabemos que el conjunto de los números primos es infinito, pero hasta el día de hoy sólo se conoce una cantidad finita. Sea P el producto de todos ellos. ¿Se puede saber cuál es la cifra de las unidades de P? ¿Y de las decenas?

($\clubsuit_2$) 1234567891, que tiene todos los dígitos no nulos, es un entero primo. ¿Habrá algún primo que tenga todos los dígitos (en cualquier orden) pero sin repetir ninguno?

($\clubsuit_3$) En una fiesta hay la misma cantidad de hombres que de mujeres y ambas son impares. Cada mujer (y cada hombre) lleva un número distinto: tenemos mujer 1, mujer 2, ... hombre 1, hombre 2, etc. Para formar una pareja de baile la suma de ambos números debe ser un número primo. Todos están bailando. ¿quién baila con “mujer 1”?

Observando la marcha de los primos no se puede inferir directamente que no tiene fin. (Tal vez, en algún momento la criba quede vacía de grano.) Fue Euclides quien trajo una respuesta efectiva a esta cuestión:

Teorema 5.3 (Teorema de Euclides). *Existen infinitos números primos.*

Demostración: Basta efectuar la demostración para primos positivos. Supongamos por el absurdo que hay sólo un número finito de primos positivos. Notamos a los primos $p_1, p_2, \dots, p_k$. Sea $n = p_1 \cdot p_2 \cdots p_k + 1$. Entonces, como $n > 1$, existe un primo positivo p tal que $p \mid n$. Por la hipótesis se tiene que $p = p_i$ para algún i , $1 \leq i \leq k$. Como $p_i \mid p_1 \cdot p_2 \cdots p_i \cdots p_k$, entonces $p_i \mid n - p_1 \cdot p_2 \cdots p_k = 1$ lo que implica que $p_i = 1$. Absurdo, pues p_i es un número primo. □

Teorema 5.4 (Lema de Euclides). *Si* p *es primo y* $p \mid b \cdot c$ *entonces* $p \mid b$ *ó* $p \mid c$ *.*

Demostración: Si $p \mid b$ no hay nada que probar. En caso contrario $(p, b) = 1$ y podemos encontrar número enteros x e y que satisfagan $1 = x \cdot p + y \cdot b$. Multiplicando ambos miembros de la igualdad por c obtenemos $c = x \cdot p \cdot c + y \cdot b \cdot c$. Como $p \mid p$ y $p \mid b \cdot c$, entonces $p \mid x \cdot p \cdot c + y \cdot b \cdot c$. □

Observación 5.7 Esta propiedad no vale si p no es primo. ®

Corolario 5.2 *Si* $p \mid b_1 \cdot b_2 \cdot \dots \cdot b_n$, *entonces* $p \mid b_i$ *para algún* $b_i \in \{b_1, b_2, \cdots b_n\}$.

Demostración: Ejercicio para el lector. (Se hace por inducción.) ®

Corolario 5.3 *Si* $p \mid p_1 \cdot p_2 \cdot \cdots \cdot p_n$*, con* p*,* p_i *números primos positivos, entonces* $p = p_i$ *para algún* $p_i \in \{p_1, p_2, \cdots p_n\}$*.*

Demostración: Ejercicio para el lector. (♠)

5.7. Teorema Fundamental de la Aritmética

Teorema 5.5 *Todo número entero* a *distinto de* $0, 1, -1$*, o bien es un número primo, o bien se puede escribir como* ± 1 *por un producto de números primos positivos. Esta representación de un entero como producto de primos es única, salvo el orden de los factores.*

Demostración: Basta demostrarlo para el caso $a > 1$.

Existencia

Para demostrar la existencia de la descomposición usaremos la segunda forma del principio de inducción (el principio fuerte de inducción). Caso base: Si $a = 2$, entonces a es primo y no hay nada que probar.
Paso inductivo: supongamos que todo entero menor que a admite descomposición en factores primos y probemos que a también.
Si a es primo, no hay nada que probar. Si a no es primo, entonces puede escribirse como producto de dos números enteros estrictamente menores que a. Es decir, existen b, c tales que $a = b \cdot c$ con $0 < b < a$ y $0 < c < a$. Por la hipótesis inductiva b y c admiten descomposición en factores primos y, por lo tanto, también a.

Unicidad

Supongamos que existen dos descomposiciones de a en factores primos,

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_n = q_1 \cdot q_2 \cdot \cdots \cdot q_m \tag{5.1}$$

Es claro que $p_1 \mid p_1 \cdot p_2 \cdot \cdots \cdot p_n$ y, en consecuencia $p_1 \mid q_1 \cdot q_2 \cdot \cdots \cdot q_m$. Por el corolario 2 del Lema de Euclides, resulta, que $p_1 \mid q_i$, para algún $q_i \in \{q_1, q_2, \cdots q_m\}$, y por la conmutatividad del producto podemos suponer que $p_1 \mid q_1$. Cancelando p_1 y q_1 en (5.1) resulta $p_2 \cdot p_3 \cdot \cdots \cdot p_n = q_2 \cdot q_3 \cdot \cdots \cdot q_m$. Como n y m son números (son cantidades finitas) el proceso para y la descomposición resulta única salvo el orden de los factores. □

Demostración: de Euclides-Gauss: Es suficiente probar el Teorema para el caso $a > 1$.

Existencia

Sea A el conjunto de todos los números enteros positivos que no verifican el Teorema, esto es, no son primos y no pueden representarse como producto de números primos. Queremos probar que $A = \emptyset$. Supongamos por el absurdo que $A \neq \emptyset$. Por el Principio de Buena Ordenación, A tiene primer elemento m. Sea p un divisor primo positivo de m. Se tiene $m = p \cdot k$, con $1 < k < m$, de donde resulta que $k \notin A$. Entonces el número k o bien es primo, o bien es producto de números primos. En ambos casos se obtiene una contradicción.

Unicidad

De nuevo usaremos el Principio de Buena Ordenación. Supongamos por el absurdo que existen enteros positivos que se pueden expresar como producto de números primos de dos formas diferentes. Sea m el menor de tales números. Entonces

$$m = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_t. \qquad (1)$$

De $p_1 \mid q_1 \cdot q_2 \cdots q_t$ resulta que $p_1 \mid q_i$ para algún i. Reordenando los factores si fuera necesario, podemos suponer que $p_1 \mid q_1$. De donde resulta $p_1 = q_1$. Cancelando este factor en (1) resulta

$$n = p_2 \cdots p_r = q_2 \cdots q_t.$$

El número n es un entero positivo menor que m y se expresa de dos formas diferentes como producto de números primos, lo cual contradice la definición de m. El absurdo provino de suponer la existencia de enteros positivos que se pueden expresar como producto de números primos de dos formas diferentes. $\square$

Observación 5.8 Hemos dado dos demostraciones diferentes del Teorema Fundamental de la Aritmética. ¿Cuál de ellas es "más fácil"? ¿Cuál es "más convincente"? ¿Cuál es "mejor"? ®

Observación 5.9 ¿Por qué no se puede demostrar existencia y unicidad simultáneamente?®

Agrupando los factores primos iguales entre sí en la representación $a = p_1 p_2 \cdots p_r$, podemos escribir

$$a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

donde ahora los primos $p_1, p_2, \ldots p_s$ son distintos dos a dos, $e_i \in \mathbb{N}$, $1 \leq i \leq s$. Por ejemplo, $420 = 10 \cdot 42 = (5 \cdot 2) \cdot (6 \cdot 7) = (5 \cdot 2) \cdot ((3 \cdot 2) \cdot 7) = 2^2 \cdot 3 \cdot 5 \cdot 7$

Ejemplo 5.14 Un número $a \neq 0, 1, -1$ es un cuadrado si y sólo si en su descomposición en factores primos, cada primo aparece un número par de veces.
Basta probarlo cuando $a > 1$. Supongamos que a es un cuadrado. Entonces $a = m^2$, $m \in \mathbb{Z}$, $m > 1$. Sea $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$, p_i primos distintos, $e_i > 0$. Entonces la factorización de a es $a = m^2 = (p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s})^2 = p_1^{2e_1} \cdot p_2^{2e_2} \cdot \ldots \cdot p_s^{2e_s}$, y cada primo aparece un número par de veces.

Recíprocamente, supongamos que en la descomposición de a en factores primos, cada primo figura un número par de veces. Entonces

$$a = p_1^{2e_1} \cdot p_2^{2e_2} \cdot \ldots \cdot p_s^{2e_s} = (p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s})^2 .$$

Luego a es un cuadrado.

Ejercicio 5.5 No existen números enteros a y b no nulos tales que $3a^2 = b^2$. Ⓡ

Ejercicio 5.6 Si a y b son enteros no negativos tales que $(a, b) = 1$ y $a \cdot b$ es un cuadrado, entonces a y b son cuadrados. Ⓡ

5.8. Divisores de un número entero

Notación 5.1 Sea $a \in \mathbb{Z}$, notamos $D(a)$ al *conjunto de divisores* de a $D^+(a)$ al *conjunto de divisores positivos* de a

Observación 5.10 Sea $a \in \mathbb{Z}$, como $D(a) = D(-a)$ consideramos el caso $a \geq 0$.

$D(0) = \mathbb{Z} \setminus \{0\}$

$D(1) = \{1, -1\}$

Si p es un número primo, $D(p) = \{1, -1, p, -p\}$

Teorema 5.6 *Sea* $a > 1$, *y sea* $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$, p_i *primos positivos distintos,* $e_i \in \mathbb{N}$, $1 \leq i \leq s$. *Sea* $b \in \mathbb{Z}$, $b > 0$, *entonces* $b \mid a$ *si y sólo si* $b = p_1^{t_1} \cdot \ldots \cdot p_2^{t_2} \cdots p_s^{t_s}$, *con* $0 \leq t_i \leq e_i \,; 1 \leq i \leq s$.

Demostración: Es claro que si $b = p_1^{t_1} \cdot \ldots \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s}$, $0 \leq t_i \leq e_i\,; 1 \leq i \leq s$, entonces $b \mid a$.

Veamos la recíproca. Los únicos divisores primos de a son los números $p_1, p_2, \ldots, p_s$, en virtud de la unicidad de la descomposición en factores primos. Luego, si $b \mid a$, cualquier divisor primo de b es uno de los números $p_1, p_2, \ldots, p_s$. Luego $b = p_1^{t_1} \cdot \ldots \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s}$, $t_i \geq 0$, $t_i \in \mathbb{Z}$.

Además, de $b \mid a$ se tiene $a = b \cdot c$ donde, por el mismo razonamiento, $c = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_s^{r_s}$, $r_i \geq 0$, $r_i \in \mathbb{Z}$. Entonces

$$a = b \cdot c = p_1^{t_1+r_1} \cdot p_2^{t_2+r_2} \cdot \ldots \cdot p_s^{t_s+r_s},$$

de donde resulta $e_i = t_i + r_i$, $1 \leq i \leq s$, por la unicidad de la factorización, y por lo tanto, $0 \leq t_i \leq e_i\,; 1 \leq i \leq s$. □

Hallados los divisores positivos de a, todos sus divisores se obtienen calculando los simétricos de los anteriores.

Ejemplo 5.15 Sea $a = 75 = 3^1 \cdot 5^2$. Los divisores positivos de a son: $3^0 \cdot 5^0 = 1$, $3^0 \cdot 5^1 = 5$, $3^0 \cdot 5^2 = 25$, $3^1 \cdot 5^0 = 3$, $3^1 \cdot 5^1 = 15$, $3^1 \cdot 5^2 = 75$., por lo tanto, $D(75) = \{\pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75\}$

Si $a > 1$, $a = p_1^{e_1} \cdot \ldots \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ resulta del teorema anterior que $D^+(a)$ tiene como cardinal $d^+(a) = (e_1 + 1) \cdot (e_2 + 1) \cdot \ldots \cdot (e_s + 1)$.

Ejemplo 5.16 Hallemos el menor natural a que posee exactamente 42 divisores. En este caso, a tiene 21 divisores positivos, esto es, $D^+(a) = 21 = 21 \cdot 1 = 3 \cdot 7 = (e_1+1) \cdot (e_2+1)$. Se tienen entonces dos posibilidades: $a = p^{20}$, p primo ó $a = p^2 \cdot q^6$; p, q primos distintos. Como busco el menor natural posible , considero los primos menores (2 y 3) obteniendo como posibles valores de a a los siguientes:
$a = 2^{20}$, $a = 3^2 \cdot 2^6$ ó $a = 2^2 \cdot 3^6$. Un fácil cálculo nos indica que $a = 3^2 \cdot 2^6 = 576$ es el natural buscado.

Ejemplo 5.17 Probar que $6 \mid n^3 - n$.
Como $6 = 2 \cdot 3$, basta demostrar que $2 \mid n^3 - n$ y $3 \mid n^3 - n$. (Recordar que si $a \mid n$ y $b \mid n$ y $(a, b) = 1$, entonces $a \cdot b \mid n$.)
$n^3 - n = n \cdot (n^2 - 1) = n \cdot (n+1) \cdot (n-1)$.
Si n es par, entonces $2 \mid n$, y en consecuencia, $2 \mid n^3 - n$. Si n es impar, entonces $2 \mid n - 1$ y entonces $2 | n^3 - n$.
Por otro lado, como $n-1$, n, $n+1$ son tres enteros consecutivos, entonces uno de ellos es múltiplo de 3. Luego $3 \mid n \cdot (n+1) \cdot (n-1) = n^3 - n$.
Luego $2 \cdot 3 = 6 \mid n^3 - n$.

Corolario 5.4 *Si* $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ *y* $b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_r^{t_r}$, $e_i \geq 0$, $t_i \geq 0$, *entonces*

$$(a,b) = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k},\ \textit{donde } k = \text{mín}(s,r)$$

y

$$[a,b] = p_1^{M_1} \cdot p_2^{M_2} \cdot \ldots \cdot p_l^{M_l},\ \textit{donde } l = \text{máx}(s,r)$$

donde m_i *y* M_i *representan, respectivamente, el menor y el mayor de los números* e_i *y* t_i.

Demostración: Es inmediata. □

Ejemplo. De $280 = 2^3 \cdot 5 \cdot 7$ y $693 = 3^2 \cdot 7 \cdot 11$ podemos escribir

$$\begin{aligned} 280 &= 2^3 \cdot 3^0 \cdot 5 \cdot 7 \cdot 11^0 \\ 693 &= 2^0 \cdot 3^2 \cdot 5^0 \cdot 7 \cdot 11, \text{ entonces} \end{aligned}$$

Luego

$$\begin{aligned} (280, 693) &= 2^0 \cdot 3^0 \cdot 5^0 \cdot 7 \cdot 11^0 = 7 \\ [280, 693] &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27720 \end{aligned}$$

Ejercicio 5.7 Los libros de una biblioteca no pasan de 10.000 y los podemos distribuir exactamente en lotes de 12 unidades, 27 unidades y también de 49 unidades. ¿Cuántos libros hay exactamente en la biblioteca? ®

Ejercicio 5.8 Los griegos llaman a un número *perfecto* si la suma de sus divisores estrictamente menores coincide con el número. Por ejemplo, los divisores de 6 son $1, 2, 3$ y 6. Además $1+2+3 = 6$, por lo tanto 6 es un número perfecto. Los divisores de 28 son $1, 2, 4, 7, 14$ y 28 y $1+2+4+7+14 = 28$, por lo tanto 28 también es perfecto. Cinco números perfectos conocidos son 6, 28, 496, 8128, 33550336. Comprobar que lo son. Es un problema abierto saber si existe algún número perfecto impar. Tampoco se sabe cuántos perfectos pares hay. ¿Será un número finito?

($\clubsuit_1$) Dijo San Agustín: El 6 es un número perfecto en sí mismo y no porque Dios haya creado todas las cosas en seis días. La verdad es más bien lo contrario. Dios creó a todas las cosas en seis días porque este número es perfecto.

($\clubsuit_2$) La suma de los inversos de todos los divisores positivos de un número perfecto da siempre 2.

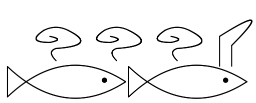
Por ejemplo, para el 6 los divisores positivos son $1, 2, 3, 6$.

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=\frac{6+3+2+1}{6}=2.$$

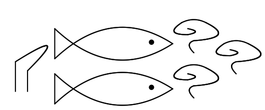
5.9. Sistemas de numeración en distintas bases

Hemos trabajado tanto y desde hace tanto tiempo con el sistema de numeración decimal que no nos cuestionamos su estructura, ni la posible existencia de otros sistemas. Analicemos, en primer lugar, qué es un sistema de numeración. Simplemente se trata de un conjunto de símbolos y reglas que nos permite escribir de forma única cada cantidad posible. Los sistemas de numeración pueden clasificarse en dos grandes grupos: posicionales y no-posicionales, es decir los sistemas en lo que no importa el orden en que se escriban los símbolos su valor no varía y los sistemas en que el valor depende tanto del símbolo, como de su posición en el número. Nos cuesta imaginar un sistema no posicional, un ejemplo es el sistema egipcio:

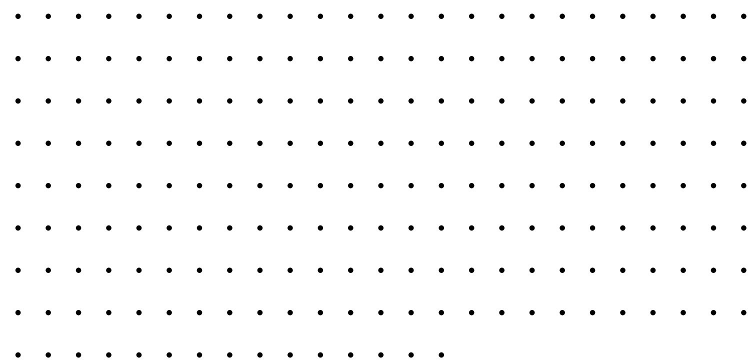
Como no importa la posición, el número 210.300 admite, entre otras, estas representaciones:



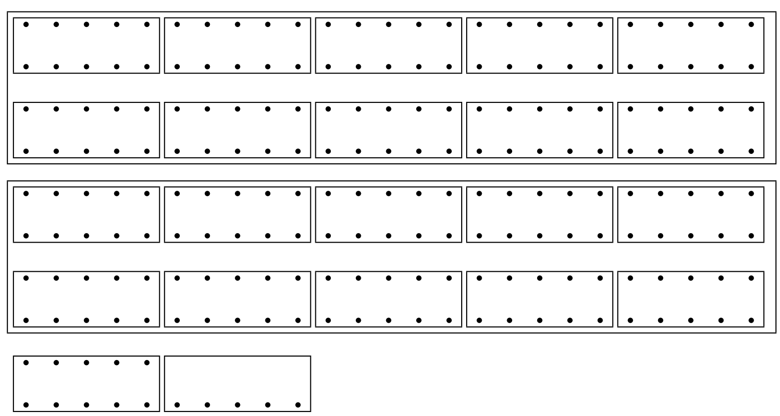
ó



Claramente un sistema no posicional no es práctico al momento de hacer cuentas.
La idea del sistema posicional parte del siguiente problema: supongamos que tenemos 215 árboles. Si tuviéramos sólo un símbolo que representara la unidad, sea $\cdot$, deberíamos escribir:



El procedimiento para simplificar esto es ir agrupando ¿de a cuántos? Lo más extendido, sobre todo a nivel lingüístico, supuestamente debido a la cantidad de dedos que suman nuestras manos, es agruparlos de a 10 y luego agrupar de a 10 los grupos de 10, y así sucesivamente.



Necesitamos, entonces símbolos para representar las cantidades "no hay", uno, dos, tres, cuatro, cinco, seis, siete, ocho y nueve. Sean: 0,1,2,3,4,5,6,7,8,9. Entonces: al hacer los grupos de "nivel uno" sobraron 5 puntitos, al hacer los grupos de "nivel dos" sobró un grupo de "nivel uno" y formamos 2 grupos de "nivel uno". Es decir: dos grupos de nivel 2, 1 de nivel 1 y 5 de nivel 0; nuestro número: 215, donde el valor de cada dígito varía según su posición en el número porque hace referencia a distinto nivel de agrupaciones.
Justifiquemos todo, a partir del algoritmo de división entera: Dado cualquier número entero (nuestro 215) existen el cociente y el resto de dividirlos por 10, unívocamente determinados (cociente: 21, resto 5). El cociente podemos volver a dividirlo, obteniendo un nuevos cociente y resto (cociente 2, resto 1). Como el cociente es menor que el divisor, se acabó el procedimiento.

Teorema 5.7 *Sea* $b \in \mathbb{N}, b > 1$. *Para todo entero* $a > 0$, *existen únicos* *enteros* $a_0, a_1, \ldots, a_n$*, con* $0 \leq a_i > b, i = 1, 2, \ldots, n$ *y* $a_n > 0$ *tales que*

$$a = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \ldots + a_2 \cdot b^2 + a_1 \cdot b + a_0$$

Escribiremos $a = a_n a_{n-1} \ldots a_2 a_1 a_{0(b)}$ *o sencillamente* $a = a_n a_{n-1} \ldots a_2 \cdot a_1 a_0$ *si no hay riesgo de confusión. Los coeficientes* a_i *se denominan las* cifras *y* b *la* base *de la representación.*

Demostración: Haremos esta demostración usando la segunda forma del principio de inducción, sobre a.
Caso base: Si $a = 1$, para todo $b \in \mathbb{N}$ resulta $a = b\ .\ 0 + 1$.
Paso inductivo: Supongamos que el teorema (tanto la existencia como la unicidad) se verifica para todo $a < k$. Sea $a = k$.
Por el algoritmo de la división $a = q \cdot b + r$, donde $q < a$ y $r < b$. Como $q < a$ resulta, por hipótesis inductiva, que $q = a_0 + a_1 \cdot b + \ldots + a_n \cdot b^n$, reemplazando en $a = q \cdot b + r$ resulta $a = (a_0 + a_1 b + \ldots + a_n b^n) \cdot b + r = r + a_0 \cdot b + a_1 \cdot b^2 + \ldots + a_n \cdot b^{n+1}$, que es el desarrollo buscado.
La unicidad es consecuencia directa de la unicidad en el desarrollo del algoritmo de la división y dejamos su demostración al lector interesado.

Observación 5.11 *En el teorema hemos trabajado con enteros no negativos. Si fuera el caso de* $a < 0$ *simplemente a su desarrollo le agregaríamos delante un signo -*

Ejemplo 5.18 Sea 215 en base 10 y queremos pasarlo a base 8.

$$\begin{array}{rrl} 215 & \multicolumn{1}{|l}{8} & \\ \cline{2-2} 7 & \multicolumn{1}{r|}{26} & 8 \\ \cline{3-3} & 2 & 3 \end{array}$$

Entonces $215 = 327_{(8)}$. En efecto: $7 + 2 \cdot 8 + 3 \cdot 8^2$=215

Ejemplo 5.19 Veamos ahora qué número es en base 10, el que en base 2 se representa 10010101011.

$1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 0 \cdot 2^9 + 1 \cdot 2^{10}$=
$1 + 2 + 0 + 8 + 0 + 32 + 0 + 128 + 0 + 0 + 1024$=1195.

Ejemplo 5.20 Un ejercicio combinado podría ser escribir en base 5 el número que en base 3 se escribe 2212.
Para resolver este tipo de ejercicio siempre hay que pasar por la base 10.

Entonces $2212_{(3)} = 2 + 1 \cdot 3 + 2 \cdot 3^2 + 2\ .\ 3^3$=2+3+18+54=77.

pasemos, entonces 77 a base 5.

$$\begin{array}{rrl} 77 & \multicolumn{1}{|l}{5} & \\ \cline{2-2} 2 & 15 & \multicolumn{1}{|l}{5} \\ \cline{3-3} & 0 & 3 \end{array}$$

$$77=302_{(5)}$$

Hemos verificado que $2212_{(3)} = 302_{(5)}$.

(♣) Hallar p, q, s sabiendo que las siguientes cifras están todas correctamente escritas: $222_{(p)},\ 3sp_{(q)},\ 21p_{(s)},\ 42q_{(6)}$.

Uno puede preguntarse si existe un sistema decimal, que es práctico, ¿para qué escribir en otras bases? Bien, una primera respuesta puede darse pensando en que al inicio de la computación se pretendía dar información a la máquina y la única herramienta con la que se contaba era "pasa corriente" y "no pasa corriente". De este modo se asoció "pasa corriente" a un 1 (la verdad de las proposiciones y también con el símbolo $\top$ o T, de 'true') y "no pasa corriente" al 0 (falsedad de las proposiciones, el símbolo $\perp$ o F, de 'false'). Así se extendió el uso del sistema binario (o base 2). Hoy en día, para representar colores sobre todo, se utiliza el sistema hexadecimal, es decir, la base 16. el inconveniente que presenta este sistema es que hay más dígitos que 10 y no tenemos tantos "dibujitos diferentes". El tema se soluciona fácilmente. En un primer momento se tomó (10), (11), (12), etc. como dígitos. El inconveniente es que se necesitan 4 caracteres para representar sólo uno y la ventaja es que no hay que explicar en qué orden se escriben. El gran descubrimiento fue pensar que el abecedario lo recitamos en un orden tan universal como los números y hoy en día, cuando se acaban los dígitos seguimos con las letras del abecedario en minúscula, comenzando por la primera. Entonces, los dígitos más comunes del hexadecimal son: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f$.

Observación 5.12 No lo usaremos en el curso, pero a modo de curiosidad, comentemos que es posible escribir todos los números racionales en otra base. Busquemos escribir en 1/2 en base 2.

$$1/2 = 0{,}5 = 2 \cdot 10^{-1}$$

Multipliquemos por la base. Tomamos la parte entera como dígito y seguimos multiplicando lo que queda después de la coma decimal. $0{,}5\ .\ 2 = 1{,}0$. La parte entera es 1 y no hay más parte decimal, entonces queda $0{,}1_{(2)}$. Si queremos pasar nuevamente a base 10, escribimos: $0{,}1_{(2)} = 0 + 1 \cdot 2^{-1} = \frac{1}{2}$.

Pasemos 0,3 a base 3: $0{,}3 \cdot 3 = 0{,}9$
$0{,}9 \cdot 3 = 2{,}7$
$0{,}7 \cdot 3 = 2, 1$
$0{,}1 \cdot 3 = 0{,}3...$
Hemos entrado en un ciclo, entonces $0{,}3_{(10)} = 0.\widehat{0220}_{(3)}$
Así como para representar un número entero mayor que 1 lo hacemos con potencias positivas de 2, para representar un número de la forma “cero coma” usamos potencias negativas de 2. Uniendo estas ideas podemos representar cualquier racional, escribiéndolo como la suma de un entero más su parte decimal. La representación de este número quedará en potencias enteras de 2.

Además de representar las cantidades debemos realizar operaciones básicas como suma, resta, multiplicación y división. Todas ellas se realizan igual que en la base 10, pero teniendo en cuenta las tablas de operaciones de los dígitos. Es decir, si pretendemos trabajar en base 8, $2_{(8)} + 2_{(8)}$ seguirá siendo $4_{(8)}$, pero $6_{(8)} + 6_{(8)}$, que en base 10 es 12, ahora será $14_{(8)}$. Trabajemos en base 4. Las tablas serán:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Es relativamente sencillo encontrar el resultado de $3 + 2$ en estas tablas. Primero elegimos la tabla que marca la operación + y luego buscamos dónde se cruzan la fila del 3 y la columna del 2 (o bien la fila del 2 y la columna del 3, porque es lo mismo). En cualquier caso encontramos 11. ¿Cómo hacemos si queremos restar? El procedimiento exactamente “al revés”. Supongamos que queremos hacer $10 - 3$, entonces en la fila del 3 buscamos dónde encontramos el número 10. Subimos por la columna y encontramos que es la columna correspondiente al número 1. Justamente, 10-3=1 porque 1+3=10.

Vamos a multiplicar 2.3: la fila del 2 se cruza con la columna del 3 y da el número: 12. Dividamos ahora $21 \div 3$: en la fila del 3 buscamos el número 21, subimos por su columna y encontramos al 3. En efecto, 3.3=21.

Hagamos algunas cuentas sencillas:

$$\begin{array}{rr} & 1231 \\ + & \\ & 33 \\ \hline & 2330 \end{array} \qquad \begin{array}{rr} & 1211 \\ \times & \\ & 23 \\ \hline & 10233 \\ & 3022 \\ \hline & 13321 \end{array}$$

$$\begin{array}{rr} & 3211 \\ - & \\ & 123 \\ \hline & 3022 \end{array} \qquad \begin{array}{l|l} 1232 & 23 \\ \cline{2-2} - & 30 \\ 122 & \\ \cline{1-1} 12 & \end{array}$$

Hemos dicho que si conocemos la representación de un número en una cierta base b y queremos conocer su representación en una base b', con $b \neq 10 \neq b'$, el método recomendado es "pasar" por nuestra conocida expresión decimal.

Ejemplo 5.21 Consideremos $34_{(5)}$ y busquemos su expresión en base 8.

$$34_{(5)} = 4 \cdot 5^0 + 3 \cdot 5^1 = 4 + 15 = 19$$

$$\begin{array}{r|l} 19 & 8 \\ \cline{2-2} 16 & 2 \\ 3 & \end{array}$$

$$19 = 2 \cdot 8 + 3 = 3 \cdot 8^0 + 2 \cdot 8^1.$$

Por lo tanto, $34_{(5)} = 23_{(8)}$.
Pero acabamos de aprender a hacer cuentas en otras bases. Hagamos el cálculo en forma directa: dividiremos por 8 en base 5.

Comencemos notando que $8 = 13_{(5)}$ y escribamos las tablas:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	21
4	0	4	13	21	31

$$\begin{array}{r|l} 34 & 13 \\ \cline{2-2} 31 & 2 \\ 3 & \end{array}$$

Y nuevamente, $34_{(5)} = 23_{(8)}$.

5.10. Ejercicios propuestos

5.10.1. Divisibilidad

Ejercicio 5.9 Si $a, b, c, s, t,$ indican números enteros arbitrarios, demostrar las siguientes proposiciones:

1. Si $a \mid b$ y $a \mid c$, entonces $a \mid (s \cdot b + t \cdot c)$ (si un número entero divide a otros dos, entonces divide a cualquier combinación lineal entera de ellos)
2. Si a y b son ambos positivos, y $a \mid b$, entonces $a \leq b$ ¿Se puede afirmar algo si no se sabe que a o b sean positivos?

Ejercicio 5.10 Decidir la veracidad de las siguientes proposiciones:

1. Si $d \cdot e \mid c$, entonces $d \mid c$
2. Si $c \mid d \cdot e$, entonces $c \mid d$

Ejercicio 5.11 Sea a y b dos números enteros pares, w y z dos números enteros impares. Determinar la paridad de:

1. $a + b$
2. $w + z$
3. $a + z$
4. $a \cdot b$
5. $w \cdot z$
6. $a \cdot z$

Ejercicio 5.12 Calcular el cociente y el resto de la división de a por b en los siguientes casos:
$a = 19, \;\; b = 36$; $a = -19, \;\; b = 36$; $a = 19, \;\; b = -36$; $a = -19, \;\; b = -36$.

Ejercicio 5.13 Sean $a, b \in \mathbb{Z}$. Probar que:

1. Si $b \mid a$ y $a \mid b$, entonces $a = b$ ó $a = -b$.
2. Si $a \mid b + c$ y $a \mid b$, entonces $a \mid c$.
   Deducir que si $a \mid a + c$, entonces $a \mid c$.

5.10.2. mcd (a, b)

Ejercicio 5.14 Hallar, utilizando el algoritmo de Euclides, el máximo común divisor de a y b y expresarlo como combinación lineal de ellos, siendo:

1. $a = 901, \quad b = 1219.$
2. $a = -120, \quad b = 176.$
3. $(\diamond)$ $a = -330, \quad b = 42.$
4. $(\diamond)$ $a = 13, \quad b = 101.$

Ejercicio 5.15 (©)(©) Propiedades del máximo común divisor: Sean $a, b, c, m, k \in \mathbb{Z}$, probar que se verifican las siguiente propiedades:

1. $(a, b) = (b, a)$ — Propiedad conmutativa
2. $(m \cdot a, m \cdot b) = m \cdot (a, b)$ — Propiedad distributiva
3. $((a, b), c) = (a, (b, c))$ — Propiedad asociativa
4. $(a, (a, b)) = (a, b)$ — Ley de absorción
5. $(a, b) = (a, b + k \cdot a)$
6. Si $b = a \cdot q + r$, entonces $(a, r) = (a, b)$

Ejercicio 5.16 ¿Existe $x \in \mathbb{Z}$ tal que $15 \mid 3x + 77$?

Ejercicio 5.17 Decir cuál es el máximo común divisor de los enteros a y b tales que:

1. $3a + 5b = 6$, a y b no son coprimos y $(a, 3) = 1$.
2. $(\diamond)$ $2a + 6b = 22$, b es impar y $(b, 11) = 1$.
3. $(\diamond)$ $7a + 5b = 8$ y a es impar.
4. $(\diamond)$ $9\,a + 7\,b = 15$, si a y b no son coprimos y $(b, 5) = 1$.

Ejercicio 5.18 (®) Probar que si a y b son enteros no simultáneamente nulos:

1. $(0, b) = \mid b \mid$.
2. $(a, b) = \mid a \mid \Leftrightarrow a \mid b$.
3. Si $c \in \mathbb{Z}$, $c > 0$, entonces $(a \cdot c, b \cdot c) = (a, b) \cdot c$.

Ejercicio 5.19 Demostrar que si $a \mid m$, $b \mid m$ y $(a, b) = 1$, entonces $a \cdot b \mid m$.

Ejercicio 5.20 (♣) Usted se encuentra en el centro de un enorme cuarto oscuro que posee puertas numeradas del 1 al 100, todas ellas inicialmente cerradas. Un mago que se encuentra a su lado comienza a pronunciar lentamente los números del 1 al 100, en orden ascendente. Cada vez que pronuncia el número k , las puertas que son múltiplos de k cambian mágicamente de estado (se cierran si estaban abiertas, y se abren si estaban cerradas). Cuando el mago haya terminado de pronunciar el número 100, ¿Cuáles puertas habrán quedado abiertas?

5.10.3. Teorema Fundamental de la aritmética

Ejercicio 5.21 Demostrar que para todo $a \in \mathbb{Z}$:

1. $a \cdot (a+1)$ es divisible por 2.
2. $(a^2-1) \cdot a$ es divisible por 3.
3. $(\diamond)$ $a \cdot (a^4-1)$ es múltiplo de 5.
4. $(\diamond)$ $a \cdot (a^6-1)$ es múltiplo de 7.
5. Si a es impar, entonces $a \cdot (a^4-1)$ es divisible por 120.
6. $(\diamond)$ $7a^3 - 7a$ es divisible por 42.

Ejercicio 5.22 $(\clubsuit)$ Probar que si p es un número primo, $p \geq 5$, entonces $24 \mid p^2 - 1$.

Ejercicio 5.23

1. $(\diamond)$ Hallar la descomposición en factores primos de los siguientes números enteros:
   $880, \ -9180, \ 1988^2, \ (12 \cdot 15)^2 \cdot 16 \cdot 30^3$.
2. Demostrar que no existen enteros no nulos a y b que satisfagan:

   a) $5a^2 = 7b^2$. *b*) $a^2 = 180$.

3. $(\diamond)$ Usar las técnicas del inciso 2. para demostrar que los siguientes números son irracionales:
   i) $\sqrt{10}$ ii) $\sqrt[3]{2}$ iii) $\sqrt[8]{8/11}$.

Ejercicio 5.24 Hallar el menor entero positivo x para el cual

1. $1260 \cdot x$ es un cubo perfecto.
2. $(\diamond)$ $31500 \cdot x$ es un cuadrado perfecto.
3. $(\diamond)$ $8640 \cdot x$ es una potencia quinta perfecta.

Ejercicio 5.25 Decir si son verdaderas o falsas las siguientes proposiciones sobre números enteros, justificando la respuesta:

1. Un número es divisible por 6 si y sólo si es divisible por 2 y por 3.
2. Si p es primo, $p \mid a$ y $p \mid a^2 + b^2$, entonces $p \mid b$.
3. Si p es primo, $p \mid a$ y $p \mid a^2 + 6b^2$, entonces $p \mid b$.

Ejercicio 5.26 (©) Sean a y b dos enteros relativamente primos. Demostrar que:

1. $(a^m, b^n) = 1$, para todo $m, n \in \mathbb{Z}$, $m \geq 0$, $n \geq 0$.
2. $(a + b, a \cdot b) = 1$.

Ejercicio 5.27 ($\diamond$) Dados los siguientes números enteros, indicar, justificando la respuesta, cuáles son números primos:
91, 97, 107, 143, 179, 121, 131, 141, 151, 161, 171.

Ejercicio 5.28 Número de divisores.

1. Determinar el número de divisores positivos de 36, 52, 39 y 72. Hallarlos.
2. Indicar la forma de todos los números naturales con exactamente 10 divisores positivos.
3. Hallar el menor natural con exactamente 10 divisores positivos.

Ejercicio 5.29 Hallar el mínimo común múltiplo $[a, b]$ de los siguientes pares de números enteros a y b:

1. $[6500, 175]$
2. $[126, 1470]$
3. $[500, 280]$

Ejercicio 5.30 Hallar todos los pares de enteros a y b positivos tales que:

1. $(a, b) = 98$ y $[a, b] = 1470$.
2. ($\diamond$) $(a, b) = 36$ y $[a, b] = 756$.

Ejercicio 5.31 ($\clubsuit$) Un agricultor quiso plantar un cierto número de árboles igualmente espaciados, colocados en varias filas paralelas.
El número de filas que hubo de emplear fue 7, ya que con un número menor de filas siempre sobraban tantos árboles como el número de filas disminuído en una unidad. Es decir, si utilizaba 3 filas le sobraban 2 árboles, con 4 filas le sobraban 3, y así siempre. ¿Cuál es el número de árboles, si se sabe que es el menor que cumple con las condiciones referidas?

Ejercicio 5.32 ($\clubsuit$) Veinte panes para veinte personas, los niños a medio pan, las mujeres a dos y los hombres a tres. ¿Cuántos hombres, niños y mujeres había?

5.10.4. Sistemas de numeración en distintas bases

Ejercicio 5.33 Escribir en las bases 2, 6 y 11 los números que en base 10 se escriben: 21, 512, 1128.

Ejercicio 5.34 Verificar que las expresiones $1447_{(8)}$, $1100100111_{(2)}$, $2(13)8_{(17)}$ representan al mismo número entero.

Ejercicio 5.35 Representar en base 2 y en base 7 el número entero $200112_{(3)}$.

Ejercicio 5.36 (®) Buscando un método para pasar de una cierta base b_1 a otra cierta base b_2 de modo directo.

1. Hallar la representación binaria de los dígitos: 1,2,3,4,5,6 y 7.
2. Hallar la representación binaria y octal de 121 y 242.
3. Deducir a partir de los incisos anteriores una forma sencilla de convertir directamente números binarios en octales y viceversa. ¿Puede generalizarse para cualquier par de bases b_1 y b_2?

Ejercicio 5.37 Expresar en sistema octal el mayor número de tres cifras que se puede escribir en base 6.

Ejercicio 5.38 (♣) Hallar n, m, p sabiendo que las siguientes cifras están todas correctamente escritas: $n23_{(m)}$, $p21_{(n)}$, $n3m_{(6)}$, $1211_{(p)}$.

Ejercicio 5.39 Operaciones en base b:

1. Efectuar las siguientes operaciones en el sistema binario:

   a) $101101_{(2)} + 10011_{(2)}$ *b*) $10111_{(2)} \cdot 110_{(2)}$

   c) $11101_{(2)} - 110_{(2)}$ *d*) $10100_{(2)} \div 111_{(2)}$

2. Efectuar las siguientes operaciones en el sistema octal:

   a) $3432_{(8)} + 24134_{(8)}$ *b*) $342_{(8)} \cdot 24_{(8)}$

   c) $4231_{(8)} - 243_{(8)}$ *d*) $414_{(8)} \div 23_{(8)}$

Ejercicio 5.40 Mostrar que $10_{(b)} \cdot 10_{(b)} = 100_{(b)}$.

Ejercicio 5.41 Hallar, si existe, una base b para la cual se verifique: $31_{(b)} \cdot 12_{(b)} = 402_{(b)}$.

Ejercicio 5.42 Determinar el valor de x para que $n = 342x_{(6)}$ sea divisible por $5_{(6)}$.

Ejercicio 5.43 Si a y b son dos dígitos diferentes del sistema octal que satisfacen $ab_{(8)} + ba_{(8)} = 132_{(8)}$, dar posibles valores para a y b, explicando el método de obtención.

Ejercicio 5.44 ($\clubsuit$) Juan compra un auto en $440_{(b)}$ unidades monetarias, paga con $1000_{(b)}$ unidades monetarias y recibe de vuelto $340_{(b)}$ unidades monetarias. Hallar la base b.

Ejercicio 5.45 ($\clubsuit$) Un almacenero tiene una balanza de platillos de 6 pesas distintas y puede pesar cualquier cantidad entera de 1 a 63 kilogramos, inclusive.

1. Indicar cuáles son las pesas.
2. Explicar cómo pesar $53\,kg$ y $27\,kg$.

Capítulo 6

Números complejos

Números complejos. Operaciones. El plano complejo. Módulo y conjugado. Propiedades. Producto y cociente en forma polar. Potenciación de exponente entero: Fórmula de De Moivre. Radicación. Propiedades.

6.1. Algo de historia

(✠) Los números complejos aparecen por primera vez en el libro *Ars Magna* de Gerolamo Cardano, en 1545, lo cual le valió una discusión con el "descubridor" de estos números, Niccolò Fontana mejor conocido como Tartaglia. Podemos decir que aparecieron muy temprano y fueron ignorados sistemáticamente por su carácter extraño y por ser imposibles de representar.
Tartaglia buscaba una fórmula general para resolver la ecuación $x^3 + px = q$ y la encontró bajo una forma bastante intimidante:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

Esta fórmula les resultó absolutamente aceptable en tanto que $\dfrac{p^3}{27} + \dfrac{q^2}{4} \geq 0.$

Pero si se quiere averiguar las soluciones de, por ejemplo, $x^3 - 15x = 4$ la fórmula queda:

$$\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} \qquad (A)$$

Recordemos que los griegos rechazaron siempre la existencia de números negativos, por la falta de un equivalente dentro de la geometría. Para ellos todo número representaba la longitud de un segmento o el área de una figura plana. Con el surgimiento del álgebra en la Edad Media, los números quedan libres de sus equivalentes geométricos, pero aún estaban sujetos a estructuras muy conservadoras.
Bombelli, a quien con todo derecho podemos llamar padre de los números complejos, ideó un método para resolver el dilema que teníamos planteado. Escribió: $\sqrt[3]{2+\sqrt{-121}} = 2 + c\sqrt{-1}$, para algún c y procedió a realizar el cálculo:

$\sqrt[3]{2+\sqrt{-121}} = 2 + c\sqrt{-1}$, entonces $2+\sqrt{-121} = (2+c\sqrt{-1})^3$

$$(2+c\sqrt{-1})^3 = 8 + 12c\sqrt{-1} - 6c^2 - c^3\sqrt{-1} = (8-6c^2) + (12c-c^3)\sqrt{-1}$$

Esta igualdad es válida para $c = 1$ y entonces obtenemos: $\sqrt[3]{2+\sqrt{-121}} = 2+\sqrt{-1}$.

Sustituyendo este valor en (A) queda $x = 2+\sqrt{-1}+2-\sqrt{-1}$ y ese "valor imaginado", $\sqrt{-1}$, desaparece y $x = 4$ es solución válida para la ecuación.

A pesar de los trabajos de Bombelli, los matemáticos de la época rechazaban estas resoluciones de ecuaciones cúbicas, considerándolos números *imposible* o *imaginarios*. Durante el siglo XVII fueron virtualmente olvidados. Matemáticos de la talla de Newton, Leibniz y Descartes nunca los comprendieron. Finalmente, en el año 1673 el matemático inglés J. Wallis, dio la primera representación geométrica que no coincide con la actual, ya que para ello debemos esperar a Wessel y Argand hasta 1806.
Con esta representación los números complejos pierden su misterio, pero por cuestiones históricas conservamos la nomenclatura de *imaginarios*.

Las sucesivas ampliaciones de los conjuntos numéricos son motivadas por la necesidad de encontrar soluciones a determinadas ecuaciones, o poder realizar ciertas operaciones. Por ejemplo, ampliamos el conjunto $\mathbb{N}$ de los números naturales al conjunto de los números enteros para poder resolver ecuaciones como $x + 2 = 1$, o lo que es lo mismo, para poder *restar*. En el conjunto $\mathbb{Z}$ no podemos resolver una ecuación como $3 \cdot x = 1$, es decir, no podemos *dividir*, y para ello lo ampliamos al conjunto $\mathbb{Q}$ de los números racionales. De la misma manera, no podemos resolver en $\mathbb{Q}$ una ecuación como $x^2 - 2 = 0$, mientras que sí es posible resolverla en $\mathbb{R}$. Pero no toda ecuación es resoluble en $\mathbb{R}$. Por ejemplo, $x^2 + 1 = 0$ no tiene solución real, ya que $x^2 \neq -1$, para todo número real x.

La ampliación del conjunto de los números reales al conjunto de los números complejos brinda un sistema numérico en el cual toda ecuación con coeficientes reales o complejos tiene solución. Este resultado se conoce con el nombre de Teorema Fundamental del Álgebra. Tanto para construir los enteros a partir de los naturales como los racionales a partir de los enteros, partimos del producto cartesiano y luego definimos una relación de equivalencia. Definiremos $\mathbb{C}$ también a partir del producto cartesiano $\mathbb{R} \times \mathbb{R}$.

6.2. Números complejos

Definición 6.1 Sea $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ el conjunto de todos los pares ordenados (a, b) de números reales sobre el cual definimos las operaciones siguientes:

1. **Suma:** $(a, b) + (c, d) = (a + c, b + d)$, para todo (a, b) y $(c, d) \in \mathbb{C}$,
2. **Producto:** $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$, para todo (a, b) y $(c, d) \in \mathbb{C}$,

El conjunto $\mathbb{C} = \{(a, b) : a \text{ y } b \in R\}$, junto con las operaciones de suma y producto definidas, recibe el nombre de conjunto de los *números complejos.*

Al definir un nuevo objeto matemático el primer paso es averiguar cuándo dos de ellos son iguales. Ese trabajo ya está hecho en este caso porque claramente $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$.
Nuestro objetivo es ampliar las operaciones que ya tenemos, entonces buscamos verificar que las operaciones recién definidas tengan las mismas propiedades que las que hemos usado hasta ahora.

Proposición 6.1 *Propiedades de las operaciones en $\mathbb{C}$:*

(S_1) $(z + u) + w = z + (u + w)$, *para todo z, u, $w \in \mathbb{C}$.(propiedad asociativa)*

(S_2) $z + w = w + z$, *para todo z, $w \in \mathbb{C}$. (propiedad conmutativa)*

(S_3) *Existe* $\mathbf{0} \in \mathbb{C}$, *tal que* $z + \mathbf{0} = \mathbf{0} + \mathbf{z} = \mathbf{z}$, *para todo $z \in \mathbb{C}$. (e.neutro)*

(S_4) *Para cada* $z \in \mathbb{C}$, *existe* $-z$ *tal que* $z + (-z) = (-z) + z = \mathbf{0}$.*(simétrico)*

(P_1) $(z \cdot u) \cdot w = z \cdot (u \cdot w)$, *para todo z, u, $w \in \mathbb{C}$. (propiedad asociativa)*

(P_2) $z \cdot w = w \cdot z$, *para todo z, $w \in \mathbb{C}$. (propiedad conmutativa)*

(P_3) *Existe* $\mathbf{1} \in \mathbb{C}$, *tal que* $z \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{z} = \mathbf{z}$, *para todo $z \in \mathbb{C}$. (unidad)*

(P$_4$) *Para cada* $z = (a, b) \in \mathbb{C}$, $z \neq 0$, *existe* z^{-1} *tal que* $z{\cdot}z^{-1} = z^{-1}{\cdot}z = \mathbf{1}$.
$z^{-1} = (\dfrac{a}{a^2+b^2}\ ,\ \dfrac{-b}{a^2+b^2})$ *(inverso)*

(D$_1$) $z \cdot (u+w) = z \cdot u + z \cdot w$, *para todo* z, u, $w \in \mathbb{C}$.*(propiedad distributiva)*

Demostración: Demostremos algunas de estas propiedades a modo de ejemplo:

(S$_1$) $(z + u) + w = z + (u + w)$, para todo z, u, $w \in \mathbb{C}$.

Sean $z = (z_x, z_y), u = (u_x, u_y), w = (w_x, w_y)$.

$(z+u)+w = ((z_x, z_y)+(u_x, u_y))+(w_x, w_y) = (z_x+u_x, z_y+u_y)+(w_x, w_y) =$

$= ((z_x + u_x) + w_x, (z_y + u_y) + w_y)).$(A)

$z+(u+w) = (z_x, z_y)+((u_x, u_y)+(w_x, w_y)) = (z_x, z_y)+(u_x+w_x, u_y+w_y) =$

$= (z_x + (u_x + w_x), z_y + (u_y + w_y)).$ (B)

Como $(z_x+u_x)+w_x = z_x+(u_x+w_x)$ y $(z_y+u_y)+w_y) = z_y+(u_y+w_y)$, por propiedad asociativa en $\mathbb{R}$ resulta (A)=(B) y $(z+u)+w = z+(u+w)$.

(S$_2$) La demostración es similar a la anterior y queda como ejercicio para el lector.®

(S$_3$) Sea $z = (z_x, z_y)$. Si $\mathbf{0} \in \mathbb{C}$, entonces $\mathbf{0} = (a, b)$ y $z + \mathbf{0} = \mathbf{z}$, resulta $(z_x, z_y) + (a, b) = (z_x, z_y)$, de donde $z_x + a = z_x$ y $z_y + b = z_y$, y se deduce $a = 0, b = 0$ y $\mathbf{0} = (0, 0)$

(S$_4$) Esta demostración también es constructiva y provoca placer en el lector que la realice con elegancia.®

Las demostraciones restantes son similares y también quedan a cargo del lector.® En el caso de (P$_4$), que también es una demostración de existencia constructiva, hemos dado la forma del inverso para simplificar la demostración. La forma está, sólo hay que probar que realmente es el inverso. Más adelante veremos cómo encontrarlo naturalmente.

Proposición 6.2 *El elemento neutro y la unidad son únicos en* $\mathbb{C}$. *para cada elemento* z *existe un uúnico simétrico y, si* $z \neq 0$, *un único inverso.*

Demostración:
Probemos que el inverso es único: Sea $z \in \mathbb{C}$, $z \neq 0$ y supongamos que existen z_1^{-1} y z_2^{-1} tales que $z\ .\ z_1^{-1} = z\ .\ z_2^{-1} = (1,0)$

$$z_1^{-1} = z_1^{-1}\ .\ 1 = z_1^{-1}(z\ .\ z_2^{-1}) = (z_1^{-1}\ .\ z)z_2^{-1} = 1\ .\ z_2^{-1} = z_2^{-1}.$$

Ya hemos construido un conjunto con dos operaciones que se comporaten igual que las operaciones entre números reales. Veamos que realmente hemos extendido a los números reales, es decir, que dentro de $\mathbb{C}$ hay una "copia" de $\mathbb{R}$. Para ello debemos encontrar lo que se llama una *función de inmersión*: una función inyectiva de $\mathbb{R}$ en $\mathbb{C}$. Sea $f : \mathbb{R} \to \mathbb{C}$ definida por: $f(a) = (a,0)$, para todo $a \in \mathbb{R}$.

Es fácil verificar que f es inyectiva y preserva las operaciones, es decir:

(F_1) $(a,0) = (b,0)$ entonces $a = b$ (f es inyectiva.)

(F_2) $f(a+b) = f(a) + f(b)$ (f preserva la suma.)

(F_3) $f(a \cdot b) = f(a) \cdot f(b)$ (f preserva el producto.)

Observación 6.1 Hemos encontrado que $\{(a,0),\ a \in \mathbb{R}\} \subseteq \mathbb{C}$ es una "copia" de $\mathbb{R}$ dentro de $\mathbb{C}$. Esto significa que los números de la forma $(a,0)$ se comportan, respecto de las operaciones de suma y multiplicación, (y respecto a muchas otras cosas más) como los números reales a.

Definición 6.2 Dado $z = (a,b) \in \mathbb{C}$, se define la *parte real de* z y se nota $Re(z)$ al número real a, y se define la *parte imaginaria de* z, que se nota $Im(z)$ al número real b.

Si $z = (a,0)$ se lo llama un *complejo real*.
Si $z = (0,b)$ se lo llama *imaginario puro*.

Veamos que nuestras expectativas se han cumplido: en $\mathbb{C}$ tiene solución la ecuación $x^2 + 1 = 0$.
Sea $x = (a,b) \in \mathbb{C}$ y hagamos las cuentas.

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

$$(a^2 - b^2, a \cdot b + b \cdot a) + (1,0) = (0,0)$$

$$(a^2 - b^2 + 1, a \cdot b + b \cdot a) = (0,0)$$

$$\begin{cases} a^2 - b^2 + 1 = 0 \\ 2a \cdot b = 0 \end{cases}$$

Las soluciones para la segunda ecuación son $a = 0$ o $b = 0$. Si tomamos $b = 0$ encontramos en la primera $a^2 = -1$ que no tiene solución, pero tomando $a = 0$ $b = \pm 1$ es solución. Resulta que los números complejos $(0, 1)$ y $(0, -1)$ son solución de la ecuación $x^2 + 1 = 0$ y esto motiva la siguiente:

Definición 6.3 Llamamos *unidad imaginaria* y notamos i al número complejo $(0, 1)$.

Por lo demostrado anteriormente sabemos que se verifica $i^2 = -1$.

Hasta aquí hemos construido un cuerpo (por las propiedades de las operaciones suma y producto) que contiene una copia de $\mathbb{R}$ y que además permite resolver ecuaciones cuadráticas de discriminante negativo. Nuestro objetivo está cumplido, pero hemos perdido el orden. Desde que comenzamos a construir los números a partir de los axiomas de Peano, dados dos números cualesquiera podíamos decidir cuál de ellos era más grande que el otro. Todos los conjuntos de números hasta ahora eran totalmente ordenados. Más aún, el orden era *compatible* con las operaciones por las *leyes de monotonía*:
Si $a \leq b$ entonces $a + c \leq b + c$. Si $a \leq b$, $c > 0$ entonces $a \cdot c \leq b \cdot c$
Veamos que esto no se verifica en $\mathbb{C}$:

Supongamos que $i > 0$, entonces $i \cdot i \geq i \cdot 0 = 0$, lo cual no es cierto porque $-1 \not\geq 0$.

Supongamos que $i < 0$, entonces $i \cdot i \geq i \cdot 0 = 0$, lo cual no es cierto porque $-1 \not\geq 0$.

Hemos definido i como un número tal que $i^2 = -1$. Veamos cómo se comportan las demás potencias de i.
Claramente la potencia natural se define recursivamente:

$$\begin{cases} i^0 = 1 \\ i^{n+1} = i \cdot i^n \end{cases}$$

y podemos calcular:

$$i^3 = i \cdot i^2 = -i, \qquad i^4 = i \cdot (-i) = 1.$$

Vemos que $i = 4 = i^0$, y como la definición es recursiva, hemos cerrado un lazo. Las potencias de i son $1, -1, i, -i$ y se repiten cíclicamente, por lo tanto para calcular i^n bastará calcular i^r, donde r es el resto de dividir n por 4.

Hagamos un cálculo que nos dará otra forma de verlo:

$$i^{215} = i^{4 \cdot 53 + 3} = i^{4 \cdot 54} \cdot i^3 = (i^4)^{53} \cdot i^3 = 1^{53} \cdot i^3 = i^3 = -i.$$

Al realizar este cálculo hemos utilizado las propiedades de potencia, es decir: potencia de otra potencia se multiplican los exponentes y producto de potencias de igual base se suman los exponentes. Justamente usaremos las propiedades de las potencias para calcular potencias negativas de i, ya que $i^{-n} = (i^n)^{-1}$ sólo debemos calcular i^{-1}.

Podemos pensar que i^{-1} es un número tal que multiplicado por i da 1 y como $i \cdot (-i) = -(i \cdot i) = -(-1) = 1$ concluímos que $i^{-1} = -i$.

Habíamos afirmado que $i^n = i^r$, donde $n = 4 \cdot k + r$, para todo $n \in \mathbb{N}$. Podemos afirmar ahora que $i^n = i^r$, donde $n = 4 \cdot k + r$, para todo $n \in \mathbb{Z}$. En efecto:

$i^{-1} = i^3$, donde $-1 = 4 \cdot (-1) + 3$.

$i^{-n} = i^{-(4 \cdot k + r)} = i^{4 \cdot (-k) - r} = i^{-r} = i^{4-r}$.

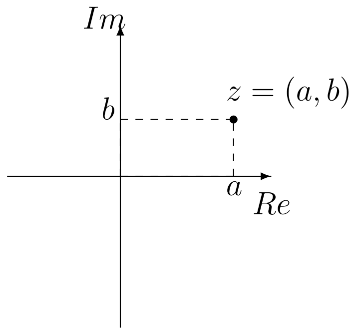
Veamos que $4 - r$ es el resto de dividir $-n$ por 4 si r lo es de dividir n por 4.

$-n = -(4 \cdot k + r) = 4 \cdot (-k) - r = 4 \cdot (-k - 1) + (4 - r)$, ya que $r < 4$.

6.2.1. Complejos en Forma Binómica

(✠) Dijimos en un comienzo que los números imaginarios no fueron aceptados fácilmente. Además de ser “extraños” operar con ellos no era nada sencillo hasta que Argand (1768-1822), un matemático autodidacta suizo los pensó en las coordenadas cartesianas. Sé que el lector interesado está ampliamente capacitado para comparar las fechas con las de 6.1 ¡200 años!

Si estamos considerando un par de números reales, lo podemos representar en el plano $\mathbb{R} \times \mathbb{R}$, la primera coordenada es la *parte real* y la segunda la *parte imaginaria* entonces el eje de las abscisas será el *eje real* y el de las ordenadas el *eje imaginario*



Podemos pensar entonces cada $z = (a, b)$ del siguiente modo:

$(a, b) = a(1, 0) + b(0, 1)$

$(1, 0)$ es el complejo real 1, $a \cdot 1 = a$

$(0, 1)$ es la unidad imaginaria i, y $b \cdot i = b \cdot i$

Resulta entonces: $z = (a, b) = a + b \cdot i$.

Acabamos de encontrar la forma binómica de escritura para un número complejo.

Ejemplo 6.1 El número complejo $z = (2, 3)$ se escribe en forma binómica $z = 2 + 3 \cdot i$, o simplemente $z = 2 + 3i$.
Si bien cuando escribimos en forma cartesiana no queda ningún lugar a dudas que $Re(z) = 2$, $Im(z) = 3$, debemos subrayar que este hecho se mantiene en la escritura en forma binómica. La i es simplemente un indicador de cuál es la parte imaginaria del número, pero tanto parte real como parte imaginaria son números reales.

Este hallazgo de Argand, exhala simplicidad y, justamente por eso, es de una gran belleza. Pensemos que estamos trabajando con números reales y sólo recordemos que $i^2 = -1$

Sean $z = (a, b) = a + bi$, $w = (c, d) = c + di$

Sumemos: $z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$.

Multipliquemos: $z \cdot w = (a + bi) \cdot (c + di) = a \cdot c + a \cdot di + bi \cdot c + di \cdot di = a \cdot c + (a \cdot d + b \cdot c)i + b \cdot d \cdot i^2 = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)i$.

El lector puede verificar fácilmente que coinciden con las "definiciones extrañas" que vimos en la forma cartesiana.Ⓡ
Busquemos la expresión para el inverso multiplicativo:

$$z^{-1} = \frac{1}{z} = \frac{1}{a + bi}$$

Usemos la imaginación como Bombelli y permitámonos pensar $i = \sqrt{-1}$. En la expresión anterior vemos que tenemos una raíz en el denominador y aprendimos que para sacarla debemos "multiplicar por el conjugado arriba y abajo". Hagamos eso mismo:

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

Gracias a esta nueva escritura, ya no hay que recordar nuevas reglas para operaciones, simplemente debemos recordar que $i^2 = -1$ y operar como si fueran números reales.

Ejercicio 6.1 Dejamos como ejercicio para el lector Ⓡ encontrar la expresión de z/w, donde $z = a + bi,\ w = c + di$

Ejemplo 6.2 Sean $z = 3 + 5i,\ w = 1 - i$. Hagamos algunas cuentas:

1. $z + w = (3 + 5i) + (1 - i) = (3 + 1) + (5 - 1)i = 4 + 4i$
2. $z - w = (3 + 5i) - (1 - i) = (3 - 1) + (5 + 1)i = 2 + 6i$
3. $z \cdot w = (3 + 5i) \cdot (1 - i) = (3 \cdot 1) + (3 \cdot (-1))i + (5 \cdot 1)i + (5 \cdot (-1))i^2 = 3 - 3i + 5i + 5 = 8 + 2i$
4. $z^2 = (3 + 2i)^2 = 3^2 + 2 \cdot 3 \cdot 2i + (2i)^2 = 9 + 12i - 4 = 5 + 12i$
5. $w^{-1} = \frac{1}{w} = \frac{1}{1-i} = \frac{1+i}{(1-i)(1+i)} = \frac{1+i}{2} = \frac{1}{2} + \frac{1}{2}i$
6. $\frac{z}{w} = \frac{3+5i}{1-i} = \frac{(3+5i)(1+i)}{(1-i)(1+i)} = \frac{(3-5)+(3+5)i}{2} = -\frac{2}{2} + \frac{8}{2}i = -1 + 4i$

El proceso de buscar el inverso multiplicativo de un número complejo nos lleva a la siguiente:

Definición 6.4 Dado el número complejo $z = (a, b)$ (ó $z = a + b\ i$), llamaremos *conjugado* de z al número complejo $\overline{z} = (a, -b)$ (ó $\overline{z} = a - b\ i$).

Ejemplo 6.3 Si consideramos los complejos z, w del ejemplo 6.2, resulta:

$$\bar{z} = 3 - 5i,\ \bar{w} = 1 + i.$$

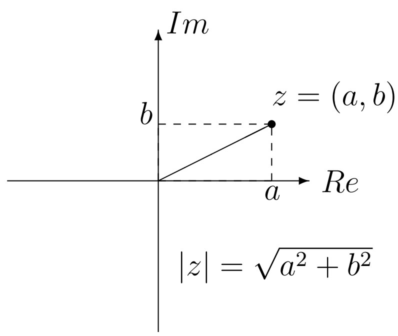
Proposición 6.3 *La conjugación de números complejos satisface las siguientes propiedades:*

1. $\overline{\overline{z}} = z$.
2. $z + \overline{z} = 2\ Re(z)$ *(O sea,* $z + \overline{z} = 2a$*).*

3. $z - \overline{z} = 2\, Im(z)\, i$ *(O sea,* $z - \overline{z} = 2b\, i$*).*
4. $z \cdot \overline{z} = a^2 + b^2$.
5. $z = \overline{z} \Leftrightarrow z$ *es real.*
6. $z = -\overline{z} \Leftrightarrow z$ *es imaginario puro.*
7. $\overline{z + z'} = \overline{z} + \overline{z'}$.
8. $\overline{z - z'} = \overline{z} - \overline{z'}$.
9. $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$.
10. $\overline{\left(\dfrac{z}{z'}\right)} = \dfrac{\overline{z}}{\overline{z'}}$, *si* $z' \neq 0$.

Demostración: : La demostración de estas propiedades se realiza en forma inmediata por medio del cálculo directo. Las dejamos a cargo del lector consciente.Ⓡ

Cuando calculamos el inverso multiplicativo de un número complejo $z = a + b\,i$, juntamente con el conjugado $\bar{z} = a - b\,i$, y también en la propiedad 4, apareció $a^2 + b^2$. Veamos el gráfico:



Al graficar z en los ejes cartesianos y dibujar las líneas paralelas a los ejes que pasan por $z = (a, b)$ queda determinado un triángulo rectángulo cuya hipotenusa es la distancia de z al 0 de $\mathbb{C}$.
Claramente la medida de la hipotenusa en cuestión es $\sqrt{a^2 + b^2}$.
Este razonamiento lleva a la siguiente:

Definición 6.5 Dado un número complejo $z = a + b\ i$, se llama *módulo* de z y se nota $|z|$, al número real, positivo o nulo, $\sqrt{a^2 + b^2}$.

Esta definición extiende la definición de valor absoluto (también distancia al origen, en $\mathbb{R}$), ya que si $z = (a, 0)$, entonces $\sqrt{a^2 + 0^2}$ es justamente el valor absoluto de a que notamos $|a|$. Este hecho justifica el uso de la misma notación para números complejos.

Ejemplo 6.4 Si consideramos nuevamente los complejos z, w del ejemplo 6.2, resulta:

$$|z| = \sqrt{3^2 + 5^2} = \sqrt{34}, \ \ |w| = \sqrt{1^2 + 1^2} = \sqrt{2}$$

Proposición 6.4 *Sea $z = a + b\,i$. Entonces:*

1. $|z| \geq 0$.
2. $|z| \geq a$ *y* $|z| \geq b$.
3. $|z|^2 = z \cdot \overline{z}$.
4. $|z| = |\overline{z}| = |-z|$.
5. $|z \cdot z'| = |z| \cdot |z'|$.
6. $\left|\dfrac{1}{z'}\right| = \dfrac{1}{|z'|}$, *si* $z' \neq 0$.
7. $\left|\dfrac{z}{z'}\right| = \dfrac{|z|}{|z'|}$, *si* $z' \neq 0$.
8. $|z + z'| \leq |z| + |z'|$.
9. $||z| - |z'|| \leq |z - z'|$.

Demostración: :
La propiedad 1 es evidente a partir de la definición, las propiedades 2,3 y 4 son fácilmente demostrables por álculo directo. Demostremos, entonces, 5, de donde se deducirán fácilmente 6 y 7 y luego seguimos con 8 y 9.

5. Para probar $|z \cdot z'| = |z| \cdot |z'|$ usemos un pequeño truco:

   A partir de la propiedad 3 escribimos:
   $$|z \cdot z'|^2 = (z \cdot z')(\overline{z \cdot z'}) = (z \cdot \overline{z})(z' \cdot \overline{z'}) = |z|^2 \cdot \left|\overline{z'}\right|^2,$$
   sacando raíz cuadrada a ambos miembros queda demostrado.
6. Si $z' \neq 0$, $1 = |z'.z'^{-1}| = |z'|.|z'^{-1}|$, de donde $\left|\dfrac{1}{z'}\right| = \dfrac{1}{|z'|}$,
7. $\left|\dfrac{z}{z'}\right| = \dfrac{|z|}{|z'|}$, si $z' \neq 0$, es consecuencia de los anteriores.

   (Ejercicio para el lector: escribirlo con cuidado)®.
8. $|z + z'| \leq |z| + |z'|$.
   Calculemos:
   $$\begin{aligned} |z + z'|^2 &= (z + z')\overline{(z + z')}, \text{ (por propiedad 3)} \\ &= (z + z')(\overline{z} + \overline{z'}) \text{ (conjugado de la suma)} \\ &= z\overline{z} + z\overline{z'} + z'\overline{z} + z'\overline{z'}, \text{ esto es,} \\ &= |z|^2 + z\overline{z'} + z'\overline{z} + |z'|^2 . \ (*) \end{aligned}$$

Si observamos el segundo y el tercer término de la última expresión se ve que son complejos conjugados. En efecto, $\overline{z\overline{z'}} = \overline{z}\overline{\overline{z'}} = \overline{z}z'$, y la suma de dos complejos conjugados es el duplo de la parte real. Luego

$$z\overline{z'} + \overline{z}z' = 2\ Re\ (z\overline{z}').$$

Sabemos que la parte real es menor o igual que el módulo, luego

$$\text{Re}\ (z\overline{z'}) \leq |z\overline{z'}|$$

$$2\ Re\ (z\overline{z'}) \leq 2(|z\overline{z'}|),$$

y como $\left|\overline{z'}\right| = |z'|$, entonces

$$2\ Re\ (z\overline{z'}) \leq 2|z||z'|. \qquad (1)$$

Reemplazando (1) en (*),

$$|z + z'|^2 = |z|^2 + 2\ Re\ (z\overline{z'}) + |z'|^2. \qquad (2)$$

Sumando (1) y (2),

$$|z + z'|^2 + 2\ Re\ (z\overline{z'}) \leq |z|^2 + 2\ Re\ (z\overline{z'}) + |z'|^2 + 2|z||z'|.$$

$$|z + z'|^2 \leq (|z| + |z'|)^2\,.$$

Como las bases son no negativas resulta

$$|z + z'| \leq |z| + |z'|.$$

que es lo que queríamos probar.

9. $||z| - |z'|| \leq |z - z'|$.
Para probar esta propiedad, pensemos que $|z| - |z'|$ es un número real a y recordemos que:

$$|a| \leq x \Leftrightarrow -x \leq a \leq x, \text{ si } x \geq 0.$$

De acuerdo a esto, probar que

$$|\underbrace{|z| - |z'|}_{a}| \leq \underbrace{|z - z'|}_{x}$$

es equivalente a probar que

$$-|z - z'| \leq |z| - |z'| \leq |z - z'|.$$

Escribamos z y z' de la siguiente forma: $z = z' + (z - z')$, $z' = z + (z' - z)$. Aplicando módulo se tiene: $|z| = |z' + (z - z')|$, pero por la propiedad anterior es $|z| \leq |z'| + |z - z'|$, de donde

$$|z| - |z'| \leq |z - z'|. \qquad (1)$$

De la misma manera,
$|z'| = |z + (z' - z)|$, luego $|z'| \leq |z| + |z' - z|$, de donde $|z'| - |z| \leq |z' - z|$.
Pero $|z' - z| = |z - z'|$
Luego

$$|z'| - |z| \leq |z - z'|$$

Multiplicando por (-1),

$$-(|z'| - |z|) \geq -|z - z'|,$$

luego

$$|z| - |z'| \geq -|z - z'|,$$

esto es,

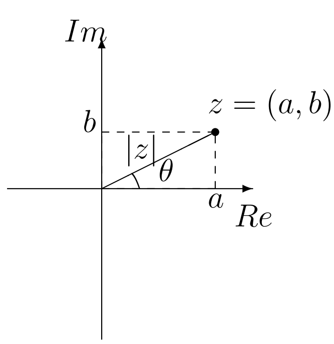
$$-|z - z'| \leq |z| - |z'|. \qquad (2)$$

Luego de (1) y (2) resulta

$$-|z - z'| \leq |z| - |z'| \leq |z - z'|$$

que es lo que queríamos probar.

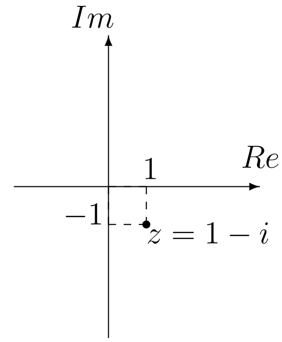
6.2.2. Complejos en Forma Polar



Hemos visto que un número complejo $z = a + bi$ se puede representar por un punto en el plano de coordenadas (a, b). Si unimos este punto con el origen de coordenadas obtenemos un segmento de longitud $|z|$ que determina un ángulo θ con el eje real positivo. Llamaremos *argumento* de z a la medida de θ, a menos de un múltiplo entero de 2π. Para determinar unívocamente el argumento de un número complejo definimos el *argumento principal* de z y lo notamos $Arg(z)$ al argumento que satisfaga $0 \leq Arg(z) < 2\pi$. Esta determinación no es única. Según la aplicación puede definirse $-\pi < Arg(z) \leq \pi$.

Ejemplo 6.5 Veamos un ejemplo. Sea $z = 1 - i$.
Calculemos el módulo:

$|z| = \sqrt{1^2 + 1^2} = \sqrt{2}$.



Calculemos el Argumento:

Debemos calcular la medida del ángulo que se forma entre el semieje real positivo y el segmento que une el punto z con el origen. Si llamamos O al origen, A al punto (1,0) y B al punto (0,-1), la medida de θ estará dada por el arco tangente de $\overline{OB}/\overline{OA}$.

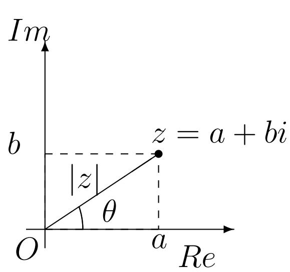
$$\theta = arctan\left(\frac{-1}{1}\right) = \frac{7}{4}\pi.$$

Podemos representar a z en forma polar de diversos modos, uno de ellos es: $z = |z|_\theta$, usando esta notación $z = \sqrt{2}_{\frac{7}{4}\pi}$.

6.2.3. Cambio de coordenadas

Comenzamos el capítulo hablando de números complejos como pares de números reales que representamos en el diagrama de Argand. En este caso tomamos como referencia a un par de ejes perpendiculares y al marcar los segmentos que determinan el punto z queda marcado un rectángulo. Llamamos a estas coordenadas *coordenadas rectangulares.*

Luego consideramos el origen de coordenadas como un polo y describimos la ubicación de z mediante su distancia al polo y el ángulo que forma con una semirrecta fija. Llamamos a estas coordenadas *coordenadas polares.*



Con z en coordenadas rectangulares:
$|a|$ es la longitud del segmento $\overline{OA}$,
$|b|$ es la longitud del segmento $\overline{OB}$.

En coordenadas polares:

$|z| = \sqrt{a^2 + b^2}$,
$arg(z) = arctan\frac{b}{a}$.

En consecuencia, las fórmulas para los cambios de coordenadas son las siguientes:

De $a+bi$ a $|z|_\theta$: $\begin{cases} |z| = \sqrt{a^2+b^2} \\ \theta = arctan\dfrac{b}{a} \end{cases}$ De $|z|_\theta$ a $a+bi$: $\begin{cases} a = |z| cos\,\theta \\ b = |z| sen\,\theta \end{cases}$

Ejercicio 6.2 Hagamos un ejemplo de cada cambio:

1. Sea $w = 1 - \sqrt{3}i$. Claramente está dado en coordenadas rectangulares. Busquemos su expresión en coordenadas polares.

   $|w| = \sqrt{1^2 + (\sqrt{3})^2} = 2$

   $\theta = arctan\dfrac{-\sqrt{3}}{1} = \dfrac{5}{3}\pi.$

   Claramente resulta: $w = 2_{\frac{5}{3}\pi}$.
2. Sea $z = 3_{\frac{5}{4}\pi}$. z está dado en coordenadas polares, debemos hacer el cambio a coordenadas rectangulares, entonces:

   $a = 3.cos\dfrac{5}{4}\pi = -\dfrac{3\sqrt{2}}{2}.$

   $b = 3.sen\dfrac{5}{4}\pi = -\dfrac{3\sqrt{2}}{2}.$

   Hemos obtenido, entonces: $z = -\dfrac{3\sqrt{2}}{2} - \dfrac{3\sqrt{2}}{2}i$

Observación 6.2 Algunas aclaraciones acerca de los argumentos:

1. El argumento de $z = (0,0)$ no está definido.
2. El argumento de z real positivo es $\theta = 0$.
3. El argumento de z real negativo es $\theta = \pi$.
4. El argumento de z imaginario puro, tal que $Im(z) > 0$, es $\theta = \dfrac{\pi}{2}$.
5. El argumento de z imaginario puro, tal que $Im(z) < 0$, es $\theta = 3\,\dfrac{\pi}{2}$.

Una vez que hemos calculado el módulo y el argumento del número complejo es bueno escribirlo de una forma que nos ayude en los cálculos. Veremos dos formas muy frecuentes:

6.2.4. Representación trigonométrica

Cuando pensamos en $z = a + bi$ y reemplazamos la a y la b por la fórmula que se usa en cambio de coordenadas obtenemos:

$$z = |z| cos\,\theta + |z| sen\,\theta\, i = |z|(cos\,\theta + i\, sen\,\theta).$$

Si resaltamos la primera letra queda $z = |z|(\mathbf{c}os\,\theta + \mathbf{i}\,\mathbf{s}en\,\theta)$, y por ello solemos escribir:

$$z = |z| cis\,\theta.$$

Esta notación es especialmente buena para comprobar propiedades usando trigonometría.

6.2.5. Representación exponencial

(✠) Leonhard Euler (1707-1873), fue el principal matemático del siglo XVIII y uno de los más grandes y prolíficos de todos los tiempos. Vivió en Rusia y Alemania la mayor parte de su vida y realizó importantes descubrimientos en áreas tan diversas como el cálculo o la teoría de grafos. También introdujo gran parte de la terminología moderna, como por ejemplo la noción de función. Se calcula que sus obras completas reunidas podran ocupar entre 60 y 80 volúmenes, pero aquí sólo nos ocuparemos de una fórmula, conocida como la *fórmula de Euler-Lindemann*.

$e^{i\pi} + 1 = 0$ es la fórmula de Euler-Lindemann, considerada por algunos la más bella del mundo, porque relaciona cinco entidades fundamentales $(e, i, \pi, 1, 0)$ en una forma sencilla y elegante y se encuentra en el celular, la meteorología, los aviones, barcos, sistemas anti robo y todo lo que use el sistema de posicionamiento global. Fue el primer paso (o uno de los primeros) para los sistemas GPS y GPRS que utilizan las coordenadas polares para determinar la posición del dispositivo y permitir su comunicación. La demostración escapa a este curso, pero voy a incluirla en la ilusión de que el lector interesado guarde estos apuntes y los retome cuando sea capaz de comprenderla. (Claramente no es la que escribo la única demostración posible, sino una de las, a mi entender, más elegantes y sencillas.)

Consideremos las series de Taylor:

$$(S_1)\ \ e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

$$(S_2)\ \ sen\, x = x - \frac{x^3}{3!} + \frac{x^5}{5!}\frac{x^7}{7!} \pm \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$

$$(S_3)\ \ cos\, x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \pm \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$$

Escribamos ahora (S_1) reemplazando x por zi:

$$(S_1)\ \ e^{z.i} = 1 + \frac{zi}{1!} + \frac{z^2.i^2}{2!} + \frac{z^3.i^3}{3!} + \cdots = 1 + \frac{z}{1!}i - \frac{z^2}{2!} - \frac{z^3}{3!}i + \frac{z^4}{4!} + \frac{z^5}{5!}i =$$

$$= \left(\sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{(2n+1)!} \right).i + \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n}}{(2n)!} = isen\, z + cos\, z$$

Sustituyendo z por π obtenemos la fórmula de Euler-Lindenbaumm, y la que usaremos en este curso sustituye z por θ:

$$e^{i\theta} = cos\, \theta + i\, sen\, \theta.$$

A partir de esta fórmula es fácil ver que $z = |z|(cos\, \theta + i\, sen\, \theta) = |z|e^{i\theta}$.

Para encontrarle algo de familiaridad a esta fórmula podemos pensar en las funciones hiperbólicas que ya hemos visto en Análisis I. Hemos definido el coseno hiperbólico y el seno hiperbólico como:

$$Ch(x) = \frac{e^x + e^{-x}}{2} \qquad Sh(x) = \frac{e^x - e^{-x}}{2}$$

y se ve fácilmente que $e^x = Ch(x) + Sh(x)$.

Claramente la representación polar no es práctica al momento de sumar o restar números complejos pero sí lo es para multiplicar, dividir y calcular potencias y veremos que es imprescindible al momento de calcular raíces.

Usemos la representación exponencial y calculemos un producto:

Sea $z = |z|e^{i\,\theta}$, $w = |w|e^{i\,\varphi}$.

$z \cdot w = |z|e^{i\,\theta} \cdot |w|e^{i\,\varphi} = |z| \cdot |w|e^{i\,\theta} \cdot e^{i\,\varphi} = |z| \cdot |w|e^{i\,(\theta+\varphi)}$.

Aquí se ve claramente:

$$|z \cdot w| = |z| \cdot |w|$$

y

$$arg(z \cdot w) = arg(z) + arg(w).$$

Es decir: para el producto se multiplican los módulos y se suman los argumentos.
Observemos que hemos usado arg y no Arg porque es probable que al efectuar la suma quedemos fuera del giro del argumento principal.

Veamos un ejemplo:

Ejemplo 6.6 $z = 4\, e^{i\,\frac{5\pi}{6}}$, $w = 2\, e^{i\,\frac{21\pi}{12}}$.

$z \cdot w = 4\, e^{i\,\frac{5\pi}{6}} \cdot 2\, e^{i\,\frac{21\pi}{12}} = 4 \cdot 2\, e^{i\,(\frac{5\pi}{6}+\frac{21\pi}{12})} = 8\, e^{i\,\frac{31\pi}{12}} = 8\, e^{i\,\frac{7\pi}{12}}$.

En este cálculo hemos restado una vuelta entera, es decir a $\dfrac{31\,\pi}{12}$ hemos restado $2\,\pi$ y resulta: $\dfrac{31\,\pi}{12} - \dfrac{24\,\pi}{12} = \dfrac{7\,\pi}{12}$.

Busquemos ahora la expresión del inverso de un número complejo no nulo.

Dado un número $z = |z|e^{i\,\theta}$ el inverso z^{-1} debe satisfacer $z \cdot z^{-1} = 1$.

Sea $z^{-1} = |z^{-1}|e^{i\,\varphi}$.

Escribamos $1 = 1\, e^{i\,0}$, entonces $z \cdot z^{-1} = 1$ resulta $|z|e^{i\,\theta} \cdot |z^{-1}|e^{i\,\varphi} = 1\, e^{i\,0}$, de donde

$|z| \cdot |z^{-1}|\, e^{i\,(\theta+\varphi)} = 1\, e^{i\,0}$, es decir $\begin{cases} |z| \cdot |z^{-1}| = 1 \\ \\ \theta + \varphi = 0 \end{cases}$

Concluimos, entonces:

$$|z^{-1}| = |z|^{-1}$$

y

$$arg(z^{-1}) = -arg(z).$$

Nuevamente cuidando dejar el argumento en la vuelta convenida para el argumento principal.

Ejemplo 6.7 $z = 4\, e^{i\,\frac{5\pi}{6}}$

$$z^{-1} = 4^{-1}\, e^{i\,(-\frac{5\pi}{6})} = \frac{1}{4}\, e^{i\,\frac{7\pi}{6}}.$$

En este cálculo hemos sumado una vuelta entera, es decir a $-\dfrac{5\,\pi}{6}$ hemos sumado $2\,\pi$ y resulta: $-\dfrac{5\,\pi}{6} + \dfrac{12\,\pi}{6} = \dfrac{7\,\pi}{6}$.

Si quisiéramos dividir dos números complejos, podemos pensarlo como multiplicar un número por el inverso del otro. Siguiendo los cálculos que hemos realizado:
$z = |z| e^{i\,\theta}$, $\;w = |w| e^{i\,\varphi}$.

$$\frac{z}{w} = z \cdot w^{-1} = |z| e^{i\,\theta} \cdot |w|^{-1} e^{-i\,\varphi} = \frac{|z|}{|w|}\, e^{i\,(\theta - \varphi)}.$$

Aquí se ve claramente $|\dfrac{z}{w}| = \dfrac{|z|}{|w|}$ y $arg\left(\dfrac{z}{w}\right) = arg(z) - arg(w)$, es decir: para el cociente se dividen los módulos y se restan los argumentos. Observemos que nuevamente hemos usado arg y no Arg porque es probable que al efectuar la suma quedemos fuera del giro del argumento principal. Veamos un ejemplo:

Ejemplo 6.8 $z = 4\, e^{i\,\frac{5\pi}{6}}$, $w = 2\, e^{i\,\frac{21\pi}{12}}$

$$\frac{z}{w} = \frac{4}{2}\, e^{i\,(\frac{5\pi}{6} - \frac{21\pi}{12})} = 2\, e^{i\,(-\frac{11\pi}{12})} = 2\, e^{i\,\frac{13\pi}{12}}.$$

6.3. Potencia y raíz de un número complejo

Hemos definido las potencias naturales de i en forma recursiva y luego las enteras utilizando $-n = (-1)\cdot n$. Hagamos lo mismo para un número complejo cualquiera.

$$\begin{cases} z^0 = 1 \\ z^{n+1} = z^n \cdot z, \text{ para todo } n \in \mathbb{N}. \end{cases}$$

Usemos la notación exponencial para encontrar una fórmula general:

Sea $z = |z|\, e^{i\theta}$, entonces $z^n = (|z|\, e^{i\theta})^n = |z|^n\, (e^{i\theta})^n = |z|^n\, e^{i(n\cdot\theta)}$.

Un buen ejercicio para el lector es demostrar inductivamente la validez de este resultado. (♠)

Ejemplo 6.9 Sea $z = \sqrt{3} - i$, calculemos z^5.

El primer paso es pasar z a notación polar, luego de haberlo ubicado en el plano:

$|z| = \sqrt{(\sqrt{3})^2 + 1^2} = \sqrt{4} = 2$

$arg(z) = arctan\left(\dfrac{-1}{\sqrt{3}}\right) = \dfrac{5\pi}{6}$,

pero se encuentra en el cuarto cuadrante, por lo tanto será: $\pi + \dfrac{5\pi}{6} = \dfrac{11\pi}{6}$

$z = 2\,e^{i\,\frac{11\pi}{6}}$, $z^5 = (2\,e^{i\,\frac{11\pi}{6}})^5 = 2^5\,e^{i\,5\cdot\frac{11\pi}{6}} = 32\,e^{i\,\frac{55\pi}{6}} = 32\,e^{i\,\frac{7\pi}{6}}$.

Analicemos este último paso de reducción al argumento principal. Tenemos que restar vueltas enteras, es decir, múltiplos enteros de $2\,\pi$. Estamos trabajando con $\dfrac{\pi}{6}$ y como buscamos el doble dividimos 55 por el doble del denominador (en este caso por 12).

$$\frac{55\,\pi}{6} = \frac{(4\cdot 12 + 7)\,\pi}{6} = \frac{(4\cdot 12)\pi}{6} + \frac{7\,\pi}{6} = 4\cdot 2\pi + \frac{7\,\pi}{6} = \frac{7\,\pi}{6}$$

Diremos que w es la raíz n-ésima de un número complejo z si $w^n = z$.

Veamos qué condiciones debe cumplir w para ser raíz n-ésima de z.

Sea $z = |z|\,e^{i\theta}$ y $w = |w|\,e^{i\varphi}$ como $z = w^n$ debe verificarse:

$z = |z|\,e^{i\theta} = |w|^n\,e^{i(n\cdot\varphi)}$.

Es decir:

$|z| = |w|^n$, de donde $|w| = \sqrt[n]{|w|}$ y

$e^{i\theta} = e^{i(n\cdot\varphi)}$, de donde $\theta = n\cdot\varphi + 2k\,\pi,\ k \in \mathbb{Z}$;

o del mismo modo $\theta + 2k\,\pi = n\cdot\varphi$ y resulta $\varphi = \dfrac{\theta + 2k\,\pi}{n},\ k \in \mathbb{Z}$.

Debido a lo que hemos escrito parecería que dado un número z existen infinitas raíces n-ésimas. Comprobemos que son sólo n.

Por el algoritmo de la división entera podemos escribir $k = q \cdot n + r$ y resulta

$$\varphi = \frac{\theta + 2(q \cdot n + r)\,\pi}{n} = \frac{\theta + 2r\,\pi}{n} + \frac{2q \cdot n\,\pi}{n} = \frac{\theta + 2r\,\pi}{n} + 2q\,\pi = \frac{\theta + 2r\,\pi}{n}.$$

Como el resto es estrictamente menor que el divisor escribimos:

$$w = \sqrt[n]{|z|}\, e^{i\dfrac{\theta + 2k\,\pi}{n}}, \;\; 0 \leq k \leq n-1.$$

Claramente las n raíces n-ésimas de un número complejo están en una circunferencia de radio $\sqrt[n]{|z|}$. Cuando $k = 0$ encontramos la primera raíz formando un ángulo de $\dfrac{\theta}{n}$ y a ese ángulo se le suma siempre $\dfrac{2\pi}{n}$.
Si unimos con una poligonal las n raíces obtenemos un polígono regular de n lados. La fórmula que acabamos de obtener se llama *fórmula de De Moivre.*

(✠) Abraham De Moivre (1667-1754) Conocido por la fórmula de De Moivre y por su trabajo en la distribución normal y probabilidad, fue elegido miembro de la Royal Society de Londres en 1697 y fue amigo de Isaac Newton y Edmund Halley. Refiriéndose a cálculos con complejos Newton dijo: *"Vayan con Abraham de Moivre a consultar ésto. Él sabe mucho más que yo de estas cosas"*. Lo cierto es que toda su vida fue pobre y era cliente regular del Slaughter's Coffee House, donde ganaba algo de dinero jugando al ajedrez. Murió en Londres, y lo curioso es que él predijo que moriría el da que murió. Observó que cada día dormía quince minutos más que la noche anterior y calculó que moriría aquel día en que durmiera veinticuatro horas. Dijo que sería el 27 de noviembre de 1754, y así ocurrió.

Veamos un ejemplo de aplicación de su fórmula:

Ejemplo 6.10 Sea $z = 729\, e^{i\dfrac{2\,\pi}{3}}$, calculemos $\sqrt[6]{z}$.

$$w = \sqrt[6]{|w|}\, e^{i\dfrac{\frac{2\,\pi}{3} + 2k\,\pi}{6}}, \;\; 0 \leq k \leq n-1.$$

Es decir: $w = \sqrt[6]{|w|}\, e^{i\dfrac{2\,\pi}{18} + \dfrac{2k\,\pi}{6}}, \;\; 0 \leq k \leq n-1.$

Finalmente: $\sqrt[6]{|729|}\, e^{i\dfrac{\pi}{9} + \dfrac{k\,\pi}{3}}, 0 \leq k \leq n-1$

$$w_0 = 3\,e^{i\,\dfrac{\pi}{9}+\dfrac{0\,\pi}{3}} = 3\,e^{i\,\dfrac{\pi}{9}}, \qquad \text{para } k=0,$$

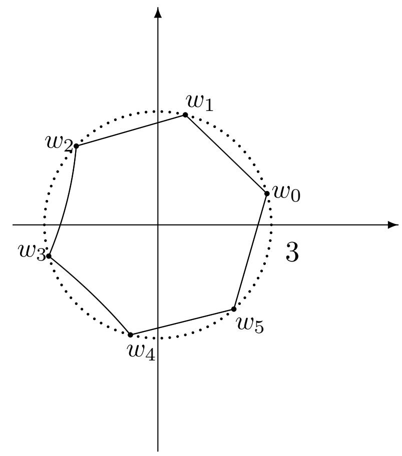
$$w_1 = 3\,e^{i\,\dfrac{\pi}{9}+\dfrac{1\,\pi}{3}} = 3\,e^{i\,\dfrac{4\,\pi}{9}}, \qquad \text{para } k=1,$$

$$w_2 = 3\,e^{i\,\dfrac{\pi}{9}+\dfrac{2\,\pi}{3}} = 3\,e^{i\,\dfrac{7\,\pi}{9}}, \qquad \text{para } k=2,$$

$$w_3 = 3\,e^{i\,\dfrac{\pi}{9}+\dfrac{3\,\pi}{3}} = 3\,e^{i\,\dfrac{10\,\pi}{9}}, \qquad \text{para } k=3,$$

$$w_4 = 3\,e^{i\,\dfrac{\pi}{9}+\dfrac{4\,\pi}{3}} = 3\,e^{i\,\dfrac{13\,\pi}{9}}, \qquad \text{para } k=4,$$

$$w_5 = 3\,e^{i\,\dfrac{\pi}{9}+\dfrac{5\,\pi}{3}} = 3\,e^{i\,\dfrac{16\,\pi}{9}}, \qquad \text{para } k=5.$$



6.3.1. Raíces de la unidad

Sea $z = 1$. Entonces $|z| = 1$ y $\theta = 0$, y por lo tanto, las n raíces n-ésimas están dadas por:

$$\sqrt[n]{1\;e^{i\,0}} = \sqrt[n]{1}\;e^{i\,\dfrac{2k\pi}{n}}, \text{ con } k = 0, 1, \cdots, n-1.$$

Una de las raíces n-ésimas de 1 es 1, que se obtiene para $k = 0$. Se puede observar que, si n es un número par, existen dos raíces reales que son $+1$ y -1, y si n es impar existe una sola raíz real, 1. Geométricamente, los afijos de las n raíces n-ésimas de la unidad, son los vértices de un polígono regular inscripto en una circunferencia de radio 1.

Ejemplo 6.11 Las cuatro raíces cuartas de 1 son:

$$\begin{aligned}
w_0 &= \sqrt[4]{1}\;e^{i\,0} = 1(1+0i) = 1,\\
w_1 &= \sqrt[4]{1}\;e^{i\,\frac{\pi}{2}} = 1(0+1i) = i,\\
w_2 &= \sqrt[4]{1}\;e^{i\,\pi} = 1(-1+0i) = -1,\\
w_3 &= \sqrt[4]{1}\;e^{i\,\frac{3\pi}{2}} = 1(0+(-1)i) = -i.
\end{aligned}$$

Observación 6.3 Dado un número $z \in \mathbb{C}$, todas sus raíces n-ésimas se obtienen multiplicando una cualquiera de ellas por cada una de las n raíces n-ésimas de la unidad.

6.4. Regiones en el plano complejo

Hemos definido ya el diagrama de Argand que nos permite representar los números complejos en el plano. Igual que representamos zonas en $\mathbb{R}^2$ mediante desigualdades, en este diagrama podemos representar regiones determinadas por números complejos, pero las desigualdades nunca se referirán al propio z sino a algún número real asociado a él como puede ser $Re(z), Im(z), Arg(z)$ o $|z|$.

Veamos algunos ejemplos:

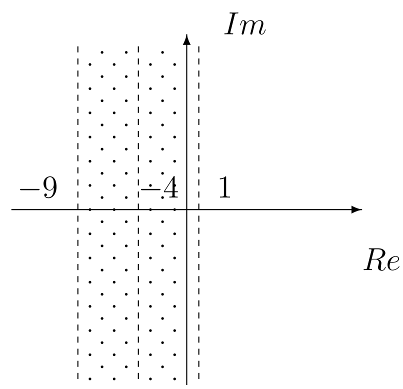
Ejemplo 6.12 Cuando la zona está dada en coordenadas rectangulares, una estrategia para traer los números complejos al campo conocido $\mathbb{R}^2$ es pensar a z como $z = x + i\,y$.

1. $|Re(z + (4 - 3\,i))| < 5$

   $|Re((x + i\,y) + (4 - 3\,i))| < 5$

   $|Re((x + 4) + i\,(y - 3))| < 5$

   $|x + 4| < 5.$



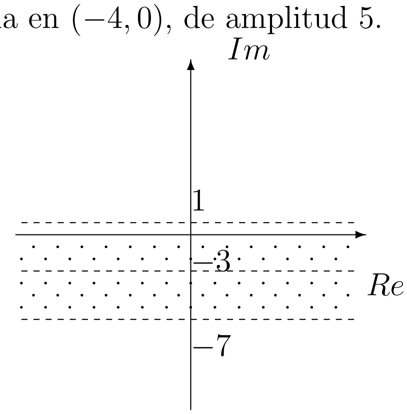
En la recta real $|x + 4| < 5$ es un intervalo centrado en -4, de amplitud 5. Como la y no tiene ningún tipo de condición en el plano $\mathbb{R}^2$ es una banda perpendicular al eje de las abscisas, centrada en $(-4, 0)$, de amplitud 5.

2. $|Im(z - (2 - 3\,i))| < 4$

   $|Im((x + i\,y) - (2 - 3\,i))| < 4$

   $|Im((x - 2) + i\,(y + 3))| < 4$

   $|y + 3| < 4.$



En la recta real $|y + 3| < 4$ es un intervalo centrado en -3, de amplitud 4. Como la x no tiene ningún tipo de condición en el plano $\mathbb{R}^2$ es una banda perpendicular al eje de las ordenadas, centrada en $(0,-3)$, de amplitud 4.

4. $Re(z-2\,i)\cdot Im(z-(2+2\,i))\leq 0$

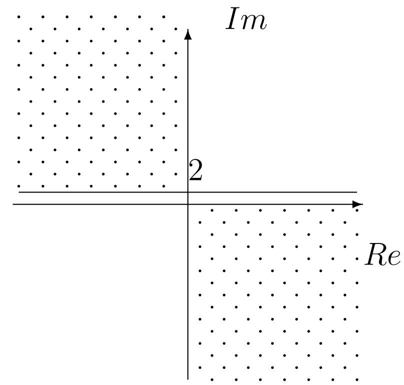
   $Re((x+i\,y)-2\,i)\cdot Im((x+i\,y)-(2+2\,i))\leq 0$

   $x\cdot(y-2)\leq 0$

   Las posibilidades son:

   $\begin{cases} x\geq 0\\ y-2\leq 0\end{cases}$ y $\begin{cases} x\leq 0\\ y-2\geq 0\end{cases}$.

   Es decir: $\begin{cases} x\geq 0\\ y\leq 2\end{cases}$ y $\begin{cases} x\leq 0\\ y\geq 2\end{cases}$.



5. $|z-2+i|\leq|z+3-i|$.

   En casos como éste, lo más recomendable es hacer las cuentas correspondientes y ver qué variables se anulan:

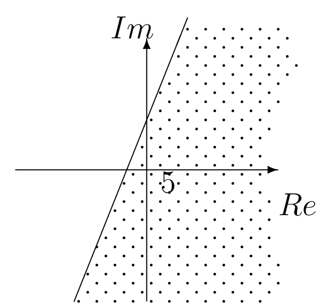
   $|(x-2)+(y+1)\,i|\leq|(x+3)+(y-1)\,i|$,

   $\sqrt{(x-2)^2+(y+1)^2}\leq\sqrt{(x+3)^2+(y-1)^2}$,

   $x^2-4\,x+4+y^2+2\,y+1\leq x^2+6\,x+9+y^2-2\,y+1$,

   $-4\,x+4+2\,y+1\leq 6\,x+9-2\,y+1$.

   Es decir $-10\,x+4\,y\leq 5$.



Ejemplo 6.13 Cuando la zona está dada en coordenadas polares, es bueno recordar que la noción de módulo en números complejos es simplemente distancia al origen, de mismo modo que el valor absoluto de números reales es distancia al origen y $|x-a|\leq r$ es un intervalo centrado en a de radio r, $|z-(a+b\,i)|\leq r$ es un círculo centrado en $a+b\,i$ de radio r.

Esta afirmación se puede verificar fácilmente recordando que la ecuación de una circunferencia de radio r centrada en (a,b) es $(x-a)^2+(y-b)^2=r^2$ y haciendo las cuentas:

$|z-(a+b\,i)| = r$ es equivalente a: $|(x+y\,i)-(a+b\,i)| = |(x-a)+(y-b)\,i| = r^2$

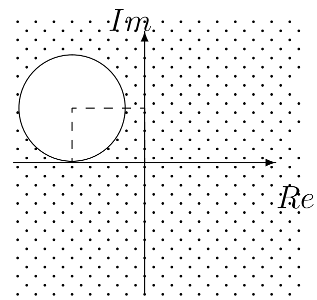
$\sqrt{(x-a)^2+(y-b)^2} = r$, que es lo mismo que: $(x-a)^2+(y-b)^2 = r^2$.

Hagamos algunos gráficos:

1. $|(z+4-3\,i| \geq 3$

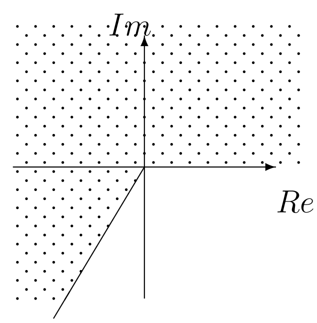
   $|(z-(-4+3\,i)| \geq 3$.

   Tenemos que graficar la circunferencia centrada en $(-4, 3)$, de radio 3. Esta circunferencia separa el plano en dos zonas, probamos con un punto a ver si satisface la inecuación y verificamos que se trata de la parte "de afuera".



2. $0 \leq Arg(z) < 4\pi/3$.

   Recordemos que cuando hablamos del argumento de z nos referimos al ángulo que forma el segmento que une el origen con el punto z con el eje real positivo.



3. $\pi < Arg(z\,i)^3 < 3\pi/2$

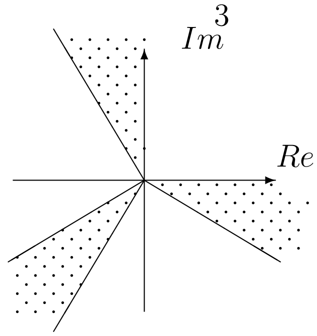
   En primer lugar distribuimos la potencia y luego recordamos que el argumento del producto es la suma de los argumentos. Resulta:

   $\pi < arg z^3 + arg(-i) < 3\pi/2$,

   $-\pi/2 < arg z^3 < 0$.

Ahora para "despejar" la z debemos sacar una raíz cúbica, lo que nos lleva a pensar en la fórmula de De Moivre y considerar:

$$\frac{-\pi/2 + 2k\pi}{3} < argz < \frac{0 + 2k\pi}{3}, \text{ con } k = 0, 1, 2$$



$k = 0 \;\; -\pi/6 < argz < 0$

$k = 1 \;\; \pi/6 < argz < 4\pi/6$

$k = 2 \;\; 3\pi/6 < argz < 8\pi/6$

Claramente el plano queda seccionado en tres zonas regulares.

Cualquiera de los ejemplos vistos puede aparecer en forma conjunta con otros similares. En dicho caso la zona será la intersección de todos ellos.

6.5. (♣) Sistema numérico imaginario.

[1] Cuando hablamos de números enteros y divisibilidad dimos como aplicación del algoritmo de la división la escritura de un número natural y posiblemente racional positivo, en distintas bases. Veamos una base de numeración denominada *quarter imaginary* que tiene a $2\,i$ como base.

Con esta base se puede representar absolutamente cualquier número complejo de forma única.

Veamos algunos ejemplos: Dado que $1 = 1 \cdot (2\,i)^0$ claramente vemos que $1_{(2\,i)} = 1$.

$103_{(2\,i)} = 3 + 0, (2\,i)^1 + 3(2\,i)^2 = 3 + 0 + 4 \cdot (-1) = 3 - 4 = -1.$

$10, 2_{(2\,i)} = 0 + 1, (2\,i)^1 + 2(2\,i)^{-1} = 2\,i + i^{-1} = 2\,i - i = i.$

$0, 2_{(2\,i)} = 0 + 2(2\,i)^{-1} = 0 - i = -i.$

Esta base fue propuesta por primera vez por Donald Knuth en 1955. Veamos cómo representar en general cualquier número $z = x + i\,y$.

[1]Esta última sección tiene objetivo informativo y tranquilizará al lector saber que no entra en parciales, coloquios ni finales ya sean regulares o libres. Donde sí puede entrar es a llenar un espacio de sana curiosidad.

El primer paso es representar a x (e $\frac{y}{2}$) en base 4, entonces obtenemos

$$x = A = \pm a_p a_{p-1} a_{p-2} \cdots a_0, a_{-1} a_{-2} \cdots a_{-q}$$

(igualmente $y = B = \pm b_t b_{t-1} b_{t-2} \cdots b_0, b_{-1} b_{-2} \cdots b_{-s}$).

La cantidad de dígitos a la izquierda de la coma debe ser siempre par, es decir p (y t) debe ser par y a la derecha de la coma impar o infinita, es decir si q (y s) es finito, debe ser impar. Si no se cumpliera en algunos de los casos (o en ambos) simplemente basta con agregar la cantidad de ceros necesaria.

El segundo paso es obtener una nueva representación A' (y B') que contenga sólo los dígitos 1,2,3 y 4, con el siguiente procedimiento:

Si $A > 0$ definimos ${a_k}' = \begin{cases} 1 + a_k & \text{si } k \text{ es par} \\ 4 - a_k & \text{si } k \text{ es impar} \end{cases}$, para $p \geq k \geq -q$.

$(B > 0)$

Si $A < 0$ definimos ${a_k}' = \begin{cases} 4 - a_k & \text{si } k \text{ es par} \\ 1 + a_k & \text{si } k \text{ es impar} \end{cases}$, para $p \geq k \geq -q + 1$

$(B < 0)$

y consideramos ${a_{p+1}}' = 1$ y ${a_{-q}}' = a_{-q}$.

El tercer y último paso consiste en "deshacerse" de los 4 que aparezcan reemplazándolos por 0 y bajando una unidad el dígito inmediato a la izquierda.

Una vez obtenidos A'' y B'' definimos $z = d_u d_{u-1} \cdots d_0, d_{-1} d_{-2} \cdots d_{-v}$ donde:

$u = 2 \cdot max(p + 2, r + 2),\ v = 2 \cdot max(q, s)$, y

$d_k = \begin{cases} a''_n & \text{k=2n} \\ b''_n & \text{k=2n+1} \end{cases}$, para $k = u, u - 1, \cdots, -v$.

Veamos un ejemplo:

Ejemplo 6.14 $z = 1 - i$

Primer paso: $x = 1,\ A = 1,00,\ \frac{y}{2} = \frac{-1}{2} = -0,5\ B = -0,20$

Segundo paso: $A' = 2,4$ y $B' = 14,2$

Tercer paso: $A'' = 1,'$ y $B'' = 0,2$

Armado final del número: $z = 1,2$

Verificación: $1,2_{(2\,i)} = 1 + 2 \cdot (2\,i)^{-1} = 1 - i$.

En este sistema también se pueden realizar operaciones, pero baste esta muestra para incentivar la curiosidad de leer el artículo completo: *An imaginary number system* Donald E. Knuth. Commun. ACM, Vol. 3 (April 1960), pp. 245-247.

(✠) Donald Ervin Knuth (10 de enero 1938, Milwaukee, Wisconsin) es uno de los más reconocidos expertos en ciencias de la computación por su análisis de algoritmos y compiladores. Es Profesor Emérito de la Universidad de Stanford, se lo conoce por ser el autor de la obra *The Art of Computer Programming*. Sentó las bases y dio nombre al análisis de algoritmos, y ha realizado numerosos aportes a varias ramas teóricas de la informática. Es el creador de TEX, con el que estoy escribiendo, del sistema de diseño de tipos METAFONT y del estilo de programación conocido como programación literaria.4

También es conocido por su humor: ofrece una recompensa de 2,56 dólares a quien encuentre errores conceptuales o tipográficos en sus libros (256 centavos son 1 dólar hexadecimal®). Numeró las distintas versiones de TEX de manera que se aproximaran al número π (3, 3.1, 3.14, etc.), al igual que los números de versión de MetaFont se van aproximando a $e = 2{,}718281828...$. Su cita más célebre, al enviarle sus comentarios a un colega autor de un algoritmo, es: *"Cuidado con los errores en el código anterior; sólo he demostrado que es correcto, no lo he probado"*.

6.6. Ejercicios propuestos

6.6.1. Representación cartesiana y binómica

Ejercicio 6.3 Representaciones en el plano complejo:

1. Escribir en la forma binómica los siguientes números complejos:
   $(3/4\,,\,-\frac{1}{2})\,,\qquad (\sqrt[3]{2}\,,\,-3)\,,\qquad (\diamond)\,(0,-1)\,,\qquad (\diamond)\,(0.3\,,\,0).$
2. Escribir en la forma de par ordenado los siguientes números complejos:
   $-8\,i\,,\qquad 2+3\,i\,,\qquad (\diamond)\ -i+3\,,\qquad (\diamond)\,\frac{1}{2}+\frac{\sqrt{3}}{2}\,i.$
3. Representar todos los números en el plano complejo.

Ejercicio 6.4 Calcular:

1. $(3-2\,i)-(4+i)+\dfrac{1}{3}\,i$,
2. $(\diamond)\,(4+5\,i)\cdot(3\,i-2)+(1-3\,i)$,
3. $(\diamond)\,3\,i\cdot(\dfrac{1}{4}+5\,i)-(1+2\,i)\cdot(-3+2\,i)$.

Ejercicio 6.5 Calcular:

1. $i^{\,38}-i^{\,5}+3\,i^{\,9}-i^{\,-3}+1$.
2. $(\diamond)\,i^{\,16}-3\,i^{\,-7}+i^{\,2}\,(1-i^{\,8})-(-i)^{\,24}$.

Ejercicio 6.6 Hallar la parte real e imaginaria, módulos y conjugados de :

$$4\,,\quad 3\,i\,,\quad \frac{1}{2\,i}\,,\quad \frac{1}{1+i}\,,\quad \frac{3-i}{1+i}\,,\quad \frac{1}{1+2\,i}+\frac{1}{-1+i}\,,\quad -\frac{1}{2}+\frac{\sqrt{3}}{2}\,i\,,\quad \frac{2}{1-\sqrt{2}\,i}.$$

Ejercicio 6.7 Dado $z\in\mathbb{C}$, cualquiera, calcular:

1. $z+\overline{z}$ ¿Cuándo $z=\overline{z}$?
2. $z-\overline{z}$ ¿Cuándo $-z=\overline{z}$?
3. $z\cdot\overline{z}$ ¿Cuándo $\dfrac{z}{\overline{z}}=\dfrac{\overline{z}}{z}$?

Ejercicio 6.8 $(\diamond)$ Ecuaciones con números complejos:

1. Hallar todos los números complejos z, tales que
   a) $z^2=i$
   b) $-z+i=-i+3$
   c) $(-1+i)\cdot z-(1-i)=2+3\,i$
2. Hallar los números complejos z, w tales que $z+w=6$ y $z-w=2\,i$.

Ejercicio 6.9 (®) Probar que:

1. $|z|=1 \;\Leftrightarrow\; z^{-1}=\overline{z}$.
2. $z+\dfrac{1}{z}\in\mathbb{R}\;\Leftrightarrow Im\,z=0$ ó $|z|=1$.
3. Si $z+w\in\mathbb{R}$ y $z\cdot w\in\mathbb{R}$ entonces $z,w\in\mathbb{R}$ ó $z=\overline{w}$.

Ejercicio 6.10 (♣) Hemos visto sistemas de numeración en distintas bases, todas ellas bases enteras. Existen, además, otras bases de sistemas de numeración en las que se puede representar números complejos y números negativos sin utilizar ni la i ni el signo menos. una de ellas es la presentada por Donald Knuth en *An Imaginary Number System* en 1955, usando $b = 2\,i$. Demostrar que $1_{10} = 1_{2\,i}$, $-1_{10} = 103_{2\,i}$, $i_{10} = 10{,}2_{2\,i}$, $-i_{10} = 0{,}2_{2\,i}$.

6.6.2. Representación polar

Ejercicio 6.11 Hallar la forma binómica de:

1. $z = 3_{\frac{\pi}{4}}$ 2. $z = e^{i\,\frac{\pi}{3}}$ 3. $z = \sqrt{3}_{-\frac{\pi}{2}}$ 4. $z = \dfrac{1}{2}\, e^{i\,\frac{\pi}{6}}$

Ejercicio 6.12 Hallar la forma polar y exponencial de:

1. $-1 + i$ 2. -17 3. $-i$

4. $i^{15} - 1$ 5. $\operatorname{sen}\dfrac{\pi}{6} + i\operatorname{sen}\dfrac{\pi}{3}$ 6. $\dfrac{1}{2} - i\operatorname{sen}\dfrac{\pi}{3}$

Ejercicio 6.13 Calcular utilizando forma polar o exponencial.

1. $(1 + \sqrt{3}\,i)(-3\,i)$ 2. $\dfrac{-1 + \sqrt{3}\,i}{-3\,i}$

Ejercicio 6.14 Calcular: $(1 + i)^{53}$, $(-\sqrt{2} - \sqrt{2}\,i)^{103}$, $(-1 + i)^{-57}$.

Ejercicio 6.15 Calcular, aplicando la fórmula de De Moivre, representar en el plano complejo y expresar en forma binómica:

1. $\sqrt{-\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}\,i}$ 2. $\sqrt[3]{-8}$

Ejercicio 6.16 (Ⓡ) Graficar en el plano $\sqrt[4]{1+i}$, $\sqrt[3]{-8i}$.

Ejercicio 6.17 Hallar los números complejos z que verifiquen:

1. $-i\,z^3 + i\,z - 5\,i\,(1 - i)^2 = -\dfrac{z}{i} - 10\,i.$
2. $z^4 = -z^2$

3. $2z^4 + 162 = 0$

Ejercicio 6.18 (©) Demostrar que $\left(\dfrac{1 + i \tan \alpha}{1 - i \tan \alpha} \right)^n = \dfrac{1 + i \tan n\,\alpha}{1 - i \tan n\,\alpha}$.

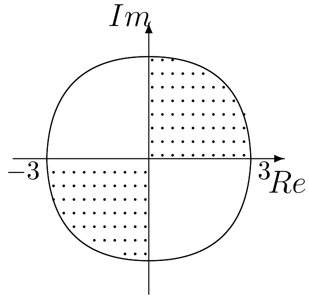
Sug.: Probar que $\dfrac{1 + i \tan n\,\alpha}{1 - i \tan n\,\alpha} = \dfrac{\cos, \alpha + i \operatorname{sen}\ \alpha}{\cos, \alpha - i \operatorname{sen}\ \alpha}$ y completar por inducción.

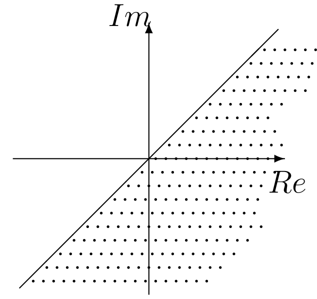
6.6.3. Regiones en el plano complejo

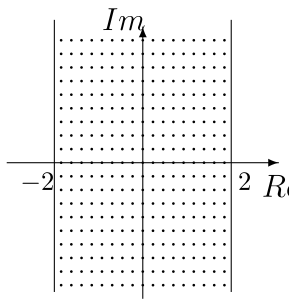
Ejercicio 6.19 Representar en el plano complejo la región determinada por los $z \in \mathbb{C}$ tales que:

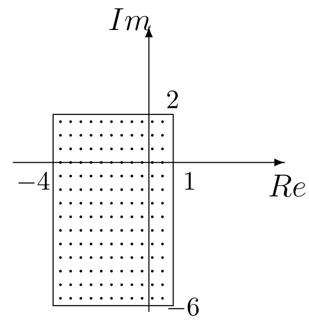
1. $Re\,(z + 4\pi\, i) \geq -1$
2. $Im\, z \leq 3\, Im\,(i\, z)$
3. $|Im\,(z - 16)| < 1$
4. $z\bar{z} = 1$
5. $|z|^2 \leq 16$
6. $|z| > 9$
7. $4 \leq |z|^2 < 7$
8. $Re\,(z^2) = 0$
9. $|z + 1| = |z - 2|$
10. $0 < Arg\ z^3 \leq 3\pi$
11. $Arg\ z = \pi$ y $|z| < 1$
12. $|z| \leq 2 \quad Re\ z \geq 0$

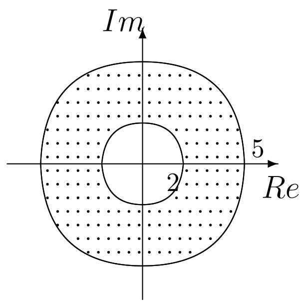
Ejercicio 6.20 Escribir las condiciones que deben verificar los $z \in \mathbb{C}$ para que pertenezcan a la región indicada:

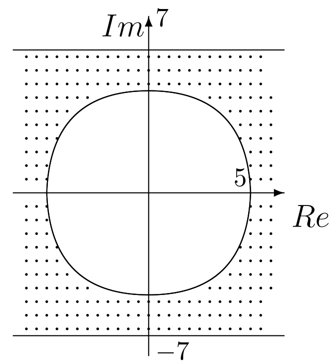












6.6.4. Raíces de la unidad

Ejercicio 6.21 (Ⓡ) Calcular las raíces de la unidad de orden 3, 5, 6 y 7, y representarlas geométricamente. Indicar en cada caso las que son primitivas de cada orden.

Ejercicio 6.22 Hallar las raíces primitivas de la unidad de orden 8, 15 y 18.

Ejercicio 6.23 (Ⓒ) La suma de las n raíces n-ésimas de la unidad, $n > 1$, es 0, y su producto es 1 ó -1, según sea n impar o par.

Ejercicio 6.24 (Ⓒ)

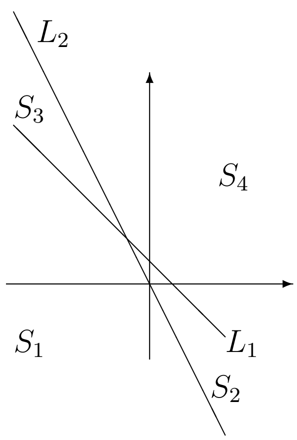
1. Demostrar que si r es una raíz de orden n de un número complejo z y ϵ_1, ϵ_2, …, ϵ_n son las raíces n-ésimas de la unidad, entonces $r \cdot \epsilon_1$, $r \cdot \epsilon_2$, …, $r \cdot \epsilon_n$ son las raíces n-ésimas de z.
2. ¿Qué se puede decir sobre la suma y el producto de las raíces n-ésimas, $n > 1$, de un número complejo $z \neq 0$?

Ejercicio 6.25 1. Probar que $-\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}\, i$ es una raíz de la unidad de orden 8. Decir si es raíz primitiva de dicho orden. En caso afirmativo, hallar todas las raíces de orden 8, a partir de la dada.

2. Usando los resultados obtenidos en el inciso a), resolver la ecuación $x^8 - 256 = 0$.

6.7. Anexo del Curso de Nivelación: Trigonometría

6.7.1. Sistemas de medición de ángulos



Si pensamos en el plano, al intersectarse dos rectas quedan determinados cuatro sectores que varían según las "inclinaciones respectivas"de las rectas, llamamos *ángulo* a cada uno de los cuatro sectores que se determinan, por ejemplo:

Consideremos el sistema de ecuaciones:

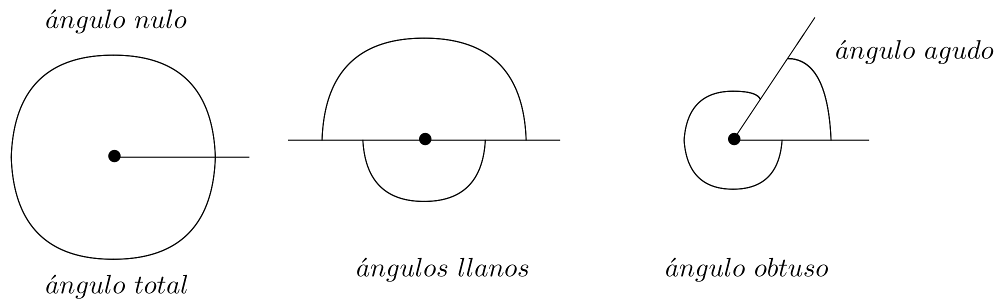
$$\begin{cases} L_1 : \ 2x + y = 0 \\ L_2 : \ x + 1 - y = 0, \end{cases}$$

Divide al plano en cuatro sectores:

$$S_1 \begin{cases} L_1 : \ 2x \leq -y \\ L_2 : \ x + 1 \leq y, \end{cases} S_2 \begin{cases} L_1 : \ 2x \leq -y \\ L_2 : \ x + 1 \geq y, \end{cases} S_3 \begin{cases} L_1 : \ 2x \geq -y \\ L_2 : \ x + 1 \leq y, \end{cases} S_4 \begin{cases} L_1 : \ 2x \geq -y \\ L_2 : \ x + 1 \geq y, \end{cases}$$

Cada uno de estos sectores lo llamaremos ángulo. Si S_1, S_2, S_3, S_4 son iguales los ángulos se dicen *rectos* y las rectas *perpendiculares*. En definitiva, un ángulo es el sector del plano delimitado por dos semirrectas de origen común.

Al dibujar dos semirrectas de origen común, observamos que, si están superpuestas, no delimitan ninguna zona, (o todo el plano), éste será el *ángulo nulo* (o *ángulo total*), si son opuestas delimitan zonas iguales y llamamos a éste *ángulo llano*. En cualquier otro caso hay una zona menor que la otra, la menor la denominamos *ángulo agudo* y la mayor *ángulo obtuso*.



¿Cómo medir los ángulos?

Al igual que para medir longitudes usamos el caprichoso *metro patrón*[2] simplemente dividimos al ángulo total en tantas partes iguales. ¿En cuántas partes iguales?

- Sistema sexagesimal: (en las calculadoras DEG)

En 360 partes iguales, cada una de ellas llamado *grado sexagesimal.* Cada grado tiene 60 minutos y cada minuto 60 segundos. Exactamente igual que en el sistema horario.

En este sistema

ángulo nulo:	ángulo recto:	ángulo llano:	ángulo total:
$0°$	$90°$	$180°$	$360°$

- Sistema centesimal: (en las calculadoras GRA)

En 400 partes iguales, cada una de ellas llamado *grado centesimal.* Cada grado tiene 100 minutos y cada minuto 100 segundos.

En este sistema

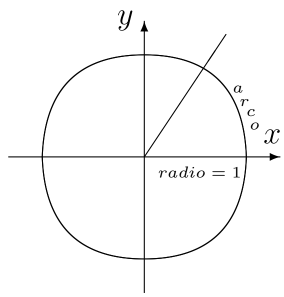
ángulo nulo:	ángulo recto:	ángulo llano:	ángulo total:
$0^{\circ C}$	$100^{\circ C}$	$200^{\circ C}$	$400^{\circ C}$

Si bien pareciera que el sistema centesimal es más sencillo, el sistema sexagesimal no ha caído en desuso, tal vez por su íntima relación con el sistema horario y el cardiovascular en reposo (En reposo total, una persona sana tiene 60 pulsaciones por minuto) En este curso no usaremos este sistema de medida.

[2] barra de platino-iridio que se conserva en la Oficina Internacional de Pesas y Medidas en Sèvres, París.

Finalmente, el sistema más usado en trabajos científicos no parte en sectores iguales el plano, sino la longitud de la circunferencia centrada en el origen común de las semirrectas.

- Sistema radial (en las calculadoras RAD)



La longitud del arco de circunferencia que describe un ángulo depende del radio de la circunferencia que hayamos elegido, por eso definimos la *circunferencia trigonométrica* como una circunferencia de radio 1.

¿Cómo medir la longitud del arco? Ya tenemos el trabajo mayor realizado, sabemos cuál es la fórmula de la longitud de la circunferencia: $long = 2.\pi.r$, si hemos dicho que el radio es $r = 1$ el ángulo total será 2π, sólo nos resta hacer las divisiones.

En este sistema

ángulo nulo:	ángulo recto:	ángulo llano:	ángulo total:
$0\,rad$	$\pi/2\,rad$	$\pi\,rad$	$2\pi\,rad$

Observación 6.4 Usualmente en el sistema radial no se usan unidades de medida, si uno dice que un determinado ángulo mide $\pi/3$ es claro que está hablando de radianes, pero si dice que mide 4, es frecuente acompaãr al número por las unidades para evitar confusiones, en cualquier caso si un ángulo se da sin unidades de medida podemos estar absolutamente seguro que estamos trabajando en sistema radial

Con el sólo objeto de ilustrar mencionamos el sistema utilizado en cálculos militares

- Sistema *mil* (no está en las calculadoras, es información clasificada)

En 6400 partes iguales, cada una de ellas llamado *mil*.

En este sistema

ángulo nulo:	ángulo recto:	ángulo llano:	ángulo total:
$0\,mil$	$1600\,mil$	$3200\,mil$	$6400\,mil$

Conversión de unidades

En este curso usaremos el *sistema sexagesimal* y el *sistema radial*. Siempre que querramos medir una longitud de arco **debemos** usar el sistema radial, cuando hablemos de ángulos será indistinto.

Para realizar la conversión de unidades basta una regla de tres simple. Sabemos que el ángulo total es 360° ó 2π, entonces:

$$\begin{array}{rcl} 360^\circ & \text{———————} & 2\pi \\ 1^\circ & \text{———————} & \dfrac{2\pi}{360} = \dfrac{\pi}{180} \\ 120^\circ & \text{———————} & \dfrac{120 \times 2\pi}{360} = \dfrac{2}{3}\pi \end{array}$$

Resulta: $120^\circ = \dfrac{2}{3}\pi$.

$$\begin{array}{rcl} 2\pi & \text{———————} & 360^\circ \\ 1 & \text{———————} & \dfrac{360^\circ}{2\pi} = \dfrac{180^\circ}{\pi} \\ \pi & \text{———————} & \dfrac{\pi \times 360^\circ}{2\pi} = 180^\circ \end{array}$$

Resulta: $\pi = 180^\circ$.

En realidad lo que hemos hecho para convertir de grados sexagesimales a radianes es multiplicar por $1 = \dfrac{\pi}{180^\circ}$ y para convertir de radianes a grados sexagesimales multiplicamos por $1^\circ = \dfrac{180^\circ}{\pi}$.

Estos números se llaman *constantes de conversión* y retenerlos en la memoria es un gasto innecesario de almacenamiento, ya que se basan en $180^\circ = \pi$

Ejemplo 6.15

$1^\circ = 1^\circ.\dfrac{\pi}{180^\circ} = 0,0174532 \quad rad$

$1\,rad = 1.\dfrac{180^\circ}{\pi} = 57,2957^\circ = 57^\circ 17' 44{,}8''$

Ejercicios propuestos

1. Expresar en radianes los siguientes valores:

   a) 1° *b*) 15° *c*) 45° *d*) 70°

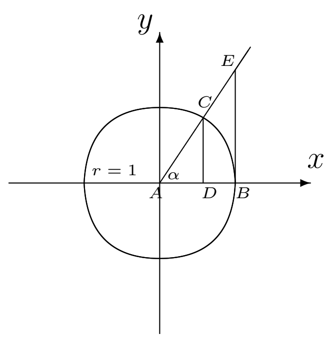
2. Expresar en grados sexagesimales los siguientes valores:

   a) 1 *b*) $5/6.\pi$ *c*) $17/12.\pi$ *d*) 3π

6.7.2. Razones trigonométricas

Volvamos a la ecuación de la recta. Dijimos que una recta está caracterizada por un punto cualquiera por el que pasa (que puede ser la ordenada al origen) y la pendiente. Dijimos también que la pendiente marca la "inclinación"de la recta, podemos ver claramente ahora que lo que marca la pendiente es la magnitud del ángulo que forma la recta con el eje positivo de las abscisas.

Hagamos las mismas cuentas que antes:



En el gráfico hemos determinado dos triángulos:

$$A\overset{\triangle}{E}B \text{ y } A\overset{\triangle}{C}D$$

Ambos triángulos son triángulos rectángulos, entonces tienen una hipotenusa y dos catetos. $\overline{AD}$ y $\overline{AB}$ son los *catetos adyacentes* a α, $\overline{CD}$ y $\overline{EB}$ son los *catetos opuestos*.

El ángulo α es común a ambos triángulos, que son rectángulos. Por lo tanto son triángulos semejantes y, en consecuencia, los lados correspondientes son proporcionales.

$$\frac{\overline{EB}}{\overline{CD}} = \frac{\overline{AB}}{\overline{DA}} = \frac{\overline{AE}}{\overline{AC}}$$

1. De $\dfrac{\overline{EB}}{\overline{CD}} = \dfrac{\overline{AE}}{\overline{AC}}$ podemos concluir que $\dfrac{\overline{EB}}{\overline{AE}} = \dfrac{\overline{CD}}{\overline{AC}}$
2. De $\dfrac{\overline{AB}}{\overline{DA}} = \dfrac{\overline{AE}}{\overline{AC}}$ podemos concluir que $\dfrac{\overline{AB}}{\overline{AE}} = \dfrac{\overline{DA}}{\overline{AC}}$
3. De $\dfrac{\overline{EB}}{\overline{CD}} = \dfrac{\overline{AB}}{\overline{DA}}$ podemos concluir que $\dfrac{\overline{EB}}{\overline{AB}} = \dfrac{\overline{CD}}{\overline{DA}}$

Es decir, los cocientes permanecen invariantes. Observamos que

1. $\dfrac{\overline{EB}}{\overline{AE}}$ es $\dfrac{\text{cateto opuesto a } \alpha}{\text{hipotenusa}}$
2. $\dfrac{\overline{AB}}{\overline{AE}}$ es $\dfrac{\text{cateto adyacente a } \alpha}{\text{hipotenusa}}$
3. $\dfrac{\overline{EB}}{\overline{AB}}$ es $\dfrac{\text{cateto opuesto a } \alpha}{\text{cateto adyacente a } \alpha}$

Llamamos al primer cociente *seno de* α y lo escribimos $sen\,\alpha$, al segundo *coseno de* α y lo notamos $cos\,\alpha$.

De este modo el tercer cociente es $\dfrac{sen\,\alpha}{cos\,\alpha}$.

Si hacemos coincidir el origen el ángulo α con el centro de una circunferencia trigonométrica, la hipotenusa del triángulo rectángulo que se forma es un radio de la circunferencia y, por lo tanto, vale 1.

De este modo, directamente

$$sen\,\alpha = \overline{CD}, \;\; cos\,\alpha = \overline{AD}$$

Observación 6.5 Es interesante notar que la primera acepción que reconoce el diccionario de la Real Academia Española (RAE) para la palabra *seno* se refiere al agujero, el hueco o la abertura de algo. Por extensión, se asocia la idea de seno al interior de una cosa. Vemos, entonces, lo apropiado de la denominación seno ya que es la abertura de la "caverna" determinada por la recta en cuestión y el eje positivo de las abscisas. Por otra parte, mencionamos que los triángulos con los que trabajamos son triángulos rectángulos. La suma de los ángulos interiores de un triángulo es π, el ángulo correspondiente al vértice A es α y sea β el ángulo correspondiente al vértice C (o E). Claramente $\alpha + \beta = \pi/2$, es decir, α y β son ángulos complementarios o co-ángulos. En esta circunferencia trigonométrica, resulta que el segmento $\overline{AD}$ es el seno de β es decir, el seno del co-ángulo de α y de allí la denominación de *co-seno.*

Se define *recta tangente a una circunferencia en un punto* como una recta que intersecta a la circunferencia sólo en dicho punto.

Analicemos nuevamente los triángulos. El lado $\overline{BE}$ está sobre una recta tangente a la circunferencia, la longitud de $\overline{AB} = 1$, y además

$$\frac{\overline{EB}}{\overline{AB}} = \frac{\overline{CD}}{\overline{AD}}$$

o lo que es lo mismo:

$$\frac{\overline{EB}}{1} = \frac{sen\,\alpha}{cos\,\alpha}$$

Llamamos entonces *tangente* de α y escribimos $tan\,\alpha$ ó $tg\,\alpha$ a:

$$tan\,\alpha = \frac{sen\,\alpha}{cos\,\alpha}.$$

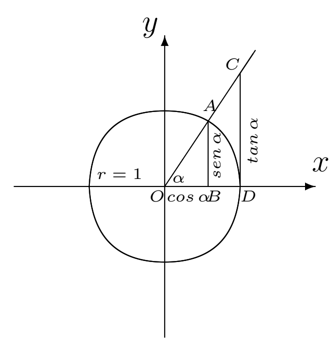
Hemos dado así tres nuevos modos de medir un ángulo. Los inversos multiplicativos de las funciones trigonométricas definidas son suficientemente importantes como para tener nombre propio, entonces definimos:

3. *secante* de α : $sec\,\alpha = \dfrac{1}{cos\,\alpha} = cos^{-1}\alpha$
4. *cosecante* de α : $cosec\,\alpha = \dfrac{1}{sen\,\alpha} = sen^{-1}\alpha$
5. *cotangente* de α : $cotan\,\alpha = \dfrac{1}{tan\,\alpha} = tan^{-1}\alpha$

Observación 6.6 una observación que no tiene nada que ver con la matemática, pero sí con la mnemotecnia: es sencillo recordar que la cotangente va con la tangente ($cotan\,\alpha = tan^{-1}\,\alpha$), pero con la secante y la cosecante empiezan las confusiones. Igual que en el caso de la tangente y la **co**tangente, una sola tiene el **co**. Entonces la **co**secante va con el seno y la secante con el **co**seno.

Cómo hallar gráficamente:

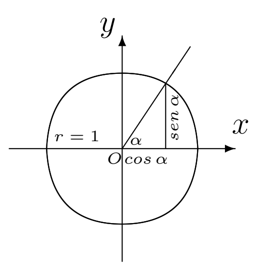
- $sen\,\alpha$
- $cos\,\alpha$
- $tan\,\alpha$



1. Tomando como segmento inicial del ángulo el eje positivo de las abscisas (eje x), y como origen el origen de coordenadas se marca la semirrecta final del ángulo α
2. Se dibuja una circunferencia trigonométrica centrada en el origen de coordenadas

3. Queda determinado el punto A (intersección de la circunferencia y la semirrecta)
4. Por A se traza una perpendicular al eje x
5. Queda determinado el punto B
6. $sen\,\alpha = \overline{AB}$, $\quad cos\,\alpha = \overline{OB}$
7. $D:\ (1,0)$ es el punto de intersección del eje x con la circunferencia
8. Se traza la recta tangente a la circunferencia por D
9. Queda determinado C, punto de intersección de la recta tangente y la semirrecta final de α
10. $tan\,\alpha = \overline{CD}$

Veamos algunas propiedades de las razones trigonométricas:



Identidad pitagórica:

El teorema de Pitágoras dice que la suma de los cuadrados de los catetos es el cuadrado de la hipotenusa.

$$sen^2\alpha + cos^2\alpha = 1$$

Esta identidad se utiliza para averiguar cuál es el valor de las demás razones trigonométricas dada una de ellas. Por ejemplo:

Ejemplo 6.16

Sea α tal que $sen\,\alpha = -\dfrac{3}{5}$.

1. Hallar las restantes razones trigonométricas
2. Graficar **exactamente** el ángulo α

Reemplazamos la información en $sen^2\alpha + cos^2\alpha = 1$ y resulta:

$\left(-\frac{3}{5}\right)^2 + cos^2\alpha = 1$

$\frac{9}{25} + cos^2\alpha = 1$

$cos\,\alpha = \pm\sqrt{1 - \frac{9}{25}} = \pm\sqrt{\frac{16}{25}}$

Entonces puede ser: $cos\,\alpha = \frac{4}{5}$ ó $cos\,\alpha = -\frac{4}{5}$

En consecuencia

$tan\,\alpha = \frac{-3/5}{4/5} = -\frac{3}{4}$ ó $tan\,\alpha = \frac{-3/5}{-4/5} = \frac{3}{4}$

Para dibujar el ángulo **con exactitud** recordemos la ecuación de la recta. Vimos ya que la pendiente de la recta es la tangente del ángulo que forma con el eje positivo de las abscisas, sabemos que esta recta pasa por el punto $(0,0)$. El ángulo ya se puede dibujar.

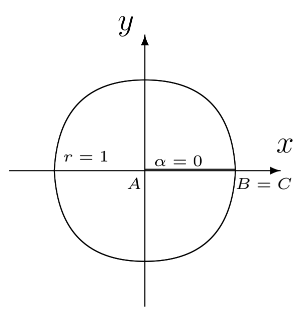
Cálculo de los valores para los ángulos distinguidos

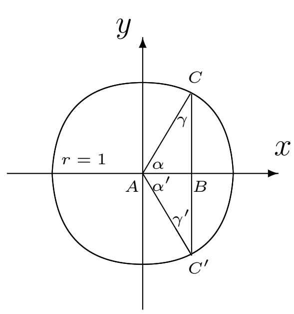
- $\alpha = 0°(0)$

$sen\,\alpha = \overline{BC} = 0$

$cos\,\alpha = \overline{AB} = r = 1$

$tan\,\alpha = \frac{sen\,\alpha}{cos\,\alpha} = 0$





- $\alpha = 30°(\pi/6)$

Reflejemos el ángulo α con respecto al eje x. Obtenemos α', $\alpha + \alpha' = 60°$. $\gamma = \gamma'$ y $60° + \gamma + \gamma' = 180°$,
de donde $\gamma = 60°$.

Es decir, es un triángulo equilátero.
$\overline{CC'} = \overline{AC} = \overline{AC'} = 1$, Como $\overline{CC'} = 2\overline{BC}$ resulta $\overline{BC} = 1/2$ $sen\,\alpha = \overline{BC} = 1/2$

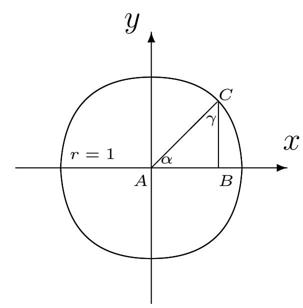
Para calcular $cos\,\alpha$ usaremos la identidad pitagórica: $sen^2\alpha + cos^2\alpha = 1$

$(1/2)^2 + cos^2\alpha = 1$ $cos^2\alpha = 1-(1/2)^2$ $cos\,\alpha = \pm\sqrt{1-(1/2)^2}$, como $\alpha \in$I^{er}C:

$cos\,\alpha = \sqrt{3}/2$

$$tan\alpha = \frac{sen\,\alpha}{cos\,\alpha} = \frac{1/2}{\sqrt{3}/2} = \frac{\sqrt{3}}{3}$$

- $\alpha = 45°(\pi/4)$



$\alpha + \gamma + 90° = 180°$, resulta $\gamma = 90° - \alpha$.

$cos\,\alpha = sen\,\gamma$, reemplazando en la identidad pitagórica:

$2sen^2\alpha = 1$ y, en consecuencia $sen\,\alpha = \pm\sqrt{1/2}$,
como $\alpha \in$ I^{er}C $sen\,\alpha = \sqrt{1/2} = \sqrt{2}/2$ $sen\,\alpha = \overline{BC} = \sqrt{2}/2$

$cos\,\alpha = \overline{AB} = \sqrt{2}/2$

$$tan\,\alpha = \frac{sen\,\alpha}{cos\,\alpha} = 1$$

- $\alpha = 60°(\pi/3)$

Usamos la propiedad de ángulos complementarios y resulta:

$sen\,\alpha = cos(90° - 60°) = cos\,30° = \sqrt{3}/2$

$cos\,\alpha = sen(90° - 60°) = sen\,30° = 1/2$

$$tan\,\alpha = \frac{\sqrt{3}/2}{1/2} = \sqrt{3}$$

Podemos calcular las razones trigonométricas del ángulo recto usando el mismo argumento, o bien simplemente observarlo en el gráfico.

- $\alpha = 90°(\pi/2)$

Usamos la propiedad de ángulos complementarios y resulta:

$sen\,\alpha = cos(90° - 90°) = cos\,0° = 1$

$cos\,\alpha = sen(90° - 90°) = sen\,0° = 0$

$tan\,90°$ no está definida. (No sabemos dividir por 0)

Los ángulos cuyas razones trigonométricas hemos calculado se llaman *ángulos distinguidos* justamente porque estas funciones pueden calcularse con sencillez.

Resumamos estos datos en una tabla:

Tabla de valores de los ángulos distinguidos:

α (DEG)	0	30	45	60	90
α (RAD)	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
$sen\,\alpha$	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	1
$cos\,\alpha$	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0
$tan\,\alpha$	0	$\sqrt{3}/3$	1	$\sqrt{3}$	

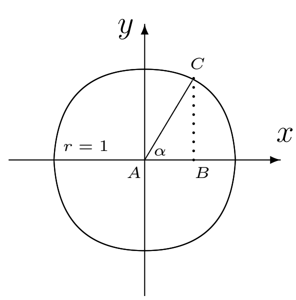
Sabemos que el plano está dividido en cuatro cuadrantes,

I^{er} cuadrante $\quad x \geq 0 \quad y \geq 0$

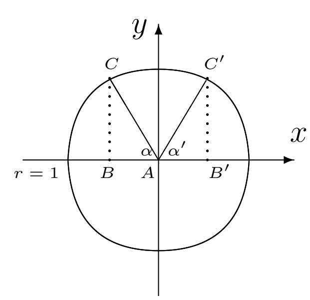
II^{do} cuadrante $\quad x \leq 0 \quad y \geq 0$

III^{er} cuadrante $\quad x \leq 0 \quad y \leq 0$

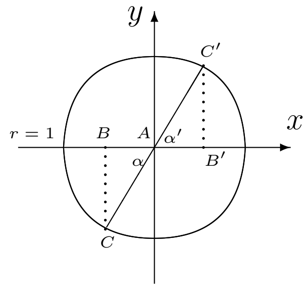
IV^{to} cuadrante $\quad x \geq 0 \quad y \leq 0$



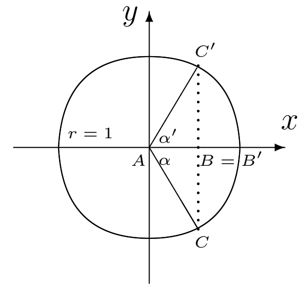
I^{er} cuadrante $\quad x \geq 0 \quad y \geq 0$



II^{do} cuadrante $\quad x \leq 0 \quad y \geq 0$



III^{er} cuadrante $\quad x \leq 0 \quad y \leq 0$



IV^{to} cuadrante $\quad x \geq 0 \quad y \leq 0$

En todos los gráficos:

$$sen\,\alpha = \overline{BC} \qquad\qquad cos\,\alpha = \overline{AB}$$

Si $0° \leq \alpha \leq 90°$ $(0 \leq \alpha \leq \pi/2)$

$$\alpha \in \text{I}^{er}\text{C, entonces} \quad sen\,\alpha \geq 0 \quad cos\,\alpha \geq 0 \quad tan\,\alpha \geq 0$$

Si $90° \leq \alpha \leq 180°$ $(\pi/2 \leq \alpha \leq \pi)$

$$\alpha \in \text{II}^{do}\text{C, entonces} \quad sen\,\alpha \geq 0 \quad cos\,\alpha \leq 0 \quad tan\,\alpha \leq 0$$

Si $180° \leq \alpha \leq 270°$ $(\pi \leq \alpha \leq 3.\pi/2)$

$$\alpha \in \text{III}^{er}\text{C, entonces} \quad sen\,\alpha \leq 0 \quad cos\,\alpha \leq 0 \quad tan\,\alpha \geq 0$$

Si $270° \leq \alpha \leq 360°$ $(3.\pi/2 \leq \alpha \leq 2.\pi)$

$$\alpha \in \text{IV}^{to}\text{C, entonces} \quad sen\,\alpha \leq 0 \quad cos\,\alpha \geq 0 \quad tan\,\alpha \leq 0$$

En estos gráficos se puede observar mucho más que simplemente el signo de las funciones trigonométricas.

Si $\alpha \in \text{II}^{do}$C, entonces

$$sen\,\alpha = \overline{BC} = \overline{B'C'} = sen\,(180° - \alpha)$$
$$cos\,\alpha = \overline{AB} = -\overline{AB'} = -cos\,(180° - \alpha)$$

Si $\alpha \in \text{III}^{er}$C, entonces

$$sen\,\alpha = \overline{BC} = -\overline{B'C'} = -sen\,(\alpha - 180°)$$
$$cos\,\alpha = \overline{AB} = -\overline{AB'} = -cos\,(\alpha - 180°)$$

Si $\alpha \in \text{IV}^{to}$C, entonces

$$sen\,\alpha = \overline{BC} = -\overline{B'C'} = -sen\,(360° - \alpha)$$

$cos\,\alpha = \overline{AB} = \overline{AB} = cos\,(360° - \alpha)$

Estas relaciones que acabamos de ver se llaman *reducción al primer cuadrante*. Un modo práctico de hacer esta reducción es el siguiente:

Es importante tener en cuenta que todos los ángulos se refieren al eje de las abscisas.

- Si un ángulo α está en el II^{do}C, "no llega" a 180°, es $\alpha = 180° - \beta$
- Si un ángulo α está en el III^{er}C, "se pasa"de 180°, es $\alpha = 180° + \beta$
- Si un ángulo α está en el VI^{to}C, "no llega" a 360°, es $\alpha = 360° - \beta$

Tomamos los valores de las fuciones trigonométricas de β y finalmente le colocamos el signo que le corresponde según el cuadrante en que esté. Veamos algunos ejemplos:

Ejemplo 6.17

$\alpha = 120°$

$90° \leq 120° \leq 180°$, $\alpha \in$ II^{do}C.

$120° = 180° - 60°$

$sen\,60° = \sqrt{3}/2, \quad cos\,60° 1/2 =, \ \ tan\,60° = \sqrt{3},$

como $120° \in$ II^{do}C

$sen\,120° = \sqrt{3}/2, \quad cos\,120° = -1/2, \ \ tan\,120° = -\sqrt{3},$

Ejemplo 6.18

$\alpha = 225°$

$180° \leq 225° \leq 270°$, $\alpha \in$ III^{er}C.

$225° = 180° + 45°$

$sen\,45° = \sqrt{2}/2, \quad cos\,45° = \sqrt{2}/2, \ \ tan\,45° = 1,$

como $225° \in$ III^{er}C

$sen\,225° = -\sqrt{2}/2, \quad cos\,225° = -\sqrt{2}/2, \ \ tan\,225° = 1,$

Ejemplo 6.19

$\alpha = 330°$

$270° \leq 330° \leq 360°$, $\alpha \in \text{IV}^{to}\text{C}$.

$330° = 360° - 30°$

$sen\, 30° = 1/2, \quad cos\, 30° = \sqrt{3}/2, \;\; tan\, 30° = \sqrt{3}/3,$

como $330° \in \text{IV}^{to}\text{C}$

$sen\, 330° = -1/2, \quad cos\, 330° = \sqrt{3}/2, \;\; tan\, 330° = -\sqrt{3}/3,$

En el ejemplo 6.16 calculamos las demás razones trigonométricas dado el seno (lo mismo podríamos haber hecho dado cualquier otra razón trignométrica) y graficamos α con exactitud, lo que no hicimos es decir cuánto vale α. Usemos esta tabla para averiguar fácilmente cuál es el valor de α conocido el del seno.

Ejemplo 6.20

Si se nos informa que $sen\, \alpha = \sqrt{2}/2$ entramos en la tablita por el renglón que dice "$sen\, \alpha$" y al encontrar el valor $\sqrt{2}/2$ subimos por la columna para verificar que $\alpha = 45°$ ó, si se quiere en radianes $\alpha = \pi/4$.

Si buscamos en la columna de $\alpha = 45°$ vemos que el $cos\, \alpha = \sqrt{2}/2$, sin embargo la identidad pitagórica dice que $cos\, \alpha = \pm\sqrt{2}/2$. Vamos a analizar este hecho.

Conociendo el valor de $y = sen\, \alpha$ hallar α, o lo que es lo mismo, conociendo el valor de $y = f(x)$, hallar x es hallar $f^{-1}(y)$, la *función inversa* de f. en el caso de las funciones trigonométricas hemos definido las funciones "inversas multiplicativas"(por ejemplo, del seno, $sen^{-1}\alpha = 1/sen\, \alpha = cosec\, \alpha$) y si habláramos de función inversa podría llevar a confusiones.

Supongamos que trabajamos en radianes. Si, como en el ejemplo 6.20 $sen\, \alpha = \sqrt{2}/2$, entonces $\alpha = \pi/4$ ¿qué es $\pi/4$? La longitud del arco de circunferencia que corresponde a un seno de $\sqrt{2}/2$, entonces hemos hallado el "arco del seno" y llamamos *arco seno* a la función inversa del seno. Del mismo modo hallamos em arco coseno, arco tangente, arco cotangente, etc. Algunas calculadoras lo tienen marcado de este modo y otras como sen^{-1}, cos^{-1}, etc.

Resolvamos nuevamente el ejemplo 6.16 usando la calculadora:

$sen\, \alpha = -3/5$, entonces buscamos $arcsen(-3/5)$ y obtenemos $\alpha = -36{,}869898$, de donde:

$cos(-36{,}869898) = 0{,}8$ y $tan(-36{,}869898) = -0{,}75$

Los valores hallados son absolutamente correctos, pero "faltan" ¿qué es lo que hay que considerar? En qué cuadrante está el ángulo.

Ejercicios propuestos

1. Completar la siguiente tabla:

Gr.		135	150		210	225		270			330	360
Rad.	$\frac{2}{3}\pi$			π			$\frac{4}{3}\pi$		$\frac{5}{3}\pi$	$\frac{7}{4}\pi$		
Sen.												
Cos.												
Tan.												

2. Calcular las razones trigonométricas de los siguientes valores, reduciendo previamente los ángulos al primer cuadrante.

   (a) $150°$ (b) $135°$ (c) $120°$

   (d) $315°$ (e) $240°$ (f) $300°$

   (g) $4/3.\pi$ (h) $5/3.\pi$ (i) $3/2.\pi$

   (j) $11/6.\pi$ (k) $7/4.\pi$ (l) $2/3.\pi$

3. Calcular las razones trigonométricas de los siguientes ángulos:

   (a) $1470\ °$ (b) $\dfrac{5}{3}\pi$ (c) $-120°$ (d) $-\dfrac{7}{4}\pi$

4. Si $\pi/2 < \alpha < \beta < \pi$, analizar la validez de las siguientes desigualdades.

   (a) $\text{sen}\alpha > \ \text{sen}\beta$ (b) $\cos\alpha < \ \cos\beta$ (c) $\text{sen}^2\alpha > \ \text{sen}^2\beta$

5. Calcular las restantes razones trigonométricas en cada uno de los siguientes casos: (a) $\cos\alpha = 0{,}77$ (b) $\text{sen}\,\beta = -0{,}64$ (c) $\text{tg}\,\gamma = 2$

6. Dibujar un ángulo α tal que $\cos\alpha = 1/3$, y su tangente sea negativa. ¿Cuánto vale el seno de α?

Capítulo 7

Polinomios

Polinomios y ecuaciones algebraicas. Suma y Multiplicacicón. Divisibilidad. Máximo común divisor. Algoritmo de Euclides. Teorema de factorización. Raíces de un polinomio. Raíces múltiples. Teorema fundamental del álgebra. Raíces complejas. Polinomios irreducibles en $\mathbb{R}[X]$. Cálculo de las raíces racionales de ecuaciones con coeficientes racionales.

7.1. Polinomios y funciones polinómicas

La definición estricta de *polinomio* y las operaciones que se realizan con polinomios escapan a los objetivos de este curso. Si vamos a la etimología de la palabra *poli* significa *muchos* y *nomio* significa *término*. En consecuencia un *polinomio* es algo con *muchos términos*. Para poder trabajar con este concepto daremos un método para determinar eficazmente si una expresión algebraica es un polinomio o no.
En primer lugar hablaremos de polinomios a coeficientes reales. Afirmamos entonces que:

1. Todo número real a es un polinomio.
2. $a \cdot x^n$ es polinomio para todo número real a y toda potencia natural n.
3. La suma de polinomios es polinomio.
4. No hay más polinomios que los que se generan de este modo.

El conjunto formado por todos los polinomios a coeficientes reales lo notamos $\mathbb{R}[X]$.
Hablamos de polinomios a coeficientes reales, y comenzamos diciendo "Todo

número real es un polinomio". En verdad no es necesario que sean números reales específicamente, en este curso trabajaremos con las constantes de los polinomios dentro de un cuerpo. Hemos visto los cuerpos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, lo cual nos permite pensar en el conjunto de polinomios a coeficientes racionales que notaremos $\mathbb{Q}[X]$, el conjunto de polinomios a coeficientes reales $\mathbb{R}[X]$ y el conjunto de polinomios a coeficientes complejos $\mathbb{C}[X]$. Claramente, del mismo modo que $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ resulta $\mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.

Ejemplo 7.1

Son polinomios:	No son polinomios:
x,	x^{-1},
π,	$(3+x)(x-1)$,
$3\,i\,x^2$,	$\sqrt{x+4}$,
5,	$\dfrac{x+4}{x}$
$4\,x^5 + (5-i)\,x - 3$,	
$6\,x^8 - 4\,x^2 + x - 7\,x^9$	

Como decíamos antes, Polinomio quiere decir, literalmente, "muchas partes" y así, considerando la etimología, un polinomio que tiene solamente "una parte" , por ejemplo $4\,x^8$, se llama *monomio* uno que tiene "dos partes", por ejemplo $5\,x + x^3$ se llama *binomio*, si tiene tres, *trinomio* y así sucesivamente.

Cada "parte" se llama *término* y está compuesta por un número (racional, real o complejo), llamado *coeficiente* y una potencia natural de la variable, (x en nuestro caso, cuando se aplican a procesos que tienen que ver con el tiempo suele usarse la t) es decir x^n; donde n se dice el *grado del término.*
Se llama *grado del polinomio* al grado del término de mayor grado. (El más grande entre todos los grados.)

Según las definiciones que hemos dado, las constantes son polinomios de grado cero. A excepción de la constante nula, cuyo grado no está definido. El término de grado 1 se llama *término lineal* y el coeficiente, *coeficiente lineal*, el de grado 2, *término cuadrático* y *coeficiente cuadrático*, de igual modo se definen *término cúbico* o *de grado 3*, etc. El término que no tiene a la variable x, o sea el de grado 0, se llama *término independiente* y el término de mayor grado se llama *término principal.* Si el *coeficiente principal*, es decir el coeficiente que acompaña al término principal, es 1 el polinomio se denomina *mónico.*

Por ejemplo, en el polinomio $6\,x^4 - 2\,i\,x + 3\,x^2 + 6 + i$ el término de mayor grado es $6\,x^4$, por lo tanto el grado del polinomio es 4. El término cuadrático es $3\,x^2$ y en consecuencia el coeficiente cuadrático es 3, el término lineal $-2\,i$ y el término independiente es $6+i$.

Decimos que dos polinomios son *iguales* si son iguales término a término, es decir, si son iguales los coeficientes de los términos de igual grado. Por ejemplo, son iguales $3x^4-2x+8$, $-2x+3x^4+8$, $8-2x+3x^4$, a fin de comparar más sencillamente los polinomios suelen escribirse en *orden creciente* (del término de menor grado al término de mayor grado) ó en *orden decreciente* (del término de mayor grado al de menor grado), en el caso anterior:

en orden creciente: $8-2x+3x^4$

en orden decreciente: $3x^4-2x+8$

De éstos el orden decreciente es el más utilizado. Al escribir un polinomio en forma decreciente se dice que se lo ha escrito en *forma ordenada*.

Si analizamos el último ejemplo vemos que es un polinomio de grado 4, entonces debería tener cinco términos y, sin embargo, sólo tiene tres. La *forma completa* de un polinomio se obtiene agregando los términos que no están presentes con coeficiente nulo, es decir:

la forma ordenada y completa de $8-2\,x+3\,x^4$ es: $3\,x^4+0\,x^3+0\,x^2-2\,x+8$.

Ejemplo 7.2 Construyamos en cada caso un polinomio $\mathbf{p}_i$ que satisfaga las siguientes condiciones:

$\mathbf{p}_1$ $\in \mathbb{R}[X]$, gr($\mathbf{p}_1$)= 4, mónico, sin término independiente.

$$\mathbf{p}_1 = x^4.$$

$\mathbf{p}_2$ $\in \mathbb{C}[X]$, gr($\mathbf{p}_2$)= 3, coeficiente cuadrático nulo, y el coeficiente principal igual al coeficiente lineal.

$$\mathbf{p}_2 = i\,x^3 + i\,x.$$

$\mathbf{p}_3$ $\in \mathbb{Q}[X]$, cada coeficiente igual al grado del término al que corresponde.

$$\mathbf{p}_3 = 5\,x^5 + 4\,x^4 + 3\,x^3 + 2\,x`2 + x.$$

En cada uno de los casos anteriores tomamos decisiones y es claro que en ningún caso la respuesta es única. Queda a cargo del lector encontrar otros ejemplos que satisfagan las condiciones pedidas. Además puede intentar contestar las siguientes preguntas:

¿Se puede dar un polinomio que satisfaga simultáneamente las condiciones de $\mathbf{p}_1$y $\mathbf{p}_2$?
¿Hay algún polinomio mónico en las condiciones de $\mathbf{p}_3$?®

Si $\mathbf{p} = a_n x^n + a_+ n - 1x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ es un polinomio en $\mathbb{K}[X]$, la función $p(x) = a_n x^n + a_+ n - 1x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$, que asocia a cada $x \in \mathbb{K}$ el resultado de hacer la cuenta propuesta por el polinomio cuando la variable vale x es una *función polinómica*. En la práctica cotidiana solemos llamar polinomios a las funciones polinómicas por simple economía de lenguaje, dado que no se presta a confusión. Claramente cada vez que necesitemos el valor numérico necesitaremos usar funciones polinómicas y en ese caso escribiré: $p(x)$ en lugar de $\mathbf{p}$.

Ejemplo 7.3 Sea $\mathbf{p} = 3x^2 + 2x - 1$,
la función polinómica asociada es $p : \mathbb{R} \to \mathbb{R}$ definida por $p(x) = 3x^2 + 2x - 1$.

Sea $\mathbf{q} = 4x^5 - x^4 + 2x^3 - 3x + 2$,
la función polinómica asociada es $p : \mathbb{R} \to \mathbb{R}$ definida por $q(x) = 4x^5 - x^4 + 2x^3 - 3x + 2$.

Sea $\mathbf{r} = x^2 + 2$,
la función polinómica asociada es $p : \mathbb{R} \to \mathbb{R}$ definida por $r(x) = x^2 + 2$.

7.2. Operaciones con polinomios

Con los polinomios se puede hacer exactamente las mismas operaciones que con los números enteros, es decir:

7.2.1. Suma de polinomios

Pensamos la suma de polinomios como suma de sumas algebraicas y sacamos factor común por grupos las potencias de x, la resultante es la suma de los coeficientes de los términos de igual grado.

Veremos en un ejemplo un método para no cometer errores.

Ejemplo 7.4 Dados dos polinomios $\mathbf{p} :\ 3x^5 - 2x^2 + 6x - x^3$ y $\mathbf{q} :\ 6x^2 + 1 - 2x^5 + 3x - x^4$: los escribimos en forma ordenada y completa uno debajo del otro y simplemente sumamos término a término.

$\mathbf{p}$	$3x^5$	$+0x^4$	$-x^3$	$-2x^2$	$+6x$	$+0$
$\mathbf{q}$	$-2x^5$	$-x^4$	$0x^3$	$+6x^2$	$+3x$	$+1$
$\mathbf{p}+\mathbf{q}$	x^5	$-x^4$	$-x^3$	$+4x^2$	$+9x$	$+1$

Observación 7.1 ¿Qué relación hay entre el grado de **p**, el grado de **q** y el grado de **p+q**? La respuesta más fácil es "el más grande" pero no siempre funciona así. Veamos un ejemplo:

Ejemplo 7.5 $\mathbf{p}: 4x^5 - 2x^2 \text{ y } \mathbf{q}: 6x^2 + 1, \quad \mathbf{p}+\mathbf{q}: 4x^5 + 4x^2 + 1$

$$gr(\mathbf{p}) = 5, \ gr(\mathbf{q}) = 2, \ gr(\mathbf{p}+\mathbf{q}) = 5 = gr(\mathbf{p})$$

$$\mathbf{p}: 3x^5 - 2x^2 \text{ y } \mathbf{q}: 6x^8 + 2x^5, \ \mathbf{p}+\mathbf{q}: 6x^8 + 5x^5 - 2x^2$$

$$gr(\mathbf{p}) = 5, \ gr(\mathbf{q}) = 8, \ gr(\mathbf{p}+\mathbf{q}) = 8 = gr(\mathbf{q})$$

$$\mathbf{p}: 3x^5 - 2x^2 \text{ y } \mathbf{q}: 6x^5 + 1, \quad \mathbf{p}+\mathbf{q}: 9x^5 - 2x^2 + 1$$

$$gr(\mathbf{p}) = 5, \ gr(\mathbf{q}) = 5, \ gr(\mathbf{p}+\mathbf{q}) = 5 = gr(\mathbf{p}) = gr(\mathbf{q})$$

$$\mathbf{p}: 3x^5 - x^3 \text{ y } \mathbf{q}: -3x^5 + 1, \quad \mathbf{p}+\mathbf{q}: -x^3 + 1,$$

$$gr(\mathbf{p}) = 5, \ gr(\mathbf{q}) = 5, \ gr(\mathbf{p}+\mathbf{q}) = 3$$

La suma de polinomios en $\mathbb{K}[X]$ es simplemente la suma de números de $\mathbb{K}$ término a término, en consecuencia tiene exactamente las mismas propiedades que en los números enteros:

Proposición 7.1 *Dados* **p**, **q**, **r** $\in \mathbb{K}[X]$ *se verifican las siguientes igualdades:*

1. **p+(q+ r)=(p+q)+r** (propiedad asociativa)
2. **p+q=q+p** (propiedad conmutativa)
3. Existe **0** (el número 0) tal que **p+0=0+p=p** (elemento neutro)
4. Para cada **p** existe **-p**, tal que **p+(-p)=(-p)+p=0** (simétricos)

Claramente construir el polinomio simétrico de un polinomio dado es simplemente cambiar todos los signos a los coeficientes. Veamos un ejemplo:

Ejemplo 7.6 Sea $\mathbf{p}: 3x^5 - 2x^2 + 6x - x^3$, entonces $-\mathbf{p}: -3x^5 + 2x^2 - 6x + x^3$

7.2.2. Producto de un polinomio por una constante

Dado $\mathbf{p} \in \mathbb{K}[X]$ y $k \in \mathbb{K}$, si $\mathbf{p}= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ se define el producto de **p** por k al polinomio: $k \cdot \mathbf{p}= k \cdot a_n x^n + k \cdot a_{n-1} x^{n-1} + \ldots + k \cdot a_1 x + k \cdot a_0$.

Proposición 7.2 *Dados* $\mathbf{p}, \mathbf{q}, \in \mathbb{K}[X]$, $k_1, k_2 \in \mathbb{K}$, *se verifican las siguientes igualdades:*

1. $k \cdot (\mathbf{p}+\mathbf{q}) = k \cdot \mathbf{p} + k \cdot \mathbf{q})$
2. $(k_1 + k_2) \cdot \mathbf{p} = k_1 \cdot \mathbf{p} + k_2 \cdot \mathbf{p}$
3. $(k_1 \cdot k_2) \cdot \mathbf{p} = k_1 \cdot (k_2 \cdot \mathbf{p})$
4. $1 \cdot \mathbf{p} = \mathbf{p}$

La demostración de estas propiedades es muy sencilla y la cedemos gentilmente al lector interesado. ®

7.2.3. Producto de polinomios

Podemos pensar el producto de dos polinomios como si estuviéramos aplicando propiedad distributiva en sumas algebraicas. Veamos un ejemplo:

Ejemplo 7.7 Dados dos polinomios: $\mathbf{p}: -2x^2 + 6x - x^3$ y $\mathbf{q}: 6 + 3x - x^2$

Un método para no cometer errores consiste en escribirlos en forma completa y ordenada y multiplicar igual que como multiplicamos cifras enteras.

Por ejemplo:

$$\begin{array}{cccc} & 3 & 2 & 5 \\ & \times & 3 & 2 \\ \hline & 7 & 5 & 0 \\ 9 & 7 & 5 & \\ \hline 1 & 9 & 2 & 5 \end{array}$$

Con los polinomios dados:

$$\begin{array}{c|cccccc} \mathbf{p} & & & -x^3 & -2x^2 & +6x & +0 \\ \mathbf{q} & & & & -x^2 & +3x & +6 \\ \hline & & & -18x^3 & -12x^2 & +36x & +0 \\ & & -3x^4 & -6x^3 & 18x^2 & 0 & \\ & x^5 & +2x^4 & -6x^3 & 0 & & \\ \hline \mathbf{p} \times \mathbf{q} & x^5 & -x^4 & -30x^3 & +6x^2 & +36x & +0 \end{array}$$

Observación 7.2 ¿Qué relación hay entre el grado de $\mathbf{p}$, el grado de $\mathbf{q}$ y el grado de $\mathbf{p.q}$?

Sabemos que el producto de potencias de igual base suma los exponentes, cuando hagamos el producto de polinomios, al multiplicar el término de mayor grado de $\mathbf{p}$, con el término de mayor grado de $\mathbf{q}$, la potencia de x será la suma de $gr(\mathbf{p})$ y $gr(\mathbf{q})$.

Es decir:

$$gr(\mathbf{p}.\mathbf{q}) = gr(\mathbf{p}) + gr(\mathbf{q})$$

Observación 7.3 Hemos dado una forma muy sencilla para realizar el producto de dos polinomios. En verdad existen fórmulas para calcularlo que no tiene sentido aplicarlas en este curso, pero analicemos brevemente de qué se tratan con un ejemplo sencillo.
Sean: $\mathbf{p} = 12x^6 + a0x^5 - x^4 + 2x^3 - x + 3$

$\mathbf{q} = -x^5 + x^4 + 3x^2 - 2$

Y supongamos que queremos calcular el coeficiente del término de grado 9.

Como "producto de potencias de igual base se suman los exponentes" analizamos todas las formas de obtener el número 9, con dos sumandos, el primero que sea un grado de algún término del polinomio $\mathbf{p}$ y el segundo un grado de algún término de $\mathbf{q}$.

Las posibilidades son: 6+3, 5+4 y 4+5. Multiplicamos los coeficientes correspondientes y luego sumamos todo, así obtenemos: $12.0 + 10.1 + (-1).(-1) = 11$.

El producto de polinomios tiene exactamente las mismas propiedades que en los números enteros:

Proposición 7.3 *Dados* $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r} \in \mathbb{K}[X]$ *se verifican las siguientes igualdades:*

1. $\mathbf{p}.(\mathbf{q}.\ \mathbf{r})=(\mathbf{p}.\mathbf{q}).\mathbf{r}$ (propiedad asociativa)
2. $\mathbf{p}.\mathbf{q}=\mathbf{q}.\mathbf{p}$ (propiedad conmutativa)
3. Existe $\mathbf{1}$ (el número 1) tal que $\mathbf{p}.\mathbf{1}=\mathbf{1}.\mathbf{p}=\mathbf{p}$ (elemento unidad)

Veremos que los únicos polinomios inversibles son las constantes.
Recordemos en primer lugar que el inverso multiplicativo de a es un elemento a^{-1} tal que multiplicado por a nos da la unidad, es decir $a\,.\,a^{-1} = a^{-1}\,.\,a = 1$.
En el caso de polinomios quedaría: $\mathbf{p}\ .\ \mathbf{p}^{-1} = 1$ y debe cumplirse

$$gr(\mathbf{p}\ .\ \mathbf{p}^{-1}) = gr(\mathbf{p}) + gr(\mathbf{p}^{-1}) = gr(1) = 0.$$

Como el grado de un polinomio es un número entero no negativo, la única posibilidad de que la suma sea cero es que ambos grados lo sean, es decir que $\mathbf{p}$ sea una constante.

7.2.4. Potenciación de polinomios

Se define exactamente igual que en números enteros:

$$\mathbf{p}^1 = \mathbf{p}$$
$$\mathbf{p}^{(n+1)} = \mathbf{p}.\mathbf{p}^{\mathbf{n}}$$

Ejemplo 7.8 *Sea* $\mathbf{p} : 3x^2 - 2$, *Hallar* $\mathbf{p}^3$

$\mathbf{p}^3 = \mathbf{p}^2.\mathbf{p}$

$\mathbf{p}^2 = (3x^2 - 2).(3x^2 - 2) = 9x^4 - 12x^2 + 4$

$\mathbf{p}^3 = (9x^4 - 12x^2 + 4).(3x^2 - 2) = 27x^6 - 54x^4 + 36x^2 - 8$

Observación 7.4 Algún lector detallista puede observar que no hemos hecho otra cosa que calcular el cuadrado primero y luego el cubo de un binomio, y decir, si existen fórmulas para calcular estas potencias ¿Existirán fórmulas generales para calcular las potencias de un polinomio. La respuesta es sí, pero escapa absolutamente a los objetivos de este curso y a las aplicaciones prácticas, ya que son extremadamente complicadas y el cálculo directo es más que accesible.

Observación 7.5 Hasta aquí a cada paso hemos repetido "como en los números enteros" es que el conjunto de los polinomios con las operaciones suma, producto, el 0 y el 1 conforman un *anillo conmutativo con unidad*, exactamente lo mismo que $\mathbb{Z}$ con sus correpondientes operaciones. Igual que en $\mathbb{Z}$ algunos números tienen raíces y otros no, podemos encontrar algunpos polinomios que tengan raíces y otros que no. Dado el cálculo que acabamos de hacer es claro que

$$\sqrt[3]{27x^6 - 54x^4 + 36x^2 - 8} = 3x^2 - 2$$

pero está demasiado lejos de nuestros objetivos intentarlo.

7.2.5. División de polinomios

Como dijimos antes, vamos a hacerlo exactamente igual que como dividimos números enteros

$$\begin{array}{rrl}
- & 3\,4\,1 & \multicolumn{1}{|l}{2\,3} \\ \cline{3-3}
 & 2\,3 & 1\,4 \\ \cline{2-2}
- & 1\,1\,1 & \\
 & 9\,2 & \\ \cline{2-2}
 & 1\,9 &
\end{array}$$

$$341 = 23 \times 14 = 19$$

$$19 < 23$$

Ejemplo 7.9 Dados dos polinomios:

$$\mathbf{p}: \ 6x^5 - 9x^4 + 6x^2 + 1 \text{ y}$$

$$\mathbf{q}: \ 3x^2 - 2,$$

Para hallar $\mathbf{p} : \mathbf{q}$

1. Escribimos **p** en forma completa y ordenada y **q** en forma completa.
2. Dividimos el término principal de **p** por el término principal de **q**
3. Multiplicamos este valor por **q**
4. Restamos a **p** el resultado anterior
5. Repetimos el procedimiento hasta que no sea posible la división

$$\begin{array}{llllll|l}
6x^5 & -9x^4 & +0x^3 & +6x^2 & +0x & +1 & 3x^2 \quad -2 \\ \cline{7-7}
6x^5 & & -4x^3 & & & & 2x^3 \ -3x^2 - \frac{4}{3}x \\ \cline{1-3}
 & -9x^4 & -4x^3 & +6x^2 & +0x & +1 & \\
 & -9x^4 & & +6x^2 & & & \\ \cline{2-4}
 & & -4x^3 & +0x^2 & +0x & +1 & \\
 & & -4x^3 & & +\frac{8}{3}x & & \\ \cline{3-5}
 & & & & +\frac{8}{3}x & +1 &
\end{array}$$

$$\frac{6x^5}{3x^2} = 2x^3$$

$$\frac{-9x^4}{3x^2} = -3x^2$$

$$\frac{-4x^3}{3x^2} = -\frac{4}{3}x$$

$$gr\left(\frac{8}{3}x\right) < gr(3x^2),$$

no se puede dividir.

Resulta entonces que:

$$6x^5 - 9x^4 + 6x^2 + 1 = (3x^2 - 2).(2x^3 - 3x^2 - \frac{4}{3}x) + (\frac{8}{3}x + 1)$$

donde:

$6x^5 - 9x^4 + 6x^2 + 1$ es el polinomio *dividendo*

$(3x^2 - 2)$ es el polinomio *divisor*

$2x^3 - 3x^2 - \frac{4}{3}x$ es el polinomio *cociente*

y $\frac{8}{3}x + 1$ es el polinomio *resto.*

Observación 7.6 ¿Qué relación hay entre el grado de **p**, el grado de **q** y el grado de **p:q**?
Sabemos que el cociente de potencias de igual base resta los exponentes, cuando hagamos el producto de polinomios, al dividir el término de mayor grado de **p**, con el término de mayor grado de **q**, la potencia de x será la resta de $gr(\mathbf{p})$ y $gr(\mathbf{q})$.

Es decir:

$$gr(\mathbf{p} : \mathbf{q}) = gr(\mathbf{p}) - gr(\mathbf{q})$$

Además, si $\mathbf{p} = \mathbf{q}.\mathbf{c} + \mathbf{r}$, donde **c** es el cociente y **r** es el resto, necesariamente debe cumplirse que $gr(\mathbf{r}) < gr(\mathbf{q})$

Esta operación se comporta exactamente igual que la división entera y no es casualidad que hayamos podido efectuarla. Escribámoslo formalmente:

Teorema 7.1 (Algoritmo de la división). *Dados dos polinomios* $\mathbf{f}$,$\mathbf{g} \in \mathbb{K}[X]$, *con* **g** *no nulo, existen dos únicos polinomios* **q** *y* $\mathbf{r} \in \mathbb{K}[X]$, *llamados cociente y resto respectivamente de dividir* **f** *por* **g**, *tal que* $\mathbf{f}=\mathbf{q}.\mathbf{g}+\mathbf{r}$, *donde* $gr(\mathbf{r}) < gr(\mathbf{g})$ *ó* $\mathbf{r}=\mathbf{0}$.

Demostración:

► *Existencia*

Probemos la existencia de los polinomios $\mathbf{q}$ y $\mathbf{r}$.

Si $\mathbf{f} = \mathbf{p}.\mathbf{g}$, para algún $\mathbf{p} \in \mathbb{K}[X]$, basta tomar $\mathbf{q} = \mathbf{p}$ y $\mathbf{r} = \mathbf{0}$.

Supongamos que esto no ocurre, es decir que $\mathbf{f} \neq \mathbf{p}.\mathbf{g}$ para todo $\mathbf{p} \in K[X]$.

Consideremos, entonces, el siguiente conjunto:

$$H = \{\mathbf{f} - \mathbf{p}.\mathbf{g} : \mathbf{p} \in \mathbb{K}[X]\}.$$

Claramente el polinomio nulo $\mathbf{0} \notin H$.Esto quiere decir que todos los polinomios de H tienen definido un grado. Los grados de los polinomios son números naturales y, por el *Principio de Buena Ordenación* podemos afirmar que existe un grado mínimo y, en consecuencia, en H existe al menos un polinomio, sea $\mathbf{r}$, de grado mínimo. Es decir $gr(\mathbf{r}) \leq gr(\mathbf{t})$, para todo $\mathbf{t} \in H$. Podemos escribir, entonces:

$$\mathbf{r} = \mathbf{f} - \mathbf{p}.\mathbf{g}, \text{ de donde: } \mathbf{f} = \mathbf{p}.\mathbf{g} + \mathbf{r}$$

Falta probar solamente que $gr(\mathbf{r}) < gr(\mathbf{g})$ (sabemos que $\mathbf{r} \neq \mathbf{0}$.)

Supongamos por el absurdo que $gr(\mathbf{r}) \geq gr(\mathbf{g})$

Escribamos los polinomios:

$$\mathbf{g} = b_n.x^n + b_{n-1}.x^{n-1} + \ldots + b_1.x + b_0$$

$$\mathbf{r} = r_s.x^s + r_{s-1}.x^{s-1} + \ldots + r_1.x + r_0, \quad s \geq n.$$

y consideremos:

$$\mathbf{r'} = \mathbf{r} - \frac{r_s}{b_n}.x^{s-n} \cdot \mathbf{g} \tag{7.1}$$

que es la diferencia de dos polinomios de grado s e idéntico coeficiente principal. Es decir, $\mathbf{r'}$ es cero ó $gr(\mathbf{r'}) < gr(\mathbf{r})$.
Reemplazando $\mathbf{r}$ en 7.1 tenemos:

$$\mathbf{r'} = (\mathbf{f} - \mathbf{p}.\mathbf{g}) - \frac{r_s}{b_n}.x^{s-n}.\mathbf{g} = \mathbf{f} - \left(\mathbf{p}.\mathbf{g} - \frac{r_s}{b_n}.x^{s-n}\right).\mathbf{g}.$$

Es decir, $\mathbf{r'} \in H$. Como $\mathbf{0} \notin H$ resulta $\mathbf{r'} \neq \mathbf{0}$ y por lo tanto $gr(\mathbf{r'}) < gr(\mathbf{r})$. Esto es un absurdo ya que $\mathbf{r}$ es un polinomio en h de grado mínimo.

- *Unicidad*

Probemos la unicidad del cociente y el resto usando la técnica más común:

Supongamos que $\mathbf{f} = \mathbf{p}.\mathbf{g}+\mathbf{r}$ y $\mathbf{f} = \mathbf{p'}.\mathbf{g}+\mathbf{r'}$, con $gr(\mathbf{r})$, $gr(\mathbf{r'}) < gr(\mathbf{g})$. Queremos probar que $\mathbf{p}=\mathbf{p'}$ y $\mathbf{r}=+\mathbf{r'}$. Restemos miembro a miembro:

$$\begin{array}{rcc} \mathbf{f} & = & \mathbf{p}.\mathbf{g}+\mathbf{r} \\ \mathbf{f} & = & \mathbf{p'}.\mathbf{g}+\mathbf{r'} \\ \hline \mathbf{0} & = & (\mathbf{p}\text{-}\mathbf{p'}).\mathbf{g}+(\mathbf{r}\text{ -}\mathbf{r'}) \end{array}$$

Si $\mathbf{r} - \mathbf{r'} \neq \mathbf{0}$, entonces $\mathbf{p}-\mathbf{p'} \neq \mathbf{0}$. Luego $gr(\mathbf{r} - \mathbf{r'}) = gr(\mathbf{p}-\mathbf{p'}) + gr(\mathbf{g})$. Por otra parte, sabemos que $gr(\mathbf{r} - \mathbf{r'}) \leq max(gr(\mathbf{r}\ ,\mathbf{r'}) < gr(\mathbf{g})$. Esta contradicción provino de suponer que $\mathbf{r} - \mathbf{r'} \neq \mathbf{0}$, en consecuencia debe ser $\mathbf{r} - \mathbf{r'} = \mathbf{0}$, lo que nos lleva a ver que $\mathbf{p}-\mathbf{p'} = \mathbf{0}$ y concluir: $\mathbf{r}=\mathbf{r'}$, $\mathbf{p}=\mathbf{p'}$. □

7.3. Divisibilidad

Desde el inicio estamos afirmando que los polinomios se comportan como los enteros y acabamos de probar el algoritmo de la división. Reescribamos la teoría de la divisibilidad en $\mathbb{K}[X]$, en forma similar a la dada en $\mathbb{Z}$.

Definición 7.1 *Dados dos polinomios $f(x), g(x) \in \mathbb{K}[X]$, se dice que $f(x)$ divide a $g(x)$ si existe un polinomio $h(x) \in \mathbb{K}[X]$ tal que $g(x) = h(x) \cdot f(x)$. Se escribe* $\mathbf{f}|\mathbf{g}$.

Ejemplo 7.10 $f(x) = x - 1$ divide a $g(x) = x^3 - x^2 + x - 1$, ya que $x^3 - x^2 + x - 1 = (x^2 + 1) \cdot (x - 1)$.

Proposición 7.4

1. *Si $\mathbf{f} \neq \mathbf{0}$, entonces $\mathbf{f}|\mathbf{g}$ si y sólo si el resto de dividir $g(x)$ por $f(x)$ es cero.*
2. $\mathbf{f}|\mathbf{0}$ *para todo $f(x) \in \mathbb{K}[X]$.*
3. $\mathbf{f}|\mathbf{f}$ *para todo $f(x) \in \mathbb{K}[X]$.*
4. *Si $k \in \mathbb{K}$, $k \neq 0$, y $f(x) \in \mathbb{K}[X]$, entonces $k|\mathbf{f}$.*
5. *Si $\mathbf{f}|\mathbf{g}$ y $\mathbf{g}|\mathbf{h}$, entonces $\mathbf{f}|\mathbf{h}$.*
6. *Si $\mathbf{f}|\mathbf{g}$ y $\mathbf{f}|\mathbf{h}$, entonces $\mathbf{f}|\mathbf{p} \cdot \mathbf{g} + \mathbf{q} \cdot \mathbf{h}$ para todo $\mathbf{p}, \mathbf{q} \in \mathbb{K}[X]$.*
7. *Si $\mathbf{f}|\mathbf{g}$ y $\mathbf{g}(x) \neq \mathbf{0}$, entonces $gr\ f(x) \leq gr\ g(x)$.*
8. $\mathbf{f}|\mathbf{g}$ *y* $\mathbf{g}|\mathbf{f}$ *si y sólo si $f(x)$ y $g(x)$ difieren en una constante no nula.*

Demostración: Las demostraciones de estas propiedades (totalmente análogas a las de divisibilidad de enteros) no guardan ningún secreto y pueden ser felizmente llevadas a cabo por el lector interesado. ®) □

Definición 7.2 *Dados dos polinomios* $\mathbf{f} = f(x)$ *y* $\mathbf{g} = g(x)$*, un polinomio* $\mathbf{d} = d(x)$ *se llama un* máximo común divisor *de* $f(x)$ *y* $g(x)$ *y se nota* $\mathbf{d} = (\mathbf{f}, \mathbf{g})$ *si se verifica que:*

1. $\mathbf{d}|\mathbf{f}$ *y* $\mathbf{d}|\mathbf{g}$.
2. *Si* **d'** *es un polinomio tal que* **d'**$|\mathbf{f}$ *y* **d'**$|\mathbf{g}$*, entonces* **d'**$|\mathbf{d}$.

Observación 7.7 Si $d_1(x)$ y $d_2(x)$ son dos m.c.d. de $f(x)$ y $g(x)$, por la propiedad 7.4 8), $d_1(x)$ y $d_2(x)$ difieren en una constante. Si se considera el m.c.d. mónico, entonces es único.

Análogamente a lo que sucede en $\mathbb{Z}$, es posible aplicar el algoritmo de Euclides para calcular el máximo común divisor de dos polinomios $f(x)$ y $g(x)$.

7.3.1. Algoritmo de Euclides.

Dados dos polinomios no nulos $f(x)$ y $g(x)$, para hallar el máximo común divisor se procede casi exactamente igual al proceso con números enteros. La diferencia primordial es que si en el camino obtenemos un resto no mónico sacamos factor común el coeficiente principal y seguimos trabajando con polinomios mónicos como se ve en el siguiente ejemplo:

Ejemplo 7.11 Hallar el m.c.d. de los polinomios

$f(x) = x^5 - 5x^4 - 5x^3 - 10x + 27$ y
$g(x) = x^4 - 4x^3 - 9x^2 - 9x - 17.$

	$x \quad -5$	$x \quad +2$	$x \quad -1$
$x^5-4x^4-3x^3-12x^2-10x-8$	$x^4+x^3+3x^2+2x+2$	x^3-x^2+2x-2	x^2+2
$x^5+x^4+3x^3+2x^2+2x$	$x^4-x^3+2x^2-2x$	x^3+2x	
$-5x^4-6x^3-14x^2-12x$-8	$2x^3+x^2+4x+2$	$-x^2$ -2	
$-5x^4-5x^3-15x^2-10x$-10	$2x^3-2x^2+4x$-4	$-x^2$ -2	
$-x^3+x^2-2x+2$	$3x^2+6$	0	
$-(x^3-x^2+2x$ -2)	$3(x^2+2)$		

El último resto no nulo, mónico es x^2+2, en consecuencia $(\mathbf{f},\mathbf{g}) = x^2+2$.

Igual que con números enteros podemos escribir al polinomio máximo común divisor como combinación polinómica de los polinomios dados: (No hay que olvidar las constantes que dejamos en el camino.)

$x^2+2 = \frac{1}{3}(3x^2+6)$

$3x^2+6 = \mathbf{g} - (x^3-x^2+2x).(x+2)$

$-(x^3-x^2+2x) = \mathbf{f} - \mathbf{g}.(x-5) =$ Reemplazando sucesivamente obtenemos:

$x^2+2 = \frac{1}{3}(\mathbf{g} - (\mathbf{f} - \mathbf{g}.(x-5)).(x+2)) = \left(-\frac{1}{3}x - \frac{2}{3}\right)\mathbf{f} + \left(\frac{x^2}{3} - x - \frac{5}{3}\right)\mathbf{g}$

¿Qué ocurre si alguno de los dos polinomios es cero? ®

7.3.2. Polinomios irreducibles

Así como vimos que existen "ladrillos" para construir los números enteros (los enteros primos), vamos en busca de los "ladrillitos para polinomios". El cero es el polinomio cero, en $\mathbb{Z}$ los únicos inversibles son el 1 y el -1, en $\mathbb{K}[X]$ vimos que los únicos inversibles son las constantes no nulas (es decir $\mathbb{K}\setminus\{0\}$) y los "ladrillitos para polinomios" serán los *irreducibles* de $\mathbb{K}[X]$

Definición 7.3 Un polinomio no constante $f(x) \in \mathbb{K}[X]$ se dice *irreducible* o *primo* en $\mathbb{K}[X]$ si no se puede expresar como producto de dos polinomios no constantes de $\mathbb{K}[X]$.

Definición 7.4 Un polinomio no constante $f(x) \in \mathbb{K}[X]$ se dice *irreducible* o *primo* en $\mathbb{K}[X]$ si los únicos divisores de $f(x)$ en $\mathbb{K}[X]$ son las constantes no nulas y los polinomios $k \cdot f(x)$, $k \in \mathbb{K}$, $k \neq 0$.

Observación 7.8 Las definiciones 7.3 y 7.4 son equivalentes. Su misión, lector interesado, si decide aceptarla, será demostrar este hecho. ®

Ejemplo 7.12 1. x^2-5 no es irreducible en $\mathbb{R}[X]$.
En efecto: $x^2-5 = (x-\sqrt{5})(x+\sqrt{5})$

2. $x^2 - 5$ es irreducible en $\mathbb{Q}[X]$.
   Si no lo fuera, sería producto de dos polinomios mónicos de grado 1:
   $x^2 - 5 = (x + a)(x + b)$, a, $b \in \mathbb{Q}$.
   Luego: $x^2 - 5 = x^2 + (a + b)x + ab$.
   De donde: $ab = -5$ y $a + b = 0$.
   De aquí resulta: $a = -b$ y $b^2 = 5$, que no tiene solución en $\mathbb{Q}$.
3. Todo polinomio de grado 1 en $\mathbb{K}[X]$ es irreducible.

Definición 7.5 Dos polinomios $f(x)$ y $g(x)$ se dicen *relativamente primos* si ($\mathbf{f}$,$\mathbf{g}$)=1.

Proposición 7.5 *Dados $f(x)$, $g(x)$ y $h(x) \in \mathbb{K}[X]$.*

1. *Si $\mathbf{f}|\mathbf{g} \cdot \mathbf{h}$ y $(\mathbf{f}, \mathbf{g}) = 1$, entonces $\mathbf{f}|\mathbf{h}$.*

1. *Si $\mathbf{f}$ es irreducible y $\mathbf{f}|\mathbf{g} \cdot \mathbf{h}$, entonces $\mathbf{f}|\mathbf{g}$ ó $\mathbf{f}|\mathbf{h}$.*
1. *Si $\mathbf{f}|\mathbf{h}$, $\mathbf{g}|\mathbf{h}$ y $(\mathbf{f}, \mathbf{g}) = 1$, entonces $\mathbf{f} \cdot \mathbf{g}|\mathbf{h}$*

Demostración: :
Gentilmente cedida al lector interesado, dado que se trata simplemente de reescribir las demostraciones dadas en divisibilidad de enteros. ®

Teorema Fundamental de la Aritmética en $\mathbb{K}[X]$

Teorema 7.2 *Todo elemento $f(x) \in \mathbb{K}[X]$ no constante, puede escribirse en la forma:*

$$\mathbf{f} = k \cdot \mathbf{p}_1^{e_1} \cdot \mathbf{p}_2^{e_2} \cdot \ldots \cdot \mathbf{p}_s^{e_s},$$

donde $k \in \mathbb{K}$, $\mathbf{p}_i$ son polinomios irreducibles mónicos distintos en $\mathbb{K}[X]$ y $e_i \in \mathbb{N}$. Esta factorización es única salvo el orden de los factores.

Demostración: Para probar la existencia de la factorización, haremos inducción sobre $n = gr\ f(x)$. (Utilizaremos la segunda forma del principio de inducción o inducción fuerte.)
Si $n = 1$, entonces $f(x) = a_1x + a_0$. Entonces $f(x) = a_1\left(x + \dfrac{a_0}{a_1}\right)$, y el polinomio $\boldsymbol{p}_1(X) = x + \dfrac{a_0}{a_1}$ es irreducible mónico en $\mathbb{K}[X]$.
Sea $n > 1$ y supongamos que la factorización existe para todo polinomio no constante de grado menor que n.
Tenemos que ver que $f(x)$ puede factorizarse en la forma indicada.

Si $f(x)$ es irreducible con coeficiente principal a_n, entonces

$$f(x) = a_n \left(\frac{1}{a_n} \cdot f(x) \right),$$

y se tiene la factorización buscada.

Si $f(x)$ no es irreducible, entonces $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in \mathbb{K}[X]$ no constantes y $gr\ g(x) < gr\ f(x)$, $gr\ h(x) < gr\ f(x)$. Por la hipótesis inductiva, $g(x)$ y $h(x)$ se pueden expresar como producto de una constante por polinomios irreducibles mónicos, y por lo tanto, lo mismo sucede con $f(x)$.

Hemos probado la existencia de la descomposición con la misma idea original de Gauss para la demostración del teorema en $\mathbb{Z}$. La unicidad tamién se prueba en forma análoga y el lector astuto ya estará sospechando que queda a su cargo. Ⓡ. □

Ejemplo 7.13 Consideremos el polinomio

$$f(x) = 3x^{10} - 15x^9 + -9x^8 + 51x^7 - 6x^6 - 144x^5 - 60x^4 - 168x^3$$

y factoricémoslo en $\mathbb{Q}[X], \mathbb{R}[X]$ y $\mathbb{C}[X]$:

En $\mathbb{Q}[X]$:
$$3 \cdot x^3 \cdot (x-5) \cdot (x+1)^2 \cdot (x^2-2) \cdot (x^2-2x+2).$$

En $\mathbb{R}[X]$:
$$3 \cdot x^3 \cdot (x-5) \cdot (x+1)^2 \cdot (x-\sqrt{2}) \cdot (x+\sqrt{2}) \cdot (x^2-2x+2).$$

En $\mathbb{C}[X]$:
$$3 \cdot x^3 \cdot (x-5) \cdot (x+1)^2 \cdot (x-\sqrt{2}) \cdot (x+\sqrt{2}) \cdot (x-(1+i)) \cdot (x-(1-i)).$$

7.3.3. Raíces

Si pensamos un polinomio $f(x) \in \mathbb{K}[X]$ como una función $f : \mathbb{K} \to \mathbb{K}$ vemos que para cada $a \in \mathbb{K}$ existe $f(a) \in \mathbb{K}$. Llamamos a este valor *especialización* o *valor numérico* de **f** en a.

Ejemplo 7.14 Sea $f(x) = x^2 - 2x + 2$.

Entonces:

$f(2) = 2$, $f(-1) = 5$, $f(1) = 1$, $f(-\sqrt{2}) = 4+2\sqrt{2}$, $f(i) = 1-2i$, $f(1+i) = 0$.

En el ejemplo anterior hemos encontrado un valor de $a \in \mathbb{K}$ para el que $f(a) = 0$. Además el polinomio es de grado 2, es decir, para todos conocido (al menos eso espero) que se trata de una parábola y llamábamos raíces de la parábola a los valores de $x \in \mathbb{R}$ para los que $f(x) = 0$. Esto no es privativo de las parábolas ni de los números reales. De hecho, $1 + i$ es una raíz de $f(x) = x^2 - 2x + 2$. Escribamos la definición formal:

Definición 7.6 Dado $f(x) \in \mathbb{K}[X]$ una constante $a \in \mathbb{K}$ es una *raíz* de $f(x)$, si $f(a) = 0$.

Claramente, si un polinomio es divisible por otro, el resto de la división es cero. Seguidamente veremos un teorema que afirma que en general el valor del resto al dividir un polinomio por $x-a$ es el valor de la función polinómica en a, es decir: $f(a)$.

Teorema del resto

Teorema 7.3 *Sea $f(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \ldots + a_2\, x^2 + a_1\, x + a_0$ una función polinómica de grado n, entonces el resto de dividir $f(x)$ por $x - a$ es $f(a)$.*

Demostración: Sabemos que $f(x) = c(x)(x - a) + r(x)$, donde $c(x)$ es el cociente y $r(x)$ el resto de la división.

Como $r(x)$ es el resto, debe ser: $gr(r) < gr((x-a)) = 1$, de donde $gr(r) = 0$, es decir, $r(x) = k$ (el polinomio es un número en $\mathbb{K}$.)

Resulta entonces que la función polinómica $f(x)$ es $f(x) = c(x)(x - a) + k$

Calculemos el valor de esta función para $x = a$:

$$f(a) = c(a)(a - a) + k$$

Sea lo que sea el valor de $c(a)$ al multiplicarlo por $a - a = 0$ se anula y queda $f(a) = k$, es decir, el valor de la función polinómica $f(x)$ en el punto $x = a$ es igual al resto de dividir $f(x)$ por $(x - a)$ $\square$

Corolario 7.1 *En las condiciones del teorema, si a es raíz de $f(x)$ resulta que $f(x)$ es divisible por $(x - a)$.*

Veamos en un ejemplo, cuál es el proceso de dividir por $x - a$.

Sea $f(x) = x^4 - 3x^2 + 5$, vamos a dividirlo por $x - 1$ (es decir, $a = 1$)

$$
\begin{array}{rrrrr|l}
x^4 & +0x^3 & -3x^2 & +0x & +5 & x\ -2 \\ \cline{6-6}
x^4 & -2x^3 & & & & x^3\ -3x^2\ +x\ \ +2 \\ \cline{1-3}
 & 2x^3 & -3x^2 & +0x & +5 & \\
 & 2x^3 & -4x^2 & & & \\ \cline{2-4}
 & & x^2 & +0x & +5 & \\
 & & x^2 & -2x & & \\ \cline{3-5}
 & & & 2x & +5 & \\
 & & & 2x & -4 & \\ \cline{4-5}
 & & & & 9 &
\end{array}
$$

¿Cuáles han sido los cálculos?

El coeficiente principal de $x-2$ es 1, entonces al dividir resulta el coeficiente principal de $c(x)$ igual al de $p(x)$.
Luego el número obtenido se multiplica por (-2) y se resta al coeficiente "que sigue". Multiplicar por (-2) y restar es lo mismo que multiplicar por 2 y sumar.

Este procedimiento se escribe abreviadamente en una criba denominada *regla de Ruffini* del siguiente modo:

$$p(x) = x^4 - 3x^2 + 5,$$

en forma completa y ordenada:

$$p(x) = x^4 + 0x^3 - 3x^2 + 0x + 5.$$

En primer lugar se copian los coeficientes en forma completa y ordenada en orden decreciente hasta el término de menor grado (no es necesario que sea el término independiente).

Vamos a dividir por $x - 2$, entonces escribimos 2 a la izquierda:

$$
\begin{array}{c|ccccc}
 & 1 & 0 & -3 & 0 & 5 \\
2 & & & & & \\ \hline
 & & & & &
\end{array}
$$

Preparada así la criba, comenzamos los cálculos: al dividir no varía, entonces: "bajo el primero"

$$
\begin{array}{c|ccccc}
 & 1 & 0 & -3 & 0 & 5 \\
2 & & & & & \\ \hline
 & 1 & & & &
\end{array}
$$

multiplico por 2, lo escribo arriba y sumo:

$$\begin{array}{c|ccccc} & 1 & 0 & -3 & 0 & 5 \\ 2 & & 2 & & & \\ \hline & 1 & 2 & & & \end{array}$$

multiplico por 2, lo escribo arriba y sumo:

$$\begin{array}{c|ccccc} & 1 & 0 & -3 & 0 & 5 \\ 2 & & 2 & 4 & & \\ \hline & 1 & 2 & 1 & & \end{array}$$

multiplico por 2, lo escribo arriba y sumo:

$$\begin{array}{c|ccccc} & 1 & 0 & -3 & 0 & 5 \\ 2 & & 2 & 4 & 2 & \\ \hline & 1 & 2 & 1 & 2 & \end{array}$$

multiplico por 2, lo escribo arriba y sumo:

$$\begin{array}{c|ccccc} & 1 & 0 & -3 & 0 & 5 \\ 2 & & 2 & 4 & 2 & 4 \\ \hline & 1 & 2 & 1 & 2 & 9 \end{array}$$

Volviendo a colocar las potencias de la variable en forma decreciente y comenzando un grado menor al de $p(x)$ obtenemos que

$$x^3 + 2x^2 + x + 2$$

es el cociente de dividir $p(x) = x^4 + 0x^3 - 3x^2 + 0x + 5$ por $x - 2$, y el resto 9.

Aplicación del teorema del resto: el sexto caso de factoreo

La pregunta es: ¿$x^n + 3^n$ es divisible por $x + 3$? ¿y por $x - 3$? ¿qué pasa con $x^n - 3^n$? todas estas preguntas tienen una respuesta muy sencilla aplicando el teorema del resto.

Supongamos que $a > 0$ y consideremos el polinomio $f(x)$. Que $f(x)$ sea divisible por $x - a$ quiere decir que el resto de dividir $f(x)$ por $x - a$ es 0, y por el teorema del resto, quiere decir que $f(a) = 0$. Del mismo modo, para ver si es divisible por $x + a$ debemos ver que $f(-a) = 0$. El sexto caso de factoreo dice, si $a > 0$:

$x^n - a^n$ siempre es divisible por $x - a$

$x^n + a^n$ nunca es divisible por $x - a$

$x^n - a^n$ es divisible por $x + a$, sólo si n es par

$x^n + a^n$ es divisible por $x + a$, sólo si n es impar

Dejamos al lector completar los detalles de la demostración. ®

Observación 7.9 Si logramos encontrar a, raíz de $p(x)$ una función polinómica de grado n, dividimos $f(x)$ por $x-a$ y encontramos una función polinómica $f_{(1)}$ de grado $n-1$, si hallamos b una raíz de $f_{(1)}$, lo dividimos por $(x-b)$ y encontramos $f_{(2)}$ de grado $n-2$ y así sucesivamente hasta llehar a $f_{(n-1)}$ de grado 1, y factorizar por completo $f(x)$. Ésta es, justamente, la importancia de hallar las raíces.
En este proceso las sucesivas raíces encontradas no son necesariamente diferentes. Si a es raíz de un polinomio $f(x)$, sabemos que $f(x)$ es divisible por $x-a$, es decir $f(x)=(x-a)\cdot f_{(1)}(x)$. Si $f_{(1)}(x)$ también es divisible por $(x-a)$, resulta $f_{(1)}(x)=(x-a)\cdot f_{(2)}(x)$ y $f(x)=(x-a)^2\cdot f_{(2)}(x)$, y el proceso puede continuar.

Definición 7.7 Si a es raíz de un polinomio $f(x)$ y k es el mayor número natural tal que $f(x)$ es divisible por $(x-a)^k$, decimos que a es una raíz múltiple de orden k. Si $k=1$ decimos que a es una *raíz simple*. El *orden de multiplicidad* de una raíz se puede hallar aplicando la regla de Ruffini.

Ejemplo 7.15 Verificar que 2 es una raíz del polinomio

$$f(x)=x^5-6x^4+11x^3-2x^2-12x+8,$$

y hallar su orden de multiplicidad.

$$\begin{array}{c|cccccc}
 & 1 & -6 & 11 & -2 & -12 & 8 \\
2 & & 2 & -8 & 6 & 8 & -8 \\
\hline
 & 1 & -4 & 3 & 4 & -4 & 0 \\
2 & & 2 & -4 & -2 & 4 & \\
\hline
 & 1 & -2 & -1 & 2 & 0 & \\
2 & & 2 & 0 & -2 & & \\
\hline
 & 1 & 0 & -1 & 0 & & \\
2 & & 2 & 4 & & & \\
\hline
 & 1 & 2 & 3\neq 0 & & &
\end{array}$$

El orden de multiplicidad es 3. Recostruyamos el polinomio, siguiendo cada instancia de la regla de Ruffini:

$$f(x)=x^5-6x^4+11x^3-2x^2-12x+8=$$
$$f(x)=(x-2)\cdot(x^4-4x^3+3x^2+4x-4)=$$
$$f(x)=(x-2)^2\cdot(x^3-2x^2-x+2)=$$

$$f(x) = (x-2)^3 \cdot (x^2-1)$$

Conocemos la factorización de $(x^2 - 1)$, ya que se trata simplemente de una diferencia de cuadrados y podemos escribir:

$$f(x) = (x-2)^3 \cdot (x-1) \cdot (x+1)$$

De este modo encontramos 5 raíces de $f(x)$: 2 de orden 3 y 1 y -1 que son raíces simples.

Formalicemos lo que hemos comentado hasta ahora:

Teorema 7.4 *Si $f(x) \in \mathbb{K}[X]$ es un polinomio de grado $n \geq 1$, entonces $f(x)$ tiene a lo sumo n raíces en $\mathbb{K}$.*

Demostración: Demostraremos usando inducción sobre el grado del polinomio.
Si gr $f(x) = 1$, entonces $f(x) = a_0 + a_1 x$, y su única raíz r es $r = -\dfrac{a_0}{a_1}$.
Supongamos que el teorema vale para todos los polinomios de grado $n-1$.
Sea $f(x)$ un polinomio de grado n.
Debemos contemplar dos casos: que tenga alguna raíz o que no tenga ninguna.

Caso 1: $f(x)$ no tiene ninguna raíz.

No hay nada que demostrar, ya que $0 < 1$.

Caso 2: $f(x)$ tiene una raíz r.

Por el corolario del Teorema del resto, es $f(x) = (x-r) \cdot q(x)$, con gr $q(x) = n-1$. De aquí resulta que toda raíz de $q(x)$ es raíz de $f(x)$, y recíprocamente, una raíz de $f(x)$ es r ó una raíz de $q(r)$, por lo tanto, las raíces de $f(x)$ son r y las raíces de $q(x)$. Pero $q(x)$ tiene grado menor que n y por la hipótesis de inducción resulta que tiene a lo sumo $n-1$ raíces . Por lo tanto, $f(x)$ tiene a lo suma n raíces. $\square$

Teorema Fundamental del Algebra.

Teorema 7.5 *Todo polinomio no constante con coeficientes en $\mathbb{C}$, tiene por lo menos una raíz en $\mathbb{C}$.*

Lamentablemente no demostrastraremos este teorema porque necesita “algunos elementos” de funciones de variable compleja.

Corolario 7.2 *Todo polinomio no constante con coeficientes en $\mathbb{C}$, tiene exactamente n raíces en $\mathbb{C}$ (contando cada raíz tantas veces como su orden de multiplicidad).*

Demostración: Si $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \;\; a_n \neq 0$, por el teorema7.5, $f(x)$ tiene una raíz, digamos r_1 en $\mathbb{C}$. Luego

$$f(x) = (x - r_1) \cdot q_1(x), \text{ con gr } q_1(x) = n - 1.$$

Nuevamente, por el teorema7.5, $q_1(x)$ tiene una raíz r_2 en $\mathbb{C}$. Luego

$$q_1(x) = (X - r_2) \cdot q_2(x), \text{ con gr } q_2(x) = n - 2.$$

y entonces

$$f(x) = (x - r_1) \cdot (x - r_2) \cdot q_2(x).$$

Iterando el procedimiento, al cabo de n pasos tenemos:

$$f(x) = (x - r_1) \cdot (x - r_2) \cdot (x - r_3) \cdot \ldots \cdot (x - r_n) \cdot a_n$$

y $f(x)$ tiene raíces $r_1, r_2, \ldots, r_n$, o sea, exactamente n raíces en $\mathbb{C}$. □

Corolario 7.3 *Los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de primer grado.*

Demostración: Resulta de la demostración del Teorema anterior que todo polinomio $f(x)$ no constante es el producto de su coeficiente principal por polinomios $x - r_1$, $x - r_2$, ..., $x - r_n$, donde $r_1, r_2, \ldots, r_n$ son las raíces de $f(x)$ en $\mathbb{C}$.

Como todo polinomio de grado 1 es irreducible, esta es la factorización de $f(x)$ en factores irreducibles en $\mathbb{C}[X]$. □

(✠) Un poco de historia del **FTA**, es decir del teorema fundamental del álgebra:

La primera observación es que existen muchas formulaciones equivalentes del FTA. Una de ellas: "Cada polinomio real puede ser expresado como producto de factores lineales reales o cudráticos reales."
Los primeros trabajos (circa 800 d.C.) se deben a Al-Khwarizmi, quien sólo buscaba raíces positivas.
Cardano fue el primero en darse cuenta que se podía trabajar con cantidades

más generales que los números reales, como vimos en el comienzo del capítulo de complejos.
Descartes en 1637 dijo que uno puede imaginar para cada ecuación de grado n, n raíces pero que estas raíces podían no corresponder con cantidad real alguna.
En 1746, D'Alembert hizo el primer intento serio de demostración del FTA, pero usando un lema sin demostración que no fue comprobado hasta 1851, por Puiseau. No obstante, sus ideas son importantes.
Al poco tiempo, Euler fue capaz de probar que todo polinomio real con grado, $n < 7$, tiene exactamente n raíces complejas. En 1749, intentó una demostración del caso general, que aparece en *Recherches sur les racines imaginaires des équations*, basada en descomponer un polinomio mónico reducido en el producto de dos polinomios mónicos de grados iguales.
En 1772, Lagrange planteó objeciones a la demostración de Euler.
En 1795, Laplace trató de probar el FTA usando el discriminante de un polinomio. Su demostración era muy elegante solo que de nuevo suponía la existencia de las raíces.
A Gauss se le concede el crédito de la primera demostración del FTA, en su tesis doctoral de 1799. Esta primera demostración de Gaus es en esencia topológica y tiene serios inconvenientes.
En 1814, el contable suizo Jean Robert Argand publicó una demostración del FTA que posiblemente sea la más simple de todas. (Nuevamente la simpleza de Argand.) Argand había esquematizado esas ideas en *Essai sur une manière de représenter les quantitiés imaginaires dans les constructions géometriques* interpretando la unidad imaginaria i como un giro de 90° en el plano, haciendo surgir lo que llamamos plano de Argand o diagrama de Argand.
En 1820, Cauchy le dedicó un capítulo completo de su *Cours d'analyse* a la demostración de Argand (aunque sorprendentemente no lo nombra).
En 1816, Gauss dio una nueva demostración que completa la de Euler y es correcta. Un tercer intento de Gauss, también en 1816 es, como la primera, de naturaleza topológica. Gauss introduce en 1831 el término *número complejo*y en 1821, Cauchy ya había introducido el término *conjugado*.
En 1849, 50 años después de su primer intento, Gauss produjo la primera demostración del enunciado general de que una ecuación de grado n con coeficientes complejos tiene n raíces complejas.
¡Y a veces uno se siente frustrado porque no le sale un ejercicio en los primeros 5 minutos!.

Teorema 7.6 *Si $z \in \mathbb{C}$ es una raíz compleja de un polinomio $f(x) \in \mathbb{R}[X]$ (es decir, polinomio a coeficientes reales), $\overline{z}$ también es raíz de $f(x)$. Además, z y $\overline{z}$ tienen el mismo orden de multiplicidad.*

Demostración: Esta demostracón es muy sencilla si recordamos:

(c_1) $\overline{z} \cdot \overline{z'} = \overline{z \cdot z'}$,

(c_2) $\overline{z}^n = \overline{z^n}$,

(c_3) $\overline{z} + \overline{z'} = \overline{z + z'}$,

(c_4) $z = \overline{z}$ si y sólo si $z \in \mathbb{R}$.

Sea $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, con $a_i \in \mathbb{R}$.
Entonces

$$\begin{array}{rcl} f(\overline{z}) & = & a_n \overline{z}^n + a_{n-1} \overline{z}^{n-1} + \ldots + a_1 \overline{z} + a_0 = \\ & \overset{(c_2)}{=} & a_n \overline{z^n} + a_{n-1} \overline{z^{n-1}} + \ldots + a_1 \overline{z} + a_0 = \\ & \overset{(c_4)}{=} & \overline{a_n} \overline{z^n} + \overline{a_{n-1}} \overline{z^{n-1}} + \ldots + \overline{a_1} \overline{z} + \overline{a_0} = \\ & \overset{(c_1)}{=} & \overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \ldots + \overline{a_1 z} + \overline{a_0} = \\ & \overset{(c_3)}{=} & \overline{a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0} = \overline{f(z)} \end{array}$$

Hemos probado que $f(\overline{z}) = \overline{f(z)}$, entonces si z es raíz de $f(x)$, resulta $f(z) = 0$, y enconsecuencia, $f(\overline{z}) = 0$. Luego, $\overline{z}$ es raíz de $f(X)$.
Veamos que z y $\overline{z}$ tienen el mismo orden de multiplicidad. Supongamos que el orden de multiplicidad de z es k y el orden de multiplicidad de $\overline{z}$ es k', y supongamos que $k > k'$.
Observemos que $(x - z)(x - \overline{z}) = (x - (a + b\ i))\,(x - (a - b\ i)) = x^2 - 2ax + (a^2 + b^2)$.
Se tiene que $f(x)$ es divisible por $(x - z)^{k'}$ y por $(x - \overline{z})^{k'}$, esto es, es divisible por $\left((x - z)(x - \overline{z})\right)^{k'} = \left(x^2 - 2ax + (a^2 + b^2)\right)^{k'}$ que tiene coeficientes reales.

Luego $f(x) = \left(x^2 - 2ax + (a^2 + b^2)\right)^{k'} \cdot g(x)$, con $g(x) \in \mathbb{R}[X]$.
Ahora, z es raíz de $g(x)$ de orden de multiplicidad $k - k' > 0$ y $g(x)$ tiene coeficientes reales. Pero $\overline{z}$ no es raíz de $g(x)$.

Esto es una contradicción que provino de suponer $k \neq k'$. $\square$

Corolario 7.4 *Todo polinomio* $\mathbb{R}[X]$*, de grado impar, tiene al menos una raíz real.*

La bella demostración de este hecho queda en manos de la no menos bella imaginación del lector entusiasta. ®

Ejemplo 7.16 Hallar todas las raíces de $f(x) = x^4 - 2x^3 - 3x^2 + 10x - 10$, sabiendo que $1 + i$ es una raíz del mismo.
Como $1 + i$ es raíz de $f(x) \in \mathbb{R}$, también lo es $1 - i$.
Esto quiere decir que $f(x)$ es divisible por $(x - (1 + i))$ y por $(x - (1 - i))$.
Por lo tanto $f(x)$ es divisible por $(x - (1 + i)).(x - (1 - i))$,
o lo que es lo mismo, $f(x)$ es divisible por $(x^2 - 2x + 2)$.
Si realizamos el cociente obtenemos: $f(x) = (x^2-2x+2)\cdot(x^2-5)$ y aplicando diferencia de cuadrados llegamos a la descomposición:

En $\mathbb{Q}[X]$: $f(x) = (x^2 - 2x + 2) \cdot (x^2 - 5)$
En $\mathbb{R}[X]$: $f(x) = (x^2 - 2x + 2) \cdot (x - \sqrt{5}) \cdot (x + \sqrt{5})$
En $\mathbb{C}[X]$: $f(x) = (x - (1 + i)) \cdot (x - (1 - i)) \cdot (x - \sqrt{5}) \cdot (x + \sqrt{5})$

Este ardid para evitar aplicar la regla de Ruffini con números complejos es válido, pero no necesario. Efectivamente, podríamos haber hecho:

$$\begin{array}{r|lrrrr}
 & 1 & -2 & -3 & 10 & -10 \\
1+i & & 1+i & -2 & -5-5\,i & 10 \\
\hline
 & 1 & -1+i & -5 & 5-5\,i & 0 \\
1-i & & 1-i & 0 & -5+5\,i & \\
\hline
 & 1 & 0 & -5 & 0 &
\end{array}$$

Y continuar igual que en el procedimiento anterior.

Corolario 7.5 *En $\mathbb{R}[X]$, los únicos polinomios irreducibles son los de grado 1 y los de segundo grado de la forma $a(x^2 + bx + c)$, con $b^2 - 4c < 0$.*

Demostración: Del teorema 9.9 resulta que si $f(x)$ es un polinomio con coeficientes reales y si $z = a + b\ i$ es raíz de $f(x)$, entonces $f(x)$ es divisible por $x - z$ y por $x - \overline{z}$. Entonces $f(x)$ es divisible por

$$(x - z) \cdot (x - \overline{z}) = x^2 - (z + \overline{z})x + z \cdot \overline{z} = x^2 - 2ax + (a^2 + b^2) = x^2 + px + q$$

que es un polinomio con coeficientes reales tal que $p^2 - 4q < 0$ (discriminante negativo), como se verifica sin dificultad. Entonces, si $f(x)$ es no constante, $c_1, c_2, \ldots, c_r$ son todas sus raíces reales y $z_1, \overline{z_1}, z_2, \overline{z_2}, \ldots, z_s, \overline{z_s}$, son todas sus raíces complejas $(r + 2s = n)$, entonces $f(x)$ se descompone en factores irreducibles en $\mathbb{R}[X]$ en la forma

$$f(x) = a_n(x - c_1) \ldots (x - c_r)(x^2 + p_1x + q_1) \ldots (x^2 + p_sx + q_s).$$

$\square$

7.4. Relación entre las raíces de un polinomio y sus coeficientes

Sabemos que podemos escribir un polinomio como suma o descomponerlo en producto de polinomios irreducibles mónicos, es decir:

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

o bien:

$$f(x) = a_n \cdot (x - r_1) \cdot (x - r_2) \cdot (x - r_3) \cdot \ldots \cdot (x - r_n)$$

Vemos que la constante por la que se multiplican los polinomios mónicos es a_n, y es claro que alguna relación debe de haber entre los a_i restantes y las r_i, $1 \leq i \leq n-1$. Hagamos algunas cuentas:

$n = 1$

$$f(x) = a_1 x + a_0 = a_1(x - r_1) = a_1 x - a_1 \cdot r_1$$

Vemos que:

$$a_0 = -a_1 \cdot r_1 \qquad -\frac{a_0}{a_1} = r_1$$

$n = 2$

$$f(x) = a_2x^2 + a_1x + a_0 = a_2(x-r_1)(x-r_2) = a_2x^2 - a_2(r_1+r_2)x + a_2 \cdot r_1 \cdot r_2$$

Vemos que:

$$\begin{array}{ll} a_0 = a_2 \cdot r_1 \cdot r_2 & \dfrac{a_0}{a_2} = r_1 \cdot r_2 \\ a_1 = -a_2(r_1 + r_2) & -\dfrac{a_1}{a_2} = r_1 + r_2 \end{array}$$

$n = 3$

$$f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = a_3(x - r_1)(x - r_2)(x - r_3) =$$

$$= a_3x^3 - a_3(r_1 + r_2 + r_3)x + a_3(r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3) - a_3 \cdot r_1 \cdot r_2 \cdot r_3$$

Vemos que:

$$\begin{array}{ll} a_0 = -a_3 \cdot r_1 \cdot r_2 \cdot r_3 & -\dfrac{a_0}{a_3} = r_1 \cdot r_2 \cdot r_3 \\ a_1 = a_3(r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3) & \dfrac{a_1}{a_3} = r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 \\ a_2 = -a_3(r_1 + r_2 + r_3) & -\dfrac{a_2}{a_3} = r_1 + r_2 + r_3 \end{array}$$

Podemos deducir una fórmula general:

$$\begin{aligned}
-\frac{a_{n-1}}{a_n} &= r_1 + r_2 + r_3 + \ldots + r_n \\
\frac{a_{n-2}}{a_n} &= r_1 \cdot r_2 + r_1 \cdot r_3 + \ldots + r_{n-1} \cdot r_n \\
\vdots & \qquad \vdots \\
(-1)^n \frac{a_0}{a_n} &= r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{n-1} \cdot r_n
\end{aligned}$$

Las expresiones $r_1 + r_2 + r_3 + \ldots + r_n$, $r_1 \cdot r_2 + r_1 \cdot r_3 + \ldots + r_{n-1} \cdot r_n$, $r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{n-1} \cdot r_n$, se llaman los *polinomios simétricos elementales* en r_1, r_2, ..., r_n.

Ejemplo 7.17 Dado el polinomio $f(x) = 3x^3 - x^2 + 5$, sabiendo que sus raíces son r_1, r_2 y r_3 hallar, sin calcularlas, la suma de sus inversos y la suma de sus cuadrados.

1. Suma de los inversos:
   $\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} = \frac{r_2.r_3 + r_1.r_3 + r_1.r_2}{r_1.r_2.r_3} =$
   $= \frac{r_2.r_3 + r_1.r_3 + r_1.r_2}{r_1.r_2.r_3} = \frac{a_1/a_3}{-a_0/a_3} = \frac{0/3}{-5/3} = 0$
2. Suma de sus cuadrados: $r_1^2 + r_2^2 + r_3^2$

   Hagamos una cuenta sencilla:

   $$(r_1 + r_2 + r_3)^2 = r_1^2 + r_2^2 + r_3^2 + 2.(r_1.r_2 + r_1.r_3 + r_2.r_3)$$

   Reemplazamos: $\left(-\frac{a_2}{a_3}\right)^2 = r_1^2 + r_2^2 + r_3^2 + \frac{a_1}{a_3}$

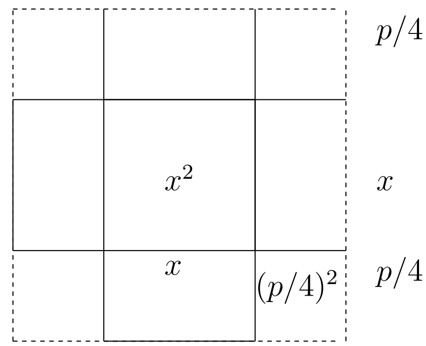
   Y despejando obtenemos: $r_1^2 + r_2^2 + r_3^2 = \left(-\frac{a_2}{a_3}\right)^2 - \frac{a_1}{a_3} = \frac{1}{9}$

7.5. Cálculo de las raíces de un polinomio

(✠) La determinación de las raíces de los polinomios, lo que llamamos *resolver ecuaciones algebraicas*, está entre los problemas más viejos de la matemática. Las ecuaciones de primer grado, es decir, las del tipo $ax+b = 0$ no revistieron demasiado interés.

Hace unos 4.000 años, los babilonios conocían la manera de encontrar la solución positiva de las ecuaciones cuadráticas que hoy en día escribimos $x^2 - bx = c, b > 0, c > 0$, aunque claramente no usaron esta notación. A principios del s. IX d.C. el matemático árabe Al-Kwarizmi interpretaba, geométricamente, $x^2 + px$ como una cruz constituída por un cuadrado de lado x y cuatro rectángulos de lados $p/4$ y x. "Completaba" esta cruz hasta obtener un cuadrado de lado $x + p/2$.

$$\begin{gathered}
x^2 + px = q \\
x^2 + 4(p/4)x + 4(p/4)^2 = (x + p/2)^2 \\
q + 4(p/4)^2 = (x + p/2)^2 \\
\sqrt{q + 4(p/4)^2} = x + p/2 \\
-p/2 + \sqrt{q + 4(p/4)^2} = x \\
\frac{-p + \sqrt{p^2 + 4q}}{2} = x
\end{gathered}$$



(observar que q "está del otro lado"). Ya en el siglo XII Bhaskara dio la forma más general.

La resolución de ecuaciones de tercer grado sería mucho más cinematográfica, por así decirlo. La gran proeza fue realizada por el matemático italiano Scipione Dal Ferro, en primer lugar, y más adelante por Nicoló Tartaglia quien la obtuvo sin conocer el trabajo de Dal Ferro. En aquellos tiempos, cuando un matemático descubría algo importante, lo guardaba en secreto, para enfrentarse en "duelos matemáticos". Estos duelos eran una especie *reality show* de la época. Se proponían los problemas que se guardaban en sobres lacrados, se nombraban jueces y se efectuaba el duelo unos 15 días después. Asistía el público y también las autoridades locales, y el perdedor podía llegar a perder hasta su empleo en una importante Universidad. Dal Ferro guardó su secreto hasta poco antes de su muerte, cuando decidió revelarlo y uno de sus discípulos, Antonio María Fiore, decidió retar a Tartaglia, quien era profesor de Matemática en Venecia, para un duelo. Fiore conocía una solución a problemas más generales que Tartaglia y lo sabía, por eso le propuso problemas que no pudiera resolver. En tanto Tartaglia sólo le planteó el caso que él conocía y así se cerraron los sobres. En esos 15 días el orgullo de Tartaglia hizo que encontrara la solución a todos los problemas planteados y salió victorioso. Girolamo Cardano, interesado en conocer estas soluciones, trató, durante 4 años, de acercarse a Tartaglia para que compartiera su conocimiento. Finalmente, logró su objetivo, jurando a Tartaglia solemnemente que jamás lo divulgaría. Pero 3 años má s tarde, en 1542, Cardano estudió los escritos de Dal Ferro, y en 1545 los publicó en su obra *Ars Magna*. Aunque Cardano reconoció el mérito de Dal Ferro y de Tartaglia este último nunca lo perdonó por faltar a su juramento. Tras un año de polémicas, Tartaglia aceptó el reto de un alumno de Cardano para un "duelo matemático", y resultó perdedor. A consecuencia perdió su trabajo de profesor en la Universidad de Brescia y murió 9 años después, humilde, en Venecia.

La cosa se pone más trágica en la búsqueda de soluciones similares para ecuaciones de quinto grado y superior: Abel y Galois.

Niels Henrik Abel (1802-1829) fue un matemático noruego, que probó en 1824 (a los 18 años) que no hay ninguna fórmula para hallar los ceros de todos los polinomios generales de grados $n \geq 5$ en términos de sus coeficientes. Con 9 años ingresó en la escuela de la Catedral de Cristianía (hoy Oslo) donde probaría sus aptitudes para la matemática con sus brillantes soluciones a los problemas originales propuestos por Bernt Holmboe. Su familia sufrió graves penurias económicas pero una beca del Estado permitió que Abel ingresara a la Universidad de Cristianía en 1821 y visitara Alemania y Francia. En 1824, demostró que no puede haber fórmulas generales para los polinomios de grado 5 o mayores en términos de sus coeficientes. En 1826 Abel viajó a París, donde conoció a los matemáticos franceses más importantes, aunque ni él ni su trabajo fueron especialmente valorados. A ello contribuyó también su modestia, que lo llevó a no hacer públicos los resultados de sus investigaciones. La tuberculosis se lo llevó con los 26 años, y terminó con una brillante y prometedora carrera. Sus investigaciones aclararon algunos de los aspectos más oscuros del análisis y abrieron nuevos campos de estudio, posibilitando numerosas ramificaciones en el conocimiento matemático y alcanzando un notable progreso.

Évariste Galois (1811-1832) Hasta los doce años, fue educado por su madre. A esa edad ingresó en el Liceo Real Louis-le-Grand, de París, donde habían estudiado Robespierre y Víctor Hugo. Allí tuvo sus primeros enfrentamientos políticos. El curso de matemática impartido por Ms Vernier, despertó el genio de Galois. Ignorando los consejos de su maestro, empezó con los textos más avanzados de aquella época: estudió la geometría de Legendre y el álgebra de Lagrange. Galois profundizó considerablemente en el estudio del álgebra, una materia que entonces todavía tenía muchas lagunas y llegó a conocer la cantidad de problemas sin resolver que encerraba. Galois tenía una idea clara: quería ser matemático y quería entrar en la École Polytechnique. Así decidió presentarse con un año de antelación (1828)y al carecer de la formación fundamental en diversos aspectos fue rechazado. Logró publicar su primer trabajo y poco después halló las condiciones de resolución de ecuaciones polinómicas por radicales. Sin embargo, sus avances más notables fueron los relacionados con el desarrollo de una teoría nueva cuyas aplicaciones desbordaban con mucho los límites de las ecuaciones algebraicas: la teoría de grupos. Sus trabajos sobre este tema fueron evaluados en la Academia de Ciencias. Inicialmente Cauchy los rechazó por tener puntos en común con un reciente artículo publicado por Abel. Luego Fourier, el secretario vitalicio de la misma y el encargado de su publicación, murió y la memoria fue traspapelada. El premio de la Academia fue otorgado ex quo a Abel y a Jacobi, y Galois acusó a la academia de una farsa para desacreditarlo. En julio de 1830 la situación política era difícil, el joven Galois participó activamente en las manifestaciones y fue expulsado por ello de la École Normale. En la primavera de 1831, con apenas 19 años, Galois fue detenido y encarcelado durante más de un mes acusado de sedición, tras un desafiante brindis en nombre del rey. Inicialmente fue absuelto, pero volvió a ser arrestado por otra actitud sediciosa en julio y esta segunda vez pasó ocho meses en prisión. Fue liberado el 29 de abril de 1832. Los detalles que condujeron a su duelo no están claros. Quedan para la historia las cartas a sus amigos republicanos y su testamento matemático escritos en la noche anterior al evento. En estos últimos papeles describió someramente las implicaciones del trabajo que había desarrollado en detalle y anotó una copia del manuscrito que había remitido a la academia junto con otros artículos. El 30 de mayo de 1832, a primera hora de la mañana, se batió en duelo y falleció al día siguiente a las diez de la mañana (probablemente de peritonitis) en el hospital Cochin. Sus últimas palabras a su hermano Alfredo fueron: “No llores! Necesito todo mi coraje para morir a los veinte años”.

Las contribuciones matemáticas de Galois fueron publicadas finalmente en 1843 cuando Joseph Liouville revisó sus manuscritos y declaró que aquel joven en verdad había resuelto el problema de Abel por otros medios que suponían una verdadera revolución en la teoría de las matemáticas empleadas. El manuscrito fue publicado en el número de octubre de 1846 del Journal des mathématiques pures et appliquées. Su trabajo ofreció las bases fundamentales para la teoría que lleva su nombre, 2 una rama principal del álgebra abstracta. Fue el primero en utilizar el término grupo en un contexto matemático. La teoría constituye una de las bases matemáticas de la modulación CDMA utilizada en comunicaciones y, especialmente, en los Sistemas de navegación por satélite, como GPS, GLONASS, etc.

Finalmente, la máquina diferencial de Charles Babbage fue diseñada para crear grandes tablas de valores de funciones logarítmicas y diferenciales automáticamente, evaluando aproximaciones polinomiales en muchos puntos usando el método de las diferencias de Newton.

7.5.1. Acotación de las raíces reales de un polinomio a coeficientes reales: Regla de Laguerre-Thibault.

En primer lugar aclaremos que acotar las raíces reales quiere decir ver en qué intervalo están contenidas todas las raíces reales de un polinomio en $\mathbb{R}[X]$. dado un conjunto $X \subseteq \mathbb{R}$, una *cota superior* para X es un $S \in \mathbb{R}$ tal que $x \leq S$ para todo $x \in X$. Dualmente (o sea, mirado “del otro lado”)una *cota inferior* para X es un $I \in \mathbb{R}$ tal que $x \geq I$ para todo $x \in X$.

Teorema 7.7 *Sea $f(x) = a_n n^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_i \in \mathbb{R}$, con $a_n > 0$. Si al dividir $f(x)$ por $x - a$, con $a \geq 0$, todos los coeficientes del cociente, y el resto, son no negativos, entonces a es una cota superior de las raíces reales de $f(x)$.*

Demostración: Por el teorema del resto es $f(x) = (x - a) \cdot q(x) + f(a)$. Si todos los coeficientes de $q(x)$ son no negativos, y $f(a)$ es también no negativo, es claro que si $b > a$, entonces $f(b) > 0$, luego, por definición de raíz, si $b > a$, b no puede ser raíz de $f(x)$, o sea, que todas las raíces reales de $f(x)$ son menores o iguales que a. Luego a es una cota superior de las raíces de $f(x)$. $\square$

Buscar el x menor, es equivalente a buscar el $-x$ mayor, ya que cuando multiplicamos por un número negativo se dan vuelta las desigualdades. Entonces, para buscar una cota inferior haremos lo siguiente: Consideramos el polinomio $f(-x)$, buscamos una cota superior K de las raíces de $f(-x)$, entonces $I = -K$ es una cota inferior de las raíces de $f(X)$. Si al calcular $f(-x)$ resultara $a_n < 0$ (esto ocurrirá toda vez que n sea impar. ¿En serio? ®) simplemente consideramos $-f(-x)$.

Ejemplo. Acotar las raíces de $f(x) = x^3 - 4x^2 + 3x - 10$.
Dividimos por $x-1$, $x-2$, $x-3$, $\ldots$, hasta que el resto y todos los coeficientes del cociente sean no negativos.

$$
\begin{array}{c|cccc}
 & 1 & -4 & 3 & -10 \\
4 & & 4 & 0 & 12 \\
\hline
 & 1 & 0 & 3 & 2
\end{array}
$$

Luego 4 es una cota superior de las raíces reales de $f(x)$.

Para hallar la cota inferior hacemos $f(-x) = -x^3 - 4x^2 - 3x - 10$, pero como el término principal debe ser positivo, consideramos $-f(-x) = x^3 + 4x^2 + 3x + 10$ y hallamos la cota superior de sus raíces.

$$\begin{array}{r|rrrr} & 1 & 4 & 3 & 10 \\ -3 & & -3 & -3 & 0 \\ \hline & 1 & 1 & 0 & 10 \end{array}$$

Luego -3 es cota superior de las raíces reales de $f(-x)$, luego 3 es cota inferior de las raíces reales de $f(x)$.

Por lo tanto, las raíces reales del polinomio $f(x)$ están todas en el intervalo $(3, 4)$.

7.5.2. Raíces racionales de un polinomio con coeficientes racionales: Teorema de Gauss.

Analicemos en primer lugar que basta encontrar un método para hallar las raíces racionales de un polinomio a coeficientes enteros.
En efecto: Consideremos la ecuación:

$$x^5 + \frac{1}{3}x^3 - \frac{1}{4}x + \frac{1}{6} = 0.$$

Si la multiplicamos por el mínimo común múltiplo de los denominadores, o sea, por 12, obtenemos:

$$12x^5 + 4x^3 - 3x + 2 = 0,$$

una bella ecuación a coeficientes enteros que tiene las mismas raíces que la anterior. Es decir, cuando tenemos un polinomio con coeficientes racionales, lo podemos transformar en un polinomio con coeficientes enteros que tiene las mismas raíces, multiplicándolo por el denominador común.

Teorema 7.8 *Si un número racional* $\frac{p}{q}$*, con* p *y* q *relativamente primos, es raíz de un polinomio* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *con coeficientes enteros, entonces* $p|a_0$ *y* $q|a_n$*.*

Demostración: Como $\dfrac{p}{q}$ es raíz de $f(x)$ tenemos:

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

Luego

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

Multiplicando por q^n se tiene:

$$a_np^n + a_{n-1}p^{n-1}\cdot q + \ldots + a_1p\cdot q^{n-1} + a_0\cdot q^n = 0.$$

Luego

$$a_np^n + a_{n-1}p^{n-1}\cdot q + \ldots + a_1p\cdot q^{n-1} = -a_0\cdot q^n,$$

esto es,

$$p(a_np^{n-1} + a_{n-1}p^{n-2}\cdot q + \ldots + a_1\cdot q^{n-1}) = -a_0\cdot q^n.$$

Luego $p|a_0\cdot q^n$, pero como p y q son relativamente primos, entonces $p|a_0$.

La demostración de $q|a_n$ es análoga y queda en manos del lector. ® $\square$

Ejemplo 7.18 Calcular las raíces racionales de $x^3 + \dfrac{1}{2}x^2 - \dfrac{7}{2}x - 3$.
Es lo mismo que calcular las raíces racionales de $2x^3 + x^2 - 7x - 6$. Estas son de la forma $\dfrac{p}{q}$, donde $p| - 6$ y $q|2$.

$$p:\ \pm1,\ \pm2,\ \pm3,\ \pm6;\ q:\ \pm1,\ \pm2.$$

Luego las posibles raíces racionales son:

$$\frac{\pm1}{\pm1},\ \frac{\pm2}{\pm1},\ \frac{\pm3}{\pm1},\ \frac{\pm6}{\pm1},\ \frac{\pm1}{\pm2},\ \frac{\pm2}{\pm2},\ \frac{\pm3}{\pm2},\ \frac{\pm6}{\pm2},\ ,$$

o sea,

$$1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 6,\ -6,\ \frac{1}{2},\ -\frac{1}{2},\ \frac{3}{2},\ -\frac{3}{2}.$$

Reemplazando en $f(x)$ o aplicando la regla de Ruffini, se ve que las raíces racionales son: -1, 2 y $-\dfrac{3}{2}$.

Observación 7.10 En general, dado un polinomio no constante $f(x)$, el procedimiento para hallar las raíces de $f(x)$ es el siguiente:

1. Se acotan las raíces reales.
2. Se determinan las raíces racionales
3. Una vez determinada una raíz de $f(x)$, se analiza su orden de multiplicidad y se obtiene un polinomio de menor grado que $f(x)$ cuyas raíces son también raíces de $f(x)$.

7.6. Ejercicios propuestos

7.6.1. Definición

Ejercicio 7.1 ($\diamond$) Decidir si las siguientes expresiones representan un elemento de $\mathbb{K}[x]$:

1. $\sqrt{2}$
2. $x^{-1} + x$
3. $\sqrt{x} - 3\,x$
4. $x + \sqrt{7}\,x^2 - x^5 + 4$
5. $e\,x + \pi$
6. x

Ejercicio 7.2 ($\diamond$) Dar, si es posible, polinomios $\mathbb{K}[x]$ que satisfagan:

1. Grado 4, mónico, sin término independiente.
2. Coeficiente cuadrático nulo, coeficiente principal igual al coeficiente lineal.
3. Cada coeficiente igual al grado del término al que pertenece.

¿Son únicas las expresiones halladas?

Ejercicio 7.3 ($\diamond$) Escribir los siguientes polinomios de $\mathbb{K}[x]$ en forma completa y ordenada según los grados de los términos de mayor a menor y clasificarlos como expresiones en $\mathbb{Q}[x]$, $\mathbb{R}[x]$ ó $\mathbb{C}[x]$:

1. $x^5 + 2\,i\,x - \sqrt{2}$
2. $3 + 5\,x - x^3$
3. $x^4 - 2\,x^2 + \sqrt[3]{27}\,x$
4. $1 + 3\,x - \dfrac{1}{2}\,x^2$

¿Son únicas las expresiones halladas?

7.6.2. Operaciones en $\mathbb{K}[x]$

Ejercicio 7.4 ($\diamond$) Efectuar las siguientes operaciones en $\mathbb{R}[x]$:

1. $(x^3 - 4\,x + 3) \cdot (x^2 + 3\,x - 2)$,

2. $(x^5 - \ x + 6)^2$,
3. $(x^4 - x^2 - x) \cdot (x^3 - 4\,x + 2) + 3\,x^2 \ - x^7 + 2\,x.$

Ejercicio 7.5 Si $gr[f(x)] = 6$ y $gr[g(x)] = 2$, determinar, si es posible

1. $gr[f(x) + g(x)^3]$
2. $gr\left[f(x) \cdot \dfrac{x^3}{g(x)}\right].$

Ejercicio 7.6

Determinar $a, b, c, d \in \mathbb{R}$ de modo tal que $h(x) = f(x) \cdot g(x)$, siendo:

$f(x) = 2\,x + c \qquad g(x) = a\,x^2 + 2\,x + b \qquad h(x) = 6\,x^3 + d\,x^2 - 2\,x - 1$.

Ejercicio 7.7 (♣) Hallar, si es posible, un polinomio $f(x)$ tal que su cuadrado sea $x^6 + a\,x^4 + b\,x^3 + c\,x^2 - 24\,x + 36$ y calcular los valores reales de a, b y c . ¿Es único?
¿Y los valores de a, b y c ?

Ejercicio 7.8 ($\diamond$) Hallar el cociente y el resto de la división de :

1. $x^5 - 2\,x^3 + 4\,x^2 - 5\,x + 6$ por $2\,x^2 - 4\,x - 1$,
2. $x^2 + x + 1$ por $x^4 + 2$,
3. $-6\,x^3 + x^2$ por $2\,x^2 - x$.

Ejercicio 7.9 Hallar el m.c.d. (mónico) de los siguientes pares de polinomios:

a) $f(x) = x^3 - 1$, $g(x) = x^4 + x^3 + 2x^2 + x + 1.$
b) $f(x) = x^3 - 1$, $g(x) = x^4 + 1.$

Expresarlo en la forma $d(x) = s(x) \cdot f(x) + t(x) \cdot g(x)$.

7.6.3. Funciones polinómicas - Regla de Ruffini

Ejercicio 7.10 ($\diamond$) Calcular el valor numérico de las siguientes funciones polinómicas, en los valores de a indicados:

1. $f(x) = x^4 - 2x^3 + x + 1\,, \quad a = 0.$
2. $f(x) = \sqrt{5}\,x^2 - \dfrac{\sqrt{2}}{5}\,x\,, \quad a = \sqrt{10}.$

3. $f(x) = 2x^5 - 7x^3 - 10x^2 + 2x + 7\,, \quad a = -i.$

Ejercicio 7.11 Aplicando la regla de Ruffini hallar el cociente y el resto de dividir:

1. $x^4 + (2+\ i)\,x^3 - 3\,i\,x^2 - 4\,x - 1 + i \quad$ por $\quad x - i\ ,$
2. $x^5 \quad$ por $\quad x - 2 + 2\,i\ ,$
3. $x^3 + x \quad$ por $\quad x + \frac{1}{2}\ .$

Ejercicio 7.12 (♣) Aplicar el teorema del resto y hallar las condiciones para que $x^n \pm a^n$ sea divisible por $x \pm a\ ,\ \ a \in \mathbb{R}^+, \ \ n \in \mathbb{N}^+,$ (sexto caso de factoreo).

7.6.4. Teorema fundamental del álgebra

Ejercicio 7.13 (Ⓡ)(◇) Hallar las raíces de los siguientes polinomios:

1. $x^4 + 4\,x^2 + 4$
2. $x^5 + i\,x^3 + x^3$
3. $x^2 - 2\sqrt{2}\,x + 3$
4. $x^6 + 2\,x^4 + x^2$
5. $x^2 + (5 + 2\,i)\ x + 5 + 5\,i$
6. $i\ x^2 - x + i.$

Ejercicio 7.14 (◇) Determinar el orden de multiplicidad de la raíz r indicada en las funciones polinómicas resultantes de las siguientes operaciones:

1. $r = 1 \quad$ en $(x^2 - 1) \cdot (x^3 - 1)\ ,$
2. $r = 0 \quad$ en $x^3 \cdot (x^3 - 2\,x^2 + x),$
3. $r = -1 \quad$ en $(x^2 - 1) \cdot (x^3 + 1)\ ,$

Ejercicio 7.15 Hallar todas las raíces de los siguientes polinomios, indicando su orden de multiplicidad:

1. $x^5 + 6\,x^4 + 15\,x^3 + 26\,x^2 + 36\,x + 24 \quad$ sabiendo que $\quad r = -2 \quad$ es una raíz múltiple,
2. $8\,x^4 - 4\,x^3 - 10\,x^2 + 9\,x - 2\ $ sabiendo que $\quad r = \dfrac{1}{2}$ es una raíz múltiple,
3. $x^5 + x^3 + (1 - i)\ x^2 + (1 - i)\ $ sabiendo que $\ x^2 + 1 \ $ es factor de dicho polinomio.

Ejercicio 7.16 Determinar el menor valor entero k para el cual la función polinómica $f(x) = 2\,x \cdot (kx - 4) - x^2 + 6$ no posea raíces reales.

Ejercicio 7.17 Hallar el valor de a para el cual $x^7 - ax^6 + ax - 1$ tenga a 1 como raíz triple.

Ejercicio 7.18 Si $-6i$ es una raíz múltiple de orden 5 de un polinomio $f(x) \in \mathbb{R}[x]$, ¿Se puede decir cuáles son sus restantes raíces si $gr\ f(x) = 11$ y su término independiente es nulo? En caso afirmativo, y suponiendo que $f(x)$ es mónico, escribirlo como producto de irreducibles en $\mathbb{R}[x]$. ¿Este resultado es válido para $f(x) \in \mathbb{C}[x]$?

Ejercicio 7.19 (♣) Si $f(x) = 8(x^2 - 2)^4(x - 3)^2(x - 5\ i)^7(x + 5\ i)^7$, hallar la descomposición de $f(x)$ en irreducibles mónicos en $\mathbb{R}[x]$.

Ejercicio 7.20 ($\diamond$) Hallar las raíces de $f(x) = x^7 + 5x^5 - 2x^4 - 33x^3 - 16x^2 + 27x + 18$ sabiendo que $-3\ i$ y -1 son raíces. Descomponer el polinomio en producto de irreducibles sobre $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

Ejercicio 7.21 (♣) Hallar las raíces de $x^4 - 3x^3 + 5x^2 - 27x - 36$ sabiendo que tiene una raíz imaginaria pura.

Ejercicio 7.22 Decidir la veracidad de las siguientes proposiciones:

1. Si $x^3 + 7x - 6\ i$ tiene a i como raíz, entonces $-i$ es otra raíz.
2. Si $x^3 + (1 - 2\sqrt{3})x^2 + (5 - 2\sqrt{3})x + 5$ tiene a $\sqrt{3} - \sqrt{2}\ i$ como raíz, entonces $\sqrt{3} + \sqrt{2}\ i$ es otra raíz.
3. Si $x^4 + (1 - 2\sqrt{2})x^3 + (4 - 2\sqrt{2})x^2 + (3 - 4\sqrt{2})x + 1$ tiene a $-1 + \sqrt{2}$ como raíz, entonces $-1 - \sqrt{2}$ es otra raíz.

Ejercicio 7.23 (©)

1. Si $\epsilon = \cos\dfrac{2\pi}{n} + i\ \mathrm{sen}\dfrac{2\pi}{n}$, demostrar que :
   $x^{n-1} + x^{n-2} + \cdots + x + 1 = (x - \epsilon)(x - \epsilon^2)\cdots(x - \epsilon^{n-1})$.
2. Si ϵ es una raíz primitiva de la unidad de orden n, probar que:
   $n = (1 - \epsilon)(1 - \epsilon^2)\cdots(1 - \epsilon^{n-1})$.
3. Hallar todas las raíces del polinomio $x^n + x^{n-1} + \cdots + x + 1$.

Ejercicio 7.24 ($\diamond$) Encontrar un polinomio a coeficientes reales de grado mínimo que posea las siguientes raíces:

1. $1 \ , \ -2 \ , \ -\frac{1}{3}$.
2. 1 raíz triple , $2\,i$.
3. $0, \ -\frac{1}{2} \ , \ \frac{1}{2} \ , \ -3$ raíz doble.
4. 0 raíz doble , $1-i$, $\sqrt{2}$.

7.6.5. Relación entre las raíces de un polinomio y sus coeficientes

Ejercicio 7.25 Acotar las raíces reales de los siguientes polinomios:

1. $x^3 - x + 4$
2. $x^3 - 7x - 7$
3. $x^7 + x^2 + 1$
4. $x^4 + 2x^3 - x^2 - 1$

Ejercicio 7.26 Hallar las raíces racionales, en caso de existir, de los siguientes polinomios:

1. $x^3 - 6\,x^2 + 15\,x - 14$,
2. $x^5 - 7\,x^3 - 12\,x^2 + 6\,x + 36$,
3. $x^4 - 2\,x^3 - 8\,x^2 + 13\,x - 24$,
4. $x^3 - x - 6$,

Ejercicio 7.27 Dado el polinomio $f(x) = 5x^7 - 2x^6 - 10x^5 + 4x^4 - 15x^3 + 6x^2$, hallar todas las raíces.

Ejercicio 7.28 Dado el polinomio $f(x) = x^5 + 12x^4 + 57x^3 + 134x^2 + 156x + 72$ hallar todas las raíces, sabiendo que admite raíces múltiples.

Ejercicio 7.29 Hallar el valor de a, sabiendo que la suma de dos raíces del polinomio $2x^3 - x^2 - 7x + a$ es 1.

Ejercicio 7.30 Hallar

1. la suma,
2. la suma de los cuadrados,
3. el producto,

4. la suma de los inversos,

de las raíces de los siguientes polinomios, sin calcularlas:

1. $x^3 + 3\,x - 1$ 2. $x^9 - 1$
3. $x^4 + x^3 + x + 1$ 4. $x^n - 1$

7.6.6. Problemas (♣)($\diamond$)

Ejercicio 7.31 Encontrar un polinomio $p(x)$ a coeficientes racionales de grado mínimo que posea las siguientes raíces: $\sqrt{2}$ raíz triple , $3\,i$ doble y tal que $p(0) = 2$.

Ejercicio 7.32 Determinar los valores reales de a y b de modo que:

1. Al dividir $f(x) = 6\,x^2 + a\,x + b$ por $g(x) = 3\,x - 2$, el resto es cero y el cociente $q(x) = 2\,x - 1$.
2. $2\,x^2 + a\,x + 3$ sea divisible por $2\,x - 5$,
3. $x^2 + a\,x + 4$ dé el mismo resto al dividirlo por $x + 2$ y $x - 2$.

Ejercicio 7.33 Escribir un polinomio de grado 5, coeficiente principal 3, que tenga a $x_1 = -1$ como raíz doble, $x_2 = 3$ como raíz simple y no tenga otras raíces reales. ¿Es único?

Ejercicio 7.34 Al dividir $a(x)$ por $b(x) = 3\,x^2 - x + 1$ resulta cociente $c(x) = x^4 + 2\,x^2 - x$ y resto $r(x) = 3\,x - 4$. Hallar $a(x)$. ¿Es único?

Ejercicio 7.35 Sabiendo que $p(x) = x^6 - x^5 - 20\,x^4 + 18\,x^3 + 117\,x^2 - 81\,x - 162$ es divisible por $q(x) = x^2 - x - 2$, hallar todas las raíces de $p(x)$, indicando su orden de multiplicidad y escribir la descomposición en factores simples en $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathcal{C}[x]$.

Ejercicio 7.36 Hallar todas las raíces del polinomio $q(x)$ que se obtiene al dividir $p(x) = x^5 - 3\,x^4 - 4\,x^3 + 12\,x^2 + 3\,x - 6$, por $x - 3$, indicando su orden de multiplicidad y escribir la descomposición en factores simples de $q(x)$ en $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathcal{C}[x]$.

Capítulo 8

Sistemas de ecuaciones lineales. Matrices

Sistemas de ecuaciones lineales. Resolución por eliminación. Matrices. Operaciones. Propiedades. Traspuesta de una matriz. Determinantes. Definición y propiedades. Desarrollo por los elementos de una fila o una columna. Determinante de un producto de matrices. Matrices inversibles. Matriz inversa. Regla de Cramer.

8.1. Sistemas de m ecuaciones lineales con n incógnitas

Ya hemos trabajado con un sistema de dos ecuaciones lineales con dos incógnitas:

$$\begin{cases} L_1 : \ a_1x + b_1y + c_1 = 0 \\ L_2 : \ a_2x + b_2y + c_2 = 0 \end{cases}$$

Sabemos que $ax + by + c = 0$ se interpreta geométricamente como una recta en el plano. Un sistema de dos ecuaciones representa entonces dos rectas en el plano que pueden ser:

1. incidentes,
2. paralelas coincidentes,
3. paralelas no coincidentes.

1. Si las rectas son incidentes quiere decir que existe un punto (x_0, y_0) que pertenece a ambas y entonces el sistema tiene solución única. Se llama *sistema compatible determinado.*

2. Si las rectas son coincidentes quiere decir que todo punto de una es punto de la otra, es decir, existen infinitos puntos que son solución del sistema. Se llama *sistema compatible indeterminado* tiene una solución generalizada e infinitas soluciones particulares.
3. Si las rectas son paralelas, claramente no existe ningún punto que pertenezca simultáneamente a ambas, por eso el sistema no tiene solución y se llama *sistema incompatible*.

Escritas en forma explícita las rectas son:

$$\begin{cases} L_1 : \, y = -\dfrac{a_1}{b_1}x - \dfrac{c_1}{b_1} \\ L_2 : \, y = -\dfrac{a_2}{b_2}x - \dfrac{c_2}{b_2} \end{cases}$$

Vemos que las pendientes son: $m_1 = -\dfrac{a_1}{b_1}$ y $m_2 = -\dfrac{a_2}{b_2}$,

y las distancias al origen de L_1 y de L_2 son respectivamente $-\dfrac{c_1}{b_1}$ y $-\dfrac{c_2}{b_2}$.

Las rectas serán paralelas coincidentes si $-\dfrac{a_1}{b_1} = -\dfrac{a_2}{b_2}$ y $-\dfrac{c_1}{b_1} = -\dfrac{c_2}{b_2}$.

o lo que es lo mismo:

$$\frac{a_1}{a_2} = \frac{b_1}{b_2} = \frac{c_1}{c_2}$$

Las rectas serán paralelas no coincidentes si:

$$\frac{a_1}{a_2} = \frac{b_1}{b_2} \neq \frac{c_1}{c_2}$$

Las rectas serán incidentes si:

$$\frac{a_1}{a_2} \neq \frac{b_1}{b_2}.$$

Es decir, el sistema será determinado si $a_1 \cdot b_2 - b_1 \cdot a_2 \neq 0$. Esta cuenta es la determinante del sistema y volveremos sobre ella más adelante.

Ejemplo 8.1 A modo de repaso veremos cómo se resuelve un sistema de dos ecuaciones con dos incógnitas.

1.
$$\begin{cases} L_1: \ 4x - 5y + 6 = 0 \\ L_2: \ -12x + 15y - 1 = 0 \end{cases}$$
$$\frac{4}{-12} = \frac{-5}{15}, \quad \frac{-5}{15} \neq \frac{6}{10}$$
Interpretación geométrica: rectas paralelas no coincidentes.
Clasificación del sistema: incompatible.(SI)
Soluciones: No hay solución.

2.
$$\begin{cases} L_1: \ 4x - 5y + 6 = 0 \\ L_2: \ -12x + 15y - 18 = 0 \end{cases}$$
$$\frac{4}{-12} = \frac{-5}{15}, \quad \frac{-5}{15} = \frac{6}{-18}$$
Interpretación geométrica: rectas paralelas coincidentes.
Clasificación del sistema: compatible indeterminado (SCI).
Soluciones: La solución general es cualquiera de las dos rectas. Puede expresarse en diversas formas:

a) Como conjunto:
$\{(x,y) \in \mathbb{R}^2 : 4x - 5y + 6 = 0\}$ (ó $\{(x,y) \in \mathbb{R}^2 : -12x + 15y - 18 = 0\}$)
$\{(x,y) \in \mathbb{R}^2 : y = \frac{4}{5}x + \frac{6}{5}\}$ (ó $\{(x,y) \in \mathbb{R}^2 : x = \frac{5}{4}y - \frac{6}{4}\}$)

b) Como solución generalizada: $\left(a, \frac{4}{5}a + \frac{6}{5}\right)_{a \in \mathbb{R}}$ ó $\left(\frac{5}{4}a - \frac{6}{4}, a\right)_{a \in \mathbb{R}}$

Y pueden mencionarse soluciones particulares, que son puntos cualesquiera en la recta y se obtienen muy fácilmente dando diversos valores a la letra a en las soluciones generalizadas.

Por ejemplo: $(1,2)$, $\left(0, \frac{6}{5}\right)$, $\left(\frac{-1}{4}, 1\right)$

3.
$$\begin{cases} L_1: \ 2x + y - 3 = 0 \\ L_2: \ 3x - 3y = 0 \end{cases}$$
$$\frac{2}{3} \neq \frac{3}{-3}.$$
Interpretación geométrica: rectas incidentes.
Clasificación del sistema: compatible determinado (SCD).
Soluciones: Existe una única solución que podemos encontrar por diversos métodos.

8.1.1. Método por sustitución

Se trata de despejar una variable (cualquiera) en una ecuación y sustituírla en la otra.

Despejamos y en la primera ecuación: $y = 3 - 2x$,

reemplazamos este valor en la segunda: $3x - 3(3-2x) = 0$, entonces $9x - 9 = 0$, $x = 1$

Una vez obtenido el valor de x, calculamos $y = 3 - 2 \cdot 1 = 1$.

La solución es: $P = (1, 1)$.

Podríamos haber despejado, por ejemplo, la x en la segunda, entonces de $3x - 3y = 0$ resulta $x = y$

reemplazamos este valor en la primera ecuación: $2x + x - 3 = 0$, entonces $3x - 3 = 0$ y resulta $x = 1$. De nuevo: $3 \cdot 1 - 3\,y = 0$ nos da $y = 1$ y obtenemos la misma solución: $(1, 1)$.

8.1.2. Método por igualación

La idea de este método es despejar en ambas ecuaciones la misma variable e igualarlo.

- despejando x

$$\begin{cases} L_1 : \; x = -\dfrac{1}{2}y + \dfrac{3}{2} \\ L_2 : \; x = y \end{cases}$$

Luego igualamos $-\dfrac{1}{2}y + \dfrac{3}{2} = y$ y resulta $\dfrac{3}{2}y = \dfrac{3}{2}$, de donde $y = 1$ y la solución $(1, 1)$.

- despejando y

$$\begin{cases} L_1 : y = -2x + 3 \\ L_2 : \; y = x \end{cases}$$

Luego igualamos $x = -2x + 3$ y resulta $3x = 3$, de donde $x = 1$ y la solución $(1, 1)$.

8.1.3. Método por eliminación (Gauss)

La idea de este método es eliminar las variables haciendo operaciones que se denominan *operaciones simples*. Es decir, multiplicar las ecuaciones por números reales y sumarlas.

El "método automático" para eliminar la variable x es multiplicar la segunda ecuación por el coeficiente de x en la primera, la primera por el coeficiente de x en la segunda y restar ambas ecuaciones:

$$\begin{cases} L_1: \ 2x + y - 3 = 0 \\ L_2: \ 3x - 3y = 0 \end{cases}$$

$3(2x + y - 3) = 3 \cdot 0$ entonces $6x + 3y - 9 = 0$

$2(3x - 3y) = 2 \cdot 0$ entonces $6x - 6y = 0$

Restamos ambas ecuaciones: $(6x+3y-9)-(6x-6y) = 0$ y resulta $9y-9 = 0$ de donde $y = 1$, reemplazando en cualquiera de las ecuaciones obtenemos $x = 1$ y la solución es $P : (1, 1)$.

Igual, para eliminar la variable y se puede multiplicar la segunda ecuación por el coeficiente de y en la primera, la primera por el coeficiente de y en la segunda y restar ambas ecuaciones:

$$\begin{cases} L_1: \ 2x + y - 3 = 0 \\ L_2: \ 3x - 3y = 0 \end{cases}$$

$-3(2x + y - 3) = -3 \cdot 0$ entonces $-6x - 3y + 9 = 0$

$1(3x - 3y) = 1 \cdot 0$ entonces $3x - 3y = 0$

Restamos ambas ecuaciones: $(-6x - 3y + 9) - (3x - 3y) = 0$ y resulta $-9x + 9 = 0$ de donde $x = 1$, reemplazando en cualquiera de las ecuaciones obtenemos $y = 1$ y la solución es $P : (1, 1)$.

Extendamos estas nociones a sistemas de m ecuaciones lineales con n incógnitas.
Una ecuación lineal con n incógnitas se escribe:

$$a_1\, x_1 + a_2\, x_2 + \ldots + a_n\, x_n = b.$$

Tenemos que escribir m de estas ecuaciones en las que las variables $x_1, x_2, \ldots, x_n$ son las mismas. Para hacerlo en la forma más clara pondremos a cada coeficiente un doble subíndice: el número de ecuación a la que pertenece y luego el número de la variable a la que acompaña. Los coeficientes independientes sólo llevarán el subíndice de la ecuación. Así la cuarta ecuación se escribe:

$$a_{41}\,x_1 + a_{42}\,x_2 + \ldots + a_{4n}\,x_n = b_4.$$

y un sistema de m ecuaciones con n incógnitas resulta:

$$\begin{cases} a_{11}\,x_1 & + a_{12}\,x_2 & + \ldots & + a_{1n}\,x_n & = & b_1 \\ a_{21}\,x_1 & + a_{22}\,x_2 & + \ldots & + a_{2n}\,x_n & = & b_2 \\ a_{31}\,x_1 & + a_{32}\,x_2 & + \ldots & + a_{3n}\,x_n & = & b_3 \\ \vdots & \vdots \quad \vdots & \vdots & \vdots \quad \vdots & \vdots & \vdots \\ a_{m1}\,x_1 & + a_{m2}\,x_2 & + \ldots & + a_{mn}\,x_n & = & b_m \end{cases}$$

Una solución de este sistema será una n-upla $(k_1, k_2, k_3, \ldots, k_n)$ que satisfaga simultáneamente las m ecuaciones. Igual que antes, si esta solución es única el sistema se clasificará como compatible determinado, si tiene infinitas soluciones será compatible indeterminado y si no existe solución alguna será un sistema incompatible. Si en un determinado sistema $b_1 = b_2 = \ldots = b_m = 0$ el sistema se llama *homogéneo*. Un sistema de este tipo claramente nunca va a ser incompatible ya que la n-upla nula es solución. Si es la única, será compatible determinado y si hay infinitas soluciones será compatible indeterminado. Para resolver un sistema de m ecuaciones con n incógnitas podemos emplear cualquiera de los métodos ya vistos, pero tanto el método de igualación como el de sustitución resultan trabajosos porque requieren de muchos pasos.

Apliquemos el método de eliminación de Gauss en forma mecánica: usando la primera ecuación eliminaremos la primera incógnita de todas las demás ecuaciones, usando esta segunda ecuación con una incógnita menos eliminaremos la segunda incógnita de todas las ecuaciones a partir de la tercera y así sucesivamente. Veamos un ejemplo:

Ejemplo 8.2 Sea el sistema

$$\begin{cases} x & + & y & + & 2\,z & - & t & = & -2 \\ 3x & + & 4\,y & + & 3\,z & - & t & = & 5 \\ 2\,x & + & y & - & z & + & 3\,t & = & 14 \\ -x & - & 2\,y & + & z & + & 4\,t & = & 6 \end{cases}$$

Para eliminar la primera variable usamos la primera ecuación:

$$\begin{array}{l} \text{queda como está:} \\ \text{Ec.2 - 3}\times\text{ec.1:}\mapsto \\ \text{Ec.3 - 2}\times\text{ec.1:}\mapsto \\ \text{Ec.4 +1}\times\text{ec.1:}\mapsto \end{array} \begin{cases} x & + & y & + & 2\,z & - & t & = & -2 \\ & & y & - & 3\,z & - & 2\,t & = & 11 \\ & - & y & - & 5\,z & + & 5\,t & = & 18 \\ & - & y & + & 3\,z & + & 3\,t & = & 4 \end{cases}$$

Para eliminar la segunda variable usamos la segunda ecuación:

$$\begin{array}{r} \text{queda como está:} \\ \text{queda como está:} \\ \text{Ec.3 + 1×ec.2:}\mapsto \\ \text{Ec.4 + 1×ec.2:}\mapsto \end{array} \left\{ \begin{array}{rcrcrcrcr} x & + & y & + & 2\,z & - & t & = & -2 \\ & & y & - & 3\,z & - & 2\,t & = & 11 \\ & & & & 8\,z & + & 3\,t & = & 29 \\ & & & & & & 5\,t & = & 15 \end{array} \right.$$

Al anular los coeficientes de las y también se anuló el coeficiente de z en la última ecuación y ya podemos resolver el sistema. Despejando de la última ecuación, obtenemos que $t = 3$, reemplazando en la anterior, resulta $z = -1$, al reemplazar estos dos valores en la segunda ecuación obtenemos que $y = 2$ y finalmente reemplazando los tres en la primera resulta que $x = 1$. La solución única de este sistema es la 4-upla: $(1, 2, -1, 3)$.

No lo demostraremos, pero es fácil ver *a priori* que siempre es posible aplicar este método. En el ejemplo no lo hemos usado, pero es factible reemplazar una ecuación por un múltiplo de ella, intercambiar ecuaciones y claramente, sacar del sistema todas aquellas ecuaciones que se anulen en su totalidad. Cuando hemos agotado este proceso nos puede quedar una última ecuación con una sola incógnita o con más de una. En cualquier caso, si la ecuación es resoluble el sistema se dice compatible, si es resoluble y con una sola incógnita, será compatible determinado. En cualquier otro caso se trata de un sistema incompatible.
En símbolos:

Caso 1: Si la última ecuación es del tipo:

$k_{n-1}\,x_{n-1} + k_n\,x_n = k$, con $k_{n-1} \neq 0$ y $k_n \neq 0$ decimos que

$$x_{n-1} = \frac{k - k_n\,x_n}{k_{n-1}},$$

y el sistema es compatible indeterminado.

Caso 2:Si la última ecuación es del tipo:

$k_n\,x_n = k$ podemos considerar tres casos:

a) $k_n = 0,\ k = 0$, entonces la ecuación se anula y resulta un sistema compatible indeterminado.

b) $k_n = 0,\ k \neq 0$, entonces la ecuación es: $0 \cdot x_n = k \neq 0$ y resulta un sistema incompatible.

c) $k_n \neq 0$, entonces $x_n = \dfrac{k}{k_n}$ y resulta un sistema compatible determinado.

Ejemplo 8.3 Comparemos las eficacias de los métodos pos sustitución, por igualación y por eliminación en un sistema de 3 ecuaciones con 3 incógnitas:
Sea el sistema:

$$\begin{cases} x + y - z = 0 \\ 2x + y + 3z = 1 \\ 2x - y + z = 3 \end{cases}$$

- Resolución por sustitución

Despejamos en la primera ecuación y reemplazamos en las otras:

$z = x + y$, el sistema queda:

$$\begin{cases} 2x + y + 3(x + y) = 1 \\ 2x - y + (x + y) = 3 \end{cases} \quad \text{ó} \quad \begin{cases} 5x + 4y = 1 \\ 3x = 3 \end{cases}$$

Realizando las cuentas pertinentes vemos que punto solución es: $(1, -1, 0)$.

- Resolución por igualación

Depejamos z e igualamos en las ecuaciones 1 y 3, queda: $x + y = 3 - 2x + y$, de donde $x = 1$

Reemplazando este valor en la segunda y tercera ecuaciones resulta:

$$\begin{cases} 2 \cdot 1 + y + 3z = 1 \\ 2 \cdot 1 - y + z = 3 \end{cases} \quad \text{ó} \quad \begin{cases} -y + 3z = -1 \\ -y + z = 1 \end{cases}$$

De donde, nuevamente vemos que el punto solución es: $(1, -1, 0)$.

- Resolución por eliminación

Para eliminar la variable x de la segunda y tercera ecuaciones le restamos la primera multiplicada por 2.

$$\begin{cases} x + y - z = 0 \\ 0x - y + 5z = 1 \\ 0x - 3y + 3z = 3 \end{cases}$$

Para eliminar la variable y en la tercera ecuación le restamos la segunda multiplicada por 3

$$\begin{cases} x + y - z = 0 \\ 0x - y + 5z = 1 \\ 0x + 0y - 12z = 0 \end{cases}$$

Despejamos en este sistema $z = 0$, reemplazando en la segunda ecuación resulta $y = -1$, finalmente reemplazando ambos valores en la primera obtenemos $x = 1$. Nuevamente el punto solución es: $(1, -1, 0)$, con menos pasos intermedios.

8.2. Matrices

En verdad cuando realizamos los cálculos para resolver un sistema de ecuaciones sólo usamos las variables para ubicarlos en el sitio correspondiente. A fin de facilitar la escritura se suelen realizar estos cálculos escribiendo únicamente los coeficientes en un arreglo rectangular que se puede delimitar por paréntesis o por corchetes, en este curso usaremos paréntesis. Si consideramos el sistema de ecuaciones del ejemplo 8.3 todos los números del sistema se pueden ubicar en el arreglo:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 2 & 1 & 3 & 1 \\ 2 & -1 & 1 & 3 \end{array}\right).$$

En algunos libros llaman a esta matriz la matriz del sistema, y la matriz sin los términos independientes, es decir:

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{pmatrix},$$

la llaman matriz reducida. Otros textos llaman matriz del sistema a la matriz sin los términos independientes y matriz ampliada a la que tiene todos los coeficientes del sistema. Independientemente de la denominación reconoceremos fácilmente cuál usar en cada caso.

Por el momento parece caprichoso este hecho, pero cuando aprendamos a trabajar con matrices veremos cómo se escribe un sistema de ecuaciones como una ecuación matricial. Por el momento, demos la definición formal de matriz:

Definición 8.1 Una *matriz* $m \times n$ es un arreglo rectangular de números ubicados en m filas (horizontales) y n columnas (verticales), decimos que esta matriz es de *orden* $m \times n$.

Notamos a cada matriz con una letra mayúscula A y a cada uno de sus elementos los distinguimos con un doble subíndice del mismo modo que a los elementos del sistema de ecuaciones. Es decir a_{23} en un sistema de ecuaciones representa al coeficiente en la ecuación 2 de la variable x_3, ahora es el número que está ubicado en la fila 2 y columna 3.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Veamos un ejemplo numérico:

$$B = \begin{pmatrix} 5 & 3 & -1 & 4 \\ 7 & -3 & 6 & 1 \\ 2 & 0 & -6 & -4 \end{pmatrix}$$

B es una matriz de 3 filas y 4 columnas, por eso decimos que es de orden 3×4.
Identificamos sus elementos como b_{ij} y escribimos: $B = (b_{ij}),\ 1 \leq i \leq m,\ 1 \leq j \leq n$.
Sólo para dar algún ejemplito veamos que $b_{12} = 3,\ b_{33} = -6,\ b_{24} = 1,\ b_{31} = 2,\ b_{32} = 0$.
Aquellas matrices que tienen la misma cantidad de filas que de columnas, digamos n, reciben el nombre de *matrices cuadradas* y decimos que son de *orden* n. Entre las matrices cuadradas podemos distinguir las matrices

triangulares, que pueden ser de dos formas:

triangular superior: $a_{ij} = 0$ si $i > j$,

$$A = \begin{pmatrix} 5 & 3 & -1 \\ 0 & -3 & 6 \\ 0 & 0 & -6 \end{pmatrix}.$$

triangular inferior: $a_{ij} = 0$ si $i < j$,

$$A = \begin{pmatrix} 5 & 0 & 0 \\ 4 & -3 & 0 \\ -2 & 1 & -6 \end{pmatrix}.$$

matrices diagonales: $a_{ij} = 0$ si $i \neq j$,

$$A = \begin{pmatrix} 5 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -6 \end{pmatrix}.$$

escalares: Matriz escalar tal que: $a_{ii} = k$,

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Del mismo modo que agrupamos los polinomios en un conjunto y definimos $\mathbb{P}_n[\mathbb{K}]$ como el conjunto de polinomios a coeficientes en el cuerpo $\mathbb{K}$, de grado menor o igual que n, definimos $\mathbb{M}_{m\times n}(\mathbb{K})$, el conjunto de las matrices de orden $m \times n$ a coeficientes en el cuerpo $\mathbb{K}$. Claramente $\mathbb{M}_n(\mathbb{K})$, denota el conjunto de las matrices cuadradas de orden n a coeficientes en el cuerpo $\mathbb{K}$.

Antes de continuar trabajando con matrices propiamente dichas, usémoslas como notación para la resolución de sistemas de ecuaciones. Si quisiéramos resolver el sistema 8.3 usando matrices escribiríamos lo siguiente:
La matriz asociada al sistema, para este cálculo es:

$$\begin{pmatrix} 1 & 1 & 1 & \vdots & 0 \\ 2 & 1 & 3 & \vdots & 1 \\ 2 & -1 & 1 & \vdots & 3 \end{pmatrix}$$

Comencemos el proceso de triangulación:

$$\begin{array}{r} \\ F_2 - 2.F_1 :\mapsto \\ F_3 - 2.F_1 :\mapsto \end{array} \quad \begin{pmatrix} 1 & 1 & 1 & \vdots & 0 \\ 0 & -1 & 1 & \vdots & 1 \\ 0 & -3 & -1 & \vdots & 3 \end{pmatrix}$$

$$\begin{array}{r} \\ \\ F_3 - 3.F_2 :\mapsto \end{array} \quad \begin{pmatrix} 1 & 1 & 1 & \vdots & 0 \\ 0 & -1 & 1 & \vdots & 1 \\ 0 & 0 & -4 & \vdots & 0 \end{pmatrix}$$

Volvemos a armar el sistema de ecuaciones:

$$\begin{cases} x + y + z = 0 \\ -y + z = 1 \\ -4z = 0 \end{cases}$$

Despejamos en este sistema $z = 0$, lo reemplazamos en la segunda ecuación y resulta $y = -1$, finalmente reemplazando ambos valores en la primera obtenemos $x = 1$. Recordemos nuevamente que la solución es: $(1, -1, 0)$.

8.2.1. Operaciones con matrices

El primer paso antes de comenzar a operar es determinar cuándo dos matrices son iguales. Comenzaremos pidiendo que tengan el mismo orden, y luego que los elementos ubicados en el mismo sitio sean iguales. Formalicemos esto:

Igualdad de matrices

Dadas $A = (a_{ij})$, $B = (b_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$, decimos que $A = B$ si $a_{ij} = b_{ij}$ para todo $1 \le i \le m,\ 1 \le j \le n$.

Suma de matrices

Dadas $A = (a_{ij})$, $B = (b_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$, definimos la suma de matrices, simplemente elemento a elemento.
Es decir:
$S = A + B$ es la matriz $S = (s_{ij})$ tal que para todo $1 \le i \le m,\ 1 \le j \le n$ tenemos $s_{ij} = a_{ij} + b_{ij}$.

Ejemplo 8.4 Dadas: $A = \begin{pmatrix} 1 & 3 & -5 \\ 2 & 4 & -1 \end{pmatrix}, B = \begin{pmatrix} 4 & 3 & 3 \\ 2 & -2 & 5 \end{pmatrix}$

$$A + B = \begin{pmatrix} 1+4 & 3+3 & -5+3 \\ 2+2 & 4-2 & -1+5 \end{pmatrix} = \begin{pmatrix} 5 & 6 & -2 \\ 4 & 2 & 4 \end{pmatrix}.$$

En verdad no hemos definido nada nuevo, sino simplemente hemos "heredado" a las matrices la suma que ya teníamos definida en el cuerpo y, en consecuencia, esta suma conservará exactamente todas sus propiedades.

Propiedades

Dadas $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$

- S_1: $(A + B) + C = A + (B + C)$, (propiedad asociativa)
- S_2: $A + B = B + A$, (propiedad conmutativa)
- S_3: Existe una matriz 0 tal que $A + 0 = 0 + A = A$, (elemento neutro)
- S_4: Dada A existe $-A$ tal que $A + (-A) = (-A) + A = 0$, (el. simétrico)

La demostración de estas propiedades es muy sencilla, y quedan a cargo del lector interesado las propiedades S_1 y S_2. Sólo vamos a trabajar sobre la S_3 y la S_4 para "construir" el neutro y el simétrico.

- S_3: Existe una matriz 0 tal que $A + 0 = 0 + A = A$, (elemento neutro)
  Sean $A = (a_{ij})$ y $0 = (x_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$, queremos que $A + 0 = A$, por lo tanto lo que queremos es que $a_{ij} = a_{ij} + x_{ij}$ para todo $1 \le i \le m,\ 1 \le j \le n$. Claramente, por las propiedades de la suma en el cuerpo $\mathbb{K}$ vemos que $x_{ij} = 0$ para todo $1 \le i \le m,\ 1 \le j \le n$. Así encontramos

que el elemento neutro es la matriz que tiene en cada lugar el elemento neutro del cuerpo. En nuestro caso:

$$0 = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

S_4: Dada A existe $-A$ tal que $A + (-A) = (-A) + A = 0$, (el. simétrico) Sean $A = (a_{ij})$ y $-A = (x_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$, queremos que $A + (-A) = 0$, por lo tanto lo que queremos es que $a_{ij} + x_{ij} = 0$ para todo $1 \leq i \leq m,\ 1 \leq j \leq n$. Claramente, por las propiedades de la suma en el cuerpo $\mathbb{K}$ vemos que $x_{ij} = -a_{ij}$ para todo $1 \leq i \leq m,\ 1 \leq j \leq n$. Así encontramos que el simétrico de una matriz es la matriz que tiene en cada lugar el elemento simétrico del cuerpo. En nuestro caso:

$$A = \begin{pmatrix} 1 & 2 & -4 & 5 \\ 5 & 6 & -1 & 9 \\ 2 & 5 & -1 & 0 \end{pmatrix}, \qquad -A = \begin{pmatrix} -1 & -2 & 4 & -5 \\ -5 & -6 & 1 & -9 \\ -2 & -5 & 1 & 0 \end{pmatrix}$$

Producto por un escalar

Dada $A = (a_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$ y $k \in \mathbb{K}$, definimos el producto por un *escalar* (es decir, por un elemento del cuerpo), del mismo modo que definimos el producto de un polinomio por un escalar, simplemente elemento a elemento. Es decir:
Dada A, $k \cdot A$ es $k \cdot A = (k \cdot a_{ij})$ para todo $1 \leq i \leq m,\ 1 \leq j \leq n$.

Ejemplo 8.5 Dadas: $A = \begin{pmatrix} 1 & 3 \\ 2 & 4 \\ -1 & 6 \end{pmatrix}$, $7 \cdot A = \begin{pmatrix} 7 & 21 \\ 14 & 28 \\ -7 & 42 \end{pmatrix}$

Veamos que este producto tiene las mismas propiedades que en polinomios:

Propiedades

Dadas $A = (a_{ij})$, $B = (b_{ij}) \in \mathbb{M}_{m\times n}(\mathbb{K})$ y $k, k' \in \mathbb{K}$

1. $k \cdot (A + B) = k \cdot A + k \cdot B$
2. $(k + k') \cdot A = k \cdot A + k' \cdot A$

3. $(k \cdot k') \cdot A = k \cdot (k' \cdot A)$
4. $1 \cdot A = A$ (Ley de conservación de la identidad)

La demostración de todas estas propiedades es muy sencilla y es absolutamente accesible a las habilidades del lector interesado.®

Producto de matrices

Más adelante vamos a ver cómo las matrices están asociadas a funciones y el producto de matrices estará asociado a la composición de funciones. Por este motivo la definición del producto de matrices que *a priori* podría resultar un tanto caprichosa resulta totalmente lógica. En primer lugar analicemos que una matriz A de orden $m \times n$ se puede asociar a una función, llamémosla f de $\mathbb{R}^n$ en $\mathbb{R}^m$, la matriz B de orden $n \times p$ la asociamos a una función g de $\mathbb{R}^n$ en $\mathbb{R}^p$. Si queremos realizar la composición, podremos encontrar $g \circ f : \mathbb{R}^m \to \mathbb{R}^p$. Y esta composición sólo es posible si el conjunto de llegada de f coincide con el conjunto de salida de g, y debemos sumar paso a paso los n productos.

Veamos un ejemplo de producto y luego daremos la definición formal:

Sean $A = (a_{ij}) \in \mathbb{M}_{2\times3}(\mathbb{K})$ y $B = (b_{ij}) \in \mathbb{M}_{3\times5}(\mathbb{K})$, por ejemplo:

$$A = \begin{pmatrix} 1 & 3 & -2 \\ 4 & 0 & 3 \end{pmatrix}, \; B = \begin{pmatrix} 4 & -3 & 2 & 3 & -2 \\ 6 & 3 & -2 & 1 & 5 \\ 1 & -1 & 2 & 3 & 3 \end{pmatrix}$$

Por lo que acabamos de decir $P = A \times B \in \mathbb{M}_{2\times5}(\mathbb{K})$.

Llamamos $P = (p_{ij})$ a la matriz producto y sabemos que $1 \leq i \leq 2, 1 \leq j \leq 5$. Construyamos todos los p_{ij}, recordando que en cada caso debemos recorrer toda la fila i de la matriz A y la columna j de la matriz B:

$$p_{11} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31} = 1 \cdot 4 + 3 \cdot 6 + (-2) \cdot 1 = 4 + 18 - 2 = 20$$
$$p_{12} = a_{11} \cdot b_{12} + a_{12} \cdot b_{22} + a_{13} \cdot b_{32} = 1 \cdot (-3) + 3 \cdot 3 + (-2) \cdot (-1) = -3 + 9 + 2 = 8$$
$$p_{13} = a_{11} \cdot b_{13} + a_{12} \cdot b_{23} + a_{13} \cdot b_{33} = 1 \cdot 2 + 3 \cdot (-2) + (-2) \cdot 2 = 2 - 6 - 4 = -8$$
$$p_{14} = a_{11} \cdot b_{14} + a_{12} \cdot b_{24} + a_{13} \cdot b_{34} = 1 \cdot 3 + 3 \cdot 1 + (-2) \cdot 3 = 3 + 3 - 6 = 0$$
$$p_{15} = a_{11} \cdot b_{15} + a_{12} \cdot b_{25} + a_{13} \cdot b_{35} = 1 \cdot (-2) + 3 \cdot 5 + (-2) \cdot 3 = -2 + 15 - 6 = 7$$
$$p_{21} = a_{21} \cdot b_{11} + a_{22} \cdot b_{21} + a_{23} \cdot b_{31} = 4 \cdot 4 + 0 \cdot 6 + 3 \cdot 1 = 4 + 0 + 3 = 7$$

$$p_{22} = a_{21} \cdot b_{12} + a_{22} \cdot b_{22} + a_{23} \cdot b_{32} = 4 \cdot (-3) + 0 \cdot 3 + 3 \cdot (-1) = -12 + 0 - 3 = -15$$
$$p_{23} = a_{21} \cdot b_{13} + a_{22} \cdot b_{23} + a_{23} \cdot b_{33} = 4 \cdot 2 + 0 \cdot (-2) + 3 \cdot 2 = 8 + 0 + 6 = 14$$
$$p_{24} = a_{21} \cdot b_{14} + a_{22} \cdot b_{24} + a_{23} \cdot b_{34} = 4 \cdot 3 + 0 \cdot 1 + 3 \cdot 3 = 12 + 0 + 9 = 21$$
$$p_{25} = a_{21} \cdot b_{15} + a_{22} \cdot b_{25} + a_{23} \cdot b_{35} = 4 \cdot (-2) + 0 \cdot 5 + 3 \cdot 3 = -8 + 0 + 9 = 1$$

La matriz producto queda finalmente:

$$P = A \times B = \begin{pmatrix} 20 & 8 & -8 & 0 & 7 \\ 7 & -15 & 14 & 21 & 1 \end{pmatrix}.$$

Habiendo hecho el procedimiento en un caso particular, demos la definición formal:

Dadas $A = (a_{ik}) \in \mathbb{M}_{m \times n}(\mathbb{K})$, $B = (b_{kj}) \in \mathbb{M}_{n \times p}(\mathbb{K})$ definimos el producto de matrices, y lo notamos $P = A \times B$ a la matriz $P = (p_{ij})$ tal que

$p_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + a_{i3} \cdot b_{3j} + \ldots + a_{in} \cdot b_{nj}$ para cada $1 \leq i \leq m, \ 1 \leq j \leq n$. Esta definición suele escribirse:

$$P = A \times B = \left(\sum_{k=1}^{p} a_{ik} \cdot b_{kj} \right)$$

Observación 8.1 Ya que hemos definido el producto, consideremos la matriz

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{pmatrix}$$

(que llamamos matriz reducida en el ejemplo 8.3), y multipliquémosla por la matriz columna

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Obtenemos:

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x + y + z \\ 2x + y + 3z \\ 2x - y + z \end{pmatrix}$$

que son las ecuaciones del sistema del ejemplo 8.3, por lo tanto este sistema de ecuaciones lo podemos escribir como una ecuación de matrices:

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$$

Propiedades

Si pensamos en el producto de matrices como composición de funciones, nos va a resultar natural conprobar que tienen las mismas propiedades. Enunciémoslas:
Dadas A, B, C matrices en condiciones de realizar las operaciones:

P_1: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$, (propiedad asociativa)

P_2: Existe una matriz I tal que $A \cdot I = I \cdot A = A$, (elemento neutro)

P_3: $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$

$(B + C) \cdot A = (B \cdot A) + (C \cdot A)$. (propiedad distributiva)

P_4: $k \cdot (A \cdot B) = (k \cdot A) \cdot B = A \cdot (k \cdot B)$, para todo $k \in \mathbb{K}$.

La demostración de la propiedad asociativa es bastante engorrosa (aunque no imposible), por una cuestión de notación. También son sencillas, pero omitiremos las demostraciones de la distributividad del producto con respecto a la suma (tanto a derecha como a izquierda) y del producto por un escalar. Sí vamos a salir a la "pesca" de la matriz identidad del mismo modo que encontramos la matriz nula.
En primer lugar veamos que tienen que estar definidos $A \cdot I$ y $I \cdot A$, de donde deducimos que I es una matriz cuadrada del mismo orden que A.
En efecto, si $A \in \mathbb{M}_{m\times n}(\mathbb{K})$, para que esté definido $A \cdot I$, debe ser $I \in \mathbb{M}_{n\times p}(\mathbb{K})$, y para que $A \cdot I = A$, $p = n$, de donde $I \in \mathbb{M}_n(\mathbb{K})$ pero también está definido $I \cdot A$, de donde $n = m$ y resulta que la matriz A también es cuadrada y del mismo orden de I.
Veamos ahora qué elementos conforman la matriz identidad:
Sea $A = (a_{ij}), I = (x_ij), 1 \leq i, j \leq n$. Como $A \cdot I = A$ tenemos que para todo $1 \leq i, j \leq n$:

$$a_{i1} \cdot x_{1j} + a_{i2} \cdot x_{2j} + \ldots + a_{ij} \cdot x_{jj} + \ldots + a_{in} \cdot x_{nj} = a_{ij}$$

lo cual se verifica fácilmente considerando $x_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{en otro caso.} \end{cases}$

De este modo vemos que la matriz identidad es una matriz cuadrada cuyos elementos son todos cero, salvo los que están en la diagonal principal. Solemos subindicar la identidad con su orden respectivo, así:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Pero no se verifican la propiedad conmutativa ni la existencia de inverso para todos los elementos:

1. $A \cdot B \neq B \cdot A$, (propiedad conmutativa)
2. Para cada $A \neq 0$ no siempre existe A^{-1} tal que $A\cdot(A^{-1}) = (A^{-1})\cdot A = I$, (elemento inverso)

Para la propiedad conmutativa en general podemos ver que simplemente en algunos casos resulta imposible. Por ejemplo, si A es una matrix de orden 2×3 y B una matriz de orden 3×5 podemos realizar el producto $A \cdot B$, pero el $B \cdot A$ simplemente no está definido. Pensemos, entonces, en matrices cuadradas, ya que ambos productos están definidos, ¿podrá ser conmutativo? Igual que en el caso de las funciones, a veces, sólo a veces y para un conjunto de funciones especiales, conmuta, pero en general no es cierto.
Veamos un ejemplo:

$$\begin{pmatrix} 5 & 3 \\ 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 19 \\ 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 5 & 3 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 1 & -6 \end{pmatrix}$$

Claramente no es necesario realizar el producto completo, basta con comparar dos elementos y que de diferente.
Se puede demostrar con relativa sencillez que las matrices escalares y en general las matrices diagonales sí son conmutativas. (Ejercicio para el lector ávido de aprender.)®
Para la no existencia de inverso, veamos que hay matrices que no son nulas y su producto sí lo es.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Combinando esto con la propiedad asociativa, vemos que estas matrices no pueden tener inversa. Supongamos que A es una matriz tal que existe B, una matriz no nula que verifica $A \cdot B = 0$ y supongamos, por el absurdo, que existe A^{-1}. Entonces, por la propiedad asociativa:

$$0 = A^{-1} \cdot 0 = A^{-1} \cdot (A \cdot B) = (A^{-1} \cdot A) \cdot B = I_n \cdot B = B,$$

lo cual es un absurdo que provino de suponer que existe la inversa de tal matriz A. Por lo tanto afirmamos que hay matrices que no tienen inversa.

Potencia natural de una matriz

Una vez definido el producto, la definición de la potencia natural en forma recursiva es inmediata. Dada una matriz cuadrada de orden n:

$$\begin{aligned} &A^0 = I_n \\ &A^{k+1} = A^k \cdot A. \end{aligned}$$

Transposición de matrices

Ya que ahora conocemos las matrices, veamos una representación de relaciones que usa matrices: Sea $A = \{a, e, i\}, B = \{m, n\}$ y

$$\mathcal{R} \subseteq A \times B = \{(a, m), (a, n), (e, n), (i, n)\},$$

una representación de esta relación es construir una matriz $\mathcal{R} = (r_{ij})$ con tantas filas como elementos de A y tantas columnas como elementos de B, fuera de la matriz ponemos como primera columna los elementos del conjunto A y como primera fila los elementos del conjunto B, en nuestro caso tenemos las columnas m, n y las filas a, e, i cada elemento r_{ij} será 1 si el par $(i, j) \in \mathcal{R}$ y 0 en caso contrario. En nuestro ejemplo:

$$\begin{array}{c} \\ a \\ e \\ i \end{array} \begin{array}{c} \begin{array}{cc} m & n \end{array} \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \end{array}$$

¿Cómo representaríamos de este modo la relación $\mathcal{R}^{op}$? Escrita como conjunto queda:
$\mathcal{R}^{op} = \{(m, a), (n, a), (n, e), (n, i)\}$ y como matriz resulta:

$$\begin{array}{c} \\ m \\ n \end{array} \begin{array}{c} \begin{array}{ccc} a & e & i \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \end{array}$$

Esto motiva la siguiente definición: Dada una matriz $A = (a_{ij}) \in M_{m\times n}(\mathbb{K})$ se define la *transpuesta* de A y se nota A^t a la matriz que se obtiene intercambiando filas y columnas. En símbolos:

$$\text{Dada } A = (a_{ij}) \in M_{m\times n}(\mathbb{K}), \text{ tenemos } A^t = (a_{ji}) \in M_{n\times m}(\mathbb{K})$$

Ejemplo 8.6 Sea $A = \begin{pmatrix} 2 & 3 & 7 \\ 4 & 5 & 3 \\ 1 & 1 & 0 \\ 4 & 6 & 9 \end{pmatrix}$, $A^t = \begin{pmatrix} 2 & 4 & 1 & 4 \\ 3 & 5 & 1 & 6 \\ 7 & 3 & 0 & 9 \end{pmatrix}$.

Vemos que $A \in M_{4\times 3}(\mathbb{K})$ y $A \in M_{3\times 4}(\mathbb{K})$

Recordemos que las relaciones que cumplen ciertas propiedades son funciones y las funciones con ciertas propiedades son inversibles. Hemos visto que en este caso si tomamos esta función inversible como relación, la inversa de la función coincide con la relación opuesta. No nos sorprendamos cuando más adelante encontremos ciertas matrices cuya inversa coincide con la transpuesta.

Propiedades

Considerando siempre matrices A, B, C para las que estén definidas las operaciones:

T_1: $(A^t)^{\,t} = A$,

T_2: $(A+B)^t = A^t + B^t$,

T_3: $(k \cdot A)^t = k \cdot A^t$,

T_4: $(A \cdot B)^t = B^t \cdot A^t$.

La demostración de las primeras propiedades es casi inmediata y queda a cargo del lector interesado. La última, más que demostrarla vamos a comentarla. Si asociamos las matrices a relaciones, pensamos el producto como composición y la transposición como la relación opuesta, vemos que ya hemos demostrado esta propiedad con otro lenguaje.

Determinante de una matriz

Cuando hablamos de sistemas de ecuaciones lineales comenzamos por intentar solucionar un sistema de dos ecuaciones con dos incógnitas.
Dado el sistema

$$\begin{cases} a_{11}\,x_1 + a_{12}\,x_2 = b_1 \\ a_{21}\,x_1 + a_{22}\,x_2 = b_2 \end{cases}$$

le asociamos la matriz

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

y vimos que el sistema es determinado si

$$a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0.$$

Podemos observar que la cuenta que hicimos es la suma algebraica de todos los productos de elementos posibles en los que no se repitan filas ni columnas, con el signo afectado por el ordenamiento entre ellos. Parece complicado, pero en verdad es sencillo. Comencemos por la primera columna: Si tomo el elemento a_{11} como no puedo repetir filas ni columnas la única posibilidad a mi alcance es multiplicarlo por a_{22}, escribo el producto ordenado por los primeros subíndices y miro el orden de los segundos: $a_{11}\ .\ a_{22}$, el orden de los primeros es 1,2 y también el orden de los segundos: 1,2, por lo tanto le corresponde signo $+$. Me queda el elemento a_{12}, para no repetir filas ni columnas sólo puedo multiplicarlo por el a_{21}. Escribo el producto ordenado por los primeros subíndices y miro el orden de los segundos: $a_{12}\ .\ a_{21}$, el orden de los primeros es 1,2 pero el orden de los segundos: 2,1, es decir, están "desordenados", por lo tanto le corresponde signo $-$. No hay más elementos en la matriz y el determinante queda expresado:

$$det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}\ .\ a_{22} - a_{12}\ .\ a_{21}.$$

Escapa a este curso fundamentar las razones por las cuales es así, pero "funciona" para sistemas de $n \times n$. Hagamos el cálculo para 3×3, es decir, calculemos :

$$det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

En verdad, como no se tienen que repetir nunca las filas ni las columnas, en los primeros subíndices tiene que estar 1,2,3 y también en los segundos. Analizaremos cuántos intercambios del ordenamiento natural con el que escribimos las i fueron necesarios para llegar al ordenamiento de las j y por cada uno de ellos cambiamos el signo

productos posibles	orden de las i	orden de las j	proceso de intercambios	signo
$a_{11} \cdot a_{22} \cdot a_{33}$	1 - 2 - 3	1 - 2 - 3	sin intercambios	$+$
$a_{11} \cdot a_{23} \cdot a_{32}$	1 - 2 - 3	1 - 3 - 2	(2-3)	$-$
$a_{12} \cdot a_{21} \cdot a_{33}$	1 - 2 - 3	2 - 1 - 3	(1-2)	$-$
$a_{12} \cdot a_{23} \cdot a_{31}$	1 - 2 - 3	2 - 3 - 1	(1-2) y (2-3)	$+$
$a_{13} \cdot a_{22} \cdot a_{31}$	1 - 2 - 3	3 - 2 - 1	(1-3)	$-$
$a_{13} \cdot a_{21} \cdot a_{32}$	1 - 2 - 3	3 - 1 - 2	(1-3) y (1-2)	$+$

Finalmente el determinante de una matriz de orden 3 queda:

$$det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$$

$$= a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33} - a_{13} \cdot a_{22} \cdot a_{31}.$$

Podríamos continuar con el cálculo de un determinante de orden 4(¡agh!). Vemos al hacer la construcción que la cantidad de sumandos es exactamente la cantidad de ordenamientos de los subíndices j, es decir la cantidad de órdenes distintos con n elementos. Para $n = 2$ son $2 = 2 \cdot 1$ (1-2 y 2-1); para $n = 3$ son $6 = 3 \cdot 2 \cdot 1$ (1-2-3 , 1-3-2 , 2-1-3 , 2-3-1 , 3-1-2 , 3-2-1); para $n = 4$ son $24 = 4 \cdot 3 \cdot 2 \cdot 1$ y ya para $n = 5$ son 120. El número crece desmesuradamente y debemos hacer algo para simplificar nuestros cálculos de determinante.

En primer lugar veamos que para los determinantes de orden 2 y 3 podemos "seguir un diseño", pero <u>sólo para orden 2 y 3</u>:

$$det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{array}{c} + \qquad\qquad - \\ \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \end{array} =$$

$$= a_{11} \cdot a_{22} - a_{12} \cdot a_{21}.$$

Para el determinante de orden 3, vamos a copiar dos filas más, para que el "dibujo" se vea más claro:

$$det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{array}{c} + \qquad\qquad\qquad - \\ \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \\ \begin{matrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{matrix} \end{array} =$$

$$= \; a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33} - a_{13} \cdot a_{22} \cdot a_{31}.$$

Al realizar estos cálculos he utilizado una notación muy habitual para el determinante que es escribir la matriz entre líneas. Y se acabó lo que se daba. A partir de ahora tendremos que buscar otros caminos para resolver el determinante. <u>Ya no hay más "diseños"</u>, lamentablemente. No intenten con las de 4×4 porque no funciona. Pero antes vamos a ver algunos ejemplos numéricos:

Ejemplo 8.7 Veamos un cálculo de un determinante de orden 2 y uno de orden 3:

1. $det\begin{pmatrix} 2 & 3 \\ -1 & -6 \end{pmatrix} = 2 \cdot (-6) - (-1) \cdot 3 = -12 + 3 = -9.$

2. $det \begin{pmatrix} 3 & -1 & 2 \\ -1 & 4 & 2 \\ 2 & -1 & 3 \end{pmatrix} = 21$. En efecto, hagamos el "truquito":

$$\begin{array}{ccc} + & & - \\ \left|\begin{array}{ccc} 3 & -1 & 2 \\ -1 & 4 & 2 \\ 2 & -1 & 3 \end{array}\right| & = & \\ \begin{array}{ccc} 3 & -1 & 2 \\ -1 & 4 & 2 \end{array} & & \end{array}$$

$$= 3\cdot4\cdot3+(-1)\cdot(-1)\cdot2+2\cdot(-1)\cdot2-2\cdot4\cdot2-2\cdot(-1)\cdot3-3\cdot(-1)\cdot(-1).$$

Propiedades de los determinantes

Dado que el mayor inconveniente que presenta el cálculo con determinantes es la notación, enunciaremos las propiedades en lenguaje habitual, evitando el uso excesivo de notaciones confusas.

D_1: El determinante de una matriz coincide con el de su transpuesta.
La demostración de esta propiedad puede ser engorrosa, pero si vamos a considerar las sumas algebraicas de todos los productos posibles y el signo de cada término depende de la ubicación relativa, intuitivamente vemos que no habrá cambios.

Ejemplo 8.8 $det \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} = 2\cdot4-3\cdot1$, $det \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = 2\cdot4-1\cdot3$

Debido a esta propiedad, cuando pensamos en determinantes ya no hablamos de *filas* o *columnas*, sino simplemente *líneas* porque cualquier cosa que se cumpla para una fila (o columna) se cumple indistintamente para una columna (o fila).

D_2: Si una línea de la matriz está constituída por cero, entonces el determinante es nulo.

Ejemplo 8.9 $det \begin{pmatrix} 0 & 0 \\ 1 & 4 \end{pmatrix} = 0\cdot4-0\cdot1 = 0$, $det \begin{pmatrix} 2 & 0 \\ 3 & 0 \end{pmatrix} = 2\cdot0-0\cdot3 = 0$

D_3: Si se intercambian dos líneas, cambia el signo del determinante.

Ejemplo 8.10 $det \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} = 2\cdot4-3\cdot1$, $det \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix} = 1\cdot3-4\cdot2$

D_4: Si la matriz tiene dos líneas iguales, el determinante es 0.

Ejemplo 8.11 $det\begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} = 2{\cdot}3-3{\cdot}2 = 0$, $det\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} = 2{\cdot}3-2{\cdot}3 =$ 0

D_5: Si se multiplican todos los elementos de una línea por k, el determinante se multiplica por k.

Ejemplo 8.12 $det\begin{pmatrix} 2\cdot k & 3 \\ 1\cdot k & 4 \end{pmatrix} = 2\cdot k\cdot 4 - 3\cdot 1\cdot k = k\cdot(2\cdot 4 - 3\cdot 1)$

$$det\begin{pmatrix} 2 & 1 \\ 3\cdot k & 4\cdot k \end{pmatrix} = 2\cdot 4\cdot k - 1\cdot 3\cdot k = (2\cdot 4 - 1\cdot 3)\cdot k$$

De esta propiedad podemos sacar inmediatamente otra. Si A es una matriz de orden n, entonces $det(k\cdot A) = k^n \cdot detA$. Esto es fácil de ver, ya que para cada línea “sale” una k.

Ejemplo 8.13 $det\begin{pmatrix} 2\cdot k & 1\cdot k \\ 3\cdot k & 4\cdot k \end{pmatrix} = 2\cdot k\cdot 4\cdot k - 1\cdot k\cdot 3\cdot k =$

$$= (2\cdot k\cdot 4 - 1\cdot k\cdot 3)\cdot k = (2\cdot 4 - 1\cdot 3)\cdot k^2$$

D_6: Si una matriz tiene dos líneas proporcionales, su determinante es cero. Esto lo podemos ver fácilmente aplicando las propiedades 4 y 5 por 5 sale la constante afuera y quedan dos líneas iguales, entonces por 4 el determinante es cero.

Ejemplo 8.14 $det\begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix} = det\begin{pmatrix} 2 & 3 \\ 2\cdot 2 & 2\cdot 3 \end{pmatrix} = 2\cdot(2\cdot 3 - 3\cdot 2) = 0$

D_7: Si una línea puede escribirse como sumas, en cierto modo se “distribuye” el determinante. Veamos un ejemplo numérico para aclarar esta propiedad:

Ejemplo 8.15 $det\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} = det\begin{pmatrix} 2 & 6-3 \\ 1 & 0+4 \end{pmatrix} \overset{\text{fórmula}}{=}$

$$2\cdot(0+4) - (6-3)\cdot 1 \overset{\text{p.distributiva}}{=}$$

$$= 2\cdot 0 + 2\cdot 4 - 6\cdot 1 - (-3)\cdot 1 \overset{\text{reordenando}}{=}$$

$$= (2\cdot 0\cdot 6\cdot 1) + (2\cdot 4 - (-3)\cdot 1) \overset{\text{fórmula}}{=}$$

$$= det\begin{pmatrix} 2 & 6 \\ 1 & 0 \end{pmatrix} + det\begin{pmatrix} 2 & -3 \\ 1 & 4 \end{pmatrix}.$$

D_8: El determinante de una matriz no varía si en una línea se coloca esa misma línea más un múltiplo de otra. Esta propiedad es consecuencia de 7 y 6 y nuevamente la entenderemos mejor con un ejemplo:

Ejemplo 8.16 $det\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} = 2\cdot 4 - 3\cdot 1 = 5.$

Escribamos en F_2, $F_2 - F_1$ y calculemos el determinante:

$$det\begin{pmatrix} 2 & 3 \\ 1-2 & 4-3 \end{pmatrix} \overset{D7}{=}$$

$$= det\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + det\begin{pmatrix} 2 & 3 \\ -2 & -3 \end{pmatrix} \overset{D5}{=}$$

$$= det\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} - det\begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} \overset{D4}{=}$$

$$= det\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + 0 = det\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}.$$

D_9: El determinante de una matriz triangular, es el producto de los elementos de la diagonal.
Esto es muy fácil de ver intuitivamente, ya que cada término que tenga un factor fuera de la diagonal se anula. Veamos un ejemplo con una matriz de orden 3:

Ejemplo 8.17 $det\begin{pmatrix} 1 & 3 & 5 \\ 0 & -2 & 7 \\ 0 & 0 & 3 \end{pmatrix} =$

$$= 1\cdot(-2)\cdot 3 + 0\cdot 0\cdot 5 + 0\cdot 3\cdot 7 - 5\cdot(-2)\cdot 0 - 7\cdot 0\cdot 1 - 3\cdot 3\cdot 0 =$$
$$= 1\cdot(-2)\cdot 3 = -6.$$

Sumemos todas las propiedades vistas haste el momento y podemos afirmar que si triangulamos una matriz reemplazando cada línea por ella misma más un múltiplo de otra, finalmente el determinante será simplemente el producto de los elementos en la diagonal. Veamos un ejemplo:

Ejemplo 8.18 $det\begin{pmatrix} 1 & 1 & 4 \\ 2 & 3 & 6 \\ 5 & 4 & 3 \end{pmatrix} = -19.$

$$= det \begin{pmatrix} 1 & 1 & 4 \\ 2 & 3 & 6 \\ 5 & 4 & 3 \end{pmatrix} \qquad \text{copiamos la matriz}$$

$$= det \begin{pmatrix} 1 & 1 & 4 \\ 0 & 1 & -2 \\ 5 & 4 & 3 \end{pmatrix} \qquad \text{en } F_2 \text{ ponemos } F_2 - 2F_1$$

$$= det \begin{pmatrix} 1 & 1 & 4 \\ 0 & 1 & -2 \\ 0 & -1 & -17 \end{pmatrix} \qquad \text{en } F_3 \text{ ponemos } F_3 - 5F_1$$

$$= det \begin{pmatrix} 1 & 1 & 4 \\ 0 & 1 & -2 \\ 0 & 0 & -19 \end{pmatrix} = -19 \qquad \text{en } F_3 \text{ ponemos } F_3 + F_2$$

Observación 8.2 Hemos visto en 7 que podemos "distribuir" el determinante en sumas de determinantes. No creamos por esto que el determinante de la suma es la suma de los determinantes. Esto lo podemos ver en un ejemplo sencillo:

Sean $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Entonces $A + B = I_2$, y tenemos que $|A| = |B| = 0$, pero $|A + B| = 1$. Una de las condiciones para definir el determinante es que la matriz sea cuadrada, es factible que no exista el determinante de dos matrices, pero sí exista el determinante del producto de las matrices.

Sean $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & -2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -1 \\ 4 & 3 \\ -5 & 2 \end{pmatrix}$, $A \cdot B = \begin{pmatrix} -6 & 11 \\ 29 & 5 \end{pmatrix}$

Claramente no está definido el determinante de la matriz A ni de B, pero sí el determinante del producto.
Finalmente, pero no menos importante, destacamos que el producto del determinante es, efectivamente el determinan del producto, en caso de que ambos existan.

$$|A \cdot B| = |A| \cdot |B|$$

Veremos más adelante cuáles son los requisitos para que exista la inversa de una matriz, pero en caso de existir la inversa de una matriz A de orden n, se verifica

$$A \cdot A^{-1} = I_n.$$

como el determinante distribuye con respecto al producto resulta:

$$|A| \cdot |A^{-1}| = |I_n| = 1, \text{ y, en consecuencia, } |A^{-1}| = \frac{1}{|A|}.$$

Desarrollo del determinante por los elementos de una línea

Analicemos el resultado obtenido en 8.2.1 para una matriz de orden 3.

productos posibles	orden de las i	orden de las j	proceso de intercambios	signo
$a_{11} \cdot a_{22} \cdot a_{33}$	1 - 2 - 3	1 - 2 - 3	sin intercambios	$+$
$a_{11} \cdot a_{23} \cdot a_{32}$	1 - 2 - 3	1 - 3 - 2	(2-3)	$-$
$a_{12} \cdot a_{21} \cdot a_{33}$	1 - 2 - 3	2 - 1 - 3	(1-2)	$-$
$a_{12} \cdot a_{23} \cdot a_{31}$	1 - 2 - 3	2 - 3 - 1	(1-2) y (2-3)	$+$
$a_{13} \cdot a_{22} \cdot a_{31}$	1 - 2 - 3	3 - 2 - 1	(1-3)	$-$
$a_{13} \cdot a_{21} \cdot a_{32}$	1 - 2 - 3	3 - 1 - 2	(1-3) y (1-2)	$+$

Finalmente el determinante de una matriz de orden 3 queda:

$$D = det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$$

$$= a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33} - a_{13} \cdot a_{22} \cdot a_{31}.$$

Consideremos una línea cualquiera, por ejemplo, la segunda fila: a_{21}, a_{22}, a_{23}: buscamos estos elementos en el determinante de la matriz y los sacamos factor común, ordenándolos según su aparición en la matriz:

D= $a_{11} \,.\underline{a_{22}} \cdot a_{33} + a_{12}.\underline{a_{23}} \cdot a_{31} + a_{13} \cdot \underline{a_{21}} \cdot a_{32} - a_{11} \cdot \underline{a_{23}} \cdot a_{32} - a_{12} \cdot \underline{a_{21}} \cdot a_{33} - a_{13} \cdot \underline{a_{22}} \cdot a_{31} =$

$= -a_{12} \cdot \underline{a_{21}} \cdot a_{33} + a_{13} \cdot \underline{a_{21}} \cdot a_{32} + a_{11} \cdot \underline{a_{22}} \cdot a_{33} - a_{13} \cdot \underline{a_{22}} \cdot a_{31} - a_{11} \cdot \underline{a_{23}} \cdot a_{32} + a_{12} \cdot \underline{a_{23}} \cdot a_{31} =$

$= \underline{a_{21}} \cdot (-a_{12} \cdot a_{33} + a_{13} \cdot a_{32}) + \underline{a_{22}} \cdot (a_{11} \cdot a_{33} - a_{13} \cdot a_{31}) + \cdot \underline{a_{23}} (-a_{11} \cdot a_{32} + a_{12} \cdot a_{31}) =$

$= \underline{a_{21}} \cdot (-1)(a_{12} \cdot a_{33} - a_{13} \cdot a_{32}) + \underline{a_{22}} \cdot (a_{11} \cdot a_{33} - a_{13} \cdot a_{31}) + \underline{a_{23}} \cdot (-1)(a_{11} \cdot a_{32} - a_{12} \cdot a_{31}) =$

$$= \underline{a_{21}} \cdot (-1)^{(2+1)} . \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + \underline{a_{22}} \cdot (-1)^{(2+2)} . \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \underline{a_{23}} \cdot (-1)^{(2+3)} . \begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}.$$

Este procedimiento pudimos haberlo realizado recorriendo cualquier línea. Para escribirlo más formalmente daremos algunas definiciones:

Dada $A = (a_{ij}) \in M_n(\mathbb{K})$ llamamos *menor complementario* del elemento a_{ij} y lo notamos M_{ij} al determinante de la matriz que se obtiene anulando la fila i y la columna j en la matriz A.
Llamamos *complemento algebraico* del elemento a_{ij} y lo notamos A_{ij} al determinante de la matriz que se obtiene anulando la fila i y la columna j en la matriz A, multiplicado por $(-1)^{(i+j)}$, es decir $A_{ij} = (-1)^{i+j} \cdot M_{ij}$.
Con esta notación, el determinante de una matriz $A = (a_{ij}) \in M_n(\mathbb{K})$, desarrollado por elementos de la fila i (de la columna j) se escribe:

$$a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + \ldots + a_{in} \cdot A_{in}$$

$$(a_{1j} \cdot A_{1j} + a_{2j} \cdot A_{2j} + \ldots + a_{nj} \cdot A_{nj})$$

Ejemplo 8.19 Sea $A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & -1 & 5 \\ -1 & 3 & 8 \end{pmatrix}$

Calculemos los menores complementarios y los complementos algebraicos para cada elemento de la matriz:

$$a_{11} = 2 \quad M_{11} = \begin{vmatrix} -1 & 5 \\ 3 & 8 \end{vmatrix} = -23 \quad A_{11} = (-1)^{(1+1)} \cdot M_{11} = -23$$

$$a_{12} = 1 \quad M_{12} = \begin{vmatrix} 4 & 5 \\ -1 & 8 \end{vmatrix} = 37 \quad A_{12} = (-1)^{(1+2)} \cdot M_{12} = -37$$

$$a_{13} = 3 \quad M_{13} = \begin{vmatrix} 4 & -1 \\ -1 & 3 \end{vmatrix} = 11 \quad A_{13} = (-1)^{(1+3)} \cdot M_{13} = 11$$

$$a_{21} = 4 \quad M_{21} = \begin{vmatrix} 1 & 3 \\ 3 & 8 \end{vmatrix} = -1 \quad A_{21} = (-1)^{(2+1)} \cdot M_{21} = 1$$

$$a_{22} = -1 \quad M_{22} = \begin{vmatrix} 2 & 3 \\ -1 & 8 \end{vmatrix} = 19 \quad A_{22} = (-1)^{(2+2)} \cdot M_{22} = 19$$

$$a_{23} = 5 \quad M_{23} = \begin{vmatrix} 2 & 1 \\ -1 & 3 \end{vmatrix} = 7 \quad A_{23} = (-1)^{(2+3)} \cdot M_{23} = -7$$

$$a_{31} = -1 \quad M_{31} = \begin{vmatrix} 1 & 3 \\ -1 & 5 \end{vmatrix} = 8 \quad A_{31} = (-1)^{(3+1)} \cdot M_{31} = 8$$

$$a_{32} = 3 \quad M_{32} = \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} = -2 \quad A_{32} = (-1)^{(3+2)} \cdot M_{32} = 2$$

$$a_{33} = 8 \quad M_{33} = \begin{vmatrix} 2 & 1 \\ 4 & -1 \end{vmatrix} = -6 \quad A_{33} = (-1)^{(3+3)} \cdot M_{33} = -6$$

Calculemos el determinante de esta matriz:

1. Por la segunda columna: $1 \cdot (-7) + (-1) \cdot 19 + 3 \cdot 2 = -50$

2. Por la tercera fila: $(-1) \cdot 8 + 3 \cdot 2 + 8 \cdot (-6) = -50$

Como para calcular el determinante por este método multiplicamos el elemento por su complemento algebraico, siempre es conveniente elegir la línea con más ceros.
Una pregunta frecuente es cuándo se debe aplicar uno u otro método. La respuesta es muy sencilla: cualquiera, cuando se quiera y aún más, se pueden combinar.

Ejemplo 8.20 Supongamos que tenemos que calcular el determinante de la siguiente matriz de orden 5:

$$\begin{pmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & -2 & 0 & 0 & -2 \\ 3 & 1 & 2 & 1 & 5 \\ 2 & 2 & 1 & 1 & 3 \end{pmatrix}$$

Las líneas con más ceros son las filas 2 y 3 y la columna 3. Desarrollemos por los elementos de la segunda fila:
$a_{21} \cdot A_{21} + a_{22} \cdot A_{22} + a_{23} \cdot A_{23} + a_{24} \cdot A_{24} + a_{25} \cdot A_{25} = 0 \cdot A_{21} + 1 \cdot A_{22} + 0 \cdot A_{23} + 0 \cdot A_{24} + 2 \cdot A_{25} =$

$$= 1 \cdot (-1)^{(2+2)} det \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 0 & 0 & 2 \\ 3 & 2 & 1 & 5 \\ 2 & 1 & 1 & 3 \end{pmatrix} + 2 \cdot (-1)^{(2+5)} det \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & -2 & 0 & 0 \\ 3 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 \end{pmatrix} =$$

$$= det \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 0 & 0 & 2 \\ 3 & 2 & 1 & 5 \\ 2 & 1 & 1 & 3 \end{pmatrix} - 2 \cdot det \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & -2 & 0 & 0 \\ 3 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 \end{pmatrix} =$$

Sigamos desarrollando por las segundas filas estas matrices:

$$= 2 \cdot (-1)^{(2+4)} det \begin{pmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} - 2 \cdot (-2)(-1)^{(2+2)} det \begin{pmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} =$$

$$= 2 \cdot (2+6-1-9) + 4 \cdot (2+9-12-1) = 2 \cdot (2) + 4 \cdot (-2) = 4 - 8 = -4.$$

Y, quiérase o no, hemos hecho menos de 120 cuentas.

Resolvamos este mismo determinante por triangulación:

$$\begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & -2 & 0 & 0 & -2 \\ 3 & 1 & 2 & 1 & 5 \\ 2 & 2 & 1 & 1 & 3 \end{vmatrix} = \begin{array}{l} F_1: \\ F_2: \\ F_3: \\ F_4 - 3 \cdot F_1: \\ F_5 - 2 \cdot F_1: \end{array} \begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & -2 & 0 & 0 & -2 \\ 0 & -5 & 2 & -8 & -7 \\ 0 & -2 & 1 & -5 & -5 \end{vmatrix} =$$

$$= \begin{array}{l} F_1: \\ F_2: \\ F_3 + 2 \cdot F_2: \\ F_4 + 5 \cdot F_2: \\ F_5 + 2 \cdot F_2: \end{array} \begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & -8 & 3 \\ 0 & 0 & 1 & -5 & -1 \end{vmatrix} = \begin{array}{l} \\ \\ F_5: \\ \\ F_3: \end{array} - \begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & -5 & -1 \\ 0 & 0 & 2 & -8 & 3 \\ 0 & 0 & 0 & 0 & 2 \end{vmatrix} =$$

$$= \begin{array}{l} \\ \\ \\ F_4 - 2 \cdot F_3: \\ \\ \end{array} - \begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & -5 & -1 \\ 0 & 0 & 0 & 2 & 5 \\ 0 & 0 & 0 & 0 & 2 \end{vmatrix} = -(1 \cdot 1 \cdot 1 \cdot 2 \cdot 2) = -4.$$

Finalmente, resolvámoslo usando la forma más habitual, que es la combinación de todas las propiedades:

$$\begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & -2 & 0 & 0 & -2 \\ 3 & 1 & 2 & 1 & 5 \\ 2 & 2 & 1 & 1 & 3 \end{vmatrix} = \begin{array}{l} \\ \\ F_3 + F_2: \\ F_4 - 3 \cdot F_1: \\ F_5 - 2 \cdot F_1: \end{array} \begin{vmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & -5 & 2 & -8 & -7 \\ 0 & -2 & 1 & -5 & -5 \end{vmatrix} =$$

$$= 1.(-1)^{1+1}. \begin{vmatrix} 1 & 0 & 0 & 2 \\ -1 & 0 & 0 & 0 \\ -5 & 2 & -8 & -7 \\ -2 & 1 & -5 & -5 \end{vmatrix} = (-1).(-1)^{2+1}. \begin{vmatrix} 0 & 0 & 2 \\ 2 & -8 & -7 \\ 1 & -5 & -5 \end{vmatrix} =$$

$$= 2.(-1)^{1+3}. \begin{vmatrix} 2 & \text{-8} \\ 1 & \text{-5} \end{vmatrix} = 2.(-10+8) = -4.$$

Inversa de una matriz

Dada una matriz cuadrada A_n, el objetivo es hallar, si existe, una matriz B_n tal que:

$$A_n.B_n = B_n.A_n = I_n.$$

Calculemos directamente:

Pongamos un ejemplo, y trabajemos con matrices pequeñitas: queremos hallar la inversa de

$$\begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix}$$

Buscamos una matriz

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

tal que

$$\begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Esto nos genera el siguiente sistema de ecuaciones:

$$\begin{cases} -1 \cdot b_{11} + 3 \cdot b_{21} = 1 \\ -1 \cdot b_{12} + 3 \cdot b_{22} = 0 \\ 2 \cdot b_{11} - 5 \cdot b_{21} = 0 \\ 2 \cdot b_{12} - 5 \cdot b_{22} = 1 \end{cases}$$

o, si se quiere, los siguientes pares de sistemas de ecuaciones:

$$\begin{cases} -1 \cdot b_{11} + 3 \cdot b_{21} = 1 \\ 2 \cdot b_{11} - 5 \cdot b_{21} = 0 \end{cases} \qquad \begin{cases} -1 \cdot b_{12} + 3 \cdot b_{22} = 0 \\ 2 \cdot b_{12} - 5 \cdot b_{22} = 1 \end{cases}$$

Estos sistemas los podemos resolver por cualquiera de los métodos conocidos y obtenemos $b_{11} = 5$, $b_{21} = 2$, $b_{12} = 3$, $b_{22} = 1$.
Armamos la matriz B_2 y verificamos los productos:

$$\begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix} \cdot \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Si bien la tarea es ardua, es sencillo extender este procedimiento a matrices de cualquier orden. Y si para encontrar la inversa de una matriz de orden 2 debimos resolver dos sistemas de dos ecuaciones con dos incógnitas, para hallar la inversa de una matriz de orden n tendremos que resolver n sistemas de n ecuaciones con n incógnitas. Basta que uno sólo de estos sistemas no sea compatible determinado para que no exista la matriz inversa.

Método de Gauss-Jordan

En la sección anterior nos encontramos con dos sistemas de ecuaciones y dijimos sencillamente que la solución se puede hallar por cualquiera de los métodos conocidos. Bien: usemos el método de Gauss y triangulemos las matrices:

$$\begin{pmatrix} -1 & 3 & \vdots & 1 \\ 2 & -5 & \vdots & 0 \end{pmatrix} \qquad \begin{pmatrix} -1 & 3 & \vdots & 0 \\ 2 & -5 & \vdots & 1 \end{pmatrix}$$

$$F_2 + 2 \cdot F_1 :\mapsto \begin{pmatrix} -1 & 3 & \vdots & 1 \\ 0 & 1 & \vdots & 2 \end{pmatrix} \qquad F_2 + 2 \cdot F_1 :\mapsto \begin{pmatrix} -1 & 3 & \vdots & 0 \\ 0 & 1 & \vdots & 1 \end{pmatrix}$$

Podríamos volver al sistema de ecuaciones, reemplazar el valor obtenido de la segunda ecuación en la primera y terminar de resolver. En cambio, pensemos: del mismo modo que despejamos la segunda incógnita en la segunda ecuación, ahora podemos despejar la primera incógnita en la primera. Procedamos:

$$F_1 - 3.F_2 :\mapsto \begin{pmatrix} -1 & 0 & \vdots & -5 \\ 0 & 1 & \vdots & 2 \end{pmatrix} \qquad F_1 - 3 \cdot F_2 :\mapsto \begin{pmatrix} -1 & 0 & \vdots & -3 \\ 0 & 1 & \vdots & 1 \end{pmatrix}$$

Aún podemos multiplicar por (-1) las primeras ecuaciones y obtenemos:

$$(-1) \cdot F_1 :\mapsto \begin{pmatrix} 1 & 0 & \vdots & 5 \\ 0 & 1 & \vdots & 2 \end{pmatrix} \qquad (-1) \cdot F_1 :\mapsto \begin{pmatrix} 1 & 0 & \vdots & 3 \\ 0 & 1 & \vdots & 1 \end{pmatrix}$$

que claramente nos lleva al resultado: $b_{11} = 5$, $b_{21} = 2$, $b_{12} = 3$, $b_{22} = 1$ que coincide con el hallado en la sección anterior. Ahora uno se pregunta: ¿por qué hacer la misma cuenta dos veces? La triangulación de la matriz fue idéntica con dos "columna solución" diferentes.
Si escribimos todo a un tiempo resulta:

$$\begin{pmatrix} -1 & 3 & \vdots & 1 & 0 \\ 2 & -5 & \vdots & 0 & 1 \end{pmatrix}$$

$$F_2 + 2 \cdot F_1 :\mapsto \begin{pmatrix} -1 & 3 & \vdots & 1 & 0 \\ 0 & 1 & \vdots & 2 & 1 \end{pmatrix}$$

$$F_1 - 3 \cdot F_2 :\mapsto \quad \begin{pmatrix} -1 & 0 & \vdots & -5 & -3 \\ 0 & 1 & \vdots & 2 & 1 \end{pmatrix}$$

$$(-1) \cdot F_1 :\mapsto \quad \begin{pmatrix} 1 & 0 & \vdots & 5 & 3 \\ 0 & 1 & \vdots & 2 & 1 \end{pmatrix}$$

Este procedimiento se conoce como el método de Gauss-Jordan debido al proceso de triangulación realizado en la matriz. Consiste simplemente en escribir al lado de la matriz cuya inversa se quiere calcular, la identidad que corresponde a su dimensión. Luego se realizan operaciones elementales hasta obtener la identidad en la matriz de la izquierda afectando exactamente del mismo modo a la matriz identidad que agregamos y cuando obtenemos la identidad a la izquierda la matriz que queda a la derecha es efectivamente la inversa de nuestra matriz original. Pareciera que con este método hallaremos la inversa de cualquier matriz. Claramente esto no es cierto, ya que si alguno de los n sistemas de n ecuacines con n incógnitas “escondidos” en el procedimiento no tiene solución, jamás podremos obtener la matriz identidad a la izquierda. Por ejemplo:

$$\begin{pmatrix} 1 & 2 & \vdots & 1 & 0 \\ 3 & 6 & \vdots & 0 & 1 \end{pmatrix}$$

$$F_1 - 3 \cdot F_2 :\mapsto \begin{pmatrix} 1 & 2 & \vdots & 1 & 0 \\ 0 & 0 & \vdots & -3 & 1 \end{pmatrix}$$

Claramente no se puede continuar el proceso para obtener la identidad a la izquierda.

Observación 8.3 Hemos triangulado la matrices realizando operaciones elementales por filas. Si quisiéramos hacer operaciones elementales por columnas, para no olvidar ningún paso del procedimiento, solemos escribir la matriz identidad debajo de la matriz original.

Usando la definición de determinante

En 8.2.1 calculamos el determinante de una matriz por elementos de una línea.

Trabajaremos con una matriz un poco más grande para que se vea cómo funciona el determinante. Sea una matriz de orden 3:

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \cdot A_{11} + a_{12} \cdot A_{12} + a_{13} \cdot A_{13}.$$

Vemos que cada coeficiente de la matriz está multiplicado por el complemento algebraico correspondiente.
¿Qué ocurre si calculamos, por ejemplo $a_{21} \cdot A_{11} + a_{22} \cdot A_{12} + a_{23} \cdot A_{13}$?

¿Y si calculamos $a_{31} \cdot A_{11} \cdot a_{32} \cdot A_{12} + a_{33} \cdot A_{13}$?

Vemos fácilmente que:

$$a_{21} \cdot A_{11} + a_{22} \cdot A_{12} + a_{23} \cdot A_{13} = \begin{vmatrix} a_{21} & a_{22} & a_{23} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = 0.$$

ya que es el desarrollo del determinante de una matriz que tiene dos filas repetidas.

Del mismo modo:

$$a_{31} \cdot A_{11} + a_{32} \cdot A_{12} + a_{33} \cdot A_{13} = \begin{vmatrix} a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = 0.$$

Nuevamente nos aparece el determinante de una matriz con dos filas repetidas.

Estos cálculos nos llevan a concluir que:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} = \begin{pmatrix} |A| & 0 & 0 \\ 0 & |A| & 0 \\ 0 & 0 & |A| \end{pmatrix}$$

Si dividimos esta matriz por $|A|$ obtendremos la identidad y de este modo hemos encontrado un método para hallar la matriz inversa, siempre que el determinante sea distinto de cero. Claramente estas cuentas son independientes del orden de la matriz y nos motivan a dar las siguientes definiciones:

Definición 8.2 Dada una matriz $A = (a_{ij}) \in M_n(\mathbb{K})$ se define la *adjunta* de A y se nota $Adj(A)$ a la matriz de los complementos algebraicos de A. En símbolos:

$$Adj(A) = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$$

Y en virtud de los cálculos que realizamos previamente decimos:

Definición 8.3 Dada $A = (a_{ij}) \in M_n(\mathbb{K})$ si $|A| \neq 0$ definimos la *matriz inversa* de A y lo notamos A^{-1} a la matriz adjunta de A, transpuesta, dividida por el determinante de A. En símbolos:

$$A^{-1} = \frac{(Adj(A))^t}{|A|}$$

Ejemplo 8.21 Ya que hicimos todas las cuentas, retomemos el ejemplo 8.19: Para

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & -1 & 5 \\ -1 & 3 & 8 \end{pmatrix} \text{ donde } |A| = -50,$$

$$\text{y } (Adj(A))^t = \begin{pmatrix} -23 & 1 & 8 \\ -37 & 19 & 2 \\ 11 & -7 & -6 \end{pmatrix},$$

de donde:

$$A^{-1} = \begin{pmatrix} \frac{23}{50} & \frac{-1}{50} & \frac{-8}{50} \\ \frac{37}{50} & \frac{-19}{50} & \frac{-2}{50} \\ \frac{-11}{50} & \frac{7}{50} & \frac{6}{50} \end{pmatrix}$$

Verifiquémoslo:

$$A^{-1}.A = \begin{pmatrix} \frac{23}{50} & \frac{-1}{50} & \frac{-8}{50} \\ \frac{37}{50} & \frac{-19}{50} & \frac{-2}{50} \\ \frac{-11}{50} & \frac{7}{50} & \frac{6}{50} \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 3 \\ 4 & -1 & 5 \\ -1 & 3 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Y ya que estamos, busquemos la inversa de esta matriz usando Gauss-Jordan

$$\left(\begin{array}{ccc} 2 & 1 & 3 \\ 4 & -1 & 5 \\ -1 & 3 & 8 \end{array}\right) \left| \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)\right.$$

$$\begin{array}{c} \frac{1}{2}.F_1 \\ F_2 - 2.F_1 \\ F_3 + \frac{1}{2}.F_1 \end{array} \quad \left(\begin{array}{ccc} 1 & \frac{1}{2} & \frac{3}{2} \\ 0 & -3 & -1 \\ 0 & \frac{7}{2} & \frac{19}{2} \end{array}\right) \left| \left(\begin{array}{ccc} \frac{1}{2} & 0 & 0 \\ -2 & 1 & 0 \\ \frac{1}{2} & 0 & 1 \end{array}\right)\right.$$

$$\begin{array}{c} F_1 + \frac{1}{6}.F_2 \\ \frac{-1}{3}.F_2 \\ F_3 + \frac{7}{6}.F_2 \end{array} \quad \left(\begin{array}{ccc} 1 & 0 & \frac{4}{3} \\ 0 & 1 & \frac{1}{3} \\ 0 & 0 & \frac{25}{3} \end{array}\right) \left| \left(\begin{array}{ccc} \frac{1}{6} & \frac{1}{6} & 0 \\ \frac{2}{3} & \frac{-1}{3} & 0 \\ \frac{-11}{6} & \frac{7}{6} & 1 \end{array}\right)\right.$$

$$\begin{array}{c} F_1 - \frac{4}{25}.F_3 \\ F_2 - \frac{1}{25}.F_3 \\ \frac{3}{25}.F_3 \end{array} \quad \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \left| \left(\begin{array}{ccc} \frac{23}{50} & \frac{-1}{50} & \frac{-4}{25} \\ \frac{37}{50} & \frac{-19}{50} & \frac{-1}{25} \\ \frac{-11}{50} & \frac{7}{50} & \frac{3}{25} \end{array}\right)\right.$$

Usando Excel

Simplemente el Excel, entre sus funciones predeterminadas tiene "MDETERM" Simplemente escribimos el cuadro de la matriz, en cualquier otra celda escribimos "=M" y en el cuadro de funciones a elegir seleccionamos MDETERM, luego seleccionamos con el ratón el cuadro de la matriz (aparecen descriptas las celdas seleccionadas en la celda en la que hacemos el cálculo) y al cerrar el paréntesis simplemente aparece el resultado del cálculo. Claramente este método no está admitido en los parciales.

8.2.2. Resolución de sistemas de ecuaciones por determinantes (Regla de Cramer)

Apliquemos el cálculo de determinantes a la resolución de ecuaciones.
Pensemos en un sistema de dos ecuaciones con dos incógnitas. Según lo que vimos antes el sistema tiene solución si y sólo si la pendiente de la primera recta es diferente de la pendiente de la segunda, es decir, si $\dfrac{-a_1}{b_1} \neq \dfrac{-a_2}{b_2}$ lo que es equivalente a: $a_1.b_2 - b_1.a_2 \neq 0$, es decir si el determinante es no nulo. Esta situación es válida para un sistema de n ecuciones con n incógnitas.

Veámoslo. Consideremos un sistema

$$\begin{cases} a_{11}\,x_1 \;+a_{12}\,x_2 \;+\ldots+a_{1n}\,x_n \;=\; b_1 \\ a_{21}\,x_1 \;+a_{22}\,x_2 \;+\ldots+a_{2n}\,x_n \;=\; b_2 \\ a_{31}\,x_1 \;+a_{32}\,x_2 \;+\ldots+a_{3n}\,x_n \;=\; b_3 \\ \;\vdots \qquad \vdots \quad \vdots \quad \vdots \qquad \vdots \quad \vdots \qquad \vdots \;\; \vdots \\ a_{n1}\,x_1 + a_{n2}\,x_2 + \ldots + \; a_{nn}\,x_n \;=\; b_n \end{cases}$$

Ahora que conocemos matrices podemos reescribirlo:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{1n} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

o

$$A \cdot X = B$$

Si el determinante del sistema no es cero, existe la matriz inversa y podemos escribir:

$$A^{-1} \cdot A \cdot X \;=\; A^{-1} \cdot B, \text{ es decir } X = \; A^{-1} \cdot B$$

Hagamos estas cuentas para un sistema de 3 ecuaciones con 3 incógnitas. Consideremos el sistema:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3 \end{cases}$$

Puede escribirse:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

Según lo que vimos antes $X = A^{-1} \cdot B = \dfrac{Adj(A)^t}{|A|} \cdot B$, es decir:

$$X = \frac{\begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}}{|A|} = \frac{\begin{pmatrix} A_{11}.b_1 + A_{21} \cdot b_2 + A_{31} \cdot b_3 \\ A_{12} \cdot b_1 + A_{22} \cdot b_2 + A_{32} \cdot b_3 \\ A_{13} \cdot b_1 + A_{23} \cdot b_2 + A_{33} \cdot b_3 \end{pmatrix}}{|A|}$$

De donde:

$$x_1 = \frac{A_{11} \cdot b_1 + A_{21} \cdot b_2 + A_{31} \cdot b_3}{|A|} = \frac{\begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & b_3 \\ a_{31} & a_{32} & a_{33} \end{vmatrix}}{|A|}$$

$$x_2 = \frac{A_{12} \cdot b_1 + A_{22} \cdot b_2 + A_{32} \cdot b_3}{|A|} = \frac{\begin{vmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{vmatrix}}{|A|}$$

$$x_3 = \frac{A_{13} \cdot b_1 + A_{23} \cdot b_2 + A_{33} \cdot b_3}{|A|} = \frac{\begin{vmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{vmatrix}}{|A|}$$

Estas cuentas podrían hacerse fácilmente en un sistema de n ecuaciones con n incógnitas y obtendríamos que la incógnita x_i es el cociente entre el determinante de la matriz del sistema en la que la columna i-ésima se reemplaza por los términos independientes y el determinante de la matriz del sistema. Es muy importante para aplicar el método de Cramer que los términos independientes estén "del otro lado" ya que un cambio de signo altera el determinante. Veamos un ejemplo en tres incógnitas:

Ejemplo 8.22 Retomemos el ejemplo 8.3

$$\begin{cases} x + y - z = 0 \\ 2x + y + 3z = 1 \\ 2x - y + z = 3 \end{cases}$$

$$x = \frac{\begin{vmatrix} 0 & 1 & -1 \\ 1 & 1 & 3 \\ 3 & -1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & -1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{vmatrix}} = \frac{12}{12} = 1 \quad y = \frac{\begin{vmatrix} 1 & 0 & -1 \\ 2 & 1 & 3 \\ 2 & 3 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & -1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{vmatrix}} = \frac{-12}{12} = -1 \quad z = \frac{\begin{vmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \\ 2 & -1 & 3 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & -1 \\ 2 & 1 & 3 \\ 2 & -1 & 1 \end{vmatrix}} = \frac{0}{12} = 0$$

Y afortunadamente encontramos la misma solución: $(1, -1, 0)$.

8.3. Ejercicios propuestos

8.3.1. Sistemas de ecuaciones

Ejercicio 8.1 Resolver y clasificar los siguientes sistemas de ecuaciones lineales. Si el sistema es compatible indeterminado, hallar además una solución particular del mismo.

$$\begin{cases} x + y + 2\,z = -1 \\ x - 2\,y + z = -5 \\ 3\,x + y + z = 3 \end{cases} \qquad \begin{cases} 2\,x - y + 3\,z = 4 \\ 3\,x - 2\,y + 2\,z = 3 \\ 5\,x - 3\,y = 2 \end{cases}$$

$$\begin{cases} 2\,x + 7\,y + 3\,z + t = 6 \\ 3\,x + 5\,y + 2\,z + 2\,t = 4 \\ 9\,x + 4\,y + z + 7\,t = 2 \end{cases} \qquad \begin{cases} 2\,x - y + 3\,z - t + u = 2 \\ 4\,x - 2\,y + 6\,z - 2\,t - 2\,u = 4 \\ 2\,x - y - z + 2\,t = 0 \\ 4\,z - 3\,t + u = 2 \end{cases}$$

Ejercicio 8.2 Hallar el valor de λ para el cual los siguientes sistemas son compatibles determinados, indeterminados ó incompatibles:

$$\begin{cases} x + 2\,y - 3\,z = 4 \\ 3\,x - y + 5\,z = 2 \\ 4\,x + y + (\lambda^2 - 14)\,z = \lambda + 2 \end{cases} \qquad \begin{cases} 2\,x + 5\,y + z + 3\,t = 2 \\ 4\,x + 6\,y + 3\,z + 5\,t = 4 \\ 4\,x + 14\,y + z + 7\,t = 4 \\ 2x - 3\,y + 3\,z + \lambda\,t = 7 \end{cases}$$

Ejercicio 8.3 Determinar, si existen, $x, y, z \in \mathbb{R}$ que verifiquen simultáneamente:

$$\begin{cases} x = 1 - 2\,\lambda \\ y = -1 + 4\,\lambda \\ z = -3 + 2\,\lambda \end{cases} , \quad \lambda \in \mathbb{R} \qquad \begin{cases} x = 3 - \gamma \\ y = -7 + 3\,\gamma \\ z = -5 + \gamma \end{cases} , \quad \gamma \in \mathbb{R}$$

Ejercicio 8.4 (♣) Problemas:

1. Hallar dos números cuya suma es 21 y al dividir uno entre el otro se obtiene de cociente 2 y de resto 3.
2. En una granja hay gallinas y conejos que hacen un total de 360 cabezas y 1.019 patas, ya que uno de los conejos perdió una. ¿Cuántos animales hay de cada especie?
3. El perímetro de un rectángulo es 38 m. Si aumentamos cada lado en 2 metros, ¿en cuántos metros cuadrados aumenta el área?

8.3.2. Matrices

Ejercicio 8.5 Construir matrices que cumplan las siguientes condiciones :

1. $B = (b_{ij})$ de orden 3 tal que $b_{ij} - b_{ji} = 0$ si $i \neq j$ $\quad b_{ij} = 0$ si $i = j$.

2. $D = (d_{ij})$ de orden 4 tal que $d_{ij} = \begin{cases} i-j & \text{si } i > j \\ 0 & \text{si } i < j \\ -2j & \text{si } i = j \end{cases}$.

3. $E = (e_{ij})$ de orden 3 tal que $e_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ \sqrt{j} & \text{si } i = j \end{cases}$.

Ejercicio 8.6 Resolver, **si es posible**, las siguientes ecuaciones matriciales :

1. $\begin{pmatrix} d & c \\ a-c & a+b \end{pmatrix} + \begin{pmatrix} 0 & -d \\ 2d & c-d \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix}$.

2. $\begin{pmatrix} a+2b & 11 \\ 2a & 2a+6b \end{pmatrix} + \begin{pmatrix} -3c & 0 \\ 5b-4c & 2c \end{pmatrix} = \begin{pmatrix} 4 & a+3b+c \\ 13 & 22 \end{pmatrix}$.

Ejercicio 8.7 Efectuar los siguientes productos entre matrices :

$$\begin{pmatrix} -3 & 4 \\ 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -4 \\ 5 & 3 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & -3 \\ -4 & 3 & 1 \\ -5 & 3 & -2 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 & 6 \\ 2 & 1 & 7 \\ -1 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & -2 \\ 0 & 5 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 1 \end{pmatrix}$$

Ejercicio 8.8 ($\diamond$) Sea $A = \begin{pmatrix} 3 & -2 \\ 1 & -2 \end{pmatrix}$, calcular A^2 y A^3.

Idem para $A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ y $A = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$.

Ejercicio 8.9 Dar ejemplos de matrices no nulas A y B de orden 2 que verifiquen:

1. $A^2 = A,\ A \neq I$.
2. $A^n = 0$, para algún $n \in \mathbb{N}$.
3. $A \cdot B + B \cdot A = I_2$.

Ejercicio 8.10 (♣) Dada la matriz $A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 4 \end{pmatrix}$, hallar una matriz B tal que se puedan efectuar los productos $A \cdot B$ y $B \cdot A$. ¿De qué órdenes son estos productos?

Ejercicio 8.11 © Sean A y B matrices cuadradas de orden n. Mostrar que :

1. En general, $A \cdot B \neq B \cdot A$.
2. Si $A \cdot B \neq B \cdot A$ entonces $(A+B)^2 \neq A^2 + B^2 + 2A \cdot B$ y $A^2 - B^2 \neq (A+B) \cdot (A-B)$.
3. En general , si $A \cdot B = 0$ no necesariamente $A = 0$ ó $B = 0$.
4. Si $A = \lambda \cdot I_n$ entonces $A \cdot B = B \cdot A$ para toda matriz B de orden n.

Ejercicio 8.12 (◇) Sean $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.
Calcular: $A \cdot B - B \cdot A$, $B \cdot C - C \cdot B$ y $A \cdot C - C \cdot A$.

Ejercicio 8.13 Una matriz cuadrada $a = (a_{i,j})$ se dice diagonal si $a_{i,j} = 0$ cuando $i \neq j$. Decidir la verdad o falsedad de las siguientes afirmaciones, justificando la respuesta.

Si A, B, C son matrices cuadradas de orden n se tiene :

1. $[2 \cdot A^t \cdot (3 \cdot B) \cdot C]^t = 6 \cdot (B \cdot C)^t \cdot A$.
2. $(2 \cdot A + B \cdot C)^t = 2 \cdot A^t + B \cdot C$, B y C matrices diagonales.
3. $(A \cdot B^t \cdot C - A)^t = (C^t \cdot B - I_n) \cdot A^t$.
4. $\left((A^t)^2\right)^t = A^2$.
5. Si A y B son matrices diagonales, entonces $A^2 - B^2 = (A-B) \cdot (A+B)$.

Ejercicio 8.14 © Una matriz cuadrada $A = (a_{i,j})$ se dice simétrica si $a_{ij} = a_{ji}$, para todo i, j. Mostrar que :

1. Si A es una matriz $m \times n$ entonces el producto $A \cdot A^t$ está definido y es una matriz simétrica .
2. La suma de matrices simétricas es una matriz simétrica.
3. El producto de dos matrices simétricas es una matriz simétrica, si las matrices conmutan.

8.3.3. Determinantes

Ejercicio 8.15 Calcular:

$$\begin{vmatrix} 2 & 1 \\ 3 & -5 \end{vmatrix} \qquad , \qquad \begin{vmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \\ -1 & 3 & 0 \end{vmatrix} \qquad , \qquad \begin{vmatrix} 2 & 0 & 1 \\ -1 & 3 & 1 \\ 0 & 1 & -2 \end{vmatrix}.$$

Ejercicio 8.16 Hallar los valores de x tales que $det\, A = 0$.

i) $A = \begin{pmatrix} x-1 & -2 \\ 1 & x-4 \end{pmatrix}$ ii) $A = \begin{pmatrix} x-6 & 0 & 0 \\ 0 & x & -1 \\ 0 & 4 & x-4 \end{pmatrix}$

Ejercicio 8.17 Si $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & m \end{pmatrix}$ y $det\, A = 5$ decir, sin calcular los determinantes, por qué valen las

siguientes igualdades:

a) $\begin{vmatrix} d & e & f \\ g & h & m \\ a & b & c \end{vmatrix} = 5$ b) $\begin{vmatrix} -a & -b & -c \\ 2\,d & 2\,e & 2\,f \\ -g & -h & -m \end{vmatrix} = 10$

c) $\begin{vmatrix} a+d & b+e & c+f \\ d & e & f \\ g & h & m \end{vmatrix} = 5$ d) $\begin{vmatrix} a & b & c \\ d-3\,a & e-3\,b & f-3\,c \\ 2g & 2h & 2m \end{vmatrix} = 10$

Ejercicio 8.18 Calcular, desarrollando por los elementos de la fila ó columna con más ceros, el siguiente determinante

$$\begin{vmatrix} 1 & -1 & 2 & 3 \\ -1 & 0 & 1 & 0 \\ 2 & 1 & -2 & -1 \\ 5 & 1 & 1 & 3 \end{vmatrix}$$

Ejercicio 8.19 ($\diamond$) Calcular los siguientes determinantes haciendo previamente todos los elementos de una fila o columna cero excepto uno y desarrollando luego por esa línea.

a) $\begin{vmatrix} 1 & -1 & 2 \\ 0 & 1 & 3 \\ -1 & 1 & 1 \end{vmatrix}$ b) $\begin{vmatrix} 1 & 2 & -1 & 3 \\ 0 & 1 & -1 & 2 \\ 2 & -1 & 5 & 0 \\ 0 & 1 & 1 & 1 \end{vmatrix}$ c) $\begin{vmatrix} 1 & -1 & 2 & 1 & 3 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & 1 & 1 & -1 & 2 \\ 0 & 1 & -1 & 3 & 0 \\ 1 & -1 & 1 & 1 & 1 \end{vmatrix}$

Ejercicio 8.20 Si A es una matriz de orden 3 y $\det A = 2$, hallar $\det(\frac{1}{2}.A)$ y $\det(A.A^t)$.

Ejercicio 8.21 © ¿ Es cierto que $\det(A+B) = \det A + \det B$? Justificar la respuesta.

Ejercicio 8.22 Dadas las siguientes matrices decir si son o no inversibles, y en caso afirmativo, hallar su inversa:

a) $\begin{pmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \\ 4 & -1 & 5 \end{pmatrix}$ c) $(\diamond)$ $\begin{pmatrix} 1 & -1 & 0 \\ 3 & 1 & 4 \\ 0 & 1 & 1 \end{pmatrix}$

b) $\begin{pmatrix} 0 & -1 & 1 & 2 \\ 0 & 0 & -1 & 3 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix}$ d) $(\diamond)$ $\begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 1 & -1 & 2 \\ 3 & 1 & -2 & 5 \\ 4 & 1 & -1 & 10 \end{pmatrix}$

Ejercicio 8.23 © Sean A, B matrices cuadradas de orden n. Probar que:

1. Si A y B son matrices inversibles, entonces $A \cdot B$ también lo es y $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.
2. Si A es inversible, entonces $\det B = \det(A^{-1} \cdot B \cdot A)$.

Ejercicio 8.24 (♣) Si A es una matriz de orden 3 y $\det A = 3$, hallar: $\det(A^{-1})$, $\det(5 \cdot A^{-1})$ y $\det(5 \cdot A)^{-1}$.

Ejercicio 8.25 Verificar si los siguientes sistemas son compatibles determinados, y en caso afirmativo, hallar la solución aplicando la regla de Cramer.

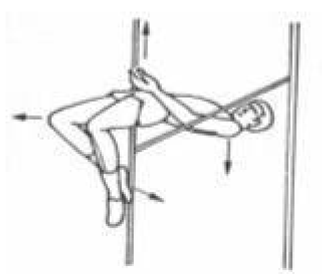
1. $\begin{cases} x + 3y + 5z = 1 \\ 4x + 3y + 2z = 1 \\ 3x + 6y + 9z = 2 \end{cases}$ 2. $\begin{cases} 2x - y + 3z = 4 \\ 3x - 2y + 2z = 3 \\ 5x - 3y = 2 \end{cases}$

Capítulo 9

Vectores

Operaciones con vectores. Bases de E^2 y E^3. Sistemas de coordenadas ortogonales. Componentes y cosenos directores. Proyección ortogonal. Producto escalar. Orientaciones del plano y del espacio. Producto vectorial. Producto mixto. Geometra del plano y del espacio: Ecuación de la recta en el plano y en el espacio. Ecuación del plano. Ángulos entre rectas y planos. Distancia de un punto a un plano y una recta, entre recta y plano, entre planos y entre rectas.

9.1. Vectores libres



Cuando queremos marcar en qué dirección se debe mover algo, o hacia dónde hay que hacer una fuerza, utilizamos “flechitas”.
Una flecha nos indica si debemos empujar o tirar para abrir una puerta. Una flecha nos muestra la dirección en que debemos hacer esa fuerza, nos dice si esa fuerza que debemos hacer “va” o “viene” y, en general, intuitivamente pensamos que si es más grande la fuerza deberá ser mayor.

Copiando esta interpretación sencilla encontramos la noción de vector libre, que vamos a definir a continuación:

Definición 9.1 Llamamos *vector libre* o *segmento orientado* a un segmento de recta, que tenga definido el *inicio* y el *extremo*. Para diferenciarlos puede ponerse un punto más gordito o nada en el inicio y una punta de flecha en el extremo. Si el punto de inicio es A y el extremo es B podemos decir que determinan un vector que llamaremos v, pero para diferenciarlo de cualquier otra cosa lo representamos con una flecha encima, así $\vec{v} = \overrightarrow{AB}$.
Un vector tiene tres atributos:

($\vec{v}1$) "Inclinación", que la llamaremos *dirección* y está dada por la pendiente del segmento.

($\vec{v}2$) "Va o viene", lo llamaremos *sentido* y se da al enunciar cuál origen y cuál el extremo.

($\vec{v}3$) "Tamaño", lo llamaremos *intensidad* y está dado por la longitud del segmento. A este valor lo llamaremos *módulo* del vector $\vec{v}$ y lo notaremos $||\vec{v}||$.

Si el origen coincide con el extremo la longitud, es decir el módulo del vector es 0, y lo denominamos el *vector nulo*. $\vec{0}$, entonces, es un vector de intensidad nula, que no tiene definida la dirección.

Decimos que dos vectores son *iguales* si tienen igual dirección, sentido e intensidad. Un vector es el *opuesto* de otro si tienen igual dirección y módulo y sentidos contrarios. Claramente $\overrightarrow{BA}$ es el opuesto de $\overrightarrow{AB}$ y escribimos $\overrightarrow{BA} = -\overrightarrow{AB}$.
Llamamos a estos vectores *libres* dado que en ningún momento hemos analizado cuál es el inicio y el extremo ni tampoco en qué espacio están ubicados.

Observación 9.1 Un comentario sobre las señales de tránsito: Podemos ver, diseminados por las ciudades cartelitos de tránsito que se interpretan como "dirección obligatoria". Que no nos confunda este error. Toda calle recta tiene una única dirección, ya que no la podemos "girar", algunas de ellas sólo pueden tansitarse en un sentido y otras en ambos. Por ejemplo, 12 de octubre tiene sentido único, creciente en altura mientras que Avenida Alem tiene una única direccción pero puede transitarse en ambos sentidos: desde el teatro a la universidad o desde la universidad hacia el teatro.

9.1.1. Operaciones con vectores

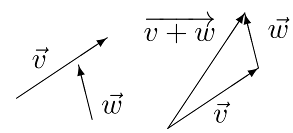
Suma de vectores

$\boxed{1}\boxed{2}$ $\boxed{1}\boxed{2}\boxed{3}$

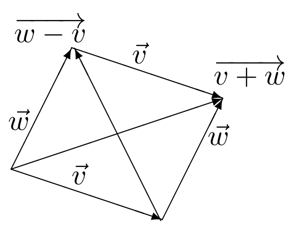
$\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}$

Cuando conocimos la suma de números en la escuela y queríamos sumar, por ejemplo, $2 + 3$ simplemente colocábamos primero dos segmentitos unitarios y a continuación tres segmentitos unitarios y finalmente contábamos desde el inicio hasta la finalización.
Lo mismo vamos a hacer con vectores:

Para sumar dos vectores, simplemente colocamos el origen del segundo en el extremo del primero. El vector suma será el que tiene origen en el origen del primero y extremo en el extremo del segundo.



Regla del paralelogramo



Es realmente interesante notar que si Colocamos los vectores $\vec{v}$ y $\vec{w}$ con origen común, y luego en el extremo de $\vec{v}$ colocamos a $\vec{w}$ y en el extremo de $\vec{w}$ colocamos a $\vec{v}$ queda construído un paralelogramo (cosa trivial, dado que los lados paralelos son copias del mismo vector libre). Observamos que la diagonal que va del origen de $\vec{v}$ y $\vec{w}$ hasta el extremo de ambos vectores es el vector suma y la diagonal que va desde el extremo de $\vec{w}$ y origen de $\vec{v}$ hasta el origen de $\vec{w}$ y extremo de $\vec{v}$ es $\vec{v} + (-\vec{w})$.

Propiedades de la suma

(V_1) $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$ (propiedad asociativa)

(V_2) $\vec{u} + \vec{v} = \vec{v} + \vec{u}$ (propiedad conmutativa)

(V_3) $\vec{u} + \vec{0} = \vec{u}$ (elemento neutro)

(V_4) Para todo $\vec{u}$ existe $+\ \vec{u}$ tal que $\vec{u} + (-\vec{u}) = \vec{0}$ (existencia de simétricos)

Estas propiedades se pueden verificar gráficamente e invitamos al lector interesado a pasar un amable momento acompañado de regla, colores y mates.®

9.1.2. Producto de un escalar por un vector

Definición 9.2 Dado un vector $\vec{v}$ y un número (escalar) $k \in \mathbb{R}, k \neq 0$ se define $\overrightarrow{k \cdot v}$ al vector que tiene los siguientes atributos:

dirección: la misma dirección que $\vec{v}$,

sentido:

- si $k > 0$ el mismo sentido que $\vec{v}$
- si $k < 0$ sentido contrario a $\vec{v}$

intensidad: $||k \cdot \vec{v}|| = |k| \cdot ||\vec{v}||$.

Según vimos en la definición, al multiplicar un vector por un escalar su dirección no cambia, entonces podemos tomar como representativo de todos los vectores en una dirección dada a uno de ellos y pensar a todos los demás como ese vector multiplicado por un escalar. Lógicamente elegimos como representante a aquel que tenga módulo 1, lo llamamos *versor* y lo notamos $\breve{v}$. Dado cualquier vector, siempre podemos hallar el versor asociado dividiendo por su módulo, es decir:

$$\breve{v} = \frac{\vec{v}}{||\vec{v}||}.$$

Otra deducción a partir de esta definición: dos vectores son *paralelos* si uno es múltiplo del otro:

$$\vec{u} \parallel \vec{v} \text{ si existe } k \in \mathbb{R} \text{ tal que } \vec{u} = k \cdot \vec{v}.$$

Propiedades

Cualesquiera que sean $\vec{u}, \vec{v} \in V$ y $k, k' \in \mathbb{R}$ se verifica:

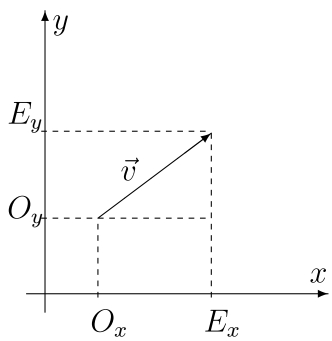
(V_5) $k \cdot (\vec{u} + \vec{v}) = k \cdot \vec{u} + k \cdot \vec{v}$ (propiedad distributiva)

(V_6) $(k + k') \cdot \vec{u} = k \cdot \vec{u} + k' \cdot \vec{u}$ (propiedad distributiva)

(V_7) $(k \cdot k') \cdot \vec{u} = k \cdot (k' \cdot \vec{u})$ (propiedad asociativa)

(V_8) $1 \cdot \vec{u} = \vec{u}$ (conservación de la identidad)

Hasta aquí hemos hablado de vectores libres que tienen un origen y un extremo, ya sea en el plano o en el espacio, pero no les hemos asignado ningún valor numérico. Veamos cómo hacerlo. Pensemos primero en el plano y luego iremos al espacio.



Un vector $\vec{v}$ tiene origen: O y extremo: E. Estamos en el plano, entonces:

1. $O = (O_x, O_y)$
2. $E = (E_x, E_y)$

Se trata de vectores libres, entonces podemos trasladarlo al origen de coordenadas sin cambiar su "personalidad". Si hacemos esto el extremo del vector quedará en el punto $(E_x - O_x, E_y - O_y)$. Representaremos a todos los vectores por las coordenadas de su extremo, considerando que el origen del vector coincide con el origen de coordenadas, así aparece la fórmula

VEO: **V**ector = **E**xtremo - **O**rigen.

Ejemplo 9.1 Veamos un ejemplo en el plano y otro en el espacio:

1. Sea $\vec{u}$ con origen en $(3, 5)$ y extremo en $(2, -1)$, entonces decimos
$$\vec{u} = (2, 1) - (3, 5) = (-1, -4).$$
2. Sea $\vec{v}$ con origen en $(1, 2, -1)$ y extremo en $(3, 7, 4)$, entonces decimos
$$\vec{v} = (3, 7, 4) - (1, 2, -1) = (2, 5, 5).$$

Claramente siempre podemos resolver los siguientes problemas:

Ejemplo 9.2

1. Hallar el extremo del vector $\vec{v}_1 = (2, 1, 3)$, sabiendo que su origen está en el punto $(7, -2, 4)$. Si **V**= **E** - **O**, claramente **E**= **V** + **O** y el extremo del vector estará en el punto $(9, -1, 7)$.
2. Hallar el origen de un vector $\vec{w}$ con igual dirección y módulo que el vector $\vec{v} = (3, 1, 1)$ y sentido contrario, si su extremo está en el origen de coordenadas.
Como el vector $\vec{w}$ tiene igual dirección y módulo, pero sentido contrario, resulta $\vec{w} = (-3, -1, -1)$ **E**:$(0, 0, 0$ y aplicando la fórmula despejada: **O**= **E** - **V**=$(3, 1, 1)$. Podríamos haber llegado a este resultado sin necesidad de hacer cuentas ¿no? ®

Esta forma de representar a los vectores por las coordenadas de su extremo, considerando que su origen coincide con el origen de coordenadas es altamente conveniente ya que las operaciones hasta ahora vistas se realizarán simplemente "coordenada a coordenada", así resulta:

1. Si $\vec{u} = (2, 1, 3), \vec{v} = (3, 7, 4)$, entonces la suma es:
   $\overrightarrow{u + v} = \vec{u} + \vec{v} = (2, 1, 3) + (3, 7, 4) = (2 + 3, 1 + 7, 3 + 4) = (5, 8, 7)$.
2. Si $\vec{u} = (1, -3, 4)$, $k = 2$ entonces el producto por el escalar $k = 2$ resulta:
   $\overrightarrow{2 \cdot u} = 2 \cdot \vec{u} = 2 \cdot (1, -3, 4) = (2 \cdot 1, 2 \cdot (-3), 2 \cdot 4) = (2, -6, 8)$.

Teniendo las coordenadas de los puntos origen y extremo de un vector podemos calcular su módulo simplemente como distancia entre puntos. Entonces, si tenemos al vector por coordenadas podemos escribir:

$$\vec{u} = (u_x, u_y) \text{ entonces } ||\vec{u}|| = \sqrt{u_x^2 + u_y^2}$$

$$\vec{u} = (u_x, u_y, u_z) \text{ entonces } ||\vec{u}|| = \sqrt{u_x^2 + u_y^2 + u_z^2}$$

Ejemplo 9.3

1. $\vec{u}_1 = (3, 4)$, entonces $||\vec{u}_1|| = \sqrt{3^2 + 4^2} = \sqrt{25} = 5$
2. $\vec{u}_2 = (-2, 1, -1)$, entonces $||\vec{u}_2|| = \sqrt{(-1)^2 + 1^2 + (-1)^2} = \sqrt{6}$
3. Si $\vec{u}_3$ es un vector con origen en $(1, 3, 1)$ y extremo en $(1, 0, -3)$ entonces
   $\vec{u}_3 = ((1 - 1), (0 - 3), 1 - (-3))$, y
   $$||\vec{u}_3|| = \sqrt{(1 - 1)^2 + (0 - 3)^2 + 1 - (-3)^2} = \sqrt{25} = 5.$$

Definición 9.3 Un vector $\vec{u}$ es *combinación lineal* de $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ si existen $k_1, k_2, \ldots, k_n \in \mathbb{R}$ tales que $\vec{u} = k_1 \cdot \vec{v}_1 + k_2 \cdot \vec{v}_2 + \ldots + k_n \cdot \vec{v}_n$.

Ejemplo 9.4

1. $(3, -2, 4)$ es combinación lineal de $(1, 0, 2)$ y $(-1, 1, 1)$.
   En efecto: $(3, -2, 4) = 1.(1, 0, 2) + (-2) \cdot (-1, 1, 1)$.
2. $(3, -2, 4)$ no es combinación lineal de $(1, 0, 2)$ y $(2, -1, 2)$.
   No existen $k_1, k_2 \in \mathbb{R}$ tales que $(3, -2, 4) = k_1 \cdot (1, 0, 2) + k_2 \cdot (2, -1, 2)$.
   Verifiquémoslo:
   $(3, -2, 4) = k_1 \cdot (1, 0, 2) + k_2 \cdot (2, -1, 2)$ genera el sistema de ecuaciones:
   $$\begin{cases} 3 = k_1 \cdot 1 + k_2 \cdot 2 \\ -2 = k_1 \cdot 0 + k_2 \cdot (-1) \\ 4 = k_1 \cdot 2 + k_2 \cdot 2 \end{cases}$$

Por la segunda ecuación $k_2 = 2$ y queda:

$$\begin{cases} 3 = k_1 \cdot 1 + 2 \cdot 2 & \text{Es decir, } k_1 = -1 \\ 4 = k_1 \cdot 2 + 2 \cdot 2 & \text{Es decir, } k_1 = 0 \end{cases}$$

3. Consideremos dos vectores no paralelos en $\mathbb{R}^2$. Sean $(1,2)$ y $(1,-1)$. Pensemos qué vectores (x,y) podemos escribir como combinación lineal de estos dos. Es decir que (x,y) podemos escribir:

$$k_1 \cdot (1,2) + k_2 \cdot (1,-1) = (x,y).$$

Generemos el sistema de ecuaciones:

$$\begin{cases} k_1 \cdot 1 + k_2 \cdot 1 = x \\ k_1 \cdot 2 + k_2 \cdot (-1) = y \end{cases}$$

Sabemos que este sistema tiene solución única si

$$\begin{vmatrix} 1 & 1 \\ 2 & -1 \end{vmatrix} \neq 0,$$

independientemente de los valores de x e y. Entonces podemos escribir cualquier vector de $\mathbb{R}^2$ de forma única como combinación lineal de $(1,2)$ y $(1,-1)$. Decimos entonces que estos vectores forman una *base* de $\mathbb{R}^2$.

4. Las mismas cuentas que hicimos en el inciso anterior las podemos hacer para cualquier (x,y,z) y los tres vectores dados en el inciso 2. Esta es una invitación formal para el lector interesado: ¡A verificarlo!®

9.1.3. Bases de $\mathbb{R}^2$ y $\mathbb{R}^3$

Los dos últimos incisos nos llevan a dar la siguiente definición:

Definición 9.4 Dos vectores no paralelos $\vec{b}_1$ y $\vec{b}_2$ en $\mathbb{R}^2$ forman *base* de $\mathbb{R}^2$. Del mismo modo, tres vectores $\vec{b}_1, \vec{b}_2$ y $\vec{b}_3$, tales que ninguno sea combinación lineal de los otros dos, forman una *base* de $\mathbb{R}^3$. Si consideramos un orden entre ellos la llamaremos una *base ordenada.*

Entre todas las bases posibles (que es una cantidad claramente infinita) se destacan bases que, entre otras cosas, hacen que nuestros cálculos sean mucho más sencillos. Se trata de las que, sin mencionarlas, hemos usado hasta el momento.
Muy fácilmente vemos que

$$(x,y) = (x,0) + (0,y) = x \cdot (1,0) + y \cdot (0,1)$$

y el conjunto ordenado

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

forma base de $\mathbb{R}^2$. Esta base se denomina la *base canónica* y escribimos:

$$\mathcal{C}_2 = \{(1,0),(0,1)\}.$$

Del mismo modo definimos la base canónica de $\mathbb{R}^3$:

$$\mathcal{C}_3 = \{(1,0,0),(0,1,0),(0,0,1)\}.$$

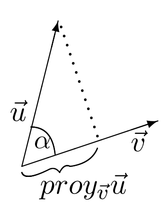
Estos vectores (que en verdad son versores) los llamamos $\breve{e}_i$ y distinguimos su dimensión por la cantidad. Cada versor $\breve{e}_i$ tiene la coordenada i-ésima igual a 1 y las demás nulas, así tenemos:

$$\mathcal{C}_2 = \{\breve{e}_1, \breve{e}_2\} \text{ y } \mathcal{C}_3 = \{\breve{e}_1, \breve{e}_2, \breve{e}_3\}$$

Más adelante veremos qué otras propiedades tienen estas bases canónicas.

9.1.4. Proyección ortogonal

Dados un punto y una recta realizamos la proyección ortogonal del punto sobre la recta calculando la intersección de la recta dada con una perpendicular a la misma que pase por el punto y la notamos $proy_L(P)$.
Si nuestra intención es proyectar un vector $\vec{u}$ sobre otro $\vec{v}$, simplemente debemos proyectar los puntos origen y extremo sobre la recta que contiene al vector. Siempre hablamos de vectores libres y entonces a efectos de simplificar los cálculos ubicamos a ambos vectores con un origen común y sólo proyectamos el punto extremo. Si el ángulo formado por los vectores es agudo, la longitud del segmento comprendido entre el origen de ambos vectores y la proyección del extremo es valor de la proyección y lo notamos $proy_{\vec{v}}\vec{u}$.



Al poner ambos vectores con origen común y trazar una perpendicular la vector $\vec{v}$ generamos un triángulo rectángulo y la proyección es el cateto adyacente al ángulo formado por ambos vectores, de donde afirmamos:

$$proy_{\vec{v}}\vec{u} = ||\vec{u}|| \cdot cos\, \alpha.$$

Generalizamos esta situación para todos los valores posibles de α:

$$\begin{array}{ccc} 0 \leq \alpha < \pi/2 & \text{entonces} & proy_{\vec{v}}\vec{u} > 0 \\ \alpha = \pi/2 & \text{entonces} & proy_{\vec{v}}\vec{u} = 0 \\ \pi/2 \leq \alpha < \pi & \text{entonces} & proy_{\vec{v}}\vec{u} < 0 \end{array}$$

¿Por qué no consideramos ángulos mayores que π?

Propiedades de las proyecciones

Si bien la demostración de las siguientes propiedades puede no resultar demasiado sencilla, debido a la necesidad de aplicar fórmulas trigonométricas, sí es una grata experiencia visualizarlas gráficamente y a ello invitamos a los lectores:
Para todo $\vec{u}_1, \vec{u}_2, \vec{v} \in V,\ k \in \mathbb{R}$ se verifica:

$P_1) : \ proy_{\vec{v}}(\vec{u}_1 + \vec{u}_2) = proy_{\vec{v}}(\vec{u} + \vec{u}_2)$

$P_2) : \ proy_{\vec{v}}(k \cdot \vec{u}) = k \cdot proy_{\vec{v}}\vec{u}$

Si quisiéramos darle dirección y sentido a la proyección, ya que estamos proyectando sobre el vector $\vec{v}$, serán la dirección y el sentido de $\vec{v}$. Para hacer esto simplemente multipplicamos el valor de la proyección por el versor $\breve{v}$:

$$\overrightarrow{proy_{\vec{v}}\vec{u}} = proy_{\vec{v}}\vec{u} \cdot \breve{v} = proy_{\vec{v}}\vec{u} \cdot \frac{\vec{v}}{||\vec{v}||} = ||\vec{u}|| \cdot cos\,\alpha \cdot \frac{\vec{v}}{||\vec{v}||}.$$

9.1.5. Producto escalar

A continuación definiremos una función $(\cdot,\cdot) : V \times V \to \mathbb{R}$, es decir: tomamos dos vectores, hacemos una cuenta y nos da un número real:

Definición 9.5 Dados dos vectores $\vec{u}$ y $\vec{v}$, se define el *producto escalar* de $\vec{u}$ y $\vec{v}$ y se nota $(\vec{u}, \vec{v})$ al número real:

$$(\vec{u}, \vec{v}) = \begin{cases} 0 & \text{si } \vec{u} = \vec{0} \text{ ó } \vec{v} = \vec{0} \\ \\ ||\vec{u}|| \cdot ||\vec{v}|| \cdot cos\,\alpha & \text{en otro caso.} \end{cases},$$

donde α es el ángulo que determinan entre ellos.

Observación 9.2 Alguien podría decir: “¿Para qué hacer la distinción? Si alguno de los vectores es cero, el módulo es cero y la cuenta da. ¿Cuál es el problema?” Pero realmente hay un problema. ¿Cuál es?®

El producto escalar, claramente denominado así porque de dos vectores se obtiene un escalar, está íntimamente relacionado con la proyección, ya que si ambos vectores son no nulos podemos afirmar:

$$(\vec{u}, \vec{v}) = ||\vec{u}|| \cdot ||\vec{v}|| \cdot cos\,\alpha = ||\vec{v}|| \cdot proy_{\vec{v}}\vec{u}$$

Propiedades del producto escalar

Para todo $\vec{u}, \vec{v}$ y $\vec{w} \in V$ y $k \in \mathbb{R}$ se verifica:

1. $(\vec{u}, \vec{v}) = (\vec{v}, \vec{u})$
2. $(\vec{u} + \vec{v}, \vec{w}) = (\vec{u}, \vec{w}) + (\vec{v}, \vec{w})$
3. $k \cdot (\vec{u}, \vec{v}) = (k \cdot \vec{u}, \vec{v}) = (\vec{u}, k \cdot \vec{v})$
4. $(\vec{u}, \vec{u}) = ||\vec{u}||^2$

   En consecuencia: $(\vec{u}, \vec{u}) \geq 0$ y sólo es nulo cuando alguno de los vectores es $\vec{0}$.

Ya que encontramos una relación entre producto escalar y proyección ortogonal, usaremos las propiedades de la proyección para probar las propiedades del producto escalar: Dado que si alguno de los vectores es $\vec{0}$ todo se anula, supongamos que $\vec{u} \neq \vec{0} \neq \vec{v}$

1. $(\vec{u}, \vec{v}) = ||\vec{u}|| \cdot ||\vec{v}|| \cdot cos\, \alpha = ||\vec{v}|| \cdot ||\vec{u}|| \cdot cos\, \alpha = (\vec{v}, \vec{u})$
2. $(\vec{u} + \vec{v}, \vec{w}) = ||\vec{w}|| \cdot proy_{\vec{w}}(\vec{u} + \vec{v}) = ||\vec{w}|| \cdot proy_{\vec{w}}\vec{u} + ||\vec{w}|| \cdot proy_{\vec{w}}\vec{v} = (\vec{u}, \vec{w}) + (\vec{v}, \vec{w})$
3. $k \cdot (\vec{u}, \vec{v}) = (k \cdot ||\vec{u}||) \cdot ||\vec{v}|| \cdot cos\, \alpha = ||k \cdot \vec{u}|| \cdot ||\vec{v}|| \cdot cos\, \alpha = (\vec{k} \cdot u, \vec{v})$, ya que el ángulo que forman $\overrightarrow{k \cdot u}$ y $\vec{v}$ es el mismo ángulo que forman $\vec{u}$ y $\vec{v}$.
   Análogamente se ve que $k \cdot (\vec{u}, \vec{v}) = (\vec{u}, k \cdot \vec{v})$.
4. $(\vec{u}, \vec{u}) = ||\vec{u}|| \cdot ||\vec{u}|| \cdot cos\, 0 = ||\vec{u}||^2 \cdot 1$.

Interpretación geométrica del producto escalar

Si $\vec{u} \neq \vec{0} \neq \vec{v}$:

$$(\vec{u}, \vec{v}) = 0 \text{ si y sólo si } \vec{u} \perp \vec{v}$$

En efecto:
Como $\vec{u} \neq \vec{0} \neq \vec{v}$ resulta que $(\vec{u}, \vec{v}) = 0$ implica $||\vec{u}|| \cdot ||\vec{v}|| \cdot cos\, \alpha = 0$ con $||\vec{u}|| \neq 0 \neq ||\vec{v}||$, de donde $cos\, \alpha = 0$ y $\alpha = \pi/2$.

Cálculo del producto escalar por coordenadas

Haremos esta cuenta en $\mathbb{R}^2$. Los conceptos son válidos para $\mathbb{R}^n$ pero para facilitar el razonamiento lo haremos en dos dimensiones.
Consideremos la base canónica de $\mathbb{R}^2$: $\mathcal{C}_2 = \{\breve{e}_1, \breve{e}_2\}$, donde $\breve{e}_1 = (1, 0)$ y

$\breve{e}_2 = (0, 1)$.

$$(\breve{e}_i, \breve{e}_j) = ||\breve{e}_i|| \cdot ||\breve{e}_j|| \cdot cos\, \alpha$$

entonces:

$$(\breve{e}_i, \breve{e}_j) = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j. \end{cases}$$

Sean ahora dos vectores $\vec{u} = (u_x, u_y)$ y $\vec{v} = (v_x, v_y)$.
Es decir:

$$\vec{u} = u_x(1, 0) + u_y(0, 1) = u_x \cdot \breve{e}_1 + u_y \cdot \breve{e}_2,$$
$$\vec{v} = v_x(1, 0) + v_y(0, 1) = v_x \cdot \breve{e}_1 + v_y \cdot \breve{e}_2$$

y calculemos su producto escalar:

$$\begin{aligned}(\vec{u}, \vec{v}) &= (u_x \cdot \breve{e}_1 + u_y \cdot \breve{e}_2, v_x \cdot \breve{e}_1 + v_y \cdot \breve{e}_2) = \\ &= (u_x \cdot \breve{e}_1, v_x \cdot \breve{e}_1) + (u_x \cdot \breve{e}_1, v_y \cdot \breve{e}_2) + (u_y \cdot \breve{e}_2, v_x \cdot \breve{e}_1) + (u_y \cdot \breve{e}_2, v_y \cdot \breve{e}_2) = \\ &= u_x \cdot v_x \cdot (\breve{e}_1, \breve{e}_1) + u_x \cdot v_y \cdot (\breve{e}_1, \breve{e}_2) + u_y \cdot v_x \cdot (\breve{e}_2, \breve{e}_1) + u_y \cdot v_y \cdot (\breve{e}_2, \breve{e}_2) = \\ &= u_x \cdot v_x \cdot 1 + u_x \cdot v_y \cdot 0 + u_y \cdot v_x \cdot 0 + u_y \cdot v_y \cdot 1 = u_x \cdot v_x + u_y \cdot v_y.\end{aligned}$$

Dijimos que esto es válido para cualquier dimensión n. Hagamos algunos ejemplos:

Ejemplo 9.5

1. En $\mathbb{R}^2$:
   $((2, 1), (-1, 3)) = 2 \cdot (-1) + 1 \cdot 3 = -2 + 3 = 1$
2. En $\mathbb{R}^3$:
   $((1, 5, 4), (-2, 3, 7)) = 1 \cdot (-2) + 5 \cdot 3 + 4 \cdot 7 = -2 + 15 + 28 = 41$
3. En $\mathbb{R}^4$:
   $((2, 3, 5, -1), (-2, 1, -1, 4)) = 2 \cdot (-2) + 3 \cdot 1 + 5 \cdot (-1) + (-1) \cdot 4 = -4 + 3 - 5 - 4 = 0$

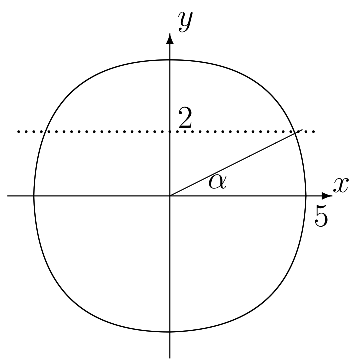
Utilizando el producto escalar podemos calcular el ángulo entre dos vectores. En efecto:

$$(\vec{u}, \vec{v}) = ||\vec{u}|| \cdot ||\vec{v}|| \cdot cos\, \alpha$$

de donde

$$cos\, \alpha = \frac{(\vec{u}, \vec{v})}{||\vec{u}|| \cdot ||\vec{v}||}.$$

Observación 9.3 Tenemos las "sensación" de que $cos\,\alpha$ no es la medida de un ángulo, pero sí lo es α. Recordemos que conocimos a $sen\,\alpha$, $cos\,\alpha$ y $tan\,\alpha$ como razones trigonométricas para medir ángulos y no como funciones. Bastante claramente vemos que si alguien nos dice que $tan\,\alpha = 2/5$ (tal vez por recuerdo de la pendiente de una recta, por "diferencia de y sobre diferencia de x") Dibujamos un triángulo rectángulo con 5 de base y 2 de altura y sabemos que el ángulo opuesto a la altura es el que satisface $tan\,\alpha = 2/5$. Tan fácilmente como eso podemos dibujar con precisión un ángulo que satisfaga $sen\,\alpha = 2/5$:



El seno de un ángulo es el opuesto sobre el radio, dibujemos, entonces, una circunferencia de 5 unidades de radio centrada en el origen. Sobre el eje de las ordenadas marcamos 2 unidades y trazamos una paralela al eje de las abscisas. Esta recta corta en dos puntos la circunferencia. Si unimos el origen de coordenadas con el punto de intersección, cualquiera de los dos ángulos satisface lo pedido. Si fuera $cos\,\alpha = 2/5$ marcaríamos las 2 unidades sobre el eje de las absisas.

Ejemplo 9.6 Determinar el ángulo formado por los vectores $\vec{u} = (3, 1, 1)$ y $\vec{v} = (1, -1, 4)$

$$cos\,\alpha = \frac{((3,1,1),(1,-1,4)}{\sqrt{3^2+1^2+1^2}\cdot\sqrt{1^2+(-1)^2+4^2}} = \frac{3-1+4}{\sqrt{11}\cdot\sqrt{6}} = \sqrt{\frac{6}{11}}.$$

Otros problemas que se pueden resolver usando la relación entre producto escalar, proyección ortogonal ángulo entre vectores y sus propiedades son del siguiente tipo:

Ejemplo 9.7 Sabiendo que los vectores coplanares $\vec{u}, \vec{v}$ y $\vec{w}$ satisfacen las condiciones: $\vec{u} \perp \vec{v}$, $\vec{u}$ es un versor,$||\vec{v}|| = 3$ $ang(\vec{v}, \vec{w}) = \frac{\pi}{6}$, $proy_{\vec{v}}(\vec{u} + \vec{w}) = 4$, calcular $(2\vec{u} - \vec{w}, \vec{u} + \vec{v})$.

Saquemos toda la información posible:

$||\vec{u}|| = 1$, porque es un versor.

$proy_{\vec{v}}(\vec{u} + \vec{w}) = proy_{\vec{v}}\vec{u} + proy_{\vec{v}}\vec{w} = proy_{\vec{v}}\vec{w} = ||\vec{w}||.cos\,\frac{\pi}{6} = 4$, entonces

$||\vec{w}|| = 8$

Porque $\vec{u}, \vec{v}, \vec{w}$ son coplanares, $\vec{u} \perp \vec{v}$ y $ang(\vec{v}, \vec{w}) = \frac{\pi}{6}$ resulta $ang(\vec{v}, \vec{w}) = \frac{\pi}{3}$.

Resolvamos, entonces:

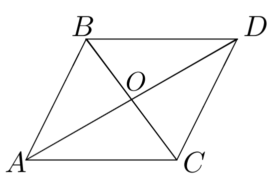
$$\begin{aligned}(2\vec{u} - \vec{w}, \vec{u} + \vec{v}) &= (2\vec{u}, \vec{u}) - (\vec{w}, \vec{u}) + (2\vec{u}, \vec{v}) - (\vec{w}, \vec{v}) = \\ &= (2\vec{u}, \vec{u}) - (\vec{w}, \vec{u}) + (2\vec{u}, \vec{v}) - (\vec{w}, \vec{v}) = \\ &= 2||\vec{u}||^2 - ||\vec{w}|| \cdot ||\vec{u}|| \cdot cos\,\tfrac{\pi}{6} + 2 \cdot 0 - ||\vec{v}|| \cdot ||\vec{w}\,||cos\,\tfrac{\pi}{3} = \\ &= 2 \cdot 1^2 - 8 \cdot 1 \cdot \tfrac{1}{2} + 2 \cdot 0 - 3 \cdot 8 \cdot \tfrac{\sqrt{3}}{2} = 2 - 4 - 12\sqrt{3} = -2 - 12\sqrt{3}.\end{aligned}$$

Leyes del paralelogramo

(L_1) Las diagonales de un paralelogramo se cortan en su punto medio.

(L_2) La suma de los cuadrados de las diagonales es igual a la suma de los cuadrados de los lados.

El uso de vectores para la demostración de estas leyes hace que sean prácticamente inmediatas.



Consideremos, según el gráfico, los vectores:

$\vec{u} = \overrightarrow{AB} = \overrightarrow{CD}$

$\vec{v} = \overrightarrow{AC} = \overrightarrow{BD}$

$\vec{D}^{(+)} = \vec{u} + \vec{v} = \overrightarrow{AD}$

$\vec{D}^{(-)} = \vec{u} - \vec{v} = \overrightarrow{BC}$.

Demostración:

(L_1) $\dfrac{\vec{D}^{(+)} + \vec{D}^{(-)}}{2} = \dfrac{(\vec{u} + \vec{v}) + (\vec{u} - \vec{v})}{2} = \vec{u}$.

¿Con esto ya está demostrado?

(L_2) $||\vec{D}^{(+)}||^2 + ||\vec{D}^{(-)}||^2 = ||\vec{u}||^2 + ||\vec{v}||^2 + ||\vec{u}||^2 + ||\vec{v}||^2$

$||\vec{D}^{(+)}||^2 + ||\vec{D}^{(-)}||^2 = 2(||\vec{u}||^2 + ||\vec{v}||^2)$

$||\vec{u} + \vec{v}||^2 + ||\vec{u} - \vec{v}||^2 = 2(||\vec{u}||^2 + ||\vec{v}||^2)$

$$\begin{aligned}||\vec{u} + \vec{v}||^2 + ||\vec{u} - \vec{v}||^2 &= (\vec{u} + \vec{v}, \vec{u} + \vec{v}) + (\vec{u} - \vec{v}, \vec{u} - \vec{v}) = \\ &= (\vec{u}, \vec{u}) + 2(\vec{u}, \vec{v}) + (\vec{v}, \vec{v}) + (\vec{u}, \vec{u}) - 2(\vec{u}, \vec{v}) + (\vec{v}, \vec{v}) = \\ &= 2(\vec{u}, \vec{u}) + 2(\vec{v}, \vec{v}) = \\ &= 2(||\vec{u}||^2 + ||\vec{v}||^2).\end{aligned}$$

□

9.1.6. Producto vectorial y producto mixto

Definiremos ahora una función $\cdot \wedge \cdot : E_3 \times E_3 \to E_3$, es decir, una operación binaria en E_3: tomamos dos vectores, los operamos y obtenemos un tercer vector.
Estamos buscando un vector perpendicular a dos vectores dados, tal que junto a los otros dos conforme una base. Dados dos vectores hay una única dirección, pero dada esa dirección hay dos sentidos posibles ¿Elegimos el que "va" o el que "viene"? Para desambiguar este hecho demos la noción de orientación del espacio:

Orientaciones del plano y el espacio

En el plano:
Dado un origen O y una base $\mathcal{B} = \{\vec{b}_1, \vec{b}_2\}$ se dice que la orientación es *positiva* si al colocar ambos vectores en el origen O la rotación necesaria para llevar el vector $\vec{b}_1$ hacia el vector $\vec{b}_2$ es contraria a las agujas del reloj (es decir, determina un ángulo positivo). Esta es la orientación que estamos acostumbrados a usar desde siempre. Por convención, uno habla de un punto (x, y), no solemos si quiera imaginar que podríamos llamarlo (y, x). En caso contrario decimos que la orientación es *negativa*.

En el espacio:
Dado un origen O y una base $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \vec{b}_3\}$ se dice que la orientación es *positiva* es un sistema *dextrógiro* o *directo* si al colocar los tres vectores en el mismo origen y un tornillo en la dirección de $\vec{b}_3$, al girar el sistema con la rotación necesaria para llevar el vector $\vec{b}_1$ hacia el vector $\vec{b}_2$, el tornillo asciende en la dirección de $\vec{b}_3$. (Nuevamente: si vamos del eje x al eje y, el tornillo "sube" por z). En caso contrario se dice que tiene orientación *negativa* es un sistema *levógiro* o *inverso*.

Aclarado este punto definamos la operación:

Definición 9.6 Sean $\vec{u}$ y $\vec{v}$ dos vectores no nulos de E_3 definimos $\vec{w}$ el *producto vectorial* de $\vec{u}$ y $\vec{v}$ y lo notamos $\vec{w} = \vec{u} \wedge \vec{v}$ al vector que satisface:

$\wedge_1)$ $(\vec{u}, \vec{w}) = (\vec{v}, \vec{w}) = 0$

$\wedge_2$) $||\vec{w}|| = ||\vec{u}|| \cdot ||\vec{v}|| \cdot sen\,\alpha$, donde α es el ángulo comprendido entre $\vec{u}$ y $\vec{v}$.

$\wedge_3$) $\{\vec{u}, \vec{v}, \vec{w}\}$ es una base de orientación positiva.

Si $\vec{u} = \vec{0}$ ó $\vec{v} = \vec{0}$, entonces $\vec{u} \wedge \vec{v} = \vec{0}$.

Nuevamente hemos tenido que hacer la distinción del vector nulo ya que en la definición utilizamos el ángulo entre ambos vectores y sabemos que no está definido para el vector nulo.
Claramente la primera condición pide la perpendicularidad buscada. Uno podría pensar que en la segunda condición faltan las barras de valor absoluto ya que el seno de un ángulo puede ser negativo y el módulo es siempre positivo. El hecho es que el ángulo comprendido entre dos vectores es siempre menor que llano y, en consecuencia, el seno siempre positivo. De cualquier modo, algunos autores prefieren escribirlo con barras de valor absoluto.

9.1.7. Propiedades del producto vectorial

Para todo $\vec{u}, \vec{v}$ y $\vec{w} \in V$ y $k \in \mathbb{R}$ se verifica:

1. $\vec{u} \wedge \vec{v} = -(\vec{v} \wedge \vec{u})$
2. $(\vec{u} + \vec{v}) \wedge \vec{w} = (\vec{u} \wedge \vec{w}) + (\vec{v} \wedge \vec{w})$
   $\vec{w} \wedge (\vec{u} + \vec{v}) = (\vec{w} \wedge \vec{u}) + (\vec{w} \wedge \vec{v})$
3. $k \cdot (\vec{u} \wedge \vec{v}) = (k \cdot \vec{u} \wedge \vec{v}) = (\vec{u} \wedge k \cdot \vec{v})$

No demostraremos estas propiedades, pero sí una propiedad que relaciona el producto escalar con el vectorial:

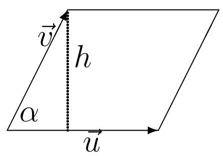
Proposición 9.1 $||\vec{u} \wedge \vec{v}||^2 - ||\vec{u}||^2 \cdot ||\vec{v}||^2 = (\vec{u}, \vec{v})^2$

Demostración: $||\vec{u} \wedge \vec{v}||^2 - ||\vec{u}||^2 \cdot ||\vec{v}||^2 =$

$$= (||\vec{u}|| \cdot ||\vec{v}|| \cdot sen\,ang(\vec{u}, \vec{v}))^2 - ||\vec{u}||^2 \cdot ||\vec{v}||^2 =$$
$$= ||\vec{u}||^2 \cdot ||\vec{v}||^2 \cdot (sen^2 ang(\vec{u}, \vec{v}) - 1) =$$
$$= ||\vec{u}||^2 \cdot ||\vec{v}||^2 \cdot cos^2 ang(\vec{u}, \vec{v}) =$$
$$= (\vec{u}, \vec{v})^2$$

□

Interpretación geométrica del producto vectorial



Recordemos que el área de un paralelogramo es el producto de la base por la altura. Sumemos a esto que dos vctores no paralelos generan un paralelogramo como en la figura. La longitud de la base de este paralelogramo es $||\vec{u}||$ y la altura es el cateto opuesto al ángulo α formado por ambos vectores y cuya hipotenusa es $||\vec{u}||$. En consecuencia, la medida de la altura es $||\vec{v}|| \cdot sen\,\alpha$ y el área del triángulo es

$$A = ||\vec{u}|| \cdot ||\vec{v}|| \cdot sen\,\alpha = ||\vec{u} \wedge \vec{v}||.$$

Cálculo del producto vectorial por coordenadas

Debemos hacer esta cuenta en $\mathbb{R}^3$.
Consideremos la base canónica de $\mathbb{R}^3$:

$$\mathcal{C}_3 = \{\breve{e}_1, \breve{e}_2, \breve{e}_3\}, \text{ donde } \breve{e}_1 = (1,0,0), \breve{e}_2 = (0,1,0) \text{ y } \breve{e}_3 = (0,0,1).$$

De las condiciones, para $i \neq j$:

$$||\breve{e}_i \wedge \breve{e}_j|| = ||\breve{e}_i|| \cdot ||\breve{e}_j|| \cdot sen\,\frac{\pi}{2} = 1$$

$$(\breve{e}_i \wedge \breve{e}_j, \breve{e}_i) = (\breve{e}_i \wedge \breve{e}_j, \breve{e}_j) = 0$$

deducimos que el producto vectorial entre dos versores diferentes de la base tiene la dirección del tercero y módulo 1, sólo falta analizar el sentido para que $\{\breve{e}_i, \breve{e}_j, \breve{e}_i \wedge \breve{e}_j\}$ tenga orientación positiva. Considerando esto obtenemos:

$$\begin{array}{lll}
\breve{e}_1 \wedge \breve{e}_1 = \vec{0} & \breve{e}_1 \wedge \breve{e}_2 = \breve{e}_3 & \breve{e}_1 \wedge \breve{e}_3 = -\breve{e}_2 \\
\breve{e}_2 \wedge \breve{e}_1 = -\breve{e}_3 & \breve{e}_2 \wedge \breve{e}_2 = \vec{0} & \breve{e}_2 \wedge \breve{e}_3 = \breve{e}_1 \\
\breve{e}_3 \wedge \breve{e}_1 = \breve{e}_2 & \breve{e}_3 \wedge \breve{e}_2 = -\breve{e}_1 & \breve{e}_3 \wedge \breve{e}_3 = \vec{0}
\end{array}$$

$\vec{u} = (u_x, u_y, u_z)$ y $\vec{v} = (v_x, v_y, v_z)$.
Es decir:

$$\vec{u} = u_x(1,0,0) + u_y(0,1,0) + u_z(0,0,1) = u_x \cdot \breve{e}_1 + u_y \cdot \breve{e}_2 + u_z \cdot \breve{e}_3,$$

$$\vec{v} = v_x(1,0,0) + v_y(0,1,0) + v_z(0,0,1) = v_x \cdot \breve{e}_1 + v_y \cdot \breve{e}_2 + v_z \cdot \breve{e}_3,$$

y calculemos su producto vectorial:

$$
\begin{aligned}
\vec{u} \wedge \vec{v} &= (u_x \cdot \breve{e}_1 + u_y \cdot \breve{e}_2 + u_z \cdot \breve{e}_3) \wedge (v_x \cdot \breve{e}_1 + v_y \cdot \breve{e}_2 + v_z \cdot \breve{e}_3) = \\
&= (u_x \cdot \breve{e}_1 \wedge v_x \cdot \breve{e}_1) + (u_x \cdot \breve{e}_1 \wedge v_y \cdot \breve{e}_2) + (u_x \cdot \breve{e}_1 \wedge v_z \cdot \breve{e}_3) + \\
&+ (u_y \cdot \breve{e}_2 \wedge v_x \cdot \breve{e}_1) + (u_y \cdot \breve{e}_2 \wedge v_y \cdot \breve{e}_2) + (u_y \cdot \breve{e}_2 \wedge v_z \cdot \breve{e}_3) + \\
&+ (u_z \cdot \breve{e}_3 \wedge v_x \cdot \breve{e}_1) + (u_z \cdot \breve{e}_3 \wedge v_y \cdot \breve{e}_2) + (u_z \cdot \breve{e}_3 \wedge v_z \cdot \breve{e}_3) = \\
&= u_x \cdot v_x(\breve{e}_1 \wedge \breve{e}_1) + u_x \cdot v_y(\breve{e}_1 \wedge \breve{e}_2) + u_x \cdot v_z(\breve{e}_1 \wedge \breve{e}_3) + \\
&+ u_y \cdot v_x(\breve{e}_2 \wedge \breve{e}_1) + u_y \cdot v_y(\breve{e}_2 \wedge \breve{e}_2) + u_y \cdot v_z(\breve{e}_2 \wedge \breve{e}_3) + \\
&+ u_z \cdot v_x(\breve{e}_3 \wedge \breve{e}_1) + u_z \cdot v_y(\breve{e}_3 \wedge \breve{e}_2) + u_z \cdot v_z(\breve{e}_3 \wedge \breve{e}_3) = \\
&= u_x \cdot v_x \cdot \vec{0} + u_x \cdot v_y \cdot \breve{e}_3 + u_x \cdot v_z \cdot (-\breve{e}_2) + \\
&+ u_y \cdot v_x \cdot (-\breve{e}_3) + u_y \cdot v_y \cdot \vec{0} + u_y \cdot v_z \cdot \breve{e}_1 + \\
&+ u_z \cdot v_x \cdot \breve{e}_2 + u_z \cdot v_y \cdot (-\breve{e}_1) + u_z \cdot v_z \cdot \vec{0}.
\end{aligned}
$$

Eliminemos los términos nulos y saquemos factor común los versores:

$$
\begin{aligned}
\vec{u} \wedge \vec{v} &= (u_y \cdot v_z - u_z \cdot v_y) \cdot \breve{e}_1 + (-u_x \cdot v_z + u_z \cdot v_x) \cdot \breve{e}_2 + (u_x \cdot v_y - u_y \cdot v_x) \cdot \breve{e}_3 \\
&= (u_y \cdot v_z - u_z \cdot v_y) \cdot \breve{e}_1 + (-1)(u_x \cdot v_z - u_z \cdot v_x) \cdot \breve{e}_2 + (u_x \cdot v_y - u_y \cdot v_x) \cdot \breve{e}_3 \\
&= \begin{vmatrix} u_y & u_z \\ v_y & v_z \end{vmatrix} \cdot \breve{e}_1 + (-1) \begin{vmatrix} u_x & u_z \\ v_x & v_z \end{vmatrix} \cdot \breve{e}_2 + \begin{vmatrix} u_x & u_y \\ v_x & v_y \end{vmatrix} \cdot \breve{e}_3
\end{aligned}
$$

Llegado a este punto podemos pensar en la deficinicón del determinante de una matriz por elementos de una línea y escribir:

$$
\vec{u} \wedge \vec{v} = \begin{vmatrix} \breve{e}_1 & \breve{e}_2 & \breve{e}_3 \\ u_x & u_y & u_z \\ v_x & v_y & v_z \end{vmatrix}.
$$

O bien recordar que estamos trabajando con vectores y que hemos encontrado las coordenadas del vector producto vectorial en la base canónica, entonces escribimos:

$$
\vec{u} \wedge \vec{v} \left(\begin{vmatrix} u_y & u_z \\ v_y & v_z \end{vmatrix}, -\begin{vmatrix} u_x & u_z \\ v_x & v_z \end{vmatrix}, \begin{vmatrix} u_x & u_y \\ v_x & v_y \end{vmatrix} \right).
$$

Ejemplo 9.8

Sean $\vec{u} = (1, 3, 2)$,
$\vec{v} = (4, -2, 5)$.

Estoy buscando un vector de tres coordenadas. La coordenada del medio cambia de signo, y en cada coordenada va el determinante de la matriz que queda tapando dicha coordenada.
Entonces resulta:

$$\left(\begin{vmatrix} 3 & 2 \\ -2 & 5 \end{vmatrix}, - \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix}, \begin{vmatrix} 1 & 3 \\ 4 & -2 \end{vmatrix} \right) = (19, 3, -14).$$

Podemos verificar este resultado porque sabemos que debe ser un vector perpendicular a los dos anteriores, es decir: al hacer el producto escalar con los anteriores da 0.
En efecto:

$$((1,3,2),(19,3,-14)) = 19 + 9 - 28 = 0$$
$$((4,-2,5),(19,3,-14)) = 76 - 6 - 70 = 0$$

Ejemplo 9.9 Calcular el área del triángulo cuyos vértices son $A = (1,1,1)$, $B = (3,2,5)$ y $C = (1,-1,6)$. Claramente al tener tres puntos si tomamos uno de ellos (digamos el A) como origen, determinamos dos vectores $\overrightarrow{AB} = (2,1,4)$ y $\overrightarrow{AC} = (0,-2,5)$. Estos tres puntos son los vértices de un triángulo cuya área es la mitad del área del paralelogramo generado por $\overrightarrow{AB}$ y $\overrightarrow{AC}$. De aquí, el área del triángulo es:

$$\frac{||\overrightarrow{AB} \wedge \overrightarrow{AC}||}{2} =$$

$$= \frac{\left|\left| \left(\begin{vmatrix} 1 & 4 \\ -2 & 5 \end{vmatrix}, - \begin{vmatrix} 2 & 4 \\ 0 & 5 \end{vmatrix}, \begin{vmatrix} 2 & 1 \\ 0 & -2 \end{vmatrix} \right) \right|\right|}{2} = \frac{\sqrt{(13)^2 + (-10)^2 + (-4)^2}}{2} = \frac{\sqrt{285}}{2}$$

Producto mixto

Dados tres vectores podemos hacer el producto vectorial entre dos de ellos y luego hacer escalar con el tercero. Así estamos usando ambos productos, por eso suele denominarse*doble producto* o bien *producto mixto*. Si escribimos el producto vectorial como tal que cada coordenada es un determinante y luego calculamos el producto escalar con $w = (w_x, w_y, w_z)$ resulta:

$$(\vec{u} \wedge \vec{v}, \vec{w}) = \left(\left(\begin{vmatrix} u_y & u_z \\ v_y & v_z \end{vmatrix}, \begin{vmatrix} u_x & u_z \\ v_x & v_z \end{vmatrix}, \begin{vmatrix} u_x & u_y \\ v_x & v_y \end{vmatrix} \right), (w_x, w_y, w_z) \right) =$$

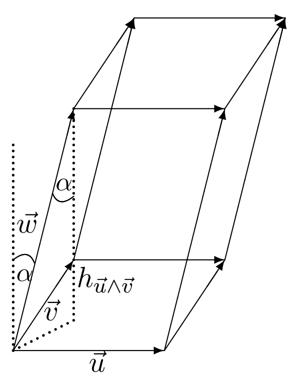
$$= \begin{vmatrix} w_x & w_y & w_z \\ u_x & u_y & u_z \\ v_x & v_y & v_z \end{vmatrix} = \begin{vmatrix} u_x & u_y & u_z \\ v_x & v_y & v_z \\ w_x & w_y & w_z \end{vmatrix}.$$

Enunciaremos ahora una propiedad de muy sencilla demostración, que dejamos gentilmente a cargo del lector interesado.

Proposición 9.2 $(\vec{u} \wedge \vec{v}, \vec{w}) = (\vec{u}, \vec{v} \wedge \vec{w})$

La demostración de esta propiedad es una simple aplicación de propiedades de determinantes. El lector interesado considérese invitado a escribirla en detalle. ®

Interpretación geométrica del producto mixto



El volumen de un paralelepípedo es superficie de la base por la altura. Sabemos que la superficie de la base es el área del paralelogramo y, en consecuencia el módulo del producto vectorial entre $\vec{u}$ y $\vec{w}$. Debemos ver cómo calcular la altura h. En la gráfica se ve que h es el cateto adyacente al ángulo α que se forma entre el producto vectorial y el vector $\vec{w}$, en consecuencia la longitud es $||\vec{w}|| \cdot |cos\, \alpha|$. En consecuencia el volumen V del paralelepípedo es

$$V = ||\vec{u} \wedge \vec{v}|| \cdot ||\vec{w}|| \cdot |cos\, \alpha| = |(\vec{u} \wedge \vec{v}, \vec{w})|$$

Dado que el valor absoluto del producto mixto da el volumen de un paralelepípedo, se suele utilizar para estudiar si tres vectores son coplanares o no.

9.1.8. Una aplicación a la física

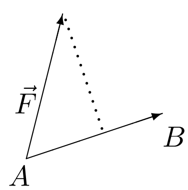
Como decíamos al inicio de este caítulo, los vectores son de gran uso para representar fuerzas.
Es interesante mencionar que en física se suele usar una notación diferente. Más precisamente: nosotros (algunos matemáticos) llamamos $\breve{e}_i$ a los versores de la base canónica, ellos (algunos físicos) usan esta equivalencia: $\breve{e}_1$: $\breve{\imath}$, $\breve{e}_2$: $\breve{\jmath}$, $\breve{e}_3$: $\breve{k}$, así el vector

$$\vec{u} = (u_x, u_y, u_z) = u_x \cdot \breve{e}_1 + u_y \cdot \breve{e}_2 + u_z \cdot \breve{e}_3$$

suelen escribirlo:

$$\vec{u} = (u_x, u_y, u_z) = u_x \cdot \breve{\imath} + u_y \cdot \breve{\jmath} + u_z \cdot \breve{k}.$$

En mecánica clásica, se dice que una fuerza realiza *trabajo* cuando altera el estado de movimiento de un cuerpo. El trabajo de la fuerza sobre ese cuerpo será equivalente a la energa necesaria para desplazarlo. El trabajo es una magnitud física escalar que se representa con la letra W (del inglés: Work) y se expresa en *julios* o *joules* (J) en el Sistema Internacional de Unidades.



Definición 9.7 Si $\overrightarrow{F}$ es una fuerza constante y $\overrightarrow{d}$ es el vector de origen A y extremo B, el *trabajo* realizado por $\overrightarrow{F}$ al ir desde A hasta B es $(\vec{F}, \vec{d})$.

Notemos que

$$(\vec{F}, \vec{d}) = ||\vec{F}|| \cdot ||\vec{d}|| \cdot \cos(\vec{F}, \vec{d}) = ||\vec{d}|| proy_{\vec{d}} \vec{F}$$

que nos recuerda a nuestra conocida fórmula:

"trabajo es fuerza por espacio".

Ejemplo 9.10 Una fuerza está dada por el vector $\vec{F} = 3\mathbf{i} + 4\mathbf{j} + 5\mathbf{k}$ y mueve una partícula del punto $P : (2, 1, 0)$ al punto $Q : (4, 6, 2)$. Calcular el trabajo realizado.
Primero calculamos el vector distancia:

$$\vec{d} = \overrightarrow{PQ} = Q - P = (4 - 2, 6 - 1, 2 - 0) = (2, 5, 2)$$

realicemos ahora el producto escalar:

$$(\vec{F}, \vec{d}) = ((3, 4, 5), (2, 5, 2)) = 3 \cdot 2 + 4 \cdot 5 + 5 \cdot 2 = 6 + 20 + 10 = 36.$$

En mecánica newtoniana, se denomina *momento de una fuerza* respecto a un punto dado a una magnitud (pseudo)vectorial, obtenida como producto vectorial del vector de posición del punto de aplicacin de la fuerza (con respecto al punto al cual se toma el momento) por el vector fuerza, en ese orden. Se lo suele llamar simplemente *momento* o *momento dinámico*.
Y hablando de las diferencias entre físicos y matemáticos podemos mencionar esta otra: los matemáticos en general notamos el producto vectorial con el símbolo $\wedge$ y ellos suelen usar $\times$, así $\vec{m}$, el producto vectorial entre $\vec{u}$ y $\vec{v}$ se puede escribir:

$$\vec{m} = \vec{u} \wedge \vec{v} = \vec{u} \times \vec{v}.$$

Definición 9.8 Se llama *momento* de una fuerza $\vec{F}$ respecto a un punto O al producto vectorial $\vec{m} = \overrightarrow{OP} \times \vec{F}$, donde P es el punto de apoyo de $\vec{F}$.

Ejemplo 9.11 Sea $\vec{F} = \mathbf{i} + \mathbf{j} - 2\mathbf{k}$ una fuerza que actúa sobre el punto $P : (2, -1, 3)$. Hallar el momento de $\vec{F}$ respecto al origen de coordenadas.
Calculemos el producto vectorial, cuidando el orden en que colocamos los vectores:

$$\vec{m} = \overrightarrow{OP} \times \vec{F} = (2, -1, 3) \wedge (1, 1, -2) = (-1, 7, 3).$$

9.2. Geometría del plano y del espacio

9.2.1. Ecuación de la recta en el plano y el espacio

Pensemos qué caracteriza a una recta: su inclinación nos da toda la familia de rectas paralelas y un punto por el que pasa distingue a una de ellas. Esto nos lleva a pensar que necesitamos dos cosas:

1. Dirección: que es lo que llamamos la *pendiente* de la recta,
2. Punto por el que pasa, que nos determina lo que llamamos la *ordenada al origen.*

Dos puntos cualesquiera, sean A y B determinan una recta L. La dirección está dada por el vector $\overrightarrow{AB}$ o bien el $\overrightarrow{BA}$, al que en cualquier caso llamamos el *director* de la recta L y lo notamos $\vec{d_L}$ y cualquiera de los dos puntos, llamémoslo P_0 es el punto por el que pasa. ¿De qué modo puedo expresar a cualquier punto P dentro de la recta? Claramente con el vector $\overrightarrow{P_0P}$ será un múltiplo del vector director, pero P es el extremo de este vector, y recordando la fórmula **V=E-O** vemos que **E=O+V** y resulta la ecuación de la recta:

$$P = P_0 + \lambda \cdot \vec{d_L}, \lambda \in \mathbb{R}.$$

Acabamos de dar la *ecuación de la recta en forma vectorial* y es interesante notar que no hemos aclarado cuál es la dimensión del espacio en cuestión. Así, resulta:

1. En $\mathbb{R}^2$:
   $(x, y) = (x_0, y_0) + \lambda \cdot (d_x, d_y), \quad \lambda \in \mathbb{R}$, donde $\vec{d_L} = (d_x, d_y)$.
2. En $\mathbb{R}^3$:
   $(x, y, z) = (x_0, y_0, z_0) + \lambda \cdot (d_x, d_y, d_z), \quad \lambda \in \mathbb{R}$, donde $\vec{d_L} = (d_x, d_y, d_z)$.

Si escribimos las ecuaciones coordenada a coordenada, obtenemos lo que se denomina *ecuación paramétrica de la recta*

En $\mathbb{R}^2$:

$$\begin{cases} x = x_0 + \lambda \cdot d_x \\ y = y_0 + \lambda \cdot d_y \end{cases}, \lambda \in \mathbb{R}$$

En $\mathbb{R}^3$:

$$\begin{cases} x = x_0 + \lambda \cdot d_x \\ y = y_0 + \lambda \cdot d_y \\ z = z_0 + \lambda \cdot d_z \end{cases}, \lambda \in \mathbb{R}$$

Observación 9.4 En más de una oportunidad consideramos que algunas de las cosas que escribimos están "de adorno". Una de esas oportunidades es la ecuación de la recta en forma vectorial o paramétrica "¿Para qué necesito escribir $\lambda \in \mathbb{R}$?", se pregunta más de uno. Justamente, no es el caso de escritura "pro forma", sino que es de vital importancia saber en qué intervalo se encuentra el parámetro. Si pusiéramos $\lambda \in [0, 1]$ en lugar de una recta habríamos dado un segmento, y si $\lambda \in \mathbb{N}$ estaríamos en presencia de una sucesión.

Consideremos la ecuación paramétrica de la recta en el plano:

$$\begin{cases} x = x_0 + \lambda \cdot d_x \\ y = y_0 + \lambda \cdot d_y \end{cases}, \lambda \in \mathbb{R}$$

si en ambas ecuaciones despejamos λ e igualamos obtenemos:

$$\frac{x - x_0}{d_x} = \frac{y - y_0}{d_y}$$

de donde:

$$x \cdot d_y - y \cdot d_x + (-x_0 \cdot d_y + y_0 \cdot d_x) = 0$$

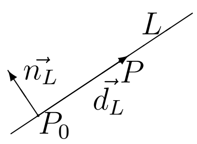
o lo que es lo mismo:

$$a \cdot x + b \cdot y + c = 0$$

que es lo que llamamos la *ecuación implícita de la recta en el plano*, y podemos encontrar la *ecuación explícita* simplemente despejando la variable y:

$$y = -\frac{a}{b} \cdot x - \frac{c}{b}.$$

Obtengamos esta ecuación por otro medio:



Tenemos una recta L, es decir: una dirección dada por el vector director $\vec{d}_L$ y un punto por el que pasa: P_0. Sabemos que en el plano existe una única dirección perpendicular a una dirección dada. Llamamos a ese vector el *normal* a la recta (no importa en qué sentido lo tomemos) y lo notamos $\vec{n}_L$. Si un punto P pertenece a la recta L el vector $\overrightarrow{P_0P}$ debe ser un múltiplo de $\vec{d}_L$, es decir, debe ser perpendicular a $\vec{n}_L$. Si escribimos esto en una ecuación obtenemos:

$$(\overrightarrow{P_0P}, \vec{n}_L) = 0$$

Pongamos $P : (x, y), P_0 = (x_0, y_0)$ y $\vec{n}_L = (a, b)$ y reescribamos la ecuación anterior:

$$((x - x_0, y - y_0), (a, b)) = 0$$

o lo que es lo mismo:

$$a(x - x_o) + b(y - y_0) = 0,$$

que es lo que conocemos como *ecuación implícita de la recta que pasa por el punto* (x_0, y_0).O bien:

$$a \cdot x + b \cdot y + (a \cdot (-x_0) + b \cdot (-y_0)) = 0,$$

que equivale a:

$$a \cdot x + b \cdot y + c = 0.$$

Si revisamos los pasos que hemos ido siguiendo vemos que $a = d_y$ y $b = -dx$, lo cual confirma que (a, b) es el vector normal a la recta de director (d_x, d_y).

Ejemplo 9.12

1. Hallar en todas las formas que conozca la ecuación de la recta L_1 que pasa por los puntos $(1, -1)$ y $(0, 2)$.
   Un vector director para la recta es $\vec{d}_{L_1} = (1 - 0, -1 - 2) = (1, -3)$ y un normal a este vector $\vec{n}_{L_1} = (3, 1)$

   Ecuación vectorial:
   $L_1 : (x, y) = (0, 2) + \lambda \cdot (1, -3),\ \lambda \in \mathbb{R}$
   Ecuación paramétrica:
   $L_1 : \begin{cases} x = 0 + 1 \cdot \lambda \\ y = 2 + (-3) \cdot \lambda \end{cases},\ \lambda \in \mathbb{R}$

Ecuación implícita:
$L_1 : 3 \cdot x + 1 \cdot y + c = 0$, como ,pasa por $(0, 2)$ resulta:$c = -2$ y $L = 3 \cdot x + y - 2 = 0$.

Ecuación explícita:
$L_1 : y = -3 \cdot x + 2$

2. Hallar en forma paramétrica la ecuación de la recta L_2 cuya forma implícita es $L_2 : 2 \cdot x + 3 \cdot y - 2 = 0$.
Sabemos que los coeficientes que acompañan a x e y son el vector normal, es decir: $\vec{n}_{L_2} = (2, 3)$ y en consecuencia $\vec{d}_{L_2} = (-3, 2)$. Dando un valor a una variable despejamos la otra u obtenemos un punto por el que pasa. En este caso, podemos tomar $y = 0$ que resulta en $x = -1$ y un punto por el que pasa la recta es $(-1, 0)$. Una ecuación en forma paramétrica será:

$$L : \begin{cases} x = -1 - 3 \cdot \lambda \\ y = 0 + 2 \cdot \lambda \end{cases}, \lambda \in \mathbb{R}.$$

Decimos "una" ecuación y no "la" ecuación porque claramente no es única, ya que hay infinitos puntos que podemos tomar y aunque la dirección es única, el vector director tiene infinitas longitudes y dos sentidos posibles.

3. Hallar la ecuación implícita de una recta L_3 cuya ecuación paramétrica es:

$$L_3 : \begin{cases} x = 2 + 3 \cdot \lambda \\ y = -1 - 5 \cdot \lambda \end{cases}, \lambda \in \mathbb{R}.$$

en la forma paramétrica está el parámetro que no figura en la forma implícita. Si simplemente hacemos alguna cuenta para eliminar este parámetro obtenemos la ecuación implícita.
En efecto: Multipliquemos la primera ecuación por el coeficiente de λ en la segunda, la segunda por el coeficiente de λ en la primera y restemos:

$$\begin{array}{rlrl} (-5) \cdot x &= (-5) \cdot 2 + 3 \cdot (-5).\lambda & \qquad -5 \cdot x &= -10 - 15\lambda \\ 3 \cdot y &= 3 \cdot (-1) - 3 \cdot 5\lambda & 3 \cdot y &= -3 - 15\lambda \end{array}$$

obtenemos:

$$-5x + 3y = -13, \text{ o lo que es lo mismo: } -5x + 3y + 13 = 0.$$

Observación 9.5 Simplemente lo que hemos hecho es resolver un sistema de dos ecuaciones con dos incógnitas que es compatible indeterminado, con grado de indeterminación 1, marcado por el parámetro.

9.2.2. Ecuación del plano

Tres puntos no alineados en el espacio A, B y C determinan un plano π. Si ponemos uno de ellos como origen, sea A, encontramos dos vectores no paralelos (es decir linealmente independientes) $\overrightarrow{AB}$ y $\overrightarrow{AC}$. Cualquier punto P del plano es el extremo de una combinación lineal entre los vectores $\overrightarrow{AB}$ y $\overrightarrow{AC}$. e igual que hicimos con la ecuación de la recta obtenemos la *forma vectorial de la ecuación del plano*

$$\pi : (x, y, z) = A + \lambda \cdot \overrightarrow{AB} + \mu.\overrightarrow{AC}, \quad \lambda, \mu \in \mathbb{R}.$$

y nuevamente escribiendo las coordenadas por renglones obtenemos la *ecuación paramétrica del plano*. Ninguna de estas formas es demasiado práctica. Pensemos ahora que dados dos vectores obtenemos una única dirección perpendicular a ambos, sea $\vec{n}_\pi = \overrightarrow{AB} \wedge \overrightarrow{AC}$ y un punto P pertenecerá a π cada vez que el vector $\overrightarrow{AP}$ sea perpendicular a $\vec{n}_\pi$.

Pongamos $P : (x, y, z), P_0 = (x_0, y_0, z_0)$ y $\vec{n}_L = (a, b, c)$ y reescribamos la ecuación anterior:

$$((x - x_0, y - y_0, z - z_0), (a, b, c)) = 0$$

o lo que es lo mismo:

$$a(x - x_o) + b(y - y_0) + c(z - z_0) = 0,$$

que es lo que conocemos como *ecuación cartesiana del plano que pasa por el punto* (x_0, y_0, z_0).

Ejemplo 9.13 Hallar la ecuación del plano que pasa por los puntos $(1, 2, 4)$, $(0, 3, 1)$ y $(-2, 1, 1)$ buscamos dos direcciones linealmente independientes generadas por estos tres puntos: $(1, 2, 4) - (0, 3, 1) = (1, -1, 3)$ y $(-2, 1, 1) - (0, 3, 1) = (-2, -1, 0)$ Hacemos el producto vectorial entre ellos y encontramos el vector normal al plano: $\vec{n}_\pi = (3, -6, -3)$, como es una dirección, bien podemos considerar: $\vec{n}_\pi = (-1, 2, 1)$.
La ecuación del plano es:

$$-x + 2y + z + d = 0,$$

como pasa por el punto $(0, 3, 1)$ resulta $d = -7$ y la ecuación:

$$-x + 2y + z - 7 = 0.$$

Observación 9.6 Analicemos el procedimiento para encontrar las ecuacines implícitas de la recta en el plano y del plano en el espacio. En ambos casos afirmamos que existe unaúnica dirección perpendicular al objeto cuya ecuación buscamos y construimos el vector normal al mismo. Esto se produce porque a cada "objeto" "le falta una pata" para completar el espacio en que vive. Es decir, la recta tiene dimensión 1 (para generarla basta un vector) y $\mathbb{R}^2$ tiene dimensión 2, por lo tanto a la recta "le falta uno" para completar el espacio en que está definida; el plano tiene dimensión 2 (para generarlo necesitamos dos vectores linealmente independientes) y $\mathbb{R}^3$ tiene dimensión 3, por lo tanto al plano "le falta uno" para completar el espacio en que está definido. Por este motivo decimos que la recta es un *hiperplano* de $\mathbb{R}^2$ y el plano es un *hiperplano* de $\mathbb{R}^3$. Son los únicos casos en que se puede hallar una ecuación implícita. Es decir, no existe la ecuación implícita de la recta en $\mathbb{R}^3$.

Ecuación de la recta en el espacio

Cuando vimos la ecuación de la recta en el plano dijimos que la forma vectorial y la paramétrica eran independientes de la dimensión del espacio en que trabajemos.
Si, al igual que hicimos para encontrar la forma implícita en el plano despejáramos λ en las tres ecuaciones de la forma paramétrica e igualáramos obtendríamos:

$$\frac{x-x_0}{d_x} = \frac{y-y_0}{d_y} = \frac{z-z_0}{d_z}$$

y es lo que denominamos *expresión en ecuaciones simétricas.* Claramente esta forma carece de sentido cuando alguna de las coordenadas del vector director de la recta es nula. (Porque no podemos dividir por 0.)
No podemos encontrar una única ecuación a partir de estas igualdades, en consecuencia, no podemos encontrar una forma implícita de la ecuación de la recta en $\mathbb{R}^3$.

Pensemos que la forma implícita en el plano la encontramos vectorialmente diciendo que existe una única dirección perpendicular a una recta en el plano. Lo propio hicimos para encontrar la ecuación implícita (o cartesiana), de un plano en el espacio. Pero perpendicular a una recta en el espacio hay infinitas direcciones.
Acabamos de ver la ecuación cartesiana de un plano en el espacio. Si consideramos dos planos podemos escribir el sistema:

$$\begin{cases} ax + by + cz + d = 0 \\ a'x + b'y + c'z + d' = 0 \end{cases},$$

o bien:

$$\begin{cases} ax + by + cz = -d \\ a'x + b'y + c'z = -d' \end{cases}.$$

Claramente se trata de un sistema de dos ecuaciones con dos incógnitas que nunca será compatible determinado. Puede ser incompatible, es decir, que no haya ningún punto en común en los planos y por lo tanto se tratará de dos planos paralelos. Puede ser que sea el mismo plano (es decir una ecuación sea múltiplo de la otra) o bien que sea un sistema compatible indeterminado con grado de indeterminación 1. Es decir: una recta.
Efectivamente, una recta en el espacio la podemos escribir como intersección de dos planos.

Ejemplo 9.14 Consideremos el sistema:

$$\begin{cases} x - 2y + 3z = -1 \\ 2x + y - z = 3 \end{cases}$$

Resolvamos el sistema por el método de Gauss:

$$\begin{array}{lrrrrrrrrr} \text{Ec.1} & & x & - & 2y & + & 3z & = & -1 \\ \text{Ec.2} & & 2x & + & y & - & z & = & 3 \end{array}$$

$$\begin{array}{lrrrrrrrrr} \text{Ec.1} & & x & - & 2y & + & 3z & = & -1 \\ \text{Ec.2-2.Ec.1} & \mapsto & & & 5y & - & 7z & = & 5 \end{array}$$

Resulta:

$$y = \frac{7z+5}{5}, \quad x = \frac{-z+5}{5}$$

y la solución generalizada es:

$$\left(\frac{-a+5}{5}, \frac{7a+5}{5}, a\right)_{a\in\mathbb{R}}$$

que se puede escribir coordenada a coordenada y cambiando a por λ del siguiente modo:

$$\begin{cases} x = 1 - \frac{1}{5}\lambda \\ y = 1 + \frac{7}{5}\lambda \\ z = \lambda \end{cases}, \lambda \in \mathbb{R}$$

que es la ecuación de una recta L que pasa por el punto $(1,1,0)$ y su vector director es $\vec{d_L} = \left(-\frac{1}{5}, \frac{7}{5}, 1\right)$ y podríamos considerar $\vec{d_L} = (-1, 7, 5)$.

Pensemos vectorialmente: Estamos buscando la ecuación de una recta que es la intersección de dos planos, supongamos π_1 y π_2 Como la recta está en el plano π_1 el vector director de la recta debe ser perpendicular al vector normal de π_1, lo mismo ocurre con el plano π_2. es decir, el vector director de la recta debe ser simultáneamente perpendicular al normal de π_1 y al normal de π_2. Ya tenemos la herramienta para calcularlo:

$$\vec{d}_L = \vec{n}_{\pi_1} \wedge \vec{n}_{\pi_2}$$

Hagamos la cuenta: $(1, -2, 3) \wedge (2, 1, -1) = (-1, 7, 5)$. Sólo falta encontrar un punto por el que pasa y fácilmente vemos que el $(1, 1, 0)$ satisface ambas ecuaciones. Ya tenemos la ecuación de la recta en forma paramétrica o vectorial.

Haz de planos

Cuando resolvemos sistemas de ecuaciones lineales, decimos que podemos reemplazar cualquier ecuación por una combinación lineal de las ecuaciones del sistema, que contenga a la ecuación en cuestión y la solución no se altera. en este caso tenemos dos ecuaciones: la del plano π_1 y la del plano π_2 y este principio dice que si $L \subseteq \pi_1$ y $L \subseteq \pi_2$ entonces $L \subseteq \alpha.\pi_1 + \beta.\pi_2$, cualesquiera que sean α y β no simultáneamente nulos. Esta combinación lineal se denomina *haz de planos*

Ejemplo 9.15 Consideremos nuevamente la recta del ejemplo 9.14. El haz de planos que la contiene está dado por:

$$\alpha \cdot (x - 2y + 3z + 1) + \beta \cdot (2x + y - z - 3) = 0, \qquad \text{con } \alpha, \beta \text{ no simultánemanete nulos.}$$

Reacomodemos los coeficientes:

$$\alpha \cdot x - 2 \cdot \alpha \cdot y + 3 \cdot \alpha \cdot z + \alpha + 2 \cdot \beta \cdot x + \beta \cdot y - \beta \cdot z - 3 \cdot \beta = 0$$

$$(\alpha + 2\,\beta) \cdot x + (-2\,\alpha + \beta) \cdot y + (3\,\alpha - \beta) \cdot z + (\alpha - 3\,\beta) = 0$$

Si quisiéramos hallar un plano que contenga a la recta L y pase por $(3, 1, 0)$ reemplazamos el punto en el haz y despejamos α y β:

$$(\alpha + 2\beta) \cdot 3 + (-2\alpha + \beta) \cdot 1 + (3\alpha - \beta) \cdot 0 + (\alpha - 3\beta) = 0$$

$$2\alpha + 4\beta = 0 \qquad\qquad \alpha = -2\beta \text{ una solución: } \alpha = 2, \beta = -1.$$

El plano buscado es: $-5\,y + 7\,z - 5 = 0$. Podemos buscar también, un plano que contenga a la recta y que sea perpendicular al vector $\vec{v} = (3, -1, 2)$. Si el plano debe ser perpendicular al vector $\vec{v}$, entonces el normal del plano debe ser $k \cdot \vec{v}$. Tenemos entonces el sistema de ecuaciones:

$$\begin{cases} \alpha + 2\beta = 3 \cdot k \\ -2\alpha + \beta = -1 \cdot k \\ 3\alpha - \beta = 2 \cdot k \end{cases}$$

Se trata de un sistema de tres ecuaciones con tres incógnitas, que puede ser compatible o no. En este caso resulta $\alpha = \beta = k$ y un plano posible es $3 \cdot x - y + 2 \cdot z - 2 = 0$.
Si hubiéramos querido que sea perpendicular al vector $(3, -1, 1)$, claramente el sistema no habría tenido solución como puede verificarlo cualquier lector interesado.

¿Cómo encuentro la ecuación de una recta como intersección de planos si tengo la forma vectorial (o paramétrica)?

Una de las formas recomendades es pasar la recta a ecuaciones simétricas y despejar de las ecuaciones de a dos. Este es un buen método, siempre que existan las ecuaciones simétricas, porque si el vector director de la recta tiene una coordenada nula, ya no lo podemos aplicar.

Veamos ejemplos de estos casos:

Ejemplo 9.16 1. Sea

$$L = \begin{cases} x = 1 + 2\lambda \\ y = 3 - 5\lambda \\ z = 2 + 2\lambda \end{cases}, \lambda \in \mathbb{R}.$$

Llevemos esta recta a su expresión en ecuaciones simétricas:

$$\frac{x-1}{2} = \frac{y-3}{-5} = \frac{z-2}{2}$$

Despejando de las dos primeras igualdades obtenemos el plano $\pi_1 : 5x + 2y - 11 = 0$ y de las dos segundas el plano $\pi_2 : 2x + 5z - 16 = 0$.
Si tenemos algún problema discriminatorio por el cual queremos que todos los planos tengan x, y y z sencillamente buscamos otros usando el haz de planos:

$$\alpha \cdot (5x + 2y - 11) + \beta \cdot (2x + 5z - 16) = 0$$

y podemos escribir π'_1 con $\alpha = \beta = 1$ y π'_2 con $\alpha = 2, \beta = -1$ y la recta queda expresada por:

$$L : \begin{cases} \pi'_1 : 7x + 2y + 5z - 27 = 0 \\ \pi'_2 : 8x + 4y - 5z - 6 = 0 \end{cases}$$

De cualquier modo, el método que recomiendo es no pasar por las ecuciones simétricas y simplemente buscar operaciones elementales entre dos (o tres) ecuaciones, que eliminen el λ.
Por ejemplo:

Ec.1-Ec.3: $x - z = -1$ y
5.Ec.1+2.Ec.2: $5x + 2y = 11$

Y ya tenemos los dos planos que generan el mismo haz. Cedo gentilmente el honor de la verificación al lector interesado. ®

Antes de avanzar hagamos un pequeño resumen:
En $\mathbb{R}^2$ la ecuación de la recta se puede escribir de las siguientes formas:

vectorial:

$$(x, y) = (x_0, y_0) + \lambda \cdot (b, -a), \lambda \in \mathbb{R}$$

paramétrica:

$$\begin{cases} x = x_0 + \lambda \cdot b \\ y = y_0 + \lambda \cdot (-a) \end{cases}, \lambda \in \mathbb{R}$$

implícita:

$$ax + by + c = 0$$

explícita:

$$y = \left(\frac{-a}{b}\right) x - \frac{c}{a}$$

Debemos notar que la forma explícita es la única que es (aunque sea redundante) única. Para todas las demás existen infinitas variantes.

En $\mathbb{R}^3$ la ecuación de la recta se puede escribir de las siguientes formas:

vectorial:

$$(x, y, z) = (x_0, y_0, z_0) + \lambda \cdot (d_x, d_y, d_z), \lambda \in \mathbb{R}$$

paramétrica:

$$\begin{cases} x = x_0 + \lambda \cdot d_x \\ y = y_0 + \lambda \cdot d_y \\ z = z_0 + \lambda \cdot d_z \end{cases}, \lambda \in \mathbb{R}$$

ecuaciones simétricas:

$$\frac{x - x_0}{d_x} = \frac{y - y_0}{d_y} = \frac{z - z_0}{d_z}$$

como intersección de planos:

$$\begin{cases} ax + by + cz + d = 0 \\ a'x + b'y + c'z + d' = 0 \end{cases}$$

Haz de planos:

$$\alpha(ax + by + cz + d) + \beta(a'x + b'y + c'z + d') = 0, \alpha, \beta \text{ no sim. } 0$$

Debemos notar que $(d_x, d_y, d_z) = (a, b, c) \wedge (a', b', c')$.

9.2.3. Distancias

Sabemos que la definición de *distancia* es la longitud del camino más corto. Veamos qué caminos podemos analizar:

Punto a punto

Dos puntos cualesquiera (ya sea en $\mathbb{R}^2$ o $\mathbb{R}^3$, determinan un vector. La distancia entre ellos es la longitud del vector que generan.

$$dist(P, Q) = ||\overrightarrow{PQ}||$$

Ejemplo 9.17

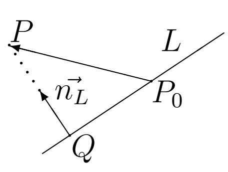
1. En $\mathbb{R}^2$: Sea $P = (1, 1), Q = (3, 5)$, entonces

$$dist(P, Q) = ||((3 - 1), (5 - 1))|| = \sqrt{2^2 + 4^2} = \sqrt{20} = 2\sqrt{5}.$$

2. En $\mathbb{R}^3$: Sea $P' = (1, 1, 2), Q' = (-1, 3, 5)$, entonces

$$dist(P', Q') = ||((-1-1), (3-1), (5-2))|| = \sqrt{(-2)^2 + 2^2 + 3^2} = \sqrt{17}.$$

Punto a recta en el plano



En primer lugar verificamos que $P \notin L$. El método constructivo dice que busquemos la única recta perpendicular a L que pasa por P, luego hallamos Q, el punto de intersección de ambas rectas y la distancia de la recta al punto P es el módulo del vector $\overrightarrow{PQ}$.

Este procedimiento es correcto y además es la única forma de conocer las

coordenadas del punto que realiza la distancia, pero si sólo queremos conocer la longitud podemos hacer una cuenta más sencilla.
Queremos conocer la longitud del vector $\overrightarrow{PQ}$ que es el valor absoluto de la proyección de un vector $\overrightarrow{P_0P}$, para cualquier punto $P_0 \in L$.
Busquemos la fórmula:

1. $L : ax + by + c = 0$, es decir $\vec{n}_L = (a, b)$.
2. $P = (x_P, y_P)$, $P_0 = (x_0, y_0)$ $\overrightarrow{P_0P} = (x_P - x_0, y_P - y_0)$.
3. $P_0 = (x_0, y_0) \in L$, por lo tanto $ax_0 + by_0 + c = 0$, es decir: $-ax_0 - by_0 = c$

$$dist(P, L) = |proy_{\vec{n}_L}\overrightarrow{P_0P}| = \frac{|(\overrightarrow{P_0P}, \vec{n}_L)|}{||\vec{n}_L||}$$

$$dist(P, L) = \frac{|((x_P - x_0, y_P - y_0), (a, b))|}{\sqrt{a^2 + b^2}} = \frac{|a(x_P - x_0) + b(y_P - y_0)|}{\sqrt{a^2 + b^2}} =$$

$$= \frac{|ax_P + by_P - ax_0 - by_0|}{\sqrt{a^2 + b^2}} = \frac{|ax_P + by_P + c|}{\sqrt{a^2 + b^2}}.$$

Ejemplo 9.18 Consideremos la recta $L = 4x - 3y + 2 = 0$ y el punto $P = (1, 1)$. Claramente $P \notin L$ ya que $4 \cdot 1 - 3 \cdot 1 - 26 \neq 0$.
Hagamos en primer lugar el método constructivo:

Buscamos Ł$'\perp L$ que pase por P. La ecuación vectorial de esta recta es: $L' = (1, 1) + \mu(4, -3), \mu \in \mathbb{R}$.

Para buscar el punto de intersección, teniendo una recta en forma implícita y la otra en forma vectorial (o paramétrica) lo más conveniente es reemplazar en la ecuación implícita las expresiones de la ecuación paramétrica y obtener una ecuación en una variable (el parámetro, en este caso: μ).

$$L \cap L' : 4 \cdot (1 + 4\mu) - 3 \cdot (1 - 3\mu) - 26 = -25 + 25\mu = 0$$

De donde $\mu = 1$, y reemplazando μ en L' obtenemos el punto $Q = (5, -2)$.

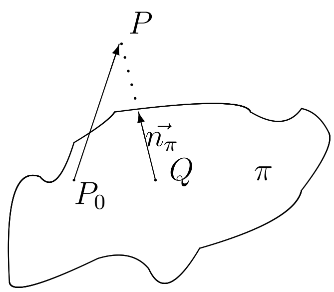
$$dist(P, L) = ||\overrightarrow{PQ}|| = \sqrt{(5 - 1)^2 + (-2 - 1)^2} = \sqrt{25} = 5.$$

Apliquemos la fórmula para simplemente calcular la distancia sin conocer el punto Q:

$$dist(P, L) = \frac{|4 \cdot 1 - 3 \cdot 1 - 26|}{\sqrt{4^2 + 3^2}} = \frac{|-25|}{\sqrt{25}} = 5.$$

Punto a plano en el espacio

El razonamiento que usaremos en esta sección es absolutamente análogo al que usamos en la sección anterior. Imaginen que se pudiera poner un plano justo a la altura de los ojos: se convertiría en una recta y veríamos este procedimiento naturalmente.



En primer lugar verificamos que $P \notin \pi$. El método constructivo dice que busquemos la única recta perpendicular a π que pasa por P, luego hallamos Q, el punto de intersección del plano y la recta y la distancia del punto P al plano π es el módulo del vector $\overrightarrow{PQ}$.

Este procedimiento es correcto y además es la única forma de conocer las coordenadas del punto que realiza la distancia, pero si sólo queremos conocer la longitud podemos hacer una cuenta más sencilla.
Queremos conocer la longitud del vector $\overrightarrow{PQ}$ que es el valor absoluto de la proyección de un vector $\overrightarrow{P_0P}$, para cualquier punto $P_0 \in \pi$.
Busquemos la fórmula:

1. $\pi : ax + by + cz + d = 0$, es decir $\vec{n}_L = (a, b, c)$.
2. $P = (x_P, y_P, z_P)$, $P_0 = (x_0, y_0, z_0)$ $\overrightarrow{P_0P} = (x_P - x_0, y_P - y_0, z_P - z_o)$.
3. $P_0 = (x_0, y_0, z_0) \in \pi$, por lo tanto $ax_0 + by_0 + cz_0 + d = 0$, es decir: $-ax_0 - by_0 - cz_0 = d$

$$dist(P,\pi) = |proy_{\vec{n}_\pi}\overrightarrow{P_0P}| = \frac{|(\overrightarrow{P_0P}, \vec{n}_\pi)|}{||\vec{n}_\pi||}$$

$$dist(P,\pi) = \frac{|((x_P - x_0, y_P - y_0, z - z_0), (a, b, c))|}{\sqrt{a^2 + b^2 + c^2}} =$$

$$= \frac{|a \cdot (x_P - x_0) + b \cdot (y_P - y_0) + c \cdot (z - z_0)|}{\sqrt{a^2 + b^2 + c^2}} =$$

$$= \frac{|ax_P + by_P + c - z_p - ax_0 - by_0 - cz_p|}{\sqrt{a^2 + b^2 + c^2}} = \frac{|ax_P + by_P + cz_p + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

Ejemplo 9.19 Sea $\pi = x - 2.y - 3z + 14 = 0,\ P = (1, -1, 1)$.

Hagamos la construcción:

$L\perp\pi$ en ecuación vectorial es: $(x, y, z) = (1, -1, 1) + \lambda \cdot (1, -2, -3), \lambda \in \mathbb{R}$.

Punto de intersección: Nuevamente reemplazamos en la ecuación de π las expresiones de x, y y z de la ecuación paramétrica de la recta:

$Q = \pi \cap L : (1 + \lambda) - 2.(-1 - 2.\lambda) - 3.(1 - 3.\lambda) = 0$ implica $\lambda = -1$ y el punto $Q = (0, 1, -2)$, de donde

$$dist(P, \pi) = ||\overrightarrow{PQ}|| = \sqrt{(0-1)^2 + (1+1)^2 + (-2-1)^2} = \sqrt{14}.$$

Si aplicamos la fórmula, obtenemos:

$$dist(P, \pi) = \frac{|1 - 2(-1) - 3(1) + 14|}{\sqrt{1^2 + 2^2 + (-3)^2}} = \frac{14}{\sqrt{14}} = \sqrt{14}.$$

Recta a plano en el espacio

Para que exista la distancia entre una recta y un plano en el espacio ambos deben ser paralelos, es decir, el vector normal del plano debe ser perpendicular al director de la recta. En símbolos $(\vec{n}_\pi, \vec{d}_L) = 0$. En caso contrario se intersectan y la distancia es nula.
Tenemos dos opciones:

1. $dist(L, \pi) = dist(L, P_\pi)$, donde P_π es un punto cualquiera del plano π.
2. $dist(L, \pi) = dist(P_L, \pi)$, donde P_L es un punto cualquiera de la recta L.

La primera opción la vimos en el inciso anterior, la segunda opción la veremos un poco más adelante.

Plano a plano en el espacio

Claramente para que exista la distancia ambos planos deben ser paralelos, es decir, sus vectores normales deben ser paralelos. Claramente la distancia entre los planos será la distancia de un punto en un plano al otro.

$$dist(\pi, \pi') = dist(P, \pi') = dist(\pi, P'), \quad \text{donde } P \in \pi,\ P' \in \pi'.$$

Ejemplo 9.20 Sea $\pi : 2x + y - 3z = -1,\ \pi' : -6x - 3y + 9z = 9$

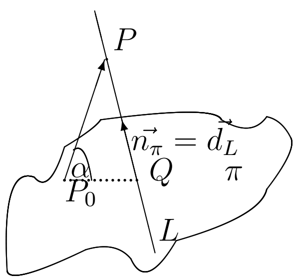
1. $dist(\pi, \pi') = dist(P, \pi')$:
   $P = (1, 0, 1) \in \pi$,

$$\frac{|-6 \cdot 1 - 3 \cdot 0 + 9 \cdot 1 - 9|}{\sqrt{(-6)^2 + 3^2 + 9^2}} = \frac{|6|}{\sqrt{126}} = \frac{2 \cdot 3}{3 \cdot \sqrt{14}} = \frac{2}{\sqrt{14}}$$

2. $dist(\pi, \pi') = dist(\pi, P')$:
   $P' = (-1, 2, 1) \in \pi'$

$$\frac{|2 \cdot (-1) + 1 \cdot 2 - 3 \cdot 1 + 1|}{\sqrt{2^2 + 1^2 + 3^2}} = \frac{|2|}{\sqrt{14}} = \frac{2}{\sqrt{14}}$$

Punto a recta en el espacio



Dada una recta L en el espacio y un punto P que no pertenece a ella, existe un único plano que pasa por el punto y es perpendicular a la recta. Si llamamos Q al punto de intersección del plano y la recta, la distancia de P a L será la distancia de P a Q o el módulo de $\overrightarrow{PQ}$. Podemos ver también que esta longitud es exactamente $||\overrightarrow{P_0P}||.sen\alpha$, para cualquier $P_0 \in L$, donde α es el ángulo entre $\overrightarrow{P_0P}$ y $\vec{d_L}$. Entonces podemos escribir:

$$dist(P, L) = \frac{||\overrightarrow{P_0P} \wedge \vec{d_l}||}{||\vec{d_L}||}$$

Ejemplo 9.21 Sea $L : (1, -2, 3) + \mu.\cdot(3, 3, 0), \mu \in \mathbb{R}$ y $P = (2, 1, 0)$. Hagamos la construcción: el plano π perpendicular a L que pasa por P es $\pi : 3x + 3y - 9 = 0$. Para calcular la intersección nuevamente reemplazamos las ecuaciones de x, y, z en función de μ en la ecuación del plano:

$$3 \cdot (1 + 3\mu) + 3 \cdot (-2 + 3\mu) - 9 = -12 + 18\mu = 0$$

y el punto de intersección es: $Q = (3, 0, 3)$.

$$dist(P, L) = ||\overrightarrow{PQ}|| = ||(1, -1, 3)|| = \sqrt{11}.$$

Aplicando la fórmula:

$$dist(P, L) = \frac{||(2, 1, 0) - (1, -2, 3) \wedge (3, 3, 0)||}{||(3, 3, 0)||} = \frac{\sqrt{198}}{\sqrt{18}} = \frac{\sqrt{18}\sqrt{11}}{\sqrt{18}} = \sqrt{11}.$$

Recta a recta en el espacio

Si vamos a considerar la posición relativa de dos rectas en el plano, sólo pueden ser paralelas o no. Si no son paralelas la distancia es nula. Si lo son tomamos como distancia entre las rectas la distancia entre una de las rectas y un punto cualquiera de la otra.

En el espacio las rectas pueden ser coplanares o no. Si son coplanares estamos en las condiciones de rectas en el plano. Si no lo son entonces se dicen *alabeadas* o *rectas que se cruzan*. Podemos definir como rectas alabeadas a dos rectas no paralelas que jamás se intersectan. Un ejemplo característico de esto es pensar en una letra X con el segmento de orientación positiva en una pared y el de orientación negativa en la pared de enfrente.
Antes de calcular distancias entre rectas alabeadas veamos algunos puntos acerca de las rectas en el espacio.

1. Dos rectas que se intersectan son siempre coplanares
2. Dos rectas paralelas son siempre coplanares
3. Dos rectas son alabeadas si y sólo si no son paralelas ni se intersectan

Veamos algunas justificaciones para estas afirmaciones:

1. Supongamos que las rectas L_1 y L_2 se cortan en el punto P_0. Siempre podemos construir el plano que pasa por el punto P_0 y cuyo vector normal es el producto vectorial de los directores de la recta.

   Ejemplo 9.22 Sean las rectas:

   $$L_1 : (1, 2, 4) + \lambda \cdot (2, 3, 1), \lambda \in \mathbb{R},$$

   $$L_2 : (1, 2, 4) + \mu \cdot (2, -3 - 1), \mu \in \mathbb{R}.$$

   $\vec{d}_{L_1} = (2, 3, 1)$, $\vec{d}_{L_2} = (2, -3, -1)$ por lo tanto son no paralelas y claramente se cortan en el punto $P_0 = (1, 2, 4)$. Construyamos el plano π que las contiene: $\vec{n}_\pi = \vec{d}_{L_1} \wedge \vec{d}_{L_2} = (0, 4, -12)$ Como buscamos una dirección podemos simplificar y considerar el vector: $\vec{n}_\pi = (0, 1, -3)$ el plano es, entonces: $\pi : y - 3z + d = 0$, de $P_0 \in \pi$ obtenemos $\pi : y - 3z + 10 = 0$.

2. Para construir un plano necesitamos tres puntos no alineados. Si dos rectas son paralelas claramente dos puntos en una de ellas y un punto en la otra son tres puntos no alineados. Con los dos puntos de la misma recta generamos el vector director de esa recta (y de la otra también, ya que son paralelos) y con uno de esos dos puntos y el tercero en la otra recta generamos un vector que no es paralelo y nos servirá para construir el vector normal del plano. Veamos un ejemplo:

Ejemplo 9.23 Sean las rectas:

$$L_1 : (1,2,1) + \lambda \cdot (2,3,1), \lambda \in \mathbb{R},$$

$$L_2 : (-1,2,4) + \mu \cdot (2,3,1), \mu \in \mathbb{R}.$$

Consideremos simplemente un vector director y el vector formado por un punto en cada una: $\vec{d}_{L_1} = (2,3,1), \overrightarrow{P_1P_2} = (-1,2,4) - (1,2,1) = (-2,0,3)$.
$\vec{n}_\pi = \vec{d}_{L_1} \wedge \overrightarrow{P_1P_2} = (-9,8,-6)$. Hacemo pasar ahora al plano por P_1 o por P_2 y obtenemos: $\pi : -9x + 8y - 6z - 1 = 0$

3. Si dos rectas L_1 y L_2 no se intersectan, tomando cualquier par de puntos $P_1 \in L_1$ y $P_2 \in L_2$ generamos el vector $\overrightarrow{P_1P_2} \neq \vec{0}$, además como L_1 y L_2 no son paralelas $\vec{d}_{L_1} \wedge \vec{d}_{L_2} \neq \vec{0}$, y también $(\vec{d}_{L_1} \wedge \vec{d}_{L_2}, \overrightarrow{P_1P_2}) \neq 0$ ya que los vectores son no coplanares.

Ejemplo 9.24 Dadas las rectas

$$L_1 : (1,2,4) + \lambda(0,2,3), \lambda \in \mathbb{R},$$

$$L_2 : (1,-1,1) + \mu(1,2,1), \mu \in \mathbb{R},$$

los vectores directores son $\vec{d}_{L_1} = (0,2,3), \vec{d}_{L_2} = (1,2,1)$ y en consecuencia no son paralelas.
Para ver que no se cortan simplemente podemos considerar el sistema de tres ecuaciones con dos incógnitas que se produce al igualar las x, y, z de ambas ecuaciones:

$$\begin{cases} 1 + 0\lambda = 1 + \mu \\ 2 + 2\lambda = -1 + 2\mu \\ 4 + 3\lambda = 1 + \mu \end{cases} \qquad \begin{cases} 0 = \mu \\ 2\lambda - 2\mu = -3 \\ 3\lambda - \mu = -3 \end{cases}$$

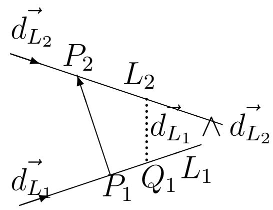
Vemos que este sistema es incompatible y, por lo tanto, las rectas no se cortan, ni son paralelas; son alabeadas.

Observación 9.7 Si en el ejemplo 9.24 calculamos el producto mixto entre los directores de las rectas y un vector formado por un punto en cada una de ellas, vemos que los tres vectores no son coplanares:

$$(\vec{d}_{L_1} \wedge \vec{d}_{L_2}, \overrightarrow{P_1P_2}) = \begin{vmatrix} 0 & 2 & 3 \\ 1 & 2 & 1 \\ 0 & -3 & -3 \end{vmatrix} = -3 \neq 0.$$

Si bien este es también un método utilizado para verificar que las rectas son alabeadas, consideramos que resulta poco claro y bastante artificial, ya que ver que no son paralelas y no se cortan es mucho más natural y refleja directamente la definición de alabeadas.

Sólo nos queda calcular la distancia entre dos rectas alabeadas:



Dadas dos rectas alabeadas L_1 y L_2, siempre podemos encontrar en el haz de planos de cada una, un par de planos paralelos π_1 que contenga a L_1 y π_2 que contenga a L_2. La distancia entre las rectas será, entonces, la distancia entre los planos. Estará dada en la dirección perpendicular a ambas rectas. Para hallar los puntos que realizan la distancia la construcción es la siguiente:

1. Calculamos $\vec{d}_{L_1} \wedge \vec{d}_{L_2} = \vec{d}_{L'}$
2. construimos la recta L' con director $\vec{d}_{L'}$ que pasa por cualquier punto Q_1 de L_1
3. como L' y L_1 se cortan en Q_1 buscamos el plano π_1 que contiene a ambas.
   $\vec{n}_{\pi_1} = \vec{d}_{L_1} \wedge \vec{d}_{L'}$ y pasa por Q_1.
4. π_1 y L_2 no pueden ser paralelos, entonces existe un punto de intersección, sea P_2
5. Por P_2 trazamos una recta L paralela a L'. Esta recta es coplanar con L_1 y no es paralela a ella, por lo tanto se intersectan en un punto P_1.
6. $dist(L_1, L_2) = ||\overrightarrow{P_1P_2}||$

O bien simplemente pensamos que la distancia es la longitud de la proyección de cualquier vector $\overrightarrow{PQ}$, con $P \in L_1, Q \in L_2$ en la dirección de $\vec{d}_{L_1} \wedge \vec{d}_{L_2}$, es decir:

$$dist(L_1, L_2) = \frac{|(\vec{d}_{L_1} \wedge \vec{d}_{L_2}, \overrightarrow{PQ})|}{||\vec{d}_{L_1} \wedge \vec{d}_{L_2}||}, P \in L_1, Q \in L_2$$

Ejemplo 9.25 Consideremos las rectas:

$$L_1 : (-1, 2, 0) + \lambda \cdot (4, -3, -5), \lambda \in \mathbb{R},$$

$$L_2 : (-2, 3, -3) + \mu \cdot (-2, 1, 2), \mu \in \mathbb{R}.)$$

Sigamos los pasos indicados en la construcción:

1. $\vec{d}_{L_1} \wedge \vec{d}_{L_2} = \vec{d}_{L'} = (-1, 2, -2)$.
2. $L' : (3, -1, -5) + \kappa.(-1, 2, -2), \kappa \in \mathbb{R}$.
3. $\vec{n}_{\pi_1} = \vec{d}_{L_1} \wedge \vec{d}_{L'} = (4, -3, -5) \wedge (-1, 2, -2) = (16, 13, 5)$

y pasa por $(-1, 2, 0)$, $\pi_1 : 16x + 13y + 5z - 10 = 0$.

4. $P_2 = \pi_1 \cap L_2 = (2, 1, -7)$, ya que
   $16(-2 - 2\mu) + 13(3 + \mu) + 5(-3 + 2\mu) - 10 = 0$ se verifica con $\mu = -2$.
5. $L : (2, 1, -7) + \eta \cdot (-1, 2, -2), \eta \in \mathbb{R}$.
6. $P_1 = L \cap L_1 = (3, -1, -5)$.
7. $dist(L_1, L_2) = ||\overrightarrow{P_1P_2}|| = ||(-1, 2, -2)|| = \sqrt{1 + 4 + 4} = 3$

Si aplicamos la fórmula usando vectores obtenemos:

$$dist(L_1, L_2) = \frac{|(\vec{d}_{L_1} \wedge \vec{d}_{L_2}, \overrightarrow{PQ})|}{||\vec{d}_{L_1} \wedge \vec{d}_{L_2}||} = \frac{|(-1, 2, -2), (-1, 1, -3)|}{\sqrt{(-1)^2 + 2^2 + (-2)^2}} = \frac{9}{\sqrt{9}} = 3.$$

9.2.4. Ángulos

En el plano sólo podemos considerar ángulos entre rectas. En el espacio debemos pensar en ángulos entre rectas, entre planos o entre una recta y un plano. Veámoslo por partes:

Entre dos rectas

Ya sea en el plano o en el espacio el ángulo entre dos rectas es el ángulo entre sus vectores directores. No hay ningún problema en tanto pensemos en rectas coplanares, pero ¿y si son rectas que se cruzan pero no se cortan? (Imaginemos un reflector que alumbra desde la izquierda, arriba y otro que alumbre desde la derecha, abajo, en forma paralela). Para el caso de las rectas alabeadas no se forma un ángulo según la definición estricta, pero como siempre podemos encontrar planos paralelos que las contengan consideramos el ángulo que se forma en uno de esos planos con la proyección sobre dicho plano de la otra recta. Como siempre hacemos cuentas con vectores libres, a efectos del cálculo no hay ninguna diferencia. en consecuencia:

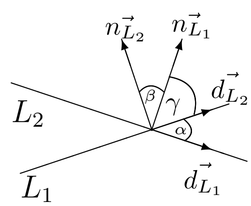
$$ang(L_1, L_2) = ang(\vec{d}_{L_1}, \vec{d}_{L_2})$$

Ejemplo 9.26 Haremos un ejemplo en el plano y otro en el espacio

1. $L_1 : 2x + y - 1 = 0, L_2 : 3x + 5y = 0$
   $\vec{d}_{L_1} = (1, -2), \vec{d}_{L_2} = (5, -3)$,
   $$cos\, \alpha = \frac{((1, -2), (5, -3))}{||(1, -2)|| \cdot ||(5, -3)||} = \frac{11}{\sqrt{170}}$$

2. $L_1 : (1,1,1) + \lambda(2,0,3), \lambda \in \mathbb{R}, L_2 : (0,0,3) + \mu(2,1,1), \mu \in \mathbb{R}$
   $\vec{d}_{L_1} = (2,0,3), \vec{d}_{L_2} = (2,1,1),$
$$cos\,\alpha = \frac{((2,0,3),(2,1,1))}{||(2,0,3)|| \cdot ||(2,1,1)||} = \frac{7}{\sqrt{78}}$$

En verdad en el plano hemos usado los directores de las rectas, pero sabemos que dada una dirección existe una única perpendiclar a la misma y podríamos haber usado los vectores normales a las rectas. En efecto:



Analicemos el gráfico: Hemos trazado las rectas L_1 y L_2 y en rojo hemos trazado las direcciones perpendiculares a L_1 que llamamos n_{L_1} y a L_2 que llamamos n_{L_2}.

$$ang(L_1, L_2) = \alpha, \;\; ang(\vec{n_{L_1}}, \vec{n_{L_2}}) = \beta$$

$$ang(L_1, \vec{n_{L_1}}) = \frac{\pi}{2} = ang(L_2, \vec{n_{L_2}}) =$$

$$\alpha + \gamma = \beta + \gamma, \text{ en consecuencia } \alpha = \beta.$$

Entre dos planos

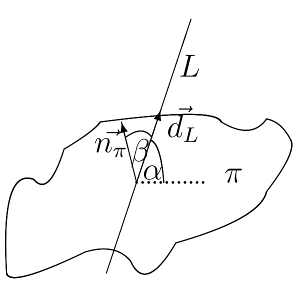
Al finalizar la sección anterior hemos demostrado que el ángulo entre las rectas y las direcciones perpendiculares a ellas son iguales. El mismo razonamiento usamos ahora y decimos:

$$ang(\pi_1, \pi_2) = ang(\vec{n}_{\pi_1}, \vec{n}_{\pi_2})$$

Ejemplo 9.27 consideremos los planos $\pi_1 : 4x + 3z = 1, \pi_2 : x - y = 3$.
$\vec{n}_{\pi_1} = (4,0,3), \vec{n}_{\pi_2} = (1,-1,0)$.

$$cos\,\alpha = \frac{((4,0,3),(1,-1,0))}{||(2,0,3)|| \cdot ||(1,-1,0)||} = \frac{4}{5\sqrt{2}} = \frac{2\sqrt{2}}{5}.$$

Entre recta y plano



Analicemos el gráfico: Queremos calcular el ángulo entre la recta y el plano, es decir, el ángulo α. Conocemos los vectores: $\vec{d}_L$ y $\vec{n}_\pi$ el ángulo entre ellos es β. Como el ángulo entre el plano y su normal es de $\pi/2$ resulta:

$$ang(\pi, L) = \frac{\pi}{2} - ang(\vec{n}_\pi, \vec{d}_L).$$

9.3. Ejercicios propuestos

9.3.1. Vectores libres

Ejercicio 9.1 Graficar tres vectores en el espacio, sean $\vec{u}$, $\vec{v}$, $\vec{w}$. Hallar $\vec{u}+\vec{v}$, $\vec{u}-\vec{v}$, $\vec{u}+\vec{v}+\vec{w}$, $\frac{1}{2}\cdot\vec{u}+\frac{1}{2}\vec{v}$, $\frac{1}{2}\vec{u}+\frac{1}{2}\vec{v}+\frac{1}{2}\vec{w}$.

Ejercicio 9.2 (®) Demostrar que si A, B y C son tres puntos no alineados, el punto medio del segmento $\overline{AB}$ es el extremo del vector $\frac{1}{2}\cdot\overrightarrow{CA}+\frac{1}{2}\cdot\overrightarrow{CB}$. ¿Vale esta igualdad si los puntos están alineados?

Ejercicio 9.3 Dados los puntos $A:(-1,5,-2)$, $B:(2,2,-1)$ y $C:(2,-1,0)$ hallar las componentes de $\overrightarrow{AB}$ y $\overrightarrow{BA}$. Dado un vector $\vec{v}$ de igual intensidad, dirección y sentido a $\overrightarrow{BA}$, si se ubica con origen en C, hallar su extremo. Y si se ubica con extremo en C, hallar su origen.

Ejercicio 9.4 Dados los puntos del ejercicio 9.3, verificar el resultado del ejercicio 9.2.

9.3.2. Proyecciones ortogonales - producto escalar

Ejercicio 9.5 (®) Dados dos vectores $\vec{u}$ y $\vec{v}$ si $\theta = ang(\vec{u},\vec{v})$, con $0\leq\theta\leq\pi$, escribir en los espacios $<$, $>$ o $=$, según corresponda, justificando la respuesta.

1. Si $\theta<\pi/2$, entonces $proy_{\vec{v}}\vec{u}\cdots 0$
2. Si $\theta=\pi/2$, entonces $proy_{\vec{v}}\vec{u}\cdots 0$
3. Si $\theta>\pi/2$, entonces $proy_{\vec{v}}\vec{u}\cdots 0$

Ejercicio 9.6 Sean $\vec{u} = (-1, 2, 2)$, $\vec{v} = (3, -1, 3)$, $\vec{w} = (3, -1, -2)$. Hallar:

1. $proy_{\vec{w}}\vec{u} + proy_{\vec{w}}\vec{v}$
2. $proy_{\vec{w}}(\vec{u} + \vec{v})$

Ejercicio 9.7 Ley del paralelogramo:

1. © Demostrar que la suma de los cuadrados de las longitudes de las diagonales de un paralelogramo es igual al doble de la suma de los cuadrados de las longitudes de dos lados consecutivos.
2. Dados dos vectores $\vec{u}$ y $\vec{v}$ tales que $||\vec{u}|| = 7$,$||\vec{u} + \vec{v}|| = 12$ y $||\vec{u} - \vec{v}|| = 5$, determinar $||\vec{v}||$. Sug.: Utilizar el resultado anterior.

Ejercicio 9.8 Ortogonalidad:

1. © Sea $\overrightarrow{proy_{\vec{u}}\vec{v}} = \dfrac{(\vec{u}\,,\,\vec{v})}{||\vec{u}||} \cdot \breve{u} = \dfrac{(\vec{u}\,,\,\vec{v})}{||\vec{u}||} \cdot \dfrac{\vec{u}}{||\vec{u}||} = \dfrac{(\vec{u}\,,\,\vec{v})}{||\vec{u}||^2} \cdot \vec{u}.$

   Demostrar que $\vec{v} - \overrightarrow{proy_{\vec{u}}\vec{v}}$ es ortogonal a $\vec{u}$. Interpretar geométricamente.
2. (♣) Dar condiciones para $\vec{u}$ y $\vec{v}$ para que $\vec{u} + \vec{v}$ sea perpendicular a $\vec{u} - \vec{v}$.

Ejercicio 9.9 Sea $\vec{u} = (2, 1)$. Hallar $\vec{v}$ tal que:

1. tenga igual dirección, sentido contrario y su módulo sea 3. ¿Es único?
2. perpendicular a $\vec{u}$ de igual módulo. ¿Es único?
3. sea un versor que forme un ángulo de $\pi/3$ con $\vec{v}$. ¿Es único?

Ejercicio 9.10 Demostrar que si el vector $\vec{w}$ es perpendicular a $\vec{u}$ y $\vec{v}$, entonces es perpendicular a cualquier combinación lineal entre ellos, es decir, es perpendicular a $\lambda_1\vec{u} + \lambda_2\vec{v}$, cualesquiera que sean $\lambda_1, \lambda_2 \in \mathbb{R}$.

Ejercicio 9.11 Idem al ejercicio 9.9 con $\vec{u} = (3, -1, 2)$.

Ejercicio 9.12 Sabiendo que A, B y C son puntos de $\mathbb{E}^n$ que satisfacen las condiciones: $d(A, B) = d(B, C) = 1$, $ang(\overrightarrow{AB}, \overrightarrow{BC}) = \pi/3$, calcular el producto escalar entre los vectores $\vec{v} = 3 \cdot \overrightarrow{AB} + 2 \cdot \overrightarrow{BC}$ y $\vec{w} = (-2) \cdot \overrightarrow{BA} + 2 \cdot \overrightarrow{CB}$.

Ejercicio 9.13 Sea $\vec{v} = (3, 0, -4)$, hallar $||\vec{v}||$, $\breve{v}$ y los cosenos directores.

Ejercicio 9.14 Hallar las componentes de un vector $\vec{w} \in \mathbb{R}^3$ tal que: $||\vec{w}|| = 2$ y forme con $\breve{e}_1$ y $\breve{e}_2$, respectivamente, ángulos de $\pi/3$ y $-\pi/3$.

9.3.3. Producto vectorial - doble producto mixto

Ejercicio 9.15 Dados $\vec{u} = (-1, 2, -2)$, $\vec{v} = (2, 0, -3)$ y $\vec{w} = (5, -1, 1)$, calcular:

1. $\vec{u} \wedge \vec{v}$, $\vec{v} \wedge \vec{u}$,
2. $\lambda \cdot (\vec{u} \wedge \vec{v})$, $(\lambda \cdot \vec{u}) \wedge \vec{v}$ $\vec{u} \wedge (\lambda \cdot \vec{v})$
3. $\vec{u} \wedge (\vec{v} + \vec{w}) = (\vec{u} \wedge \vec{v}) + (\vec{u} \wedge \vec{w})$

Ejercicio 9.16 (✠) Probar que en $\mathbb{R}^3$, para que dos vectores no nulos $\vec{u}$ y $\vec{v}$ sean paralelos es condición necesaria y suficiente que $\vec{u} \wedge \vec{v} = 0$.

Ejercicio 9.17 Hallar el área del triángulo que tiene por vértices los puntos $A = (-1, 2, 5)$, $B = (1, 3, -2)$, $C = (3, 3, 6)$.

Ejercicio 9.18 Dados $\vec{u} = (-1, 2, -2)$, $\vec{v} = (2, 0, -3)$ y $\vec{w} = (5, -1, 1)$, calcular $(\vec{u} \wedge \vec{v}, \vec{w})$.

Ejercicio 9.19 (♣) Hallar el tercer vector que genera un paralelepípedo cuya base está determinada por los vectores $\vec{u} = \langle -1, 1, 2 \rangle$, $\vec{v} = \langle 1, 2, 3 \rangle$ y su volumen es de 5 unidades cúbicas, sabiendo que es paralelo a $\breve{e}_1 + \breve{e}_2 + \breve{e}_3$.

9.3.4. Aplicaciones a la física

Ejercicio 9.20 Un hombre ejerce una fuerza horizontal de $25\overrightarrow{Kg}$ sobre un embalaje de tablas, conforme lo empuja sobre una rampa que tiene $10m$ de largo y una inclinación de 20^o sobre la horizontal. Calcular el trabajo realizado sobre la caja.

Ejercicio 9.21 Una tuerca se sujeta al aplicar una fuerza de $40N$ (N: Newton, unidad de fuerza) a una llave de $0,25m$ de longitud, como se muestra en la figura. Calcular la magnitud del momento de la fuerza respecto del centro de la tuerca.

9.3.5. Rectas en el espacio

Ejercicio 9.22 Representar los puntos: $P : (5, 2, 3)$, $Q : (3, -2, 5)$, $R : (0, 0, 4)$ y $S : (0, 6, 3)$, y verificar que no son coplanares.

1. Dar la ecuación de los planos π_1 determinado por los puntos P, Q, R, π_2 por P, Q, S y π_3 por R, Q, S.
2. Dar las ecuaciones de las rectas que pasan por $\overline{PQ}$ y $\overline{QS}$ en forma: vectorial, paramétrica, ecuaciones simétricas-si existe- e intersección de planos. Hallar el haz de planos que contiene a cada una de ellas.

Ejercicio 9.23 (♣) Hallar el simétrico del punto $(-2, 3, 0)$ respecto del punto $(1, -1, 2)$.

Ejercicio 9.24 Hallar a y b para que los puntos $(1, 2, -1)$, $(3, 0, -2)$ y $(4, a, b)$ estén alineados.

Ejercicio 9.25 Dar las ecuaciones en forma paramétrica y simétricas de una recta L tal que:

1. pase por $(2, 2, 1)$ y sea paralela a $\vec{v} : (3, -1 - 4)$.
2. pase por $(1, 3, 2)$ y $(3, 3, 1)$
3. pase por $(3, 4, 6)$ y es perpendicular al plano $\pi : 3x + 5y - z = 6$
4. pase por $(1, -1, 3)$ y sea paralela al vector $\vec{w} = \vec{u} \wedge \vec{v}$, donde $\vec{u} : (1, 3, 4)$ y $\vec{v} : (3, -1, -1)$.

Ejercicio 9.26 Determinar los valores de m y n tales que $L_1 \parallel L_2$, siendo:

$$L_1 : \begin{cases} x = 5 + 4\lambda \\ y = 3 + \lambda \\ z = -\lambda \end{cases}, \ \lambda \in \mathbb{R} \text{ y } L_2 : \frac{x}{m} = \frac{y-1}{3} = \frac{z+3}{n}.$$

Ejercicio 9.27 ($\diamond$) Hallar posición relativa (paralelas, incidentes o alabeadas) de los siguientes pares de rectas y expresarlas como intersección de planos y por sus ecuaciones simétricas.

1. $L_1 : \begin{cases} x = 1 - 5\lambda \\ y = 2 + 3\lambda \\ z = -5 + \lambda \end{cases}, \ \lambda \in \mathbb{R} \quad L_2 : \begin{cases} x = 1 \\ y = 1 \\ z = \mu \end{cases}, \ \mu \in \mathbb{R}$
2. $L_1 : \begin{cases} x = 3 + 2\lambda \\ y = 1 - \lambda \\ z = 5 \end{cases}, \ \lambda \in \mathbb{R} \quad L_2 : \begin{cases} x = 1 - 6\mu \\ y = 3 + 3\mu \\ z = 5 \end{cases}, \ \mu \in \mathbb{R}$
3. $L_1 : \begin{cases} x = 3 + \lambda \\ y = -2 - \lambda \\ z = 1 \end{cases}, \ \lambda \in \mathbb{R} \quad L_2 : \begin{cases} x = -2\mu \\ y = 3 + 2\mu \\ z = -1 \end{cases}, \ \mu \in \mathbb{R}$

4. $L_1 : \begin{cases} x = -4 + 2\lambda \\ y = 4 - \lambda \\ z = -1 - 2\lambda \end{cases}, \lambda \in \mathbb{R} \quad L_2 : \begin{cases} x = -5 + 4\mu \\ y = 5 - 3\mu \\ z = 5 - 5\mu \end{cases}, \mu \in \mathbb{R}$

Ejercicio 9.28 (♣) ¿Se puede construir un triángulo con dos de sus lados en las rectas

$$L_1 : \frac{x-1}{2} = y = z + 1 \text{ y } L_2 : \begin{cases} x = 2\lambda \\ y = -1 + \lambda \\ z = \lambda \end{cases}, \lambda \in \mathbb{R}?$$

9.3.6. Rectas y planos en el espacio

Ejercicio 9.29 (◇) Hallar las ecuaciones paramétricas y cartesiana de un plano que pase por $(1, 7, -2)$, $(4, 5, 0)$ y $(6, 3, 8)$. Dar otros dos puntos en el plano. Hallar n tal que $(1, n, 5)$ pertenezca al plano.

Ejercicio 9.30 Verificar que el plano π y la recta L son paralelos y calcular la distancia $d(L, \pi)$. Justificar vectorialmente la fórmula.

$$\pi : 2x - y + 3z - 8 = 0 \qquad L : \begin{cases} x = 2 + 3\lambda \\ y = -1 + 3\lambda \\ z = -\lambda \end{cases}, \lambda \in \mathbb{R}.$$

Ejercicio 9.31 (♣) Calcular m y n para que los planos $\pi_1 : m\,x + y - 3\,z - 1 = 0$ y $\pi_2 : 2\,x + n\,y - z - 3 = 0$ sean paralelos. ¿Pueden ser coincidentes?

Ejercicio 9.32 Dar la ecuación del plano que contiene al punto $(2, 1, 2)$ y a la recta $x - 2 = \dfrac{y-3}{-1} = \dfrac{z-4}{-3}$.

Ejercicio 9.33 Verificar que las rectas $L_1 = \begin{cases} x - 2z = 5 \\ x - 2y = 11 \end{cases}$ y $L_2 = \dfrac{x-1}{2} = y = z - 2$ son paralelas y hallar el plano que las contiene.

Ejercicio 9.34 Hallar la ecuación del plano que pasa por los puntos $(1, 3, 2)$ y $(-2, 5, 0)$ y es paralelo a la recta $L : \begin{cases} x = 3 - \lambda \\ y = 2 + \lambda \\ z = -2 - 3\lambda \end{cases}, \lambda \in \mathbb{R}.$

Ejercicio 9.35 (♣) Hallar m tal que los puntos $(m, 0, 1)$, $(0, 1, 2)$, $(1, 2, 3)$, $(7, 2, 1)$ sean coplanares. Dar la ecuación del plano que los contiene.

Ejercicio 9.36 (♣) Dados los planos $\pi_1 : mx + 2y - 3z - 1 = 0$ y $\pi_2 : 2x - 4y + 6z + 5 = 0$ hallar m tal que $\pi_1 \parallel \pi_2$ ó $\pi_1 \perp \pi_2$.

Ejercicio 9.37 ($\diamond$) Dados $L : \begin{cases} x - 2z + 3 = 0 \\ y - z - 4 = 0 \end{cases}$ y $\pi : x + 2y + 3z - 1 = 0$, hallar la ecuación de una recta $L^{'}$ contenida en el plano π que pase por el punto $P : (2, 1, -1)$, y sea perpendicular a L.

Ejercicio 9.38 ($\diamond$) Hallar la ecuación de la recta que pasa por el punto $(1, 2, 3)$ y es perpendicular al plano que pasa por el origen y los puntos $(1, 1, 1)$, $(1, 2, 1)$.

Ejercicio 9.39 ($\diamond$) Decidir si el plano $x + y + z + 2 = 0$ pertenece al haz de planos de arista

$$L \begin{cases} x + 2\,y - z - 1 = 0 \\ x - 3\,y + 4\,z + 2 = 0 \end{cases}$$

Ejercicio 9.40 ($\diamond$) Determinar el ángulo que forman las rectas

$$L_1 : \frac{x-2}{2} = \frac{y+5}{1} = \frac{z-4}{3} \text{ y } L_2 : \frac{x+1}{6} = \frac{y+7}{-4} = \frac{z}{2},$$

averiguando previamente su posición relativa.

Ejercicio 9.41 Determinar en cada caso el ángulo que forman la recta L y el plano π, siendo:

1. $L : \dfrac{x+1}{6} = \dfrac{y+7}{-4} = \dfrac{z}{2}, \qquad \pi : 3\,x - 2\,y + z = 0,$
2. $L : \dfrac{x+1}{6} = \dfrac{y+7}{-4} = \dfrac{z}{2}, \qquad \pi : x + y - z + 8,$
3. $L : \dfrac{x+1}{2} = \dfrac{y+7}{-2} = \dfrac{z}{\sqrt{24}}, \qquad \pi : x + y - z + 8,$

Ejercicio 9.42 Dar las ecuaciones de dos rectas alabeadas L_1 y L_1 que pasen respectivamente por los puntos $P_1 : (2, 1, 1)$ y $P_2 : (1, 2, -1)$.

Ejercicio 9.43 Dadas las rectas

$$L_1 \begin{cases} x = 2 + \lambda \\ y = 3 + 3\,\lambda \\ z = 4 + 4\,\lambda \end{cases}, \ \lambda \in \mathbb{R} \text{ y } L_2 \begin{cases} x = 1 - \mu \\ y = -2 - \mu \\ z = -3\,\mu \end{cases}, \ \mu \in \mathbb{R},$$

determinar su posición relativa y hallar, si es posible, la distancia entre ellas.

Ejercicio 9.44 Sea L_1 la recta con ecuación vectorial $L_1 : (3, 0, -4) + \lambda\,(1, -1, 0)$,$\lambda \in \mathbb{R}$. Hallar una recta L_2 alabeada con L_1 tal que $d(L_1, L_2) = 2$.

Capítulo 10

Espacios vectoriales

Espacios vectoriales. Subespacios. Ejemplos. Subespacio generado. Dependencia lineal. Bases. Bases ortonormales. Dimensión. Cambio de base. Cambio de coordenadas. Transformaciones lineales. Matriz asociada a una transformación lineal.

A lo largo de este curso hemos visto conjuntos de elementos distintos en los que definimos operaciones con propiedades similares. Pensemos en vectores, matrices o polinomios, en todos ellos definimos una operación suma y en todos los casos esta operación es:

1. asociativa,
2. conmutativa,
3. tiene elemento neutro,
4. dado cualquier elemento existe el simétrico.

En todos los casos anteriores los coeficientes pertenecen a un cuerpo y dado un k en el cuerpo definimos una multiplicación por escalar con las propiedades:

1. el producto escalar distribuye con respecto a la suma de elementos,
2. si multiplicamos dos escalares y luego multiplicamos un elemento del conjunto es lo mismo que multiplicar el elemento del conjunto por cada uno de los escalares a la vez,
3. multiplicar por la unidad deja invariante el elemento.

Nuestro objetivo ahora es dar una visión más amplia y ubicar todos estos casos dentro de una definición más general.

10.1. Espacios Vectoriales

Definición 10.1 Dado un cuerpo $\mathbb{K}$, un $\mathbb{K}$-*espacio vectorial* es:

- un conjunto no vacío V: los elementos de este conjunto los llamaremos vectores, y los escribiremos $\vec{v}$
- una operación interna denominada *suma*: $+ : V \times V \to V$
  (se llama interna porque tomamos dos vectores, los sumamos y tenemos un vector, todo queda "adentro")
- una operación externa denominada *producto por escalar*. $: \mathbb{K} \times V \to V$
  (se llama externa porque un elemento externo al conjunto de vectores actúa sobre el vector convirtiéndolo en otro)

satisfaciendo las siguientes propiedades para todo $k \in \mathbb{K}, \vec{v}, \vec{v}_1, \vec{v}_2, \vec{v}_3 \in V$:

$V_1 :\ (\vec{v}_1 + \vec{v}_2) + \vec{v}_3 = \vec{v}_1 + (\vec{v}_2 + \vec{v}_3)$ (propiedad asociativa de la +)

$V_2 :\ \vec{v}_1 + \vec{v}_2 = \vec{v}_2 + \vec{v}_1$ (propiedad conmutativa de la +)

$V_3 :$ Existe $\vec{0}$ tal que $\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v}$ (neutro de la +)

$V_4 :$ Dado $\vec{v}$ existe $-\vec{v}$ tal que $\vec{v} + (-\vec{v}) = (-\vec{v}) + \vec{v} = \vec{0}$ (simétrico de la +)

$V_5 :\ k.(v_1 + v_2) = k.\vec{v}_1 + k.\vec{v}_2$ (distributividad de . con +)

$V_6 :\ (k_1 + k_2).\vec{v} = k_1.\vec{v} + k_2.\vec{v}$ (distributividad de + en $\mathbb{K}$ con .)

$V_7 :\ (k_1.k_2).\vec{v} = k_1.(k_2.\vec{v})$

$V_8 :\ 1.\vec{v} = \vec{v}$ (ley de conservación de la identidad)

Dado que para tener un espacio vectorial necesitamos un cuerpo, un conjunto no vacío y dos operaciones, el modo correcto de mencionarlo y notarlo es: *el* $\mathbb{K}$-*espacio vectorial* $(V, +, .)$. Como un abuso más de notación y dado que, a menos que se especifique en el momento, hablaremos siempre de $\mathbb{R}$ espacios vectoriales con las operaciones habituales mencionaremos simplemente "el espacio vectorial V" lo cual, como acabo de aclarar, es absolutamente incorrecto.

Ejemplo 10.1 Claramente, si construimos la definición de espacio vectorial viendo las propiedades que tienen en común matrices, polinomios y vectores, todos ellos serán espacios vectoriales. Escribámoslo más precisamente:

1. $\mathbb{C}$ es $\mathbb{R}$-espacio vectorial.
   Sabemos que la suma y el producto de de números complejos satisfacen las propiedades V_1 a V_8 y dado que los números reales también son complejos fácilmente se trata de un $\mathbb{R}$-espacio vectorial.

2. $\mathbb{R}$ no es un $\mathbb{C}$-espacio vectorial.
   Si bien las propiedades V_1 a V_8 se satisfacen, no todo número complejo es real, entonces la operación externa ya no es operación. Más precisamente: si tomo un número complejo no real y lo multiplico por un número real obtengo como resultado un número complejo no real, "caigo afuera" del conjunto que estoy considerando. En estos casos (y cada vez que queremos mostrar que algo no es cierto) mostramos un contraejemplo para afirmar que $(\mathbb{R}, +, .)$ no es $\mathbb{C}$-espacio vectorial.:
   $i \cdot 3 = 3\,i \notin \mathbb{R}$

3. $(M_{2\times 5}(\mathbb{R}), +, .)$ es $\mathbb{R}$-espacio vectorial.

4. $(\mathbb{P}_4(\mathbb{R}), +, .)$ es $\mathbb{R}$-espacio vectorial. Recordemos que $\mathbb{P}_4(\mathbb{R})$ es el conjunto de los polinomios de grado menor o igual que cuatro, a coeficientes reales. Con un razonamiento similar al inciso 2 podemos ver que $(\mathbb{P}_4(\mathbb{R}), +, .)$ no es $\mathbb{C}$-espacio vectorial y $(\mathbb{P}_4(\mathbb{Q}), +, .)$ no es $\mathbb{R}$-espacio vectorial.

5. Construyamos algo diferente: Consideremos $V = \mathbb{R}^3$ en donde definimos nuevas operaciones. Las vamos a notar con otro símbolos para no confundirnos con las operaciones habituales:

   $\bigoplus$: la operación suma interna:

   $$(x, y, z) \bigoplus (x', y', z') = (y + y', x + x', z + z')$$

   $\bigodot$: la operación producto externo:

   $$k \bigodot (x, y, z) = (k.x, k.y, z)$$

   Analicemos si $(\mathbb{R}^3, \bigoplus, \bigodot)$ es o no $\mathbb{R}$-espacio vectorial:
   Ante todo verifiquemos que las operaciones son realmente operaciones:
   Si tomo dos ternas de números reales y hago la cuenta que me propone $\bigoplus$ ¿obtengo una terna de números reales? La respuesta es AFIRMATIVA. Avanzamos.
   Si tomo una terna de números reales, otro número real k y hago la cuenta que propone $\bigodot$ ¿obtengo una terna de números reales? La respuesta es AFIRMATIVA. Avanzamos.

   V_1 : $(\vec{v}_1 + \vec{v}_2) + \vec{v}_3 = \vec{v}_1 + (\vec{v}_2 + \vec{v}_3)$ (propiedad asociativa de la $+$)

   $((x, y, z) \bigoplus (x', y', z')) \bigoplus (x'', y'', z'') =$ (definición de $\bigoplus$)

   $= (y + y', x + x', z + z') \bigoplus (x'', y'', z'') =$ (definición de $\bigoplus$)

   $= (y'' + (y + y'), x'' + (x + x'), (z + z') + z'')) =$ (asoc. y conmut.

de $\mathbb{R}$)

$= ((y'' + y') + y\,,\ (x'' + x') + x\,,\ z + (z' + z'')) =$(definición de $\oplus$)

$= (x, y, z) \bigoplus (y'' + y')\,,\ (x'' + x')\,,\ (z' + z'')) =$ (definición de $\oplus$)

$= (x, y, z) \bigoplus ((x', y', z') \bigoplus (x'', y'', z''))$.

V_2 : $\vec{v}_1 + \vec{v}_2 = \vec{v}_2 + \vec{v}_1$ (propiedad conmutativa de la +)

$(x, y, z) \bigoplus (x', y', z') = (y + y', x + x', z + z') =$ (definición de $\bigoplus$)

$= (y' + y, x' + x, z + z') =$ (conmutativa de $\mathbb{R}$)

$= (x', y', z') \bigoplus (x, y, z)$. (definición de $\oplus$)

V_3 : Existe $\vec{0}$ tal que $\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v}$) (neutro de la +)

Buscamos a un $(0_x, 0_y, 0_z)$ que operado con (x, y, z) lo deje invariante, es decir, buscamos los elementos $0_x, 0_y, 0_z$ tales que:
$(x, y, z) \bigoplus (0_x, 0_y, 0_z) = (x, y, z)$ (definición de $\bigoplus$)

$(x, y, z) = (y + 0_y, x + 0_x, z + 0_z)$

Vemos que a menos que las dos primeras coordenadas sean iguales la cosa no va a funcionar. Demostrémoslo por el absurdo:

Supongamos que existe un tal $(0_x, 0_y, 0_z)$ entonces debe ocurrir:

$(1, 2, 3) \bigoplus (0_x, 0_y, 0_z) = (1, 2, 3)$

$(2 + 0_y, 1 + 0_x, 3 + 0_z) = (1, 2, 3)$, es decir:

$$\begin{aligned} 2 + 0_y &= 1, \\ 1 + 0_x &= 2, \\ 3 + 0_z &= 3 \end{aligned}$$

de donde concluímos que $(0_x, 0_y, 0_z) = (1, -1, 0)$

Pero $(1, 1, 1) \bigoplus (1, -1, 0) = (0, 2, 1) \neq (1, 1, 1)$.

Como encontramos una propiedad que no se cumple, no es necesario demostrar ninguna más. Con una que falle, ya no es espacio vectorial. Tampoco es necesario demostrar todas hasta que alguna falle, si intuímos que una no va a funcionar, comenzamos por esa, para ahorrar cálculos.

6. Sea $V = \mathbb{R}^2$ con la suma habitual, pero definimos el producto externo

$k \odot (x, y) = (0, 0)$

Claramente no necesitamos probar las propiedades de la suma habitual, porque son conocidas. El producto es nuevo y lo primero que probamos es la conservación de la identidad, con un caso particular, vamos en busca de un contraejemplo:

$1 \odot (1,1) = (0,0) \neq (1,1)$. (aplicamos la definición de $\odot$)

Y concluimos que no es un $\mathbb{R}$-espacio vectorial.

7. $(\mathbb{F}, \oplus, \odot)$ donde $\mathbb{F}$ es el conjunto de todas las funciones reales y las operaciones son:

   $\oplus$: $f \oplus g$ está definida por $(f \oplus g)(x) = f(x) + g(x)$ para cada $x \in \mathbb{R}$,

   $\odot$: $k \odot fg$ está definida por $(k \odot f)(x) = k.(f(x))$ para cada $x \in \mathbb{R}$.

   $(\mathbb{F}, \oplus, \odot)$ es $\mathbb{R}$-espacio vectorial y los cálculos quedan a cargo del lector interesado. (Recuerden que siempre es bienvenida su consulta ya sea on line o dentro del horario prefijado.)®

Ya que tenemos dos operaciones posibles podemos *combinarlas* y así llegar a la siguiente definición:

Definición 10.2 Dado un $\mathbb{K}$-espacio vectorial $(V, +, .)$, $k_1, k_2, \ldots, k_n \in \mathbb{K}$ y los vectores $\vec{v}_1, \vec{v}_2, \ldots \vec{v}_n \in V$, $\vec{u} = k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots + k_n.\vec{v}_n$ es una *combinación lineal* de los vectores $\vec{v}_1, \vec{v}_2, \ldots \vec{v}_n$.

Ejemplo 10.2

1. Consideremos $\mathbb{R}^2$ con la suma y producto habituales. ¿Podemos escribir $(1,2)$ como combinación lineal de $(2,-3)$ y $(1,-1)$?

   $(1,2) = k_1.(2,-3) + k_2.(1,-1)$ genera el sistema de ecuaciones:

   $$\begin{cases} 1 = k_1.2 + k_2.1 \\ 2 = k_1.(-3) + k_2.(-1) \end{cases}, \text{ o lo que es lo mismo: } \begin{cases} 2.k_1 + k_2 = 1 \\ -3.k_1 - k_2 = 2 \end{cases}$$

   que tiene solución $k_1 = -3$, $k_2 = 7$.
   En efecto: $(1,2) = (-3).(2,-3) + 7.(1,-1)$
   y hemos escrito a $(1,2)$ como combinación lineal de $(2,-3)$ y $(1,-1)$.

Esto no siempre es posible, pensemos que la propuesta de escribir un vector de n coordenadas como combinación lineal de m vectores (también de n coordenadas necesariamente) nos genera un sistema de m ecuaciones con n incógnitas que sabemos puede ser compatible determinado o no y también incompatible.
Si el sistema es compatible (determinado o no) el vector $\vec{u}$ *depende* de los vectores $\vec{v}_1, \vec{v}_2, \ldots \vec{v}_n$ si el sistema es incompatible el vector $\vec{u}$ es *independiente*

de los vectores $\vec{v}_1, \vec{v}_2, \ldots \vec{v}_n$. Es decir no existen $k_1, k_2, \ldots, k_n \in \mathbb{K}$ tales que $\vec{u} = k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots + k_n.\vec{v}_n$ Dicho de otro modo:

$$\vec{u} \neq k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots + k_n.\vec{v}_n$$

$$\vec{0} \neq -\vec{u} + k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots + k_n.\vec{v}_n.$$

Generalicemos esto:

Definición 10.3 Un conjunto de vectores $\{\vec{v}_1, \vec{v}_2, \ldots \vec{v}_n\} \subseteq V$ se dice *linealmente independiente* si no existen escalares no nulos $k_1, k_2, \ldots, k_n \in \mathbb{K}$ tales que $\vec{0} = k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots + k_n.\vec{v}_n$. En caso contrario se dicen *linealmente dependientes.*

Observemos que decimos escalares *no nulos* ya que el sistema que se genera igualando al vector nulo es un sistema homogéneo y sabemos que siempre admite la solución nula, es decir, siempre se trata de un sistema compatible, entonces podríamos reformular esta definición diciendo:
Un conjunto de vectores es linealmente independiente si se genera un sistema compatible determinado, y si se trata de un sistema de n ecuaciones con n incógnitas podemos decidir si los vectores son dependientes o no calculando el determinante de la matriz del sistema, que debe ser diferente de cero para que el sistema sea compatible determinado y, en consecuencia, los vectores linealmente independientes.

10.1.1. Subespacios Vectoriales

A diferencia de los deportes donde una "sub" es un equipo de jugadores con "menos de tantos años", en matemática lo que sea "sub" cumple exactamente lo mismo, y con las mismas operaciones que uno más grande que lo contiene. Por ejemplo, en el curso hemos dicho que $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son conjuntos numéricos y sabemos que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ entonces podemos decir que $\mathbb{N}$ es un *subconjunto* de $\mathbb{R}$, de $\mathbb{Q}$ o de $\mathbb{Z}$ o $\mathbb{C}$ simplemente porque está contenido. Si pensamos en cuerpos sólo podemos considerar a $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ y decimos que $\mathbb{Q}$ (porque es cuerpo) es un subcuerpo de $\mathbb{R}$ o de $\mathbb{C}$. Si pensamos en cuerpos ordenados $\mathbb{Q}$ será un *subcuerpo ordenado* de $\mathbb{R}$ pero no de $\mathbb{C}$ ya que sabemos que $\mathbb{C}$ no es cuerpo ordenado.
Si pensamos en espacios vectoriales un *subespacio vectorial* debe ser un espacio vectorial totalmente dentro de otro espacio vectorial. ¿Será necesario verificar todas las propiedades V_1 a V_8? La respuesta es negativa, ya que claramente si los elementos están en un subconjunto $W \subseteq V$ también están en V y se verificarán en forma inmediata V_1, V_2, V_5, V_6, V_7 y V_8. ¿Qué diferencia

tienen V_3 y V_4? Hablan de la existencia de elementos que se dan en V pero hay que ver que estén dentro e W. Al pedirle al neutro para la suma de V que esté dentro de W ya estamos diciendo que W es no vacío. Debemos garantizar que las operaciones en V sean operaciones en W. Es decir, que al hacer cuentas con elementos de W se obtengan elementos de W. (esto se enuncia como W es cerrado con respecto a la suma y el producto externo). Por otra parte, V_4 está garantizada porque la operación producto por un escalar sea cerrada. Es decir, si para cava $k \in \mathbb{K}, \vec{in}W$ resulta $k.\vec{v} \in W$, como al multiplicar $\vec{v}$ por -1 obtenemos $-\vec{v}$ esto basta para garantizar que W es subespacio. Escribamos entonces una definición formal:

Definición 10.4 Dado un $\mathbb{K}$-espacio vectorial $(V, +, .)$, un subconjunto no vacío W de V se dice un *subespacio* si verifica:

S_1 : Si $\vec{u}, \vec{v} \in W$, entonces $\vec{u} + \vec{v} \in W$.

S_2 : Si $k \in \mathbb{K}$, $\vec{v} \in W$ entonces $k.\vec{v} \in W$.

¿Qué pasó? Insistimos en que $\vec{0} \in W$ ¿y no lo mencionamos? Pedimos que sea no vacío, entonces hay algún vector, llamémoslo $\vec{v}$. Por S_1 está el producto por cualquier elemento del cuerpo entonces $(-1).\vec{v} = -\vec{v} \in W$ y por S_1 están las sumas de los elementos, entonces $\vec{v} + (-\vec{v}) = \vec{0} \in W$.
Un razonamiento muy interesante, pero para probar que $W \neq \emptyset$ usamos el elemento neutro del espacio vectorial y así estamos absolutamente seguros de que $\vec{0} \in W$.
Resumiendo: para probar que $W \subseteq V$ es subespacio vectorial hay que probar tres cosas:

S_0 : $\vec{0} \in W$

S_1 : Si $\vec{u}, \vec{v} \in W$, entonces $\vec{u} + \vec{v} \in W$.

S_2 : Si $k \in \mathbb{K}$, $\vec{v} \in W$ entonces $k.\vec{v} \in W$.

Es evidente que todas las propiedades de subespacio se cumplen para los subconjuntos $\{\vec{0}\}$ y V, que se denominan *subespacios triviales.*

Para indicar que W es un subespacio de V solemos escribir

$$W \trianglelefteq V.$$

Claramente, si un subconjunto S no es subespacio escribimos

$$S \ntrianglelefteq V.$$

Ejemplo 10.3 Consideremos el $\mathbb{R}-$espacio vectorial $M_2(\mathbb{R})$ con la suma y producto por un escalar habituales:

1. $W_1 : \{A \in M_2(\mathbb{R}) : |A| \neq 0\}$. $W_1 \ntrianglelefteq V$.
   Claramente la matriz nula tiene determinante nulo, por lo tanto no pertenece al conjunto y no es subespacio.

2. $W_2 : \{A \in M_2(\mathbb{R}) : a_{11} + a_{22} = a_{12}\}$.
   Veamos cómo es una de estas matrices: La condición que se nos impone es que el elemento que está en la primera fila, segunda columna sea la suma del elemento que está en la primera fila, primera columna más el que está en segunda fila segunda columna. Todos los demás elementos son totalmente libres, por eso el "aspecto" de la matriz es:
   $$\begin{pmatrix} a & a+b \\ c & b \end{pmatrix}.$$
   Ahora que ya tenemos la forma de las matrices que componen este conjunto W_2 veamos que se cumplen las condiciones:
   $S_0 :$ $\begin{pmatrix} 0 & 0+0 \\ 0 & 0 \end{pmatrix} \in W_2$.
   $S_1 :$ Sean $A = \begin{pmatrix} a & a+b \\ c & b \end{pmatrix}$, $B = \begin{pmatrix} e & e+f \\ g & f \end{pmatrix}$ y sumémoslas:
   $$A + B = \begin{pmatrix} a+e & (a+b)+(e+f) \\ c+g & b+f \end{pmatrix} = \begin{pmatrix} a+e & (a+e)+(b+f) \\ c+g & b+f \end{pmatrix} \in W_2.$$
   $S_2 :$ Si $k \in \mathbb{R}$, $\begin{pmatrix} a & a+b \\ c & b \end{pmatrix} \in W_2$ entonces
   $$\begin{pmatrix} k.a & k.(a+b) \\ k.c & k.b \end{pmatrix} = \begin{pmatrix} k.a & k.a+k.b \\ k.c & k.b \end{pmatrix} \in W_2.$$
   Concluımos que $W_2 \trianglelefteq V$.

3. Comentemos un poco y dejamos como ejercicio para el lector que cualquier recta que pase por el origen es un subespacio de $\mathbb{R}^2$ y cualquier plano que pase por el origen lo es de $\mathbb{R}^3$ ¿Y si no pasan por el origen? Ⓡ

4. Análogamente al ejemplo anterior las soluciones de un sistema homogéneo forman subespacio vectorial. ¿Y si no es homogéneo? Ⓡ

Propiedades

Finalmente un subespacio es un subconjunto, entonces podemos realizar con subespacios las mismas operaciones que realizamos con subconjuntos.
Claramente como el $\vec{0}$ es único y debe pertenecer al subespacio el complemento de un subespacio no será subespacio (¿Realmente es claro?)
La unión de subespacios en general no es un subespacio. Pensemos en $\mathbb{R}^2$ y tomemos dos rectas que pasen por el origen, digamos $L_1 : y = 2x$ y $L_s : y = 5x$ y consideremos del elementos de la unión $L_1 \cup L_2$, pero uno en cada subespecio. $(1, 2) \in L_1$, $(1, 5) \in L_2$ si los sumamos: $(2, 7)$ no pertenece ni a L_1 ni a L_2, por lo tanto no pertenece a la unión. Extiendo una gentil invitación al lector interesado a realizar el gráfico de la situación que acabamos de mencionar.®
Con la intersección sí funciona:

Proposición 10.1 *Dado V un $\mathbb{K}$-especio vectorial, si S y T son dos subespacios de V, entonces $S \cap T$ también es subespacio de V.*

Demostración: Debemos probar las tres condiciones de subespacio:

- S_0 Como S y T son subespacios, $\vec{0} \in S$ y $\vec{0} \in T$, entonces $\vec{0} \in S \cap T$.
- S_1 Sean $\vec{v}_1$ y $\vec{v}_2 \in S \cap T$, entonces $\vec{v}_1$ y $\vec{v}_2 \in S$ y como S es subespacio $\vec{v}_1 + \vec{v}_2 \in S$. Del mismo modo afirmamos $\vec{v}_1$ y $\vec{v}_2 \in T$ y como T es subespacio $\vec{v}_1 + \vec{v}_2 \in T$ y, en consecuencia $\vec{v}_1 + \vec{v}_2 \in S \cap T$.
- S_2 Sea ahora $k \in \mathbb{K}$ y $\vec{v} \in S \cap T$, claramente $\vec{v} \in S$ y $\vec{v} \in T$, como ambos son subespacios $k.\vec{v} \in S$ y $k.\vec{v} \in T$, de donde: $k.\vec{v} \in S \cap T$.

Por lo antes visto, $S \cap T$ es subespacio de V. □

Ejemplo 10.4 Consideremos el $\mathbb{R}$-espacio vectorial $\mathbb{R}^4$ con la suma y el producto habituales, y los subespacios:
$S = \{(x, y, z, t) : x + 2y = z - t\}$ y $T = \{(x, y, z, t) : 2x + y - t = 0,\ 3z = 4t\}$
La intersección de los subespacios es el conjunto de soluciones del sistema de ecuaciones que se genera poniendo las tres ecuaciones juntas, es decir:

$$\begin{cases} 2x + y - t = 0 \\ x + 2y = z - t \\ 3z = 4t \end{cases}$$

que escribimos más usualmente como:

$$\begin{cases} 2x + y - t = 0 \\ x + 2y - z + t = 0 \\ 3z - 4t = 0 \end{cases}.$$

Es un sistema de tres ecuaciones con cuatro incógnitas y podemos encontrar la solución, por ejemplo, triangulando la matriz:

$$\begin{pmatrix} 1 & 2 & -1 & 1 \\ 2 & 1 & 0 & -1 \\ 0 & 0 & 3 & -4 \end{pmatrix}$$

Solo poniendo en la fila 2, $F_2 - 2.F_1$ obtenemos:

$$\begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & -3 & 2 & -3 \\ 0 & 0 & 3 & -4 \end{pmatrix}$$

de donde:

$$\begin{cases} x + 2y - z + t = 0 \\ -3y + 2z - 3t = 0 \\ 3z - 4t = 0 \end{cases}$$

Tenemos cuatro incógnitas, tres ecuaciones, entonces el sistema es compatible indeterminado y el grado de indeterminación es: $4 - 3 = 1$. Es decir, la solución general nos queda con una letra.

Solución general: $\left(-\frac{1}{3}a, \frac{1}{3}a, \frac{4}{3}a, a\right)_{a\in\mathbb{R}}$, que es la forma que tendrá un elemento en la interseccón de subespacios.

Subespacio generado

Dado un espacio vectorial, subconjunto cualquiera no es subespacio, pero podemos construir un subespacio agregando al conjunto todo lo que le falta para que las operaciones sean cerradas. Este espacio es exactamente la interseccón de todos los subespacios que contienen al conjunto dado. Formalizamos la definición poniendo:

Definición 10.5 Dado un $\mathbb{K}$-espacio vectorial $(V, +, .)$ y un subconjunto cualquiera X de V definimos el *subespacio generado por* X y lo notamos $\overline{X}$ (o bien $[X]$) al menor subespacio que contiene a X.

En símbolos:

$G_1: \ X \subseteq \overline{X}$,

$G_2: \ \overline{X}$ es un subespacio de V,

$G_3: $ Si S es un subespacio de V tal que $X \subseteq S$, entonces $\overline{X} \subseteq S$.

Se puede probar que $\overline{X}$ es la interseccón de todos los subespacios que contienen a X, es decir:

$$\overline{X} = \bigcap \{S : S \text{ es subespacio de } V, X \subseteq S\}.$$

No vamos a demostrarlo en este curso, pero tampoco obligamos a los lectores a pasarlo por alto. Quien quiera regocijarse demostrándolo y se encuentre perdido será bien recibido para brindarle el GPS adecuado. Sí vamos a mencionar y demostrar el siguiente resultado:

Proposición 10.2 *El subespacio generado por X es el conjunto de todas las combinaciones lineales de elementos de X.*

Demostración: Probemos las tres condiciones, pero antes definamos formalmente el conjunto de todas las combinaciones lineales de elementos en X y llamémoslo S. Queremos ver que S cumple las tres condiciones de subespacio generado por X.

$$S = \{k_1.\vec{x}_1 + k_2.\vec{x}_2 + \ldots + k_n.\vec{x}_n : k_1, k_2, \ldots, k_n \in \mathbb{K}, \vec{x}_1, \vec{x}_2, \ldots, \vec{x}_n \in X\}$$

$G_1 :$ $X \subseteq S$, Para cada $\vec{x} \in X$ la combinación lineal $1.\vec{x}$ satisface lo pedido y así $X \subseteq S$.

$G_2 :$ S es un subespacio de V: Tomando $k_i = 0$ para todo i el elemento que resulta es $\vec{0}$ y vemos que $\vec{0} \in S$.
Claramente la suma de dos combinaciones lineales de elementos de X sigue siendo una combinación lineal de elementos de X y también el producto por un escalar de una combinación lineal de elementos de X es una combinación lioneal de elementos de X.

$G_3 :$ Si S' es un subespacio de V tal que $X \subseteq S'$, entonces $S \subseteq S'$.Supongamos que S' es un subespacio vectorial que contiene a X y sea una combinación lineal de elementos de X. Claramente como S' es subespacio es cerrado con respecto al producto por un escalar y a la suma, entonces la combinación lineal pertenece también a S'.

Finalmente concluimos que $S = \overline{X}$. □

Ejemplo 10.5 Demos algunos ejemplos de subespacios generados:

1. $\overline{\emptyset} = \{\vec{0}\}$,
2. $\overline{V} = V$,

3. $V = \mathbb{R}^2$, $X = \{(1,2)\}$, entonces $\overline{X} = \{(x,y) = (k,2k), k \in \mathbb{R}\}$ y es la recta $y = 2x$,
4. $V = M_2(\mathbb{R})$, $X = \{A \in M_2(\mathbb{R}) : a_{11} = a_{22}, a_{12} = a_{21}\}$.

   La forma de estas matrices será:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

   Estas matrices tienen dos letras diferentes. Busquemos escribir esta matriz como combinación lineal de matrices que tengan la mayor cantidad de ceros posibles:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} = a.\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b.\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

   las matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ generan el espacio.
   Escribimos:

$$X = \overline{\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}}$$

10.1.2. Bases

Cuando generamos un espacio vectorial a partir de un conjunto X puede ocurrir que generemos todo el espacio, en dicho caso decimos que X es un conjunto de generadores. Más formalmente:

Definición 10.6 Dado un $\mathbb{K}$ espacio vectorial $(V, +, .)$ un conjunto G se dice un *sistema de generadores* de V si $\overline{G} = V$.

¿Qué quiere decir que este conjunto G sea un conjunto de generadores? Que todo elemento $\vec{v}$ de V puede escribirse como combinación lineal de elementos de G.
Este es un buen resultado, pero nos gustaría poder encontrar una forma única de escribir cada $\vec{v}$. Vimos, cuando comenzamos a hablar de espacios vectoriales, la definición 10.3 que habla de la independencia lineal. Veamos propiedades de los vectores linealmente independientes:

Proposición 10.3 *Consideremos los vectores $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$. Las siguientes condiciones son equivalentes:*

LI_1 $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ *es linealmente independiente.*

LI_2 *Si* $k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots k_n.\vec{v}_n = t_1.\vec{v}_1 + t_2.\vec{v}_2 + \ldots + t_n.\vec{v}_n$*, entonces* $k_i = t_i$ *para todo* $i = 1, 2, \ldots, n$.

LI_3 *Ningún* $\vec{v}_i$ *es combinación lineal de los restantes.*

LI_4 $\vec{v}_1 \neq \vec{0}$ *y ningún* $\vec{v}_i$ *es combinación lineal de los precedentes, para* $1 < i \leq n$.

Demostración: Estas equivalencias de "todos con todos" pueden probarse siguiendo un ciclo y sólo requiere, en este caso, cuatro demostraciones. Comencemos:

$1 \Rightarrow 2$: Supongamos que $k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots k_n.\vec{v}_n = t_1.\vec{v}_1 + t_2.\vec{v}_2 + \ldots + t_n.\vec{v}_n$, entonces

$(k_1 - t_1).\vec{v}_1 + (k_2 - t_2).\vec{v}_2 + \ldots (k_n - t_n).\vec{v}_n = \vec{0}$, pero sabemos que $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}0$ es linealmente independiente entonces necesariamente $k_i - t_i = 0$, o lo que es lo mismo $k_i = t_i$ para todo $1 \leq i \leq n$.

$2 \Rightarrow 3$: Supongamos que $\vec{v}_j$ es combinación lineal de los restantes, entonces podemos escribir:

$$0.\vec{v}_1 + 0.\vec{v}_2 + \ldots + 1.\vec{v}_j + \ldots + 0.\vec{v}_n = t_1.\vec{v}_1 + t_2.\vec{v}_2 + \ldots + 1.\vec{v}_j + \ldots + t_n.\vec{v}_n$$

por el inciso anterior los coeficientes son iguales dos a dos y resulta $t_i = 0$ para todo $i \neq j$.

$3 \Rightarrow 4$: $\vec{v}_1 \neq \vec{0}$ ya que existe una combinación lineal de los restantes igualada al vector nulo (poniendo todos los $k_i = 0$) y como se verifica 3, ningún vector es combinación lineal de los restantes. Supongamos, por el absurdo, que un vector es combinación lineal de los precedentes. Sumamos a esa combinación todos los demás vectores multiplicados por $k = 0$ y tenemos un vector escrito como combinación lineal de los restantes, lo cual es un absurdo que provino de suponer que un vector era combinación linela de los precedentes.

$4 \Rightarrow 1$: Finalmente supongamos que $\vec{v}_1 \neq \vec{0}$ y ningún $\vec{v}_i$ es combinación lineal de los precedentes, para $1 < i \leq n$ y probemos que $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ es linealmente independiente.
Podemos hacer esta demostración por inducción: en el caso base tomamos el conjunto $\{\vec{v}_1\}$ que es linealmente independiente ya que $\vec{v}_1 \neq \vec{0}$. Supongamos que $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_l\}$ es linealmente independiente y probemos que $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{l+1}\}$ es linealmente independiente.
Como $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_l\}$ es linealmente independiente resulta

$$k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots k_l.\vec{v}_l = \vec{0}$$

lo que implica $k_i = 0$ para todo $1 \leq i \leq l$.
Supongamos que

$$k_1.\vec{v}_1 + k_2.\vec{v}_2 + \ldots k_l.\vec{v}_l + \ldots k_{l+1}.\vec{v}_{l+1} = \vec{0},$$

entonces

$$-\frac{k_1}{k_{l+1}}.\vec{v}_1 - \frac{k_2}{k_{l+1}}.\vec{v}_2 - \ldots - \frac{k_l}{k_{l+1}}.\vec{v}_l = \vec{v}_{l+1} = \vec{0}$$

y $\vec{v}_{l+1}$ es combinación lineal de los anteriores, lo cual es un absurdo porque suponemos que vale 4. En consecuencia $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ para cualquier cantidad n.

□

® El lector interesado puede ejercitar sus habilidades demostrando que, si $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ es linealmente independiente:

1. la manera de expresar un vector $\vec{v}$ como combinación lineal de $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ es única.
2. todo subconjunto lo es.
3. $\vec{v}_i \neq \vec{v}_j$ para todo $i \neq j$
4. si $\vec{u}$ no es combinación lineal de $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$, entonces $\{\vec{u}, \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ es linealmente independiente.

Repasemos un poco: Tenemos un $\mathbb{K}$-espacio vectorial V. Encontramos que puede haber un conjunto G tal que $\overline{G} = V$, es decir que todo vector en V pueda escribirse como combinación lineal de vectores en G. También vimos que si un conjunto es linealmente independiente, los vectores que son combinación lineal de ellos se escriben de manera única. Unamos ambas condiciones: si tenemos un conjunto de vectores B linealmente independientes que genere todo el espacio, entonces podremos escribir cualquier vector del espacio de forma única como combinación lineal de los vectores de B. Una buena base para poder comenzar a trabajar. Definámoslo, entonces:

Definición 10.7 Dado un $\mathbb{K}$-espacio vectorial $(V, +, .)$, un conjunto $\mathcal{B}$ se dice una *base* del espacio si:

$\mathcal{B}_1$: $\mathcal{B}$ es un conjunto linealmente independiente.

$\mathcal{B}_2$: $\overline{\mathcal{B}} = V$ ($\mathcal{B}$ genera todo el espacio)

Definición 10.8 Dado un $\mathbb{K}$-espacio vectorial $(V, +, .)$, de base $\mathcal{B}$ llamamos *dimensión* del espacio al orden (cantidad de elementos) del conjunto $\mathcal{B}$. Si $\mathcal{B}$ es finito diremos que el espacio vectorial V es de dimensión finita.

Tal vez en un primer momento piensen ¿Y qué espacio puede no tener una base finita? Tienen uno muy cerca: el espacio de los polinomios a coeficientes reales. Una base para este conjunto puede ser $\mathcal{B} = \{x^i : i \in \mathbb{N}\}$. Cualquiera que sea el polinomio se escribe como combninación lineal finita de potencias de x (incluido $x^0 = 1$), pero no hay ningún conjunto finito para escribir cualquier polinomio y la demostración, que es muy sencilla, queda a cargo del lector interesado.®
Analicemos un poco la definición de base: Una base es un conjunto de generadores linealmente independiente.

- Como es linealmente independiente, si saco un vector del conjunto, no tengo forma de escribirlo como combinación lineal de los restantes y resulta que el conjunto que queda ya no es de generadores. Se dice entonces que es un *conjunto de generadores minimal* (si le saco algo ya no genero).
- Como es un conjunto de generadores, cualquier vector del espacio se escribe como combinación lineal de ellos, entonces cualquier vector que agregue al conjunto ya no es linealmente independiente. Se dice que es un *conjunto linealmente independiente maximal* (si le agrego algo, ya no es linealmente independiente).

En esta observación es especialmente práctico la utilización del concepto "linealmente independiente maximal", ya que es más sencillo comprobar la independencia lineal que el hecho de ser generador.
Veamos algunos ejemplos:

Ejemplo 10.6

1. $V = \mathbb{R}^2,\ \mathcal{B} = \{(1,-1),(1,1)\}$
   Comprobemos que se trata de un conjunto de generadores, es decir, que todo (x,y) se puede escribir como combinación lineal de $(1,-1)$ y $(1,1)$: $(x,y) = a(1,-1) + b.(1,1)$ genera el sistema de ecuaciones:
   $$\begin{cases} x = a + b \\ y = -a + b \end{cases}$$
   Solución para este sistema: $a = \dfrac{x-y}{2},\ \ b = \dfrac{x+y}{2}$.
   En efecto:
   $$a(1,-1) + b.(1,1) = \frac{x-y}{2}.(1,-1) + \frac{x+y}{2}.(1,1) =$$
   $$= \left(\frac{x-y}{2}, -\frac{x-y}{2}\right) + \left(\frac{x+y}{2}, \frac{x+y}{2}\right) = (x,y)$$

Comprobemos ahora que es linealmente independiente: Como son dos vectores de dos coordenadas, podemos armar la matriz. Escribámoslos por columna y calculemos el determinante:

$$\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} = 2 \neq 0$$

Levantemos un poco la mirada. Acabamos de calcular el determinante de la matriz del sistema que usamos para probar que es generador. Si el sistema fuera homogéneo, que el determinante sea no nulo indica que el sistema es compatible determinado y los vectores linealmente independientes.

En verdad como tienen dos coordenadas este es un conjunto linealmente independiente maximal y el simple cálculo de este determinante alcanzaba para probar que $\mathcal{B}$ es una base de $\mathbb{R}^2$

2. $V = \mathbb{R}^n,\ \mathbb{C} = \{(1,0,0,\ldots,0),(0,1,0\ldots,0),\ldots(0,0,0,\ldots,1)\}$.

   Considerando el razonamiento que acabamos de hacer, basta con ver que el determinante de la matriz formada por los vectores del conjunto es no nula. Específicamente el determinante de esta matriz es 1, ya que se trata de la matriz identidad. Esta base es conocida como la *base canónica.*

   Usualmente se escribe $\mathcal{C}_n = \{\check{e}_i\}_{1\leq i\leq n}$, donde $\check{e}_{ij} = \begin{cases} 1 & \text{si } i=j \\ 0 & \text{en otro caso.} \end{cases}$

3. $V = M_2(\mathbb{R}),\ \mathcal{B} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix} \right\}$

   Podemos pensar a cada una de estas matrices como vectores de 4 coordenadas leyendo, por ejemplo, la primera columna y luego la segunda columna. Escribimos estos cuatro vectores por fila en una matriz para calcularle el determinante.

$$\begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 4 \end{vmatrix} = 4 \neq 0$$

   Comprobamos que se trata de un conjunto linealmente independiente maximal y, por lo tanto, de una base.

   Las bases canónicas son las que tienen ceros y unos. Es claro que una base de $M_2(\mathbb{R})$ tendrá cuatro elementos ¿En qué orden? Dos posibilidades son:

$$\mathcal{C}_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$\mathcal{C}_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Ambas son igualmente válidas como base canónica y por eso, cuando hablamos de matrices, especificamos siempre a qué base canónica nos referimos.

4. $V = \mathbb{P}_2(\mathbb{R})$ $\mathcal{B} = \{x^2, 1 + 2\,x, x - x^2\}$
Pensemos un poco: un polinomio de grado a lo sumo dos se escribe: $a_2\,x^2 + a_1\,x + a_0$ Podemos asociar este polinomio al vector: (a_2, a_1, a_0) y de ese modo reescribimos el conjunto $\mathcal{B} = \{(1,0,0),(0,2,1),(-1,1,0)\}$. Hagamos el determinante de la matriz:

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ -1 & 1 & 0 \end{vmatrix} = -1 \neq 0$$

y, en consecuencia, es una base del espacio de polinomios de grado a lo sumo 3.

Componentes

Hemos visto, por ejemplo, que la base canónica de $\mathbb{R}^3$ es

$$\mathcal{C}_3 = \{(1,0,0),(0,1,0),(0,0,1)\}$$

y $\vec{v} = (2,-1,7)$ es el extremo del vector $2.(1,0,0) + (-1).(0,1,0) + 7.(0,0,1)$, es decir, las componentes del vector son los escalares de la combinación lineal puestos en el orden correspondiente. Podemos extender esta misma idea a otras bases, por ejemplo, si consideramos:

$$\mathcal{B} = \{(0,-1,0),(2,1,0),(0,0,-1)\}$$

vemos que:

$$(2,-1,7) = 2.(0,-1,0) + 1.(2,1,0) + (-7).(0,0,-1),$$

afirmamos, entonces, que las componentes de $\vec{v}$ en la base $\mathcal{B}$ son: $\langle 2, 1-7\rangle$. Escribamos la definición formal:

Definición 10.9 Dado un $\mathbb{K}$-espacio vectorial $(V,+,.)$ Una *base ordenada* es una sucesión de vectores linealmente independientes $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ que genera el espacio.

En verdad cuando alguien habla del punto $(1,2)$ en el plano, todos interpretamos intuitivamente que el 1 es el valor de las abscisas y el 2 es es las ordenadas. Decimos, además, que la base canónica de $\mathbb{R}^2$ es $\mathcal{B}=\{(1,0),(0,1)\}$ y lo escribimos en forma de conjunto. En la primera unidad, cuando estudiamos conjuntos vimos que no existe el orden entre los elementos, por lo tanto $\{(1,0),(0,1)\}=\{(0,1),(1,0)\}$ Este hecho hace que debamos definir la noción de base ordenada, como una sucesión, pero en la práctica la escribiremos en forma de conjunto, cuidado, siempre, que el orden sea el correcto.

Definición 10.10 Sea un $\mathbb{K}$-espacio vectorial $(V,+,.)$, $\mathcal{B}=\{\vec{v}_1,\vec{v}_2,\ldots,\vec{v}_n\}$ una base ordenada, entonces todo vector $\vec{v}\in V$ puede escribirse de forma única como combinación lineal de los vectores de la base, es decir

$$a_1.\vec{v}_1+a_2.\vec{v}_2+\ldots+a_n.\vec{v}_n.$$

La n-upla $(a_1,a_2,\ldots,a_n)$ se denomina las *componentes de* $\vec{v}$ *en la base* $\mathcal{B}$. a_i es, entonces, la i-ésima componente de $\vec{v}$ en la base $\mathcal{B}$.

En general, cuando la base ordenada no es la canónica, estas n-uplas suelen escribirse subindicadas con la base, y a veces con ángulos en lugar de paréntesis, para distinguirlas fácilmente. Por ejemplo, en el inicio de esta sección escribimos

$$(2,-1,7)=\langle 2,1,-7\rangle=(2,1,-7)_{\mathcal{B}}$$

No lo demostraremos en este curso, pero afirmamos que todo espacio vectorial de dimensión finita tiene una base. Este hecho tiene una consecuencia muy interesante. Supongamos que tenemos un espcio vectorial V cualquiera de dimensión n, entonces tiene una base $\mathcal{B}$ y las coordenadas de cualquier vector conformarán una n-upla, lo que nos permitirá identificar a cualquier espacio vectorial de dimensión n cohn $\mathbb{R}^n$. Veamos un ejemplo:

Ejemplo 10.7 Consideremos $V=M_2(\mathbb{R})$. Una base para V es

$$\mathcal{B}=\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}$$

Podemos escribir

$$A=\begin{pmatrix}2&3\\-1&4\end{pmatrix}=2.\begin{pmatrix}1&0\\0&0\end{pmatrix}+(-1).\begin{pmatrix}0&0\\1&0\end{pmatrix}+3.\begin{pmatrix}0&1\\0&0\end{pmatrix}+4.\begin{pmatrix}0&0\\0&1\end{pmatrix}$$

es decir, las coordenadas de la matriz A en la base $\mathcal{B}$ son: $(2,-1,3,4)_{\mathcal{B}}$ y la podemos identificar con el punto $(2,-1,3,4)\in\mathbb{R}^4$.

10.1.3. Cambio de base

Dijimos que una base es un conjunto linealmente independiente de generadores y es claro que no existe una única base para cada espacio. Vamos a analizarlo en $\mathbb{R}^2$ para ver sencillamente qué es lo que ocurre. Pensemos en $\vec{v} = (1, 5)$. No lo hemos dicho explícitamente pero sabemos que estamos dando las coordenadas en la base canónica y nadie dudará al ubicarlo en un gráfico.
$\mathcal{B}_1 = \{(1, -1), (2, 1)\}$ y $\mathcal{B}_2 = \{(1, 2), (0, 1)\}$ son dos bases para $\mathbb{R}^2$.

En efecto: la dimensión del espacio es 2 y se trata de conjuntos de vectores linealmente independientes, ya que el determinante de la matriz formada por ellos es no nulo:

$$\begin{vmatrix} 1 & 2 \\ -1 & 1 \end{vmatrix} = 3 \neq 0 \qquad \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = 1 \neq 0$$

$$(1, 5) = -3.(1, -1) + 2.(2, 1) \text{ entonces } (-3, 2)_{\mathcal{B}_1}$$

¿Cómo encontramos estos valores?
Buscamos a y b tales que $(1, 5) = a.(1, -1) + b.(2, 1)$, lo que se puede escribir como el sistema

$$\begin{cases} a + 2.b = 1 \\ -a + b = 5 \end{cases}$$

que vectorialmente se escribe:

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$$

de donde:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 \\ 5 \end{pmatrix}$$

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \end{pmatrix} = \begin{pmatrix} -3 \\ 2 \end{pmatrix} \tag{10.1}$$

Supongamos que queremos encontrar las coordenadas en la base canónica de $(1, 3)_{\mathcal{B}_2}$.
Buscamos c y d tales que $1.(1, 2) + 3.(0, 1) = c.(1, 0) + d.(0, 1)$, lo que se puede escribir vectorialmente:

$$\begin{cases} 1.1 + 3.0 = c \\ 1.2 + 3.1 = d \end{cases}$$

que vectorialmente se escribe:

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix} \tag{10.2}$$

Vemos que para encontrar las coordenadas del vector en la base canónica conociendo sus coordenadas en la base $\mathcal{B}_2$ hemos multiplicado la matriz cuyas columnas son los vectores de la base $\mathcal{B}_2$ expresados en la base canónica.
Analicemos las columnas de la matriz con que pasamos de la base canónica a la base $\mathcal{B}_1$:

$$\frac{1}{3}.(2,-1)+\frac{1}{3}.(2,1)=(1,0)$$
$$-\frac{2}{3}.(2,-1)+\frac{1}{3}.(2,1)=(0,1)$$

Es decir, son las coordenadas de los vectores de la base canónica en la base $\mathcal{B}_1$.
Y vemos que para encontrar las coordenadas del vector en la base $\mathcal{B}_2$ conociendo sus coordenadas en la base canónica hemos multiplicado la matriz cuyas columnas son los vectores de la base canónica expresados en la base $\mathcal{B}_1$.

¿Qué ocurre si multiplicamos estas dos matrices?

$$\begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -\frac{2}{3} \\ 1 & \frac{1}{3} \end{pmatrix} \tag{10.3}$$

Son las matrices que usamos para ir de la base $\mathcal{B}_2$ a la canónica y la matriz que usamos para ir de la base canónica a $\mathcal{B}_1$. Es decir, hemos ido de $\mathcal{B}_2$ a $\mathcal{B}_1$ pasando por la base canónica Verifiquemos que sus columnas son los vectores de la base $\mathcal{B}_2$ escritos como combinación lineal de los vectores de la base $\mathcal{B}_1$.

$$-1.(1,-1)+1.(2,1)=(1,2)$$

$$-\frac{2}{3}.(1,-1)+\frac{1}{3}.(2,1)=(0,1)$$

¿Podremos calcular las coordenadas de $\vec{v}$ en $\mathcal{B}_1$ a partir de sus coordenadas en $\mathcal{B}_2$?

$$\begin{pmatrix} -1 & -\frac{2}{3} \\ 1 & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} -3 \\ 2 \end{pmatrix} \tag{10.4}$$

Nada de lo que hemos hecho es casualidad y podemos generalizarlo para cualquier espacio vectorial dimensión finita.
Sea, entonces V un espacio vectorial y $\mathcal{B}=\{\vec{b}_1,\vec{b}_2,\ldots,\vec{b}_n\}$ y $\mathcal{B}'=\{\vec{b}'_1,\vec{b}'_2,\ldots,\vec{b}'_n\}$ dos bases ordenadas para V. Consideremos un vector escrito en la base $\mathcal{B}$

$$\vec{v}=(\alpha_1,\alpha_2,\ldots,\alpha_n)_{\mathcal{B}}.$$

Supongamos además que:
$\vec{b}_1 = a_{11}.\vec{b}'_1 + a_{21}.\vec{b}'_2 + \ldots + a_{n1}.\vec{b}'_n$
$\vec{b}_2 = a_{12}.\vec{b}'_1 + a_{22}.\vec{b}'_2 + \ldots + a_{n2}.\vec{b}'_n$
...
$\vec{b}_n = a_{1n}.\vec{b}'_1 + a_{2n}.\vec{b}'_2 + \ldots + a_{nn}.\vec{b}'_n$
Como $\vec{v} = \alpha_1.\vec{b}_1 + \alpha_2.\vec{b}_2 + \ldots, \alpha_n.\vec{b}_n$ reemplazamos para obtener:

$$\vec{v} = \alpha_1.(a_{11}.\vec{b}'_1 + a_{21}.\vec{b}'_2 + \ldots + a_{n1}.\vec{b}'_n) +$$

$$+\alpha_2.(a_{12}.\vec{b}'_1 + a_{22}.\vec{b}'_2 + \ldots + a_{n2}.\vec{b}'_n) + \ldots$$

$$\ldots + \alpha_n.(a_{1n}.\vec{b}'_1 + a_{2n}.\vec{b}'_2 + \ldots + a_{nn}.\vec{b}'_n)$$

Distribuyendo los α y sacando factor común los $\vec{b}'$ queda:

$$\vec{v} = (\alpha_1.a_{11} + \alpha_2.a_{12}. + \ldots + \alpha_n.a_{1n}).\vec{b}'_1 +$$

$$+(\alpha_1.a_{21} + \alpha_2.a_{22}. + \ldots + \alpha_n.a_{2n}).\vec{b}'_2 + \ldots$$

$$\ldots + (\alpha_1.a_{n1} + \alpha_2.a_{n2}. + \ldots + \alpha_n.a_{nn}).\vec{b}'_n$$

que matricialmente se escribe:

$$\vec{v}_{\mathcal{B}'} \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} . \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Esto nos lleva a:

Definición 10.11 Dado un $\mathbb{K}$-espacio vectorial de dimensión n y dos bases $\mathcal{B}$ y $\mathcal{B}'$ se llama *matriz de cambio de base de $\mathcal{B}$ a $\mathcal{B}'$* y se nota $[\mathcal{B}]_{\mathcal{B}'}$ a la matriz cuyas columnas son las coordenadas de los vectores de la base $\mathcal{B}$ en la base $\mathcal{B}'$.

Escribir la matriz de cambio de base de cualquier base $\mathcal{B}$ a $\mathbb{C}$ (la base canónica) simplemente se trata de escribir los vectores de la base ordenada por columna.
Si retomamos las bases $\mathcal{B}_1 = \{(1, -1), (2, 1)\}$ y $\mathcal{B}_2 = \{(1, 2), (0, 1)\}$ podemos ver que

$$[\mathcal{B}_1]_{\mathcal{C}} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \qquad [\mathcal{B}_2]_{\mathcal{C}} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

En 10.1 hemos hecho

$$[\mathcal{C}]_{\mathcal{B}_1}.[\vec{v}]_{\mathcal{C}} = [\vec{v}]_{\mathcal{B}_1}$$

En 10.2 hemos hecho

$$[\mathcal{B}_2]_{\mathcal{C}}.[\vec{v}]_{\mathcal{B}_2} = [\vec{v}]_{\mathcal{C}}$$

Es muy interesante ver que en 10.3 multiplicamos las matrices de cambio

$$[\mathcal{C}]_{\mathcal{B}_1}.[\mathcal{B}_2]_{\mathcal{C}} = [\mathcal{B}_2]_{\mathcal{B}_1}$$

Vuelvo a comentar que las matrices en verdad se pueden considerar como funciones y su producto como la composición de funciones. Si aplicamos primero la función f y luego la función g tomamos un elemento x, por f encontramos $f(x)$ y luego por g llegamos a $g(f(x)) = (g \circ f)(x)$. De cierto modo, a partir del elemento x escribimos las funciones “para atrás”. Esto mismo pasa con los productos de matrices en cambio de base: Queremos ir de la base $\mathcal{B}_2$ a la base $\mathcal{B}_1$, pero vamos a pasar por la base canónica, entonces vamos de la base $\mathcal{B}_2$ a $\mathcal{C}$ y luego de $\mathcal{C}$ a $\mathcal{B}_1$. Para realizar el producto de matrices escribimos el vector, a si izquierda la matriz de cambio de base de $\mathcal{B}_2$ a $\mathcal{C}$ y a la izquierda de ésta la matriz de cambio de base de $\mathcal{C}$ a $\mathcal{B}_1$. Podemos ver entonces en 10.4 que calculamos directamente

$$[\mathcal{B}_2]_{\mathcal{B}_1}.[\vec{v}]_{\mathcal{B}_2}$$

que en forma conjunta con 10.3 podríamos escribir:

$$[\mathcal{B}_2]_{\mathcal{B}_1}.[\vec{v}]_{\mathcal{B}_2} = ([\mathcal{C}]_{\mathcal{B}_1}.[\mathcal{B}_2]_{\mathcal{C}}).[\vec{v}]_{\mathcal{B}_2} = [\mathcal{C}]_{\mathcal{B}_1}.([\mathcal{B}_2]_{\mathcal{C}}.[\vec{v}]_{\mathcal{B}_2})$$

Muy fácilmente podemos ver que la matriz “de vuelta” del cambio de base es la matriz inversa, ya que:

$$[\mathcal{B}_2]_{\mathcal{B}_1}.[\vec{v}]_{\mathcal{B}_2} = [\vec{v}]_{\mathcal{B}_1}$$

multiplicando a la izquierda por la inversa de la matriz de cambio: (Lo dije muy tranquilamente ¿siempre existe? El lector seguramente sabrá contestar esta pregunta. Si no es así, no se quede con la duda.)

$$[\mathcal{B}_2]_{\mathcal{B}_1}^{-1}.([\mathcal{B}_2]_{\mathcal{B}_1}.[\vec{v}]_{\mathcal{B}_2}) = [\mathcal{B}_2]_{\mathcal{B}_1}^{-1}.[\vec{v}]_{\mathcal{B}_1}$$

y por la propiedad asociativa resulta:

$$[\vec{v}]_{\mathcal{B}_2} = [\mathcal{B}_2]_{\mathcal{B}_1}^{-1}.[\vec{v}]_{\mathcal{B}_1}$$

pero como

$$[\vec{v}]_{\mathcal{B}_2} = [\mathcal{B}_1]_{\mathcal{B}_2}.[\vec{v}]_{\mathcal{B}_1}$$

resulta entonces que

$$[\mathcal{B}_2]_{\mathcal{B}_1}^{-1} = [\mathcal{B}_1]_{\mathcal{B}_2}$$

Ejemplo 10.8 Veremos algunas construcciones de matrices de cambio de base.

1. Sea $\mathcal{B} = \{(1,2),\,(3,3)\}$ una base para $\mathbb{R}^3$. La matriz de cambio de base de $\mathcal{B}$ a la base canónica $\mathcal{C}_2$ es :

$$[\mathcal{B}]_{\mathcal{C}_2} = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$$

   y la matriz de cambio de base de $\mathcal{C}_2$ a $\mathcal{B}$ es la inversa:

$$[\mathcal{C}_2]_{\mathcal{B}} = ([\mathcal{B}]_{\mathcal{C}_2})^{-1} = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix}$$

2. Sean $\mathcal{B}_1 = \{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ y $\mathcal{B}_2 = \{\vec{w}_1, \vec{w}_2, \vec{w}_3\}$ tales que:

$$\vec{w}_1 = 3\,\vec{v}_1 - 2\,\vec{v}_2 - \vec{v}_3$$
$$\vec{w}_2 = 4\,\vec{v}_1 + 5\,\vec{v}_2 + \vec{v}_3$$
$$\vec{w}_3 = -\vec{v}_1 + 3\,\vec{v}_2 - \vec{v}_3$$

   Como tenemos todos los vectores de la base $\mathcal{B}_2$ escritos como combinación lineal de los vectores de la base $\mathcal{B}_1$ para armar la matriz de cambio de base de $\mathcal{B}_2$ a $\mathcal{B}_1$ basta escribir los coeficientes de las combinaciones lineales en forma de columna:

$$[\mathcal{B}_2]_{\mathcal{B}_1} = \begin{pmatrix} 3 & 4 & -1 \\ -2 & 5 & 3 \\ -1 & 1 & -1 \end{pmatrix}$$

   Para encontrar la matriz de cambio de $\mathcal{B}_1$ a $\mathcal{B}_2$ sólo tendremos que calcular la inversa de la matriz. Si las coordenadas de un vector $\vec{u}$ n la base $\mathcal{B}_2$ son $\langle 3, -1, 1\rangle_{\mathcal{B}_2}$ fácilmente obtenemos sus coordenadas en la base $\mathcal{B}_1$.

$$[\vec{u}]_{\mathcal{B}_1} = [\mathcal{B}_2]_{\mathcal{B}_1}.[\vec{u}]_{\mathcal{B}_2} = \begin{pmatrix} 3 & 4 & -1 \\ -2 & 5 & 3 \\ -1 & 1 & -1 \end{pmatrix} . \begin{pmatrix} 3 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ -8 \\ -5 \end{pmatrix}$$

   ¿Podemos encontrar las coordenadas del vector $\vec{u}$ en la base canónica?

3. Dado el espacio vectorial V y las bases de V: $\mathcal{B}_1, \mathcal{B}_2$ y $\mathcal{B}_3$ conocemos las matrices de cambio de base:

$$[\mathcal{B}_1]_{\mathcal{B}_2} = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 2 & -1 \\ 0 & 2 & 1 \end{pmatrix}, \qquad [\mathcal{B}_2]_{\mathcal{B}_3} = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & -1 \\ 2 & 0 & 0 \end{pmatrix}$$

¿Podemos escribir los vectores de la base $\mathcal{B}_1$ como combinación lineal de los vectores de la base $\mathcal{B}_3$?
La respuesta es afirmativa. Los coeficientes de las combinaciones lineales que buscamos son las colunas de la matriz de cambio de base de $\mathcal{B}_1$ a $\mathcal{B}_3$ y esta composición de cambios de base la encontramos por producto de matrices:

$$[\mathcal{B}_1]_{\mathcal{B}_3} = [\mathcal{B}_2]_{\mathcal{B}_3}.[\mathcal{B}_1]_{\mathcal{B}_2} = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & -1 \\ 2 & 0 & 0 \end{pmatrix} . \begin{pmatrix} 2 & 1 & -1 \\ 3 & 2 & -1 \\ 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 & -3 \\ 2 & -1 & -2 \\ 4 & 2 & -2 \end{pmatrix}$$

Y si $\mathcal{B}_1 = \{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ y $\mathcal{B}_3 = \{\vec{w}_1, \vec{w}_2, \vec{w}_3\}$ podemos escribir:

$$\vec{v}_1 = 5\,\vec{w}_1 + 2\,\vec{w}_2 + 4\,\vec{w}_3$$

$$\vec{v}_2 = 1\,\vec{w}_1 - 1\,\vec{w}_2 + 2\,\vec{w}_3$$

$$\vec{v}_3 = -3\,\vec{w}_1 - 2\,\vec{w}_2 - 2\,\vec{w}_3.$$

Cuando trabajamos con el plano y el espacio, con $\mathbb{R}^n$ en general definimos el producto escalar y lo usamos, entre otras aplicaciones, para calcular módulos y verificar que dos vectores son perpendiculares. Justamente el hecho de que los vectores de la base canónica sean de módulo uno y perpendiculares dos a dos nos hizo encontrar la "formulita" para calcular el producto escalar.
Si pensamos en $\mathbb{R}^2$ podemos encontrar que tanto

$$\mathcal{B}_1 = \left\{ \left(\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} \right), \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} \right) \right\}$$

como

$$\mathcal{B}_2 = \left\{ \left(\frac{3}{5}, \frac{4}{5} \right), \left(-\frac{4}{5}, \frac{3}{5} \right) \right\}$$

son dos bases formadas por vectores unitarios (versores) perpendiculares entre sí. Generalicemos esta situación:

Definición 10.12 Una base $\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ de $\mathbb{R}^n$ se dice *ortogonal* si $(\vec{v}_i, \vec{v}_j) = o$ para todo $i \neq j$. Si además $(\vec{v}_i, \vec{v}_i) = 1$ para todo $1 \leq i \leq n$ se dice *ortonormal*.

Observación 10.1 En verdad esta noción se puede hacer mucho más amplia. Si se define en un espacio vectorial una operación de las mismas características del producto escalar de $\mathbb{R}^n$ esta operación se llama *producto* *interno* y el espacio vectorial será un *espacio vectorial con producto interno* y en cualquier espacio vectorial con producto interno, de dimensión n, podemos definir la noción de base ortonormal como lo hemos hecho para $\mathbb{R}^n$ es decir, pidiendo:

$$(\vec{v}_i, \vec{v}_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{en otro caso.} \end{cases}$$

Veamos algo tan interesante como útil: Sea $\mathcal{B}$ una base ortonormal y pensemos en la matriz $[\mathcal{B}]_{\mathcal{C}}$. Las columnas de esta matriz son las coordenadas de los vectores que conforman la base. Multipliquemos $[\mathcal{B}]_{\mathcal{C}}^t$ por $[\mathcal{B}]_{\mathcal{C}}$:

$$[\mathcal{B}]_{\mathcal{C}}^t.[\mathcal{B}]_{\mathcal{C}} = (\vec{v}_i, \vec{v}_j) = I_n$$

Hagámoslo en $\mathbb{R}^2$:

$$\mathcal{B} = \{(v_{11}, v_{12}), (v_{21}, v_{22})\}, \text{ entonces } [\mathcal{B}]_{\mathcal{C}} = \begin{pmatrix} v_{11} & v_{21} \\ v_{12} & v_{22} \end{pmatrix}$$

$$[\mathcal{B}]_{\mathcal{C}}^t.[\mathcal{B}]_{\mathcal{C}} = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} . \begin{pmatrix} v_{11} & v_{21} \\ v_{12} & v_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} v_{11}.v_{11} + v_{12}.v_{12} & v_{11}.v_{21} + v_{12}.v_{22} \\ v_{21}.v_{22} + v_{21}.v_{22} & v_{21}.v_{21} + v_{22}.v_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Igualmente,

$$[\mathcal{B}]_{\mathcal{C}}.[\mathcal{B}]_{\mathcal{C}}^t = I_n,$$

Y esto se verifica no sólo para la base canónica, sino para la matriz de cambio de base entre dos bases ortonormales cualesquiera (Es un muy buen ejercicio para el lector interesado verificar esto)®
¡No más cálculos! Dadas dos bases ortonormales $\mathcal{B}_1$ y $\mathcal{B}_2$:

$$[\mathcal{B}_1]_{\mathcal{B}_2}^{-1} = [\mathcal{B}_1]_{\mathcal{B}_2}^t.$$

Observación 10.2 Una matriz A que satisface $A.A^t = A^t.A = I_n$ se dice una *matriz ortogonal*. Entonces, la matriz de cambio de base entre bases ortonormales es una matriz ortogonal.

10.1.4. Cambio de coordenadas

Pensemos en el plano ¿Cómo identificamos un punto? Fijamos dos ejes coordenados que se cortan en el origen. Podemos escribir el punto de coordenadas (x_0, y_0) como combinación lineal de los vectores de la base $\mathcal{C}_2$:

$$(x_0, y_0) = x_0.\breve{e}_1 + y_0.\breve{e}_2$$

y podemos pensar (porque en verdad es así) que los ejes coordenados son una suerte de "vector infinito" con la dirección y el sentido de los vectores que forman la base. (Por esta razón es que jamás podemos poner los ejes coordenados "con todas las flechitas para afuera".)
Llamamos sistema $(0, XY)$ al asociado a la base canónica y al asociado a otra base lo llamaremos $(0, X'Y')$ ó $(0, X''Y'')$. (ó $(0, X'Y'Z')$ si trabajáramos en $\mathbb{R}^3$.)

Ejemplo 10.9 Supongamos que tenemos un punto $P = \langle 1, 3\rangle$ en el sistema $(0, X'Y')$ asociado a la base

$$\mathcal{B} = \left\{ \left(\frac{3}{5}, \frac{4}{5}\right), \left(-\frac{4}{5}, \frac{3}{5}\right) \right\}$$

y queremos calcular las coordenadas de P en $(0, XY)$, simplemente hacemos el cambio de base considerando al punto P como el vector $\overrightarrow{0P}$:

$$[P]_{\mathcal{C}} = [\mathcal{B}]_{\mathcal{C}}[P]_{\mathcal{B}}.$$

Hagamos las cuentas:

$$[P]_{\mathcal{C}} = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{3}{5} & \frac{4}{5} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} -\frac{9}{5} \\ \frac{15}{5} \end{pmatrix}$$

Si hiciéramos las cuentas "a pulmón" quedaría:

$$\overrightarrow{0P} = 1.\left(\frac{3}{5}, \frac{4}{5}\right) + 3.\left(-\frac{4}{5}, \frac{3}{5}\right) = \left(1.\frac{3}{5} - 3.\frac{4}{5}\,,\, 1.\frac{4}{5} + 3.\frac{3}{5}\right) = \left(-\frac{9}{5}, \frac{15}{5}\right)$$

que es exactamente (y por suerte) el mismo resultado.

Cada vez que querramos pasar puntos o vectores realizamos este procedimiento y, por ejemplo, para pasar la ecuación de una recta dada en forma paramétrica, pasamos el punto, el vector y luego la reconstruímos en el otro sistema. Por ejemplo:

Ejemplo 10.10 Sea L una recta que en el sistema $(0, XY)$ tiene ecuación:

$$L = \begin{cases} x = 2 + \lambda, \\ y = 3 - 2\lambda \end{cases}, \lambda \in \mathbb{R}.$$

buscamos la expresión de la recta L en el sistema $(0, X'Y')$ asociado a la base $\mathcal{B} = \{(1, 2), (-1, -1)\}$.
Tenemos:

un punto P que lo consideramos como el vector $\overrightarrow{0P} = (2,3)$
y el vector director $\overrightarrow{d_L} = (1,-2)$.

Necesitamos la matriz de cambio de base:

$$[\mathcal{C}]_{\mathcal{B}} = [\mathcal{B}]_{\mathcal{C}}^{-1} = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix}.$$

$$[P]_{\mathcal{B}} = [\mathcal{B}]_{\mathcal{C}}^{-1}[P]_{\mathcal{C}} = \begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

$$[\overrightarrow{d_L}]_{\mathcal{B}} = [\mathcal{B}]_{\mathcal{C}}^{-1}[\overrightarrow{d_L}]_{\mathcal{C}} = \begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -2 \end{pmatrix} = \begin{pmatrix} -3 \\ -4 \end{pmatrix}.$$

y la ecuación paramétrica de L en el sistema $(0, X'Y')$ es:

$$L = \begin{cases} x' = 1 - 3\mu, \\ y' = -1 - 4\mu \end{cases}, \mu \in \mathbb{R}.$$

A partir de las ecuaciones paramétrica de L en $(0, XY)$ y en $(0, X'Y')$ podemos encontrar las ecuaciones implícitas, que son respectivamente:

$$L : 2\,x + y - 7 = 0 \qquad \text{y} \qquad L : 3\,x' - 4\,y' - 7 = 0.$$

También podríamos haber hecho el cambio de sistemas buscando las fórmulas de cambio, es decir:

$$[P]_{\mathcal{C}} = [\mathcal{B}]_{\mathcal{C}}.[P]_{\mathcal{B}}$$

nos permite escribir:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} . \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x' - y' \\ 2'x' - y' \end{pmatrix}$$

de donde:

$$\begin{cases} x = x' - y' \\ y = 2'x' - y' \end{cases}$$

Si reemplazamos x e y en la ecuación del sistema $(0, XY)$ por las fórmulas de cambio obtenemos:

$$L : 2\,x + y - 7 = 2.(x' - y') + (2'x' - y') - 7 = 4\,x' - 3\,y' - 7 = 0$$

Este método de buscar la fórmula de cambio y reemplazar las variables siempre es válido. Si hubiéramos querido rearmar la recta con el vector normal y un punto por el que pasa, como construimos vectorialmente la ecuación implícita de la recta incurriríamos en un error en tanto la base asociada al sistema $(0, X'Y')$ no sea ortonormal. En efecto:

$$[\overrightarrow{n_L}]_{\mathcal{B}} = [\mathcal{B}]_{\mathcal{C}}^{-1}[\overrightarrow{n_L}]_{\mathcal{C}} = \begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ -3 \end{pmatrix}.$$

Si la hacemos pasar por el punto $\langle 1, -1\rangle_{\mathcal{B}}$ queda: $L : -x' - 3\,y' - 2 = 0$ que, obviamente, no es la ecuación de L como se puede ver gráficamente.

Ejemplo 10.11 Sea $pi : 3\,x - 2\,y + z - 8 = 0$ la ecuación de un plano en el sistema $(0, XYZ)$ busquemos su ecuación en el sistema $(0, X'Y'Z')$ asociado a la base $\mathcal{B} = \{(\frac{\sqrt{3}}{2}, \frac{1}{2}, 0), (0, 0, 1), (-\frac{1}{2}, \frac{\sqrt{3}}{2}, 0)\}$
Busquemos las fórmulas de cambio:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2}\,x' - \frac{1}{2}\,z' \\ \frac{1}{2}\,'x' + \frac{\sqrt{3}}{2}\,z' \\ y' \end{pmatrix}$$

De donde:

$$\begin{cases} x = \frac{\sqrt{3}}{2}\,x' - \frac{1}{2}\,z' \\ y = \frac{1}{2}\,'x' + \frac{\sqrt{3}}{2}\,z' \\ z = y' \end{cases}.$$

Reemplazando en la ecuación del plano obtenemos:

$$\pi : 3\,(\frac{\sqrt{3}}{2}\,x' - \frac{1}{2}\,z') - 2\,(\frac{1}{2}\,'x' + \frac{\sqrt{3}}{2}\,z') + (y') - 8 =$$

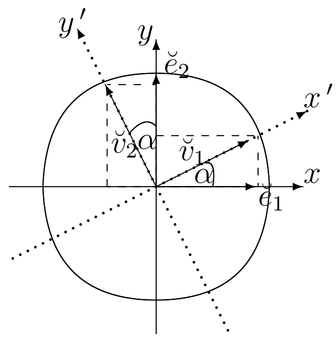
$$= \frac{3\sqrt{3} - 2}{2}\,x' + y' - \frac{3 + 2\sqrt{3}}{2}\,z' - 8 = 0$$

En este caso, si hubiéramos pasado el vector normal, las cuentas habrían dado bien. ®¿Por qué? dejamos la experimentación y la respuesta a cargo del lector.

Una observación interesante es notar que el término independiente permanece inmutable por estos cambios de base. ¿A qué se debe? sencillamente es porque el origen se ha quedado en el mismo sitio, hemos hecho un cambio de base, pero no una traslación.

Rotaciones

Busquemos la fórmula de cambio de base en $\mathbb{R}^2$ para una rotación de los vectores de la base en un ángulo α alrededor del origen, en sentido antihorario. Tomemos, porque es conveniente, una base normalizada, es decir con vectores de módulo 1. De este modo, si trazamos una circunferencia de radio 1, los extremos de los cuatro versores están en la circunferencia.



La coordenada del vector $\vec{v}_1$ según las abscisas es el cateto adyacente al ángulo α y la coordenada según las ordenadas es el cateto opuesto, en consecuencia el vector será:

$$\vec{v}_1 = (cos\,\alpha, sen\,\alpha)$$

Análogamente:
La coordenada del vector $\vec{v}_2$ según las abscisas es el cateto opuesto al ángulo α, pero tiene signo negativo y la coordenada según las ordenadas es el cateto adyacente, en consecuencia el vector será:

$$\vec{v}_1 = (-sen\,\alpha, cos\,\alpha).$$

Resulta entonces que

$$\mathcal{B} = \{(cos\,\alpha, sen\,\alpha), (-sen\,\alpha, cos\,\alpha)\}$$

y la matriz de cambio de base

$$[\mathcal{B}]_{\mathcal{C}} = \begin{pmatrix} cos\,\alpha & -sen\,\alpha \\ sen\,\alpha & cos\,\alpha \end{pmatrix}$$

Dado que se trata de una rotación de una base ortonormal, sigue siendo una base ortonormal y en consecuencia, la inversa de la matriz de cambio de base coincide con su transpuesta.

Ejemplo 10.12 Dada la recta $L : 2\,x + y = 0$ hallar su expresión en el sistema $(O, X'Y')$, que se obtiene rotando el (O, XY) un ángulo de $\pi/3$ alrededor del origen, en sentido positivo.

$$[P]_{\mathcal{C}} = [\mathcal{B}]_{\mathcal{C}}.[P]_{\mathcal{B}}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} cos\,\pi/3 & -sen\,\pi/3 \\ sen\,\pi/3 & cos\,\pi/3 \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} (x' - 3\,y')/2 \\ (3\,x' + y')/2 \end{pmatrix}$$

Reemplazamos:

$$L : 2\,x + y = 2\,(x' - 3\,y')/2 + (3\,x' + y')/2 = (5\,x' - 5\,y')/2 = 0$$

que se puede escribir:

$$L : x' - \, y' = 0.$$

Las rotaciones en $\mathbb{R}^3$ las vamos a pensar siempre como composiciones de rotaciones alrededor de un eje. Claramente el eje alrededor del que se rota es fijo y así las matrices de cambio de base por rotación en un ángulo α en sentido positivo serán

alrededor del eje X	alrededor del eje Y	alrededor del eje Z
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & cos\,\alpha & -sen\,\alpha \\ 0 & sen\,\alpha & cos\,\alpha \end{pmatrix}$	$\begin{pmatrix} cos\,\alpha & 0 & -sen\,\alpha \\ 0 & 1 & 0 \\ sen\,\alpha & 0 & cos\,\alpha \end{pmatrix}$	$\begin{pmatrix} cos\,\alpha & -sen\,\alpha & 0 \\ sen\,\alpha & cos\,\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Ejemplo 10.13 Dada la recta $L : (1,2,4) + \lambda(3,-1-1); \lambda \in \mathbb{R}$ en el sistema (O, XYZ) dar su ecuación en el sistema $(O, X'Y'Z')$ que se obtiene al girar la base canónica $\pi/4$ alrededor del eje y.
Como la recta está dada en forma vectorial con conviene pasar punto y vector director de $\mathcal{C}$ a $\mathcal{B}$.

$$[\mathcal{C}]_{\mathcal{B}} = [\mathcal{B}]^t_{\mathcal{C}} = \begin{pmatrix} \sqrt{2}/2 & 0 & \sqrt{2}/2 \\ 0 & 1 & 0 \\ -\sqrt{2}/2 & 0 & \sqrt{2}/2 \end{pmatrix}.$$

$$[P]_{\mathcal{B}} = [\mathcal{B}]^t_{\mathcal{C}}[P]_{\mathcal{C}} = \begin{pmatrix} \sqrt{2}/2 & 0 & \sqrt{2}/2 \\ 0 & 1 & 0 \\ -\sqrt{2}/2 & 0 & \sqrt{2}/2 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 5\sqrt{2}/2 \\ 2 \\ 3\sqrt{2}/2 \end{pmatrix}.$$

$$[\overrightarrow{d_L}]_{\mathcal{B}} = [\mathcal{B}]^t_{\mathcal{C}}[\overrightarrow{d_L}]_{\mathcal{C}} = \begin{pmatrix} \sqrt{2}/2 & 0 & \sqrt{2}/2 \\ 0 & 1 & 0 \\ -\sqrt{2}/2 & 0 & \sqrt{2}/2 \end{pmatrix} \begin{pmatrix} 3 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} \sqrt{2} \\ -1 \\ -2\sqrt{2} \end{pmatrix}.$$

y la ecuación paramétrica de L en el sistema $(0, X'Y')$ es:

$$L_{\mathcal{B}} : (\,5\sqrt{2}/2, 2, 3\sqrt{2}/2\,) + \mu(\sqrt{2}, -1, -2\sqrt{2}); \mu \in \mathbb{R}.$$

Traslación del origen

Supongamos que tenemos una traslación del origen al punto O. En cada sistema de coordenadas asociamos el punto P al vector $\overrightarrow{OP}$. Al cambiar el origen a O' debemos asociarlos al vector $\overrightarrow{O'P}$. Como $\overrightarrow{O'P} = \overrightarrow{OP} - \overrightarrow{OO'}$ resultan las fórmulas de traslación, respectivamente en $\mathbb{R}^2$ y $\mathbb{R}^3$:

$$\text{En } \mathbb{R}^2 : O' = (x_0, y_0) \qquad \begin{cases} x' = x - x_0 \\ y' = y - y_0 \end{cases}, \qquad \begin{cases} x = x' + x_0 \\ y = y' + y_0 \end{cases}$$

$$\text{En } \mathbb{R}^3 : O' = (x_0, y_0, z_0) \qquad \begin{cases} x' = x - x_0 \\ y' = y - y_0 \\ z' = z - z_0 \end{cases}, \qquad \begin{cases} x = x' + x_0 \\ y = y' + y_0 \\ z = z' + z_0 \end{cases}$$

Ejemplo 10.14 Traslademos en $\mathbb{R}^2$ el origen a $(1, -4)$ y busquemos en el sistema $(O'XY)$ la ecuación de la recta $L : x - y = 0$.
Reemplazando por las fórmulas de cambio queda:

$$L : (x' + 1) - (y' - 4) = x' - y' + 5 = 0$$

No es para extrañarse que no haya cambiado el vector normal a la recta. La base no cambió. Como hubo un traslado cambió el término independiente.

Traslación y cambio de base

Claramente si podemos trasladar el origen y podemos cambiar la base podemos trasladar y cambiar la base. Esto puede hacerse en dos pasos, o bien con una única operación matricial. Si nos dan las coordenadas del nuevo origen en la base canónica, para ir de sistema original a la nueva base trasladada, simplemente primero hacemos la traslación y luego el cambio de base. Si queremos volver a la canónica, primero hacemos el cambio de base y luego la traslación. Así, las "fórmulas integradas" son:

En $\mathbb{R}^2 : O' = (x_0, y_0)$

$$\begin{pmatrix} x'' \\ y'' \end{pmatrix} = [\mathcal{B}]_{\mathcal{C}}^{-1} . \begin{pmatrix} x - x_0 \\ y - y_0 \end{pmatrix}, \qquad \begin{pmatrix} x \\ y \end{pmatrix} = [\mathcal{B}]_{\mathcal{C}} \begin{pmatrix} x'' \\ y'' \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

En $\mathbb{R}^3 : O' = (x_0, y_0, z_0)$

$$\begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix} = [\mathcal{B}]_{\mathcal{C}}^{-1} . \begin{pmatrix} x - x_0 \\ y - y_0 \\ z - z_0 \end{pmatrix}, \qquad \begin{pmatrix} x \\ y \\ z \end{pmatrix} = [\mathcal{B}]_{\mathcal{C}} \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$$

Ejemplo 10.15 Sea $\pi : 3\,x + 2\,z - 3 = 0$ la ecuación de un plano en el sistema (O, XYZ).
Hallar la ecuación de π en el sistema $(O, X''Y''Z'')$ asociado a la base

$$\mathcal{B} = \{(1,2,1),(0,0,-1),(-1,2,2)\} \text{ con origen en } O' = (3,3,1)$$

.Según las fórmulas que acabamos de ver:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 0 & 2 \\ 1 & -1 & 2 \end{pmatrix} \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix} + \begin{pmatrix} 3 \\ 3 \\ 1 \end{pmatrix}$$

Entonces:

$$\begin{cases} x = x'' - z'' + 3 \\ y = 2\,x'' + 2\,z'' + 3 \\ z = x'' - y'' + 2\,z'' + 1 \end{cases}$$

Reemplazando en la ecuación resulta:

$$\pi : 3\,(x'' - z'' + 3) + 2\,(x'' - y'' + 2\,z'' + 1) - 3 = 0$$

Es decir:

$$\pi : 5\,x'' - 2\,y'' + z'' + 8 = 0.$$

10.2. Transformaciones Lineales

Hemos trabajado con conjuntos y nos es familiar la noción de función. Ahora tenemos entre manos espacios vectoriales, es decir, conjuntos pero ahora munidos de dos operaciones. Nos van a interesar las funciones, pero no todas ellas, sino las que respeten las operaciones definidas: la suma interna y el producto externo. Más precisamente:

Definición 10.13 Dados dos $\mathbb{K}$-espacios vectoriales V y W, una función $T : V \to W$ se dice una *transformación lineal* si para todo $\vec{u}, \vec{v} \in V, \lambda \in \mathbb{K}$ se verifica:

$T_1 :\ T(\vec{u} + \vec{v}) = T(\vec{u}) + T(\vec{v})$

$T_2 :\ T(\lambda\vec{u}) = \lambda\,\vec{u}.$

Podemos justificar plenamente la denominación transformación lineal, ya que en un espacio vectorial las operaciones que podemos hacer son combinaciones lineales y esta función es una transformación que las respeta. De la definición podemos deducir que $T(\vec{0}) = \vec{0}$.
En efecto:

$$T(\vec{0}) = T(\vec{0}+\vec{0}) \qquad \text{(por: } \vec{0}=\vec{0}+\vec{0}\text{)}$$
$$T(\vec{0}) = T(\vec{0}) + T(\vec{0}) \qquad \text{(por } T_1\text{)}$$
$$\vec{0} + T(\vec{0}) = T(\vec{0}) + T(\vec{0}) \qquad \text{(porque } \vec{0} \text{ es el neutro)}$$
$$\vec{0} = T(\vec{0}) \qquad \text{(por propiedad cancelativa)}$$

Entonces si una cierta función es transformación lineal, debe cumplir esto. Si no lo cumple no es transformación lineal. Si sí lo cumple puede ser que lo sea o no.

Observación 10.3 Probamos que en cualquier transformación lineal $T(\vec{0}) = \vec{0}$, pero lo hemos hecho con un procedimiento bastante "complicado". Hay un camino más directo, desafiamos a los lectores entusiastas a salir en su busca.®

Ejemplo 10.16 Veamos algunos ejemplos:

1. $T_1 : \mathbb{R}^2 \to \mathbb{R}^3$ definida por $T_1((x,y)) = (x, x+y, 2y)$.
   Claramente $T_1((0,0)) = (0,0,0)$. Veamos que respeta la suma y el producto:
   Sean $(x,y), (x', y') \in \mathbb{R}^2$. Calculemos $T((x,y)) + T((x',y'))$ y $T((x+x', y+y'))$ y veamos que son iguales:
   $T((x,y)) + T((x',y')) =$
   $= (x, x+y, 2y) + (x', x'+y', 2y') =$
   $= (x+x', (x+y)+(x'+y'), 2(y+2y'))$ (A)
   $T((x+x', y+y')) =$
   $= (x+x', (x+x')+(y+y'), 2(y+2y'))$
   $= (x+x', (x+y)+(x'+y'), 2(y+2y'))$ (B)
   (A)=(B) y respeta la suma.
   $T(\lambda(x,y)) = T((\lambda x, \lambda y)) = (\lambda x, \lambda x + \lambda y, 2\,\lambda y) = \lambda(x, x+y, 2\,y) = \lambda T(x,y)$.
   Concluimos que T_1 es una transformación lineal.

2. $T_2 : M_2(\mathbb{R}) \to \mathbb{R}$ definida por $T_2(A) = |A|$.
   Sabemos que el determinante de la matriz nula es cero, pero también sabemos que $|A+B| \neq |A| + |B|$ y $|\lambda A| \neq \lambda |A|$, en conclusión T_2 no es transformación lineal.

3. $T_3 : \mathbb{R}^2 \to \mathbb{R}^2$ definida por $T_3((x,y)) = (x^2, y)$ no es transformación lineal, ya que $3.T_3((2,1)) = 3.(4,1) = (12,3) \neq (36,3) = T(3.(2,1))$

Pongámonos en una situación muy conveniente, pero no por eso poco frecuente. Sea $T : V \to W$ una transformación lineal, que V y W $\mathbb{K}$-espacios vectoriales de dimensión finita. Sea $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ una base de V y

supongamos que conocemos los vectores $T(\vec{b}_1), T(\vec{b}_2), \ldots, T(\vec{b}_n)$, entonces conocemos $T(\vec{v})$ cualquiera que sea $\vec{v} \in V$.
En efecto: $\vec{v}$ se escribe de forma única como combinación lineal de los vectores de la base $\mathcal{B}$:

$$\vec{v} = \lambda_1 \vec{b}_1 + \lambda_2 \vec{b}_2 + \ldots + \lambda_n \vec{b}_n$$

y la transformación repeta las combinaciones lineales, entonces:

$$\begin{aligned} T(\vec{v}) &= \\ &= T(\lambda_1 \vec{b}_1 + \lambda_2 \vec{b}_2 + \ldots + \lambda_n \vec{b}_n) = \\ &= T(\lambda_1 \vec{b}_1) + T(\lambda_2 \vec{b}_2) + \ldots + T(\lambda_n \vec{b}_n) = \\ &= \lambda_1 T(\vec{b}_1) + \lambda_2 T(\vec{b}_2) + \ldots + \lambda_n T(\vec{b}_n). \end{aligned} \tag{10.5}$$

veamos un ejemplo.

Ejemplo 10.17 Sea $T : M_2(\mathbb{R}) \to \mathbb{R}$ tal que:

$T\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) = 1,\ T\left(\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\right) = 1,\ T\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) = 0,\ T\left(\begin{pmatrix} 0 & 1 \\ -2 & 0 \end{pmatrix}\right) = 0.$

Son cuatro matrices linealmente independientes en un espacio de dimensión 4, entonces generan el espacio. Podemos resolver el sistema para obtener:

$$\begin{pmatrix} x & z \\ y & t \end{pmatrix} = (x - y - 2z + t) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + (y + 2z) \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} +$$

$$+(y + 2z - t) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + z \begin{pmatrix} 0 & 1 \\ -2 & 0 \end{pmatrix}$$

Y podemos calcular

$$\begin{aligned} T\left(\begin{pmatrix} x & z \\ y & t \end{pmatrix}\right) &= (x-y-2z+t).T\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) + (y+2z).T\left(\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\right) + \\ &+ (y + 2z - t).T\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) + z.T\left(\begin{pmatrix} 0 & 1 \\ -2 & 0 \end{pmatrix}\right) = \\ &= (x - y - 2z + t).1 + (y + 2z).1 + (y + 2z - t).0 + z.0 = x + t. \end{aligned}$$

Podemos notar que la transformación lineal que acabamos de encontrar es única, ya que la forma de escribir cada vector del espacio como combinación lineal de los vectores de una base, es única. De hecho, enunciaremos un teorema que lo afirma:

Teorema 10.1 *Sean* $(V, +, .)$ *y* $(W, +, .)$ *dos* $\mathbb{K}$*-espacios vectoriales. Si* $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ *es una base de* V *y conocemos* $\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_n \in W$*, entonces existe una única transformación lineal* $T : V \to W$ *tal que* $T(\vec{b}_i) = \vec{w}_i$*,* $1 \leq i \leq n$*.*

Si miramos la igualdad escrita en 10.5 pensando en cálculo matricial, vemos que se trata del producto de una matriz cuyas columnas son los transformados de los vectores de la base, con la matriz columna formada por las coordenadas del vector. Veámoslo en un ejemplo.

Ejemplo 10.18 Sea $T : \mathbb{R}^3 \to \mathbb{R}^2$ tal que $T((1,0,0)) = (3,4),\ T((0,1,0)) = (1,6)$ y $T((0,0,1)) = (5,2)$.

$$(x,y,z) = x.(1,0,0) + y.(0,1,0) + z.(0,0,1)$$

$$T((x,y,z)) = x.T((1,0,0)) + y.T((0,1,0)) + z.T((0,0,1))$$

$$T((x,y,z)) = x.(3,4) + y.(1,6) + z.(5,2)$$

$$T((x,y,z)) = (3.x + 1.y + 5.z, 4.x + 6.y + 2.z)$$

$$\begin{pmatrix} T(x) \\ T(y) \\ T(z) \end{pmatrix} = \begin{pmatrix} 3 & 1 & 5 \\ 4 & 6 & 2 \end{pmatrix} . \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

En este ejemplo vemos claramente que la primera columna es el transformado del primer vector de la base, la segunda columna el transformado del segundo y en la tercera columna encontramos el transformado del tercer vector.
Estas observaciones nos llevan a dar la siguiente definición:

Definición 10.14 Sean $(V,+,.)$ y $(W,+,.)$ dos $\mathbb{K}$-espacios vectoriales de dimensión finita. $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ y $\mathcal{B}' = \{\vec{b}'_1, \vec{b}'_2, \ldots, \vec{b}'_m\}$ bases ordenadas respectivamente de V y W y $T : V \to W$ una transformación lineal.
El transformado de cada $\vec{b}_i$ es un vector en W, por eso se escribe como combinación lineal de los vectores $\vec{b}'_1, \vec{b}'_2, \ldots, \vec{b}'_m$:

$$\begin{aligned} T(\vec{b}_1) &= a_{11}\vec{b}'_1 + a_{21}\vec{b}'_2 + \ldots + a_{m1}\vec{b}'_m \\ T(\vec{b}_2) &= a_{21}\vec{b}'_1 + a_{22}\vec{b}'_2 + \ldots + a_{m2}\vec{b}'_m \\ &\ldots \\ T(\vec{b}_n) &= a_{n1}\vec{b}'_1 + a_{n2}\vec{b}'_2 + \ldots + a_{mn}\vec{b}'_m \end{aligned}$$

Si escribimos estos coeficientes a_{ij} por columna, obtenemos una matriz de m filas y n columnas que es la matriz de la transformación de los vectores de la base $\mathcal{B}$ como combinación lineal de los vectores de la base $\mathcal{B}'$:

$$[T]_{\mathcal{B}\mathcal{B}'} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

De este modo podemos escribir:

$$[T(\vec{v})]_{\mathcal{B}'} = [T]_{\mathcal{B}\mathcal{B}'}[\vec{v}]_{\mathcal{B}}.$$

Cuando la matriz tiene por columnas los transformados de los vectores de una base $\mathcal{B}$ como combinación de la misma base $\mathcal{B}$, en lugar de $[T]_{\mathcal{B}\mathcal{B}}$, simplemente escribimos $[T]_{\mathcal{B}}$.

Veamos un ejemplo de construcción de la matriz de la transformación:

Ejemplo 10.19 Sean $\mathcal{B} = \{(1,2),(-1,1)\}$ y $\mathcal{B}' = \{(1,1,1),(0,1,1),(0,0,1)\}$, respectivamente bases de $\mathbb{R}^2$ y $\mathbb{R}^3$ y consideremos la transformación T tal que $T((1,2)) = (2,0,3)$ y $T((-1,1)) = (5,3,2)$.
$(2,0,3)_{\mathcal{C}} = \langle 2,-2,3\rangle_{\mathcal{B}'}$, $(5,3,2)_{\mathcal{C}} = \langle 5,-2,-1\rangle_{\mathcal{B}'}$.
La matriz de la transformación de $\mathcal{B}$ en $\mathcal{B}'$ es:

$$[T]_{\mathcal{B}\mathcal{B}'} = \begin{pmatrix} 2 & 5 \\ -2 & -2 \\ 3 & -1 \end{pmatrix} \in M_{3\times 2}(\mathbb{R}).$$

Calculemos $T((0,3))$. $(0,3) = (1,2) + (-1,1)$, entonces $(0,3)_{\mathcal{C}} = (1,1)_{\mathcal{B}}$:

$$[T((1,1))]_{\mathcal{B}'} = \begin{pmatrix} 2 & 5 \\ -2 & -2 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}_{\mathcal{B}} = \begin{pmatrix} 7 \\ -4 \\ 2 \end{pmatrix}_{\mathcal{B}'}.$$

Esto quiere decir que $T(0,3) = 7.(1,1,1) - 4.(0,1,1) + 2.(0,0,1) = (7,3,5)$.

Hagamos estos cálculos sin usar para nada matrices:

$$T((0,3)) = T(1.(1,2) + 1.(-1,1)) =$$

$$= 1.T((1,2)) + 1.T((-1,1)) =$$

$$= 1.(2,0,3) + 1.(5,3,2) = (7,3,5).$$

Hagamos estos cálculos usando matrices de cambio de base:
Recordemos que $[\mathcal{B}_1]_{\mathcal{B}_2}[\vec{v}]_{\mathcal{B}_1} = [\vec{v}]_{\mathcal{B}_2}$.
Para tener todos los vectores en la base adecuada debemos en primer lugar llevar el vector de la base canónica a la base $\mathcal{B}$, luego hacemos la transformación que nos lleva de la base $\mathcal{B}$ a la base $\mathcal{B}'$ y finalmente debemos hacer el cambio de base de $\mathcal{B}'$ a la base canónica: (Recordemos siempre que estamos haciendo composición de funciones, y entonces todos los pasos que mencionamos se escriben "para atrás".)

$$[T(\vec{v})]_{\mathcal{C}} = [\mathcal{B}']_{\mathcal{C}}.[T]_{\mathcal{B}\mathcal{B}'}.[\mathcal{C}]_{\mathcal{B}}.[\vec{v}]_{\mathcal{C}} \tag{10.6}$$

$$[T(\vec{v})]_{\mathcal{C}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} 2 & 5 \\ -2 & -2 \\ 3 & -1 \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}^{-1} . \begin{pmatrix} 0 \\ 3 \end{pmatrix} =$$

$$[T(\vec{v})]_{\mathcal{C}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} 2 & 5 \\ -2 & -2 \\ 3 & -1 \end{pmatrix} . \left(\begin{pmatrix} 1/3 & 1/3 \\ -2/3 & 1/3 \end{pmatrix} . \begin{pmatrix} 0 \\ 3 \end{pmatrix} \right) =$$

$$[T(\vec{v})]_{\mathcal{C}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} 2 & 5 \\ -2 & -2 \\ 3 & -1 \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \end{pmatrix} =$$

$$[T(\vec{v})]_{\mathcal{C}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} 7 \\ -4 \\ 2 \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \\ 5 \end{pmatrix}.$$

¿Cuál es el mejor método para la obtención de $T(\vec{v})$? El que más le complazca al usuario. Claramente el cálculo matricial es el más práctico, pero tiene sentido sólo si se entiende el proceso realizado.

En 10.6 hemos dado la fórmula completa para el cálculo de $T(\vec{v})$. Simplemente la matriz de la transformación en la base canónica, si conocemos la matriz de la transformación de una base $\mathcal{B}$ en una base $\mathcal{B}'$ es:

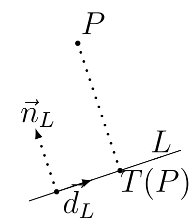
$$[T]_{\mathcal{C}} = [\mathcal{B}']_{\mathcal{C}}.[T]_{\mathcal{B}\mathcal{B}'}.[\mathcal{C}]_{\mathcal{B}}. \tag{10.7}$$

10.2.1. Transformaciones lineales con base adecuada

La fórmula que acabamos de ver en 10.7 es de gran utilidad para encontrar la expresión de una transformación lineal cuando conocemos los transformados de los vectores de una base.

Ejemplo 10.20 Veamos diferentes casos:

1. Hallar la expresión de una transformación lineal que a cada punto del plano le asocia su proyección sobre la recta $y = 2x$.
   En primer lugar, verifiquemos que la recta sobre la que se hace la proyección pase por el origen. Si esto no fuera así, $T(\vec{0}) \neq \vec{0}$ y la aplicación no sería una transformación lineal.
   Como es una transformación en $\mathbb{R}^2$ necesitamos dos vectores. El paso más importante en este tipo de ejercicios es encontrar los vectores que formarán la base, de los que conoceremos cuál será su transformado sin hacer cuentas.
   Dejemos de lado los valores particulares del ejercicio y pensemos simplemente en la proyección (si nadie aclara nada será ortogonal) sobre una recta, digamos L. ¿Qué vectores tenemos a disposición? Claramente el director de la recta, llamémoslo $\vec{d}_L$ y el normal a la recta $\vec{n}_L$. La proyección consiste en llevar "dentro" de la recta los puntos que están "fuera". Si fijamos el director y el normal en el origen (ya que la recta pasa por el origen) conformamos una base. El extremo del vector director en un punto de la propia recta y, en consecuencia, invariante. El extremo del vector normal, en forma ortogonal, proyecta justamente sobre su origen, entonces:



   $T(\vec{d}_L) = \vec{d}_L = 1.\vec{d}_L + 0.\vec{n}_L$
   $T(\vec{n}_L) = \vec{0} = 0.\vec{d}_L + 0.\vec{n}_L$

   Ponemos, entonces la base ordenada $\mathcal{B} = \{\vec{d}_L, \vec{n}_L\}$ y resulta

$$[T]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

   Por la fórmula 10.7 podemos calcular

$$[T]_{\mathcal{C}} = [\mathcal{B}]_{\mathcal{C}}.[T]_{\mathcal{B}}.[\mathcal{C}]_{\mathcal{B}}.$$

   Ahora sí, volvamos a los números: $\vec{d}_L = (1, 2)$ y $\vec{n}_L = (-2, 1)$. Como ya son perpendiculares, nos conviene definir una base ortonormal, para evitar el cálculo de la matriz inversa y la fórmula queda:

$$[T]_{\mathcal{C}} = [\mathcal{B}]_{\mathcal{C}}.[T]_{\mathcal{B}}.[\mathcal{B}]^t_{\mathcal{C}}.$$

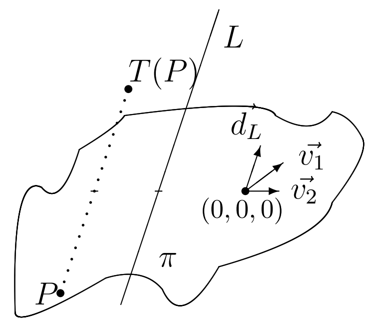
   $\mathcal{B} = \{(1/\sqrt{5}, 2/\sqrt{5}), (-2/\sqrt{5}, 1\sqrt{5})\}$

$$[T]_{\mathcal{C}} = \begin{pmatrix} 1/\sqrt{5} & -2/\sqrt{5} \\ 2/\sqrt{5} & 1\sqrt{5} \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 1/\sqrt{5} & 2/\sqrt{5} \\ -2/\sqrt{5} & 1\sqrt{5} \end{pmatrix} = \begin{pmatrix} 1/5 & 2/5 \\ 2/5 & 4/5 \end{pmatrix}.$$

Para encontrar la expresión de la transformación simplemente escribimos

$$[T(x,y)]_{\mathcal{C}} = [T]_{\mathcal{C}}.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1/5 & 2/5 \\ 2/5 & 4/5 \end{pmatrix}.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \dfrac{x+2y}{5} \\ \dfrac{2x+4y}{5} \end{pmatrix}.$$

2. Busquemos la expresión de una transformación que a cada punto del espacio le hace corresponder el simétrico con respecto a un plano en la dirección de una recta.
¿En qué consiste la transformación?
Dado cualquier punto P del espacio, debemos hacer pasar por ese punto una recta L_P paralela a la recta dada y encontrar el punto $T(P)$ que pertenece a la recta L_P y dista del plano lo mismo que P. Igual que antes, el plano debe pasar por el origen. Allí ubicamos el origen de los tres vectores que serán la base adecuada. El transformado del director de la recta será claramente un vector de sentido contrario y el transformado de cualquier vector que pertenezca al plano, será el mismo vector. De este modo:



$\mathcal{B} = \{\vec{d_L}, \vec{v_1}, \vec{v_2}\}$, $\vec{v_1}, \vec{v_2}$ son vectores linealmente independientes en el plano π.

$$\begin{aligned} T(\vec{d_L}) = -\vec{d_L} &= -1.\vec{d_L} + 0.\vec{v_1} + 0.\vec{v_2} \\ T(\vec{v_1}) \ = \ \vec{v_1} \ &= \ 0.\vec{d_L} + 1.\vec{v_1} + 0.\vec{v_2} \\ T(\vec{v_1}) \ = \ \vec{v_1} \ &= \ 0.\vec{d_L} + 0.\vec{v_1} + 1.\vec{v_2} \end{aligned}$$

La matriz de la transformación es, entonces:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

independientemente de cuál sea elplano o la recta.
Sean, ahora, $\pi : 2\,x + y - z = 0$ y $L : (1,0,0) + \lambda.(2,1,1)$, $\lambda \in \mathbb{R}$.
En primer lugar verificamos que $(0,0,0) \in \pi$ y que $L \not\parallel \pi$, o lo que es lo mismo $(\vec{d_L}, n_\pi) \neq 0$. Dado que $\vec{d_L} \not\parallel \vec{n}_\pi$ no se puede construir una base ortonormal, entonces simplemente buscaremos dos vectores linealmente independientes en el plano. Como el plano pasa por el origen cualquier

punto puede representar un vector. Más exactamente, pensamos al punto P como el vector $\overrightarrow{OP}$. Sea

$$\mathcal{B} = \{(2,1,1),(0,1,1),(1,1,-1)\}$$

que efectivamente es base ya que:

$$\begin{vmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & \text{-1} \end{vmatrix} = -4 \neq 0$$

Apliquemos la fórmula para encontrar la matriz de la transformación en la base canónica:

$$[T]_{\mathcal{C}} = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} . \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix}^{-1}$$

$$[T]_{\mathcal{C}} = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} . \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 2/4 & -1/4 & 1/4 \\ -2/4 & 3/4 & 1/4 \\ 0 & 2/4 & -2/4 \end{pmatrix}$$

$$[T]_{\mathcal{C}} = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} . \begin{pmatrix} -2/4 & 1/4 & -1/4 \\ -2/4 & 3/4 & 1/4 \\ 0 & 2/4 & -2/4 \end{pmatrix} = \begin{pmatrix} -1 & 1 & -1 \\ -1 & 3/2 & -1/2 \\ -1 & 1/2 & 1/2 \end{pmatrix}$$

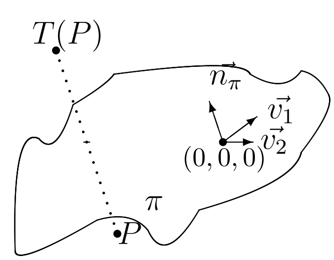
Para encontrar la expresión de la transformación multiplicamos la matriz de T en la base canónica por (x,y,z):

$$\begin{pmatrix} -1 & 1 & -1 \\ -1 & 3/2 & -1/2 \\ -1 & 1/2 & 1/2 \end{pmatrix} . \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -x+y-z \\ -x+\frac{3}{2}y-\frac{1}{2}z \\ -x-\frac{1}{2}y-\frac{1}{2}z \end{pmatrix}.$$

$$T((x,y,z)) = \left(-x+y-z, -x+\frac{3}{2}y-\frac{1}{2}z, -x-\frac{1}{2}y-\frac{1}{2}z\right)$$

3. Busquemos la expresión de una transformación que a cada punto del espacio le hace corresponder el simétrico con respecto a un plano.

   ¿En qué consiste la transformación?
   Esencialmente es igual al ejemplo anterior, pero en este caso la simetría es en la dirección ortogonal al plano. Es decir, en lugar del vector director de la recta tomamos el vector normal al plano y podemos armar una base ortonormal. Para ello buscamos un vector en el plano y el tercer vector de la base lo obtenemos como el producto vectorial entre los anteriores. (¿Es seguro que este vector va a pertenecer al plano?)



$\mathcal{B} = \{\vec{n}_\pi, \vec{v}_1, \vec{v}_2 = \vec{n}_\pi \wedge \vec{v}_1\}$, $\vec{v}_1$ en el plano π.

$$\begin{array}{lcl} T(\vec{n}_\pi) = -\vec{n}_\pi & = & -1.\vec{n}_\pi + 0.\vec{v}_1 + 0.\vec{v}_2 \\ T(\vec{v}_1) \;=\; \vec{v}_1 & = & 0.\vec{n}_\pi + 1.\vec{v}_1 + 0.\vec{v}_2 \\ T(\vec{v}_2) \;=\; \vec{v}_1 & = & 0.\vec{n}_\pi + 0.\vec{v}_1 + 1.\vec{v}_2 \end{array}$$

La matriz de la transformación coincide, claramente, con la del ejemplo anterior:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Sea, ahora, $\pi : 3\,x - 4\,z = 0$.
En primer lugar verificamos que $(0,0,0) \in \pi$
$\vec{n}_\pi = (3,0,-4)$, un vector en π: $\vec{v}_1 = (0,1,0)$, entonces $\vec{v}_2 = \vec{n}_\pi \wedge \vec{v}_1 = (4,0,3)$. Hasta aquí tenemos tres vectores perpendiculares dos a dos, para armar la base ortonormal, dividimos cada uno de ellos por su módulo:

$$\mathcal{B} = \{(3/5,0,-4/5),(0,1,0),(4/5,0,3/5)\}$$

Apliquemos la fórmula para encontrar la matriz de la transformación en la base canónica, recordando que la inversa de la matriz de cambio de base entre bases ortonormales coincide con la transpuesta:

$$[T]_{\mathcal{C}} = \begin{pmatrix} 3/5 & 0 & 4/5 \\ 0 & 1 & 0 \\ -4/5 & 0 & 3/5 \end{pmatrix} . \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 3/5 & 0 & 4/5 \\ 0 & 1 & 0 \\ -4/5 & 0 & 3/5 \end{pmatrix}^t$$

$$[T]_{\mathcal{C}} = \begin{pmatrix} 3/5 & 0 & 4/5 \\ 0 & 1 & 0 \\ -4/5 & 0 & 3/5 \end{pmatrix} . \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 3/5 & 0 & -4/5 \\ 0 & 1 & 0 \\ 4/5 & 0 & 3/5 \end{pmatrix}$$

$$[T]_{\mathcal{C}} = \begin{pmatrix} 3/5 & 0 & 4/5 \\ 0 & 1 & 0 \\ -4/5 & 0 & 3/5 \end{pmatrix} . \begin{pmatrix} -3/5 & 0 & 4/5 \\ 0 & 1 & 0 \\ 4/5 & 0 & 3/5 \end{pmatrix} = \begin{pmatrix} 7/25 & 0 & 24/25 \\ 0 & 1 & 0 \\ 24/25 & 0 & -7/25 \end{pmatrix}$$

Para encontrar la expresión de la transformación multiplicamos la matriz de T en la base canónica por (x,y,z):

$$\begin{pmatrix} 7/25 & 0 & 24/25 \\ 0 & 1 & 0 \\ 24/25 & 0 & -7/25 \end{pmatrix} . \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{7\,x+24\,z}{25} \\ y \\ \frac{24\,x-7\,z}{25} \end{pmatrix}.$$

$$T((x,y,z)) = \left(\frac{7\,x+24\,z}{25}, y, \frac{24\,x-7\,z}{25} \right)$$

10.3. Ejercicios propuestos

10.3.1. Espacios y subespacios vectoriales

Ejercicio 10.1 Determinar si es un espacio vectorial $V = \mathbb{R}^2$, con las operaciones:
$(x, y) + (x', y') = (x + x', y + y')$ y $k \cdot (x, y) = (0, 0)$, para todo $k \in \mathbb{R}$.

Ejercicio 10.2 Verificar que $\mathbb{R}^n$ es un $\mathbb{R}$ espacio vectorial. ¿$\mathbb{C}^n$ es $\mathbb{R}$ espacio vectorial? ¿$\mathbb{R}^n$ es $\mathbb{C}$ espacio vectorial?

Ejercicio 10.3 (Ⓡ) Sea V un espacio vectorial real, demostrar:

1. $0 \cdot \vec{v} = \vec{0}$, para todo $\vec{v} \in V$.
2. Si $\vec{u} + \vec{v} = \vec{u} + \vec{w}$, entonces $\vec{v} = \vec{w}$.
3. El elemento neutro respecto de la adición es único.

Ejercicio 10.4 Determinar en cada caso, si W_i es subespacio de V_i

1. $V_1 = M_{2\times 2}[\mathbb{R}]$, $\quad W_1 = \left\{ \begin{pmatrix} a & a+b \\ a+b & b \end{pmatrix} \in V_1 \right\}$,
2. $V_3 = \mathbb{P}_3[x]$, $\quad W_3 = \{a \cdot x^3 + b : a, c \in \mathbb{R}^+\}$,
3. $V_3 = \mathbb{P}_3[x]$, $\quad W_3 = \{a \cdot x^2 + b : a, c \in \mathbb{R}\}$,
4. $V_4 = \mathbb{R}^4$, $\quad W_4$ el conjunto de soluciones de $\begin{cases} x + y + z - t = 2 \\ z - t = 0 \end{cases}$,

Ejercicio 10.5 ⓒ Probar que el conjunto de todas las combinaciones lineales de los vectores $\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n$ de un espacio vectorial V, es subespacio vectorial de V.

10.3.2. Dependencia lineal

Ejercicio 10.6 Determinar si los siguientes conjuntos de vectores son linealmente independientes. En caso de no serlo expresar, si es posible, cada uno de ellos como combinación lineal de los otros. Justificar, teniendo en cuanta la dimensión del espacio vectorial.

1. $\vec{v}_1 = (-1, 0, 1)$, $\vec{v}_2 = (2, 2, 2)$, $\vec{v}_3 = (-3, -2, -1)$.
2. $\vec{p} = 3\,t^3 + 4\,t^2 - 2\,t + 3$, $\vec{q} = t^3 + t^2 - 2\,t + 4$, $\vec{r} = 3\,t^3 + 6\,t^2 - 15$.

3. $M_1 = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, M_4 = \begin{pmatrix} 2 & 0 \\ 6 & 2 \end{pmatrix},$

Ejercicio 10.7 (♣) Dados los vectores $(1,0,0,)$ y $(1,1,0)$, dar un vector (x,y,z) no nulo, que sea combinación lineal de los anteriores y perpendicular a $(0,1,0)$.

Ejercicio 10.8 Dados los vectores $\vec{v}_1 = (1,0,k)$, $\vec{v}_2 = (k,1,1)$, $\vec{v}_3 = (3,k,0)$, determinar $k \in \mathbb{R}$ tal que sean:

1. linealmente independientes,
2. linealmente dependientes.

10.3.3. Bases

Ejercicio 10.9 Si los vectores $\vec{u}, \vec{v}$ y $\vec{w}$ son linealmente independientes en $\mathbb{R}^3$, el conjunto $\{\vec{u}+\vec{v},\ \vec{u}+2\,\vec{w},\ \vec{u}+1/2\,\vec{v}+\vec{w}\}$ ¿es una base para $\mathbb{R}^3$?

Ejercicio 10.10 ($\diamond$) Hallar un vector $\vec{v} = (v_1,\ v_2,\ v_3) \in \mathbb{R}^3$ que satisfaga simultáneamente las siguientes condiciones:

1. $v_1 + v_2 + v_3 = 3$,
2. $\vec{v}$ es combinación lineal de $(2,2,2)$ y $(-1,0,1)$,
3. $B = \{\vec{v}, (1,0,1),\ (0,1,0)\}$ es base de $\mathbb{R}^3$.

Ejercicio 10.11 Para los subespacios del ejercicio 1.4 del práctico anterior, hallar, en cada caso,

1. Un conjunto de vectores linealmente independientes que no formen base del subespacio.
2. Un conjunto de vectores generadores que no formen base del subespacio.

Ejercicio 10.12 Dar dos bases ortonormales para $\mathbb{R}^2$ distintas de la base canónica. Idem para $\mathbb{R}^3$ y $\mathbb{R}^4$.

Ejercicio 10.13 Dado $\{(1/\sqrt{2}, -1/\sqrt{2})\}$ extenderlo a una base ortonormal de $\mathbb{R}^2$.
Realizar lo mismo para $\mathbb{R}^3$ y $\{(3/5, 0, -4/5)\}$.
¿Es posible para $\{(3/5, 0, -4/5),\ (1,0,0)\}$?

Ejercicio 10.14 ($\diamond$) Dado $\vec{v} = (3, -1)$ hallar una base ortonormal de $\mathbb{R}^2$ que contenga un vector con su misma dirección. Realizar lo mismo para $\mathbb{R}^3$ y $\vec{v} = (2, -3, 1)$.

Ejercicio 10.15 ($\clubsuit$) Determinar, si es posible, valores de $k \in \mathbb{R}$ para los cuales el conjunto $B = \{(1, 0, k), (0, 1, k), \ (0, k, 1)\}$ sea una base de $\mathbb{R}^3$. Indicar, si existe, un valor de k para el cual B sea base ortonormal.

10.3.4. Cambio de base

Ejercicio 10.16 Sean dos bases de $\mathbb{R}^3$: $B = \{(1, 0, -1), (2, 1, 3), (1, 1, 0)\}$ y $B' = \{(1, -1, 1), (1, 3, 4), (1, 2, 3)\}$.

1. Hallar las matrices de cambio de base $[B]_{B'}$ y $[B']_B$.
2. Si $[\vec{v}]_{B'} = \langle\langle 1, -1, 1\rangle\rangle$, hallar $[v]_C$ y $[v]_B$.

Ejercicio 10.17 Sean $B = \{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ y $B' = \{\vec{v}_1', \vec{v}_2', \vec{v}_3'\}$ dos bases de $\mathbb{R}^3$ tales que $\vec{v}_1 = 2\vec{v}_1' - \vec{v}_2'$, $\vec{v}_2 = \vec{v}_1' + \vec{v}_2' + 2\,\vec{v}_3'$ y $\vec{v}_3 = \vec{v}_2' + 3\vec{v}_3'$.

1. Hallar las matrices de cambio de base $[B]_{B'}$ y $[B']_B$.
2. Sabiendo que $[\vec{v}]_B = \langle 3, 1, 1\rangle$, hallar $[\vec{v}]_{B'}$.

Ejercicio 10.18 Sea $B = \{(1, -1, 0), (0, 2, 1), (1, 0, 1)\}$ una base de $\mathbb{R}^3$. Hallar una base B' tal que la matriz de cambio de base de B a B' sea

$$[B]_{B'} = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix}.$$

Ejercicio 10.19 ($\diamond$) Sea $V = \mathbb{P}_2[\mathbb{R}]$ y las bases $B = \{1 - x, 3\,x, x^2 - x + 1\}$ y
$B' = \{1 + x, 3 - 2\,x, x + x^2\}$. Si $[p]_B = \langle 2, 1, 3\rangle$, hallar $[p]_{B'}$.

10.3.5. Cambio de base

Ejercicio 10.20 Sea $V = \mathbb{P}_2[\mathbb{R}]$ y las bases $B = \{1 - x, 3\,x, x^2 - x + 1\}$ y $B' = \{1 + x, 3 - 2\,x, x + x^2\}$. Si $[p]_B = \langle 2, 1, 3\rangle$, hallar $[p]_{B'}$.

Ejercicio 10.21 Sean $B = \{(-1,0),\,(1,1)\}$ y $B' = \{(2,3),\,(-1,2)\}$ bases ordenadas de $\mathbb{R}^2$; $(0, XY)$ el sistema de coordenadas asociado a la base B y $(0, X'Y')$ A B', respectivamente. Si en $(0, XY)$, la ecuación de la recta L es $2\,x + y - 1 = 0$, hallar su ecuación en $(0, X'Y')$.

Ejercicio 10.22 Sea $(0, X'Y')$ el sistema de coordenadas obtenido rotando el sistema $(0, XY)$ en un ángulo θ.

1. Si $\theta = \dfrac{5}{6}\pi$ y P tiene coordenadas $(2, -1)$ en el sistema $(0, XY)$, hallar sus coordenadas en el $(0, X'Y')$.
2. Si $\theta = \dfrac{3}{4}\pi$ y P tiene coordenadas $\langle -1, 3\rangle$ en el sistema $(0, X'Y')$, hallar sus coordenadas en el $(0, XY)$.

Ejercicio 10.23 ($\diamond$) Sea $(0, XYZ)$ el sistema de coordenadas asociado a la base canónica de $\mathbb{R}^3$ y $(0', X''Y''Z'')$ el sistema asociado a la base $B = \{(\frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}}, 0),\,(0,0,1),\,(\frac{1}{\sqrt{5}}, \frac{-2}{\sqrt{5}}, 0)\}$, con origen en el punto $0'$, cuyas coordenadas en el sistema $(0, XYZ)$ son $0' = (2,1,0)$.

1. Dada la recta L como intersección de planos $\begin{cases} x'' - y'' + z'' = 0 \\ x'' + y'' - 2\,z'' - 1 = 0 \end{cases}$, en el sistema $(0', X''Y''Z'')$, hallar su ecuación en el sistema $(0, XYZ)$.
2. Dada la recta de ecuación $\begin{cases} x = 3 + \lambda \\ y = 2 \\ z = 1 + \lambda \end{cases}$, $\lambda \in \mathbb{R}$, en el sistema $(0, XYZ)$

   y el plano π de ecuación $x'' + \sqrt{5}\,y'' + 3\,z'' + \sqrt{5} = 0$ en el sistema $(0', X''Y''Z'')$,

   hallar $\pi \cap L$ en el sistema $(0, XYZ)$ y en el $\langle 0', X''Y''Z''\rangle$.

10.3.6. Transformaciones lineales

Ejercicio 10.24 Determinar cuáles de las funciones $T : V_1 \to V_2$ son transformaciones lineales. En caso afirmativo hallar $[T]_{C_1C_2}$, siendo C_i la base canónica de V_i

1. $T : \mathbb{R}^2 \to \mathbb{R}^3$, definida por $T((x,y)) = (x - y, x + 1, y + 2\,x)$
2. $T : \mathbb{R}^3 \to \mathbb{R}^3$, definida por $T((x,y,z)) = (z, 0, y)$

3. $T : \mathcal{C} \to \mathcal{C}$, definida por $T(z) = \overline{z}$ (Considerando a $\mathcal{C}$ como $\mathbb{R}$-espacio vectorial y como $\mathcal{C}$-espacio vectorial.
4. $T : M_2(\mathbb{R}) \to \mathbb{R}$, definida por $T(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}) = a_{11} \cdot a_{22} - a_{21} \cdot a_{12}$
5. $T : M_{2\times 3}\mathbb{R} \to \mathbb{R}^2$, definida por $T(\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}) = (a_{11} - a_{23}, -a_{13} + a_{12})$

Ejercicio 10.25 Interpretar geométricamente y dar la matriz en las bases canónicas de las siguientes transformaciones lineales $T : \mathbb{R}^2 \to \mathbb{R}^2$.

<u>Observación:</u> Como el espacio de llegada coincide con el espacio de salida y ambos son $\mathbb{R}^2$, la matriz de la transformación, que en verdad es $[T]_{C_2C_2}$ puede escribirse simplemente $[T]_{C_2}$ o bien $[T]_C$, ya que no hay riesgo de confusión.

1. $T_1((x, y)) = (x, 0)$
2. ($\diamond$) $T_2((x, y)) = (0, y)$
3. $T_3((x, y)) = (x, -y)$
4. ($\diamond$) $T_4((x, y)) = (\frac{1}{2}(x + y), \frac{1}{2}(x + y))$
5. $T_5((x, y)) = (x \cdot cos\,\alpha - y \cdot \text{sen } \alpha, x \cdot \text{sen } \alpha + y \cdot cos\,\alpha)$

Ejercicio 10.26 Determinar si existe una transformación lineal $T_i : \mathbb{R}^2 \to \mathbb{R}^2$ tal que

1. $T_1((1, 1)) = (2, 6)$, $T_1((-1, 1)) = (2, 1)$ y $T_1((3, 7)) = (14, 32)$.
2. $T_2((3, 6)) = (2, 6)$ y $T_2((-1, 1)) = (2, 1)$, $T_2((3, 7)) = (14, 32)$
3. $T_3((3, -9)) = (12, 6)$ y $T_3((-1, 3)) = (-4, -2)$, $T((2, -6)) = (8, 4)$

En cada caso, si existe, hallar la expresión y calcularla en $(3, 4)$ y $(0, 2)$. ¿Es única?

Ejercicio 10.27 Determinar si $T_1 = T_2$, donde $T_1, T_2 : \mathbb{R}^3 \to \mathbb{R}^3$ tales que:

$T_1((1, 0, 1)) = (1, 2, 1)$, $\quad T_1((2, 1, 0)) = (2, 1, 0)$, $\quad T_1((-1, 0, 0)) = (1, 2, 1)$
$T_2((1, 1, 1)) = (1, 1, 0)$, $\quad T_2((3, 2, 1)) = (0, 0, 1)$. $\quad T_2((2, 2, -1)) = (3, -1, 2)$.

Ejercicio 10.28 (♣) Hallar todos los $a \in \mathbb{R}$ para los cuales exista una transformación lineal $T : \mathbb{R}^3 \to \mathbb{R}^3$ que satisfaga:
$T((1, -1, 1)) = (2, a, -1), T((1, -1, 2)) = (a^2, -1, 1)$ y $T((1, -1, -2)) = (5, -1 -7)$.

Ejercicio 10.29 Dadas las transformaciones lineales $T, S : \mathbb{R}^2 \to \mathbb{R}^2$ definidas por:

$T((x, y)) = (2\,x + y\,,\, x + y)$, $S((x, y)) = (-2\,x + y\,,\, -x - y)$, hallar:

$[T]_{\mathcal{C}_2}$	$[T \circ S]_{\mathcal{C}_2}$	$[T]_{\mathcal{C}_2} \cdot [S]_{\mathcal{C}_2}$
$[S]_{\mathcal{C}_2}$	$[S \circ T]_{\mathcal{C}_2}$	$[S]_{\mathcal{C}_2} \cdot [T]_{\mathcal{C}_2}$

¿Se puede inferir una ley general que asocie el producto de matrices y la composición de transformaciones lineales?

Ejercicio 10.30 ($\clubsuit$) Dada la transformación lineal $T((x, y)) = (2\,x + y, 3\,y)$, hallar una expresión para $T^2 = T \circ T$ y para $T^3 = T^2 \circ T = T \circ T^2$. ¿Podrá hallarse la expresión general para $T^n, n \in \mathbb{N}$?

Ejercicio 10.31 ($\diamond$) Hallar, por construcción, la transformación lineal en el plano que describa la simetría respecto a la recta $L : x + y = 0$. Dar la expresión de la transformada de $x - y = 1$.

Ejercicio 10.32 ($\diamond$) Hallar la matriz en la base canónica de las siguientes transformaciones:

1. $T : \mathbb{R}^2 \to \mathbb{R}^2$, rotación en un ángulo de $\dfrac{\pi}{3}$.
2. $T : \mathbb{R}^3 \to \mathbb{R}^3$, rotación en un ángulo de $\dfrac{\pi}{4}$ alrededor del eje x.

Capítulo 11

Transformación lineal simétrica

Transformaciones lineales simétricas. Autovalores y autovectores. Polinomio característico. Reducción de una matriz simétrica a la forma diagonal.

11.1. Autovalores y autovectores

En la unidad anterior hemos trabajado con transformaciones lineales y hemos visto que toda transformación está asociada a una matriz. En esta unidad trabajaremos con transformaciones lineales de un $\mathbb{R}$-espacio vectorial en sí mismo. La primera observación que podemos hacer es que la matriz de una transformación de este tipo, siempre será cuadrada. Otra cosa que hemos observado (en las transformaciones con base adecuada) es que existen algunos vectores que se transforman en un múltiplo de sí mismos, ya sea con igual o distinto sentido. algo que va “en sí mismo” o “por sí mismo” se denomina *auto* y motiva la siguiente definición:

Definición 11.1 Dado $(V, +, .)$ un $\mathbb{R}$ espacio vectorial de dimensión finita y una transformación $T : V \to V$ un vector <u>no nulo</u> $\vec{v}$ se dice un *autovector* asociado al *autovalor* λ si $T(\vec{v}) = \lambda.\vec{v}$.

Un primer comentario bastante evidente: ¿por qué pedimos que el vector sea no nulo? Sabemos que $T(\vec{0}) = \vec{0} = \lambda.\vec{0}$, cualquiera que sea $\lambda \in \mathbb{K}$. Podríamos llegar a aceptar la idea de un autovector asociado a infinitos autovalores, pero no tendría demasiado sentido. Los atributos de un vector son dirección, sentido e intensidad, según la definición un autovector de T es un vector que al transformarse puede cambiar el sentido si está asociado a un autovalor negativo, la intensidad si el autovalor no es 1 o -1, pero jamás cambia la dirección. Y esto es lo que caracteriza a un autovector, que conserva la dirección. El vector nulo tiene intensidad (nula), pero no tiene dirección y, en consecuencia, no puede conservarla.

Estamos trabajando con $\mathbb{R}$-espacios vectoriales, por lo cual no tiene sentido hacer énfasis en que λ debe ser un valor real, pero esta aclaración es importante ya que la definición de autovalor y autovector se da para cualquier $\mathbb{K}$-espacio vectorial. Recordemos que al multiplicar por i se produce un giro de $\pi/2$, y en general, multiplicando por cualquier número complejo "se suma" su argumento principal y claramente, la dirección de un vector, al multiplicarlo por un número complejo, cambia.

Ejemplo 11.1 Consideremos algunas transformaciones en busca de autovalores y autovectores:

1. En cualquier espacio vectorial V, la transformación identidad tiene un único autovalor $\lambda = 1$ asociado a todos los vectores no nulos del espacio. En forma análoga, la transformación nula (es decir $T : V \to V$ definida por $T(\vec{v}) = \vec{0}$ para todo $\vec{v} \in V$) tiene un único autovalor $\lambda' = 0$, asociado a todos los vectores no nulos del espacio.
2. En el plano, proyección sobre una recta L que pase por el origen.
   Esta transformación consiste en "traer dentro de la recta" los puntos que están fuera. Claramente los puntos de la recta son puntos fijos, así $T(\vec{d}_L) = \vec{d}_L$ y el director de la recta es un autovector asociado al autovalor $\lambda = 1$. El vector normal a la recta, dado que es proyección ortogonal, proyecta sobre su origen y resulta $T(\vec{n}_L) = \vec{0}$, es decir $\vec{n}_L$ es un autovector asociado al autovalor $\lambda' = 0$.
3. En el espacio, simetría con respecto a un plano que pasa por el origen.
   Esta transformación consiste en "reflejar hacia el otro lado" todo punto que no esté en el plano, por lo tanto $T(\vec{n}_\pi) = -\vec{n}_\pi$, es decir, el vector normal es un autovector asociado al autovalor $\lambda_1 = -1$, y cualquier vector en el plano conserva su posición, es decir $T(\vec{v}) = \vec{v}$, cualquiera que sea $\vec{v}$ en π, o lo que es lo mismo, los vectores en el plano están asociados al autovalor $\lambda_2 = 1$.
4. En el plano, rotación de los ejes un ángulo α en sentido positivo.
   Claramente la transformación propone que los vectores roten, es decir, no existirá ninguno que conserve su dirección original.
5. En el espacio, rotación del plano YZ sobre el eje X en un ángulo α en sentido positivo.
   Como comentamos en el inciso anterior, todos los vectores que tengan

coordenadas no nulas en y o z cambiarán de dirección. Sin embargo los vectores de la forma $(k, 0, 0)$ están asociados al autovalor $\lambda = 1$, es decir $T((k, 0, 0)) = (k, 0, 0)$.

Hemos visto que dada una transformación puede ser que tenga uno, varios o ningún autovector. Veamos algunas propiedades de los autovectores asociados a una transformación:

Proposición 11.1 *Todo autovector está asociado a un único autovalor.*

Demostración: Supongamos que $\vec{v}$ está asociado a dos autovalores, sean λ y λ' entonces podemos escribir:

$$T(\vec{v}) = \lambda\vec{v}, \qquad\qquad T(\vec{v}) = \lambda'\vec{v}$$

Es decir:

$$(\lambda - \lambda')\vec{v} = \vec{0}, \text{ con } \vec{v} \neq \vec{0}$$

de donde:

$$\lambda = \lambda'$$

$\square$

Proposición 11.2 *El conjunto de todos los autovectores asociados a un autovalor forma subespacio.*

Demostración: Escribamos el conjunto de todos los vectores asociados a un autovalor λ y llamémoslo V_λ:

$$V_\lambda = \{\vec{v} \in V : T(\vec{v}) = \lambda.\vec{v}\}.$$

(SE_1) : $\vec{0} \in V_\lambda$:
$T(\vec{0}) = \vec{0} = \lambda.\vec{0}$.

(SE_2) : Sean $\vec{v}_1, \vec{v}_2 \in V_\lambda$, veamos que $\vec{v}_1 + \vec{v}_2 \in V_\lambda$:
$T(\vec{v}_1 + \vec{v}_2) = T(\vec{v}_1) + T(\vec{v}_2) = \lambda.\vec{v}_1 + \lambda.\vec{v}_2 = \lambda.(\vec{v}_1 + \vec{v}_2)$.

(SE_3) : Sea $\vec{v} \in V_\lambda$, veamos que $k.\vec{v} \in V_\lambda$:
$T(k.\vec{v}) = k.T(\vec{v}) = k.\lambda.\vec{v} = \lambda.(k.\vec{v})$.

Como satisface las tres condiciones, $V_\lambda \trianglelefteq V$ $\square$

Proposición 11.3 *A autovalores distintos se corresponden autovectores linealmente independientes.*

Corolario 11.1 *Sea* $(V, +, .)$ *un* $\mathbb{R}$ *espacio vectorial de dimensión finita* $dimV = n$ *y* $T : V \to V$ *una transformación lineal. Si* T *tiene* n *autovalores distintos, entonces los autovectores forman una base del espacio* V.

Demostremos la proposición:

Demostración: Haremos esta demostración por inducción. Para el caso base, sean λ_1, λ_2 y $\vec{v}_1, \vec{v}_2$ tales que: $T(\vec{v}_1) = \lambda_1.\vec{v}_1$ y $T(\vec{v}_2) = \lambda_2.\vec{v}_2$.
Si $\vec{v}_1$ y $\vec{v}_2$ no fueran linealmente independientes sería

$$\vec{v}_1 = k.\vec{v}_2 \text{ y } T(\vec{v}_1) = T(k.\vec{v}_2) = k.T(\vec{v}_2).$$

O lo que es lo mismo:

$$\lambda_1.\vec{v}_1 = k.\lambda_2.\vec{v}_2 = \lambda_2.(k.\vec{v}_2) = \lambda_2.\vec{v}_1.$$

Lo cual es imposible por la Proposición 11.1.

Supongamos ahora que a n autovalores diferentes corresponden n autovectores linealmente independientes, y que estamos en un espacio de dimensión mayor ó igual a $n+1$. Sea $\lambda_1, \lambda_2, \ldots, \lambda_{n+1}$ $n+1$ autovalores diferentes y probemos que el conjunto de autovectores asociados $\{\vec{v}_1, \vec{v}_2, \ldots \vec{v}_{n+1}\}$ es linealmente independiente. Para probar que $\{\vec{v}_1, \vec{v}_2, \ldots \vec{v}_{n+1}\}$ es linealmente independiente, por la proposición 10.3 basta ver que $\vec{v}_1 \neq \vec{0}$ y que $\vec{v}_{n+1}$ no es combinación lineal de los anteriores.
Supongamos que $\vec{v}_{n+1} = k_1\vec{v}_1 + k_2\vec{v}_2 + \ldots + k_n\vec{v}_n$, entonces

$$T(\vec{v}_{n+1}) = k_1T(\vec{v}_1)+k_2T(\vec{v}_2)+\ldots+k_nT(\vec{v}_n) = k_1\lambda_1\vec{v}_1+k_2\lambda_2\vec{v}_2+\ldots+k_n\lambda_n\vec{v}_n,$$

como

$$T(\vec{v}_{n+1}) = \lambda_{n+1}\vec{v}_{n+1}$$

igualamos

$$\lambda_{n+1}(\vec{v}_{n+1}) = \lambda_{n+1}(k_1\vec{v}_1 + k_2\vec{v}_2 + \ldots + k_n\vec{v}_n)$$

y restando $T(\vec{v}_{n+1}) - \lambda_{n+1}(\vec{v}_{n+1})$obtenemos:

$$k_1(\lambda_1 - \lambda_{n+1})\vec{v}_1 + k_2(\lambda_2 - \lambda_{n+1})\vec{v}_2 + \ldots + k_n(\lambda_n - \lambda_{n+1})\vec{v}_n = \vec{0}$$

Como $\{\vec{v}_1, \vec{v}_2, \ldots \vec{v}_n\}$ es linealmente independiente, y $\lambda_i \neq \lambda_{n+1}$ resulta que $k_i = 0$ para todo $1 \leq i \leq n$ y $\vec{v}_{n+1} = \vec{0}$, lo cual es un absurdo.
Podemos concluir, entonces que a autovalores distintos corresponden autovectores linealmente independientes, para todo $n \leq dimV$.

□

El corolario ahora es trivial. Si tenemos n vectores linealmente independientes en un espacio vectorial de dimensión n, claramente conforman un conjunto linealmente independiente maximal y, por lo tanto, una base.

Observación 11.1 Este resultado es realmente interesante. En las condiciones del corolario tenemos una base de autovectores $\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ y para cada $1 \leq i \leq n$ se cumple $T(\vec{v}_i) = \lambda_i.\vec{v}_i$, en consecuencia:

$$[T]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

¿Habrá alguna posibilidad de asegurar la existencia de esta base? ¿Podremos encontrar todos los autovalores asociados a una transformación lineal?

Busquemos las respuestas:
Tenemos una transformación lineal $T : V \to V$ con una matriz asociada

$$[T]_{\mathcal{C}} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn} \end{pmatrix}$$

Buscamos un $\vec{v} = (v_1, v_2, \ldots, v_n), \vec{v} \neq \vec{0}$, que satisfaga $T(\vec{v}) = \lambda.\vec{v}$, es decir:

$$[T(\vec{v})]_{\mathcal{C}} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn} \end{pmatrix} . \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} \lambda.v_1 \\ \lambda.v_2 \\ \vdots \\ \lambda.v_n \end{pmatrix}$$

Escrito como sistema de ecuaciones:

$$\begin{cases} a_{11}\, v_1 \ + a_{12}\, v_2 \ + \ldots + a_{1n}\, v_n \ = \ \lambda.v_1 \\ a_{21}\, v_1 \ + a_{22}\, v_2 \ + \ldots + a_{2n}\, v_n \ = \ \lambda.v_2 \\ \vdots \qquad \vdots \quad \vdots \quad \vdots \qquad \vdots \quad \vdots \qquad \vdots \\ a_{n1}\, v_1 + a_{n2}\, v_2 + \ldots + a_{nn}\, v_n = \ \lambda.v_n \end{cases}$$

Pero cuando escribimos los sistemas de ecuaciones, todas las incógnitas están "del igual a la izquierda". Si solucionamos esta situación nos queda:

$$\begin{cases} (a_{11} - \lambda)\, v_1 \ + a_{12}\, v_2 \ + \ldots + a_{1n}\, v_n \ = \ 0 \\ a_{21}\, v_1 \ + (a_{22} - \lambda)\, v_2 \ + \ldots + a_{2n}\, v_n \ = \ 0 \\ \vdots \qquad \vdots \quad \vdots \quad \vdots \qquad \vdots \quad \vdots \qquad \vdots \\ a_{n1}\, v_1 + a_{n2}\, v_2 + \ldots + (a_{nn} - \lambda)\, v_n = \ 0 \end{cases}$$

Claramente estamos ante un sistema homogéneo y por lo tamto compatible, pero nosotros buscamos que tenga solución <u>no nula</u>, es decir que se trate de un sistema compatible indeterminado, lo cual se garantiza pidiendo que el determinante del sistema sea 0. Esto justifica la siguiente definición:

Definición 11.2 Dada una transformación $T : V \to V$ se denomina *polinomio característico* y se nota $P_T(\lambda)$ al siguiente determinante:

$$P_T(\lambda)=\begin{vmatrix} a_{11}-\lambda & {}_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn}-\lambda \end{vmatrix}$$

Las raíces reales del determinante, si existen, serán los autovalores reales. Para cada uno de estos λ el sistema es compatible indeterminado y el conjunto de soluciones asociado es el subespacio de autovectores para dicho autovalor. Veamos un ejemplo.

Ejemplo 11.2 Consideremos $T : \mathbb{R}^2 \to \mathbb{R}^2$ definida por

$$T((x, y)) = (3x + 8y, -y).$$

El primer paso es construir la matriz de la transformación en la base canónica:

$$T((1, 0)) = (3, 0) \qquad [T]_{\mathcal{C}} = \begin{pmatrix} 3 & 8 \\ 0 & -1 \end{pmatrix}$$

$$T((0, 1)) = (8, -1)$$

El siguiente paso es construir el polinomio característico:

$$P_T(\lambda) = \begin{vmatrix} 3-\lambda & 8 \\ 0 & -1-\lambda \end{vmatrix} = (3 - \lambda).(-1 - \lambda)$$

Las raíces de este polinomio son $\lambda_1 = 3$ y $\lambda_2 = -1$.

$\lambda_1 = 3$:
Debemos resolver el sistema $T((x, y)) = 3.(x, y)$, es decir:

$$\begin{cases} 3x + 8y = 3x \\ -y = 3y \end{cases} \text{ o lo que es lo mismo: } \begin{cases} 8y = 0 \\ -4y = 0 \end{cases}$$

Es un sistema compatible indeterminado y su solución generalizada es $(a, 0)_{a\in\mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:

$$V_3 = \{(a, 0) : a \in \mathbb{R}\}.$$

$\lambda_1 = -1$:
Debemos resolver el sistema $T((x,y)) = (-1).(x,y)$, es decir:

$$\begin{cases} 3x + 8y = -x \\ -y = -y \end{cases} \text{ o lo que es lo mismo: } \begin{cases} 4x + 8y = 0 \\ -y = -y \end{cases}$$

Es un sistema compatible indeterminado y su solución generalizada es $(-2b, b)_{b\in\mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:

$$V_{-1} = \{(-2b, b) : b \in \mathbb{R}\}.$$

Como los autovalores son distintos, los autovectores son linealmente independientes y forman una base del espacio. Consideremos

$$\mathcal{B} = \{(1,0), (-2,1)\}$$

Escribamos la matriz de la transformación en esta base:

$$\begin{aligned} T((1,0)) &= 3.(1,0) + 0(-2,1) \\ T((-2,1)) &= 0.(1,0) - 1.(-2,1) \end{aligned} \qquad [T]_{\mathcal{B}} = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}$$

Hemos encontrado los autovalores y autovectores como raíces del polinomio característico, utilizando la matriz de T en la base canónica. Podríamos pensar que al cambiar de base estos valores varían. Afortunadamente esto no ocurre:

Teorema 11.1 *Sea $(V,+,.)$ un $\mathbb{R}$-espacio vectorial, $T : V \to V$ una transformación lineal y dos bases ordenadas $\mathcal{B}_1$ y $\mathcal{B}_2$ de V, entonces $|[T]_{\mathcal{B}_1} - \lambda.I_n| = |[T]_{\mathcal{B}_2} - \lambda.I_n|$*

Corolario 11.2 *Los autovalores de una transformación lineal no dependen de la base elegida.*

Demostración: Demostremos el teorema:
Consideremos la matriz de cambio de base $[\mathcal{B}_1]_{\mathcal{B}_2}$:

$$\begin{aligned} |[T]_{\mathcal{B}_1} - \lambda.I_n| &= |[\mathcal{B}_1]_{\mathcal{B}_2}||[T]_{\mathcal{B}_1} - \lambda.I_n||[\mathcal{B}_1]_{\mathcal{B}_2}|^{-1} = \\ &= |[\mathcal{B}_1]_{\mathcal{B}_2}.([T]_{\mathcal{B}_1} - \lambda.I_n).[\mathcal{B}_1]_{\mathcal{B}_2}|^{-1} = \\ &= |[\mathcal{B}_1]_{\mathcal{B}_2}.[T]_{\mathcal{B}_1}[\mathcal{B}_1]^{-1}_{\mathcal{B}_2} - [\mathcal{B}_1]_{\mathcal{B}_2}(\lambda.I_n).[\mathcal{B}_1]^{-1}_{\mathcal{B}_2}| = \\ &= |[\mathcal{B}_1]_{\mathcal{B}_2}.[T]_{\mathcal{B}_1}[\mathcal{B}_2]_{\mathcal{B}_1} - (\lambda.I_n).[\mathcal{B}_1]_{\mathcal{B}_2}.[\mathcal{B}_1]_{\mathcal{B}_2}|^{-1} = \\ &= |[T]_{\mathcal{B}_2} - \lambda.I_n|. \end{aligned}$$

. □

La demostración del corolario es inmediata.

Ejemplo 11.3 Hagamos algunos ejemplos:

1. Dada
$$[T]_{\mathcal{C}} = \begin{pmatrix} a & -1 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -5 \end{pmatrix},$$
hallar el valor de a tal que la transformación tenga $\lambda_1 = 3$ como autovalor doble y $\lambda_2 = -5$ como autovalor simple. Hallar los autovectores asociados.
$$P_T(-\lambda) = \begin{vmatrix} a-\lambda & -1 & 0 \\ 0 & 3-\lambda & 0 \\ 0 & 0 & -5-\lambda \end{vmatrix} = (a-\lambda).(3-\lambda).(-5-\lambda)$$
Para que 3 sea autovalor doble, necesariamente $a = 3$.
Hallemos los autovectores:

   $\lambda_1 = 3$:
   Debemos resolver el sistema $T((x, y, z)) = 3.(x, y, z)$, es decir:
$$\begin{cases} 3x - y = 3x \\ 3y = 3y \\ -5z = 3z \end{cases} \text{ o lo que es lo mismo: } \begin{cases} y = 0 \\ 0 = 0 \\ -8z = 0 \end{cases}$$
   Es un sistema compatible indeterminado y su solución generalizada es $(a, 0, 0)_{a\in\mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:
$$V_3 = \{(a, 0, 0) : a \in \mathbb{R}\}.$$
   $\lambda_1 = -5$:
   Debemos resolver el sistema $T((x, y, z)) = (-5).(x, y, z)$, es decir:
$$\begin{cases} 3x - y = -5x \\ 3y = -5y \\ -5z = -5z \end{cases} \text{ o lo que es lo mismo: } \begin{cases} 8x - y = 0 \\ 8y = 0 \\ 0 = 0 \end{cases}$$
   Es un sistema compatible indeterminado y su solución generalizada es $(0, 0, b)_{b\in\mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:
$$V_{-5} = \{(0, 0, b) : b \in \mathbb{R}\}.$$
   El primer autovalor es una raíz doble del polinomio característico, pero el espacio de autovectores que genera tiene dimensión 1, por lo tanto no es posible encontrar una base en que la matriz de la transformación tenga forma diagonal.

2. Sea T tal que
$$[T]_{\mathcal{C}} = \begin{pmatrix} 3 & a \\ -1 & b \end{pmatrix}.$$
Determinar a y b para que $\lambda = 1$ sea un autovalor asociado $\vec{v} = (-1, 1)$. Hallar, si es posible, el otro autovalor y el espacio de autovectores asociado.
$$[T(-1,1)]_{\mathcal{C}} = 1.\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & a \\ -1 & b \end{pmatrix}.\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -3+a \\ 1+b \end{pmatrix}$$
Resolviendo la ecuación obtenemos $a = 2, b = 0$, entonces
$$[T]_{\mathcal{C}} = \begin{pmatrix} 3 & 2 \\ -1 & 0 \end{pmatrix}, \ P_T(\lambda) = \begin{vmatrix} 3-\lambda & 2 \\ -1 & -\lambda \end{vmatrix}$$
Es decir, $P_T(\lambda) = (3-\lambda).(-\lambda) + 2 = \lambda^2 - 3\lambda + 2 = (\lambda - 1).(\lambda - 2)$
Es decir, el otro autovalor es 2 y el espacio de autovectores asociado es $V_2 = \{(-2a, a) : a \in \mathbb{R}\}$.

11.2. Transformación lineal simétrica

Ya hemos visto cómo encontrar, si existen, los autovalores reales de una transformación lineal. Hemos visto también, en la observación 11.1, que si encontramos en un espacio de dimensión n, n autovalores distintos los autovectores asociados forman una base, y la matriz de la transformación en dicha base tiene forma diagonal, todo esto nos habilita a formular la siguiente definición:

Definición 11.3 Una transformación lineal se dice *diagonalizable* si existe una base del espacio tal que la matriz de la transformación en dicha base tenga forma diagonal.

Supongamos que T es una transformación lineal diagonalizable en una base ortonormal de autovectores $\mathcal{B}_1$. ¿Qué forma tendrá T en cualquier otra base ortonormal $\mathcal{B}_2$? Consideremos las matrices de cambio de base:

$$[\mathcal{B}_1]_{\mathcal{B}_2} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

$$[\mathcal{B}_2]_{\mathcal{B}_1} = [\mathcal{B}_1]^t_{\mathcal{B}_2} = \begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{n1} \\ a_{12} & a_{22} & a_{32} & \dots & a_{n2} \\ a_{13} & a_{23} & a_{33} & \dots & a_{n3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{pmatrix}$$

y calculemos $[T]_{\mathcal{B}_2} = [\mathcal{B}_1]_{\mathcal{B}_2}[T]_{\mathcal{B}_1}[\mathcal{B}_1]^t_{\mathcal{B}_2}$:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} . \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix} . \begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{n1} \\ a_{12} & a_{22} & a_{32} & \dots & a_{n2} \\ a_{13} & a_{23} & a_{33} & \dots & a_{n3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}.\lambda_1 & a_{12}.\lambda_2 & a_{13}.\lambda_3 & \dots & a_{1n}.\lambda_n \\ a_{21}.\lambda_1 & a_{22}.\lambda_2 & a_{23}.\lambda_3 & \dots & a_{2n}.\lambda_n \\ a_{31}.\lambda_1 & a_{32}.\lambda_2 & a_{33}.\lambda_3 & \dots & a_{3n}.\lambda_n \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1}.\lambda_1 & a_{n2}.\lambda_2 & a_{n3}.\lambda_3 & \dots & a_{nn}.\lambda_n \end{pmatrix} . \begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{n1} \\ a_{12} & a_{22} & a_{32} & \dots & a_{n2} \\ a_{13} & a_{23} & a_{33} & \dots & a_{n3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{pmatrix} .$$

A estas alturas, en lugar de hacer todo el producto veamos cómo es un elemento del producto que está en la fila i y la columna j:

$$p_{ij} = a_{i1}.\lambda_1.a_{j1} + a_{i2}.\lambda_2.a_{j2} + a_{i3}.\lambda_3.a_{j3} + \ldots + a_{in}.\lambda_n.a_{jn} =$$

$$= a_{j1}.\lambda_1.a_{i1} + a_{j2}.\lambda_2.a_{i2} + a_{j3}.\lambda_3.a_{i3} + \ldots + a_{jn}.\lambda_n.a_{in} = p_{ji}$$

Es decir, la matriz de T es cualquier base ortonormal coincide con su transpuesta, es decir, es una matriz simétrica. Esto nos lleva a la siguiente definición:

Definición 11.4 Una transformación lineal en un $\mathbb{R}$-espacio vectorial se dice *simétrica* si $[T]_{\mathcal{C}} = [T]^t_{\mathcal{C}}$.

Proposición 11.4 *Sea $T : V \to V$ uns TLS, $\vec{u}, \vec{v} \in V$, entonces*

$$(\vec{u}, T(\vec{v})) = (T(\vec{u}), \vec{v})$$

Demostración: Dado que T es una TLS, $[T]_{\mathcal{C}}$ es una matriz simétrica. Sea

$$[T]_{\mathcal{C}} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{12} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix}$$

$$[T(\vec{u})]_{\mathcal{C}} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{12} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{pmatrix}$$

$$T(\vec{u}) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{12} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} a_{11}.u_1 + a_{12}.u_2 + \ldots + a_{1n}.u_n \\ a_{12}.u_1 + a_{22}.u_2 + \ldots + a_{2n}.u_n \\ \vdots \\ a_{1n}.u_1 + a_{2n}.u_2 + \ldots + a_{nn}.u_n \end{pmatrix}$$

$$(T(\vec{u}), \vec{v}) =$$

$$= (a_{11}.u_1 + a_{12}.u_2 + \ldots + a_{1n}.u_n).v_1 + (a_{12}.u_1 + a_{22}.u_2 + \ldots + a_{2n}.u_n).v_2 + \ldots +$$

$$(a_{1n}.u_1 + a_{2n}.u_2 + \ldots + a_{nn}.u_n).v_n =$$

$$= a_{11}.u_1.v_1 + a_{12}.u_2.v_1 + \ldots + a_{1n}.u_n.v_1 + a_{12}.u_1.v_2 + a_{22}.u_2.v_2 + \ldots + a_{2n}.u_n.v_2 +$$

$$\ldots + a_{1n}.u_1.v_n + a_{2n}.u_2.v_n + \ldots + a_{nn}.u_n.v_n.(A)$$

$$T(\vec{v}) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{12} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{11}.v_1 + a_{12}.v_2 + \ldots + a_{1n}.v_n \\ a_{12}.v_1 + a_{22}.v_2 + \ldots + a_{2n}.v_n \\ \vdots \\ a_{1n}.v_1 + a_{2n}.v_2 + \ldots + a_{nn}.v_n \end{pmatrix}$$

$$(\vec{u}, T(\vec{v})) = (T(\vec{v}), \vec{u}) =$$

$$= (a_{11}.v_1 + a_{12}.v_2 + \ldots + a_{1n}.v_n).u_1 + (a_{12}.v_1 + a_{22}.v_2 + \ldots + a_{2n}.v_n).u_2 + \ldots +$$

$$(a_{1n}.v_1 + a_{2n}.v_2 + \ldots + a_{nn}.v_n).u_n =$$

$$= a_{11}.v_1.u_1 + a_{12}.v_2.u_1 + \ldots + a_{1n}.v_n.u_1 + a_{12}.v_1.u_2 + a_{22}.v_2.u_2 + \ldots + a_{2n}.v_n.u_2 +$$

$$\ldots + a_{1n}.v_1.u_n + a_{2n}.v_2.u_n + \ldots + a_{nn}.v_n.u_n(B)$$

Reordenando los términos se ve que

$$(T(\vec{u}), \vec{v}) = (T(\vec{v}), \vec{u}).$$

□

Llegamos a esta definición partiendo de una transformación diagonalizable, en una base ortonormal. Se puede probar que toda transformación lineal simétrica es diagonalizable en una base ortonormal. Esta demostración escapa a nuestro alcance y se basa en dos resultados realmente fuertes:

1. Todas las raíces del polinomio característico son reales.
2. A autovalores distintos corresponden autovectores ortogonales.

Esta segunda afirmación es fácilmente demostrable a la luz de la proposición 11.4, y se la recomendamos al lector interesado ®.

Ejemplo 11.4 Veamos algunas transformaciones lineales simétricas:

1. $T((x, y, z)) = (x - y, -x + 2y - z, -y + z)$
   Construyamos la matriz de la transformación en la base canónica:
   $T((1, 0, 0)) = (1, -1, 0)$
   $T((0, 1, 0)) = (-1, 2, -1)$
   $T((0, 0, 1)) = (0, -1, 1)$
   $$[T]_{\mathcal{C}} = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$$
   El polinomio caracteístico es:
   $$P_T(\lambda) = \begin{vmatrix} 1-\lambda & -1 & 0 \\ -1 & 2-\lambda & -1 \\ 0 & -1 & 1-\lambda \end{vmatrix} = (1-\lambda)^2.(2-\lambda) - 2.(1-\lambda) =$$
   $$= (1-\lambda)((1-\lambda).(2-\lambda) - 2) = (1-\lambda)(\lambda^2 - 3\lambda)) = (1-\lambda)(\lambda - 3).\lambda$$
   Las raíces de este polinomio son $\lambda_1 = 3$ y $\lambda_2 = 1$ y $\lambda_3 = 0$.

   $\lambda_1 = 3$:
   Debemos resolver el sistema $T((x, y, z)) = 3.(x, y, z)$, es decir:
   $$\begin{cases} x - y = 3x \\ -x + 2y - z = 3y \\ -y + z = 3z \end{cases} \text{ o lo que es lo mismo: } \begin{cases} -2x - y = 0 \\ -x - y - z = 0 \\ -y - 2z = 0 \end{cases}$$
   Es un sistema compatible indeterminado y su solución generalizada es $(a, -2a, a)_{a \in \mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:
   $$V_3 = \{(a, -2a, a) : a \in \mathbb{R}\}.$$
   $\lambda_1 = 1$:
   Debemos resolver el sistema $T((x, y, z)) = 1.(x, y, z)$, es decir:
   $$\begin{cases} x - y = x \\ -x + 2y - z = y \\ -y + z = z \end{cases} \text{ o lo que es lo mismo: } \begin{cases} -y = 0 \\ -x + y - z = 0 \\ -y = 0 \end{cases}$$
   Es un sistema compatible indeterminado y su solución generalizada es $(a, -2a, a)_{a \in \mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:
   $$V_1 = \{(b, 0, -b) : b \in \mathbb{R}\}.$$

$\lambda_1 = 0$:
Debemos resolver el sistema $T((x, y, z)) = 0.(x, y, z)$, es decir:

$$\begin{cases} x - y = 0 \\ -x + 2y - z = 0 \\ -y + z = 0 \end{cases}$$

Es un sistema compatible indeterminado y su solución generalizada es $(c, c, c)_{c\in\mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:

$$V_0 = \{(c, c, c) : a \in \mathbb{R}\}.$$

Como los autovalores son distintos, los autovectores son ortogonales. Busquemos una base ortonormal:

$$\mathcal{B} = \{(1/\sqrt{6}, -2/\sqrt{6}, 1/\sqrt{6}), (1/\sqrt{2}, 0, -1/\sqrt{2}), (1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3})\}$$

Escribamos la matriz de la transformación en esta base:

$T(\vec{v}_1) = 3.\vec{v}_1 + 0.\vec{v}_2 + 0.\vec{v}_3$

$T(\vec{v}_2) = 0.\vec{v}_1 + 1.\vec{v}_2 + 0.\vec{v}_3$ $\qquad [T]_{\mathcal{B}} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$T(\vec{v}_3) = 0.\vec{v}_1 + 0.\vec{v}_2 + 0.\vec{v}_3$

En verdad, sabíamos, por ser una transformación simétrica que la base de autovectores es siempre ortonormal. Por este motivo, en lugar de calcular el tercer autovector podramos haber hecho el producto vectorial entre los dos anteriores.Demo como ejercicio para el lector la comprobación de este hecho.

2. $T((x, y, z)) = \left(\dfrac{7\,x + 24\,z}{25}, y, \dfrac{24\,x - 7\,z}{25} \right)$

$$[T]_{\mathcal{C}} = \begin{pmatrix} 7/25 & 0 & 24/25 \\ 0 & 1 & 0 \\ 24/25 & 0 & -7/25 \end{pmatrix}, \; P_T(\lambda) = \begin{vmatrix} 7/25 - \lambda & 0 & 24/25 \\ 0 & 1 - \lambda & 0 \\ 24/25 & 0 & -7/25 - \lambda \end{vmatrix}.$$

Las raíces de $P_T(\lambda) = (1 - \lambda)(\lambda^2 - 1)$ son:$\lambda_1 = 1$ (doble) y $\lambda_2 = -1$.

$\lambda_1 = 1$:
Debemos resolver el sistema $T((x, y, z)) = 1.(x, y, z)$, es decir:

$$\begin{cases} \dfrac{7}{25}\,x + \dfrac{24}{25}\,z = x \\ \qquad\qquad y = y \\ \dfrac{24}{25}\,x - \dfrac{7}{25}\,z = z \end{cases} \text{ o lo que es lo mismo: } \begin{cases} -\dfrac{18}{25}\,x + \dfrac{24}{25}\,z = 0 \\ \qquad\qquad 0 = 0 \\ \dfrac{24}{25}\,x - \dfrac{32}{25}\,z = 0 \end{cases}$$

Es un sistema compatible indeterminado y su solución generalizada es $(a, b, \frac{3}{4}a)_{a,b\in\mathbb{R}}$. El subespacio de los autovectores asociado es, entonces:

$$V_1 = \{(a, b, \frac{3}{4}a), a, b \in \mathbb{R}\} = \overline{\{(4, 0, 3), (0, 1, 0)\}}.$$

$\lambda_2 = -1$:
Podemos hacer el mismo procedimiento, pero sabemos que la base de autovectores es ortogonal y ya tenemos dos, entonces el tercero lo podemos obtener como el producto vectorial entre los anteriores:

$$\vec{v}_3 = (4, 0, 3) \wedge (0, 1, 0) = (-3, 0, 4).$$

Armemos ahora una base ortonormal, simplemente dividiendo cada vector por su módulo:

$$\mathcal{B} = \{(4/5, 0, 3/5), (0, 1, 0), (-3/5, 0, 4/5)\}.$$

Encontramos la base en la que la transformación tiene forma diagonal, la forma es:

$$[T]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Cuando hablamos de autovalores y autovectores hay que recordar siempre que van absolutamente uno de la mano del otro y su relación es $T(\vec{v}) = \lambda.\vec{v}$. Hay casos en que no es necesario hacer casi cuenta alguna. Por ejemplo, si queremos encontrar una transformación lineal con autovalores $\lambda_1 = 3$ y $\lambda_2 = -5$ asociados respectivamente a los vectores $\vec{v}_1 = (1, 2)$ y $\vec{v}_2 = (1, 3)$, la respuesta más rápida es decir:

$$\mathcal{B} = \{(1, 2), (1, 3)\}, [T]_{\mathcal{B}} = \begin{pmatrix} 3 & 0 \\ 0 & -5 \end{pmatrix}.$$

Si, además queremos su expresión en la base canónica, sí, hacemos el producto:

$$[T]_{\mathcal{C}} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & -5 \end{pmatrix} \cdot \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 3 & -5 \\ 6 & -15 \end{pmatrix} \cdot \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 19 & -8 \\ 48 & -21 \end{pmatrix}.$$

Entonces la expresión de la transformación es:

$$T((x, y)) = (19x - 8y, 48x - 21y).$$

Verifiquemos los autovalores y autovectores:

$$T((1, 2)) = (19 - 16, 48 - 42) = (3, 6) = 3.(1, 2)$$
$$T((1, 3)) = (19 - 24, 48 - 63) = (-5, -15) = -5.(1, 3)$$

11.3. Ejercicios propuestos

11.3.1. Transformaciones lineales con base adecuada

Ejercicio 11.1 Hallar la matriz en la base canónica de las siguientes transformaciones:

1. $T : \mathbb{R}^2 \to \mathbb{R}^2$, simetría respecto de la recta de ecuación $x + y = 0$.
2. $T : \mathbb{R}^3 \to \mathbb{R}^3$, simetría respecto del plano de ecuación $\pi : x + y - z = 0$.
3. $T : \mathbb{R}^3 \to \mathbb{R}^3$, simetría respecto de la recta de ecuación $\begin{cases} x + y = 0 \\ -y + z = 0 \end{cases}$.
4. $T : \mathbb{R}^3 \to \mathbb{R}^3$, proyección sobre el plano de ecuación $\pi : x + y - z = 0$, en forma paralela a la recta de ecuación $L : \dfrac{x-1}{-1} = \dfrac{y-22}{-3} = \dfrac{z+3}{2}$.

11.3.2. Autovalores y autovectores

Ejercicio 11.2 Analizar los autovalores y autovectores de las siguientes transformaciones lineales $T : \mathbb{R}^n \to \mathbb{R}^n$:

1. $n = 3$ y T la proyección ortogonal sobre un plano que pasa por el origen.
2. $n = 2$ y T la proyección ortogonal sobre una recta que pasa por el origen.
3. $n = 3$ y T la proyección ortogonal sobre una recta que pasa por el origen.
4. $n = 3$ y T la simetría respecto de un plano que pasa por el origen.
5. $n = 2$ y T la simetría respecto de una recta que pasa por el origen.
6. $n = 3$ y T la rotación alrededor de una recta que pasa por el origen.
7. $n = 3$ y T la proyección en dirección de una recta, sobre un plano que pasa por el origen.

Ejercicio 11.3 (✠) Sea V un espacio vectorial de dimensión finita y $T : V \to V$ una transformación lineal. Probar que si $\vec{u}$ y $\vec{v}$ son autovectores no paralelos de T, asociados a λ, entonces para todo $\alpha, \beta \in \mathbb{R}$, con α y β no simultáneamente nulos, $\alpha \cdot \vec{u} + \beta \cdot \vec{v}$ es un autovector de T, asociado a λ.

Ejercicio 11.4 Determinar los elementos a y b para que $\lambda = 4$ sea un autovalor asociado al autovector $\vec{v} = (-3, 6)$ para la transformación T cuya matriz en la base canónica es:
$$[T]_{\mathcal{C}} = \begin{pmatrix} b & a \\ -4 & b \end{pmatrix}.$$

Ejercicio 11.5 Se sabe que una transformación lineal en el espacio tiene a $\vec{v}_1 = (1, 0, 1)$ y $\vec{v}_2 = (0, 0, 1)$ como autovectores asociados a $\lambda = 3$, además se sabe que el transformado de $(0, 1, 1)$ es $(2, 3, 0)$. Hallar la matriz de la transformación en la base canónica.

Ejercicio 11.6 ($\diamond$) T es una transformación lineal diagonalizable con autovectores
$\vec{v}_1 = (1, 2)$ y $\vec{v}_2 = (3, 1)$. Se sabe que el transformado de $(5, -5)$ es $(2, -1)$. Hallar, si es posible, la expresión de T, la matriz de T en la base canónica y los autovalores asociados.

11.3.3. Polinomio característico

Ejercicio 11.7 Hallar los autovalores y autovectores asociados a las transformaciones

1. $T((x, y, z)) = \vec{0}$
2. $T((x, y, z)) = (x, y, z)$
3. $T((x, y, z)) = (2\,x + y\,,\, y - z\,,\, 2\,y + 4\,z)$.
4. $T((x, y)) = (4\,x + 3\,y\,,\, 3\,x - 4\,y)$.
5. $T((x, y, z)) = (x + y + z\,,\, 2\,y + z\,,\, 2\,x + 3\,z)$.

Ejercicio 11.8 ($\clubsuit$) Determinar los elementos a y b de modo tal que el polinomio característico asociado a A sea $\lambda^2 - \lambda + 2$, siendo $A = \begin{pmatrix} a & -2 \\ 1 & b \end{pmatrix}$.

Ejercicio 11.9 ($\clubsuit$) Determinar los elementos a, b y c de modo tal que A sea diagonalizable, siendo $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.

11.3.4. Diagonalización

Ejercicio 11.10 En cada uno de los siguientes casos determinar si la matriz es diagonalizable, y en caso afirmativo, determinar la matriz C tal que $C^{-1} \cdot$

$A \cdot C$ es la matriz diagonal.

1. $\begin{pmatrix} 1 & 0 \\ 6 & -1 \end{pmatrix}$

2. $\begin{pmatrix} 3 & -2 & 0 \\ -2 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}$

3. $\begin{pmatrix} 1 & 3 \\ -3 & -1 \end{pmatrix}$

4. $\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$

5. $\begin{pmatrix} 3 & 1 & 0 \\ -4 & -1 & 0 \\ 4 & -8 & -2 \end{pmatrix}$

6. $\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & a & 1 \end{pmatrix}$

Capítulo 12

Cónicas y cuádricas

En esta materia, pese a que es excesivamente breve, no se incluye el famoso tema *cónicas y cuádricas*. No voy a explayarme sobre él, sino simplemente dar una muy breve noción. Para cada una de las secciones cónicas daré la deducción de la ecuación canónica, claramente se puede obtener cualquier otra haciendo cambio de coordenadas por cambio de base y traslaciones.

12.1. Cónicas

Hemos visto la definición de distancia entre dos puntos del plano: Dados dos puntos $P_0 = (x_0, y_0)$ y $P_1 = (x_1, y_1)$ sabemos que

$$dist(P_0, P_1) = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}$$

hagamos algunas cuentitas:

12.1.1. Circunferencia

Supongamos que tenemos un hilo en un extremo atado a un clavo fijo en una superficie y en su otro extremo un lápiz. Si trazamos una línea con el lápiz manteniendo el hilo siempre tenso obtendremos lo que en el jardín de infantes llamábamos un *redondel*: una circunferencia. Ahora que sabemos cómo nació podemos dar la definición formal:

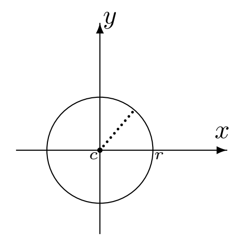
Definición 12.1 Fijado un punto c y un número real positivo r, llamamos *circunferencia* de *centro* c y *radio* r y notamos $\mathcal{C}(c, r)$ al conjunto de puntos

que distan r de c.
En símbolos:

$$\mathcal{C}(c,r) = \{P \in \mathbb{R}^2 : dist(P,c) = r\}.$$

Busquemos la fórmula:

Sea $c = (x_c, y_c)$, un punto $P = (x,y) \in \mathcal{C}$ si



$$dist(P,c) = r$$

$$\sqrt{(x-x_0)^2 + (y-y_0)^2} = r$$

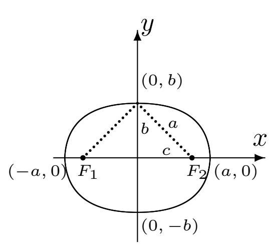
o lo que es lo mismo:

$$(x-x_0)^2 + (y-y_0)^2 = r^2$$

Observación 12.1 En general, una recta *tangente* a una curva en un punto P (el punto perteneciente a la curva, claro) es una recta que la corta sólo en P, en un entorno de P. En el caso de una circunferencia resulta ser una perpendicular al radio que pasa por el punto. El lector interesado se puede remitir a la observación 6.5 para refrescar lo ya visto acerca de la tangente trigonométrica.

12.1.2. Elipse

Supongamos ahora que el hilo lo tenemos clavado de sus dos puntas con sendos clavitos.



La longitud del hilo es mayor que la distancia entre los dos clavitos. Como también tenemos el lápiz podemos trazar una línea sobre la superficie manteniendo el hilo tenso. En cada lugar que paremos la longitud de hilo es la misma y es la suma del pedacito que va del clavo 1 hasta el lápiz más el pedacito que va del lápiz al clavo 2.
Estamos en condiciones de dar la definición formal:

Definición 12.2 Fijados dos puntos F_1 y F_2 llamados *focos* y un número real positivo d, llamamos *elipse* $\mathcal{E}$ al conjunto de puntos cuya suma de las distancias a los focos es d.
En símbolos:

$$\mathcal{E} = \{P \in \mathbb{R}^2 : dist(P,F_1) + dist(P,F_2) = d\}.$$

Busquemos la fórmula:
Dos puntos (los focos) determinan una recta, supongamos que esa recta es el eje de las abscisas. Por el punto medio de los focos trazamos una perpendiclar que será nuestro eje de ordenadas. De este modo las coordenadas de los focos están en los puntos $F_1 = (-c, 0)$ y $F_2 = (c, 0)$. ¿Recordamos el hilo que está clavado en F_1 y F_2? cuando la punta del lápiz toca el eje de las ordenadas (positivas o negativas), se forma un triángulo isósceles entre el hilo y el eje de las abscisas, de altura, digamos b. El lado del triángulo digamos que mide a, vemos entonces que la longitud del hilo es $2a$ y que $a^2 = b^2 + c^2$.
Un punto $P = (x, y) \in \mathcal{E}$ si

$$dist(P, F_1) + dist(P, F_1) = 2a$$

$$\sqrt{(x+c)^2 + (y-0)^2} + \sqrt{(x-c)^2 + (y-0)^2} = 2a$$

o lo que es lo mismo:

$$\sqrt{(x+c)^2 + (y-0)^2} = 2a - \sqrt{(x-c)^2 + (y-0)^2}$$

Elevemos ambos miembros al cuadrado:

$$(x+c)^2 + (y-0)^2 = 4a^2 - 4a\sqrt{(x-c)^2 + (y-0)^2} + (x-c)^2 + (y-0)^2$$

$$x^2 + 2xc + c^2 + y^2 = 4a^2 - 4a\sqrt{(x-c)^2 + (y-0)^2} + x^2 - 2xc + c^2 + y^2$$

Eliminamos los sumandos iguales:

$$2xc = 4a^2 - 4a\sqrt{(x-c)^2 + (y-0)^2} - 2xc$$

Dejamos la raíz sola:

$$4xc - 4a^2 = -4a\sqrt{(x-c)^2 + (y-0)^2}$$

Elevamos nuevamente al cuadrado:

$$(4xc - 4a^2)^2 = 16a^2((x-c)^2 + (y-0)^2)$$

$$16x^2c^2 + 16a^4 - 32xca^2 = 16a^2(x^2 - 2xc + c^2 + y^2)$$

$$16x^2c^2 + 16a^4 - 32xca^2 = 16a^2x^2 - 32a^2xc + 16a^2c^2 + 16a^2y^2)$$

Eliminamos los sumandos iguales y dejamos las constantes a un lado del igual:

$$16a^4 - 16a^2c^2 = 16a^2x^2 - 16x^2c^2 + 16a^2y^2$$

Sacamos factor común:

$$16a^2(a^2 - c^2) = 16(a^2 - c^2)x^2 + 16a^2y^2$$

Simplificamos y, recordando que $a^2 = b^2 + c^2$ sustituímos $b^2 = a^2 - c^2$.

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

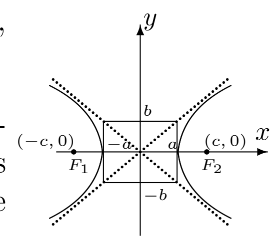
Dividimos por a^2b^2:

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

Que es finalmente la ecuación del óvalo inscripto en un rectángulo de vértices (a, b), $(-a, b)$, $(-a, -b)$ y $(a, -b)$.

12.1.3. Hipérbola

Si en lugar de pedir que la suma de sus distancias sea un número fijo, pedimos que la diferencia lo sea, obtenemos la llamada hipérbola:



Definición 12.3 Fijados dos puntos F_1 y F_2 llamados *focos* y un número real positivo $2a$, llamamos *hipérbola* $\mathcal{H}$ al conjunto de puntos cuya diferencia de las distancias a los focos es $2a$.
En símbolos:

$$\mathcal{H} = \{P \in \mathbb{R}^2 : dist(P, F_1) - dist(P, F_2) = 2a\}.$$

Busquemos la fórmula:
Un punto $P = (x, y) \in \mathcal{H}$ si

$$dist(P, F_1) - dist(P, F_1) = 2a$$

$$\sqrt{(x+c)^2 + (y-0)^2} - \sqrt{(x-c)^2 + (y-0)^2} = 2a$$

o lo que es lo mismo:

$$\sqrt{(x+c)^2 + (y-0)^2} = 2a + \sqrt{(x-c)^2 + (y-0)^2}$$

Elevemos ambos miembros al cuadrado:

$$(x+c)^2 + (y-0)^2 = 4a^2 + 4a\sqrt{(x-c)^2 + (y-0)^2} + (x-c)^2 + (y-0)^2$$

$$x^2 + 2xc + c^2 + y^2 = 4a^2 + 4a\sqrt{(x-c)^2 + (y-0)^2} + x^2 - 2xc + c^2 + y^2$$

Eliminamos los sumandos iguales:

$$2xc = 4a^2 + 4a\sqrt{(x-c)^2 + (y-0)^2} - 2xc$$

Dejamos la raíz sola:

$$4xc - 4a^2 = 4a\sqrt{(x-c)^2 + (y-0)^2}$$

Elevamos nuevamente al cuadrado:

$$(4xc - 4a^2)^2 = 16a^2((x-c)^2 + (y-0)^2)$$

$$16x^2c^2 + 16a^4 - 32xca^2 = 16a^2(x^2 - 2xc + c^2 + y^2)$$

$$16x^2c^2 + 16a^4 - 32xca^2 = 16a^2x^2 - 32a^2xc + 16a^2c^2 + 16a^2y^2)$$

Eliminamos los sumandos iguales y dejamos las constantes a un lado del igual:

$$16a^4 - 16a^2c^2 = 16a^2x^2 - 16x^2c^2 + 16a^2y^2$$

Sacamos factor común:

$$16a^2(a^2 - c^2) = 16(a^2 - c^2)x^2 + 16a^2y^2$$

Venimos igual que en la elipse, pero recordemos que estamos restando, entonces $a^2 - c^2 < 0$¿Por qué? Tenemos los dos focos en el eje de las abscisas. La distancia entre los focos es $2c$, la diferencia de las distancias es $2a$, entonces $2a \leq 2c$ y como son distancias, son positivas, $a < c$ y $a^2 < c^2$, entonces podemos decir que $a^2 - c^2 = b^2 < 0$ (aquí la b no aparece por la construcción, sino por los cálculos.)

Simplificamos y, sustituímos $-b^2 = a^2 - c^2$.

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

Dividimos por $-a^2b^2$:

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

Que es finalmente la ecuación de la curva que queda fuera del rectángulo de vértices $(a, b), (-a, b), (-a, -b)$ y $(a, -b)$. Esta curva se pega asintóticamente a las rectas que contienen a las diagonales del rectángulo, por eso se llama *asíntotas* de la hipérbola a las rectas:

$$L_1 : y = \frac{b}{a}x$$

$$L_2 : y = -\frac{b}{a}x$$

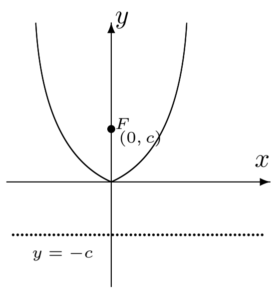
Los puntos $(a, 0)$ y $(-a, 0)$ se denominan *vértices* de la hipérbola.

12.1.4. Parábola

Ahora, en lugar medir distancias a dos puntos vamos a pedir que sean iguales las distancias a un punto y a una recta fijos, obtenemos entonces la llamada parábola:

Definición 12.4 Fijados un puntos F llamado *foco* y una recta d llamada *directriz*, llamamos *parábola* $\mathcal{P}$ al conjunto de puntos que distan lo mismo del foco que de la directriz.
En símbolos:

$$\mathcal{P} = \{P \in \mathbb{R}^2 : dist(P, F) = dist(P, d)\}.$$



Ubiquemos un sistema conveniente: consideremos una recta perpendicular a la directriz que pase por el foco. Ése será el eje de las ordenadas. El eje de las abscisas será paralelo a la directriz y pasará por el punto medio del segmento determinado por la intersección de la directriz y el eje de las ordenadas, y el foco. Supongamos, por el momento que la recta directriz ha quedado "abajo" y el foco "arriba". De este modo las coordenadas del foco son: $F = (0, c)$ y la ecuación de la directriz: $y = -c$. Pensemos tamién que en estas condiciones la distancia de un punto $P = (x, y)$ a la recta $y = -c$ es la distancia de $P = (x, y)$ a $Q = (x, -c) \in d$.

Busquemos la fórmula:
Un punto $P = (x, y) \in \mathbb{P}$ si

$$dist(P, F) = dist(P, d)$$

$$\sqrt{(x-0)^2 + (y-c)^2} = \sqrt{(x-x)^2 + (y-(-c))^2}$$

o lo que es lo mismo:

$$(x-0)^2 + (y-c)^2 = (x-x)^2 + (y-(-c))^2$$

$$x^2 + y^2 - 2cy + c^2 = y^2 + 2cy + c^2$$

Eliminando los sumandos iguales y despejando la y resulta:

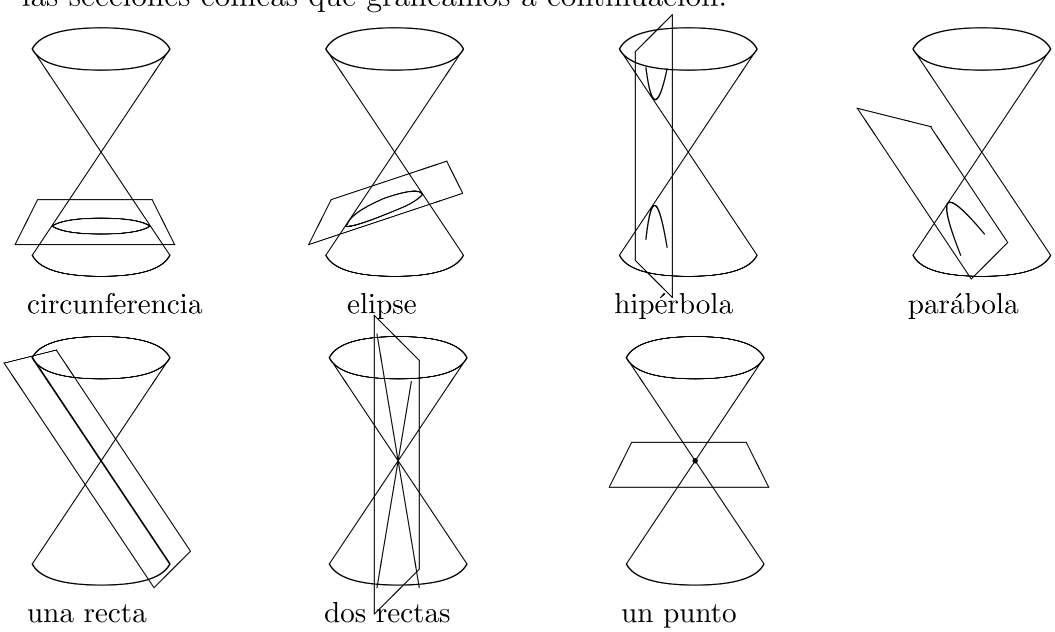
$$\frac{1}{4c}x^2 = y$$

El origen de coordenadas es el *vértice* y el eje de las ordenadas es el *eje de simetría* .

Es interesante comentar el nombre de la recta directriz. Pusimos los ejes de modo tal que el foco quedaba "arriba" y la directriz "abajo", esto nos hace obtener una parábola altamente "optimista" (sus brazos están levantados.) y la constante que acompaña a la x^2 es positiva. De haber dejado la recta "arriba" habríamos obtenido una triste parábola deprimida, es decir, de "brazos caídos" y la constante que acompaña a la x^2 es negativa.

12.1.5. Razón de ser

Hemos dado las ecuaciones y gráficas de circunferencia, elipse, hipérbola y parábola a partir de conservar ciertas relaciones cos distancias y las llamamos *cónicas* o bien *secciones cónicas*. No son todas. Además de ellas son secciones cónicas una recta, dos rectas que se cruzan y un punto.
Si bien en la heladería nos ofrecen un cono helado y nos dan un cucurucho y ni hablemos de los "conos" que se ponen en las calles, porque sobre todo los separadores de nuestro playón de Alem distan mucho de la noción geométrica, un cono es una superficie infinita que se parece a un cucurucho para arriba y otro para abajo. Cuando un plano corta este cono se producen en el plano las secciones cónicas que graficamos a continuación.



Para no olvidar ningún detalle, pongamos que la ecuación de dos rectas que se cortan es

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0$$

y la ecuación del origen (un punto) es

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 0.$$

Queda como entretenimiento para el lector comprobar estas ecuaciones. ®

12.2. Cuádricas

Una *cuádrica* es simplemente la superficie cuya ecuación tiene la forma:

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz + gx + hy + jz + k = 0$$

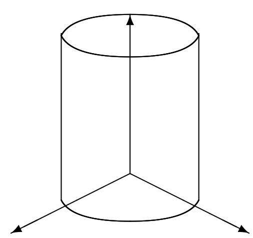
y siempre se puede encontrar un sistema de coordenadas en el que tenga alguna de las formas canónicas que describiremos a continuación y que se pueden ver ilustradas en la figura **??**:

12.2.1. Cilindro elíptico

La ecuación

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

representa una elipse (una circunferencia si $a = b$) en el plano XY. Si vamos al espacio, la z no tiene ningún tipo de restricción, por lo tanto se mantiene el mismo gráfico a lo largo de todo el eje z en planos paralelos al XY. (Si $a = b$ decimos que es un cilindro circular.)

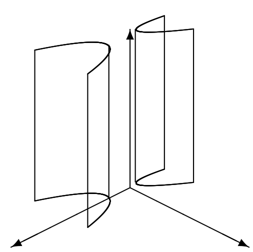


12.2.2. Cilindro hiperbólico

La ecuación

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

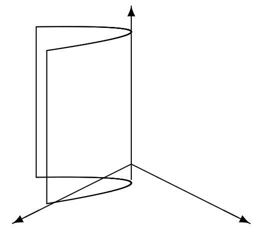
representa una hipérbola en el plano XY. Si vamos al espacio, la z no tiene ningún tipo de restricción, por lo tanto se mantiene el mismo gráfico a lo largo de todo el eje z en planos paralelos al XY.



12.2.3. Cilindro parabólico

La ecuación

$$\frac{x^2}{4a} = y$$

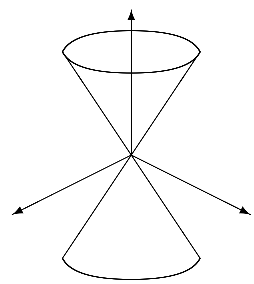


representa una parábola. Si vamos al espacio, la z no tiene ningún tipo de restricción, por lo tanto se mantiene el mismo gráfico a lo largo de todo el eje z en planos paralelos al XY. Suele escribirse se ecuación:

$$x^2 + ay = 0$$

12.2.4. Cono elíptico

Consideremos la ecuación:



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 0$$

Para cada valor de $z \neq 0$ tenemos:

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

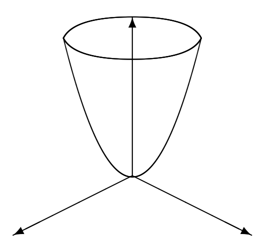
Es decir: para todos y cada uno de los posibles valores de $z \neq 0$ tenemos elipses en planos paralelos al XY (circunferencias si $a = b$ y entonces es un *cono circular*) que se van agrandando a medida que aumenta el valor absoluto de z y si $z = 0$ tenemos el origen de coordenadas.
Para cada valor de y (de x) tenemos:

$$\frac{x^2}{a'^2} - \frac{z^2}{c'^2} = 1 \quad (\frac{y^2}{a'^2} - \frac{z^2}{c'^2} = 1)$$

Es decir: hipérbolas en planos paralelos al XZ (YZ).

12.2.5. Paraboloide elíptico

Consideremos la ecuación:



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - z = 0$$

Para cada valor de z tenemos:

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

que tiene solución sólo si $z \geq 0$ y para todos y cada uno de los posibles valores de z tenemos elipses en planos paralelos al XY (circunferencias si $a = b$ y entonces es un *paraboloide circular*) que se van agrandando a medida que aumenta el valor de z.
Para cada valor de y (de x) tenemos:

$$\frac{x^2}{a'^2} = z - k_y \quad (\frac{y^2}{a'^2} = z - k_x)$$

Es decir: parábolas en planos paralelos al XZ (YZ).

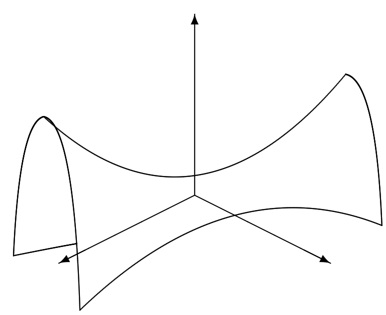
12.2.6. Paraboloide hiperbólico

Consideremos la ecuación:

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} - z = 0$$

Para cada valor de z tenemos:

$$\frac{x^2}{a'^2} - \frac{y^2}{b'^2} = z$$



Para todos y cada uno de los posibles valores de z tenemos hiperbólas en planos paralelos al XY.
Para cada valor de y tenemos parábolas "optimistas" en planos paralelos al XZ:

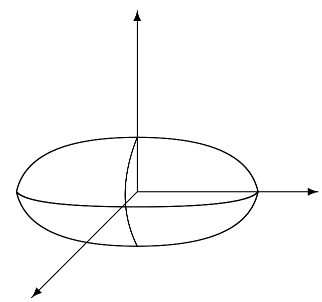
$$\frac{x^2}{a^2} = z - k_y$$

Para cada valor de x tenemos parábolas "pesimistas" en planos paralelos al YZ:

$$-\frac{y^2}{a^2} = z - k_x$$

Estamos en presencia de la "silla de montar". Para recordar el nombre notemos que hyallamos dos veces parábolas y una vez hipérbolas, de allí que es parabolOIDE (por las dos veces) hiperbólICO (un encuentro).

12.2.7. Elipsoide



Consideremos la ecuación:

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

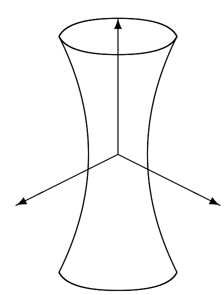
Para cada valor de z (y,x)tenemos elipses en planos paralelos al XY (XZ, YZ):

$$\frac{x^2}{a'^2}+\frac{y^2}{b'^2}=1(\frac{x^2}{a'^2}+\frac{z^2}{c'^2}=1)(\frac{y^2}{b'^2}+\frac{z^2}{c'^2}=1)$$

Claramente si $a=b=c$ estamos es presencia de una *esfera*.

Esto es lo que llamamos "pelota de rugby". Nuevamente, para recordar vemos que sólo hallamos elipses y de allí elipsOIDE.

12.2.8. Hiperboloide de una hoja o hiperboloide hiperbólico



Consideremos la ecuación:

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

Para cada valor de z quedan elipsoides es planos paralelos al XY:

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

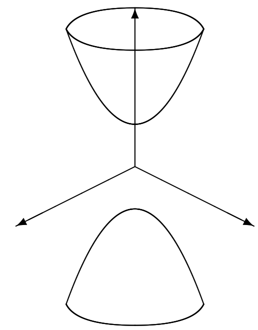
y para cada valor de y (de x) quedan hipérbolas en planos paralelos al XZ (YZ):

$$\frac{x^2}{a'^2}-\frac{z^2}{c'^2}=1(\frac{y^2}{b'^2}-\frac{z^2}{c'^2}=1).$$

12.2.9. Hiperboloide de dos hojas o hiperboloide elíptico

Consideremos la ecuación:

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



Para cada valor de z tal que tenga solución se obtienen elipses en planos paralelos al XY:

$$-\frac{x^2}{a'^2}-\frac{y^2}{b'^2}1,\ \text{para } 1-\frac{z^2}{c^2}<0,\ \text{es decir } \mid z\mid>\mid c\mid$$

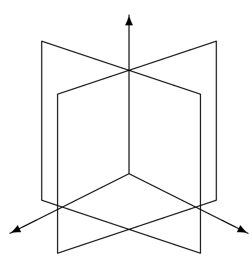
y para cada valor de y (de x) quedan hipérbolas en planos paralelos al XZ (YZ):

$$-\frac{x^2}{a'^2}+\frac{z^2}{c'^2}=1(-\frac{y^2}{b'^2}+\frac{z^2}{c'^2}=1).$$

12.2.10. Planos que se cortan

La ecuación que representa planos que se cortan en $\mathbb{R}^2$, con z libre en $\mathbb{R}^3$:

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



12.2.11. Una recta

La ecuación que representa el origen en $\mathbb{R}^2$, con z libre en $\mathbb{R}^3$ se convierte en el eje z:

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

Observación 12.2 Claramente hemos dado una posición de cada una, pero el lector interesado podrá fácilmente encontrar la ecuación del eje x:

$$\frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$$

o del hiperboloide de dos hojas, sobre el eje y:

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

sobre todo porque se las estamos dando en este momento.
Lo que sí es interesante es que podrá usarlas de ejemplo para hallar cualquiera que desee.

12.2.12. Comentario final

Hemos dicho que una cuádrica es una superficie con ecuación de la forma $ax^2 + by^2 + cz^2 + dxy + exz + fyz + gx + hy + jz + k = 0$ y luego dimos las "formas canónicas" de las cuádricas. ¿Cómo se relaciona esto? (Claramente una sección cónica, también es una expresión cuadrática, pero en dos variables).

Encontremos la forma canónica de una sección cónica y de una cuádrica para ver el proceso, simplemente a modo ilustrativo de una aplicación más para autovalores y autovectores.

Ejemplo 12.1 Comencemos con una sección cónica. Sea la ecuación

$$8\,x^2 + 17\,y^2 + 12\,x\,y - 8\,x - 16\,y - 8 = 0.$$

Vemos que es la suma de una parte cuadrática:
$T((x, y)) = 8\,x^2 + 17\,y^2 + 12\,x\,y,$
una parte lineal:
$L((x, y)) = -8\,x - 16\,y$
y término independiente:
$K = 8.$

1. Construimos la matriz de T:

Pensamos $T((x,y)) = 8\,x^2 + 17\,y^2 + 12\,x\,y$ como una transformación lineal simétrica en $\mathbb{R}^2$. Escribamos la matriz de esta transformación:

$$[T]_{\mathcal{C}_2} = \begin{array}{cc} & \begin{array}{cc} x & y \end{array} \\ \begin{array}{c} x \\ y \end{array} & \begin{pmatrix} 8 & 6 \\ 6 & 17 \end{pmatrix} \end{array}$$

Vemos que el coeficiente de x^2 está en la primera fila, primera columna, donde "se encuentra" x con x. Algo similar ocurre con 17, el coeficiente de y^2. Tanto en la primera fila segunda columna como en la segunda fila primera columna se encuentra x con y, entonces el coeficiente de xy va mitad para cada ubicación y nos garantizamos una matriz simétrica.

2. Buscamos autovalores y autovectores:

$$\begin{aligned} P_T(\lambda) &= |T - \lambda.I_2| = 0 \\ &= (8-\lambda)(17-\lambda) - 36 = \lambda^2 - 25\lambda + 136 - 36 = \lambda^2 - 25\lambda + 100 = \\ &= (\lambda - 20)(\lambda - 5) = 0 \end{aligned}$$

Los autovalores son $\lambda_1 = 5, \lambda_2 = 20$.

Busquemos los autovectores, para $\lambda_1 = 5$.

Planteamos el sistema $T((x,y)) = (5x, 5y)$, y obtenemos $x + 2y = 0$ y el subespacio de autovectores asociados a $\lambda_1 = 5$ es $V_5 = \{(-2a, a) : a \in \mathbb{R}\}$. Un versor en este espacio es $(-2/\sqrt{5}, 1\sqrt{5})$.

Como los autovalores son distintos y es una transformación lineal simétrica los autovectores son perpendiculares y podemos afirmar que el subespacio asociado a $\lambda_2 = 20$ es $V_{20} = \{(b, 2b) : b \in \mathbb{R}\}$. Un versor en este espacio es $(1\sqrt{5}, 2/\sqrt{5})$.

3. Definimos la base $\mathcal{B}$ asociada al sistema $0X'Y'$:

La base de autovectores es $\mathcal{B} = \{(-2/\sqrt{5}, 1\sqrt{5}), (1\sqrt{5}, 2/\sqrt{5})\}$.

$$[\mathcal{B}]_{\mathcal{C}} = \begin{pmatrix} -2/\sqrt{5} & 1\sqrt{5} \\ 1/\sqrt{5} & 2\sqrt{5} \end{pmatrix}$$

En esta base $[T]_{\mathcal{B}} = \begin{pmatrix} 5 & 0 \\ 0 & 20 \end{pmatrix}$.

4. Llevamos la parte lineal a la base $\mathcal{B}$ asociada al sistema $0X'Y'$:

$$[L]_{\mathcal{B}} = [\mathcal{B}]_{\mathcal{C}}^{t} \cdot [L]_{\mathcal{C}}$$

$$\begin{pmatrix} -2/\sqrt{5} & 1\sqrt{5} \\ 1/\sqrt{5} & 2\sqrt{5} \end{pmatrix} \cdot \begin{pmatrix} -8 \\ -16 \end{pmatrix} = \begin{pmatrix} 0 \\ -40/\sqrt{5} \end{pmatrix}$$

5. Reconstruimos la ecuación en el sistema $0X'Y'$:

La parte cuadrática ha quedado reducida a $5x'^2 + 20y'^2$ y la parte lineal a $0x' - 40/\sqrt{5}y'$. El término independiente no varía por cambio de base, entonces tenemos:

$$5\,x'^2 + 20\,y'^2 - 40/\sqrt{5}\,y' - 8 = 0$$

6. Hacemos completamiento de cuadrados para correr el origen:

$$5\,x'^2 + 20\,y'^2 - 40/\sqrt{5}\,y' - 8 = 0,$$

y la podemos pensar como

$$5\,x'^2 + 20(y'^2 - 2/\sqrt{5}y') - 8 = 5\,x'^2 + 20(y'^2 - 2/\sqrt{5}y' + 1/5 - 1/5) - 8 = 0$$

$$5\,x'^2 + 20(y' - 1/\sqrt{5})^2 - 12 = 0.$$

Sea

$$\begin{aligned} x'' &= x', \\ y'' &= y' - 1/\sqrt{5}, \end{aligned}$$

es decir, $0' = \langle 0, 1/\sqrt{5} \rangle$ y la ecuación, en el sistema $0'X''Y''$ queda:

$$5\,x''^2 + 20\,y''^2 = 12$$

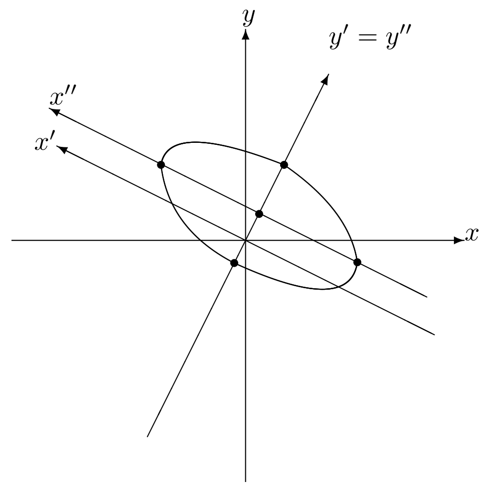
o lo que es lo mismo:

$$\frac{x''^2}{12/5} + \frac{y''^2}{12/20} = 1$$

y se trata de una elipse, que podemos dibujar sin inconvenientes:

1. Graficamos los ejes coordenados.
2. Buscamos el sistema $X'Y'$ graficando el vector $(-2, 1)$ como base para el eje X' y el $(1, 2)$ como base para el Y'.
3. En este nuevo sistema marcamos el punto $\langle 0, 1 \rangle$.
4. Trasladamos los ejes a este nuevo origen.

5. En el eje X'' marcamos los vértices $\pm 2\sqrt{3/5}$ y en el Y'' marcamos $\pm\sqrt{3/5}$
6. Graficamos la elipse.



Ejemplo 12.2 Vayamos ahora al espacio y trabajemos con una cuádrica. Sea la ecuación

$$2\,x^2 + 2\,y^2 + 5\,z^2 - 4\,x\,y - 2\,x\,z + 2\,x\,y + 10\,x - 26\,y - 2\,z = 0.$$

Vemos que, igual que antes, es la suma de una parte cuadrática:
$T((x,y,z)) = 2\,x^2 + 2\,y^2 + 5\,z^2 - 4\,x\,y - 2\,x\,z + 2\,x\,y,$
una parte lineal:
$L((x,y,z)) = 10\,x - 26\,y - 2\,z$
y en este caso no tiene término independiente:
$K = 0,$
pero ahora en tres variables.

1. Construimos la matriz de T:

Pensamos $T((x,y,z)) = 2\,x^2 + 2\,y^2 + 5\,z^2 - 4\,x\,y - 2\,x\,z + 2\,x\,y$ como una transformación lineal simétrica en $\mathbb{R}^3$. Escribamos la matriz de esta transformación:

$$[T]_{\mathcal{C}_3} = \begin{array}{c} \\ x \\ y \\ z \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 2 & -2 & -1 \\ -2 & 2 & 1 \\ -1 & 1 & 5 \end{pmatrix} \end{array}$$

Igual que en las secciones cónicas, los coeficientes de x^2, y^2 y z^2 están en la diagonal y los de xy, xz e yz (que en este caso son nulos) repartidos para lograr la matriz simétrica.

2. Buscamos autovalores y autovectores:

$$P_T(\lambda) = |T - \lambda.I_3| = 0$$
$$= (2-\lambda)^2(5-\lambda)+2+2-(2-\lambda)-(2-\lambda)-4(5-\lambda) = -\lambda(\lambda^2-9\lambda+18) =$$
$$= -\lambda(\lambda-6)(\lambda-3) = 0$$

Los autovalores son $\lambda_1 = 6, \lambda_2 = 3, \lambda_3 = 0$.

Busquemos los autovectores, para $\lambda_1 = 6$.

Planteamos el sistema $T((x, y, z)) = (6x, 6y, 6z)$, y obtenemos el subespacio de autovectores asociados a $\lambda_1 = 6$:

$V_6 = \{(a, -a, -2a) : a \in \mathbb{R}\}$, un versor en este espacio es $(1/\sqrt{6}, -1\sqrt{6}, -2/\sqrt{6})$.

Planteamos el sistema $T((x, y, z)) = (3x, 3y, 3z)$, y obtenemos el subespacio de autovectores asociados a $\lambda_2 = 3$:

$V_3 = \{(-b, b, -b) : b \in \mathbb{R}\}$, un versor en este espacio es $(-1/\sqrt{3}, 1\sqrt{3}, -1/\sqrt{3})$.

Como los autovalores son distintos y es una transformación lineal simétrica los autovectores son perpendiculares y podemos afirmar que el subespacio asociado a $\lambda_3 = 0$ está generado por el producto vectorial de loa autovectores hallados, entonces

$V_0 = \{(c, c, 0) : c \in \mathbb{R}\}$, un versor en este espacio es $(1\sqrt{2}, 1/\sqrt{2}, 0)$.

3. Definimos la base $\mathcal{B}$ asociada al sistema $0X'Y'Z'$:

La base de autovectores es

$$\mathcal{B} = \{(1/\sqrt{6}, -1\sqrt{6}, -2/\sqrt{6}), (-1/\sqrt{3}, 1\sqrt{3}, -1/\sqrt{3}), (1\sqrt{2}, 1/\sqrt{2}, 0)\}.$$

En esta base $[T]_{\mathcal{B}} = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

4. Llevamos la parte lineal a la base $\mathcal{B}$ asociada al sistema $0X'Y'$:

$$[L]_{\mathcal{B}} = [\mathcal{B}]_{\mathcal{C}}^t \cdot [L]_{\mathcal{C}}$$

$$\begin{pmatrix} 1/\sqrt{6} & -1\sqrt{6} & -2/\sqrt{6} \\ -1/\sqrt{3} & 1\sqrt{3} & -1/\sqrt{3} \\ 1/\sqrt{2} & 1/\sqrt{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ -26 \\ -2 \end{pmatrix} = \begin{pmatrix} 40/\sqrt{6} \\ -34/\sqrt{3} \\ -16/\sqrt{2} \end{pmatrix}$$

5. Reconstruimos la ecuación en el sistema $0X'Y'$:

La parte cuadrática ha quedado reducida a $6\,x'^2 + 3\,y'^2 + 0\,z'^2$ y la parte lineal a $40/\sqrt{6}\,x' - 34/\sqrt{3}\,y' - 16/\sqrt{2}\,z'$. El término independiente no varía por cambio de base, entonces tenemos:

$$6x'^2 + 3y'^2 + 0\,z'^2 + 40/\sqrt{6}\,x' - 34/\sqrt{3}\,y' - 16/\sqrt{2}\,z' = 0$$

6. Hacemos completamiento de cuadrados para correr el origen:

$(6\,x'^2 + 40/\sqrt{6}\,x') + (3\,y'^2 - 34/\sqrt{3}\,y') - 16/\sqrt{2}\,z' = 0$, y la podemos pensar como $6\,x''^2 + 3\,y''^2 = z''$ y concluimos que se trata de un cono elíptico.

Capítulo 13

"Profe... ¿Cómo se demuestran las cosas?"

"Uno cuando quiere demostrar algo,
se desespera y agarra lo que encuentra."
G.E.

A lo largo de los cuatrimestres, la pregunta sigue siendo la misma: "Profe... ¿Cómo se demuestran las cosas?" La respuesta dista mucho de ser breve, porque cada proposición es un mundo. Pero ya que estamos sentados charlando...

Comencemos aclarando que matemáticamente un hecho es verdadero si lo es en todas sus instancias. Una afirmación verdadera es, por ejemplo "todos los humanos tienen al menos un corazón". Independientemente del grado de sensibilidad de cada uno, sin el motor, la máquina humana no funciona y cada humano que veamos tendrá dentro (al menos por ahora) un corazón. La frase "todos los humanos tienen 20 dedos" no es verdadera porque debido a malformaciones o accidentes puede haber alguien que no llegue a tener los "20 dedos estándar" o que tenga alguno de más. Entonces para demostrar que una determinada afirmación es verdadera, habrá que realizar algún tipo de demostración.
Siguiendo con la misma idea, basta 1 ejemplo de lo contrario para ver que algo no es cierto. Es decir, si yo afirmo "todos los perros de la universidad son negros" me alcanza para convencerme de que no es cierto que me muestren que hay uno marrón. Al mostrar el perro marrón estamos dando un ejemplo

de lo contrario, es decir, un *contraejemplo*.

Ejemplo 13.1 “La función $f(x) = |x|$ es positiva en todo su dominio” es una afirmación FALSA. Contraejemplo. $0 \in D(f)$ y $|0| = 0 \not> 0$. Me pueden decir, “pero... justo acertaste al único valor en que no es cierta.” Correcto. Con uno alcanza.

13.1. Demostraciones

El primer paso para demostrar algo es tener la total certeza de que somos capaces de hacerlo. Sin dicho convencimiento, no hay posibilidad de éxito.
Una vez saltada esta valla, comenzamos el proceso:

1. Distinguir claramente cuáles son las *hipótesis*, que son las cosas que sabemos, podemos y debemos usar en la demostración y qué es los que queremos probar, es decir, la *tesis*.
2. Analizar de qué tema se trata y tener a mano todas las definiciones, propiedades y caracterizaciones que conocemos (Es muy bueno tenerlas en la cabeza, pero de usarlas, realmente entran solas. Al principio basta con tenerlas en una hoja al lado.)
3. Escribir las hipótesis y la tesis en un lenguaje que nos resulte conocido.
4. Caso1: Unir los pedacitos, siguiendo el camino. Porque a esta altura, verán claramente que tienen la demostración delante de los ojos.
   Caso 2: Si no se pueden unir los pedacitos fácilmente, probar con ejemplos sencillos. La búsqueda de este ejemplo sencillo nos puede dar la pista de cómo unir los pedacitos. También es posible que buscando el ejemplo sencillo, encontremos un contraejemplo. Finalmente si no hay contraejemplo y no podemos construir una demostración directa, trataremos por el absurdo. (Vamos a comentar este punto a la brevedad.)
5. Al terminar la demostración, avisarlo tal vez con un *cqd* (como queríamos demostrar) que es la versión castellana del viejo *qed* (quod erat demostrandum) o bien el elegante y nunca bien ponderado: (ver al final del renglón.) $\square$.

Cada vez que tenemos que probar una afirmación del tipo *si... entonces...* lo que está entre *si* y *entonces* son las *hipótesis*. Lo que está escrito después del *entonces* es la *tesis*, lo que queremos probar. Hay enunciados “disfrazados” como puede ser el caso de:

La suma de dos números impares es par.

Este tipo de afirmaciones lo podemos pasar a un *si... entonces...* fácilmente:

Si a y b son impares, entonces $a + b$ es par.

Hay diversos métodos que se utilizan según el caso.

13.1.1. Método directo

Suponemos que las hipótesis son verdaderas y probamos la tesis.

Ejemplo 13.2 Demostremos la propiedad que acabamos de enunciar. Analicemos el caso:
Hipótesis: a y b impares.
Tesis: $a + b$ par.

Lo reescribimos según los conocimientos matemáticos que tenemos:
Hipótesis: $a = 2k_a + 1,\ b = 2k_b + 1$.
Tesis: $a + b = 2k$.

Demostración: Analizamos de qué habla la propiedad: dice "la suma...", entonces ¡sumemos! (Usando siempre las hipótesis.)

$a+b = (2k_a+1)+(2k_b+1) \overset{1}{=} 2k_a+2k_b+1+1 \overset{2}{=} 2k_a+2k_b+2 \overset{3}{=} 2(k_a+k_b+1) = 2k$.

1: por propiedades asociativa y conmutativa de la suma,
2: por la suma de 1+1,
3: sacando factor común. □

Observación 13.1 En este tipo de demostraciones, en las que se dice "es par entonces lo escribo $2k$" (o es impar, da lo mismo) acerca de dos o más números, hay que diferenciar bien los "k" que se usan porque no necesariamente son iguales y no debemos forzar a que lo sean. En este caso usamos k_a y k_b y cuando terminamos, arbitrariamente llamamos k a la suma $k_a + k_b + 1$.

Ejemplo 13.3 Sea $f : A \to B$ una función. $X_1, X_2 \subseteq A$ Probar que si $X_1 \subseteq X_2$, entonces $f(X_1) \subseteq f(X_2)$.

Analicemos el caso:
Hipótesis: $f : A \to B$ una función. $X_1, X_2 \subseteq A$, $X_1 \subseteq X_2$.

Tesis: $f(X_1) \subseteq f(X_2)$.

Buscamos tener a mano todas las definiciones que nos puedan ser útiles:
$f(X_1) = \{f(x) \in B : x \in X_1\}, f(X_2) = \{f(x) \in B : x \in X_2\}$,
y reescribimos la proposición en lenguaje matemático:
Hipótesis: $x \in X_1 \Rightarrow x \in X_2$.
Tesis: $f(x) \in \{f(x) \in B : x \in X_1\} \Rightarrow f(x) \in \{f(x) \in B : x \in X_2\}$.

Demostración: Analizamos de qué habla la propiedad: dice "está contenido", entonces tenemos que ver que todo habitante de $f(X_1)$ es habitante de $f(X_2)$. (Aquí lo más importante es ver qué aspecto tiene un habitante de los que buscamos y para eso usamos la definición. (La demostración YA es nuestra.)

Sea $f(x) \in f(X_1)$, por la definición de $f(X_1)$ resulta que $x \in X_1$ pero por hipótesis, si $x \in X_1$ resulta que $x \in X_2$ y, en consecuencia $f(x) \in f(X_2)$. $\square$

13.1.2. Método por cálculo directo

Cuando tenemos que probar una igualdad, el proceso siempre consiste en "salir de un lado" para "llegar al otro". Nunca debemos "llevar el igual" y modificar ambas expresiones. ¿Por qué? En primer lugar porque debemos estar seguros de que las expresiones a ambos lados del signo igual son realmente equivalentes y en segundo lugar porque nos puede llevar a "pasar términos" o realizar otro tipo de procedimientos que nos alejen del buen camino.
Por si fuera poco, supongamos que dos personas se quieren encontrar. Si ambas comienzan a caminar simultáneamente, la probabilidad de desencuentro es alta. Sin embargo si una permanece en un sitio esperando a la otra seguramente se encontrarán.
En caso de no saber continuar a partir de un cierto punto es factible dejar la expresión y comenzar a trabajar con el otro miembro hasta llegar al mismo punto.

Ejemplo 13.4 Probar que:

$$z.\bar{z} = |z|^2$$

En primer lugar busquemos una expresión para trabajar: Si $z = a + i\,b$ resulta $\bar{z} = a - i\,b$ y $|z|^2 = a^2 + b^2$.
Ahora hagamos cuentas:
$z.\bar{z} = (a + i\,b).(a - i\,b) = a^2 - i\,ab + i\,ab + b^2 = a^2 + b^2 = |z|^2$. $\square$

Ejemplo 13.5 Probar que:

$$\frac{n(n+1)(4n-1)}{3} + [2(n+1)-1]2(n+1) = \frac{(n+1)(n+2)[4(n+1)-1]}{3}$$

Este es uno de los casos en que resulta complicado hacer un "trayecto directo", entonces comencemos a caminar hasta donde podamos:

$$\frac{n(n+1)(4n-1)}{3} + [2(n+1)-1]2(n+1) = \frac{n(n+1)(4n-1)}{3} + (2n+1)2(n+1) =$$

$$= \frac{n(n+1)(4n-1)+3(2n+1)2(n+1)}{3} = \frac{(n+1)(n(4n-1)+6(2n+1))}{3} =$$

$$\frac{(n+1)(4n^2+11n+6)}{3} \quad (\bigstar)$$

Ahora empecemos del otro lado, tenemos todo dividido por 3 y y tenemos un factor común $n+1$. Eso no lo toquemos:

$$\frac{(n+1)(n+2)[4(n+1)-1]}{3} = \frac{(n+1)(n+2)(4n+3)}{3} = \frac{(n+1)(4n^2+3n+8n+6)}{3}$$

$$= \frac{(n+1)(4n^2+11n+6)}{3} \quad (\bigstar\bigstar)$$

Como $(\bigstar)$ es igual a $(\bigstar\bigstar)$ resulta

$$\frac{n(n+1)(4n-1)}{3} + [2(n+1)-1]2(n+1) = \frac{(n+1)(n+2)[4(n+1)-1]}{3}$$

$\square$

13.1.3. Igualdad de conjuntos

Se define que dos conjuntos son iguales si tienen exactamente los mismos elementos. Es decir $A = B$ si todo elementos de A es elemento de B y viceversa. Todo elemento de A es elemento de B se representa $A \subseteq B$ y todo elemento de B es elemento de A es lo mismo que $A \supseteq B$. Entonces resulta $A = B$ es equivalente a $A \subseteq B$ y $B \subseteq A$.
En consecuencia, para probar que dos conjuntos son iguales ($A = B$) debemos probar siempre dos proposiciones:

(P1) $A \subseteq B$

(P2) $B \subseteq A$

Por este motivo decimos que las demostraciones de igualdad de conjuntos son por doble inclusión. Cuando ya conocemos propiedades, que hemos demostrado por doble inclusión, podemos utilizarlas para simplificar el enunciado que hay que probar.

Método por doble inclusión

Ejemplo 13.6 Demostrar $(A \cup B)' = A' \cap B'$.

a) $(A \cup B)' \subseteq A' \cap B'$:
Sea $x \in (A \cup B)'$, entonces $x \notin A \cup B$, es decir $x \notin A$ y $x \notin B$, por lo tanto $x \in A'$ y $x \in B'$, y, en consecuencia, $x \in A' \cap B'$.

b) $(A \cup B)' \supseteq A' \cap B'$:
Sea $x \in A' \cap B'$, por lo tanto $x \in A'$ y $x \in B'$, es decir, $x \notin A$ y $x \notin B$ y, en consecuencia, $x \notin A \cup B$, es decir, $x \in (A \cup B)'$.

Por a) y b) afirmamos $(A \cup B)' = A' \cap B'$. $\square$

Método por cálculo directo

Las demostraciones para probar igualdad por cálculo directo consisten simplemente en "salir de un lado y llegar al otro". Lo más conveniente es tomar el lado de la igualdad que tenga "más cosas" porque es más fácil simplificar que añadir.

Ejemplo 13.7 Demostrar que $[A \setminus (A \cap B)] \cup [B \setminus (A \cap B)] \cup (A \cap B) = A \cup B$.

$$[A \setminus (A \cap B)] \cup [B \setminus (A \cap B)] \cup (A \cup B) \overset{1}{=} [A \cap (A \cap B)'] \cup [B \cap (A \cap B)'] \cup (A \cap B) \overset{2}{=}$$

$$\overset{2}{=} [(A \cup B) \cap (A \cap B)'] \cup (A \cap B) \overset{3}{=} [(A \cup B) \cup (A \cap B)] \cap [(A \cap B)' \cup (A \cap B)] \overset{4}{=}$$

$$\overset{4}{=} (A \cup B) \cap \mathcal{U} \overset{5}{=} A \cup B.$$

1: por definición de $A \setminus B$.
2: por propiedad distributiva (saqué "factor común").
3: por propiedad distributiva (ahora si distribuí).
4: por ley de absorción y ley de complemento.
5: por propiedades del conjunto $\mathcal{U}$.

$\square$

13.1.4. Método por casos

Hay algunas veces en que intentamos aplicar el método directo pero el camino "se bifurca" o aún más. El procedimiento en este caso es seguir todos los caminos posibles hasta el final y si absolutamente, por todos los caminos posibles llegamos al mismo sitio, afirmamos que la propiedad es verdadera. Es muy importante chequear todos. Si sólo uno entre mil caminos lleva a la princesa a ser comida por el tigre... Es probable que nos quedemos sin princesa.

Ejemplo 13.8 Sean A, B, C tres conjuntos. $A \subseteq C, B \subseteq C \Rightarrow (A \cup B) \subseteq C$. Hay que demostrar que cualquier elemento de $A \cup B$ es elemento de C.

Demostración: Sea $x \in A \cup B$. Hay dos casos posibles:

Caso 1: $x \in A$. Como $A \subseteq C$ resulta $x \in C$.

Caso 2: $x \in B$. Como $B \subseteq C$ resulta $x \in C$.

En cualquier caso, $x \in C$.

En consecuencia, $A \cup B \subseteq C$. □

Ejemplo 13.9 $A \cup A' = \mathcal{U}$.

Tenemos que probar que dos conjuntos son iguales. Hay dos opciones: por cálculo directo o por doble inclusión. Las demostraciones por cálculo directo son simples aplicaciones de reglas que se han demostrado ya por doble inclusión y se pueden realizar sólo si hay "algo para simplificar". Como no es ese el caso, necesariamente hay que probarlo por doble inclusión.

$A \cup A' \subseteq \mathcal{U}$ es trivial a partir de la definición de conjunto universal.

$A \cup A' \supseteq \mathcal{U}$. Sea $x \in \mathcal{U}$. Hay dos posibilidades: $x \in A$ o $x \notin A$.

Caso 1: $x \in A \subseteq A \cup A'$, por lo tanto $x \in A \cup A'$.
Caso 2: $x \notin A$, entonces $x \in A' \subseteq A \cup A'$, por lo tanto $x \in A \cup A'$.
En cualquier caso, $x \in A \cup A'$ y, en consecuencia, $\mathcal{U} = A \cup A'$.

□

Ejemplo 13.10 $a^3 - a$ es múltiplo de 3.

Esta es una demostración típica de divisibilidad. Queremos ver que algo es divisible por 3, y ese algo está en función del número a. ¿qué posibilidades hay para el número a relacionado con 3? Por el algoritmo de la divisi'on entera $a = 3k + r$ y el resto puede ser 0, 1 o 2. Esto va a ser una demostración por casos, con 3 casos.

Comencemos por factorizar $a^3 - a = a(a^2 - 1) = a(a-1)(a+1) = (a-1)a(a+1)$.

Caso 1: $a = 3k$, entonces $(a-1)a(a+1) = (3k-1)\underline{(3k)}(3k+1) = 3t$.

Caso 2: $a = 3k+1$, entonces $(a-1)a(a+1) = \underline{(3k)}(3k+1)(3k+2) = 3t$.

Caso 3: $a = 3k+2$, entonces $(a-1)a(a+1) = (3k+1)(3k+2)(3k+3) =$

$= (3k+1)(3k+2)\underline{(3(k+1))} =$ $3t$.

En cualquier caso resulta $a^3 - a$ múltiplo de 3.

□

13.1.5. Método por el absurdo

En este tipo de demostraciones negamos lo que queremos probar y llegamos a una contradicción.

Ejemplo 13.11 $A \cap \emptyset = \emptyset$.
Queremos probar que $A \cap \emptyset = \emptyset$, suponemos, por el absurdo que no. Entonces existe un elemento $x \in A \cap \emptyset$. Por definición de intersección $x \in A$(no hay ningún problema con esto) y $x \in \emptyset$, lo cual es un absurdo que provino de suponer $A \cap \emptyset \neq \emptyset$. En consecuencia $A \cap \emptyset = \emptyset$. □

Ejemplo 13.12 $\sqrt{2} \in \mathbb{Q}$.

Suponemos por el absurdo que sí es un número racional. Es decir, suponemos que existe $\frac{a}{b} = \sqrt{2}$, con $(a, b) = 1$.

Le estamos pidiendo a $(a, b) = 1$ para no enredarnos con fracciones que se puedan reducir (como es el caso de 2/6 o 5/15). No olvidemos tener a mano todas las propiedades de divisibilidad de enteros, que es lo que vamos a usar. Las siguientes afirmaciones son equivalentes:

$$\frac{a}{b} = \sqrt{2}$$

$$\frac{a^2}{b^2} = 2$$
$$a^2 = 2b^2$$

Si esto fuera cierto, la descomposición en factores primos (que es única) de a^2 sería igual a la de $2b^2$, pero claramente el número 2 está “una vez más” a la derecha del igual que a la izquierda. Con mayor rigor matemático afirmamos que en a^2 el factor 2 está un número par de veces y en $2b^2$ está un número par más una vez más. Absurdo que provino de suponer que $\sqrt{2}$ es un número racional, por lo tanto, $\sqrt{2} \notin \mathbb{Q}$. $\square$

13.1.6. Método de la contrapositiva

Para hacer un razonamiento usando la ley contrapositiva usamos la equivalencia entre “si p entonces q” y “si no q entonces no p”. Podemos verla en lenguaje cotidiano. Supongamos que yo voy todos los lunes al cine. Absolutamente todos los lunes, sin faltar, entonces es verdadero:

Si es lunes, entonces Rosana está en el cine.

Alguien va al cine y no me encuentra. Dice a su acompañante con total seguridad: “hoy no es lunes”. ¿Por qué?

Rosana no está en el cine, entonces no es lunes.

La línea que separa una demostración por el absurdo con una demostración usando la ley contrapositiva es bastante débil. Cuando hacemos una demostración por el absurdo suponemos que son válidas simultáneamente las hipótesis y la negación de lo que queremos probar y llegamos a un hecho no posible. Sin embargo en la contrapositiva partimos sólo de la negación de lo que queremos probar y llegamos a negar las hipótesis.

13.1.7. Pruebas de unicidad

Podría pensarse que estas demostraciones son por el absurdo, porque cada vez que se quiere probar que algo es único partimos de “supongamos que hay dos”.

Si sólo decimos “supongamos que hay dos” y llegamos a probar que son iguales, no hay ningún absurdo. Para estar usando la ley del absurdo debemos decir, supongo que hay dos distintos. De cualquier modo, es algo que hace más a la formalidad que al hecho en sí. Veamos ejemplos:

Ejemplo 13.13 El elemento neutro para la suma en $\mathbb{Z}$ es único. Dicho de otro modo: el 0 es único. Buscamos en la definición qué es el neutro para la suma, es un elemento que notamos con 0 tal que $0 + a = a + 0 = a$ para todo $a \in \mathbb{Z}$. Usemos esto en la demostración: Supongamos que existen dos elementos neutros para la suma en $\mathbb{Z}$, sean 0 y $0'$

(1) $0 = 0 + 0'$, (porque $0'$ es neutro)

(2) $0' = 0 + 0'$, (porque 0 es neutro)

(3) Como $0 + 0' = 0 + 0'$ de (1) y (2) resulta $0 = 0'$.

$\square$

Ejemplo 13.14 El teorema del algoritmo de división entera dice que dados a y b enteros, $b \neq 0$ existen q y r unívocamente determinados tales que $a = q.b + r$, $0 \leq r < b$. Ese “unívocamente determinados” indica que hay que probar la unicidad. Como siempre partimos de suponer que hay dos:

Sean q_1, r_1 y q_2, r_2 tales que $a = q_1.b + r_1$ y $a = q_2.b + r_2$. Entonces $q_1.b + r_1 = q_2.b + r_2$ y resulta $(q_1 - q_2).b = r_2 - r_1$.
Las posibilidades son $r_2 = r_1$ o $r_2 \neq r_1$.
Si fuera $r_2 \neq r_1$ resultaría $r_2 - r_1 \neq 0$, es decir, $(q_1 - q_2).b \neq 0$ y, en consecuencia $|r_2 - r_1| = |(q_1 - q_2).b| = |q_1 - q_2|.|b| \geq |b|$ (si $q_1 - q_2 \neq 0$, entonces $|q_1 - q_2| \geq 1$), lo cual es un absurdo.
Veamos explícitamente este absurdo: Ha quedado escrito $|r_2 - r_1| \geq |b|$. Los restos son “los que sobran” que siempre son menos que b, la diferencia entre dos cantidades menores que b jamás puede ser mayor o igual que b. $\square$

Observación 13.2 Mencionamos el algoritmo de la división entera que es un teorema de existencia y unicidad, como también lo es la existencia y unicidad del mínimo común múltiplo. Menciono estos dos teoremas porque en las demostraciones dadas en el apunte tienen una gran diferencia:

- La demostración del algoritmo de la división entera se basa en el Principio de Buena Ordenación y dice, en una forma muy elegante, por cierto “existen q y r”. ¡qué lindos! ¿a verlos? No, lo siento, sólo he demostrado que existen, no tengo ni idea de cómo son.
- La demostración de existencia del mínimo común múltiplo dice: Sea $m = d.k_a.k_b$ donde $d = (a, b), a = d.k_a, b = d.k_b$, veamos que $m = [a, b]$. Es lo que se llama una demostración constructiva. No requiere en absoluto de profesión de fe.

13.1.8. Demostraciones de equivalencias

Los enunciados que tienen el símbolo $\Leftrightarrow$ o dicen *si y sólo si* o en sus formas abreviadas *sssi* o *sii* o *condición necesaria y suficiente* son todas demostraciones de hechos equivalentes. Claramente admiten ser demostrados en dos partes. Veamos un ejemplo en lenguaje cotidiano:

Supongamos que en un pueblo hay un único teatro que abre absolutamente todos los sábados y nada más que los sábados, sin excepción. Podemos decir:

El teatro abre $\Leftrightarrow$ es sábado.

El teatro abre si y sólo si es sábado.

Es condición necesaria y suficiente que sea sábado para que abra el teatro.

Vamos a escribir lo anterior como pares de implicaciones:
Las implicaciones ($\Rightarrow$):

Si el teatro abre, entonces es sábado.

El teatro abre $\Rightarrow$ es sábado.

El teatro abre sólo si es sábado.

Es condición necesaria que sea sábado para que abra el teatro.

Las implicaciones ($\Leftarrow$):

Si es sábado, entonces el teatro abre.

El teatro abre $\Leftarrow$ es sábado.

El teatro abre si es sábado.

Es condición suficiente que sea sábado para que abra el teatro.

Veamos ejemplo:

Ejemplo 13.15 Es condición necesaria y suficiente que a sea par para que a^2 sea par.

Veamos la condición suficiente "a^2 es par $\Leftarrow$ a es par" o "a^2 par si a" es par.

Supongamos que $a = 2k$. Como habla de elevar al cuadrado, elevamos al cuadrado: $a^2 = (2k)^2 = 2.(2.k^2) = 2.t$ y queda demostrado que a^2 es par.

La condición necesaria "a^2 es par $\Rightarrow a$ es par" o "a^2 par sólo si a es par".

Para demostrarlo usaremos el principio contrapositivo. Ya que un número sólo puede ser par o impar, supongamos que es impar.

Sea $a = 2k+1$ entonces $a^2 = (2k+1)^2 = (2k)^2 + 2.2k + 1 = 2.(k^2 + 2k) + 1 = 2t + 1$.
Es decir, a^2 es impar. $\square$

13.1.9. Método por equivalencias

Este tipo de demostraciones se reduce a una sucesión de expresiones equivalentes. En verdad, nunca se han hecho así, sino que al realizar la prueba "de vuelta" se nota que es el camino exactamente al revés y se ponen las flechitas para el otro lado. No es necesario hacerlas de este modo, pero sí, en los textos, queda muy elegante.

Ejemplo 13.16 Probar $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Son equivalentes:

$$\begin{aligned}
&(x, y) \in A \times (B \cap C)\\
&x \in A, y \in B \cap C\\
&x \in A,\ y \in B,\ y \in C\\
&(x, y) \in A \times B, (x, y) \in A \times C\\
&(x, y) \in (A \times B) \cap (A \times C)
\end{aligned}$$

Esto demuestra la igualdad de conjuntos. $\square$

13.1.10. Método inductivo

El método inductivo se usa (se debe usar siempre) para demostrar cualquier cosa que tenga que ver con los números naturales. La caracterización de los números naturales es que si elijo uno cualquiera tengo sólo dos posibilidades:

Es el primero.

Es el sucesor de alguien.

Inducción débil

"Si soy capaz de subir al primer escalón y, parada en cualquier escalón acceder al siguiente, puedo llegar a cualquier altura que me proponga."

Debemos probar que somos capaces de pararnos en el primer escalón (es decir, que se verifica lo que llamamos "el caso base") y que parados en cualquier escalón somos capaces de subir al siguiente (es decir, suponemos que lo que queremos probar es válido para $n = k$ y, usando esta hipótesis, llamada "hipótesis inductiva", probar que la propiedad se verifica para $n = k + 1$. Lo que hemos hecho es ver que somos capaces de acceder a cualquier nivel, es decir, la conclusión que sacamos es que la propiedad es válida para todo $n \in \mathbb{N}$.

Ejemplo 13.17 $3^n - 1$ es par.

(1) Caso base: $(n = 1)$ $3^1 - 1 = 2$, que es par, $\therefore$ es válido el caso base.

(2) Paso inductivo: Supongo que $3^k + 1$ es par y debo probar $3^{k+1} - 1$ es par.

$3^{k+1}-1 = 3^k.3-1$. por hipótesis inductiva $3^k-1 = 2s$, entonces $3^k = 2s+1$ y reemplazando obtenemos $3^{k+1}-1 = (2s+1).3-1 = 2s.3+3-1 = 2s.3+2 = 2(3s+1)$, en consecuencia, par.

De (1) y (2) resulta que $3^n - 1$ es par, para todo $n \in \mathbb{N}$. $\square$

Inducción fuerte

"Si soy capaz de subir el primer escalón y habiendo pasado por todos los anteriores subir al siguiente, entonces puedo llegar a cualquier altura de la escalera".

Si bien parece más fuerte que el anterior (y de hecho se llama fuerte) es absolutamente equivalente, pero hay casos en que no es posible subir los escalonres de a uno, como en la demostración de la descomposición en factores primos. Veamos otro ejemplo:

Ejemplo 13.18 La sucesión Fibonacci se define: $F_0 = 1, F_1 = 1, F_{n+2} = F_n + F_{n+1}$. Demostrar que $F_n \leq 2^n$, para todo $n \in \mathbb{N}$.

(1) Caso base: $(n = 0)$, $F_0 = 1 \leq 2^0$, $(n = 1)$, $F_1 = 1 \leq 2^1$. Se verifican ambos.

(2) Paso inductivo. Supongamos que $F_k \leq 2^k$ para todo $k < n$ y probémoslo para n.

$$F_n = F_{n-1} + F_{n-2} \leq 2^{n-1} + 2^{n-2} \leq 2^{n-1} + 2^{n-1} = 2.2^{n-1} = 2^n.$$

Afirmamos entonces que $F_n \leq 2^n$, para todo $n \in \mathbb{N}$. □

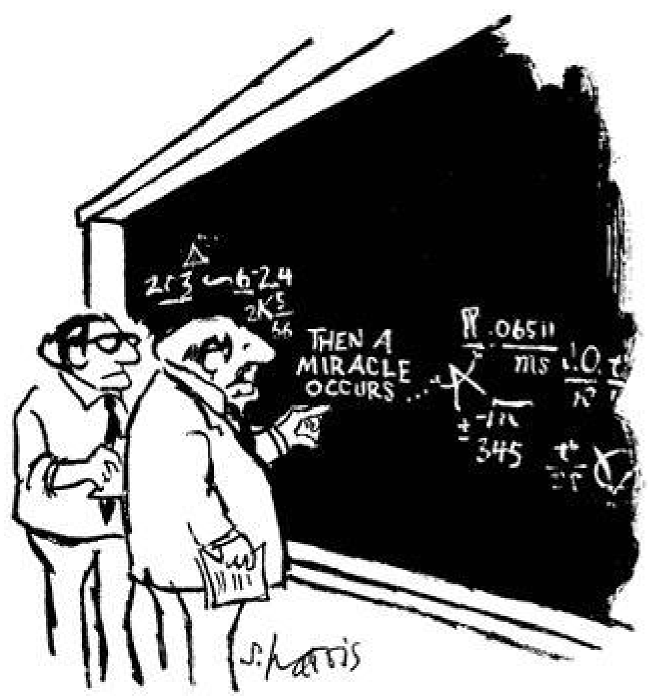
13.2. (♣)42 métodos de demostración

A continuación enunciaremos 42 métodos que no serán aceptables en parciales, finales y/o coloquios:

1. Demostración por Obviedad: "La demostración es tan evidente que no hace falta que sea mencionada"
2. Demostración por Acuerdo General: "¿Todos a favor… ? "
3. Demostración por Imaginación: "Bien, fingiremos que es cierto."
4. Demostración por Conveniencia: "Sería magnífico si esto fuera cierto, por tanto…"
5. Demostración por Necesidad: "Tendría que ser cierto o la estructura completa de la Matemática se derrumbaría."
6. Demostración por Verosimilitud: "Suena muy bien. Por tanto debe ser cierto."
7. Prueba por Intimidación: "No seas estúpido, naturalmente que es cierto."
8. Demostración por Falta de Tiempo: "Por problemas de tiempo te dejaré la demostración a ti."
9. Demostración por Aplazamiento: "La demostración de esto es demasiado larga. Por eso se da en el apéndice."
10. Demostración por Accidente: "Vaya!, qué tenemos aquí?"
11. Demostración por Falta de Importancia: ¿A quién le importa realmente?"
12. Demostración por Mumbo-Jumbo: "Para cada epsilon mayor que cero existe un delta mayor que cero tal que $f(x) - L$ es menor que epsilon siempre y cuando $x - a$ sea menor que delta."
13. Demostración por Blasfemia: (Ejemplo omitido)
14. Demostración por Definición: "Lo definiremos para que sea cierto."

15. Demostración por Tautología: “Es cierto porque es cierto.”
16. Demostración por Plagio: “Como podemos ver en la página 238…”
17. Demostración por Referencia Perdida: “Sé que lo vi en algún sitio…”
18. Demostración por Cálculo: “Esta demostración requiere muchos cálculos. Por lo tanto la pasaremos por alto.”
19. Demostración por Terror: Usada cuando la Intimidación (7.) falla.
20. Demostración por Falta de Interés: “Realmente alguien quiere ver esto?”
21. Demostración por Ilegibilidad: “‡¥$\hbar\aleph\partial\nabla\Im$”
22. Demostración por Lógica: “Si está en la hoja de problemas entonces debe ser cierto.”
23. Demostración por la Regla de la Mayoría: Usada cuando Acuerdo General (2.) no puede usarse.
24. Demostración por Elección Inteligente de la Variable: “Sea A el número tal que la demostración funciona.”
25. Demostración por Mosaico: “Esta prueba es justo la misma que la anterior.”
26. Demostración por Palabra Divina: “Y el Señor dijo: *Sea cierto*. Y ocurrió.”
27. Demostración por Testarudez: “¡No me importa lo que digas! Es cierto!”
28. Demostración por Simplificación: “Esta prueba se reduce al hecho de que $1 + 1 = 2$.”
29. Demostración por Generalización Precipitada: “Bien, es cierto para el 17, por tanto lo es para todos los números reales.”
30. Demostración por Engaño: “Ahora que todo el mundo se de la vuelta …”
31. Demostración por Súplica: “Por favor, que sea cierto.”
32. Demostración por Analogía Pobre: “Bien, esto es igual que …”
33. Demostración por Escape: Límite de Aplazamiento (9.) cuando $t \to \infty$.
34. Demostración por Diseño: “Si no es cierto en la Matemática actual invento un nuevo sistema donde sí lo es.”
35. Demostración por Intuición: “Tengo la sensación de que …”
36. Demostración por Autoría: “Bill Gates dice que es cierto. Por tanto debe serlo.”
37. Demostración por Afirmación Rotunda: “YO REALMENTE QUIERO DECIR ESTO!”

38. Demostración por el Teorema C.T.L.S.: “¡Cualquier Tonto Lo Sabe!”
39. Demostración por Vigoroso Agitamiento Manual: Funciona bien en clase.
40. Demostración por Seducción: “Convéncete tú mismo de que es cierto.”
41. Demostración por Evidencia Acumulada: “Largas y concienzudas búsquedas no han revelado ningún contraejemplo.”
42. Demostración por Intervención Divina: “Entonces un milagro ocurre y . . .”



“I think you should be more explicit here in step two.”

Capítulo 14

¿Con qué me entretengo si no estudio matemática?

¡Jugando con la matemática!
¡Leyendo cosas interesantes de la matemática!

142857
Les puedo proponer que si tienen una calculadora cerca tomen el número 142857 y empiecen a jugar:

$$142857 \times 2 =$$

$$142857 \times 3 =$$

$$\ldots$$

Varios geómetras notables estudiaron las propiedades de este número.
...
Para los antiguos matemáticos el número 142857 era cabalístico, con propiedades misteriosas; sin embargo estudiándolo desde el punto de vista matemático, no es más que un período en una proporción decimal periódica simple.

Matemática divertida y curiosa. Malba Tahan

Casi todas las grandes creaciones científicas de Newton sucedieron en la primera parte de su larga vida de 85 años. Luego fue miembro del Parlamento y ocupó diversos cargos públicos importantes en los que se sumergió profundamente. Se cuenta que durante su estancia en el Parlamento apenas intervino. Solamente una vez, en medio de una acalorada sesión, manifestó el deseo de decir algo. La cámara enmudeció para escuchar al gran Isaac Newton. Mientras dirigía el dedo a un lugar impreciso del espacio, sentenció: "Propongo cerrar esa ventana, porque aquí hace un frío considerable."

Los matemáticos no son gente seria. CLAUDI ALSINA-MIGUEL DE GUZMÁN

Por eso, es muy interesante saber que alguna vez se intentó fijar el valor de π por ley, como si se tratara de un límite superior de valocidad para automóviles. El proyecto de ley fue presentado ante la cámara de representantes (diputados) de la legislatura del estado de Indiana, Estados Unidos, en 1897. Según el proyecto, el valor de pi debía fijarse en 4. Así nomás. No deja de ser curioso el trámite que siguió el proyecto. Fue girado directamente al Comité de Tierras Anegadas. El Comité, por alguna razón consideró que el valor de pi no era de su incumbencia, y recomendó que el proyecto se tratara en la Comisión de Educación a la que fue girado inmediatamente. La Comisión de Educación estudió el proyecto y lo devolvió a la cámara de representantes recomendando que se aprobara; a su vez la Honorable Cámara, siguiendo al pie de la letra la recomendación lo aprobó por unanimidad; sesenta y siete votos contra cero. El Senado, créase o no, giró el proyecto a la Comisión de Temperancia que le dio su aprobación, y, en primera instancia, la ley estuvo a punto de ser sancionada. Un poquito más y el valor de pi quedaba fijado en 4 en todo el estado de Indiana. Sin embardo, en el momento de la votación definitiva, los senadores-tal vez asesorados por algún geómetra infiltrado en las deliberaciones- resolvieron rechazar el proyecto, y dejar el valor de π librado al arbitrio de los matemáticos.

Curiosidades de la ciencia LEONARDO MOLEDO

A Descartes, Pascal, Newton, Leibniz, Euler, Lagrange, Comte ¡Alá se compadezca de estos infieles! A Buchafar Mohamed Abenmusa Al Kwarizmi ¡Alá lo tenga en su gloria! A todos los que estudian, enseñan o admiran la prodigiosa verdad de los tamaños, de las medidas, de las cifras, del movimiento y de la ciencia yo, el hadj jerife Ali, Iezid Izz-Edim Malba Tahan les dedico estos problemas de matemática llenos de poesía. En Bagdad, en la luna de Ramadán de 1321.

El hombre que calculaba Malba Tahan

El libro de Penrose es el ataque más poeroso nunca escrito contra la IA fuerte. (...) Penrose tiene el valor de mantener, frente al creciente rechazo de un pequeño grupo de físicos, un vigoroso realismo. No sólo el universo "está ahí", sino que la verdad matemática tiene también su propia independencia e intemporalidad misteriosa. Como Newton y Einstein, Penrose tiene un profundo sentido de humildad y respeto hacia el mundo físico, tanto como hacia el ámbito platónico de la matemática pura. Al famoso especialista en números Paul Erdös le gusta hablar del "Libro de Dios" en el que están registradas las mejores demostraciones. A los matemáticos se les permite de cuando en cuando echar una ojeada a una parte de una página. Penrose cree que cuando un físico o un matemático experimenta una repentina inspiración "ajá" no se trata simplemente de algo producido por un cálculo complicado: es la mente que por un momento entra en contacto con la verdad objetiva. ¿No sería posible, se pregunta, que el mundo de Platón y el mundo físico (que los físicos han diluido ahora en las matemáticas) fueran realmente uno y el mismo?-

Prefacio de Martin Gardner a *La nueva mente del emperador* Roger Penrose

Erdös era un monje de la matemática. Renunció al placer físico y a las posesiones materiales por una vida ascética, contemplativa, una vida dedicada a una misión única y específica: descubrir la verdad matemática. qué tenía la matemática que la hacía tan apasionante y absorbente? "Hay un viejo debate-decía Erdös- sobre si la matemática se crea o simplemente se descubre. En otras palabras las verdades matemáticas ya están ahí, aún si nadie las conoce todavía? Si uno cree en Dios, la respuesta es obvia. Las verdades están en la mente del FS [1] y uno sólo las redescubre."

El hombre que sólo amaba los números (la historia de Paul Erdös y la búsqueda de la verdad matemática) Paul Hoffman

Galois tomó el álgebra y la puso patas arriba. Si uno quiere saber si una ecuación se puede resolver o no, simplemente lo intenta, verdad? Pues Galois dijo que no. Sólo hay que examinar las permutaciones de las supuestas

[1] Erdös llamaba a Dios el Fascista Supremo

soluciones. ¿Cómo nos pueden decir las permutaciones de supuestas soluciones que ni siquiera conocemos algo sobre la resolubilidad? El hecho de que las permutaciones ofrecen, al menos, cierta información nueva se conoce desde muy antiguo en el mundo matemático. Eso es lo que hacen los anagramas.(...) El cubo Rubik está formado por una matriz de 3x3x3 cubos más pequeños. Las caras de estos pequeños cubos son se diferentes colores y las caras del cubo grande son rotatorias de modo que pueden girarse en diferentes direcciones (...) Dado que el cubo Rubik puede mostrar no menos de 43.252.003.274.489.856.000 patrones diferentes, cabe suponer que nadie ha intentado nunca tratar de resolverlos todos. Mas bien, cada movimiento del cubo Rubik puede representarse como una permutación de sus vértices. En efecto, la solución del puzzle del cubo puede ser trasladada por completo al lenguaje de la teoría de grupos. El matemático David Joyner de la U.S. Naval Academy ha sistematizado incluso un curso completo de teoría de grupos en torno al cubo Rubik y juguetes matemáticos parecidos.

La ecuación jamás resuelta (cómo dos genios matemáticos descubrieron el lenguaje de la simetría) Mario Livio

Los individuos afligidos por el desorden obsesivo-compulsivo están con frecuencia impelidos a cometer actos repetitivos que en apariencia no tienen importancia, tal como lavarse persistentemente las manos, contar objetos, comprobar si las puertas están cerradas, y evitar situaciones raramente perturbadoras como pisar sobre las pequeñas grietas de las aceras. El desorden obsesivo-compulsivo que tyiene relación con los números es especialmente triste a la vez que fascinante. El gran inventor Nicola Tesla tenía una "manía aritmética", también llamada desorden numérico obsesivo-compulsivo. Pedía exactamente 18 toallas limpias cada día. Si se le preguntaba por qué no proporcionaba ninguna explicación. Los accesorios de mesa y las toallas no eran lo únicos artículos que pedía en múltiplos de 3. Con frecuencia, por ejemplo, se sentía impelido a dar 3 vueltas alrededor de una manzana de casas, y siempre contaba los pasos mientras paseaba. Eligió la habitación número 207 en el hotel Alta Vista, debido a que 207 es divisible por 3. Durante la cena apilaba sin cesar 18 servilletas de forma escrupulosa, siempre en busca de números divisibles por 3.

La maravilla de los números. Clifford Pickover

Robert, un niño que teme a la matemática porque no la entiende y que suele tener extrañas pesadillas. Una noche aparece en sus sueños un personaje inesperado: el diablo de los números. Por doce noches, que serán doce capítulos ambos, niño y diablillo viajan por el fascinante mundo de la matemática descubriendo conceptos desde los números naturales hasta la sucesión Fibonacci y la proporción áurea. Como se trata de un mundo no real, las denominaciones no son siempre las usuales. Por ejemplo, a los números imaginarios los llama números imaginados, a los irracionales irrazonables y a los primos números de primera.

El diablo de los números (un libro para todos aquellos que temen a las matemáticas) HANS MAGNUS ENZENSBERGER

A nuestras ideas del espacio y el tiempo les han sucedido muchas cosas desde que salió a la luz Planilandia. Pero, a pesar de tanto hablar de una cuarta dimensión, los fundamentos de la dimensionalidad no han cambiado. Mucho antes de que apareciese la teoría de la relatividad, los científicos consideraban el tiempo una dimensión extra. Tiempo, el tirano, domina en Planilandia lo mismo que en nuestro propio mundo. Los habitantes de Planilandia son seres sensibles, a quienes atribulan nuestros problemas y conmueven nuestras emociones. Aunque sean planos físicamente, sus características están bien redondeadas. Son parientes nuestros, de carne y hueso como nosotros. Retozamos con ellos en Planilandia. Y retozando, nos hallamos de pronto nosotros mismos contemplando de un modo nuevo nuestro mundo rutinario con el asombro boquiabierto de la juventud.

Comentario a *Planilandia (una novela de muchas dimensiones)* E. ABBOT

Casi todos los 72 problemas planteados a continuación son verdaderos "problemas de almohada" que han sido resueltos mentalmente mientras yacía despierto en la cama por la noche (algunos van acompañados por la fecha exacta). El 37 y uno o dos más son hijos del día y fueron resueltos durante paseos en solitario; pero todos ellos fueron resueltos por completo antes de escribir una sola palabra o hacer dibujos. Por lo general lo primero que escribo es la respuesta, y luego el enunciado y la solución. Por ejemplo, las primeras palabras del 70 que escribí fueron las siguientes: (1) baja por el lado trasero, vuelve a subir y así sucesivamente; (2) aproximadamente a 0,7 bajando por el lado trasero; (3) aproximadamente $18°18'$ (4) aproximadamente $14°$. Estas respuestas no son absolutamente correctas, pero al menos son auténticas, como resultado únicamente de un trabajo mental. "¡No es gran cosa, señor, pero es mía!"

Un cuento enmarañado y otros problemas de almohada. LEWIS CARROLL.

Laringitis, un orador griego, nació el 4 de julio del año 30 aC y murió el 4 de julio del año 30 dC. ¿Qué edad tenía cuando murió?

Matemática para divertirse (Un paseo por las diversas áreas de la matemática a través de 50 problemas de ingenio) MARTIN GARDNER

Reacomodar las piezas para obtener la figura de un pony más precisa posible.

Los acertijos de Sam Loyd. SAM LOYD

Índice alfabético

Bibliografía

[Aba00] Manuel Abad. *Elementos de álgebra*. EDIUNS, 2000.

[Ant86] H Anton. *Introducción al álgebra lineal*. 1986.

[Efi] M. Efimov. *Curso breve de geometría analítica*. "Mir", Moscow. Translated from the Russian.

[Flo79] F. G. Florey. *Fundamentos de álgebra lineal y aplicaciones*. 1979.

[Gas70] María Luisa Gastaminza. *Nociones de álgebra*. 1970.

[Gen65] Enzo R. Gentile. *Notas de álgebra*. Cursos y Seminarios de Matemática, Fasc. 22. Universidad de Buenos Aires, Buenos Aires, 1965.

[Gen88] Enzo R. Gentile. *Notas de álgebra I*. Universidad de Buenos Aires, Buenos Aires, 1988.

[Gol74] L. Golovina. *Álgebra lineal y algunas aplicaciones*. "Mir", Moscow, 1974. Translated from the Russian.

[Kin88] J. Kindle. *Teoría y problemas de geometría analítica*. 1988.

[Kur87] A. G. Kurosch. *Curso de álgebra superior*. "Mir", Moscow, fifth edition, 1987. Translated from the Russian and with an introduction by Emiliano Aparicio Bernardo.

[Mur73] D. Murdoch. *Geometría analítica*. LIMUSA, 1973.

[PR91] H Pita Ruiz, Claudio. *Álgebra lineal*. 1991.

[San61] Luis A. Santaló. *Vectores y tensores, con sus aplicaciones*. Manuales de EUDEBA/Matemática. Editorial Universitaria de Buenos Aires, !uenos Aires, 1961.

[San77] Luis A. Santaló. *Vectores y tensores*. Manuales de EUDEBA, 1977.

[Sew99] Ana María Sewald, Julio y Suardíaz. *Álgebra y geometría. Notas de curso*. 1999.

[Sew02] Julio Sewald. *Geometría Analítica. Notas de curso*. 2002.

La Unidad Aritmética

CON LAS FORMAS DEL AYER
por Mario Minervino
mminervino@lanueva.com

Hace 56 años, en agosto de 1959, el laboratorio de computadoras de la Universidad Nacional del Sur construyó, de acuerdo con un diseño propio, una Unidad Aritmética Experimental, hecho inédito en el país en materia de calculadoras.

La materialización de esta pionera calculadora-computadora fue dirigida por el ingeniero Jorge Santos, secundado por los estudiantes Natalio Kerlleñevich y Enrique Chapunov y por la ingeniera industrial Betty Kerlleñevich.

Se trataba de un aparato programado para realizar operaciones de multiplicación, hasta un resultado de 10.000.

Los primeros ensayos fueron alentadores: la máquina realizó una operación de alta complejidad en apenas 16 milésimas de segundo.

La Unidad era, en rigor, una compleja máquina de 200 circuitos independientes, 190 transistores, 115 iodos, 850 resistencias y 220 condensadores.

Su conexión demandó la fabricación de 1.700 pares de contactos, realizados mediante máquinas y matrices elaboradas en el taller de ingeniería.

El resultado de las cuentas podía visualizarse, claramente, en un luminoso tablero de 48 lámparas de neón -para los registros numéricos- y de 9 para el reloj y el contador que detenía la máquina apenas finalizada la operación.

Completada la obra, Santos viajó a especializarse en la Universidad de Manchester.

Pero dejó trabajo: el laboratorio comenzó a analizar el uso de cerámicas magnéticas, ensayadas con éxito en el Japón, con el objetivo de construir, a mediano plazo, "una computadora digital completa".

Pocos podían seguramente imaginar por aquellos días la revolución informática que comenzaría unas décadas más tarde en el mundo, y que modificaría para siempre su funcionamiento y aun nuestro modo de vida.

La Nueva Provincia, agosto de 2015.