ÁLGEBRA I

Fernando Chamizo Lorente

1º de Ingeniería Informática. Curso 1996-1997

Versión del 22/1/2002

Prefacio al comenzar la edición de 1996/1997

Estas notas corresponden a la asignatura de Álgebra I de primero de Ingeniería Informática de la Universidad Autónoma de Madrid. Cuando se terminen, seguramente sean casi una copia de las que elaboré el curso pasado. Todo lo que dije acerca de ellas se podría repetir aquí, pero como seguramente no dije nada interesante y sólo lo leí yo, no me parece conveniente repetirlo. Quizá sólo hacer notar con respecto a los ejercicios que algunos de ellos están marcados con asteriscos, lo que significa que tienen un nivel de dificultad mayor, y que considero que un problema con dos asteriscos es muy difícil incluso para los mejores alumnos de la clase.

Varias modificaciones se han previsto con respecto a las notas del curso pasado aunque no es seguro que se lleven a cabo y en cualquier caso no serán sustanciales. Quizá el único cambio notable se advierta al final de cada capítulo, donde se añadirán algunos episodios de la historia de las Matemáticas a través de resultados relacionados con la teoría. La exposición en ellos será más informal y no muy exhaustiva.

Al igual que hice es una versión anterior, quisiera copiar en estas insignificantes notas el *copyright* que puso Juan Ruiz a la obra de arte que constituyen las suyas:

Qualquier omne que·l oya, si bien trobar sopiere,
más á ý [a] añadir e emendar, si quisiere;
ande de mano en mano a quienquier que·l pidiere,
como pella a las dueñas, tómelo quien podiere.

Índice

Primer Curso de Ingeniería Informática (Curso 1996-1997)

1. Teoría de Conjuntos

-Conjuntos 1

-Funciones 4

-Relaciones 7

-Estructuras algebraicas elementales 9

2. Los Anillos $\mathbb{Z}$ y $\mathbb{Z}_m$

-Máximo común divisor, mínimo común múltiplo, algoritmo de Euclides 23

-Números primos y primos entre sí, teorema de factorización 29

-Congruencias, divisibilidad, pequeño teorema de Fermat 31

3. Anillos de Polinomios

-Máximo común divisor, mínimo común múltiplo, algoritmo de Euclides 49

-Polinomios irreducibles, teorema de factorización 52

-Raíces 56

4. Teoría Elemental de Grupos

-Definición, subgrupos, ejemplos 67

-Homomorfismos, núcleo, imagen 74

-Subgrupos normales, grupo cociente 77

-Grupos cíclicos, grupos de permutaciones, grupos diédricos 84

-Grupos de orden bajo 90

5. Espacios Vectoriales

-Espacios, subespacios, propiedades y ejemplos 105

-Base, dimensión, cambio de base 111

-Suma e intersección de subespacios, fórmula de Grassmann 123

Bibliografía: Aunque no haya un texto que se ajuste totalmente al temario, los capítulos §2, §3, §4 y §5 corresponden más o menos a los cuatro primeros capítulos del libro de M. Castellet e I. Llerena "Álgebra Lineal y Geometría" (Ed. Reverté).

1. Teoría de Conjuntos

1.1. Conjuntos

Todos tenemos una idea intuitiva de lo que es un conjunto, pero al igual que ocurre con otros conceptos de matemática elemental (número, punto, etc.) es realmente difícil encontrar una definición adecuada y rigurosa. Esta dificultad se resuelve normalmente en Matemáticas enunciando algunos axiomas y diciendo que los objetos que queremos definir son "algo" que guarda las relaciones indicadas en dichos axiomas.

La formulación axiomática de la teoría de conjuntos es bastante complicada (quizá porque el concepto de conjunto es uno de los más básicos), por ello no consideraremos en este curso más que la idea intuitiva de conjunto:

Un conjunto *es una colección de objetos a los que se llama elementos del conjunto.*

Es conveniente considerar también el conjunto que no tiene ningún elemento o conjunto vacío. Éste se denota con el símbolo $\emptyset$.

Normalmente los conjuntos se designan con letras mayúsculas y los elementos con letras minúsculas.

Un conjunto se puede determinar de dos formas:

1) (explícita) Citando sus elementos

$$A = \{\text{elemento1, elemento2, elemento3, \ldots etc.}\}$$

2) (implícita) Dando una propiedad que caracteriza a sus elementos

$$A = \{x \,/\, \text{ se cumple la propiedad } P\}.$$

La barra "$/$" se lee "tal que" y a veces también se escribe ":".

Ejemplo 1. $A = \{-1, 1\}$ $\qquad$ $A = \{x \,/\, x \text{ es un número real y } x^2 - 1 = 0\}$.

Ejemplo 2. $B = \{16\}$ $\qquad$ $B = \{n \,/\, n \text{ es un número natural y } 2^n = 65536\}$.

Ejemplo 3. $C = \{2, 3, 5, 7, 11\}$ $\qquad$ $B = \{n \,/\, n \text{ es primo y } 1 < n \leq 12\}$.

Ejemplo 4. $D = \big\{\{0,0\}, \{0,1\}, \{1,1\}\big\}$ $\qquad$ $D = \{E \,/\, E$ es un conjunto de ceros y unos con dos elementos$\}$.

A continuación se da una lista de algunos símbolos que se usan con frecuencia en teoría de conjuntos:

Símbolo	Significado	Nombre
1) $x \in A$	x es un elemento de A	(x pertenece a A)
2) $x \notin A$	x no es un elemento de A	(x no pertenece a A)
3) $A = B$	$x \in A \Leftrightarrow x \in B$	(A igual a B)
4) $A \neq B$	No se cumple $A = B$	(A distinto de B)
5) $A \subset B$	$x \in A \Rightarrow x \in B$	(A incluido en B, A subconjunto de B)
6) $A \supset B$	$x \in B \Rightarrow x \in A$	(A incluye a B)
7) $A \cap B$	$\{x \,/\, x \in A \text{ y } x \in B\}$	(intersección)
8) $A \cup B$	$\{x \,/\, x \in A \text{ ó } x \in B\}$	(unión)
9) $A - B$	$\{x \,/\, x \in A \text{ y } x \notin B\}$	(diferencia)
10) $A \triangle B$	$(A \cup B) - (A \cap B)$	(diferencia simétrica)
11) $A \times B$	$\{(a,b) \,/\, (a,b) \text{ par ordenado con } a \in A,\ b \in B\}$	(producto cartesiano)
12) $\mathcal{P}(A)$	$\{B \,/\, B \subset A\}$	(conjunto potencia)

Cuando suponemos que todos los conjuntos con que trabajamos son subconjuntos de uno mayor, $\mathcal{U}$, llamado conjunto universal, entonces también se usa

13) A' $\quad \mathcal{U} - A$ $\quad$ (complementario)

Observación: Para definir $A \times B$ se ha usado el concepto de par ordenado. Aunque de nuevo es mejor confiar en nuestra intuición acerca de su significado; rigurosamente un par ordenado (a,b) se puede definir como el conjunto $\big\{\{a\},\{a,b\}\big\}$. Obsérvese que también se pueden considerar productos cartesianos de n factores, $A_1 \times A_2 \times \ldots \times A_n$, que se identifican con las n-uplas ordenadas $(a_1, a_2, \ldots, a_n)$ con $a_i \in A_i$.

Existen multitud de relaciones que permiten transformar fórmulas que involucran $\cup$, $\cap$, $'$, $\triangle$, $\times$ (véanse los ejercicios). A modo de ejemplo demostraremos dos de las más conocidas

Proposición 1.1 (Leyes de De Morgan)**:** *Sean A y B dos conjuntos, entonces se verifica*

$$1)\ (A \cup B)' = A' \cap B' \qquad 2)\ (A \cap B)' = A' \cup B.'$$

DEM.: Como es habitual omitiremos en esta demostración cualquier referencia al conjunto universal que suponemos que contiene todos los elementos y conjuntos que aparecen.

1) $x \in (A \cup B)' \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A$ y $x \notin B$ (porque si $x \in A$ o si $x \in B$ entonces $x \in A \cup B$ y viceversa) $\Leftrightarrow x \in A'$ y $x \in B' \Leftrightarrow x \in A' \cap B'$.

Se puede demostrar 2) de forma análoga (ejercicio). También, suponiendo que conocemos la relación $(C')' = C$, es posible deducir 2) de 1) sin más que tomar A' en lugar de A y B' en lugar de B.

La demostración de $(C')' = C$ es como sigue: $x \in (C')' \Leftrightarrow x \notin C' \Leftrightarrow x \in C$ (porque o bien $x \in C$ o bien $x \notin C$). ■

Algunas definiciones que se utilizan con frecuencia en la teoría de conjuntos son

DEFINICIÓN: *Se dice que A y B son* <u>disjuntos</u> *si $A \cap B = \emptyset$.*

DEFINICIÓN: *El número de elementos de un conjunto finito, A, se llama* <u>cardinal</u> *u* <u>orden</u> *y se escribe $|A|$.*

<u>Nota</u>: G. Cantor (1845-1918) demostró que la noción de cardinal se puede extender a conjuntos infinitos y que hay diferentes tipos de cardinales "infinitos". Aquí no entraremos en estos detalles y escribiremos simplemente $|A| = \infty$ si A no tiene un número finito de elementos.

DEFINICIÓN: *Una* <u>partición</u> *de un conjunto A es una familia de subconjuntos no vacíos, A_α, tales que*

$$1)\ A_\alpha \neq A_\beta \ \Rightarrow\ A_\alpha \text{ y } A_\beta \text{ son disjuntos} \qquad 2)\ \bigcup A_\alpha = A.$$

Obsérvese que si A es un conjunto finito entonces dar partición equivale a escribir A como $A_1 \cup A_2 \cup \ldots \cup A_n$ con los $A_i \neq \emptyset$ y disjuntos dos a dos. En este caso se tiene $|A| = |A_1| + |A_2| + \ldots + |A_n|$.

<u>Ejemplo</u> . Los conjuntos $A_1 = \{1, 2\}$, $A_2 = \{5\}$ y $A_3 = \{7, \sqrt{11}\}$, conforman una partición de $A = \{1, 2, 5, 7, \sqrt{11}\}$. Además $|A_1| = 2$, $|A_2| = 1$, $|A_3| = 2$ y $|A| = 5$.

El siguiente resultado nos dice cómo se comporta el cardinal con respecto a las operaciones $\cup$, $\cap$ y $\times$.

Proposición 1.2 : *Sean A y B conjuntos finitos, entonces*

$$1)\ |A \cup B| = |A| + |B| - |A \cap B| \qquad 2)\ |A \times B| = |A||B|.$$

<u>DEM.</u>: 1) Cada elemento de $A \cup B$ está en A o en B, así pues $|A| + |B|$ cuenta todos los elementos de $A \cup B$ una vez excepto los comunes que son contados dos veces, por tanto $|A \cup B| = |A| + |B| - |A \cap B|$. Una manera más formal de proceder es considerar la partición $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ y concluir

$$\begin{aligned} |A \cup B| &= |A - B| + |B - A| + |A \cap B| \\ &= (|A - B| + |A \cap B|) + (|B - A| + |A \cap B|) - |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

2) Cada elemento de A figura en $|B|$ pares ordenados de $A\times B$. (Esto es equivalente a considerar la partición $A\times B=\bigcup_{a\in A}\{(a,b)\,/\,b\in B\}$). Como A tiene $|A|$ elementos se tiene $|A\times B|=|A||B|$. ■

Tras una breve reflexión, las proposiciones dadas anteriormente son tan obvias que parece difícil entender qué hay que demostrar. A continuación se dan algunos ejemplos en los que se insiste en la idea de que para demostrar una propiedad de teoría de conjuntos sólo debemos usar las definiciones de los símbolos involucrados (dadas al comienzo de la sección) y reglas de deducción tomadas de la lógica.

Ejemplo 1. Demostrar que $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

$x\in A\cap(B\cup C)\Leftrightarrow x\in A$ y $x\in B\cup C\Leftrightarrow x\in A$ y ($x\in B$ o $x\in C$) $\Leftrightarrow$ ($x\in A$ y $x\in B$) o ($x\in A$ y $x\in C$) $\Leftrightarrow x\in A\cap B$ o $x\in A\cap C\Leftrightarrow x\in(A\cap B)\cup(A\cap C)$.

Ejemplo 2. Demostrar que $A\subset B$, $B\subset A\Rightarrow A=B$.

Las definiciones de $B\subset A$ y $A\subset B$ nos indican respectivamente que

$$x\in B\ \Rightarrow\ x\in A,\qquad x\in A\ \Rightarrow\ x\in B,$$

así pues $x\in A\ \Leftrightarrow\ x\in B$ y por tanto $A=B$.

Ejemplo 3. Demostrar que $A\times(B\cap C)=(A\times B)\cap(A\times C)$.

$(x_1,x_2)\in A\times(B\cap C)\ \Leftrightarrow\ x_1\in A$ y $x_2\in B\cap C\Leftrightarrow x_1\in A$, $x_2\in B$ y $x_2\in C\Leftrightarrow(x_1,x_2)\in A\times B$ y $(x_1,x_2)\in A\times C\Leftrightarrow(x_1,x_2)\in(A\times B)\cap(A\times C)$.

Nota: En esta sección hemos supuesto que el lector conocía el significado de "$\Rightarrow$" y de "$\Leftrightarrow$". Recuérdese que

"$p\Rightarrow q$" significa "*si p, entonces q*"   "$p\Leftrightarrow q$" significa "*p si y sólo si q*".

donde p y q son lo que se llaman proposciones, es decir, expresiones de las que podemos afirmar o negar su certeza. Aunque no hayan aparecido explícitamente aquí, también son muy usados en lógica los símbolos $\vee$, $\wedge$ y $\sim$ que guardan cierta analogía con $\cup$, $\cap$ y $'$ en teoría de conjuntos. Su significado es el siguiente:

"$p\vee q$" significa "*p ó q*"   "$p\wedge q$" significa "*p y q*"   "$\sim p$" significa "*lo contrario de p*".

Finalmente mencionaremos que también se usan los llamados cuantificadores "$\forall$" y "$\exists$" que significan "*para todo*" y "*existe*", respectivamente.

1.2. Funciones

Intuitivamente una función entre dos conjuntos A y B es una manera de asignar a cada elemento de A un elemento de B. Desde el punto de vista de la teoría de conjuntos se puede dar una definición muy rigurosa (aunque bastante antiintuitiva)

Definición: *Una función de A en B es un subconjunto, f, de $A \times B$ tal que*

$$1)\ \forall x \in A\ \exists y \in B \,/\, (x,y) \in f \qquad 2)\ (x,y_1) \in f,\ (x,y_2) \in f \ \Rightarrow\ y_1 = y_2.$$

Normalmente se escribe $f : A \longrightarrow B$ para indicar que f es una función de A en B. Además $(x,y) \in f$ se escribe $y = f(x)$.

Definición: *Si $f : A \longrightarrow B$ y $C \subset A$, $D \subset B$, se definen los conjuntos*

$$f(C) = \{y \in B \,/\, y = f(x) \text{ para algún } x \in C\} \qquad f^{-1}(D) = \{x \in A \,/\, f(x) \in D\}.$$

Definición: *Si $f : A \longrightarrow B$, al conjunto A se le llama* <u>dominio</u> *de f y al conjunto $f(A)$* <u>imagen</u> *(o rango) de f. Se suelen denotar con los símbolos* Dom f *e* Im f *respectivamente.*

<u>Ejemplo 1</u>. Si $f : \mathbb{R} \longrightarrow \mathbb{R}$ con $f(x) = x^2$ entonces Im $f = \{x \geq 0\}$.

<u>Ejemplo 2</u>. Si $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ con $f(n) = (-1)^n$ entonces Im $f = \{-1, 1\}$, $f^{-1}(\{1\}) = \{\text{números pares}\}$, $f(\{1,2,3\}) = \{-1,1\}$.

<u>Ejemplo 3</u>. Si $f : T \longrightarrow \mathbb{R}$ donde T es el conjunto de todos los triángulos y f asigna a cada uno de ellos la suma de sus ángulos (en grados), entonces Im $f = \{180\}$, $f^{-1}(\{90\}) = \emptyset$.

Las funciones se clasifican de la siguiente forma:

Definición: *Dada $f : A \longrightarrow B$ diremos que*

1) f es <u>sobreyectiva</u> *(o suprayectiva o sobre) si* Im $f = B$

2) f es <u>inyectiva</u> *(o uno a uno) si $f(x) = f(y) \Rightarrow x = y$.*

3) f es <u>biyectiva</u> *si es inyectiva y sobreyectiva.*

Nótese que según esta definición, una función $f : A \longrightarrow B$ es sobre si y sólo si se alcanzan todos los valores de B, y es inyectiva si dos elementos distintos de A se aplican siempre en dos elementos distintos de B; así pues si queremos demostrar que cierta f no es sobreyectiva debemos encontrar un elemento de B que no esté en la imagen de f, y si queremos demostrar que no es inyectiva debemos encontrar dos elementos distintos de A cuyas imágenes por f coincidan.

<u>Ejemplo 1</u>. $f : \mathbb{R} \longrightarrow \mathbb{R}$ con $f(x) = x^2 + 2$ no es sobreyectiva porque Im $f = \{x \geq 2\}$, tampoco es inyectiva porque $f(1) = f(-1)$.

<u>Ejemplo 2</u>. $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ con $f(x) = 2x$ es sobreyectiva ya que cada número racional a/b está en la imagen de f porque $f(a/2b) = a/b$, también es inyectiva porque $f(x) = f(y) \Rightarrow x = y$; por tanto, es biyectiva.

<u>Ejemplo 3</u>. $f : \mathbb{Z} \times \mathbb{Z}^+ \longrightarrow \mathbb{Q}$ con $f\big((a,b)\big) = a/b$ ($\mathbb{Z}^+$ indica los enteros positivos), es sobreyectiva pero no es inyectiva porque, por ejemplo, $f\big((-6,9)\big) = f\big((-4,6)\big)$.

A continuación definimos la composición de funciones, que no es otra cosa más que aplicarlas sucesivamente.

DEFINICIÓN: *Sean $f : A \longrightarrow B$, $g : B \longrightarrow C$, entonces se define la* <u>*composición*</u> *de g y f como la función $g \circ f : A \longrightarrow C$ tal que $(g \circ f)(x) = g\big(f(x)\big)$.*

<u>Ejemplo 1</u>. Sean $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ y $g : \mathbb{Z} \longrightarrow \mathbb{Q}$ tales que $f(n) = 2n-1$ y $g(n) = 2/(n^2+1)$, entonces $g \circ f : \mathbb{Z} \longrightarrow \mathbb{Q}$ con $(g \circ f)(n) = 1/(2n^2 - 2n + 1)$.

<u>Ejemplo 2</u>. Sean $f : \mathbb{R} - \{-1\} \longrightarrow \mathbb{R} - \{1\}$ y $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{-1\}$ definidas por $f(x) = (x + 2)/(x + 1)$ y $g(x) = (2 - x)/(x - 1)$, entonces $g \circ f : \mathbb{R} - \{-1\} \longrightarrow \mathbb{R} - \{-1\}$ cumple $(g \circ f)(x) = x$.

DEFINICIÓN: *La función $f : A \longrightarrow A$ que deja todos los elementos invariantes, esto es, $f(x) = x$ para todo $x \in A$, se llama* <u>*función identidad*</u> *y se suele denotar con 1_A ó Id_A.*

DEFINICIÓN: *Dada $f : A \longrightarrow B$, se dice que $g : B \longrightarrow A$ es la* <u>*inversa*</u> *de f (y se escribe $g = f^{-1}$) si se cumple*

$$\textit{1)}\ g \circ f = 1_A \qquad \textit{2)}\ f \circ g = 1_B.$$

<u>Ejemplo</u> . Las funciones del último ejemplo son inversas la una de la otra.

Nótese que en la definición anterior no basta comprobar *1* ó *2)* para que la otra condición se cumpla automáticamente. Por ejemplo, si $f : A \longrightarrow \mathbb{R}$ y $f : \mathbb{R} \longrightarrow A$ donde $A = \{x \in \mathbb{R} \,/\, x \geq 0\}$ vienen dadas por $g(x) = x^2$ y $f(x) = +\sqrt{x}$ (donde $+\sqrt{\ }$ indica la raíz cuadrada positiva), se cumple $(g \circ f)(x) = (+\sqrt{x})^2 = x$ para todo $x \in A$, sin embargo no se cumple $(f \circ g)(x) = x$ para todo $x \in \mathbb{R}$ ya que los negativos no cumplen $+\sqrt{x^2} = x$.

Intuitivamente, la inversa de una función de A en B es simplemente considerarla en sentido contrario, de B en A. Esto requiere que cada elemento de B tenga exactamente una preimagen, es decir, que la función sea biyectiva. De hecho se tiene

Proposición 2.1 : *$f : A \longrightarrow B$ es invertible (tiene inversa) si y sólo si f es biyectiva. Además $\left(f^{-1}\right)^{-1} = f$.*

<u>Ejemplo 1</u>. Ya habíamos visto que $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, $f(x) = 2x$ es biyectiva. Para calcular su inversa supongamos que $x = f^{-1}(y)$, entonces $f\big(f^{-1}(y)\big) = 2f^{-1}(y)$ y por tanto $f^{-1}(y) = y/2$.

<u>Ejemplo 2</u>. Si $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{2\}$ con $f(x) = 2x/(x - 1)$, se puede probar que f es biyectiva (ejercicio) y su inversa se puede calcular poniendo como antes $x = f^{-1}(y)$ y por tanto $y = 2f^{-1}(y)/(f^{-1}(y) - 1) \Rightarrow yf^{-1}(y) - y = 2f^{-1}(y) \Rightarrow (y - 2)f^{-1}(y) = y \Rightarrow f^{-1}(y) = y/(y - 2)$.

<u>Observación</u>: Es fácil darse cuenta de que el proceso llevado a cabo para calcular la inversa de $y = f(x)$ se reduce a despejar la y en $x = f(y)$, obteniéndose $y = f^{-1}(x)$.

1.3. Relaciones

Definir una relación en un conjunto quiere decir dar una forma de comparar unos elementos con otros. En ciertas condiciones (relaciones de equivalencia) esto permitirá subdividir los elementos de un conjunto en diferentes grupos que comparten propiedades similares.

Definición: *Una* relación *en un conjunto A es un subconjunto, $\mathcal{R}$, de $A \times A$. Si $a, b \in A$ cumplen $(a, b) \in \mathcal{R}$, se dice que* a está relacionado con b *y se suele escribir $a\mathcal{R}b$.*

La definición de relación no es muy complicada, pero es demasiado general ya que habitualmente tenemos algunas propiedades adicionales que enunciamos a continuación.

Definición: *Diremos que una relación, $\mathcal{R}$, definida en un conjunto, A, es*

1) Reflexiva, *si* $\forall a \in A\ a\mathcal{R}a$

2) Simétrica, *si* $\forall a, b \in A\ a\mathcal{R}b \Rightarrow b\mathcal{R}a$

3) Antisimétrica, *si* $\forall a, b \in A\ a\mathcal{R}b,\ b\mathcal{R}a \Rightarrow a = b$

4) Transitiva, *si* $\forall a, b, c \in A\ \ a\mathcal{R}b,\ b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

Según estas propiedades es conveniente destacar dos tipos de relaciones

Definición: *Una* relación de equivalencia *es una relación reflexiva, simétrica y transitiva.*

Definición: *Una* relación de orden *es una relación reflexiva, antisimétrica y transitiva. Si además para todo a, b se cumple $a\mathcal{R}b$ ó $b\mathcal{R}a$, entonces se dice que es una* relación de orden total. *En el resto de los casos se dice que es* de orden parcial.

Ejemplo 1. Si definimos en $\mathbb{N}$, $n\mathcal{R}m$ como n y m coinciden en su última cifra, entonces $\mathcal{R}$ es reflexiva, simétrica y transitiva; por tanto es una relación de equivalencia.

Ejemplo 2. Si definimos en el conjunto de subconjuntos de $\mathcal{U}$ (esto es, en $\mathcal{P}(\mathcal{U})$) la relación $A\mathcal{R}B$ como $A \subset B$, entonces $\mathcal{R}$ es reflexiva, antisimétrica y transitiva; por tanto es una relación de orden. No es difícil ver sobre algún ejemplo que en general no es de orden total.

Ejemplo 3. En $\mathbb{Z}$ la relación $n\mathcal{R}m \Leftrightarrow 2n \ne 3m$ no es reflexiva (porque $0 \not\mathcal{R} 0$) ni simétrica ($2\mathcal{R}3$, $3 \not\mathcal{R} 2$), ni antisimétrica ($1\mathcal{R}5$, $5\mathcal{R}1$, $1 \ne 5$), ni transitiva ($3\mathcal{R}1$, $1\mathcal{R}2$, $3 \not\mathcal{R} 2$).

Ejemplo 4. En $\mathbb{Z}^+$ la relación $n\mathcal{R}m \Leftrightarrow n$ divide a m es reflexiva, antisimétrica y transitiva. Es un orden parcial porque, por ejemplo, 2 no está relacionado con 5 ni 5 con 2.

Ejemplo 5. En $\mathbb{R}$ la relación $x\mathcal{R}y \Leftrightarrow x \le y$ es de orden total, pero $x\mathcal{R}'y \Leftrightarrow x < y$ no lo es porque no cumple la propiedad reflexiva.

Propiedades de las relaciones de equivalencia: Si $\mathcal{R}$ es una relación de equivalencia en A, entonces para cada $a \in A$ se define la clase de equivalencia de a como el conjunto $\{x \in A \big/ x\mathcal{R}a\}$. Las clases de equivalencia correspondientes a elementos no relacionados son disjuntas y no vacías, así que definen una partición de A. Al conjunto de clases de equivalencia se le llama conjunto cociente.

Ejemplo . En el conjunto $A = \{1,2,3,5,6,9\}$ la relación $n\mathcal{R}m \Leftrightarrow 3$ divide a $n-m$, es de equivalencia. Para abreviar designaremos con $\overline{a}$ la clase de equivalencia de a. Se tiene

$$\overline{1} = \{1\} \qquad \overline{2} = \overline{5} = \{2,5\} \qquad \overline{3} = \overline{6} = \overline{9} = \{3,6,9\}.$$

El conjunto cociente es $\{\overline{1}, \overline{2}, \overline{3}\}$, o más explícitamente

$$\big\{\{1\}, \{2,5\}, \{3,6,9\}\big\}.$$

Nótese que $\{1\} \cup \{2,5\} \cup \{3,6,9\} = A$ y que las tres clases de equivalencias son disjuntas y no vacías.

En las relaciones de orden hay algunos elementos distinguidos. En las tres definiciones siguientes supondremos que $\mathcal{R}$ es una relación de orden en A. Para entender la notación es aconsejable pensar que $\mathcal{R}$ es $\leq$.

DEFINICIÓN: *Se dice que $x \in A$ es un elemento maximal si $x\mathcal{R}y \Rightarrow x = y$, y que es minimal si $y\mathcal{R}x \Rightarrow y = x$.*

DEFINICIÓN: *Se dice que $x \in A$ es un máximo si $\forall y \in A$ se cumple $y\mathcal{R}x$, y un mínimo si $\forall y \in A$ se cumple $x\mathcal{R}y$.*

DEFINICIÓN: *Si $B \subset A$, se dice que $x \in A$ es una cota superior de B si $\forall y \in B$ $y\mathcal{R}x$. Si el conjunto de cotas superiores tiene un mínimo, a éste se le llama cota superior mínima o supremo. De la misma forma $x \in A$ es una cota inferior de B si $\forall y \in B$ $x\mathcal{R}y$. Si existe el máximo de todas las cotas inferiores, se le llama cota inferior máxima o ínfimo.*

Quizá es difícil distinguir a primera vista estos tres conceptos. Para ello veamos los siguientes ejemplos:

Ejemplo 1. Sea $A = \big\{\{1\}, \{2\}, \{1,2\}, \{3\}, \emptyset\big\}$ con la relación de orden entre los elementos de A dada por $C\mathcal{R}D \Leftrightarrow C \subset D$.

El conjunto $\{1,2\}$ es maximal porque $C \in A$, $\{1,2\} \subset C \Rightarrow C = \{1,2\}$, pero no es máximo porque $\{3\} \not\subset \{1,2\}$; de la misma forma $\{3\}$ es maximal pero no máximo. El conjunto vacío, $\emptyset$, es minimal y también es un mínimo porque $\forall C \in A$, $\emptyset \subset C$. El subconjunto de A, $B = \big\{\{1\}, \{3\}\big\}$ no tiene cota superior en A, y el subconjunto $B = \big\{\{1\}, \{2\}\big\}$ tiene a $\{1,2\}$ como cota superior, que también es su supremo.

Ejemplo 2. Sea el conjunto $A = \{x \in \mathbb{R} \big/ 0 < x \leq 1\}$ con la relación de orden $x\mathcal{R}y \Leftrightarrow x \leq y$, entonces 1 es un elemento maximal y también un máximo, sin embargo no existen ni elemento minimal ni mínimo. El subconjunto $B = \{x \in \mathbb{R} \,/\, 0 < x < 1/2\}$ tiene a $1/2$ como supremo y no tiene ínfimo.

1.4. Estructuras algebraicas elementales

Contar es una de las habilidades más básicas del ser humano y por ello el concepto de número es casi intrínseco a nosotros. *

Desde tiempos muy antiguos, el conjunto de los números naturales se extendió por necesidades prácticas hasta crear los racionales y los enteros. Los enteros, además de sumarse y multiplicarse, se pueden restar (apuntar ganancias y deudas) y los racionales también se pueden dividir (cambiar de escala de medida o cambiar monedas). El desarrollo de las Matemáticas llevó a considerar $\mathbb{R}$ y $\mathbb{C}$ por necesidades más teóricas (tomar límites y resolver ecuaciones). En la actualidad hay objetos más generales, como las matrices, formados por conjuntos en los que se han definido relaciones que recuerdan a las operaciones elementales. Muchos de estos objetos han sido muy útiles para expresar o medir ciertas propiedades físicas, por ejemplo, los tensores en la teoría de la relatividad o los operadores funcionales en la mecánica cuántica. El álgebra intenta aislar la estructura que subyace a estos conjuntos y sus operaciones tratando de no hacer distinciones entre objetos *isomorfos* (con igual forma); así por ejemplo, los números naturales son intrínsecamente los mismos si usamos símbolos griegos, latinos o árabes para representarlos.

En esta sección definiremos algunas de las estructuras que aparecen con más frecuencia en Matemáticas. Aunque puedan parecer generalizaciones innecesarias, son bastante útiles para no tener que probar el mismo resultado en diferentes contextos.

Definición: *Sea $A \subset \mathcal{U}$, una <u>operación</u> en A es una función de $A \times A$ en $\mathcal{U}$. Cuando su imagen está en A se dice que es una <u>ley de composición interna</u> o que es <u>cerrada</u>.*

Definición: *Un <u>grupo</u>, G, es un conjunto dotado con una operación cerrada, $*$, tal que se verifican las siguientes propiedades:*

i) $*$ es asociativa: $g * (h * f) = (g * h) * f$.

ii) Existe el elemento neutro: $\exists e \in G \,/\, \forall g \in G \;\; e * g = g * e = g$.

iii) Existe el elemento inverso: $\forall g \in G \; \exists h \in G \,/\, h * g = g * h = e$. (Se escribe $h = g^{-1}$).

<u>Nota</u>: Si además $*$ es una operación conmutativa ($g * h = h * g$) se dice que el grupo es <u>abeliano</u> o <u>conmutativo</u>. En ese caso se escribe a veces $+$ en vez de $*$ y 0 en vez de e.

---

* Una frase famosa de L. Kronecker (1823-1891) afirma “Die ganzen Zahlen hat der liebe Gott gemacht alles anderes ist Menschenwerk” (“Dios hizo los números, todo lo demás es obra del hombre”). Obviamente, Kronecker fue un matemático.

Definición: *Un* <u>anillo</u>*, A, es un conjunto dotado con dos operaciones cerradas, $\oplus$ y $\otimes$ (suma y multiplicación), de modo que se verifican las siguientes propiedades:*

i) A es un grupo abeliano con respecto a $\oplus$.

ii) $\otimes$ es una operación asociativa en A.

iii) Se cumplen las leyes distributivas (por la izquierda) $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ y (por la derecha) $c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$.

<u>Nota</u>: Si $\otimes$ es conmutativa, se dice que el anillo es <u>conmutativo</u> y si $\otimes$ tiene un elemento neutro se dice que el anillo es <u>unitario</u>.

Definición: *Un* <u>cuerpo</u>*, K es un anillo tal que $K - \{0\}$ es un grupo abeliano con respecto a la multiplicación.*

Para recobrarse de la abstracción de las anteriores definiciones nótese que si olvidamos por un momento el rigor, un grupo abeliano es un conjunto en el que podemos sumar y restar (sumar el inverso), mientras que en un anillo conmutativo además podemos multiplicar; y en un cuerpo, también dividir (salvo por cero).

Cuando no está claro qué operaciones estamos considerando en un conjunto, se suelen indicar explícitamente al lado del conjunto escribiendo todo entre paréntesis. Así por ejemplo, $(\mathbb{Z}, +)$ significa los enteros con la suma.

<u>Ejemplo 1</u>. $(\mathbb{Z}, +)$ es un grupo abeliano.

<u>Ejemplo 2</u>. $(\mathbb{Z}, \times)$ y $(\mathbb{N}, +)$ no son grupos abelianos, porque, por ejemplo, 3 no tiene inverso en ninguno de los dos conjuntos.

<u>Ejemplo 3</u>. $(\mathbb{Z}, +, \times)$ es un anillo pero no es un cuerpo.

<u>Ejemplo 4</u>. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ y $(\mathbb{C}, +, \times)$ son cuerpos.

<u>Ejemplo 5</u>. $(\mathcal{M}_{n\times n}(\mathbb{R}), +, \cdot)$ es un anillo no conmutativo. (Recuérdese que $\mathcal{M}_{n\times n}(\mathbb{R})$ denota las matrices con elementos en $\mathbb{R}$ y dimensiones $n \times n$).

<u>Ejemplo 6</u>. El conjunto, $\mathcal{M}$ de matrices reales 2×2 con determinante 2, no son un grupo con el producto porque esta operación no es cerrada.

$$\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \in \mathcal{M}, \qquad \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \in \mathcal{M} \qquad \text{pero} \quad \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \notin \mathcal{M}.$$

<u>Ejemplo 7</u>. Las funciones $f(x) = x$ y $g(x) = 1/x$ con la composición, es decir, $(\{f, g\}, \circ)$, es un grupo abeliano.

Hoja 1

1) Si $A \cup B = A$, ¿qué relación hay entre A y B?

2) Demostrar que los conjuntos $A - B$, $B - A$ y $A \cap B$ definen una partición de $A \cup B$.

3) Decir si es verdadero o falso

$$i)\ A - B = A \cap B' \qquad ii)\ (A - B) \cup (B - A) = A \cup B$$

$$iii)\ A \triangle B = B \triangle A \qquad iv)\ |A \times B \times C| = |A||B||C|.$$

4) Si $A = \{0, 7\}$ y $B = \{1, 7\}$, hallar $(A \times B) \cap (B \times A)$.

5) Demostrar que $A \cap (A \cup B) = A$.

6) Si A y C son disjuntos, ¿a qué es igual $A \cap (B \cup C)$?

7) Si $A \triangle B = \emptyset$, ¿qué relación hay entre A y B?

8) Demostrar que $A \subset B$ si y sólo $\mathcal{P}(A) \subset \mathcal{P}(B)$.

9) Demostrar que $(A \cap B) \times (C \cap D) = (A \times C) \cap (A \times D) \cap (B \times C) \cap (B \times D)$.

10) Demostrar que $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

11) ¿Qué conjunto es $A \times \emptyset$?

En los tres ejercicios siguientes suponemos que todos los conjuntos son finitos. El asterisco indica un nivel de dificultad mayor.

***12)** Sabiendo $|A|$, calcular $|\mathcal{P}(A)|$. *Pista para informáticos*: Si $A = \{x_1, x_2, \ldots x_n\}$, cada subconjunto de A se puede escribir como una palabra de *n-bits*.

Opcional: Escribe un programa en tu lenguaje de programación favorito que dé una lista de todas las particiones de $\{1, 2, \ldots, n\}$.

13) Demostrar que $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$.

***14)** Intentar generalizar el problema anterior obteniendo una fórmula para $|A_1 \cup A_2 \cup \ldots \cup A_n|$. ¿Cuántos términos tiene?

Opcional: Escribe un programa en tu lenguaje de programación favorito que escriba dicha fórmula en pantalla.

El propósito de este último ejercicio es mostrar que una definición intuitiva de conjunto puede llevar a contradicción.

15) (Paradoja de Russell) Sea C el conjunto de todos los conjuntos que no son elementos de sí mismos, $C = \{A \,/\, A \notin A\}$. Por ejemplo, el conjunto de todos los conjuntos no está en C, o el conjunto de todas las cosas que se pueden describir con palabras; sin embargo el conjunto de números naturales está en C. Demostrar que $C \notin C \Leftrightarrow C \in C$, lo cual es una contradicción.

<u>Nota para el lector interesado</u>: La moderna axiomática de conjuntos no permite construir conjuntos tan "grandes" como C, para ello distingue los conjuntos de otro concepto llamado clases. La paradoja anterior se explica porque C no es un conjunto sino una clase y por tanto $C \notin C$ no implica $C \in C$. De hecho la diferencia entre conjuntos y clases es que estas últimas pueden no ser elementos de ninguna otra clase.

Hoja 2

En los siguientes ejercicios el superíndice $+$ en los conjuntos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ indica que sólo se consideran los elementos estrictamente positivos.

1) Calcular la imagen de las siguientes funciones: *i)* $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, $f(x) = 3x + 1$; *ii)* $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2 + 3$; *iii)* $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$, $f(n) = 2n + 4$; *iv)* $f : \mathbb{R} - \{3\} \longrightarrow \mathbb{R}$, $f(x) = (x + 3)/(x - 3)$.

2) Sea T el conjunto de todos los triángulos y sea $f : T \longrightarrow \mathbb{R}^+$ la función que asigna a cada una de ellos el valor (en grados) del menor de sus ángulos. Hallar $f^{-1}(\{60\})$ y $f(\{\text{triángulos rectángulos}\})$.

3) Comprobar que $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{1\}$ dada por $f(x) = x/(x - 1)$ es biyectiva y que coincide con su inversa.

4) Decidir de qué tipo son las funciones f, $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ definidas por

$$f(n) = \begin{cases} n+1 & \text{si } n \text{ es par} \\ 2n & \text{si } n \text{ es impar} \end{cases} \qquad g(n) = \begin{cases} n+2 & \text{si } n \text{ es par} \\ (n+1)/2 & \text{si } n \text{ es impar.} \end{cases}$$

5) Sean f, g, $h : \mathbb{R} \longrightarrow \mathbb{R}$ definidas por $f(x) = 2x - 1$, $g(x) = x^2 - x + 4$, $h(x) = 1/\sqrt{x^2 + 2}$. Estudiar si f, g y h son inyectivas o sobreyectivas y calcular $f \circ g$, $g \circ f$ y $h \circ h$.

6) Sea $f : A \longrightarrow B$, demostrar que $\operatorname{Im} f = \{x \in B \,/\, f^{-1}(\{x\}) \neq \emptyset\}$ y que f es inyectiva si y sólo si $|f^{-1}(\{x\})| \leq 1$ para todo $x \in B$.

7) Se dice que $f_A : \mathcal{U} \longrightarrow \{0, 1\}$ es la función característica de A si toma el valor 1 en A y 0 en A'. Demostrar que $f_A \cdot f_B = f_{A\cap B}$ y $\max(f_A, f_B) = f_{A\cup B}$.

8) Si $f : \mathcal{U} \longrightarrow \mathcal{U}$ y $A, B \subset \mathcal{U}$, decir si son verdaderas o falsas las siguientes fórmulas

$$i)\ f(A) \cap f(B) = f(A \cap B) \qquad ii)\ f^{-1}(A) \cap f^{-1}(B) = f^{-1}(A \cap B)$$
$$iii)\quad f(A') = \big(f(A)\big)' \qquad iv)\quad f^{-1}(A') = \big(f^{-1}(A)\big)' \quad .$$

9) Si A y B son conjuntos finitos y $f : A \longrightarrow B$, ¿qué relación hay entre $|A|$ y $|B|$ cuando f es inyectiva, sobreyectiva o biyectiva, respectivamente? <u>Nota</u>: G. Cantor demostró que hay una función biyectiva entre $\mathbb{N}$ y $\mathbb{Q}$ pero que no existe ninguna entre $\mathbb{Q}$ y $\mathbb{R}$. En ese sentido $\mathbb{R}$ es "más infinito" que $\mathbb{N}$ o que $\mathbb{Q}$.

10) Sea $f : \mathbb{N} \longrightarrow \mathbb{Z}^+$ tal que $f(n) =$ número de cifras de 10^n. Describir f^{-1}.

11) Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son biyectivas, demostrar que $g \circ f$ también lo es y que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

12) Demostrar que si $g \circ f$ es inyectiva entonces f es inyectiva, y si $g \circ f$ es sobreyectiva, g es sobreyectiva.

Recuérdese que $V_n^m = n!/(n - m)!$ es el número de formas de escoger m objetos entre n dados importando el orden y sin repetición.

13) Si A y B son conjuntos finitos calcular cuántas funciones inyectivas y cuántas biyectivas hay de A en B.

Opcional: Escribe un programa en tu lenguaje de programación favorito que calcule todas la funciones inyectivas de $\{1, 2, \ldots, i\}$ en $\{1, 2, \ldots, j\}$ donde $i < j$.

Hoja 3

1) Sea $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ y la relación $a\mathcal{R}b \Leftrightarrow 3$ divide a $b^2 - a^2$. Comprobar que es una relación de equivalencia y hallar las clases.

2) Dada la relación de orden $n\mathcal{R}m \Leftrightarrow n$ divide a m, hallar los elementos maximales, minimales, máximos y mínimos (si existen) en el conjunto $A = \{2, 3, 5, 6, 10, 15, 30\}$. ¿Es $\mathcal{R}$ una relación de orden total en A?

3) Demostrar que en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ la relación $(a, b)\mathcal{R}(c, d) \Leftrightarrow ad - bc = 0$ es de equivalencia.

4) En $C = \{f \,/\, f : [0, 1] \longrightarrow \mathbb{R}$ con f continua$\}$ definimos la relación $f\mathcal{R}g \Leftrightarrow \max f \leq \max g$. Estudiar si es de orden.

5) En $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ se define la relación $(a, b)\mathcal{R}(c, d) \Leftrightarrow$ se cumple $a < c$ ó se cumple $a = c$ y $b \leq d$. Estudiar de qué tipo de es.

6) Generalizar el ejercicio anterior para obtener una relación de orden en $\mathbb{R}^3$.

<u>Nota</u>: A la generalización de esta relación a $\mathbb{R}^n$ se le llama <u>orden lexicográfico</u>. Este nombre viene porque si asignamos en orden creciente a cada letra un número (por ejemplo su código ASCII), ordenar palabras de n letras con esta relación (desde el mínimo al máximo) es lo mismo que escribirlas por orden alfabético.

Opcional: Escribir un progama en tu lenguaje de programación favorito que ordene por orden lexicográfico los elementos de cualquier subconjunto dado de $A \times A \times \overset{n \text{ veces}}{\cdots\cdots} \times A$ con $A = \{1, 2, 3, \ldots, m\}$.

7) Demostrar que la relación en $\mathbb{Z}^+$ definida por $n\mathcal{R}m \Leftrightarrow mn$ es un cuadrado perfecto, es una relación de equivalencia. Hallar las clases de 1, 2 y p con p primo.

8) Estudiar si $A = \{\frac{2-n}{n}$ con $n \in \mathbb{Z}^+\}$ tiene supremo e ínfimo como subconjunto de $\mathbb{R}$.

9) Comprobar que en $C = \{0, 1, 2, 3, 4, 5, 6\}$, la relación $n\mathcal{R}m \Leftrightarrow 7$ divide a $n^2m - m^2n - n + m$, es de equivalencia.

***10)** Si cambiamos 7 por cualquier primo, p, ¿es la relación del ejercicio anterior de equivalencia en $C = \{0, 1, 2, \ldots, p - 1\}$?

11) ¿Cuántas relaciones distintas de orden total se pueden definir en un conjunto de n elementos?

12) En $\mathcal{P}(\mathbb{R})$ se define la relación $A\mathcal{R}B \Leftrightarrow$ existe una función biyectiva de A en B. Demostrar que es una relación de equivalencia y que $\mathbb{N}$ y $\mathbb{Z}$ pertenecen a la misma clase.

*****13)** En las clases de equivalencia del ejercicio anterior se define la relación $C_\alpha\mathcal{R}C_\beta \Leftrightarrow$ existe una función inyectiva de un elemento de C_α en otro de C_β. Demostrar que esta relación es de orden. *Indicación*: Lo más complicado es probar la propiedad antisimétrica. La idea es encontrar particiones $A = A_1 \cup A_2$ y $B = B_1 \cup B_2$ para cada par de funciones inyectivas $f : A \longrightarrow B$, $g : B \longrightarrow A$, de manera que $f : A_1 \longrightarrow B_1$ y $g : B_2 \longrightarrow A_2$ sean biyectivas. Para ello A_1 debe satisfacer $A_1 = g(B - f(A - A_1))$.

Hoja 4

1) Las matrices de $\mathcal{M}_{2\times 2}(\mathbb{R})$ se suelen escribir en la forma $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Decir si es verdadero o falso que los siguientes subconjuntos de $\mathcal{M}_{2\times 2}(\mathbb{R})$ tienen la estructura que se afirma:

i) $\big(\{A \,/\, a_{21} = 0\}, +, \cdot\big)$ es un cuerpo.

ii) $\big(\{A \,/\, a_{12} = 0\}, +, \cdot\big)$ es un anillo no conmutativo.

iii) $\big(\{A \,/\, a_{11}a_{22} - a_{12}a_{21} = 1\}, \cdot\big)$ es un grupo.

iv) $\big(\{A \,/\, a_{11} = a_{22},\ a_{12} = a_{21} = 0\}, +, \cdot\big)$ es un cuerpo.

v) $\big(\{A \,/\, a_{ij} \in \mathbb{Z},\ a_{11}a_{22} - a_{12}a_{21} = 1 \text{ y } a_{21} \text{ es par}\}, \cdot\big)$ es un grupo.

vi) $\big(\{A \,/\, a_{12} = a_{21}\}, +, \cdot\big)$ es un anillo.

2) Comprobar que el conjunto $\{n + m\sqrt{2} \,/\, n, m \in \mathbb{Z}\}$ es un anillo con la suma y producto habituales.

3) Comprobar que $x * y = \frac{x+y}{1+xy}$ define una operación cerrada en $C = \{-1 < x < 1\}$. ¿Es $(C, *)$ un grupo abeliano?

4) Estudiar si en $\mathbb{Z}$ la operación $n * m = n + m + 2mn$ es conmutativa y asociativa.

5) Comprobar que el conjunto de funciones $C = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$ no es un grupo abeliano con la composición. ¿Lo es si exigimos que las funciones sean biyectivas?

6) Comprobar que la operación $n * m = nm(n+1)(m+1)/4$ es cerrada en $\mathbb{Z}$. ¿Es conmutativa y asociativa?

7) En el conjunto $P = \{\diamondsuit, \clubsuit, \spadesuit, \heartsuit\}$ se definen las operaciones $\oplus$ y $\otimes$ con las siguientes tablas:

$\oplus$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$
$\diamondsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$
$\clubsuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$

$\otimes$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$
$\diamondsuit$	$\diamondsuit$	$\diamondsuit$	$\diamondsuit$	$\diamondsuit$
$\clubsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$
$\spadesuit$	$\diamondsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$
$\heartsuit$	$\diamondsuit$	$\heartsuit$	$\clubsuit$	$\spadesuit$

Con estas operaciones, P es un cuerpo.

i) Comprobar la propiedad asociativa para $\clubsuit \oplus \spadesuit \oplus \heartsuit$.

ii) ¿Cuál es el inverso multiplicativo de $\spadesuit$?

iii) Resolver la ecuación $x \oplus x \oplus (\heartsuit \otimes x) = \clubsuit$.

Nota: El grupo abeliano $(P, \oplus)$ se llama grupo de Klein o *Viergruppe*. En el libro de Miguel de Guzmán "Cuentos con cuentas", se dan un par de aplicaciones de este grupo a la resolución de algunos rompecabezas.

8) Demostrar que la diferencia simétrica de conjuntos es una operación conmutativa y asociativa.

Miscelánea.

La teoría de conjuntos fue iniciada por G. Cantor (1845-1918) a finales del siglo pasado. A pesar de las duras críticas iniciales a sus métodos (Cantor tuvo que ser hospitalizado varias veces por las fuertes depresiones que éstas le ocasionaron), sus ideas convenientemente formalizadas han alcanzado un lugar muy importante en las Matemáticas, de hecho D. Hilbert (1862-1943) acuñó la frase *"del paraíso que ha creado Cantor nadie nos sacará"*.

Una de las contribuciones más importantes de Cantor fue la de crear una teoría de cardinales infinitos. La idea es que, por ejemplo, hay tantos números naturales como números pares positivos (a pesar de la inclusión $\{\text{números pares}\} \subset \mathbb{N}$) en el sentido de que existe una función biyectiva

$$\begin{aligned} f_1 :&\mathbb{N} \longrightarrow \{\text{números pares}\} \\ &n \longrightarrow \ 2n+2 \end{aligned}$$

De la misma forma, los naturales y los impares positivos, o los pares y los impares tienen el mismo cardinal en el sentido de que se tienen las funciones biyectivas

$$\begin{aligned} f_2 :&\mathbb{N} \longrightarrow \{\text{números impares}\} \\ &n \longrightarrow \ 2n+1 \end{aligned} \qquad \begin{aligned} f_3 : \{\text{números impares}\} &\longrightarrow \{\text{números pares}\} \\ n &\longrightarrow \ n+1 \end{aligned}$$

A todos los conjuntos que se pueden poner en biyección con $\mathbb{N}$, Cantor les asignó el cardinal infinito $\aleph_0$ (se lee "alef sub cero"). Considerando, por ejemplo, la función

$$\begin{aligned} f_4 : \mathbb{R} &\longrightarrow (0,1) \\ x &\longrightarrow \frac{1}{2} + \frac{1}{\pi}\operatorname{arctg} x \end{aligned}$$

se prueba que $\mathbb{R}$ y el intervalo $(0,1)$ tienen el mismo cardinal. Cantor asignó el cardinal infinito c a estos conjuntos. La pregunta natural es si c es igual a $\aleph_0$, es decir

¿Existe una función biyectiva de $\mathbb{N}$ en $\mathbb{R}$?

La respuesta es negativa. Si existiera una función tal, componiendo con f_4 tendríamos $f : \mathbb{N} \longrightarrow (0,1)$ biyectiva, y la imposibilidad de esta función se prueba por el *"proceso diagonal de Cantor"*. Para ilustrarlo, supongamos que escribimos los valores que toma la función f en una tabla

$$\begin{aligned} 0 &\longrightarrow f(0) = 0'a_{11}a_{12}a_{13}a_{14}\dots \\ 1 &\longrightarrow f(1) = 0'a_{21}a_{22}a_{23}a_{24}\dots \\ 2 &\longrightarrow f(2) = 0'a_{31}a_{32}a_{33}a_{34}\dots \\ 3 &\longrightarrow f(3) = 0'a_{41}a_{42}a_{43}a_{44}\dots \\ &\dots \quad \dots\dots \quad \dots \quad \dots \end{aligned}$$

Consideremos el *número diagonal* $\alpha = 0'a_{11}a_{22}a_{33}a_{44}\dots$ y construyamos a partir de él un nuevo número $\beta = 0'b_1b_2b_3b_4\dots$ tal que su cifra b_i es 1 si $a_{ii} \neq 1$ y es 2 si $a_{ii} = 1$. El número β está en $(0,1)$ pero no pertenece a la imagen de la función f, ya que no es $f(0)$ porque las primeras cifras decimales no coinciden, no es $f(1)$ porque las segundas cifras decimales no coinciden, etc.

Variaciones de este proceso prueban que el cardinal de un conjunto A es siempre distinto (y menor en el sentido que se indica más abajo) al de $\mathcal{P}(A)$, de hecho si Card $A = \aleph_0$ entonces Card $\mathcal{P}(A) = c$. También se puede demostrar que existe un cardinal infinito inmediatamente posterior a $\aleph_0$, llamado $\aleph_1$, pero no es en absoluto claro si $c = \aleph_1$ (hipótesis del continuo), es decir, si hay un conjunto, C, de cardinal mayor que $\mathbb{N}$ y menor que $\mathbb{R}$ en el sentido de que existan funciones inyectivas $f : \mathbb{N} \longrightarrow C$ y $f : C \longrightarrow \mathbb{R}$.

Los resultados conjuntistas de Cantor antes de que la teoría estuviera bien fundamentada, daban lugar a contradicciones que motivaron grandes controversias. Por ejemplo, B. Russell (1872-1970) notó que Card $A <$ Card $\mathcal{P}(A)$ es contradictorio si tomamos como A el conjunto de todos los conjuntos, ya que éste debiera contener a todos los elementos de $\mathcal{P}(A)$ y por tanto cumplir la desigualdad contraria. Situaciones como ésta fueron el detonante de un desarrollo axiomático y riguroso de la teoría de conjuntos que culminó con el sistema de axiomas ZF por E. Zermelo (1871-1953) y A. Fraenkel (1891-1965). La mayoría de los matemáticos admiten un axioma adicional llamado de elección y se habla del sistema ZFC.

El desarrollo de la teoría de conjuntos fue paralelo al de la lógica matemática y a la preocupación por los fundamentos de las Matemáticas. En el terreno de la Filosofía este ambiente se reflejó en el Neopositivismo y otras tendencias afines que propugnaban en diferentes versiones que los hechos tienen una estructura lógica y lingüística (*La proposición es una pintura de la realidad* según el "primer" Wittgenstein), con lo cual la Filosofía se reduce al descubrimiento de la forma lógica de las proposiciones. Russell y A.N. Whitehead (1861-1947) intentaron dar el primer paso escribiendo una obra enciclopédica en la que trataban de hacer de las Matemáticas una rama de la Lógica. El resultado no fue satisfactorio porque eran necesarios algunos conceptos que escapaban del ámbito de esta última. Por otro lado la escuela formalista de Hilbert se preguntaba acerca de la consistencia y completitud de las Matemáticas, es decir, si es posible probar que no hay nada contradictorio en los axiomas y si se puede probar que todas las "verdades" son demostrables en el sentido de que siempre un teorema o su negación es deducible a partir de los axiomas. En 1931 K. Gödel (1906-1978) acabó con todas estas cuestiones demostrando que es imposible (en algún sentido) probar la consistencia de los sistemas formales de la Matemática clásica y que además, si fueran consistentes siempre habrá sentencias indecidibles (no demostrables) por muchos axiomas que añadamos. En esta línea merece mencionar el resultado del propio Gödel y P.J. Cohen (1934-) afirmando que la hipótesis del continuo, $c = \aleph_1$, es indemostrable con los axiomas ZF. Quizá para algunos todo este panorama sea desalentador y en la más dura línea posmoderna de "no hay futuro", pero a otros no les da miedo pensar que las Matemáticas no son ciencias exactas y esta situación de indeterminación e incertudumbre las hace más infinitas y más cercanas todavía a la poesía (*La esencia de las Matemáticas está en su libertad*, según Cantor). En cualquier caso, la duda acerca de la consistencia de las Matemáticas no ha sido razón para que los matemáticos dejen de trabajar en ellas.

> Desque están dubdando los omnes qué han de fazer,
> poco trabajo puede sus coraçones vençer;
> torre alta desque tienbla non ay sinon caer:
> la muger que está dubdando, ligera es de aver.
> *LBA, 642*

Con respecto a las estructuras algebraicas elementales que tratamos en la última sección, queremos insistir en que todas ellas aparecieron históricamente por un proceso de abstracción sobre la estructura que subyace a algunos problemas concretos. Aunque las definiciones de grupo, anillo, etc. surgieron de los ejemplos particulares, en estas notas (y en la mayor parte de los libros de Matemáticas) se sigue la política contraria definiendo primero estos concepto abstractos y estudiando más tarde algunos ejemplos particulares. Seguramente el matemático profesional y especialmente el algebrista saben tolerar este proceso y soportan sin pestañear definiciones muy enrevesadas, pero muchos de los estudiantes de una asignatura de Matemáticas quedan apabullados por esta tendencia a la abstracción generalizadora y al Definición-Teorema-Corolario previo a los ejemplos. Desde el punto de vista pedagógico esta situación se refleja en dos posturas más o menos opuestas: La primera (que tuvo su auge hace años en Francia) propone un aprendizaje lógico de las Matemáticas, comenzando por los conceptos más elementales como conjunto, número, etc. y siguiendo un proceso deductivo hasta llegar a los ejemplos y resultados que involucran todos esos conceptos. La segunda (según parece, más de moda en el bachillerato actual) intenta desarrollar cierta intuición sobre los ejemplos e inducir de ellos los principios básicos que están involucrados. Seguramente las dos tendencias llevadas al extremo son igualmente disparatadas aunque cuenten con *fans* de prestigio.

> Dotores más de çiento, en libros e en qüestiones,
> con fuertes argumentos, con sotiles razones,
> tienen sobre estos casos diversas opiniones:
> pues, por non dezir tanto, non me rebtedes, varones.
> *LBA, 1153*

2. Los Anillos $\mathbb{Z}$ y $\mathbb{Z}_m$

2.1. Máximo común divisor, mínimo común múltiplo, algoritmo de Euclides

Ya sabemos que $\mathbb{Z}$ es un anillo, pero entre los anillos tiene una propiedad muy especial y es que todo número entero se puede factorizar de manera única en términos de ciertos números enteros "especiales" llamados primos. Realmente, esto es consecuencia de una propiedad muy sencilla (recogida en la siguiente proposición) pero que muchas veces no comparten otros anillos.

Proposición 1.1 : *Dados $a, b \in \mathbb{Z}$, $b \neq 0$, existen dos únicos números enteros q y r (llamados cociente y resto) que cumplen*

$$a = bq + r \qquad \textit{con} \;\; 0 \le r < |b|.$$

<u>Dem.</u>: Sea r el menor valor no negativo que toma $a - bq$ cuando $q \in \mathbb{Z}$, entonces $r < |b|$ ya que si $r \ge |b|$, aumentando o disminuyendo (si b es negativo) q en una unidad obtendríamos un valor de r menor. el cociente y el resto son únicos porque $a = bq_1 + r_1$, $a = bq_2 + r_2$ implica $b(q_2 - q_1) = r_1 - r_2$ lo que contradice que $0 \le r_1, r_2 < |b|$ excepto en el caso trivial $q_2 - q_1 = r_1 - r_2 = 0$. ■

Si en la proposición anterior r es cero, entonces b divide a a y se escribe $b|a$. En caso contrario se escribe $b \not| a$. Muchas veces al cáculo del cociente y el resto se le llama "división entera de a y b".

Nótese que el resto siempre se toma mayor o igual que cero, aunque a o b sean negativos.

<u>Ejemplo</u> .

$$a = 12, \;\; b = 7 \;\Rightarrow 12 = 7 \cdot 1 + 5 \qquad a = 12, \;\; b = -7 \;\Rightarrow 12 = -7 \cdot (-1) + 5.$$

La consecuencia más importante del resultado anterior es que se puede definir el máximo común divisor y que hay un método para hallarlo llamado "algoritmo de Euclides". Por ello, cuando en un anillo se cumple una propiedad análoga a la Proposición 1.1 se dice que es un dominio euclídeo. Veremos otro ejemplo de dominio euclídeo en el siguiente capítulo pero ahora nos restringiremos a $\mathbb{Z}$.

Definición: *Se dice que d es un <u>máximo común divisor</u> de dos enteros a y b no simultáneamente nulos si*

$$1) \; d|a, \; d|b \quad \text{(es divisor común)} \qquad 2) \; d'|a, \; d'|b \;\Rightarrow\; d'|d \quad \text{(es “máximo”)}$$

Definición: *Se dice que m es un <u>mínimo común multiplo</u> de dos enteros a y b no nulos si*

$$1) \; a|m, \; b|m \quad \text{(es múltiplo común)} \qquad 2) \; a|m', \; b|m' \;\Rightarrow\; m|m' \quad \text{(es “mínimo”)}$$

La notación habitual es escribir $d = \operatorname{mcd}(a,b)$ y $m = \operatorname{mcm}(a,b)$. Obsérvese que d y m no son únicos, concretamente, si d es un máximo común divisor, entonces $-d$ también lo es y lo mismo ocurre con el mínimo común múltiplo. Por ello, cuando escribimos $\operatorname{mcd}(a,b)$ o $\operatorname{mcm}(a,b)$ dentro de alguna igualdad, queremos indicar, con el abuso de notación obvio, que dicha igualdad se satisface para alguna elección del máximo común divisor o del mínimo común múltiplo, respectivamente. Normalmente se suelen escoger positivos para eliminar toda ambigüedad.

Si tenemos $n > 2$ números enteros, $a_1, a_2, \ldots, a_n$, se puede definir el máximo común divisor y el mínimo común múltiplo de ellos usando las siguientes fórmulas recursivas

$$\begin{aligned} \operatorname{mcd}(a_1, a_2, \ldots, a_n) =& \operatorname{mcd}\big(\operatorname{mcd}(a_1, a_2, \ldots, a_{n-1}), a_n\big) \\ \operatorname{mcm}(a_1, a_2, \ldots, a_n) =& \operatorname{mcm}\big(\operatorname{mcm}(a_1, a_2, \ldots, a_{n-1}), a_n\big). \end{aligned}$$

No es difícil comprobar que el orden de $a_1, a_2, \ldots, a_n$ no es relevante a la hora de calcular el máximo común divisor y el mínimo común múltiplo.

Ejemplo 1. 2 y -2 son máximos comunes divisores de 6 y 10. 30 y -30 son mínimos comunes múltiplos de 6 y 10.

Ejemplo 2. mcd (168,77,50)=mcd (mcd (168,77),50)=mcd (7,50)=1 (y también -1 es un máximo común divisor).

El algoritmo de Euclides es simplemente un método iterativo para calcular el máximo común divisor basado en la aplicación repetida del siguiente lema

Lema 1.2 : *Sea $a = bq + r$ la división entera de a y b, entonces* $\operatorname{mcd}(a,b) = \operatorname{mcd}(b,r)$.

DEM.: La ecuación $a = bq + r$ implica que si d divide a b y a r entonces también divide a a. De la misma forma, de $r = a - bq$ se deduce que si d divide a a y a b también divide a r. Así pues, los divisores comunes de a, b y de b, r coinciden y, por tanto, sus máximos comunes divisores son iguales. ■

Ejemplo . Calcular $\operatorname{mcd}(85, 65)$ usando el algoritmo de Euclides

$$\begin{aligned} 85 = 65 \cdot 1 + 20 \quad &\Rightarrow \quad \operatorname{mcd}(85,65) = \operatorname{mcd}(65,20) \\ 65 = 20 \cdot 3 + 5 \quad &\Rightarrow \quad \operatorname{mcd}(65,20) = \operatorname{mcd}(20,5) \\ 20 = 5 \cdot 4 + 0 \quad &\Rightarrow \quad \operatorname{mcd}(20,5) = \operatorname{mcd}(5,0) = 5 \end{aligned}$$

Observación: El algoritmo de Euclides no sólo permite reducir el cálculo de $\operatorname{mcd}(a,b)$ al de $\operatorname{mcd}(n,0)$ (que es trivialmente n), sino que también prueba que $\operatorname{mcd}(a,b)$ siempre existe para a y b no simultáneamente nulos, ya que $\text{mcd}\,(n,0)$ existe. Nótese que la existencia del máximo común divisor no es inmediata a partir de la definición que hemos dado aquí.

El algoritmo de Euclides puede usarse indirectamente para calcular también el mcm gracias a la siguiente relación

Lema 1.3 : *Para* $a, b \neq 0$

$$\text{mcm}\,(a,b) = \frac{ab}{\text{mcd}\,(a,b)}.$$

<u>Ejemplo</u> . Calcular $\text{mcm}\,(168,77)$ con el algoritmo de Euclides.

$$\left.\begin{aligned} 168 =& 77 \cdot 2 + 14 \\ 77 =& 14 \cdot 5 + 7 \\ 14 =& 7 \cdot 2 + 0 \end{aligned}\right\} \Rightarrow \text{mcd}\,(168,77) = 7 \ \Rightarrow \text{mcm}\,(168,77) = \frac{168 \cdot 77}{7} = 168 \cdot 11 = 1848.$$

La siguiente proposición nos dice cómo hallar las soluciones enteras de una ecuación lineal con dos incógnitas

Proposición 1.4 : *Si* $d = \text{mcd}\,(a,b)$, *entonces existen enteros* n *y* m *tales que*

$$d = an + bm \qquad (\textit{Identidad de Bezout}).$$

De hecho todas las soluciones $x, y \in \mathbb{Z}$ *de la ecuación* $d = ax + by$ *vienen dadas por*

$$(1.1) \qquad \begin{cases} x =& n - bt/d \\ y =& m + at/d \end{cases} \qquad \textit{con } t \in \mathbb{Z}.$$

Obsérvese que hubiera bastado enunciar la proposición en el caso $d = 1$, porque dividiendo por d la ecuación $d = ax + by$ se obtiene $1 = a'x + b'y$ que tiene las mismas soluciones.

Muchas veces es sorprendentemente difícil hallar “por tanteos” n y m tales que $d = an + bm$. Nuevamente, el algoritmo de Euclides resuelve este problema. El método está indicado en la siguiente observación cuyo significado recomendamos entender a través de los ejemplos subsiguientes.

<u>Observación</u>: Los números n y m de la proposición anterior se pueden calcular escribiendo el algoritmo de Euclides para a y b, despejando d de la penúltima identidad,

sustituyendo el divisor usando la identidad anterior hasta escribir d en términos del dividendo y divisor de dicha identidad y repitiendo este último proceso hasta agotar todas las identidades que constituyen el algoritmo de Euclides.

Ejemplo 1. Hallar n y m tales que $7 = 168n + 77m$. Como ya hemos visto en un ejemplo anterior, $\mathrm{mcd}\,(168, 77) = 7$ y el algoritmo de Euclides viene dado por

$$168 = 77 \cdot 2 + 14 \qquad 77 = 14 \cdot 5 + 7 \qquad 14 = 7 \cdot 2 + 0.$$

De la penúltima identidad se obtiene $7 = 77 - 14 \cdot 5$ Ahora sustituyendo el divisor, 14, utilizando la primera identidad y dejando todo en función de 168 y 77, se obtiene

$$\begin{aligned} 7 =& 77 - (168 - 77 \cdot 2) \cdot 5 \\ =& 77 - 168 \cdot 5 + 77 \cdot 10 \\ =& 168(-5) + 77 \cdot 11. \end{aligned}$$

Por tanto se puede tomar $n = -5$ y $m = 11$. De hecho, según (1.1), todas las soluciones enteras de $7 = 168x + 77y$ vienen dadas por

$$\begin{cases} x = & -5 - 11t \\ y = & 11 + 24t \end{cases} \qquad \text{con } t \in \mathbb{Z}.$$

Ejemplo 2. Hallar n y m tales que $1 = 29n + 8m$

$$\begin{aligned} 29 &= 8 \cdot 3 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 1 \cdot 2 + 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} &(4^{\underline{a}} \text{ ecuación}) \ 1 = 3 - 2 \cdot 1 \\ &(3^{\underline{a}} \text{ ecuación}) \ 1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 5 \cdot (-1) + 3 \cdot 2 \\ &(2^{\underline{a}} \text{ ecuación}) \ 1 = 5 \cdot (-1) + (8 - 5 \cdot 1) \cdot 2 = 8 \cdot 2 + 5 \cdot (-3) \\ &(1^{\underline{a}} \text{ ecuación}) \ 1 = 8 \cdot 2 - (29 - 8 \cdot 3) \cdot 3 = 29 \cdot (-3) + 8 \cdot 11. \end{aligned}$$

Así pues podemos tomar $n = -3$ y $m = 11$. Todas las soluciones enteras de $1 = 29x + 8y$ son

$$\begin{cases} x = & -3 - 8t \\ y = & 11 + 29t \end{cases} \qquad \text{con } t \in \mathbb{Z}.$$

Por ejemplo, tomando $t = -1$ se tiene que $x = 5$, $y = -18$ es una solución.

Hay ecuaciones de la forma $ax + by = c$ que tienen soluciones en enteros aunque $c \neq \mathrm{mcd}\,(a, b)$. Por ejemplo, $x = 2$, $y = 3$ resuelven $5x + 7y = 31$. En realidad todo se basa en una observación muy sencilla: Si resolvemos $5n+7m=1$ con el algoritmo de Euclides se obtiene $n=3$, $m=-2$ y por tanto $n'=31\cdot 3=93$, $m'=31\cdot(-2)=-62$ cumplen $5n'+7m'=31$ y de hecho todas las soluciones de $5x+7y=31$ son

$$\begin{cases} x = 93-7t \\ y = -62+5t \end{cases} \qquad \text{con } t\in\mathbb{Z}.$$

Tomando $t=13$ se obtiene la solución $x=2$, $y=3$ que anunciábamos al principio.

Nótese, de nuevo, que el cálculo de las soluciones de ecuaciones tales como $10x+14y=62$ o $15x+21y=63$ no requieren ningún trabajo adicional, ya que pueden ser simplificadas obteniéndose la ecuación de partida.

Todas estas observaciones acerca de las soluciones de $ax+by=c$ se resumen en la siguiente proposición

Proposición 1.5 : *Sea la ecuación*

$$ax+by=c \qquad \textit{con} \quad d=\operatorname{mcd}(a,b)\big|c \tag{1.2}$$

y sea $Ax+By=C$ la misma ecuación una vez simplificada por d. Si n,m es una solución de $An+Bm=1$ entonces todas las soluciones enteras de $Ax+By=C$, y por tanto de (1.2), *vienen dadas por*

$$\begin{cases} x = Cn-Bt \\ y = Cm+At \end{cases} \qquad \textit{con } t\in\mathbb{Z}.$$

Observación: Nótese que $\operatorname{mcd}(A,B)=1$ y, por tanto, siempre es posible hallar n y m tales que $An+Bm=1$. Nótese también que la ecuación (1.2) no tendría solución si $d\not| c$ (ejercicio).

DEM.: Basta demostrar que si x,y es una solución, entonces $\alpha=x-Cn$, $\beta=y-Cm$ cumplen $\alpha=-Bt$, $\beta=At$ para algún $t\in\mathbb{Z}$.

De $A\alpha+B\beta=0$ (Cn, Cm y x,y son soluciones) se deduce $A|B\beta$ y, como además $A\beta n+B\beta m=\beta$, se tiene $A|\beta$. De la misma forma se prueba $B|\alpha$. Así pues $\beta=At$ y $\alpha=Bt'$ para ciertos $t,t'\in\mathbb{Z}$, y $A\alpha+B\beta=0$ implica $t'=-t$. ■

Ejemplo . Hallar todas las soluciones enteras de la ecuación $15x+6y=153$.

Primero simplificamos por $3=\operatorname{mcd}(15,6)$, obteniéndose

$$5x+2y=51.$$

Ésta es la ecuación $Ax + By = C$. Por el algoritmo de Euclides

$$\left.\begin{aligned} 5 =& 2 \cdot 2 + 1 \\ 2 =& 1 \cdot 2 + 0 \end{aligned}\right\} \Rightarrow \; 1 = 5 \cdot 1 - 2 \cdot 2.$$

Entonces $n = 1$, $m = -2$ cumplen $5n + 2m = 1$ y todas las soluciones de la ecuación son

$$\begin{cases} x =& 51 \cdot 1 - 2t \\ y =& 51 \cdot (-2) + 5t \end{cases} \qquad \text{con } t \in \mathbb{Z}.$$

Si sólo quisiéramos hallar las soluciones naturales, en lugar de las enteras, entonces tendríamos que imponer $51 - 2t \geq 0$, $-102 + 5t \geq 0$ de donde se deduce $20'4 \leq t \leq 25'5$. Como t toma valores enteros, sólo hay cinco posibilidades:

$$t = 21 \to x = 9, \; y = 3 \qquad t = 22 \to x = 7, \; y = 8 \qquad t = 23 \to x = 5, \; y = 13$$
$$t = 24 \to x = 3, \; y = 18 \qquad t = 25 \to x = 1, \; y = 23.$$

Para generalizar los conceptos introducidos en esta sección a otros anillos, es conveniente introducir el lenguaje de los llamados ideales. Su definición sólo es necesaria en un marco bastante abstracto. Aquí la utilizaremos para dar definiciones alternativas de máximo común divisor y mínimo común múltiplo.

DEFINICIÓN: *Un <u>ideal</u>, I en $\mathbb{Z}$ es un subconjunto de $\mathbb{Z}$ tal que*

$$1) \; a, b \in I \Rightarrow a + b \in I \qquad 2) \; a \in I, \; c \in \mathbb{Z} \Rightarrow ac \in I.$$

Proposición 1.6 : *En $\mathbb{Z}$ cada ideal está formado por los múltiplos de cierto número entero, n.*

Normalmente se escribe $I = (n)$ y se dice que n es un <u>generador</u> de I.

<u>Ejemplo</u> . Los números pares son un ideal igual a (2). También se tiene

$$(1) = (-1) = \mathbb{Z}, \qquad (0) = \{0\} \qquad (-3) = \text{múltiplos de tres.}$$

DEFINICIÓN: (alternativa de mcm) Un mínimo común múltiplo de $a_1, a_2, \ldots, a_n$ es un generador de $(a_1) \cap (a_2) \cap \ldots \cap (a_n)$.

DEFINICIÓN: (alternativa de mcd) Un máximo común divisor de $a_1, a_2, \ldots, a_n$ es un generador del menor ideal que contiene a $\{a_1, a_2, \ldots a_n\}$.

<u>Observación</u>: Se puede probar que el ideal al que se refiere la última definición es

$$\{a_1 k_1 + a_2 k_2 + \ldots + a_n k_n \,/\, k_i \in \mathbb{Z}\}.$$

Observación: Nótese que estas definiciones alternativas y la última proposición demuestran que el mcd y el mcm siempre existen. Sin embargo esta demostración es en cierta forma engañosa, ya que para probar la proposición es necesario, de una forma u otra, conocer la existencia del máximo común divisor.

2.2. Números primos y primos entre sí, teorema de factorización

Es bien conocida la definición tradicional de que un número primo es aquel que sólo es divisible por él mismo y por la unidad. Sin embargo, este concepto de primalidad debe ser ligeramente revisado en $\mathbb{Z}$ que también incluye posibles divisores negativos; además hay razones teóricas que sugieren excluir 1 y -1 del conjunto de los primos.

Definición: *Se dice que $p \in \mathbb{Z}$ es primo si $p \neq \pm 1$ y sólo es divisible por ± 1 y $\pm p$.*

También reciben un nombre especial los pares de números que sólo tienen divisores comunes triviales, concretamente

Definición: *Se dice que dos enteros a, b son primos entre sí cuando* $\operatorname{mcd}(a, b) = 1$.

Obsérvese que si p es primo, para cualquier n, o bien $p|n$ o bien p y n son primos entre sí.

El estudio de los números primos es un tema muy difícil en el que todavía quedan muchas cuestiones básicas sin resolver (más adelante daremos algunos ejemplos). De hecho, los únicos resultados que demostraremos en esta sección ya estaban enunciados y probados en la obra de Euclides *"Elementos"* hace unos 2.300 años.

Proposición 2.1 : *El conjunto de primos es infinito.*

Dem.: Dados p_1, p_2,..., p_m primos, veamos que existe un número primo distinto de ellos.

Sea $n = p_1 p_2 \dots p_m + 1$. Este número no es divisible por p_i porque

$$p_i | n \;\Rightarrow\; p_i | (n - p_1 p_2 \dots p_m) = 1.$$

Todo número (distinto de ± 1) tiene un divisor primo (ejercicio) y como n no es divisible por ningún p_i, existe un primo distinto de ellos. ■

A modo de curiosidad diremos que el primo más grande conocido hasta la fecha (Octubre de 1996) es $2^{1257787} - 1$.

El hecho de que los enteros se puedan descomponer en factores primos de forma esencialmente única es tan básico que se llama "Teorema fundamental de la aritmética" al siguiente teorema de factorización. Curiosamente, desde el punto de vista computacional, con los algoritmos disponibles actualmente es mucho más difícil descomponer en factores un número grande, que decidir si es primo o no. En ello se basan algunos sistemas criptográficos.

Teorema 2.2 (fundamental de la aritmética): *Todo número entero distinto de 0, 1 y −1, se puede descomponer como producto de factores primos, además esta descomposición es única salvo el orden de los factores y cambios de signo.*

El principal ingrediente para demostrar el teorema anterior es el siguiente resultado

Teorema 2.3 (de Euclides): *Si a y b son primos entre sí, $a|bc \Rightarrow a|c$.*

<u>DEM.</u>: Si a, b son primos entre sí, existen n, m tales que $an + bm = 1$ y por tanto $acn + bcm = c$, y como a divide al primer miembro de esta igualdad, también divide al segundo. ∎

Quizá la demostración anterior parezca demasiado complicada (aunque sea corta) para lo sencillo del resultado, pero debe observarse que no podemos usar nada acerca de la factorización en números primos ya que el teorema fundamental de la aritmética se deduce después de probar el de Euclides.

<u>DEM.(del teorema fundamental de la aritmética)</u>: Obsérvese en primer lugar que todo entero $n \neq 0, \pm 1$ se descompone en primos, ya que si n sólo tuviera divisores triviales (± 1 y $\pm n$) sería primo, y en otro caso se tendría un divisor no trivial, d, con lo cual se podría escribir como $n = d \cdot (n/d)$. Repitiendo el proceso con d y n/d se llega a escribir n como un producto de números que sólo tienen divisores triviales, es decir, primos.

Para probar que la descomposición es esencialmente única, supongamos que hay dos factorizaciones de n, entonces se tendría

$$p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s$$

con $p_1, \ldots, p_r, q_1, \ldots, q_s$ primos. Quizá cambiando el signo a algunos de estos primos, podemos suponer que todos son positivos. Si la descomposición no fuera única, tras simplificar los factores iguales en la igualdad anterior también podemos suponer que ninguno de los p_i aparece en el segundo miembro; lo cual contradiría a una aplicación repetida del Teorema de Euclides, ya que $p_1 | q_1 \cdot q_2 \cdot \ldots \cdot q_s$ (porque $p_1 | p_1 \cdot p_2 \cdot \ldots \cdot p_r$) pero $p_1 \nmid q_i$ para ningún $1 \leq i \leq s$. ∎

Concluimos esta sección con algunos comentarios que se salen fuera del contenido del curso, pero que quizá resulten interesante para alguien.

La sucesión de primos es bastante caótica y constituye un subconjunto bastante misterioso de los números enteros. De hecho, algunas conjeturas acerca de ellos siguen sin respuesta tras varios siglos. Por ejemplo, no se sabe si entre dos cuadrados existe siempre un número primo, aunque la opinión generalizada es que sí. También parece que todo entero par $n \geq 4$ se puede escribir como suma de dos primos (positivos), pero no se ha conseguido ninguna prueba de este hecho. Por otra parte, también ha habido avances en tantos siglos de investigación acerca de los primos, por ejemplo, hoy en día (en realidad desde hace un siglo) se sabe que la distribución de los primos no es del todo caótica, ya que si los ordenamos de forma creciente (consideramos sólo los positivos) $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, etc. entonces se cumple $\lim p_n/(n \log n) = 1$. Sin embargo la demostración de este hecho es muy difícil.

2.3. Congruencias, divisibilidad, pequeño teorema de Fermat

Dado un entero, m, mayor que uno, definimos la relación de equivalencia $\mathcal{R}_m$ en $\mathbb{Z}$

$$a\mathcal{R}_m b \;\Leftrightarrow\; m|a-b.$$

Definición: *Si $a\mathcal{R}_m b$, se dice que a y b son* congruentes módulo m *y se suele escribir $a \equiv b \ (m)$.*

Ejemplo . Se cumple

$$2 \equiv 7 \ (5), \qquad -13 \equiv 21 \ (17), \qquad 90 \equiv 126 \ (6).$$

Lema 3.1 : *Dos números son congruentes módulo m si y sólo si al efectuar la división entera por m dejan el mismo resto.*

Dem.: Supongamos

$$a = mq_1 + r_1 \qquad b = mq_2 + r_2.$$

Entonces

$$a \equiv b \ (m) \;\Rightarrow\; (a - mq_1) - (b - mq_2) \;\Rightarrow\; m|r_1 - r_2$$

y como $0 < r_1, r_2 < |m|$, esto último implica $r_1 = r_2$. ■

Del lema anterior se deduce que $\mathcal{R}_m$ divide a $\mathbb{Z}$ en m clases de equivalencia que corresponden a los m posibles valores del resto ($r = 0, 1, 2, \ldots, |m| - 1$).

La clase de un número, n, se indica con $\overline{n}$, $[n]$ o a veces simplemente con n si no da lugar a confusión.

Ejemplo . Si $m = 5$ las clases de equivalencia son

$$\begin{aligned}
\overline{0} &= \{0, 5, 10, 15, \ldots\} \cup \{-5, -10, -15, \ldots\} \\
\overline{1} &= \{1, 6, 11, 16, \ldots\} \cup \{-4, -9, -14, \ldots\} \\
\overline{2} &= \{2, 7, 12, 17, \ldots\} \cup \{-3, -8, -13, \ldots\} \\
\overline{3} &= \{3, 8, 13, 18, \ldots\} \cup \{-2, -7, -12, \ldots\} \\
\overline{4} &= \{4, 9, 14, 19, \ldots\} \cup \{-1, -6, -11, \ldots\}.
\end{aligned}$$

Obsérvese que como las clases de equivalencia son una partición, se tiene

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}.$$

Definición: *Se llama $\mathbb{Z}_m$ al conjunto cociente (conjunto de clases de equivalencia) de la relación de congruencia módulo m en $\mathbb{Z}$.*

Nota: Algunos autores usan la notación $\mathbb{Z}/m\mathbb{Z}$ ó $\mathbb{Z}/(m)$ en lugar de $\mathbb{Z}_m$. De esta forma se "ve" que es un conjunto cociente y además se evita la posible confusión con cierto conjunto bien distinto que se denota con $\mathbb{Z}_p$ en ciertas áreas avanzadas (los enteros p-ádicos). Sin embargo, aquí nos quedaremos con la notación más simple.

Ejemplo .

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Una de las cosas que hace interesante el estudio del conjunto $\mathbb{Z}_m$ es que se pueden definir dos operaciones en él que son parecidas a la suma y el producto habituales. Concretamente se tiene

Proposición 3.2 : *Si definimos en $\mathbb{Z}_m$ las operaciones*

$$\overline{a} + \overline{b} = \overline{a+b} \qquad y \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

entonces $(\mathbb{Z}, +, \cdot)$ es un anillo (conmutativo y unitario).

Observación: Nótese que a primera vista no está claro que estas operaciones estén bien definidas, ya que podemos elegir diferentes representantes de una misma clase. Por ejemplo, en $\mathbb{Z}_5$ se tiene $\overline{2} = \overline{7}$ y $\overline{4} = \overline{19}$, y

$$\overline{2} + \overline{4} = \overline{6} \qquad \overline{7} + \overline{19} = \overline{26}.$$

Como $\overline{6} = \overline{26}$, la elección de diferentes representantes de una misma clase de equivalencia no ha conllevado ningún problema en este ejemplo. No es difícil comprobar que esta es la situación general en $\mathbb{Z}_m$ porque dos representantes de una clase se diferencian siempre en un múltiplo de m. Prácticamente esta observación es lo único necesario en la prueba de la proposición anterior (que no daremos aquí).

Ejemplo . Las tablas de suma y multiplicación en $\mathbb{Z}_5$ son

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

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Obsérvese que en este anillo todos los elementos no nulos tienen inverso multiplicativo. Así por ejemplo, el inverso de $\overline{2}$ es $\overline{3}$, el de $\overline{4}$ es él mismo, etc. Por tanto $\mathbb{Z}_5$ es un cuerpo, de hecho se tiene el siguiente resultado general

Proposición 3.3 : $(\mathbb{Z}_m, +, \cdot)$ *es un cuerpo si y sólo si* m *es primo.*

Ejemplo . Las tablas de multiplicación en $\mathbb{Z}_3$ y $\mathbb{Z}_4$ son respectivamente

$$\begin{array}{c|ccc} \cdot & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{2} & \overline{1} \end{array} \qquad \begin{array}{c|cccc} \cdot & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{2} & \overline{0} & \overline{2} & \overline{0} & \overline{2} \\ \overline{3} & \overline{0} & \overline{3} & \overline{2} & \overline{1} \end{array}$$

Obsérvese que en $\mathbb{Z}_3$ (la tabla de la izquierda) los elementos no nulos, $\overline{1}$ y $\overline{2}$, tienen inverso multiplicativo (que casualmente coincide con ellos mismos), sin embargo en $\mathbb{Z}_4$ (tabla de la derecha), $\overline{2}$ no tiene inverso, es decir, $\overline{2} \cdot \overline{x} = \overline{1}$ no tiene solución. La razón última de esto es que 3 es primo y 4 no lo es.

DEM.: Si m no es primo, $m = ab$ con $0 < |a|, |b| < |m|$, por tanto $\overline{a}, \overline{b} \neq \overline{0}$ y $\overline{a} \cdot \overline{b} = \overline{m} = \overline{0}$. Pero entonces $\overline{b}$ no puede tener inverso multiplicativo porque

$$\overline{b} \cdot \overline{c} = \overline{1} \Rightarrow \overline{a} = \overline{a} \cdot \overline{b} \cdot \overline{c} = \overline{0}$$

y esto contradice nuestras hipótesis sobre a. Por tanto $\mathbb{Z}_m$ no es un cuerpo.

Por otra parte, si $m = p$ primo, entonces cualquier a con $1 \leq a < p$ cumple mcd $(a, p) = \pm 1$ y esto implica que existen enteros x e y tales que $ax + py = 1$. Una vez hallados estos enteros se tiene

$$\overline{ax + py} = \overline{1} \Rightarrow \overline{ax} + \overline{py} = \overline{1} \Rightarrow \overline{ax} = \overline{1}.$$

Por tanto la clase $\overline{a}$ tiene inverso (y es $\overline{x}$). ■

Ejemplo . Calcular el inverso multiplicativo de $\overline{7}$ en $\mathbb{Z}_{41}$.

Como en la demostración anterior, si hallamos x, y tales que $7x + 41y = 1$ se tiene que el inverso de $\overline{7}$ es $\overline{x}$, porque

$$7x + 41y = 1 \Rightarrow \overline{7x + 41y} = \overline{1} \Rightarrow \overline{7}\overline{x} + \overline{41y} = \overline{1} \Rightarrow \overline{7}\overline{x} = \overline{1}.$$

Por tanto basta resolver $7x + 41y = 1$, para ello usamos el algoritmo de Euclides

$$\left.\begin{aligned} 41 &= 7 \cdot 5 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 + 0. \end{aligned}\right\} \Rightarrow \begin{aligned} 1 =& 7 - 6 \cdot 1 \\ =& 7 - (41 - 7 \cdot 5) \cdot 1 = 7 - 41 + 7 \cdot 5 = 7 \cdot 6 + 41 \cdot (-1) \end{aligned}$$

Así pues, $x = 6$, $y = -1$ son posibles soluciones y $\overline{x} = \overline{6}$ es el inverso de $\overline{7}$ en $\mathbb{Z}_{41}$.

Una vez que sabemos que invertir $\overline{a}$ en $\mathbb{Z}_m$ equivale a resolver $ax + my = 1$, de los resultados de la primera sección se deduce

Proposición 3.4 : *La clase $\overline{a}$ tiene inverso multiplicativo en $\mathbb{Z}_m$ si y sólo si a y m son primos entre sí.*

Notación: Normalmente se designa con $\mathbb{Z}_m^*$ al conjunto formado por las clases de $\mathbb{Z}_m$ que tienen inverso multiplicativo.

Ejemplo .

$$\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}, \qquad \mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}, \qquad \mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

La solución de $ax + by = 1$ no sólo sirve para calcular inversos en $\mathbb{Z}_m$ sino también puede utilizarse para resolver sistemas de congruencias. Problemas de este tipo fueron estudiados por matemáticos chinos hace 2.000 años.

Ejemplo . Hallar x tal que $x \equiv 3\ (5)$ y $x \equiv 1\ (8)$.

$$\left.\begin{array}{l} x \equiv 3\ (5) \\ x \equiv 1\ (8) \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} x = 3 + 5k_1 \\ x = 1 + 8k_2 \end{array}\right\} \text{con } k_1, k_2 \in \mathbb{Z}.$$

Multiplicando la primera ecuación por 8 y la segunda por 5, se obtiene

$$\left.\begin{array}{l} 8x = 24 + 40k_1 \\ 5x = 5 + 40k_2 \end{array}\right\} \text{es decir} \left.\begin{array}{l} 8x \equiv 24\ (40) \\ 5x \equiv 5\ (40) \end{array}\right\}$$

Con esto hemos reducido al mismo módulo. Sean n y m tales que $8n+5m = 1$, por ejemplo $n = 2$ $m = -3$, multiplicando la primera ecuación por n y la segunda por m y sumando (para quitar los coeficientes) se obtiene

$$\big(8 \cdot 2 + 5 \cdot (-3)\big)x \equiv 24 \cdot 2 + 5 \cdot (-3)\ (40) \ \Rightarrow\ x \equiv 33\ (40).$$

Compruébese que $33 \equiv 3\ (5)$ y $33 \equiv 1\ (8)$.

Teorema 3.5 (chino del resto): *Si $m_1, m_2, \ldots, m_k$ son primos entre sí dos a dos, el sistema*

$$x \equiv a_1\ (m_1), \qquad x \equiv a_2\ (m_2), \qquad \ldots\ldots\ldots, \qquad x \equiv a_k\ (m_k)$$

tiene solución única módulo $m = m_1 m_2 \ldots m_k$.

<u>Dem.</u>: Procediendo como en el ejemplo anterior

$$\left.\begin{array}{l} x \equiv a_1\ (m_1) \\ x \equiv a_2\ (m_2) \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} x = a_1 + l_1 m_1 \\ x = a_2 + l_2 m_2 \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} m_2 x \equiv a_1 m_2\ (m_1 m_2) \\ m_1 x \equiv a_2 m_1\ (m_1 m_2) \end{array}\right\}$$

y como $\operatorname{mcd}(m_1, m_2) = 1$, siempre existen n_1 y n_2 tales que $m_1 n_1 + m_2 n_2 = 1$. Multiplicando la primera ecuación por n_2 y la segunda por n_1 y sumando los resultados, se obtiene

$$x \equiv a_1 m_2 n_2 + a_2 m_1 n_1 \ (m_1 m_2). \tag{3.1}$$

De hecho $a_1 m_2 n_2 + a_2 m_1 n_1$ resuelve las dos primeras ecuaciones porque $m_1 n_1 + m_2 n_2 = 1$ implica $m_2 n_2 \equiv 1 \ (m_1)$ y $m_1 n_1 \equiv 1 \ (m_2)$. Con esto hemos probado la existencia y unicidad (módulo $m_1 m_2$) de la solución de las dos primeras ecuaciones. A partir de (3.1) y la tercera ecuación se obtiene, de la misma forma, la única solución módulo $m_1 m_2 m_3$ de las tres primeras ecuaciones, y repitiendo el proceso se llega a una solución de todas. ■

Concluimos esta sección con tres sorprendentes teoremas que involucran congruencias. Por razones de simplicidad supondremos (sin mencionarlo cada vez) que los primos que aparecen en sus eneunciados y demostraciones son positivos.

Teorema 3.6 (pequeño teorema de Fermat): *Si $a \in \mathbb{Z}$ y p es primo*

$$a^p \equiv a \quad (p).$$

Ejemplo . Tomando $p = 5$ y $a = 2$ se tiene $32 \equiv 2 \ (5)$.

Aunque quisiéramos comprobar el teorema de Fermat para primos grandes, esto no requeriría calcular completamente la potencia a^p, por ejemplo, para hallar 3^{11} módulo 11 podríamos proceder de la siguiente manera

$$3^{11} \equiv (3^4)^2 3^3 \equiv 4 \cdot 4 \cdot 5 \equiv 5 \cdot 5 \equiv 3 \ (11)$$

donde hemos usado que $3^4 = 81 \equiv 4 \ (11)$ y $3^3 = 27 \equiv 5 \ (11)$.

Teorema 3.7 (Congruencia de Wilson): *Si p es primo entonces*

$$(p-1)! \equiv -1 \ (p).$$

Obsérvese que este teorema también podría formularse diciendo que un primo, p, siempre divide a $(p-1)! + 1$.

Ejemplo . Tomando $p = 7$ se tiene $6! = 720$ y $720 \equiv -1 \ (7)$.

Antes de enunciar el último resultado, que generaliza al pequeño teorema de Fermat, es necesario definir para $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ con p_i primos distintos y $\alpha \geq 1$, la función

$$\phi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1).$$

Ejemplo . $\phi(40) = \phi(2^3 \cdot 5) = 2^2(2-1) \cdot (5-1) = 16$, $\phi(243) = \phi(3^5) = 3^4(3-1) = 162$.

Nótese que si $m = p^\alpha$ con p primo y $\alpha \geq 1$, entonces $\phi(m)$ es el número de clases con inverso en $\mathbb{Z}_m$ ya que los $p^{\alpha-1}$ "múltiplos de p" $\overline{p}$, $\overline{2p}$, $\overline{3p}$, $\dots \overline{p^{\alpha-1}p}$ son las únicas clases sin inverso en $\mathbb{Z}_m$. En realidad siempre hay exactamente $\phi(m)$ clases con inverso en $\mathbb{Z}_m$, incluso si m no es potencia de un primo, pero no usaremos este hecho aquí.

Teorema 3.8 (Euler-Fermat): *Si a y m son primos entre sí, entonces*

$$a^{\phi(m)} \equiv 1 \ (m).$$

Ejemplo . Si $m = 12$ y $a = 5$, $\phi(12) = 2^1(2-1)(3-1) = 4$ y $5^4 \equiv 1\ (12)$.

Aunque el pequeño teorema de Fermat se reduce al de Euler-Fermat para módulo primo, preferimos dar, a modo ilustrativo, una demostración independiente.

DEM.(del pequeño teorema de Fermat): Como todo número es congruente a un número positivo, podemos suponer $a > 0$. Ahora demostramos el teorema por inducción:

i) Para $a = 1$ es cierto. Es obvio, porque $1^p \equiv 1\ (p)$.

ii) Si es cierto para a también es cierto para $a+1$. Nótense las siguientes implicaciones:

$$(a+1)^p \equiv (a+1)\ (p) \ \Leftrightarrow\ p|(a+1)^p - a - 1$$

$$\Leftrightarrow\ p|a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a - a.$$

Por la hipótesis de inducción p divide a $a^p - a$ y todos los coeficientes binomales anteriores son divisibles por p, así pues $p|a^p - a \Rightarrow p|(a+1)^p - (a+1)$. ■

DEM.(de la congruencia de Wilson): Nótese que $\overline{1}$ y $\overline{p-1}$ son sus propios inversos ($\overline{1} \cdot \overline{1} = \overline{p-1} \cdot \overline{p-1} = \overline{1}$) además son las únicas clases con esta propiedad porque la ecuación $x^2 - 1 \equiv 0\ (p)$ sólo tiene dos soluciones (ya que $p|x^2 - 1 = (x-1)(x+1) \Rightarrow p|x-1$ o $p|x+1$). Entonces

$$-(p-1)! = 1 \cdot (p-1)! \cdot (p-1) = 1 \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \cdot (p-1) \equiv 1\ (p)$$

porque en el producto anterior aparece un representante de cada clase y de su inverso. ■

DEM.(del teorema de Euler-Fermat): Por simplicidad escribiremos x en lugar de $a^{\phi(m)}$.

Supongamos primero que m es potencia de un primo, $m = p^\alpha$, entonces, como ya hemos mencionado, hay exactamente $\phi(m)$ clases, $\overline{n_1}, \overline{n_2}, \ldots, \overline{n_{\phi(m)}}$, con inverso en $\mathbb{Z}_m$. Al ser a y m primos entre sí, $\overline{a}$ tiene inverso y, por tanto, $\overline{a}\,\overline{n_1}, \overline{a}\,\overline{n_2}, \ldots, \overline{a}\,\overline{n_{\phi(m)}}$ son de nuevo clases con inverso. Además deben ser todas (quizá reordenadas) porque hay $\phi(m)$ de ellas. Así pues

$$\overline{a}\,\overline{n_1} \cdot \overline{a}\,\overline{n_2} \cdot \ldots \cdot \overline{a}\,\overline{n_{\phi(m)}} = \overline{n_1} \cdot \overline{n_2} \cdot \ldots \cdot \overline{n_{\phi(m)}}.$$

Multiplicando por los inversos de las clases $\overline{n_1}, \overline{n_2}, \ldots \overline{n_{\phi(m)}}$ se tiene $\overline{x} = \overline{1}$ en $\mathbb{Z}_m$, o lo que es lo mismo, $x \equiv 1\ (m)$.

Si m no es potencia de un solo primo, entonces m se descompone en factores primos como $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ con $\alpha_i \geq 1$ y $k \geq 2$. Nótese que $\phi(p_i^{\alpha_i})|\phi(m)$ (los p_i son distintos) y por tanto para cada i, x se escribe como $x = A_i^{\phi(p_i^{\alpha_i})}$. Como ya hemos probado el teorema para potencia de primos, se tiene

$$x \equiv 1\ (p_1^{\alpha_1}), \qquad x \equiv 1\ (p_2^{\alpha_2}), \qquad \ldots\ldots\ldots, x \equiv 1\ (p_k^{\alpha_k}).$$

Finalmente, obsérvese que este sistema se cumple sustituyendo x por 1, y como el teorema chino del resto asegura que la solución es única módulo m, se debe cumplir $x \equiv 1$ (m). ∎

Los tres teoremas anteriores permiten decidir la divisibilidad de algunos números de tamaño astronómico.

Ejemplo 1. $1996^{103} + 6991^{103} - 26$ es divisible por 103.

Como 103 es primo (compruébese), se tiene

$$1996^{103} + 6991^{103} - 26 \equiv 1996 + 6991 - 26 \equiv 8961 \equiv 0 \quad (103)$$

donde la última congruencia se cumple porque $103|8961$.

Ejemplo 2. $(70!)^2 - 1$ es divisible por 71.

Usando la congruencia de Wilson

$$(70!)^2 - 1 = (70! + 1)(70! - 1) \equiv (70! - 1)(-1 + 1) \equiv 0 \quad (71).$$

Ejemplo 3. $10^{600} - 1$ es divisible por 93.

Como $\phi(93) = \phi(3 \cdot 31) = 2 \cdot 30 = 60$, por el teorema de Euler-Fermat se tiene

$$10^{600} - 1 = (10^{10})^{60} - 1 \equiv 1 - 1 \equiv 0 \ (93).$$

Nota: Como curiosidad diremos que el número del primer ejemplo tiene 396 cifras, el del segundo 201 y el del tercero 600.

1) ¿Cuál es el mcd y el mcm de dos números consecutivos?

2) Hallar todas las soluciones enteras de $7x + 10y = 1$.

3) Justificar por qué $35x + 21y = 3$ no tiene solución.

4) Hallar las soluciones enteras de $11x - 13y = 1$ que tienen $|x|, |y| < 13$.

5) Dos números naturales son múltiplos de 12 y 15 respectivamente y su suma es 81. Hallarlos.

6) Si $\operatorname{mcd}(a, b) = 1$, ¿qué valores puede tomar $\operatorname{mcd}(a + b, a - b)$?

7) Sabiendo que $d = \operatorname{mcd}(a, b)$, ¿cuánto vale $\operatorname{mcm}(a^2, b^2)$?.

8) Si Venus, la Tierra y Marte tardan 225, 365 y 687 días respectivamente en dar la vuelta alrededor del Sol ¿cada cuánto tiempo están en la misma posición que hoy?

9) Considérese la sucesión de números de Fibonacci 1,1,2,3,5,8,13,21...definidos por $a_1 = a_2 = 1$ y $a_{n+2} = a_{n+1} + a_n$. ¿Cuántos pasos requiere el algoritmo de Euclides para hallar $\operatorname{mcd}(a_{n+1}, a_{n+2})$? *Sugerencia*: Comprobarlo con algunos ejemplos.

<u>Nota</u>: Estos números son para los que el algoritmo de Euclides es más lento. Si $n > 1$, a_{n+5} tiene una cifra más que a_n, con ello se puede demostrar que el número de pasos necesario para hallar el mcd de dos enteros positivos con el algoritmo de Euclides no excede a cinco veces el número de cifras del menor de ellos.

10) El laboratorio se ha gastado 8.390.000 ptas en ordenadores IBM y HP. si los ordenadores IBM cuestan a 250.000 ptas cada uno y los HP a 180.000 ptas. ¿Cuántos se han comprado de cada marca?

11) Un dólar canadiense son 101 ptas y un dólar americano son 123 ptas. Si al cambiar los dos tipos de monedas me han dado en total 6.215 ptas. ¿Cuántos dólares de cada tipo he cambiado?

12) En Madrid tocan los A y simultáneamente en las afueras los B. Una pandilla de amigos se divide entre los dos conciertos. La entrada para A cuesta 5.300 ptas y para B, 2.500 ptas, si se han gastado en total 64.600 ptas, ¿cuántos amigos formaban la pandilla?

13) Hallar todas las soluciones enteras de $17x + 13y = -1$.

14) Decimos que un punto de coordenadas enteras $(x, y) \in \mathbb{Z}^2$ es visible desde el origen si el segmento que une dicho punto con el origen no pasa por ningún otro punto. ¿Cuánto vale $\operatorname{mcd}(x, y)$ si (x, y) es un punto visible? ¿Cuántos puntos impiden "ver" el punto $(42, 45)$?

15) Calcular <u>a mano</u> $\operatorname{mcd}(675683, 674041)$ y obsérvese que factorizar cualquiera de estos números podría llevar mucho tiempo.

Opcional: Escribe un programa en tu lenguaje de programación favorito que calcule el mcd y el mcm usando el algoritmo de Euclides y otro que los calcule descomponiendo en factores primos. Tras algunas pruebas, borrar el segundo.

16) Hallar una solución entera de $15x + 10y + 6z = 1$. En general, demostrar que si $\operatorname{mcd}(a, b, c) = 1$ entonces existen $x, y, z \in \mathbb{Z}$ tales que $ax + by + cz = 1$.

***17)** hallar dos enteros positivos cuya suma sea 798 y su mcm sea 10780.

Hoja 6

En toda esta hoja consideraremos los primos con signo positivo.

1) Descomponer $19! = 19 \cdot 18 \cdot \ldots \cdot 2 \cdot 1$ en factores primos. Calcular la potencia de 11 que aparece en la descomposición en factores primos de 190!

2) Demostrar que hay intervalos de la forma $(n+1, n+100]$ que no contienen ningún primo. *Indicación*: Considérese $100! = 100 \cdot 99 \cdot \ldots \cdot 1$.

3) Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$ es la descomposición en factores primos de n, calcular el número de divisores positivos de n.

4) En la demostración del pequeño teorema de Fermat se usa que si m es primo entonces los números combinatorios

$$\binom{m}{1}, \quad \binom{m}{2}, \quad \binom{m}{3}, \quad , \ldots \binom{m}{m-1}$$

son divisibles por m. Demostrarlo. ¿Es cierto si m no es primo?

5) Comprobar que $2^{1002} - 1$ no es primo.

6) Si n es un número natural, demostrar que n, $n + 10$ y $n + 32$ no pueden ser simultáneamente primos. *Indicación*: Demostrar que 3 divide a uno de ellos.

7) Si p es primo, ¿cuántos enteros positivos menores que p^m cumplen $\operatorname{mcd}(n, p^m) = 1$?

8) Comprobar que el número $1999\,1999\,1999 \overset{1999 \text{ veces}}{\cdots\cdots} 1999$ no es primo.

9) Demostrar que $13 < n < 169$ es primo si y sólo si n y 30030 son primos entre sí.

10) Sea el conjunto $\mathcal{H} = \{1, 5, 9, 13, 17, 21, \ldots\}$. Decimos que $p \in \mathcal{H}$ es un $\mathcal{H}$-primo si $p \neq 1$ y no es divisible por ningún elemento de $\mathcal{H}$ salvo por sí mismo y por uno. Por ejemplo, 5 y 9 son $\mathcal{H}$-primos, pero $25 = 5 \cdot 5$ no. Comprobar que 693 tiene varias posibles descomposiciones en factores $\mathcal{H}$-primos.

<u>Nota</u>: Hilbert (1862-1943) propuso $\mathcal{H}$ como un conjunto sencillo en el que no se cumple el análogo del teorema fundamental de la aritmética. Hay ejemplos más complicados (y de mayor interés) en los que el conjunto tiene estructura de anillo.

***11)** Demostrar que si n es un entero positivo mayor que uno $n^4 + 4$ no es primo.

***12)** Comprobar que $2^{1997^2} - 1$ no es primo.

<u>Nota</u>: En general, se puede demostrar que si n no es primo, entonces $2^n - 1$ tampoco lo es.

****13)** Euler (1707-1783) demostró que $\sum 1/n^2 = \pi^2/6$ donde n recorre los enteros positivos. Sabiendo esto, hallar la probabilidad de que dos enteros positivos elegidos al azar sean primos entre sí. *Indicación*: Comenzar demostrando que $6/\pi^2 = \prod(1 - 1/p^2)$ donde p recorre los primos.

Hoja 7

1) Sabiendo que $1/7 = 0'142857\,142857\,142857\,142857\ldots$ Calcular la cifra decimal que ocupa el lugar 1000.

2) Efectuar la siguiente operación en $\mathbb{Z}_{203}$

$$\overline{3} + \overline{5} \cdot \frac{\overline{4}}{\overline{13} + \overline{4}}$$

3) Calcular el resto que se obtiene al dividir 4^{111} por 103.

4) Si m es producto de dos primos distintos, ¿cuántos elementos no se pueden invertir en $\mathbb{Z}_m$?

5) ¿Qué hora marca un reloj 777 horas después de que sean las once?

6) Demostrar que $2^{341} \equiv 2\ (341)$ pero $341 = 11 \cdot 31$ no es primo.

Nota: No son muy frecuentes los números que no siendo primos verifiquen el pequeño teorema de Fermat.

7) Demostrar que si n es entero, $(n+6)(n+13)(n-4)/6$ también lo es.

8) ¿Con qué es congruente $(m-1)!$ módulo m si m es impar y no es primo?

9) Calcular x tal que $x \equiv 1\ (11)$ y $x \equiv 9\ (13)$.

10) Demostrar que si n es un entero $n^3 + 11n$ es divisible por 6.

11) Demostrar que no existe ningún entero, x, tal que $x \equiv 3\ (15)$ y $x \equiv 5\ (12)$.

12) Hallar el inverso de $\overline{7}$ en $\mathbb{Z}_{15}$ y utilizarlo para resolver $7x \equiv 2\ (15)$.

13) La función `RND` del ZX Spectrum utiliza(ba) los términos de la sucesión definida por $x_n \equiv 75^n\ (65537)$ con $0 < x_n \le 65536$ para generar números aleatorios, mostrando el valor $(x_n - 1)/65536$ para normalizar el resultado entre 0 y 1. Si `RND` produce cierta vez 0.01524353... = 999/65536 ¿qué número producirá la siguiente vez que accedamos a ella?

14) Fermat (1601-1665) afirmó que los números $2^{2^0}+1$, $2^{2^1}+1$, $2^{2^2}+1$, $2^{2^3}+1, \ldots$ son todos primos. Demostrar que $2^{2^5} \equiv -1\ (641)$ y concluir que Fermat era un mentiroso.

Nota: En 1990 se consiguió factorizar $2^{512}+1 = 2^{2^9}+1$, que tiene 155 cifras, y para ello se necesitaron métodos teóricos muy avanzados (álgebra en anillos "extraños"), setecientas "workstations", un supercomputador y cuatro meses.

15) Se puede demostrar (pero es no es fácil) que si p es primo, existe un elemento en $\mathbb{Z}_p$ tal que él y sus potencias da todos los elementos de $\mathbb{Z}_p$ excepto $\overline{0}$. Calcular un elemento con esas características en $\mathbb{Z}_5$, $\mathbb{Z}_7$ y $\mathbb{Z}_{17}$.

*__16)__ Demostrar que si k y n son impares, n divide a $1^k + 2^k + \ldots + n^k$.

*__17)__ Demostrar que no hay ningún triángulo rectángulo de lados enteros cuya hipotenusa sea 111^{111}.

Miscelánea.

El estudio de los enteros constituye una de las ramas más antiguas de las Matemáticas. Clásicamente se llamó a esta disciplina "Aritmética", pero desde el siglo pasado el nombre oficial parece ser "Teoría de Números". Ya los griegos hace más de dos mil años se maravillaron con las propiedades de los enteros. Algunos de los problemas a que dieron lugar sus investigaciones siguen sin resolverse hoy en día. Por ejemplo, 6 es la suma de todos sus divisores (positivos) excepto él mismo

$$6 = 1 + 2 + 3.$$

También 28 tiene la misma propiedad

$$28 = 1 + 2 + 4 + 7 + 14.$$

Se dice que los números con estas características son números perfectos. Euclides (aprox. 365-275 a. d. C.) encontró una "fórmula" para todos los números perfectos que son pares, sin embargo todavía se desconoce si existe algún número perfecto impar.

Hay otros problemas acerca de los números enteros que se han resuelto pero la dificultad de su solución no concuerda en absoluto con la sencillez de su enunciado. El más famoso en nuestros días (por la reciente solución debida a A. Wiles en 1995) es el llamado "Último teorema de Fermat" propuesto hace unos 350 años por P. de Fermat (1601-1665) y que consiste en demostrar que si $n > 2$, no existen números $a, b, c \in \mathbb{Z}^+$ tales que

$$a^n + b^n = c^n.$$

Fermat afirmó que lo había resuelto, pero la opinión generalizada es que se equivocó. Una razón de peso para pensar así es que matemáticos posteriores de mucha más altura que Fermat, incluyendo al *princeps mathematicorum* C.F. Gauss (1777-1855), no lo consiguieron resolver y la solución actual involucra nuevas ramas de las Matemáticas impensables en el siglo XVII.

> A vezes non fazemos todo lo que dezimos,
> e quanto prometemos, quizá non lo conplimos:
> al mandar somos largos e al dar escasos primos;
> por vanas promisiones trabajamos e servimos.
> *LBA, 816*

La misma situación se muestra en un resultado mucho más asequible que Fermat sí demostró y que afirma que si para todo primo, p, mayor que 2 se cumple

$$p \textit{ es suma de dos cuadrados} \Leftrightarrow p - 1 \textit{ es divisible por } 4.$$

Por ejemplo, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, pero $7 \neq a^2 + b^2$. A pesar de que el resultado cae dentro de la teoría de números elemental, requiere grandes dosis de ingenio encontrar una demostración (en la miscelánea del próximo capítulo daremos una usando polinomios). Si el lector lo consigue, es casi seguro que el libro en el que ha encontrado la solución no contiene el siguiente resultado menos conocido (y más difícil) que cumplen los primos mayores que 5:

$$p \textit{ es suma de un cuadrado y cinco veces otro cuadrado} \Leftrightarrow p - 1 \textit{ ó } p - 9 \textit{ es divisible por } 20.$$

Por ejemplo, $61 = 4^2 + 5 \cdot 3^2$, $29 = 3^2 + 5 \cdot 2^2$, pero $13 \neq a^2 + 5b^2$. L. Euler (1707-1783) conjeturó que el resultado era cierto pero fue incapaz de probarlo, aunque esta vez sí que Gauss cumplió con su merecida fama. Un lector que sea capaz de dar una demostración por su cuenta seguramente tiene un gran futuro como investigador en Matemáticas.

En comparación con $a^2+b^2 = p$, la ecuación $a^2-b^2 = p$ es muy sencilla porque $(a-b)(a+b) = p$ implica (salvo signos) $a - b = 1$ y $a + b = p$ o viceversa, de aquí se deduce que $a = (p + 1)/2$, $b = (p - 1)/2$ es siempre una solución (entera si $p \neq 2$) de $a^2 - b^2 = p$; por tanto

$$p \textit{ es resta de dos cuadrados} \Leftrightarrow p \neq 2.$$

La diferencia entre estos dos ejemplos se basa en que $a^2 + b^2$ no se puede factorizar y $a^2 - b^2$ sí, lo que sugiere crear anillos que extiendan al de los números enteros y en los que se pueda llevar a acabo la factorización de la ecuación dada, por ejemplo

$$a^2 + b^2 = (a + bi)(a - bi) \text{ en } \mathbb{Z}[i], \quad \text{donde } \mathbb{Z}[i] = \{n + mi \,/\, n, m \in \mathbb{Z}\}$$
$$a^2 + 5b^2 = (a + bi\sqrt{5})(a - bi\sqrt{5}) \text{ en } \mathbb{Z}[i\sqrt{5}], \quad \text{donde } \mathbb{Z}[i\sqrt{5}] = \{n + mi\sqrt{5} \,/\, n, m \in \mathbb{Z}\}$$

Es posible definir máximo común divisor, números primos, etc. en $\mathbb{Z}[i]$ y se puede probar (pero no es fácil) que

$$\{\text{primos de } \mathbb{Z}[i]\} \cap \mathbb{Z} = \{\pm p \,/\, p \text{ primo en } \mathbb{Z}^+,\ 4|p - 3\}.$$

Esto implica que $a^2+b^2 = p$ no puede tener solución para $4|p-3$, porque si la tuviera, $(a+bi)(a-bi) = p$ y, por tanto, p no sería primo en $\mathbb{Z}[i]$. Recíprocamente, si $4 \not| p - 3$, entonces como p no es primo en $\mathbb{Z}[i]$, se puede factorizar como $p = (a + bi)(a - bi) = a^2 + b^2$. Con esto se demuestra el resultado de Fermat suponiendo conocida la teoría de primos en $\mathbb{Z}[i]$.

El anillo $\mathbb{Z}[i\sqrt{5}]$ es mucho más difícil de estudiar ya que en él no se puede definir el máximo común divisor ni se cumple la unicidad en el teorema de factorización, por ejemplo, $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ son primos distintos en $\mathbb{Z}[i\sqrt{5}]$ pero

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

E. Kummer (1810-1893) creó la teoría de ideales para explicar esta situación en ciertos anillos que contienen a $\zeta = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\frac{2\pi}{n}$ y que aparecen en el Último teorema de Fermat (con n impar) tras la factorización

$$a^n + b^n = (a + b)(a + b\zeta)(a + b\zeta^2) \cdot \ldots \cdot (a + b\zeta^{n-1}).$$

La "factorización en ideales primos" sí que es única, pero estos ideales pueden tener una estructura complicada, por ejemplo, $I = \{2n + m + im\sqrt{5} \,/\, n, m \in \mathbb{Z}\}$ es un ideal primo en $\mathbb{Z}[i\sqrt{5}]$.

Con todo lo dicho anteriormente no es de extrañar que el álgebra sea una herramienta fundamental en la teoría de números; por otra parte, sobre todo tras un famoso trabajo de B. Riemann (1826-1866), las técnicas analíticas también han adquirido gran relevancia. Para ilustrar el tema, citaremos la siguiente fórmula debida a Euler (p recorre los primos positivos)

$$\sum_{n=1}^{\infty} \frac{1}{n^x} = \prod_p \frac{1}{1 - p^{-x}}$$

cuya demostración se reduce a escribir $1/(1 - p^{-x}) = 1 + p^{-x} + p^{-2x} + p^{-3x} + \ldots$ y usar que todo número factoriza en primos. Tomando $x = 1$ el primer miembro es ∞ (véase un libro de análisis) de donde se deduce que hay infinitos primos y que además no pueden crecen muy rápido porque si no el segundo miembro sería finito. Un análisis muy detallado de la función del primer miembro (hay libros enteros estudiando sus propiedades) permite deducir resultados precisos acerca de la distribución de los primos. Es increíble que de una fórmula tan simple se pueda obtener tanta información.

> A vezes pequeña fabla bien dicha e chico ruego
> obra mucho en los fechos, a vezes recabda luego;
> de chica çentella nasçe grand llama e grant fuego,
> e vienen grandes peleas a vezes de chico juego.
> *LBA, 734*

Una vez que ya hemos mencionado la antigüedad, dificultad e interrelación con otras partes de las Matemáticas de la teoría de números; queremos concluir esta sección citando la famosa frase de Gauss:

"Las Matemáticas son la reina de las ciencias y la teoría de números es la reina de las Matemáticas". Para acreditar esta opinión (que pocos compartirían en la actualidad) se puede decir que Gauss abrió una nueva era en la teoría de números, fue un matemático de primera línea y su contribución es muy importante en otras áreas de la ciencia.

Si lo dexiés de mío, sería de culpar;
dízelo grand filósofo, non só yo de rebtar:
de lo que dize el sabio non devemos dubdar,
ca por obra se prueva el sabio e su fablar.
LBA, 72

3. Anillos de Polinomios

3.1. Máximo común divisor, mínimo común múltiplo, algoritmo de Euclides

Un definición rigurosa de polinomio requeriría un lenguaje un poco técnico que omitiremos aquí ya que el concepto de intuitivo de polinomio es bien conocido. Para nuestros propósitos la siguiente "definición" será suficiente

Definición: *Un polinomio es una expresión de la forma*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

donde los coeficientes a_i pertenecen a un cuerpo K.

Al conjunto de todos los polinomios con coeficientes en K se le suele denotar $K[x]$. Aunque los resultados de este capítulo son generales, nuestra atención estará centrada principalmente en los casos $K = \mathbb{R}$ y $K = \mathbb{C}$.

Definición: *Sea $P \in K[x] - \{0\}$, $P = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Si $a_n \neq 0$ se dice que P tiene grado n y se escribe* $\operatorname{gr} P = n$.

Nota: La definición anterior no se aplica al polinomio cero (que tiene todos los coeficientes nulos). Algunos autores definen $\operatorname{gr} 0 = -\infty$ lo cual es útil en muchas ocasiones (por ejemplo en el Lema 1.2 o la Proposición 1.3), pero nosotros dejaremos el grado de este polinomio sin definir.

En $K[x]$ existen dos operaciones naturales que son la suma y producto de polinomios, como son suficientemente conocidas no repetiremos su definición aquí. Partiendo de las propiedades del cuerpo K no es difícil comprobar el siguiente resultado

Proposición 1.1 : *$(K[x], +, \times)$ es un anillo.*

El grado se comporta de la siguiente forma con respecto a la suma y producto

Lema 1.2 : *Si $P, Q \in K[x]$*

1) $\operatorname{gr}(P+Q) \le \max(\operatorname{gr} P, \operatorname{gr} Q)$ 2) $\operatorname{gr}(PQ) = \operatorname{gr} P + \operatorname{gr} Q$,

donde suponemos $P, Q, P+Q, PQ$ no nulos.

Ejemplo . $P = x^3+1$, $Q = -x^3+x^2+1 \Rightarrow P+Q = x^2+2$ y $PQ = -x^6+x^5+x^2+1$. Por tanto $\operatorname{gr} P = 3$, $\operatorname{gr} Q = 3$, $\operatorname{gr}(P+Q) = 2$ y $\operatorname{gr}(PQ) = 6$.

En el anillo $K[x]$ se cumple el análogo de la Proposición 1.1 del capítulo anterior. En el lenguaje del álgebra se dice que es un "dominio euclídeo". Esto hace que las propiedades de los enteros y de los polinomios sean parecidas lo cual permite una interrelación interesante entre el álgebra en $K[x]$ y en $\mathbb{Z}$. A modo de curiosidad diremos que los anillos de "congruencias con polinomios" (el análogo de los $\mathbb{Z}_n$) permiten deducir algunos resultados acerca de números enteros, números primos, etc.

En toda esta sección, y en parte de las otras, omitiremos las demostraciones porque son similares a las del capítulo anterior.

Proposición 1.3 : *Dados $P, Q \in K[x]$, $Q \neq 0$, existen dos polinomios, C y R, determinados únicamente, tales que*

$$P = Q \cdot C + R \qquad \textit{con } \operatorname{gr} R < \operatorname{gr} Q \; \textit{ ó } \; R = 0.$$

Como en el caso de los enteros, C y R se llaman cociente y resto respectivamente.

Para definir máximo común divisor y mínimo común múltiplo podemos usar las definiciones del capítulo anterior cambiando enteros por polinomios

Definición: *Decimos que $D \in K[x]$ es un* <u>máximo común divisor</u> *de $P, Q \in K[x]$ no simultáneamente nulos, si*

1) $D|P,\ D|Q$ (es divisor común) 2) $D'|P,\ D'|Q \;\Rightarrow\; D'|D$ (es "máximo").

Definición: *Decimos que M es un* <u>mínimo común multiplo</u> *de $P, Q \in K[x] - \{0\}$, si*

1) $P|M,\ Q|M$ (es múltiplo común) 2) $P|M',\ Q|M' \;\Rightarrow\; M|M'$ (es "mínimo").

La notación habitual es escribir $D = \operatorname{mcd}(P, Q)$ y $M = \operatorname{mcm}(P, Q)$. Obsérvese que, de nuevo, D y M no son únicos. En este caso no es sólo cuestión de un signo sino que

$$D \ (\textit{ó } M) \textit{ es un } \operatorname{mcd} \ (\textit{o un } \operatorname{mcm}) \Rightarrow kD \ (\textit{ó } kM) \textit{ también lo es para todo } k \in K - \{0\}$$

De nuevo, el <u>algoritmo de Euclides</u> es simplemente la aplicación iterada del siguiente resultado

Lema 1.4 : *Si R es el resto obtenido al dividir P entre Q, entonces* $\operatorname{mcd}(P, Q) = \operatorname{mcd}(Q, R)$.

<u>Ejemplo</u> . Calcular $\operatorname{mcd}(x^4 + x^3 - 5x^2 + 4x + 3, x^3 - 6x + 9)$ con el algoritmo de Euclides.

$$\begin{aligned} x^4 + x^3 - 5x^2 + 4x + 3 =& (x^3 - 6x + 9)(x + 1) + x^2 + x - 6 \\ x^3 - 6x + 9 =& (x^2 + x - 6)(x - 1) + x + 3 \\ x^2 + x - 6 =& (x + 3)(x - 2) \end{aligned}$$

Por tanto $\operatorname{mcd}(x^4 + x^3 - 5x^2 + 4x + 3, x^3 - 6x + 9) = x + 3$.

Como en $\mathbb{Z}$, el máximo común divisor y el mínimo común múltiplo están ligados por la siguiente fórmula

Lema 1.5 : *Si* $P, Q \in K[x] - \{0\}$

$$\text{mcm}\,(P, Q) = \frac{PQ}{\text{mcd}\,(P, Q)}.$$

Observación: Por la ambigüedad en la definición del mcd y el mcm, nótese que podríamos escribir un factor $k \in K - \{0\}$ en cualquiera de los miembros de la igualdad.

También en este contexto se puede hablar de máximo común divisor y mínimo común múltiplo de varios polinomios gracias a las fórmulas

$$\begin{aligned}
\text{mcd}\,(P_1, P_2, \ldots, P_n) =& \text{mcd}\,\big(\text{mcd}\,(P_1, P_2, \ldots, P_{n-1}), P_n\big)\\
\text{mcm}\,(P_1, P_2, \ldots, P_n) =& \text{mcm}\,\big(\text{mcm}\,(P_1, P_2, \ldots, P_{n-1}), P_n\big).
\end{aligned}$$

Ejemplo . Calcular $\text{mcd}\,(x^4 + x^3 - 5x^2 + 4x + 3, x^3 - 6x + 9, x + 3)$.

Según las fórmulas anteriores y los cálculos del último ejemplo

$$\begin{aligned}
D =& \text{mcd}\,(x^4 + x^3 - 5x^2 + 4x + 3, x^3 - 6x + 9, x + 3)\\
=& \text{mcd}\,(x + 3, x + 3)\\
=& x + 3
\end{aligned}$$

Como en $K[x]$ se tiene el algoritmo de Euclides también se puede demostrar el análogo de la identidad de Bezout.

Proposición 1.6 : *Si* $P, Q \in K[x] - \{0\}$ *y* D *es su máximo común divisor, entonces existen* $A, B \in K[x]$ *tales que*

$$D = AP + BQ.$$

Ejemplo . Hallar el máximo común divisor de $P = x^5 + 4x^4 + 6x^3 + 4x^2 - x - 3$ y $Q = x^4 + 2x^3 + x^2 - 1$, y escribirlo en la forma $AP + BQ$.

Por el algoritmo de Euclides

$$\begin{aligned}
x^5 + 4x^4 + 6x^3 + 4x^2 - x - 3 =& (x^4 + 2x^3 + x^2 - 1)(x + 2) + x^3 + 2x^2 - 1\\
x^4 + 2x^3 + x^2 - 1 =& (x^3 + 2x^2 - 1)x + x^2 + x - 1\\
x^3 + 2x^2 - 1 =& (x^2 + x - 1)(x + 1) + 0
\end{aligned}.$$

Por tanto el máximo común divisor es $D = x^2 + x - 1$.

$$\begin{aligned}(2^{\underline{a}}\ \text{ecuación}) \ &\Rightarrow\ D = Q - (x^3 + 2x^2 - 1)x\\ (1^{\underline{a}}\ \text{ecuación}) \ &\Rightarrow\ D = Q - \big(P - Q(x+2)\big)x\end{aligned}$$

y operando en esta última expresión, se tiene

$$D = (-x)P + (x^2 + 2x + 1)Q.$$

Nota: No entraremos en la solución general de la ecuación $AX + BY = C$ en $K[x]$ pero formalmente se tiene un resultado análogo al que vimos en la primera sección del capítulo anterior.

En $K[x]$ también es posible definir ideales y dar con ellos definiciones alternativas de máximo común divisor y mínimo común múltiplo.

DEFINICIÓN: *Un ideal, I en $K[x]$ es un subconjunto de $K[x]$ tal que*

$$1)\ P, Q \in I \Rightarrow P + Q \in I \qquad 2)\ P \in I,\ R \in K[x] \Rightarrow PR \in I.$$

Proposición 1.7 : *En $K[x]$ cada ideal está formado por los múltiplos de cierto polinomio, P.*

Normalmente se escribe $I = (P)$ y se dice que P es un generador de I.

DEFINICIÓN: (alternativa) Un mínimo común múltiplo de $P_1, P_2, \dots, P_n$ es un generador de $(P_1) \cap (P_2) \cap \dots \cap (P_n)$.

DEFINICIÓN: (alternativa) Un máximo común divisor de $P_1, P_2, \dots, P_n$ es un generador del menor ideal que contiene a $\{P_1, P_2, \dots, P_n\}$.

Observación: La definición alternativa y la última proposición demuestran que el mcd y el mcm siempre existen (lo cual no es evidente partiendo de la primera definición).

3.2. POLINOMIOS IRREDUCIBLES, TEOREMA DE FACTORIZACIÓN

DEFINICIÓN: *Se dice que un polinomio $P \in K[x] - \{0\}$ con $\operatorname{gr} P \geq 1$ es irreducible, si no puede escribirse como $P = QR$ con $Q, R \in K[x]$ tales que $\operatorname{gr} Q, \operatorname{gr} R < \operatorname{gr} P$.*

Nota: A veces a los polinomios irreducibles se les llama polinomios primos, aunque esta notación no es muy habitual. Obsérvese que la definición anterior es equivalente a decir que P sólo es divisible por k y por kP con $k \in K - \{0\}$.

Ejemplo . $P = x^2 + 1$ es irreducible en $\mathbb{R}[x]$, pero no lo es en en $\mathbb{C}[x]$ porque $P = (x - i)(x + i)$.

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

Los polinomios de grado 1 son siempre irreducibles en $K[x]$.

DEFINICIÓN: *Se dice que dos polinomios están* asociados *si son iguales salvo multiplicar por un factor de* $K-\{0\}$

Ejemplo . x^2+7x+3 está asociado con $3x^2+21x+9$ y con $\frac{1}{3}x^2+\frac{7}{3}x+1$.

DEFINICIÓN: *Se dice que* $P,Q\in K[x]$ *son* primos entre sí *cuando* $\operatorname{mcd}(P,Q)=1$.

Observación: Nótese que también podríamos haber escrito en la definición $\operatorname{mcd}(P,Q)=k$ con $k\in K-\{0\}$

El siguiente resultado es más notorio que en el caso de $\mathbb{Z}$ ya que hay algunos cuerpos que son finitos (por ejemplo los $\mathbb{Z}_p$ del capítulo anterior).

Proposición 2.1 : *En* $K[x]$ *hay infinitos polinomios irreducibles no asociados.*

Teorema 2.2 (de factorización)**:** *Todo polinomio no constante se puede descomponer como producto de polinomios ireducibles, además esta descomposición es única salvo el orden y factores asociados.*

De nuevo el principal ingrediente de la prueba es

Teorema 2.3 (de Euclides): *Si* P *y* Q *son primos entre sí,* $P|QR\Rightarrow P|R$.

No daremos aquí las demostraciones de los tres resultados anteriores porque son totalmente similares a sus análogos en $\mathbb{Z}$.

En $\mathbb{C}[x]$ y en $\mathbb{R}[x]$ la cuestión de irreducibilidad de un polinomio es muy sencilla gracias al siguiente importante resultado

Teorema 2.4 (Teorema fundamental del álgebra): $P\in\mathbb{C}[x]$ *es irreducible* $\Leftrightarrow$ $\operatorname{gr}P=1$. *Equivalentemente, todo polinomio no constante de* $\mathbb{C}[x]$ *se puede descomponer en factores lineales.*

Observación: Del teorema anterior se puede deducir que todo polinomio irreducible en $\mathbb{R}[x]$ es de grado uno o dos. Volveremos sobre esto en la próxima sección, pero la idea es que $\mathbb{C}$ es lo mismo que $\mathbb{R}$ salvo añadir la solución de la ecuación de segundo grado x^2+1.

Ejemplo . $P=x^3+2x^2+2x+1$ factoriza en $\mathbb{C}[x]$ como

$$P=(x+1)(x+\frac{1}{2}+i\frac{\sqrt{3}}{2})(x+\frac{1}{2}-i\frac{\sqrt{3}}{2}).$$

Comprobar esta factorización se reduce a un cálculo, pero deducirla requiere los resultados de la sección siguiente.

Si $K \neq \mathbb{C}, \mathbb{R}$, en general es muy complicado saber si $P \in K[x]$ es irreducible. Por ejemplo, como veremos a continuación, descomponer un polinomio en $\mathbb{Q}[x]$ se reduce a descomponer un polinomio con coeficientes enteros, pero esto da lugar a una descomposición en dos factores del término independiente, así que en algún sentido descomponer un polinomio en $\mathbb{Q}[x]$ es al menos tan difícil como descomponer un número entero, lo cual no es absoluto sencillo si el tamaño de éste es grande. Incluso cuando los coeficientes son pequeños, puede llevar bastante tiempo factorizar un polinomio si su grado es moderadamente alto.

Si llamamos $\mathbb{Z}[x]$ al anillo de polinomios con coeficientes enteros, el siguiente lema asegura que en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ el concepto de irreducibilidad es el mismo.

Lema 2.5 (Lema de Gauss)**:** *Si $P \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ también lo es en $\mathbb{Q}[x]$.*

<u>DEM.</u>: Si $P = P_1P_2$ con $P_1, P_2 \in \mathbb{Q}[x]$ multiplicando por cierto número natural, n, que cancele todos los denominadores tenemos que

(2.1) $nP = (b_l x^l + b_{l-1}x^{l-1} + \ldots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0) \qquad \text{con } b_i, c_i \in \mathbb{Z}.$

Supongamos que n es el menor número tal que nP se descompone en $\mathbb{Z}[x]$. si $n = 1$ el lema está probado. Supongamos que $n > 1$, sea p un divisor primo de n, entonces no todos los b_i ni todos los c_i pueden ser divisibles por p (ya que en ese caso podríamos simplificar por p en (2.1) reduciendo n a n/p). Sean b_i y c_j tales que $p \nmid b_i$, $p \nmid c_j$ pero $p|b_r$, $p|c_s$ si $r < i$, $s < j$ (podría ocurrir que $i, j = 0$), entonces igualando en (2.1) los coeficientes de grado $i + j$ se tiene

$$na_{i+j} = b_{i+j}c_0 + b_{i+j-1}c_1 + \ldots + b_i c_j + \ldots + b_0 c_{i+j}$$

y de aquí se deduce que $p|b_i c_j$ en contra de nuestra hipótesis $p \nmid b_i$, $p \nmid c_j$. ■

<u>Ejemplo</u> . Estudiar la irreducibilidad de $\frac{1}{2}x^4 - \frac{1}{2}x^3 - \frac{1}{2}x - \frac{1}{2}$ en $\mathbb{Q}[x]$.

Es obvio que basta estudiar la irreducibilidad de $P = x^4 - x^3 - x - 1$. Como veremos en la sección siguiente, es fácil comprobar que P no tiene factores de grado 1, por tanto, si P no es irreducible debe factorizar como

$$P = (x^2 + ax + b)(x^2 + cx + d).$$

Operando e igualando los coeficientes del mismo grado

$$-1 = bd \qquad 0 = b + d + ac$$
$$-1 = ad + bc \qquad -1 = a + c.$$

El lema de Gauss asegura que a, b, c, d son <u>enteros</u>, con lo cual la primera ecuación implica $b = 1$, $d = -1$ ó $b = -1$, $d = 1$. En el primer caso, es fácil comprobar que $a = 0$ y $c = -1$, con lo cual P se descompone como

$$P = (x^2 + 1)(x^2 - x - 1)$$

y, por tanto, el polinomio de partida no es irreducible en $\mathbb{Q}[x]$.

Un criterio que es de utilidad en algunos casos para estudiar la irreducibilidad en $\mathbb{Q}[x]$ es el siguiente

Proposición 2.6 (Criterio de Eisenstein)**:** *Si $P = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ es un polinomio con coeficientes enteros y p es un primo tal que $p\not| a_n$, $p|a_i$ si $0 \le i < n$ y $p^2\not| a_0$ entonces P es irreducible en $\mathbb{Q}[x]$.*

<u>Dem.</u>: Por el Lema de Gauss, si P no es irreducible se puede escribir como $P = (b_l x^l + b_{l-1}x^{l-1} + \ldots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0)$ con $l + m = n$ y $b_i, c_i \in \mathbb{Z}$. Igualando los coeficientes de los términos del mismo grado, se tiene

$$a_0 = b_0 c_0, \qquad a_1 = b_1 c_0 + b_0 c_1, \qquad a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2, \qquad \ldots$$

Por hipótesis $p|a_0$ pero $p^2\not| a_0$, así pues p divide a b_0 o a c_0 pero no a ambos simultáneamente. Supongamos por ejemplo que p divide a b_0, entonces por la segunda igualdad, $p|b_1$ y por la tercera $p|b_2$ y en general $p|b_i$ $0 \le i \le l$, lo que implica que p divide a todos los a_i lo que contradice nuestra hipótesis $p\not| a_n$. ■

<u>Ejemplo</u>. El polinomio $x^3 - 2x^2 + 10x + 2$ es irreducible en $\mathbb{Q}[x]$ por el criterio de Eisenstein con $p = 2$.

El interés práctico del criterio de Eisenstein está bastante limitado porque sólo es aplicable en casos muy particulares. Una de las razones que justifican su interés es que permite demostrar la irreducibilidad de cierta importante familia de polinomios. La situación se recoge en el siguiente ejemplo que sólo se cita aquí a título ilustrativo.

<u>Ejemplo</u>. Gauss demostró que si p es primo el polinomio (llamado ciclotómico) $P = x^{p-1} + x^{p-2} + \ldots + x + 1$ es irreducible en $\mathbb{Q}[x]$. Esto se puede demostrar usando el criterio de Eisenstein a pesar de que no es posible su aplicación directa. Para ello nótese que si P es irreducible $Q = (x+1)^{p-1} + (x+1)^{p-2} + \ldots + (x+1) + 1$ también lo es (ejercicio) y como

$$Q = \frac{(x+1)^p - 1}{x + 1 - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \ldots + \binom{p}{p-2} x + \binom{p}{p-1},$$

el criterio de Eisenstein es aplicable sobre Q (ejercicio).

La irreducibilidad en $\mathbb{Z}_p[x]$ es, en principio, mucho más sencilla de estudiar que en $\mathbb{Q}[x]$, ya que sólo hay un número finito de polinomios de cada grado. Por ejemplo, todos los polinomios de grado 2 en $\mathbb{Z}_2[x]$ son

$$x^2, \quad x^2 + \overline{1}, \quad x^2 + x, \quad x^2 + x + \overline{1}.$$

Claramente, ni el primer ni el tercer polinomio son irreducibles. El segundo tampoco lo es ya que $x^2 + \overline{1} = (x + \overline{1})(x + \overline{1})$ en $\mathbb{Z}_2[x]$. Finalmente, no es difícil comprobar que $x^2 + x + \overline{1}$

no se puede descomponer y por tanto es irreducible. Con esto, se tiene que los polinomios irreducibles en $\mathbb{Z}_2[x]$ de grado menor o igual que 2 son

$$x, \quad x+\overline{1}, \quad x^2+x+\overline{1}.$$

Si, por ejemplo, quisiéramos estudiar si un polinomio de grado 4 es irreducible en $\mathbb{Z}_2[x]$, bastaría comprobar si es divisible por alguno de estos tres polinomios. Si el polinomio fuera de grado 6, tendríamos que ampliar nuestra lista de irreducibles hasta grado 3 (porque podría descomponerse como producto de dos polinomios de grado 3), y así sucesivamente.

3.3. Raíces

Un polinomio $P \in K[x]$ se puede considerar también como una función $P : K \to K$ sin más que sustituir la variable indeterminada por elementos del cuerpo K.

Definición: *Se dice que $\alpha \in K$ es un cero o una raíz de $P \in K[x]$ si $P(\alpha) = 0$.*

Ejemplo . x^2+x+1 no tiene raíces en $\mathbb{R}$; sin embargo tiene dos raíces distintas en $\mathbb{C}$ que son $\alpha_1 = (-1+i\sqrt{3})/2$ y $\alpha_2 = (-1-i\sqrt{3})/2$.

Proposición 3.1 (Regla de Ruffini)**:** *α es un cero de un polinomio de $K[x]$ si y sólo si $x-\alpha$ divide a ese polinomio.*

Dem.: Por la Proposición 1.3 con $Q = x-\alpha$

$$P = (x-\alpha)C + R \tag{3.1}$$

con $\operatorname{gr} R = 0$ o $R = 0$, es decir, R es un polinomio constante. Sustituyendo x por α en (3.1) se tiene $P(\alpha) = R(\alpha)$ y por tanto α es raíz si y sólo si $R = 0$. ■

Ejemplo . En algunos libros se denomina *Regla de Ruffini* al bien conocido esquema abreviado que se representa a continuación y que sirve para calcular la división de un polinomio $P = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ entre $x-\alpha$

$$\begin{array}{c|ccccc} & a_n & a_{n-1} & a_{n-2} & \cdots\cdots\cdots & a_0 \\ \alpha & & a_n\alpha & a_n\alpha^2 + a_{n-1}\alpha & \cdots\cdots\cdots & \ldots \\ \hline & a_n & a_n\alpha + a_{n-1} & \cdots\cdots\cdots & \cdots\cdots\cdots & \lfloor r \end{array}$$

La línea inferior indica los coeficientes del cociente y r es el resto, que coincide con $P(\alpha)$.

Ejemplo . Hallar el cociente y el resto al dividir x^3-6x^2-6x-7 entre $x+1$.

$$\begin{array}{c|cccc} & 1 & -6 & -6 & -7 \\ -1 & & -1 & 7 & -1 \\ \hline & 1 & -7 & 1 & \lfloor -8 \end{array}$$

Por tanto $x^3-6x^2-6x-7 = (x^2-7x+1)(x+1)-8$.

DEFINICIÓN: *Sea* α *un cero de* $P \in K[x]$. *Se dice que* α *tiene* multiplicidad n *si* $(x-\alpha)^n | P$ *y* $(x-\alpha)^{n+1} \nmid P$.

Nota: A un cero de multiplicidad uno se le suele llamar cero simple.

Corolario 3.2: *El número de raíces de* $P \in K[x]$ *contadas con su multiplicidad es menor o igual que* $\operatorname{gr} P$.

DEM.: Si P tiene raíces (distintas) $\alpha_1, \alpha_2, \ldots, \alpha_n$ con multiplicidades $m_1, \ldots, m_n$ respectivamente, entonces $Q = (x-\alpha_1)^{m_1} \ldots (x-\alpha_n)^{m_n}$ divide a P, es decir, $P = QR$ y por el Lema 1.2

$$\operatorname{gr} P = \operatorname{gr} Q + \operatorname{gr} R \geq \operatorname{gr} R = m_1 + m_2 + \ldots + m_n$$

y esto concluye la demostración. ■

El corolario anterior, así como otros muchos de los resultados que hemos visto, puede ser falso si consideramos polinomios con coeficientes en un anillo en lugar de en un cuerpo. Por ejemplo, el polinomio $P = x^2 + \overline{7} \in \mathbb{Z}_8[x]$ tiene cuatro raíces, $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$, a pesar de que su grado es dos, y tampoco hay unicidad en la factorización, ya que $P = (x+\overline{1})(x+\overline{7})$ y $P = (x+\overline{3})(x+\overline{5})$. Sin embargo, todas las propiedades se recuperan si uno se limita a anillos que tengan ciertas propiedades, esencialmente aquellos anillos en los que se puede definir el máximo común divisor.

Se puede saber si un polinomio de coeficientes enteros tiene raíces en $\mathbb{Q}$ gracias al siguiente resultado

Proposición 3.3 : *Si* $p/q \in \mathbb{Q}$, *con* p, q *primos entre sí, es un cero del polinomio de grado* n

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad \text{con } a_i \in \mathbb{Z}$$

entonces $p|a_0$ *y* $q|a_n$.

DEM.: Sustituyendo p/q en el polinomio y multiplicando por q^n

$$a_n p^n + a_{n-1}p^{n-1}q + \ldots a_1 p q^{n-1} + a_0 q^n = 0.$$

De esta igualdad se deduce

$$p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \ldots a_1 q^{n-1}) = -a_0 q^n,$$
$$q(a_{n-1}p^{n-1} + \ldots a_1 p q^{n-2} + a_0 q^{n-1}) = -a_n p^n.$$

Por tanto, $p|a_0 q^n$ y $q|a_n p^n$. Como p y q son primos entre sí, por el teorema de Euclides $p|a_0$ y $q|a_n$. ■

Ejemplo . Las únicas posible raíces racionales de $P = 2x^3 - 5x^2 - 5x - 7$ son $\pm 1/1$, $\pm 7/1$, $\pm 1/2$, $\pm 7/2$. Algunos cálculos pruebas que sólo $7/2$ es verdaderamente una raíz, así pues, P es divisible por $x-7/2$, concretamente,

$$\begin{array}{c|cccc} & 2 & -5 & -5 & -7 \\ 7/2 & & 7 & 7 & 7 \\ \hline & 2 & 2 & 2 & \boxed{0} \end{array}$$

implica $P=(x-7/2)(2x^2+2x+2)$. Además ésta es la factorización de P en $\mathbb{Q}[x]$, ya que $2x^2+2x+2$ no puede descomponerse en dos factores lineales porque no tiene raíces racionales.

El teorema fundamental del álgebra se puede fórmulas en términos de raíces de polinomios. Dos sencillas consecuencias de él y la Proposición 3.1 son

Proposición 3.4 : *Un polinomio de grado n en $\mathbb{C}[x]$ tiene n raíces en $\mathbb{C}$ (contando multiplicidades).*

<u>Dem.</u>: Por el Teorema fundamental del álgebra, un polinomio de grado n se descompone como producto de n factores lineales en $\mathbb{C}[x]$, y según la Proposición 3.1 cada uno de ellos corresponde a una raíz. ■

Proposición 3.5 : *Si $P\in\mathbb{R}[x]$ es irreducible, entonces $\operatorname{gr}P=1$ ó $\operatorname{gr}P=2$.*

<u>Dem.</u>: Veamos que si $P\in\mathbb{R}[x]$ es irreducible su grado no puede ser mayor que dos. Si P es irreducible no puede tener raíces reales. Sea z una raíz compleja (no real) de P, entonces $\overline{z}$ (el conjugado) es también una raíz (porque $P(z)=0\Rightarrow\overline{P(z)}=P(\overline{z})=0$). Por tanto $Q=(x-z)(x-\overline{z})$ divide a P, pero $Q=x^2-2x\mathrm{Re}\,z+|z|^2\in\mathbb{R}[x]$ y si el grado de P fuera mayor que 2, Q sería un factor no trivial de P en $\mathbb{R}[x]$, lo cual llevaría a contradicción. ■

Los resultados de esta sección reducen el problema de factorizar un polinomio en $\mathbb{R}[x]$ o $\mathbb{C}[x]$ al cálculo de sus raíces. Los siguientes ejemplos están preparados para que dicho cálculo se pueda llevar a cabo.

<u>Ejemplo 1</u>. Factorizar $P=x^4-16$ en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$.

Es claro que

$$P=(x^2-4)(x^2+4)$$

y como

$$x^2-4=0\ \Rightarrow\ x\begin{array}{l}\nearrow\ 2\\ \searrow\,-2\end{array}\qquad x^2+4=0\ \Rightarrow\ x\begin{array}{l}\nearrow\ 2i\\ \searrow\,-2i\end{array}$$

se tiene que

$$
\begin{aligned}
P =&(x-2)(x+2)(x^2+4) \text{ en } \mathbb{R}[x]\\
P =&(x-2)(x+2)(x-2i)(x+2i) \text{ en } \mathbb{C}[x].
\end{aligned}
$$

<u>Ejemplo 2</u>. Factorizar $P = x^3 + 2x^2 + 2x + 1$ en $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

Según la Proposición 3.3 las únicas posibles raíces racionales de P son 1 y -1. Es fácil comprobar que -1 es raíz y por tanto $x + 1|P$, concretamente

$$P = (x+1)(x^2+x+1).$$

Usando la fórmula de la ecuación de segundo grado, se tiene

$$x^2 + x + 1 = 0 \;\Rightarrow\; x \begin{cases} -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ -\frac{1}{2} - i\frac{\sqrt{3}}{2} \end{cases}$$

Por tanto P factoriza como

$$
\begin{aligned}
P =&(x+1)(x^2+x+1) \text{ en } \mathbb{R}[x]\\
P =&(x+1)(x+\frac{1}{2}-i\frac{\sqrt{3}}{2})(x+\frac{1}{2}+i\frac{\sqrt{3}}{2}) \text{ en } \mathbb{C}[x].
\end{aligned}
$$

1) Hallar mcd $(x^5 + x^4 + 4x + 4, x^3 - 3x^2 + 4x - 2)$.

2) Sean P_1, P_2, P_3 tres polinomios primos entre sí dos a dos (esto es, mcd $(P_i, P_j) = 1$ si $i \neq j$). Calcular mcd (P_1P_2, P_1P_3, P_2P_3) y mcm (P_1P_2, P_1P_3, P_2P_3).

3) Hallar el máximo común divisor de $P = x^4+3x^3+4x^2+5x+2$ y $Q = x^3+3x^2+3x+2$ y escribirlo en la forma $AP + BQ$.

4) Hallar polinomios A y B tales que $A(x^2 + 2x - 2) + B(x^2 + x - 1) = 1$.

Opcional: Escribe un programa en tu lenguaje de programación favorito que decida si dos polinomios dados con coeficientes enteros son primos entre sí.

5) Descomponer $P = x^3 - 2$ en producto de irreducibles en $\mathbb{R}[x]$ y después en $\mathbb{C}[x]$. ¿Es irreducible en $\mathbb{Q}[x]$?

6) Comprobar que $n(n^2 + 1)$ con $n \in \mathbb{Z}$ siempre es par y usarlo para demostrar que $P = x^3 + x - 105^{105}$ no tiene raíces enteras. ¿Tiene raíces racionales?

7) Hallar todos los polinomios irreducibles de $\mathbb{R}[x]$.

8) Si $x_1, x_2, \ldots, x_n$ son números reales distintos y $1 \leq k \leq n$, comprobar que

$$P_k = \prod_{\substack{i=1 \\ i \neq k}}^{n} \frac{x - x_i}{x_k - x_i}$$

es un polinomio que se anula en todos los x_i excepto en x_k donde vale 1.

9) En cálculo numérico muchas veces es conveniente construir un polinomio que tome los mismos valores que una función dada. Demostrar usando el problema anterior y con la notación allí introducida, que

$$P = y_1P_1 + y_2P_2 + \ldots + y_nP_n$$

es un polinomio de grado menor que n tal que $P(x_i) = y_i$ para $1 \leq i \leq n$.

Nota: Este polinomio se llama polinomio interpolador. Existen varios algoritmos que partiendo de los x_i y los y_i calculan sus coeficientes bastante rápido.

10) Demostrar que $x^3 - 3x + 3$ sólo tiene una raíz real. *Indicación*: Dibujar la gráfica.

11) Factorizar $x^4 - x^2 - 2$ en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$.

12) Hallar polinomios A y B tales que $A(x^2 + 4x + 1) + B(x^2 + 3x + 1) = 1$.

13) Sea $P \in \mathbb{R}[x]$, P' su derivada, $D = \text{mcd}\,(P, P')$ y α un cero de P. Demostrar que α es un cero simple de $P \Leftrightarrow D(\alpha) \neq 0$.

14) Hallar un polinomio en $\mathbb{R}[x]$ tal que $z = 1 + \sqrt{-2}$ sea una de sus raíces.

15) Decidir si $x^4 + 6x^3 + 9x - 15$, $x^5 - 6$, $x^3 - 16$ y $x^4 + 2x^3 + 3x^2 + 2x + 1$ son irreducibles en $\mathbb{Q}[x]$.

***16)** Sea $P = 1 + x + x^2 + \ldots + x^{n-1}$ con $n > 1$. Demostrar que P es irreducible en $\mathbb{Q}[x]$ si y sólo si n es primo.

Miscelánea.

El teorema fundamental del álgebra, esencialmente afirma que con los números complejos podemos resolver todas las ecuaciones polinómicas. Se puede afirmar que la primera vez que esas entidades misteriosas llamadas números complejos aparecieron en el mundo matemático, fue en el siglo XVI al resolver ecuaciones de tercer grado. Curiosamente la fórmula de resolución involucra a veces inevitablemente raíces de números negativos en cálculos intermedios, que más tarde se pueden simplificar para obtener un número real. Durante mucho tiempo los matemáticos trataron los números complejos con bastante desconfianza, porque aunque permitían hacer algunos cálculos no parecían tener ningún sentido.

Uno de los matemáticos del siglo XVIII que manipularon con mayor soltura (pero todavía sin rigor) los números complejos fue el genial L. Euler (1707-1783), quien "demostró" la fórmula

$$e^{ix} = \cos x + i \operatorname{sen} x.$$

Aunque no fue exactamente así como la dedujo Euler, esta fórmula se puede obtener sustituyendo e^{ix}, $\cos x$ y $\operatorname{sen} x$ por sus respectivas series de Taylor. Nótese que tomando $x = \pi$ se obtiene

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

lo cual es constituye una bella relación entre cuatro de las constantes que más veces aparecen en Matemáticas: 0, 1, $\sqrt{-1}$, e y π. Utilizando que $e^{i(nx)} = (e^{ix})^n$, se obtiene también la llamada fórmula de De Moivre

$$\cos nx + i \operatorname{sen} nx = (\cos x + i \operatorname{sen} x)^n,$$

que es útil para calcular senos y cosenos de múltiplos de ángulos. Es conveniente asociar a cada número complejo $a + bi$ el punto del plano (a, b). Como este punto puede expresarse como $(R\cos\alpha, R\operatorname{sen}\alpha)$ donde α es el ángulo que forma el vector (a, b) con el eje X positivo y R es su longitud, podemos escribir

$$a + bi = R\cos\alpha + iR\operatorname{sen}\alpha = Re^{i\alpha}.$$

Habitualmente se dice que $R(\cos\alpha + i\operatorname{sen}\alpha)$ es la forma trigonométrica de $a + bi$. También se escribe a veces R_α y se dice que ésta es la forma polar de $a + bi$. Con esta notación es muy fácil multiplicar (y dividir y extraer raíces de) números complejos

$$R_\alpha \cdot R'_{\alpha'} = Re^{i\alpha} \cdot R'e^{i\alpha'} = RR'e^{i(\alpha+\alpha')} = (RR')_{\alpha+\alpha'}.$$

Gracias a estas fórmulas los matemáticos fueron capaces de dar un significado a los números complejos identificándolos con vectores del plano que tienen ciertas propiedades de dilatación y rotación al ser multiplicados. Curiosamente estos números tan misteriosos que durante casi 300 años parecieron entelequias matemáticas, ahora son fundamentales para nuestro entendimiento del mundo físico, concretamente, la ecuación de Schrödinger, en la que se basa la mecánica cuántica, es una ecuación con coeficientes complejos.

> Todo nuestro trabajo e nuestra esperança
> está en aventura e está en balança;
> por buen comienço espera omne la buena andança;
> a vezes viene la cosa, pero faga tardanza.
> *LBA, 805*

A causa de las grandes dudas iniciales acerca del significado de los números complejos, la primera demostración válida del teorema fundamental del álgebra es relativamente tardía. De hecho, un matemático tan ilustre como G.W. Leibniz (1646-1716) pensaba en 1702 que el resultado no era cierto, concretamente, que el polinomio $x^4 + a^4$ no se podía factorizar para ningún a como producto de polinomios de grado 1 ó 2 en $\mathbb{R}[x]$. Por otra parte, Euler, J.R. d'Alambert (1717-1783) y J.-L. Lagrange (1736-1813) dieron en el siglo XVIII demostraciones incompletas del teorema y hubo que esperar hasta 1799 para que C.F. Gauss (1777-1855) obtuviera la primera demostración válida. Más tarde, él mismo dio otras tres pruebas.

Expondremos aquí la idea geométrica, o más bien topológica (la topología estudia las propiedades invariantes por deformaciones continuas), que subyace a la demostración del teorema fundamental del álgebra.

Sea $P \in \mathbb{C}[x]$ un polinomio de grado n. Quizá multiplicando por una constante, podemos suponer que su coeficiente de mayor grado es 1, esto es,

$$P = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} \ldots + a_1x + a_0.$$

Basta demostrar que P tiene siempre una raíz, ya que en ese caso $P = (x-r)Q$ con $\operatorname{gr} Q = n-1$ y aplicando el mismo argumento repetidas veces sobre Q se llega a una descomposición de P en factores lineales.

Si $a_0 = 0$, P tiene a $x = 0$ como raíz. Supongamos, por tanto, que $a_0 \neq 0$. Sustituyendo x por $R(\cos\alpha + i\operatorname{sen}\alpha)$, se tiene

$$P = R^n(\cos n\alpha + i\operatorname{sen} n\alpha) + a_{n-1}R^{n-1}(\cos(n-1)\alpha + i\operatorname{sen}(n-1)\alpha) + \ldots + a_0.$$

Si R es muy grande (y positivo), el primer término domina sobre los otros y P es aproximadamente (con poco error relativo) $R^n(\cos n\alpha + i\operatorname{sen} n\alpha)$, lo que cuando α varía entre 0 y 2π representa la circunferencia centrada en $(0,0)$ de radio R^n (recorrida n veces). Por otra parte, si $R = 0$ se tiene que P es a_0. Es decir, el conjunto $\{P\big(R(\cos\alpha + i\operatorname{sen}\alpha)\big) \,/\, 0 \leq \alpha \leq 2\pi\}$ representa para R grande una curva parecida a una circunferencia centrada en $(0,0)$ y de radio R^n, y cuando R se acerca a 0, esta curva se tiene que deformar hasta reducirse al punto $a_0 \neq 0$. Está claro que en este proceso de deformación continua las curvas intermedias tienen que atravesar el cero, por tanto existe algún R y algún α para el que $P\big(R(\cos\alpha + i\operatorname{sen}\alpha)\big) = 0$, o lo que es lo mismo, P tiene una raíz en $\mathbb{C}$.

El teorema fundamental del álgebra hace que sea trivial el estudio de la irreducibilidad en $\mathbb{C}[x]$, veremos ahora cómo el estudio de la irreducibilidad en $\mathbb{Z}_p[x]$ no es en absoluto sencillo pero es útil para resolver algunos problemas aritméticos, concretamente demostraremos un resultado de P. de Fermat (1601-1665) que enunciamos en el capítulo anterior: Si $p > 2$ es primo

$$p \textit{ es suma de dos cuadrados} \Leftrightarrow p-1 \textit{ es divisible por } 4.$$

Si a, b es una solución de $a^2 + b^2 = p$ entonces tomando módulo p y definiendo $x = \overline{a}\overline{b}^{-1}$ donde $\overline{b}^{-1}$ es el inverso de $\overline{b}$ en $\mathbb{Z}_p$

$$a^2 + b^2 = p \;\Rightarrow\; a^2 + b^2 \equiv 0\ (p) \;\Rightarrow\; x^2 + 1 = \overline{0} \text{ en } \mathbb{Z}_p.$$

Con esto hemos probado

$$p \textit{ es suma de dos cuadrados} \Rightarrow x^2 + 1 \textit{ tiene una raíz en } \mathbb{Z}_p.$$

Por otra parte, si $x^2 + 1$ tiene una raíz, $\overline{x_0}$, entonces $p | x_0^2 + 1$. Sea N la parte entera (sin decimales) de $\sqrt{p}$. Cuando evaluamos $x_0x - y$ tomando $0 \leq x, y \leq N$, algún par de resultados deben ser congruentes módulo p, ya que (x, y) puede tomar en total $(N+1)^2 > p$ valores. Así pues digamos que $x_0x_1 - y_1 \equiv x_0x_2 - y_2\ (p)$ con $0 \leq x_1, x_2, y_1, y_2 \leq N$ y $(x_1, y_1) \neq (x_2, y_2)$. Definiendo $a = x_1 - x_2$ y $b = y_1 - y_2$ se tiene que $p | a^2 + b^2$, ya que

$$a^2 + b^2 \equiv (x_1 - x_2)^2 + (y_1 - y_2)^2 \equiv (x_1 - x_2)^2 + x_0^2(x_1 - x_2)^2 \equiv (x_1 - x_2)^2(1 + x_0^2) \equiv 0\ (p).$$

Por otra parte, como $0 \leq x_1, x_2, y_1, y_2 \leq N$, $(x_1, y_1) \neq (x_2, y_2)$, se tiene que $0 < a^2 + b^2 < 2p$ y, por tanto, $p|a^2+b^2$ implica $p=a^2+b^2$. Con esto hemos probado

$$x^2+1 \textit{ tiene una raíz en } \mathbb{Z}_p \Rightarrow p \textit{ es suma de dos cuadrados.}$$

Así pues hemos "reducido" un problema acerca de números primos a otro de factorización de polinomios, concretamente, sabemos que

$$p \textit{ es suma de dos cuadrados} \Leftrightarrow x^2+1 \textit{ no es irreducible en } \mathbb{Z}_p.$$

Pero el problema de la irreducibilidad de polinomios cuadráticos en $\mathbb{Z}_p$ no es en absoluto sencillo, de hecho Euler no lo consiguió resolver y fue Gauss quien obtuvo una solución completa. Sin embargo en el caso de x^2+1 es posible dar una solución breve contenida en el siguiente resultado que termina la demostración del teorema que enunciamos al principio

$$x^2+1 \textit{ no es irreducible en } \mathbb{Z}_p \Leftrightarrow p-1 \textit{ es divisible por } 4.$$

Demostraremos separadamente cada una de las implicaciones:

Si x^2+1 es irreducible, por lo dicho anteriormente, $p=a^2+b^2$. Dando valores (módulo 4) se tiene que para cualquier n entero $\overline{n}^2=\overline{0},\overline{1}$ en $\mathbb{Z}_4$, por tanto $p\equiv 0, 1$ ó $2\ (4)$, como p es impar la única posibilidad es $p\equiv 1\ (4)$ y por tanto 4 divide a $p-1$.

Supongamos ahora que $4|p-1$, entonces $p=4k+1$. El pequeño teorema de Fermat asegura que x^p-x tiene p raíces en $\mathbb{Z}_p$ (todas las clases) así pues la factorización $x^p-x=x(x^{2k}+1)(x^{2k}-1)$ implica que $x^{2k}+1$ tiene $2k$ raíces en $\mathbb{Z}_p$. Finalmente, tomando $X_0=x_0^k$ donde x_0 es una raíz de $x^{2k}+1$ se tiene que X_0 es raíz de x^2+1 que por tanto no es irreducible.

Como ya hemos mencionado, Gauss dio una solución completa al problema de la irreducibilidad de polinomios cuadráticos en $\mathbb{Z}_n$. El resultado clave es la llamada "Ley de reciprocidad cuadrática" que afirma que para cada par de primos, $p, q>2$

$$x^2-q \text{ es irreducible en } \mathbb{Z}_p \;\Leftrightarrow\; x^2-(-1)^{\frac{p-1}{2}}p \text{ es irreducible en } \mathbb{Z}_q.$$

Gauss dio ocho demostraciones distintas de este resultado (recuérdese que dio cuatro del teorema fundamental del álgebra) lo cual no indica en absoluto que publicase sus resultados antes de que tuvieran forma definitiva, ya que las diferentes demostraciones no fueron mejoras sucesivas de una original imperfecta, sino que constituyen realmente visiones distintas del problema que en algunos casos han sido pioneras de nuevas áreas de las Matemáticas. Gauss sólo presentaba sus trabajos cuando éstos formaban una teoría completa y perfeccionada, con lo cual a veces se atribuyen a otros matemáticos resultados que él había obtenido con anterioridad. Su lema fue *pauca sed matura* (pocos pero maduros), lo cual contrasta con el *Publish or perish* (publica o muere, es el nombre de una editorial) que parece imperar en el mundo científico actual.

Quiérovos abreviar la mi predicaçión,
que sienpre me pagué de pequeño sermón
e de dueña pequeña e de breve razón,
ca lo poco e bien dicho finca en el coraçón.
LBA, 1606

Mejor cosa es al omne, al cuerdo e al entendudo,
callar do non le enpeçe e tiénenle por sesudo,
que fablar lo que non le cunple porque sea arrepentudo:
o piensa bien lo que fablas, o calla, fazte mudo.
LBA, 722

4. Teoría elemental de Grupos

4.1. Definición, subgrupos, ejemplos

Como vimos en la sección 1.4, un grupo, G, es un conjunto (no vacío) dotado con una operación cerrada, $*$, que cumple

i) $*$ *es asociativa:* $g*(h*f)=(g*h)*f$.

ii) Existe el elemento neutro: $\forall g\in G \ \ \exists e\in G \,/\, e*g=g*e=g$.

iii) Existe el elemento inverso: $\forall g\in G\ \exists g^{-1}\in G \,/\, g^{-1}*g=g*g^{-1}=e$.

Cuando se quieren evitar confusiones con respecto a la operación definida en el conjunto, se suele escribir $(G,*)$.

Se dice que el grupo es abeliano o conmutativo si además $*$ es una operación conmutativa, es decir, $g*h=h*g$.

Observación: Muchas veces se usa la notación multiplicativa en los grupos, escribiéndose $g\cdot h$, o simplemente gh, en vez de $g*h$. Con esta notación g^n es una abreviatura para $g*g*\overset{n\,\text{veces}}{\cdots}*g$ y g^{-n} es el inverso de g^n. Pero en los grupos abelianos es más frecuente usar la notación aditiva, escribiéndose $g+h$, 0 y $-g$, en vez de $g*h$, e y g^{-1} respectivamente.

Ejemplo 1. $(\mathbb{Z},+)$ es un grupo.

Ejemplo 2. $(\mathbb{Z},\cdot)$ no es un grupo (por ejemplo 2 no tiene inverso).

Ejemplo 3. $(\mathbb{R}-\{0\},\cdot)$ es un grupo.

Ejemplo 4. Los giros alrededor del origen forman un grupo con la composición. Si g_α denota el giro de α grados, entonces $g_\alpha\cdot g_\beta=g_{\alpha+\beta}$.

Ejemplo 5. $(S^1,\cdot)$ es un grupo, donde $S^1=\{z\in\mathbb{C}\,/\,|z|=1\}$ y $\cdot$ es el producto habitual de números complejos. Nótese que $\cdot$ es cerrada porque el producto de dos números complejos de módulo 1 es también un número complejo de módulo 1.

Ejemplo 6. $(\mathcal{M},\cdot)$ es un grupo, donde

$$\mathcal{M}=\left\{\begin{pmatrix} a & -b\\ b & a\end{pmatrix} \qquad \text{con } a^2+b^2=1, \quad a,b\in\mathbb{R}\right\}$$

y $\cdot$ es el producto habitual de matrices. Requiere algunos cálculos comprobar que la operación es cerrada y tampoco es totalmente evidente que exista el elemento inverso.

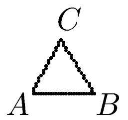
Más adelante veremos que los ejemplos 4, 5 y 6 son "isomorfos", es decir, los tres grupos son el mismo salvo cambiar el nombre (la forma) de sus elementos. Esto permite pasar información de cada uno de estos grupos a los otros. Por ejemplo, es bastante obvio que $g^{10} = e$ tiene solución en el ejemplo 4, para ello basta tomar como g el giro de 36^{o} (aplicado diez veces da la identidad); de hecho no es difícil ver que tiene diez soluciones (los giros de ángulos $0 \cdot 36^{\text{o}}$, $1 \cdot 36^{\text{o}}$, $2 \cdot 36^{\text{o}}$,...,$9 \cdot 36^{\text{o}}$). Sabiendo que los grupos de los ejemplos 5 y 6 son "iguales", esto permite concluir que 1 tiene diez raíces décimas complejas de módulo uno y, lo que es menos intuitivo, que hay exactamente diez matrices en $\mathcal{M}$ que elevadas a la décima potencia dan la identidad.

Con los comentarios del párrafo anterior hemos querido ilustrar cómo la existencia de una operación que dé lugar a la misma estructura de grupo permite resolver problemas aparentemente muy distintos. Por ello tiene sentido considerar en abstracto las propiedades de los grupos para obtener resultados concretos en diferentes contextos.

Todos los grupos que hemos considerado en los ejemplos anteriores son abelianos. Veamos algunos grupos no conmutativos:

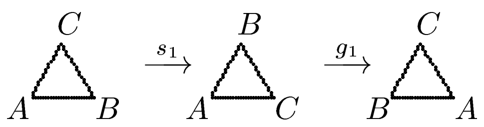
<u>Ejemplo 7</u>. Las traslaciones y los giros (sin ningún origen fijado) en el plano, forman un grupo no abeliano. No es del todo sencillo "ver" que la composición de dos giros alrededor de puntos distintos es un giro (o una traslación), pero no es difícil percatarse de que la composición de giros no es conmutativa en general. Por ejemplo, si g y h son giros de 45^{o} alrededor de $O = (0,0)$ y $O' = (1,0)$ respectivamente, es claro (con un dibujo) que gh y hg trasladan O a puntos distintos y por tanto $gh \neq hg$.

<u>Ejemplo 8</u>. Un grupo no abeliano más sencillo de visualizar es el grupo de movimientos del plano que dejan invariante al triángulo equilátero



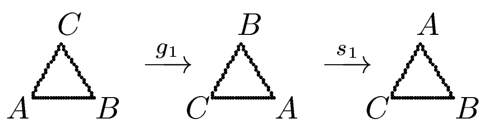
No es difícil convencerse de que este grupo es $G = \{e, g_1, g_2, s_1, s_2, s_3\}$ donde g_1 y g_2 son giros de 120^{o} y 240^{o} (alrededor del centro del triángulo) y s_1, s_2, s_3 son las simetrías que tienen como ejes las alturas que pasan por A, B, C respectivamente. Para ver que el grupo no es conmutativo veamos la acción de $g_1 s_1$ sobre el triángulo ABC

$g_1 s_1 :$



Mientras que el efecto de aplicar $s_1 g_1$ es

$s_1 g_1 :$



por tanto $g_1 s_1 \neq s_1 g_1$.

Antes de seguir con otros ejemplos más importantes, veamos dos definiciones sencillas:

Definición: *Se dice que un grupo es* finito *si tiene un número finito de elementos, en caso contrario se dice que es* infinito.

Recuérdese que el número de elementos de un conjunto (finito) se denomina cardinal u orden. Sin embargo, si este conjunto tiene estructura de grupo, el término "cardinal" apenas se usa, prefiriéndose hablar del orden de un grupo G denotándolo (como en el caso de conjunto generales) por $|G|$.

El único grupo finito en los ejemplos anteriores es el grupo de movimientos del plano que dejan invariante el triángulo equilátero, su orden es 6.

Otros ejemplos importantes: Destacaremos tres grupos que por su sencillez e importancia aparecerán continuamente en este capítulo

1) $\mathbb{Z}_n$ con la operación suma es un grupo abeliano. Su orden es $|\mathbb{Z}_n| = n$. Dentro de la teoría de grupos abelianos ocupa un lugar muy destacado, ya que se puede demostrar que todo grupo abeliano finito se obtiene "uniendo" (en un sentido que se precisará más adelante) varios $\mathbb{Z}_n$.

2) Sea $\mathbb{Z}_n^*$ el conjunto formado por los elementos de $\mathbb{Z}_n$ que tienen inverso multiplicativo. $\mathbb{Z}_n^*$ es un grupo abeliano con la multiplicación.

Las tablas de grupo de $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ y de $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ son

$\mathbb{Z}_4$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\mathbb{Z}_5$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Obsérvese que ambas tablas son iguales haciendo los cambios $\overline{0} \leftrightarrow \overline{1}$, $\overline{1} \leftrightarrow \overline{2}$, $\overline{2} \leftrightarrow \overline{4}$ y $\overline{3} \leftrightarrow \overline{3}$. Se puede demostrar (pero no es fácil) que, en general, si p es primo los grupos $\mathbb{Z}_{p-1}$ y $\mathbb{Z}_p^*$ son iguales salvo cambios de este tipo (hablando en rigor, son isomorfos). En ese caso, la función que pasa de la tabla de $\mathbb{Z}_{p-1}$ a la de $\mathbb{Z}_p^*$ "descoloca" muy bien las clases y tiene ciertas propiedades especiales (su inversa es muy complicada de hallar si p es grande) que hacen que sea muy útil para codificar información.

Nota: Si n no es primo, los grupos $\mathbb{Z}_{n-1}$ y $\mathbb{Z}_n^*$ son bien distintos, de hecho ni siquiera tienen el mismo orden, por ejemplo, $|\mathbb{Z}_7| = 7$ pero $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \Rightarrow |\mathbb{Z}_8^*| = 4$.

3) Sea S_n el conjunto formado por las funciones biyectivas $\sigma : \{1,2,\ldots,n\} \longrightarrow \{1,2,\ldots,n\}$, estas funciones se llaman <u>permutaciones</u> porque su efecto es intercambiar (permutar) los números de 1 a n. S_n es un grupo tomando como operación la composición de funciones. El elemento neutro corresponde a la función identidad, Id. Una permutación $\sigma \in S_n$ se suele representar mediante la matriz

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

Por ejemplo, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$ es la permutación que intercambia 1 y 2 y deja 3 fijo. No es difícil comprobar que S_n es un grupo de orden $|S_n| = n!$ y que no es abeliano si $n > 2$ (S_2 es trivialmente abeliano). Por ejemplo, para las permutaciones $\sigma, \tau \in S_3$ definidas por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

se cumple

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Recuérdese que $\sigma\tau$ significa $\sigma \circ \tau$, es decir, hay que aplicar primero τ y después σ sobre el conjunto $\{1,2,3\}$. Para componer dos permutaciones es útil hacerse un diagrama con flechas de la acción de cada uno de ellos, en nuestro caso

$$\sigma\tau :\ \begin{array}{ccccc} 1 & - & 1 & & 1 \\ 2 & & 2 & \times & 2 \\ 3 & \times & 3 & - & 3 \\ & \tau & & \sigma & \end{array} \Rightarrow\ \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \tau\sigma :\ \begin{array}{ccccc} 1 & & 1 & - & 1 \\ 2 & \times & 2 & & 2 \\ 3 & - & 3 & \times & 3 \\ & \sigma & & \tau & \end{array} \Rightarrow\ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Para hallar el inverso de una permutación basta seguir las flechas en sentido contrario, por ejemplo, el inverso de $\sigma\tau$ es

$$(\sigma\tau)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Nótese que $(\sigma\tau)^{-1}$ coincide con $\tau^{-1}\sigma^{-1}$.

Veamos ahora algunas definiciones. La primera intenta dar la noción de un grupo contenido en otro.

DEFINICIÓN: *Se dice que un subconjunto no vacío, H, de un grupo G es un* subgrupo *de G si*

$$1)\ g,h\in H \ \Rightarrow\ gh\in H \qquad 2)\ g\in H \ \Rightarrow\ g^{-1}\in H.$$

A veces se escribe $H < G$ o $H \le G$ o simplemente $H\subset G$ para indicar que H es un subgrupo de G. La primera notación puede dar lugar a confusión porque G es un subgrupo de sí mismo.

Ejemplo 1. $H_1 = \{\overline{0},\overline{2},\overline{4}\}$ es un subgrupo de $\mathbb{Z}_6$.

Ejemplo 2. $H_2 = \Big\{\text{Id}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\Big\}$ es un subgrupo de S_3.

Ejemplo 3. $H_3 = \{\overline{1},\overline{3},\overline{9}\}$ es un subgrupo de $\mathbb{Z}_{13}^*$.

DEFINICIÓN: *Si H es un subgrupo de G, al número $[G:H]=|G|/|H|$ se le llama* índice* *del sugrupo.*

Más adelante demostraremos que el índice es siempre un entero, lo cual no es en absoluto evidente. Como un reto (bastante difícil) para el lector, sugerimos que intente probar esta propiedad.

Ejemplo . En los ejemplos anteriores se tiene

$$[\mathbb{Z}_6:H_1]=\frac{6}{3}=2, \qquad [S_3:H_2]=\frac{3!}{2}=3, \qquad [\mathbb{Z}_{13}^*:H_3]=\frac{12}{3}=4.$$

Las condiciones 1) y 2) en la definición de sugrupo se pueden reducir a una sola. Esto no es algo demasido importante, pero lo demostraremos para ejercitarnos en el manejo de la definición de subgrupo.

Proposición 1.1 : *Un subconjunto no vacío, H, es un subgrupo de G si y sólo si $h_1h_2^{-1}\in H$ para todo $h_1,h_2\in H$.*

DEM.:

$\Rightarrow$) Dados $h_1,h_2\in H$, 2) $\Rightarrow h_2^{-1}\in H$ y 1) $\Rightarrow h_1h_2^{-1}\in H$.

* Normalmente se define el índice como el cardinal de cierto conjunto cociente (de clases de equivalencia) y después se prueba que coincide con la fórmula aquí dada; no obstante, para no complicar la exposición en esta incursión tan breve en la teoría de grupos, preferimos comenzar con esta definición menos conveniente pero más operativa y fácil de entender.

$\Leftarrow$) Tomando $h_1 = h_2$, $h_1 h_2^{-1} \in H \Rightarrow e \in H$, tomando ahora $h_1 = e \in H$ y $h_2 = g \in H$ arbitrario, se tiene $g^{-1} \in H$, es decir 2). Ahora si $h^{-1} \in H$ para todo $h \in H$, tomando $h_1 = g \in H$ y $h_2 = h^{-1} \in H$, se concluye $g(h^{-1})^{-1} = gh \in H$, esto es, 1). $\blacksquare$

Ejemplo . Si $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, entonces $S = \{\mathrm{Id}, \tau\}$ no es un subgrupo de S_3 porque

$\mathrm{Id}\,\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \notin S$.

Definición: *Sea S un subconjunto no vacío de un grupo G. Se dice que H es el subgrupo generado por S, y se escribe $H = \langle S \rangle$, si H es el menor subgrupo de G (en el sentido de la inclusión) que contiene a S.*

Observación: No es difícil convencerse de que

$$\langle S \rangle = \{g_1 g_2 \dots g_r \,/\, g_i \in S \text{ ó } g_i^{-1} \in S\},$$

pero esto puede ser de poca ayuda a la hora de calcular $\langle S \rangle$ (sobre todo en grupos no abelianos infinitos o de orden muy grande) porque no hay ninguna cota *a priori* para la longitud máxima, r, de los productos $g_1 g_2 \dots g_r$. Es decir, un conjunto pequeño puede generar un subgrupo grande e incluso infinito.

Nota: Como S es un conjunto, si lo representamos de forma explícita citando sus elementos, debiéramos escribirlos entre llaves, pero habitualmente se suprimen para mayor simplicidad de la notación.

Ejemplo 1. Si S es como en el último ejemplo, $\langle S \rangle = \{\mathrm{Id}, \tau, \tau^{-1}\}$. En cierto sentido, τ^{-1} es lo único que le falta a S para ser un subgrupo.

Ejemplo 2. Hallar $H = \langle \overline{13} \rangle$ en $\mathbb{Z}_{17}^*$.

Como $\overline{13} \in H$, entonces $\overline{13} \cdot \overline{13} = \overline{16} \in H \Rightarrow \overline{13} \cdot \overline{16} = \overline{4} \in H \Rightarrow \overline{13} \cdot \overline{4} = \overline{1} \in H$. Es decir, $\{\overline{1}, \overline{4}, \overline{13}, \overline{16}\} \subset H$ pero este conjunto es ya un subgrupo (ejercicio: comprobarlo) por tanto $H = \{\overline{1}, \overline{4}, \overline{13}, \overline{16}\}$.

Ejemplo 3. Hallar $H = \langle \sigma, \tau \rangle$ en S_3, donde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{y} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Nótese que $\sigma^2 = \tau^2 = \mathrm{Id}$. Para generar nuevos elementos de H multiplicamos σ y τ

entre sí, obteniendo

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in H \quad \text{y} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in H.$$

Por tanto $\{\mathrm{Id}, \sigma, \tau, \sigma\tau, \tau\sigma\} \subset H$. Como $H \subset S_3$ y $|S_3| = 6$, H sólo puede tener un elemento más. Un cálculo prueba

$$\sigma\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

y se tiene $H = S_3$.

Como hemos visto, la palabra "orden" cuando se aplica a grupos significa el cardinal, pero cuando se aplica a un elemento de un grupo su significado es aparentemente bien distinto.

DEFINICIÓN: *Si G es un grupo finito, el* <u>*orden*</u> *de $g \in G$ es el menor entero positivo, n, tal que $g^n = e$.*

<u>Observación</u>: Nótese que el orden de $g \in G$ coincide con el orden del subgrupo generado por g, de ahí que se use la misma terminología.

La misma definición sirve para grupos infinitos, pero en ellos la existencia del orden de un elemento no está asegurada, por ejemplo, en $(\mathbb{R} - \{0\}, \cdot)$, tenemos que $3 \in \mathbb{R} - \{0\}$ pero $3^n \neq 1$ para cualquier entero positivo, n. En este caso se dice que el elemento tiene orden infinito.

El siguiente sencillo resultado implica que esto no puede ocurrir en grupos finitos.

Proposición 1.2 : *Sea G un grupo finito y sea $g \in G$, entonces para algún entero positivo, n, se tiene $g^n = e$.*

<u>Observación</u>: La proposición también se puede formular diciendo que cada elemento de un grupo finito tiene siempre orden finito.

<u>DEM.</u>: Como G es finito, hay elementos iguales en la sucesión

$$g^1,\ g^2,\ g^3,\ g^4,\ g^5,\ \ldots$$

pero $g^n = g^m$ con $m > n \Rightarrow g^{m-n} = e$. ■

Incluso un resultado tan elemental como éste sirve para ilustrar la versatilidad de la teoría de grupos. La proposición anterior se transforma en un teorema aparentemente diferente para cada grupo.

<u>Ejemplo 1</u>. Demostrar que existe una potencia de 2 ($\neq 2^0$) que deja resto 1 al ser dividida por 85.

Hay que probar $2^n \equiv 1\ (85)$, es decir $\overline{2}^n = \overline{1}$ en $\mathbb{Z}_{85}^*$ ($\overline{2} \in \mathbb{Z}_{85}^*$ porque 2 y 85 son primos entre sí) y esto se deduce de la proposición con $G = \mathbb{Z}_{85}^*$.

Ejemplo 2. Cualquier permutación de los elementos de un conjunto ordenado $A = (a_1, a_2, \ldots, a_n)$, si la aplicamos cierto número de veces deja dicho conjunto invariante. Esto es una consecuencia de la proposición con $G = S_n$.

4.2. Homomorfismos, núcleo e imagen

Una vez que hemos definido los grupos como conjuntos que tienen una estructura especial, es natural considerar funciones que preservan esa estructura; es decir, las funciones que transforman grupos en grupos.

Definición: *Sean G y G' grupos, decimos que una función $\phi : G \longrightarrow G'$ es un homomorfismo de grupos si para todo $g_1, g_2 \in G$ se cumple $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.*

Observación: Nótese que en la igualdad $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$, utilizamos la operación de grupo de G para calcular $g_1 g_2$, y la de G' para calcular $\phi(g_1)\phi(g_2)$. Estas operaciones pueden ser bien distintas.

No es difícil comprobar (ejercicio) que si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos, se cumple $\phi(e) = e'$, donde e y e' son los elementos neutros en G y G' respectivamente. También se cumple $\phi(g^{-1}) = (\phi(g))^{-1}$.

Ejemplo 1. La función $\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ definida por $\phi(\overline{x}) = \overline{2x}$ es un homomorfismo, porque

$$\phi(\overline{x} + \overline{y}) = \overline{2(x+y)} = \overline{2x} + \overline{2y} \qquad \phi(x) + \phi(y) = \overline{2x} + \overline{2y}.$$

Ejemplo 2. La función $\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ definida por $\phi(\overline{x}) = \overline{x}^2$ no es un homomorfismo porque, por ejemplo,

$$\phi(\overline{1} + \overline{2}) = \phi(\overline{3}) = \overline{9} = \overline{3} \quad \text{pero} \quad \phi(\overline{1}) + \phi(\overline{2}) = \overline{1} + \overline{4} = \overline{5}.$$

Ejemplo 3. La función $\phi : \mathbb{Z}_2 \longrightarrow S_4$ definida por

$$\phi(\overline{0}) = \mathrm{Id} \quad \text{y} \quad \phi(\overline{1}) = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

es un homomorfismo. Para comprobarlo basta observar los siguientes cálculos

$$\begin{array}{ll} \phi(\overline{0} + \overline{0}) = \phi(\overline{0})\phi(\overline{0}) = \mathrm{Id} & \phi(\overline{0} + \overline{1}) = \phi(\overline{0})\phi(\overline{1}) = \sigma \\ \phi(\overline{1} + \overline{0}) = \phi(\overline{1})\phi(\overline{0}) = \sigma & \phi(\overline{1} + \overline{1}) = \phi(\overline{1})\phi(\overline{1}) = \mathrm{Id}. \end{array}$$

No es difícil comprobar (ejercicio) que que la composición de dos homomorfismos es también un homomorfismo.

Al igual que distinguíamos funciones inyectivas, sobreyectivas y biyectivas; hay definiciones análogas para los homomorfismos, pero suelen utilizarse nombres diferentes.

DEFINICIÓN: *Un homomorfismo* $\phi : G \longrightarrow G'$ *se dice que es:*

i) Un <u>monomorfismo</u> *si* ϕ *es una función inyectiva.*

ii) Un <u>epimorfismo</u> *si* ϕ *es una función sobreyectiva.*

iii) Un <u>isomorfismo</u> *si* ϕ *es una función biyectiva.*

DEFINICIÓN: *Si existe un isomorfismo* $\phi : G \longrightarrow G'$ *se dice que los grupos* G *y* G' *son* <u>isomorfos</u> *y se suele escribir* $G \cong G'$.

Hay dos conjuntos que están estrechamente relacionados con la clasificación anterior de homomorfismos, ambos están recogidos en la siguiente definición.

DEFINICIÓN: *Se llama* <u>núcleo</u> *de un homomorfismo* $\phi : G \longrightarrow G'$, *al conjunto*

$$\operatorname{Nuc}\phi = \{g \in G \,/\, \phi(g) = e'\}$$

donde e' *es el elemento neutro de* G', *y se llama* <u>imagen</u> *de* ϕ *a* $\phi(G)$, *es decir, al conjunto*

$$\operatorname{Im}\phi = \{g' \in G' \,/\, g' = \phi(g) \text{ con } g \in G\}.$$

<u>Nota</u>: Otra forma bastante extendida para designar el núcleo es $\operatorname{Ker}\phi$.

Obviamente un homomorfismo $\phi : G \longrightarrow G'$ es un epimorfismo si y sólo si $G' = \operatorname{Im}\phi$. Por otra parte, se puede comprobar que ϕ es un monomorfismo con el siguiente resultado

Proposición 2.1 : *Un homomorfismo,* ϕ, *es un monomorfismo si y sólo si* $\operatorname{Nuc}\phi = \{e\}$.

<u>DEM.</u>:

$\Rightarrow$) Si no se cumpliera $\operatorname{Nuc}\phi = \{e\}$ entonces existiría $g \neq e$ tal que $\phi(g) = e' = \phi(e)$ y por tanto ϕ no sería una función inyectiva.

$\Leftarrow$) Si ϕ no fuera una función inyectiva, existirían $g_1 \neq g_2$ tales que $\phi(g_1) = \phi(g_2)$, y esto implica $e' = \phi(g_1)\big(\phi(g_2)\big)^{-1} = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1 g_2^{-1})$ y como $g_1 g_2^{-1} \neq e$, se tiene $\operatorname{Nuc}\phi \neq \{e\}$. ■

Proposición 2.2 : *Si* $\phi : G \longrightarrow G'$ *es un homomorfismo entonces* $\operatorname{Im}\phi$ *es un subgrupo de* G' *y* $\operatorname{Nuc}\phi$ *es un subgrupo de* G.

<u>DEM.</u>: Nótese que

$$h_1, h_2 \in \operatorname{Im}\phi \;\Rightarrow\; h_1 = \phi(g_1),\; h_2 = \phi(g_2) \;\Rightarrow\; h_1 h_2^{-1} = \phi(g_1 g_2^{-1}) \in \operatorname{Im}\phi.$$

También se tiene

$$g_1, g_2 \in \operatorname{Nuc}\phi \;\Rightarrow\; \phi(g_1) = \phi(g_2) = e \;\Rightarrow\; \phi(g_1 g_2^{-1}) = e \;\Rightarrow\; g_1 g_2^{-1} \in \operatorname{Nuc}\phi.$$

Por la Proposición 2.1, esto prueba el resultado. ■

Ejemplo 1. El homomorfismo $\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$ definido por $\phi(\overline{x}) = \overline{2x}$ no es un monomorfismo porque $\overline{3} \in \operatorname{Nuc}\phi$ (ya que $\overline{2 \cdot 3} = \overline{0}$ en $\mathbb{Z}_6$). Dando valores a ϕ se comprueba

$$\operatorname{Nuc}\phi = \{\overline{0}, \overline{3}\} \qquad \operatorname{Im}\phi = \{\overline{0}, \overline{2}, \overline{4}\},$$

como $\operatorname{Im}\phi \neq \mathbb{Z}_6$ tampoco es epimorfismo. Nótese que $\operatorname{Im}\phi$ y $\operatorname{Nuc}\phi$ son subgrupos de $\mathbb{Z}_6$, tal como asegura la Proposición 2.2.

Ejemplo 2. En la primera sección habíamos considerado el grupo de giros alrededor del origen y el grupo de números complejos de módulo uno, llamemos a estos grupos G y G' respectivamente y consideremos la función $\phi : G \longrightarrow G'$ definida por $\phi(g_\alpha) = \cos\alpha + i \operatorname{sen}\alpha$ donde g_α es el giro de ángulo α. Veamos que ϕ es un isomorfismo y por tanto $G \cong G'$.

i) Es un homomorfismo, porque

$$\begin{aligned}
\phi(g_\alpha g_\beta) =& \phi(g_{\alpha+\beta}) = \cos(\alpha+\beta) + i \operatorname{sen}(\alpha+\beta) \\
\phi(g_{\alpha+\beta}) =& (\cos\alpha + i \operatorname{sen}\alpha)(\cos\beta + i \operatorname{sen}\beta) \\
=& (\cos\alpha\cos\beta - \operatorname{sen}\alpha \operatorname{sen}\beta) + i(\operatorname{sen}\alpha\cos\beta + \operatorname{sen}\beta\cos\alpha)
\end{aligned}$$

y las fórmulas de adición para cos y sen implican $\phi(g_\alpha g_\beta) = \phi(g_\alpha)\phi(g_\beta)$.

ii) Es un monomorfismo, porque

$$g_\alpha \in \operatorname{Nuc}\phi \Leftrightarrow \cos\alpha + i \operatorname{sen}\alpha = 0 \Leftrightarrow \alpha = 360^o k \Leftrightarrow g_\alpha = e.$$

iii) Es un epimorfismo, porque $|x+iy| = 1 \Rightarrow x^2 + y^2 = 1 \Rightarrow (x, y)$ pertenece a la circunferencia de radio uno $\Rightarrow x = \cos\alpha$, $y = \operatorname{sen}\alpha$ para algún α. Con esto hemos demostrado que para cualquiere número complejo de módulo uno, $x + iy$, existe α tal que $\phi(g_\alpha) = x + iy$, por tanto $\operatorname{Im}\phi = G'$

Ejemplo 3. También se puede comprobar que si G es como en el ejemplo anterior y G'' es el grupo de matrices introducido en el ejemplo 6 de la primera sección, la función $\phi : G \longrightarrow G''$ definida por

$$\phi(g_\alpha) = \begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}$$

también es un isomorfismo.

Ejemplo 4. La función $\phi : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_5^*$ definida por $\phi(\overline{x}) = \overline{2}^x$ es un epimorfismo pero no un monomorfismo. Nótese que no es claro que ϕ sea una función bien definida ya que, por ejemplo, $\overline{1} = \overline{9}$ en $\mathbb{Z}_8$ y esto define $\phi(\overline{1})$ simultáneamente como $\overline{2}^1$ y $\overline{2}^9$.

i) ϕ está bien definida: Si $\overline{x} = \overline{y}$ en $\mathbb{Z}_8$ tenemos que probar que $\overline{2}^x = \overline{2}^y$ en $\mathbb{Z}_5^*$. $\overline{x} = \overline{y}$

$\Rightarrow x = y + 8k$, y como $\overline{2}^8 = 1$ en $\mathbb{Z}_5^*$, se tiene $\overline{2}^8 = \overline{1}$ en $\mathbb{Z}_5^*$ y $\overline{2}^x = \overline{2}^{y+8k} = \overline{2}\big(\overline{2}^8\big)^k = \overline{2}^y$.

ii) ϕ es un homomorfismo porque

$$\phi(\overline{x}+\overline{y}) = \overline{2}^{x+y} = \overline{2}^x \cdot \overline{2}^y \qquad \phi(\overline{x})\phi(\overline{y}) = \overline{2}^x \cdot \overline{2}^y.$$

iii) ϕ es un epimorfismo porque $\overline{1} = \phi(\overline{0})$, $\overline{2} = \phi(\overline{1})$, $\overline{3} = \phi(\overline{3})$, $\overline{4} = \phi(\overline{2})$, así que $\operatorname{Im}\phi \supset \mathbb{Z}_5^* \Rightarrow \operatorname{Im}\phi = \mathbb{Z}_5^*$.

iv) ϕ no es un monomorfismo porque, por ejemplo, $\phi(\overline{0}) = \phi(\overline{4})$. De hecho, se tiene que $\operatorname{Nuc}\phi = \{\overline{0}, \overline{4}\}$.

Ejemplo 5. El homomorfismo $\phi : S_n \longrightarrow S_{n+1}$ que pasa cada permutación de $\{1, 2, \ldots, n\}$ a otra de $\{1, 2, \ldots, n, n+1\}$ que actúa de la misma manera pero dejando fijo $n+1$, es decir

$$\phi\left(\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix} \right) = \begin{pmatrix} 1 & 2 & 3 & \ldots & n & n+1 \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) & n+1 \end{pmatrix},$$

es un monomorfismo pero no un epimorfismo.

Ejemplo 6. El homomorfismo $\phi : \mathbb{Z}_7^* \longrightarrow \mathbb{Z}_7^*$ definido por $\phi(\overline{x}) = \overline{x}^2$ no es un monomorfismo, ya que $-\overline{1} = \overline{6} \in \operatorname{Nuc}\phi$. Sin necesidad de hacer ningún cálculo más, se puede concluir que ϕ no es un epimorfismo, ya que si lo fuera $\phi(\mathbb{Z}_7^*) = \mathbb{Z}_7^* \Rightarrow \phi(\mathbb{Z}_7^* - \{\overline{1}, \overline{6}\}) \supset \mathbb{Z}_7^* - \{\overline{1}\}$ (porque $\phi(\overline{1}) = \phi(\overline{6}) = \overline{1}$) y esto es imposible porque $\mathbb{Z}_7^* - \{\overline{1}, \overline{6}\}$ tiene cuatro elementos y $\mathbb{Z}_7^* - \{\overline{1}\}$ tiene cinco elementos.

Ejemplo 7. El homomorfismo $\phi : \mathbb{Z}_7^* \longrightarrow \mathbb{Z}_7^*$ definido por $\phi(\overline{x}) = \overline{x}^5$ es un isomorfismo. Para comprobarlo basta observar la tabla de valores

$$\phi(\overline{1}) = \overline{1}, \quad \phi(\overline{2}) = \overline{4}, \quad \phi(\overline{3}) = \overline{5}, \quad \phi(\overline{4}) = \overline{2}, \quad \phi(\overline{5}) = \overline{3}, \quad \phi(\overline{6}) = \overline{6};$$

de la que se deduce $\operatorname{Im}\phi = \mathbb{Z}_7^*$ y $\operatorname{Nuc}\phi = \{\overline{1}\}$. Los isomorfismos, como éste, de un grupo en sí mismo se llaman automorfismos.

4.3. Subgrupos normales, grupo cociente

Los conceptos subgrupo normal y grupo cociente suelen ser los más difíciles de entender para el principiante en la teoría de grupos. Por ello no está de más comenzar con algunas consideraciones elementales y ejemplos.

Recordemos primero cómo habíamos definido $\mathbb{Z}_n$, por ejemplo $\mathbb{Z}_3$. Los elementos de $\mathbb{Z}_3$ son $\overline{0}$, $\overline{1}$ y $\overline{2}$. Cada uno de ellos es en realidad una clase de equivalencia que contiene a infinitos enteros. Así se tiene $\overline{1} = \{1, 4, 7, \ldots, -2, -5, \ldots\}$ o de forma más breve, pero poco rigurosa, podemos escribir $\overline{1} = 1 + 3\mathbb{Z}$. Cada número entero es un elemento de alguna clase, concretamente

$$\mathbb{Z} = \bigcup_{a=1,2,3} a + 3\mathbb{Z} = \bigcup_{a=1,2,3} \overline{a}.$$

De modo que podemos entender que $\mathbb{Z}_3$ es el resultado de "factorizar" (descomponer) $\mathbb{Z}$ en tres clases de equivalencia, donde la relación viene dada por el grupo $3\mathbb{Z}$. Por ello muchas se usa la notación $\mathbb{Z}/3\mathbb{Z}$ en lugar de $\mathbb{Z}_3$.

Después del ejemplo anterior, se deduce que $\mathbb{Z}_n$ es en realidad como el grupo de los enteros salvo sumar elementos del grupo $n\mathbb{Z}$. Dado un grupo general, G, con la estructura multiplicativa esto sugiere intentar "factorizarlo" definiendo lo que llamaremos el grupo cociente por un subgrupo, H, y que consiste en considerar los elementos de G salvo multiplicar por elementos de H. Sin embargo, por algunos problemas técnicos que sólo aparecen en grupos no abelianos, el grupo cociente puede no existir para muchos de los subgrupos, lo que provoca que la situación sea mucho más complicada que en el caso de $\mathbb{Z}_n$.

Insistiendo en la idea de que $\overline{a} \in \mathbb{Z}_3$ es "igual" a $a \in \mathbb{Z}$ salvo sumar un elemento de $3\mathbb{Z}$, tratemos de copiar la misma definición cambiando $\mathbb{Z}$ por G, $3\mathbb{Z}$ por un subgrupo, H, de G y la operación $+$ por la operación $\cdot$ de G. El análogo de $\mathbb{Z}_3$ vendría dado ahora por la siguiente definición

DEFINICIÓN: *Sea H un subgrupo de G, se llama* <u>conjunto de cogrupos por la izquierda</u> *y se denota por G/H, al conjunto cuyos elementos son $[g] = gH$ con $g \in G$.*

<u>Observación</u>: Con gH se quiere indicar el conjunto obtenido al multiplicar g por cada elemento de H. Nótese que diferentes elementos g pueden dar lugar a la misma clase (igual que en $\mathbb{Z}_3$ se tiene $\overline{2} = \overline{5}$).

<u>Nota</u>: Como veremos más adelante, la notación G/H tiene cierta ambigüedad, por ello algunos autores escriben $(G/H)_i$. También otros nombran este conjunto como <u>coclases por la izquierda</u> o simplemente <u>clases por la izquierda</u>. Todas estas notaciones son equivalentes.

Quizá el lector esté un poco sorprendido porque hemos llamado "clase" al conjunto $[g] = gH$. La razón es la siguiente

Proposición 3.1 : *Dado un grupo G y H uno de sus subgrupos, la relación $g_1 \mathcal{R} g_2$ (con $g_1, g_2 \in G$) definida por $g_1 \mathcal{R} g_2 \Leftrightarrow g_1 \in g_2 H$, es de equivalencia, y sus clases son $[g] = gH$.*

<u>Ejemplo</u> . Tomando $G = \mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ y H el subgrupo $H = \{\overline{1}, \overline{6}\}$. Al calcular gH para todos los $g \in G$ se tiene

$$\left.\begin{matrix}\overline{1}H \\ \overline{6}H\end{matrix}\right\} = H = \{\overline{1}, \overline{6}\} \qquad \left.\begin{matrix}\overline{2}H \\ \overline{5}H\end{matrix}\right\} = \{\overline{2}, \overline{5}\} \qquad \left.\begin{matrix}\overline{3}H \\ \overline{4}H\end{matrix}\right\} = \{\overline{3}, \overline{4}\}$$

Por tanto sólo hay tres cogrupos (o clases) distintos $[\overline{1}] = [\overline{6}]$, $[\overline{2}] = [\overline{5}]$ y $[\overline{3}] = [\overline{4}]$. Así pues

$$G/H = \{[\overline{1}], [\overline{2}], [\overline{3}]\}.$$

El principal problema técnico es que también se puede dar una definición para zurdos (¿o diestros?) de los cogrupos, y si el grupo no es abeliano no tiene por qué coincidir con la anterior. Esto causa que habitualmente los cogrupos no sean un grupo, lo que reduce su interés.

DEFINICIÓN: *Sea H un subgrupo de G se llama* conjunto de cogrupos por la derecha *y se denota con $H\backslash G$, al conjunto formado por las clases $[g] = Hg$ con $g \in G$.*

Nota: De nuevo, otras notaciones para referirse a $H\backslash G$ son coclases por la derecha o simplemente clases por la derecha. También se escribe a veces $(G/H)_d$.

El análogo de la anterior proposición también se cumple en este contexto definiendo $g_1 \mathcal{R} g_2$ (con $g_1, g_2 \in G$) como $g_1 \in Hg_2$.

Recuérdese que en una relación de equivalencia las clases definen una partición del conjunto, así pues podemos escribir

$$G = \bigcup_{[g]\in H\backslash G} [g] \qquad \text{y} \qquad G = \bigcup_{[g]\in G/H} [g].$$

Cada clase contiene $|H|$ elementos distintos (por ser de la forma gH ó Hg), si denotamos por $|G/H|$ y $|H\backslash G|$ el cardinal de los cogrupos por la izquierda y por la derecha, de las igualdades anteriores deducimos el siguiente resultado

Proposición 3.2 : *Para todo subgrupo H de G, se cumple*

$$|G| = |H| \cdot |H\backslash G| \qquad |G| = |H| \cdot |G/H|.$$

Observación: Nótese que esto implica que los cardinales de G/H y de $H\backslash G$ son iguales y coinciden con el índice $[G : H]$, lo cual se toma habitualmente como su definición. En particular, el índice es siempre un entero (positivo).

Una consecuencia importante del resultado anterior es

Teorema 3.3 (Teorema de Lagrange): *El orden de un subgrupo divide al orden del grupo, y el orden de un elemento divide al orden del grupo.*

Observación: Obsérvese que la segunda parte del teorema se deduce de la primera porque un elemento de orden n genera un subgrupo de orden n.

Ejemplo . En $\mathbb{Z}_{12}$, $\overline{2}$ tiene orden 6, $\overline{3}$ tiene orden 4, $\overline{4}$ tiene orden 3, etc. Todos estos órdenes dividen a $|\mathbb{Z}_{12}| = 12$.

Observación: Para hacer notar la profundidad del teorema anterior, obsérvese la siguiente cadena de implicaciones que demuestra en una línea el pequeño teorema de Fermat a partir del Teorema de Lagrange

$$|\mathbb{Z}_p^*| = p - 1 \Rightarrow \overline{a}^{p-1} = \overline{1} \;\; \forall \overline{a} \in \mathbb{Z}_p^* \Rightarrow a^{p-1} \equiv 1 \ (p) \text{ si } p \not| a \Rightarrow a^p \equiv a \ (p).$$

También el teorema de Euler-Fermat admite una brevísima demostración a través del teorema de Lagrange si suponemos conocido $|\mathbb{Z}_n^*| = \phi(n)$.

$|\mathbb{Z}_n^*| = \phi(n) \Rightarrow \overline{a}^{\phi(n)} = \overline{1} \;\; \forall \overline{a} \in \mathbb{Z}_n^* \Rightarrow a^{\phi(n)} \equiv 1 \;(n)$ si a y n son primos entre sí.

Hasta ahora hemos conseguido definir unos conjuntos un tanto extraños que permiten "dividir" G a través de H. Al igual que en $\mathbb{Z}$ al factorizar por el subgrupo $3\mathbb{Z}$ obtenemos un nuevo grupo, $\mathbb{Z}_3$, la idea de todo este procedimiento es que el resultado de dividir G por H debiera ser otro grupo. Resulta que esto no es así en general, a veces G/H y $H\backslash G$ son grupos y a veces no. Veamos la situación sobre dos ejemplos.

Ejemplo 1. Tomemos $G = S_3 = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ y $H = \{\mathrm{Id}, \sigma_1\}$ donde $\sigma_1, \sigma_2, \sigma_3$ son las permutaciones que dejan fijo 1, 2 y 3, respectivamente e intercambian los otros dos elementos y

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Algunos cálculos prueban que

$$\left.\begin{matrix} \mathrm{Id}\, H \\ \sigma_1 H \end{matrix}\right\} = H = \{\mathrm{Id}, \sigma_1\} \qquad \left.\begin{matrix} \sigma_2 H \\ \sigma_5 H \end{matrix}\right\} = \{\sigma_2, \sigma_5\} \qquad \left.\begin{matrix} \sigma_3 H \\ \sigma_4 H \end{matrix}\right\} = \{\sigma_3, \sigma_4\}.$$

Por tanto los cogrupos por la izquierda son $G/H = \{[\mathrm{Id}], [\sigma_2], [\sigma_3]\}$.

La única operación que tenemos es la de de G así que uno debiera definir la multiplicación en G/H como

$$[\sigma] \cdot [\tau] = [\sigma\tau].$$

Por tanto, como $\sigma_2\sigma_3 = \sigma_4$, tendría que cumplirse

$$[\sigma_2] \cdot [\sigma_3] = [\sigma_2\sigma_3] = [\sigma_4] = [\sigma_3],$$

y esto implicaría que $[\sigma_2]$ es el elemento neutro, lo cual no es cierto ya que $[\sigma_2] \neq [\mathrm{Id}]$. Otra manera de obtener una contradicción, todavía más evidente, es notar $[\sigma_2] = [\sigma_5]$ y entonces $\sigma_2\sigma_3 = \sigma_4$ y $\sigma_5\sigma_3 = \sigma_1$ implican simultáneamente

$$[\sigma_2] \cdot [\sigma_3] = [\sigma_4] = [\sigma_3], \qquad [\sigma_2] \cdot [\sigma_3] = [\sigma_1],$$

Por tanto la operación ni siquiera está bien definida, el resultado depende de los representantes que elijamos para representar cada clase.

Veamos ahora cómo en el ejemplo que dimos tras la Proposición 3.1 todo parece funcionar bien.

Ejemplo 2. Recuérdese que si $G = \mathbb{Z}_7^*$ y H el subgrupo $H = \{\overline{1}, \overline{6}\}$, entonces $G/H = \{[\overline{1}], [\overline{2}], [\overline{3}]\}$. De nuevo, la operación que podemos definir en G/H viene dada por

$$[\overline{x}] \cdot [\overline{y}] = [\overline{xy}].$$

Con algunos ejemplos parece que la definición de esta operación es adecuada y que, por tanto, G/H hereda todas las propiedades de grupo de $\mathbb{Z}_7^*$. Así por ejemplo, $[\overline{2}] = [\overline{5}]$ y se tiene

$$[\overline{2}] \cdot [\overline{3}] = [\overline{6}] = [\overline{1}], \qquad [\overline{5}] \cdot [\overline{3}] = [\overline{15}] = [\overline{1}].$$

Obviamente la operación en G/H es conmutativa, así que la tabla de multiplicación en G/H queda totalmente determinada por

$$\begin{array}{lll} [\overline{1}] \cdot [\overline{1}] = [\overline{1}] & [\overline{1}] \cdot [\overline{2}] = [\overline{2}] & [\overline{1}] \cdot [\overline{3}] = [\overline{3}] \\ [\overline{2}] \cdot [\overline{2}] = [\overline{4}] = [\overline{3}] & [\overline{2}] \cdot [\overline{3}] = [\overline{6}] = [\overline{1}] & [\overline{3}] \cdot [\overline{3}] = [\overline{2}] \end{array}$$

Con esta tabla no es difícil deducir de que G es un grupo de tres elementos generado por $[\overline{2}]$ y por tanto isomorfo a $\mathbb{Z}_3$.

Si uno es capaz de superar la abstracción de todas estas definiciones, no es difícil percatarse de que esta situación tiene algo que ver con la conmutatividad. Obsérvese que si G es conmutativo, no hay ninguna dificultad en definir $[g_1] \cdot [g_2]$ como $[g_1 g_2]$, porque (véase la definición de las clases) $g_1 H \cdot g_2 H = g_1 g_2 H$. Sin embargo si G no es conmutativo pudiera ocurrir (como en el primer ejemplo) que $g_1 H \cdot g_2 H \neq g_1 g_2 H$. Este mismo razonamiento sugiere que sólo es necesaria la conmutatividad con H, esto es, lo necesario para escribir $H g_2 = g_2 H$, y por tanto que G/H va a tener una estructura de grupo sin más que tomemos H de manera que los elementos de G conmuten con él. Eso nos lleva a la definición fundamental de esta sección

DEFINICIÓN: *Si G es un grupo, se dice que un subgrupo, H, es un subgrupo normal de G si para todo $g \in G$ las clases de g por la derecha y por la izquierda coinciden, es decir, si $gH = Hg$.*

Proposición 3.4 : *G/H es un grupo (con el producto de clases $[g_1] \cdot [g_2] = [g_1 g_2]$) si y sólo si H es un subgrupo normal de G.*

DEM.: $\Rightarrow$) Si H no fuera normal, existiría g tal que $gH \neq Hg$, por tanto existiría $h \in H$ tal que $ghg^{-1} \notin H$, o lo que es lo mismo, $[ghg^{-1}] \neq [e]$. Lo cual contradice la cadena de igualdades

$$[ghg^{-1}] = [g][h][g^{-1}] = [g][e][g^{-1}] = [geg^{-1}] = [e].$$

$\Leftarrow$) Basta demostrar que la operación $[g_1][g_2] = [g_1 g_2]$ está bien definida, es decir, que

$$[g_1] = [g_1'], \quad [g_2] = [g_2'], \quad \Rightarrow \quad [g_1 g_2] = [g_1' g_2'].$$

Si esto se cumple, las propiedades de grupo de G implican las correspondientes de G/H; por ejemplo, $[e]$ es el elemento neutro, $[g^{-1}]$ es el inverso, etc.

Si $[g_1] = [g_1']$ y $[g_2] = [g_2']$, entonces $g_1H = g_1'H$ y $g_2H = g_2'H$. Además, como H es normal $g_2'H = Hg_2'$, por tanto

$$[g_1g_2] = g_1g_2H = g_1g_2'H = g_1Hg_2' = g_1'Hg_2' = g_1'g_2'H = [g_1'g_2'].$$

Lo cual completa la demostración. ■

Definición: *Si H es un subgrupo normal de G, entonces al grupo G/H (que coincide con $H\backslash G$) se le llama* <u>grupo cociente</u>.

<u>Observación</u>: Según la Proposición 3.2 el orden de G/H es $[G:H] = |G|/|H|$.

<u>Nota</u>: Como ya hemos comentado con anterioridad, hay una leve ambigüedad en la notación, porque el mismo símbolo, G/H, sirve para designar el grupo cociente (lo que requiere que el subgrupo sea normal) y los cogrupos a la izquierda (que existen para cualquier subgrupo).

Hay una manera equivalente a la definición de comprobar si un subgrupo es normal

Proposición 3.5 : *H es un subgrupo normal de G $\Leftrightarrow$ $g^{-1}hg \in H$ para todo $g \in G$ y todo $h \in H$.*

<u>Dem.</u>: Nótese que $g^{-1}hg \in H\ \forall h \in H$ equivale a $g^{-1}Hg \subset H$ y por tanto a $Hg \subset gH$. Como g es arbitrario, tomando en su lugar g^{-1} también se tiene $gHg^{-1} \subset H$, de donde $gH \subset Hg$. Estas inclusiones equivalen a $gH = Hg$, o lo que es lo mismo, a que H es normal. ■

De aquí o de la propia definición se deduce

Corolario 3.6: *Todo subgrupo de un grupo abeliano es normal.*

<u>Ejemplo 3</u>. Del corolario se deduce que el subgrupo del ejemplo 2 es normal.

<u>Ejemplo 4</u>. El subgrupo H de S_3 del ejemplo 1 no es normal, ya que tomando $g = \sigma_3$

$$g^{-1}Hg = \sigma_3^{-1}H\sigma_3 = \sigma_3^{-1}H\sigma_3 = \sigma_3\{\mathrm{Id}\sigma_1\}\sigma_3 = \{\sigma_3\sigma_3, \sigma_3\sigma_1\sigma_3\} = \{\mathrm{Id}\,\sigma_2\} \neq H$$

lo que contradice la conclusión de la Proposición 3.4.

<u>Ejemplo 5</u>. Con la notación del ejemplo 1, el subgrupo $\widetilde{H} = \{\mathrm{Id}, \sigma_4, \sigma_5\}$ es un subgrupo normal de S_3.

Si $g = \mathrm{Id}, \sigma_4, \sigma_5$, entonces $g, g^{-1} \in \widetilde{H}$ y por tanto se tiene

$$g^{-1}\widetilde{H}g = \widetilde{H}.$$

Si $g=\sigma_1,\sigma_2,\sigma_3$, entonces $g=g^{-1}$ y se reduce a un cálculo el comprobar

$$\sigma_1^{-1}H\sigma_1 = \{\mathrm{Id}, \sigma_1\sigma_4\sigma_1, \sigma_1\sigma_5\sigma_1\} = \widetilde{H}$$

$$\sigma_2^{-1}H\sigma_2 = \{\mathrm{Id}, \sigma_2\sigma_4\sigma_2, \sigma_2\sigma_5\sigma_2\} = \widetilde{H}$$

$$\sigma_3^{-1}H\sigma_3 = \{\mathrm{Id}, \sigma_3\sigma_4\sigma_3, \sigma_3\sigma_5\sigma_3\} = \widetilde{H}.$$

Ejemplo 6. El subgrupo de S_4, $H=\{\mathrm{Id},\tau\}$ donde τ es la permutación que intercambia 1 y 2 no es un subgrupo normal, porque tomando, por ejemplo, $\sigma=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$ se tiene

$$\sigma^{-1}H\sigma = \{\sigma^{-1}\sigma, \sigma^{-1}\tau\sigma\} = \left\{\mathrm{Id}, \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}\right\} \neq H.$$

Nota: Como curiosidad diremos que hay un teorema que afirma que para $n>4$, S_n sólo tiene un subgrupo normal aparte de $\{\mathrm{Id}\}$ y de él mismo.

Ya hemos comentado que la definición del grupo cociente G/H está motivada por la idea de "factorizar", en el sentido de subdividir, un grupo. Por otra parte, si tenemos un homomorfismo $\phi: G\longrightarrow G'$ podemos subdividir G en las clases de elementos que tienen la misma imagen. Ambas ideas se conjugan en el siguiente teorema que implica que muchas veces los grupos cocientes son isomorfos a otros grupos menos misteriosos.

Teorema 3.7 (del isomorfismo): *Si $\phi: G\longrightarrow G'$ es un homomorfismo de grupos, entonces $\mathrm{Nuc}\,\phi$ es un subgrupo normal de G y existe un isomorfismo*

$$\Phi: G/\mathrm{Nuc}\,\phi \longrightarrow \mathrm{Im}\,\phi$$

dado por $\Phi([g])=\phi(g)$.

Nótese que, intuitavemente, lo que afirma el teorema es que podemos transformar cualquier homomorfismo en un isomorfismo quitando de G' lo que no está en la imagen (para que sea epimorfismo) y "quitando" de G (en algún sentido) lo que está en el núcleo para que sea monomorfismo.

DEM.: Veamos primero que $\mathrm{Nuc}\,\phi$ es un subgrupo normal de G. Basta demostrar que $g^{-1}hg\in\mathrm{Nuc}\,\phi$ y esto es consecuencia de las siguientes implicaciones

$$\phi(h)=e' \Rightarrow (\phi(g))^{-1}\phi(h)\phi(g)=e' \Rightarrow \phi(g^{-1}hg)=e' \Rightarrow g^{-1}hg\in\mathrm{Nuc}\,\phi.$$

Si $[g_1]=[g_2]$ entonces $g_2\in g_1\mathrm{Nuc}\,\phi$ y por tanto $g_2=g_1h$ con $h\in\mathrm{Nuc}\,\phi$, así pues, $\Phi([g_2])=\phi(g_1h)=\phi(g_1)\phi(e)=\phi(g_1)=\Phi([g_1])$ y se tiene que Φ está bien definida. Por otra parte, es claro que Φ es un homomorfismo porque ϕ lo es.

Como los elementos de $\operatorname{Im}\phi$ son de la forma $\phi(g)$, Φ es obviamente un epimorfismo. También es un monomorfismo porque $\operatorname{Nuc}\phi = \{[g] \,/\, \phi(g) = e'\} = \{[g] \,/\, g \in \operatorname{Nuc}\phi\} = \{[e]\}$. Así pues, Φ es un isomorfismo. ■

Ejemplo . Comprobar el teorema del isomorfismo para $\phi : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_{11}^*$ definido por $\phi(\overline{x}) = \overline{10}^x$.

Recordando la definición de núcleo e imagen, tras algunos cálculos se tiene

$$\begin{aligned} \operatorname{Nuc}\phi =& \{\overline{x} \in \mathbb{Z}_{10} \,/\, \overline{10}^x = \overline{1} \text{ en } \mathbb{Z}_{11}^*\} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\} \\ \operatorname{Im}\phi =& \{\overline{y} \in \mathbb{Z}_{11}^* \,/\, \overline{y} = \overline{10}^x \text{ con } \overline{x} \in \mathbb{Z}_{10}\} = \{\overline{1}, \overline{10}\}. \end{aligned}$$

Como $\mathbb{Z}_{10}$ es abeliano, $\operatorname{Nuc}\phi$ es un subgrupo normal, además se tiene

$$\left.\begin{matrix} \overline{0}+H,\ \overline{2}+H,\ \overline{4}+H \\ \overline{6}+H, \overline{8}+H \end{matrix}\right\} = H \qquad \left.\begin{matrix} \overline{1}+H,\ \overline{3}+H,\ \overline{5}+H \\ \overline{7}+H, \overline{9}+H \end{matrix}\right\} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}\}$$

por tanto

$$G/\operatorname{Nuc}\phi = \{[\overline{0}], [\overline{1}]\}.$$

Los grupos $G/\operatorname{Nuc}\phi$ y $\operatorname{Im}\phi$ son claramente isomorfos enviando $[\overline{0}]$ a $\overline{1}$ y $[\overline{1}]$ a $\overline{10}$. Éste es justamente el isomorfismo, Φ, que aparece en el teorema

$$\Phi([\overline{0}]) = \phi(\overline{0}) = \overline{1} \qquad \Phi([\overline{1}]) = \phi(\overline{1}) = \overline{10}.$$

4.4. Grupos cíclicos, grupos de permutaciones, grupos diédricos

En esta sección estudiaremos tres familias de grupos que incluyen muchos de los ejemplos vistos hasta ahora. Para mayor claridad distinguiremos tres subsecciones correspondiendo a cada una de estas familias.

1. Grupos cíclicos:

Definición: *Se dice que un grupo, G, es* cíclico *si puede generararse con un solo elemento, es decir, si existe $g \in G$ tal que $\langle g \rangle = G$.*

Obsérvese que $\langle g \rangle$ sólo contiene a la identidad y potencias de g y de g^{-1}. Por tanto si G es cíclico

$$G = \langle g \rangle = \{g^n \,/\, n \in \mathbb{Z}\}$$

donde hemos usado el convenio de notación $g^0 = e$, $g^{-n} = (g^{-1})^n$. En particular, *todo grupo cíclico es abeliano.* También es fácil comprobar que *todo subgrupo de un grupo cíclico es también cíclico.*

Ejemplo 1. $\mathbb{Z}_n$ es cíclico porque $\overline{m} \in \mathbb{Z}_n \Rightarrow \overline{m} = \overline{1} + \overline{1} + \overset{m \text{ veces}}{\cdots\cdots} + \overline{1}$ y por tanto $\langle \overline{1} \rangle = \mathbb{Z}_n$. Un argumento similar demuestra que $\mathbb{Z}$ también es cíclico (los negativos se pueden obtener a partir de 1 tomando el inverso, que es -1).

Ejemplo 2. $\mathbb{Z}_5^*$ es cíclico, porque $\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{3}$, $\overline{2}^4 = \overline{1}$ implica $\langle \overline{2} \rangle = \mathbb{Z}_5^*$.

Ejemplo 3. $\mathbb{Z}_{14}^*$ es cíclico. Recuérdese que $\mathbb{Z}_{14}^*$ está formado por las clases, $\overline{n}$, invertibles módulo 14, y estas son aquellas con $\text{mcd}(n, 14) = 1$. Por consiguiente

$$\mathbb{Z}_{14}^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}.$$

Las igualdades $\overline{3}^1 = \overline{3}$, $\overline{3}^2 = \overline{9}$, $\overline{3}^3 = \overline{13}$, $\overline{3}^4 = \overline{11}$, $\overline{3}^5 = \overline{5}$, $\overline{3}^6 = \overline{1}$ implican $\langle \overline{3} \rangle = \mathbb{Z}_{14}^*$.

Ejemplo 4. $\mathbb{Z}_8^*$ no es cíclico. $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, como $\overline{3}^2 = \overline{1}$, $\overline{5}^2 = \overline{1}$, $\overline{7}^3 = \overline{1}$, ninguno de ellos genera los cuatro elementos de $\mathbb{Z}_8^*$.

Ejemplo 5. Es fácil comprobar que todos los elementos de S_3 distintos de la identidad tienen orden 2 ó 3, así pues ninguno genera S_3 que tiene orden 6; por tanto S_3 no es cíclico. Una forma más sencilla de llegar al mismo resultado es comprobar que S_3 no es abeliano.

Los grupos cíclicos tienen una estructura tan sencilla que no añaden nada nuevo al primer ejemplo que dimos. Concretamente, se tiene

Proposición 4.1 : *Sea G un grupo cíclico*

a) G es infinito $\Rightarrow$ G es isomorfo a $\mathbb{Z}$.

b) G es finito, $|G| = n \Rightarrow G$ es isomorfo a $\mathbb{Z}_n$.

Ejemplo . Los ejemplos 2 y 3 y el resultado anterior, implican $\mathbb{Z}_5^* \cong \mathbb{Z}_4$ y $\mathbb{Z}_{14}^* \cong \mathbb{Z}_6$.

2. Grupos de permutaciones:

Una de las familias más importantes de grupos son los grupos de permutaciones, S_n, que introdujimos en la primera sección. Históricamente, la teoría de grupos comenzó estudiando S_n y, de hecho, existe un teorema (Teorema de Cayley) que asegura que todo grupo finito es isomorfo a un subgrupo de S_n.

Uno de los problemas al estudiar los S_n es que son grupos no abelianos de orden muy grande en general. Como ya habíamos mencionado en la primera sección, se tiene

Lema 4.2 : *Si $n \geq 3$, S_n es un grupo no abeliano de orden $n!$*

Ejemplo . S_7 tiene 5040 elementos. (Según Platón este número era el número ideal de habitantes de una *polis* griega porque posee muchos divisores).

Entre las permutaciones se distinguen algunas más sencillas llamadas ciclos.

DEFINICIÓN: *Se dice que $\sigma \in S_n$ es el ciclo de orden k o k−ciclo dado por $\sigma = (a_1, a_2, \ldots, a_k)$ con a_i distintos, $1 \leq a_i \leq n$; si σ aplica a_1 en a_2, a_2 en a_3, $\ldots$, a_{k-1} en a_k, a_k en a_1 y deja fijos al resto de los elementos del conjunto $\{1, 2, \ldots, n\}$.*

Ejemplo 1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \in S_4$ es el ciclo $(1,4,3)$. Intuitivamente, este ciclo corresponde a "girar" los elementos 1,4,3

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \quad \leftrightarrow \quad 1 \to 4 \to 3\,.$$

Ejemplo 2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in S_4$ no es un ciclo, sino el producto de dos 2−ciclos, $\sigma = (1,4)\cdot(2,3)$. Esquemáticamente

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \leftrightarrow \quad 1 \to 4 \quad \text{y} \quad 2 \to 3\,.$$

Observación: Es bastante obvio que un ciclo de orden k tiene verdaderamente orden igual a k (ejercicio).

Antes de seguir, veamos un par de cuestiones de notación

DEFINICIÓN: *Se dice que $\sigma \in S_n$ es una trasposición si es un 2−ciclo.*

DEFINICIÓN: *Se dice que dos ciclos de S_n, $c_1 = (a_1, a_2, \ldots, a_k)$, $c_2 = (b_1, b_2, \ldots, b_l)$, son disjuntos si actúan sobre diferentes elementos, es decir, si $a_i \neq b_j$, $1 \leq i \leq k$, $1 \leq j \leq l$.*

Observación: Los ciclos disjuntos siempre conmutan.

Tras los ejemplos anteriores no es difícil demostrar el siguiente resultado

Proposición 4.3 : *Toda permutación $\sigma \neq Id$ de S_n se puede escribir como producto de ciclos disjuntos.*

Ejemplo . Consideremos las permutaciones $\sigma_1 \in S_6$, $\sigma_2 \in S_3$, $\sigma_3 \in S_7$, dadas por

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 1 & 2 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 1 & 7 & 6 \end{pmatrix}.$$

Entonces σ_1 actúa sobre 1 enviándolo al 5 y el 5 lo envía al 1, esquemáticamente $1 \to 5$, pero σ_1 no deja fijo al resto de los elementos, sino que están incluidos en la cadena $2 \to 4 \to 3 \to 6$. Por tanto

$$\sigma_1 = (1,5)\cdot(2,4,3,6).$$

De la misma forma se tiene

$$\sigma_2 = (1,2,3) \quad \text{y} \quad \sigma_3 = (1,4,5)\cdot(2,3)\cdot(6,7).$$

Esta descomposición es útil para calcular de manera sencilla el orden de una permutación

Proposición 4.4 : *Si $\sigma = c_1 \cdot c_2 \cdot \ldots c_m$ con c_i ciclos disjuntos de órdenes k_i, entonces*

$$\text{orden de } \sigma = \operatorname{mcm}(k_1, k_2, \ldots, k_m).$$

<u>DEM.</u>: Por la conmutatividad de los ciclos disjuntos, $\sigma^n = c_1^n \cdot c_2^n \cdot \ldots c_m^n$. Por tanto $\sigma^n = \mathrm{Id}$ implica que $k_i | n$, $1 \le i \le m$, de donde se deduce el resultado. ■

<u>Ejemplo</u> . En el ejemplo anterior los órdenes de σ_1, σ_2 y σ_3 son respectivamente

$$\operatorname{mcm}(2,4) = 4, \qquad \operatorname{mcm}(3) = 3, \qquad \operatorname{mcm}(3,2,2) = 6.$$

Hay varias maneras de definir el "signo" de una permutación. Nosostros optaremos aquí por una definición más o menos intuitiva pero inútil desde el punto de vista práctico, y más adelante daremos un resultado (la Proposición 4.8) que permite hacer cálculos.

DEFINICIÓN: *Se dice que $\sigma \in S_n$ es una <u>permutación par</u> o que tiene <u>signo +1</u> (y se escribe $\operatorname{sgn}(\sigma) = +1$) si efectúa un número par de cambios de ordenación al aplicar todos los pares ordenados $i < j$ en $\sigma(i)$, $\sigma(j)$, $1 \le i < j \le n$. En caso contrario se dice que es una <u>permutación impar</u> o que tiene <u>signo −1</u> (y se escribe $\operatorname{sgn}(\sigma) = -1$).*

<u>Ejemplo</u> . Sea $\sigma = (1,2,3) \in S_3$. Veamos cómo actúa sobre los pares ordenados $1 \le i < j \le n$

$1 < 2, \quad 1,2 \xrightarrow{\sigma} 2,3 \quad 2 < 3 \Rightarrow$ no hay cambio de ordenación.

$1 < 3, \quad 1,3 \xrightarrow{\sigma} 2,1 \quad 2 > 1 \Rightarrow$ hay cambio de ordenación.

$2 < 3, \quad 2,3 \xrightarrow{\sigma} 3,1 \quad 3 > 1 \Rightarrow$ hay cambio de ordenación.

Por tanto σ es par (dos cambios de ordenación) o equivalentemente $\operatorname{sgn}(\sigma) = +1$.

Otra forma de definir el signo, pero todavía poco práctica, es por medio del siguiente resultado

Lema 4.5 : *Sea $\sigma \in S_n$, entonces*

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

<u>DEM.</u>: No es difícil comprobar que la expresión de la izquierda tiene modulo 1, porque al operarla tanto en el numerador como en el denominador aparece el producto de todos los numeros de la forma $j - i$, salvo quizá el orden en que aparecen y el signo. Por otra parte $(\sigma(j) - \sigma(i))/(j - i)$ es positivo si y sólo si σ no cambia la ordenación de i y j. ■

Proposición 4.6 : sgn : $S_n \longrightarrow \big(\{-1,1\},\cdot\big)$ *es un homomorfismo, es decir,*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

<u>DEM.</u>: Obsérvese que

$$\prod_{1\le i<j\le n}\frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} = \prod_{1\le i<j\le n}\frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}\cdot\prod_{1\le i<j\le n}\frac{\tau(j)-\tau(i)}{j-i}$$

y que los números $\tau(1),\tau(2),\dots,\tau(n)$ no son más que una reordenación de $1,2,\dots,n$. Así pues, el resultado se deduce del lema anterior. ■

Antes de dar una manera práctica de calcular el signo necesitamos un resultado más

Lema 4.7 : *Toda permutación $\sigma\in S_n$ se puede escribir como un producto de trasposiciones (no necesariamente disjuntas). De hecho, un ciclo de orden k se puede escribir como producto de $k-1$ trasposiciones.*

<u>DEM.</u>: Obviamente basta demostrar la segunda parte del lema. Esto puede hacerse de varias maneras, por ejemplo, comprobando cualquiera de las igualdades

$$\begin{aligned}(a_1,a_2,\dots,a_n) =&(a_1,a_2)(a_2,a_3)\dots(a_{k-1},a_k)\\ =&(a_1,a_k)\dots(a_1,a_3)(a_1,a_2).\end{aligned}$$

(para comprobar cualquiera de estas igualdades, recuérdese que las permutaciones se componene como las funciones, comenzando por la derecha). ■

<u>Ejemplo</u> . Escribir $\sigma = \begin{pmatrix}1&2&3&4&5&6\\5&4&6&3&1&2\end{pmatrix}$ como producto de trasposiciones.

Como ya habíamos visto antes, $\sigma=(1,5)(2,4,3,6)$. Por tanto, procediendo como en la demostración anterior

$$\sigma = (1,5)(2,4)(4,3)(3,6).$$

<u>Observación</u>: A diferencia de lo que ocurre con la descomposición como producto de ciclos disjuntos, la descomposición como producto de trasposiciones no es única en general.

La manera más sencilla de calcular el signo de una permutación es el siguiente resultado

Proposición 4.8 : *Si $\sigma = c_1c_2\dots c_m$ con c_i ciclos de orden k_i, entonces*

$$\operatorname{sgn}(\sigma) = (-1)^n \qquad \textit{con}\;\; n=\sum_{i=1}^{m}(k_i-1).$$

DEM.: Basta observar que el signo de una trasposición es -1 (ejercicio), y por tanto la fórmula es consecuencia de los dos resultados anteriores. ■

Ejemplo . Hallar el signo de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 6 & 7 & 5 & 1 & 4 & 2 \end{pmatrix}$.

Descomponiendo σ como producto de ciclos disjuntos, se tiene $\sigma = (1,8,2,3,6)(4,7)$, por tanto $\operatorname{sgn}(\sigma) = (-1)^{(5-1)+(2-1)} = -1$.

Observación: Si escribimos $\sigma \in S_n$ como producto de trasposiciones, $\sigma = \tau_1\tau_2\ldots\tau_r$, entonces la proposición anterior implica $\operatorname{sgn}(\sigma) = (-1)^r$. Por tanto una permutación par debe escribirse como producto de un número par de trasposiciones y una permutación impar debe escribirse como producto de un número impar de trasposiciones.

Cerramos este apartado con una propiedad importante de las permutaciones pares.

Proposición 4.9 : *Las permutaciones pares, $A_n = \{\sigma \in S_n \,/\, \operatorname{sgn}(\sigma) = +1\}$, forman un subgrupo normal de S_n.*

DEM.: Nótese que A_n es el núcleo del homomorfismo de la Proposición 4.6, por tanto el resultado se sigue del teorema del isomorfismo. ■

Nota: Al grupo de permutaciones pares, A_n, se le suele llamar grupo alternado. Obsérvese que como el teorema del isomorfismo asegura que $S_n/A_n \cong \{-1,1\}$ se tiene en particular $|S_n/A_n| = 2$ y por tanto $|A_n| = n!/2$.

3. Grupos diédricos:

En la primera sección hemos comentado que el conjunto de giros y simetrías que dejan fijo un triángulo forma un grupo. Esta idea se puede generalizar para definir los grupos diédricos.

DEFINICIÓN: *Se llama grupo diédrico de orden $2n$, y se escribe D_n (ó D_{2n} según otros autores), al grupo formado por los movimientos del plano que dejan invariante al polígono regular de n lados.*

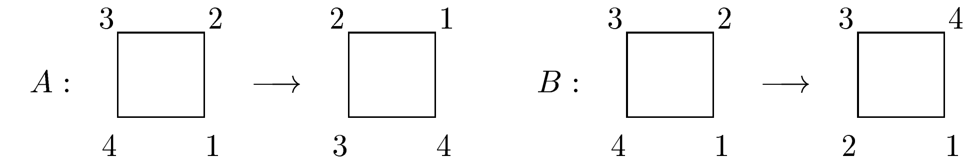
Los grupos diédricos no son abelianos, pero tienen una estructura relativamente sencilla.

Proposición 4.10 : *El grupo diédrico de orden $2n$ está generado por el giro, A, de ángulo $360^o/n$ y por una simetría, B. De hecho*

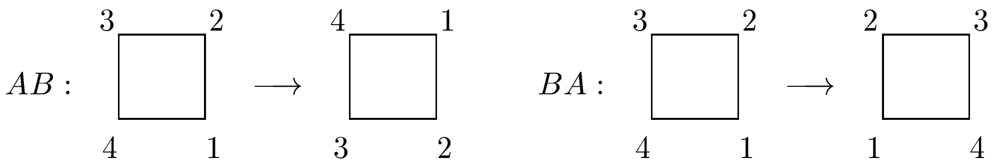
$$D_n = \{Id, A, A^2, \ldots, A^{n-1}, B, AB, A^2B, \ldots, A^{n-1}B\}$$

y se cumple la relación $BA = A^{n-1}B$.

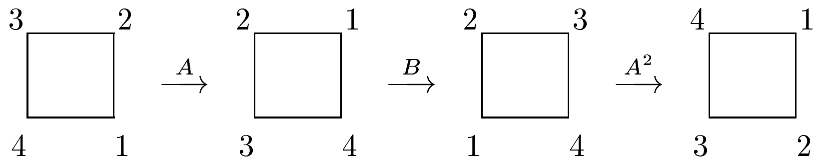
Ejemplo . Estudiemos el caso $n = 4$. Se tiene



Es fácil ver que el grupo no es abeliano:



Según la proposición, $\mathcal{D} = \langle A, B\rangle$ y en nuestro caso cuenta con 8 elementos: Id, A, A^2, A^3, B, AB, A^2B A^3B. Quizá al lector le sorprenda que no falten elementos en la lista anterior. Por ejemplo A^2BA parece que no está, pero gracias a la relación $BA = A^3B$ se tiene $A^2BA = A^2A^3B = A^4AB = AB$. Comprobémoslo:



lo que coincide con el cálculo anterior de AB.

4.5. Grupos de orden bajo

En general es muy difícil saber cuántos grupos hay de un orden dado, pero si éste es suficientemente pequeño o tiene algunas características especiales se pueden obtener algunos resultados. Por ejemplo, es obvio que todo grupo de orden 2 es de la forma $G = \{e, a\}$ con a un elemento de orden 2, y por tanto $G \cong \mathbb{Z}_2$. De la misma manera, no es difícil convencerse de que todos los grupos de orden 3 son de la forma $G = \{e, a, a^2\}$ con a un elemento de orden 3, y por tanto $G \cong \mathbb{Z}_3$. En general, si $|G| = p$ primo, por el teorema de Lagrange cualquier elemento $g \neq e$ tiene orden p y por tanto $G = \langle g\rangle$, lo que implica $G \cong \mathbb{Z}_p$ por la Proposición 4.1, con ello hemos demostrado

Proposición 5.1 : *Todo grupo de orden primo, p, es isomorfo a $\mathbb{Z}_p$.*

Hay varias maneras de "pegar" grupos pequeños para conseguir otros mayores, la más fácil y conocida viene recogida en la siguiente definición.

DEFINICIÓN: *Si G_1 y G_2 son grupos, se llama* <u>producto directo</u> *de G_1 y G_2, al grupo*

$$G_1 \times G_2 = \{(g_1, g_2) \,/\, g_1 \in G_1,\ g_2 \in G_2\}$$

con la operación $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$, $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$.

<u>Observación</u>: De la definición se sigue que $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

El concepto de producto directo es a veces inverso al de grupo cociente. Por ejemplo, es bastante obvio que

$$(G_1 \times G_2)/(G_1 \times \{e_2\}) \cong G_2 \quad \text{y} \quad (G_1 \times G_2)/(\{e_1\} \times G_2) \cong G_1$$

donde e_1 y e_2 son los elementos neutros de G_1 y G_2. Sin embargo no es siempre cierto que $G/H \times H \cong G$.

<u>Ejemplo 1</u>. $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ y se tiene

$$(\overline{0}, \overline{1}) + (\overline{1}, \overline{0}) = (\overline{1}, \overline{1}), \qquad (\overline{0}, \overline{1}) + (\overline{1}, \overline{1}) = (\overline{1}, \overline{0}), \qquad (\overline{1}, \overline{0}) + (\overline{1}, \overline{1}) = (\overline{0}, \overline{1}).$$

Al grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ (o a uno isomorfo a él) se le llama <u>grupo de Klein</u> o *Viergruppe*.

<u>Ejemplo 2</u>. $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\}$. No es difícil comprobar que $(\overline{1}, \overline{2})$ tiene orden 6. Con lo cual, se tiene que $\mathbb{Z}_2 \times \mathbb{Z}_3$ es cíclico de orden 6 y por tanto isomorfo a $\mathbb{Z}_6$.

Con unos cuanto cálculos, no muy sistemáticos, uno puede demostrar los siguientes resultados

Proposición 5.2 : *Todo grupo de orden 4 es isomorfo a $\mathbb{Z}_4$ o al grupo de Klein.*

Proposición 5.3 : *Todo grupo de orden 6 es isomorfo a $\mathbb{Z}_6$ o a S_3.*

Como ya hemos comentado, no existen generalizaciones de estos teoremas cuando el orden es grande, sin embargo, si sólo nos interesamos en la teoría de grupos abelianos, el siguiente teorema contiene toda la información que podríamos esperar

Teorema 5.4 (de estructura de los grupos abelianos finitos): *Si G es un grupo abeliano finito, entonces*

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}.$$

Además $n_1, n_2, \ldots, n_k$ están totalmente determinados si imponemos la condición $n_1|n_2$, $n_2|n_3$,. . . ,$n_{k-1}|n_k$

<u>Ejemplo 1</u>. El grupo $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ no es isomorfo a $\mathbb{Z}_9 \times \mathbb{Z}_9$ (aunque ambos tienen orden 81) porque

$$G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \cong \mathbb{Z}_9 \times \mathbb{Z}_9$$

contradiría que los n_i están totalmente determinados (bajo la condición del teorema).

En general se tiene que $\mathbb{Z}_n \times \mathbb{Z}_n \not\cong \mathbb{Z}_{n^2}$. Una demostración directa de ello se puede obtener simplemente observando que en $\mathbb{Z}_n \times \mathbb{Z}_n$ todos los elementos tienen orden menor o igual que n, mientras que en $\mathbb{Z}_{n^2}$ hay al menos un elemento (el $\overline{1}$) de orden n^2. Variaciones sobre este mismo argumento muestran que, de hecho, $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ si y sólo si n y m son primos entre sí.

Ejemplo 2. El grupo $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ tiene orden 4, así que por el teorema de estructura, podría ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ o a $\mathbb{Z}_4$ (esto también se podría obtener a partir de la Proposición 5.2). Como ya habíamos visto que $\mathbb{Z}_8^*$ no es cíclico (todos sus elementos excepto $\overline{1}$ tienen orden 2) se tiene $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Ejemplo 3. El grupo $\mathbb{Z}_{13}^* = \{\overline{1}, \overline{2}, \dots, \overline{12}\}$ podría ser isomorfo, según el teorema de estructura, a $\mathbb{Z}_2 \times \mathbb{Z}_6$ o a $\mathbb{Z}_{12}$ (nótese que no hace falta considerar, por ejemplo, $\mathbb{Z}_3 \times \mathbb{Z}_4$ porque $3 \nmid 4$). Algunos cálculos prueban que el orden de $\overline{2}$ en $\mathbb{Z}_{13}^*$ es 12, con lo cual $\mathbb{Z}_{13}^*$ debe ser cíclico y por tanto $\mathbb{Z}_{13}^* \cong \mathbb{Z}_{12}$.

Ejemplo 4. Según el teorema de estructura, un grupo abeliano de orden 100 debe ser isomorfo a $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$ con $100 = n_1 n_2 \dots n_k$ y $n_i | n_{i+1}$ para $1 \le i \le k-1$. Las únicas factorizaciones de 100 que dan lugar a valores de los n_i satisfaciendo estas condiciones son

$$100 = 2 \cdot 50, \qquad 100 = 5 \cdot 20, \qquad 100 = 10 \cdot 10, \qquad 100 = 100.$$

Por tanto los únicos grupos abelianos de orden 100 son, salvo isomorfismos,

$$\mathbb{Z}_2 \times \mathbb{Z}_{50}, \qquad \mathbb{Z}_5 \times \mathbb{Z}_{20}, \qquad \mathbb{Z}_{10} \times \mathbb{Z}_{10}, \qquad \mathbb{Z}_{100}.$$

Terminamos esta sección dando una sorprendente consecuencia del teorema de estructura. Aunque la demostración sea breve es realmente ingeniosa.

Proposición 5.5: *Si p es primo $\mathbb{Z}_p^*$ es cíclico.*

DEM.: Si $\mathbb{Z}_p^*$ no fuera cíclico entonces no sería isomorfo a un solo $\mathbb{Z}_n$ sino que

$$\mathbb{Z}_p^* \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$$

con $k \ge 2$ y $n_1 | n_2$, $n_2 | n_3$,... $n_{k-1} | n_k$. Como en el segundo grupo todos los elementos tienen orden que divide a n_k, lo mismo debe ocurrir en $\mathbb{Z}_p$. Por tanto el polinomio $x^{n_k} - 1 \in \mathbb{Z}_p[x]$ tiene como raíces a las $p-1$ clases de $\mathbb{Z}_p - \{\overline{0}\}$, lo cual es imposible porque su grado es $n_k < p-1$. ■

Hoja 9

1) Estudiar el grupo de movimientos del plano que deja fijo el cuadrado. ¿Cuál es su orden? ¿Es abeliano?

2) Si $g^n = e$, demostrar que el orden de g divide a n.

3) Si el orden de g es n, ¿cuánto puede valer el orden de g^2?

4) Demostrar que las soluciones enteras de $x^2 - 3y^2 = 1$ forman un grupo con la operación

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + 3y_1y_2, x_1y_2 + y_1x_2).$$

Sabiendo esto hallar tres soluciones y demostrar que existen infinitas soluciones.

$***$**5)** En el ejercicio anterior, ¿pertenecen todas las soluciones con $x > 0$ a $\langle(2, -1)\rangle$?

6) Hallar todos los $x \in \mathbb{Z}_7^*$ tales que $\langle x\rangle = \mathbb{Z}_7^*$.

7) Sea r_n el resto que se obtiene al dividir 75^n por 65537. Sabiendo que el orden de 75 en $\mathbb{Z}_{65537}^*$ es 65536 (ver el problema siguiente), demostrar que r_n alcanza todos los valores entre 1 y 65536. Hallar el orden de 5625.

8) La "Ley de reciprocidad cuadrática" es un bello resultado de Gauss (1777-1855) que implica (entre otras cosas) que si $p > 3$, $q > 2$ son primos y $p - 1$ es una potencia de dos, entonces

$$\textit{El orden de } \overline{p} \textit{ en } \mathbb{Z}_q^* \textit{ es } q-1. \Rightarrow \textit{ El orden de } \overline{q} \textit{ en } \mathbb{Z}_p^* \textit{ es } p-1$$

Sabiendo esto, demostrar que el orden de 3 en $\mathbb{Z}_{65537}^*$ es 65536 y concluir que 75 tiene el mismo orden. *Indicación*: $75 = 5^2 \cdot 3$ y $5^{65536} \equiv 1$ (65537).

9) Se dice que una permutación, $\sigma \in S_n$, deja invariante la función f de n variables, si $f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$. Demostrar que forman un subgrupo de S_n. Calcular el índice de los subgrupos de S_3 que dejan invariantes a

a) $f_1 = x_1 + 2x_2 + x_3$ *b)* $f_2 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ *c)* $f_3 = x_1x_2 + x_1x_3 + x_2x_3$.

10) Demostrar que $S_n = \langle\sigma_2, \sigma_3, \dots, \sigma_n\rangle$ donde σ_k es la permutación que intercambia 1 y k.

11) La Física relativista asegura que si v es la velocidad relativa de O' con respecto de O y w la velocidad relativa de O'' con respecto de O', entonces la velocidad relativa de O'' con respecto de O no viene dada por $v + w$, sino por $v * w = \frac{v+w}{1+\epsilon vw}$ donde $\epsilon^{-1} = c^2 = 9 \cdot 10^9$. Demostrar que $*$ define un grupo en el conjunto $\{v \in \mathbb{R} \,/\, v^2 < \epsilon^{-1}\}$. Las llamadas transformaciones de Lorentz están asociadas a las matrices de la forma $L_v = (1 - \epsilon v^2)^{-1/2}\begin{pmatrix} 1 & -v \\ -\epsilon v & 1 \end{pmatrix}$. Demostrar que $L_v \cdot L_w = L_{v*w}$ y que $\{L_v \,/\, v^2 < \epsilon^{-1}\}$ es un grupo con el producto usual de matrices (el grupo de Lorentz).

12) El cubo de Rubik tiene 20 piezas móviles: 12 aristas y 8 vértices. Cada arista tiene dos posibles orientaciones y cada vértice tres. El grupo teórico del cubo, $\mathcal{T}$, está formado por las posiciones que se pueden obtener al desarmar las piezas y volverlas a montar y el grupo real del cubo, $\mathcal{C}$, es el formado por posiciones a las que se puede llegar con movimientos admisibles (sin romper nada). Sorprendentemente $\mathcal{C} \neq \mathcal{T}$. Sabiendo que $\mathcal{C}$ es un subgrupo de $\mathcal{T}$ de índice 12, hallar $|\mathcal{C}|$.

Hoja 10

1) Si $\phi : G \longrightarrow G'$ es un homomorfismo, demostrar que si G es abeliano y G' no lo es, entonces ϕ no es un isomorfismo. ¿Puede ser un monomorfismo? ¿y un epimorfismo?

2) Si $\phi : G \longrightarrow G'$ es un isomorfismo y n es el orden de $g \in G$ ¿cuál es el orden de $\phi(g)$?

3) Estudiar si son homorfismos y de qué tipo las funciones

$$\phi_1 : S_3 \longrightarrow S_3 \ , \quad \phi_1(\sigma) = \sigma^2 \qquad \phi_2 : (\mathbb{R}, +) \longrightarrow (\mathbb{C}, +) \ , \quad \phi_2(x) = 2x + ix$$
$$\phi_3 : \mathbb{Z}_5^* \longrightarrow \mathbb{Z}_5^* \quad \phi_3(\overline{x}) = \overline{x}^5 \qquad \phi_4 : (\mathbb{R}, +) \longrightarrow (\mathbb{R} - \{0\}, \cdot) \ , \quad \phi_4(x) = \pi^x$$

4) Sea G el grupo definido en $-1 < x < 1$ con la operación $x * y = \frac{x+y}{1+xy}$. Demostrar que

$$\phi : (\mathbb{R}, +) \longrightarrow G \qquad \phi(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \quad (\text{donde } e = 2\text{'}7182\ldots)$$

es un homorfismo. ¿Es un isomorfismo? En caso afirmativo calcular su inverso.

5) Si G es finito demostrar que un homomorfismo $\phi : G \longrightarrow G$ es un isomorfismo si y sólo si $\operatorname{Nuc} \phi = \{e\}$. Hallar un contraejemplo si G es infinito.

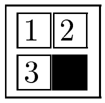
6) Sea $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_9$ la función que aplica cada número entero en la clase módulo 9 de la suma de sus cifras, cambiada de signo si es negativo (por ejemplo $\phi(-83) = -(\overline{8+3}) = \overline{7}$). Demostrar que es un homomorfismo.

7) Sea $G = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, es decir, el grupo de vectores de dos coordenadas en $\mathbb{Z}_2$. Demostrar que $|G| = |\mathbb{Z}_4| = 4$ pero que G y $\mathbb{Z}_4$ no son isomorfos.

8) Sabiendo que $\overline{3}$ tiene orden 256 en $\mathbb{Z}_{257}^*$, demostrar que $\phi : \mathbb{Z}_{256} \longrightarrow \mathbb{Z}_{257}^*$ definido por $\phi(\overline{x}) = \overline{3}^x$ es un isomorfismo.

9) Una clave de acceso ("password") de una letra, L_1, se puede codificar con el número $\psi(L_1) = \phi(ASC(L_1))$ donde ϕ es el isomorfismo del ejercicio anterior y ASC indica el número de código ASCII. Sabiendo que $ASC(A) = 65$, hallar $\psi(A)$. *Nota*: El ordenador, por seguridad, almacenará internamente $\psi(A)$ pero no el "password", A. Incluso en este ejemplo tan sencillo es difícil recuperar L_1 a partir de $\psi(L_1)$, el que no lo crea que intente descodificar "a mano" 89.

10) Consideramos el rompecabezas plano de la figura donde las fichas numeradas pueden desplazarse para ocupar el hueco libre. Sea $\mathcal{M}$ el grupo de series de movimientos que dejan el hueco libre en la posición inicial.



Si $g \in \mathcal{M}$ transforma $\begin{smallmatrix} 1 & 2 \\ 3 & \blacksquare \end{smallmatrix}$ en $\begin{smallmatrix} a & b \\ c & \blacksquare \end{smallmatrix}$ le asociamos la permutación $\phi(g) = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix} \in S_3$. Sabiendo que $\phi : \mathcal{M} \to S_3$ es un homomorfismo hallar $[S_3 : \operatorname{Im} \phi]$.

****11)** Demostrar que en el rompecabezas análogo de 4×4 (quince fichas y un hueco libre) $[S_{15} : \operatorname{Im} \phi] \neq 1$, es decir, que hay permutaciones de las fichas numeradas que no se pueden alcanzar. *Nota*: De hecho $\operatorname{Im} \phi$ es un grupo de orden $15!/2$ llamado A_{15}.

1) Un grupo, G, con menos de 100 elementos tiene un elemento de orden 10 y otro de orden 14, hallar $|G|$.

2) Demostrar que si $\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$ es una cadena de subgrupos de G, entonces $|G| = \prod_{i=1}^{n}[G_i : G_{i-1}]$.

3) Demostrar que si $\phi : G \longrightarrow G$ definido por $\phi(x) = x^2$ es un homomorfismo, entonces G es abeliano.

4) Demostrar que un subgrupo de índice 2 es siempre normal.

5) Hallar un subgrupo de orden 3 de S_5 y comprobar que no es normal.

6) Hallar las coclases a la derecha y a la izquierda de $H = \{\mathrm{Id}, \sigma\}$ en S_3 donde σ es la permutación que intercambia 1 y 2. ¿Es un subgrupo normal?

7) Demostrar que si H_1 y H_2 son subgrupos normales de G, entonces $H_1 \cap H_2$ es normal.

8) Demostrar que si H_1 y H_2 son subgrupos normales de G y $H_1 \cap H_2 = \{e\}$ entonces $\forall h_1 \in H_1,\ \forall h_2 \in H_2\ h_2 h_1 = h_1 h_2$.

9) Sea H un subgrupo normal de G. Demostrar que si el orden de $g \in G$ y $[G : H]$ son primos entre sí, entonces $g \in H$.

10) Demostrar que si G es finito y está generado por $\{g_1, g_2, \ldots, g_n\}$, entonces, H es un subgrupo normal de G si y sólo si $g_1^{-1} h g_1,\ g_2^{-1} h g_2,\ \ldots, g_n^{-1} h g_n \in H\ \ \forall h \in H$.

11) Sea $H = \Big\{\mathrm{Id}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\Big\}$. Demostrar que H es un subgrupo de S_4 y, sabiendo que $S_4 = \Big\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \Big\rangle$, aplicar el ejercicio anterior para concluir que H es un subgrupo normal.

12) Sea $\phi : G \longrightarrow G'$ un homomorfismo, y sean H y H' subgrupos normales de G y G', respectivamente. Demostrar que $\phi^{-1}(H')$ es un subgrupo normal de G y que si ϕ es un epimorfismo, $\phi(H)$ es un subgrupo normal de G'.

$**$**13)** Sea G un grupo, $\mathcal{G} = G \times G \times \overset{p-1 \text{ veces}}{\cdots\cdots} \times G$ y p un primo, $p \big| |G|$. Demostrar que la función $f : \mathcal{G} \longrightarrow \mathcal{G}$ definida por

$$f(g_1, g_2, \ldots, g_{p-1}) = (g_2, g_3, \ldots, g_{p-1}, g_{p-1}^{-1} g_{p-2}^{-1} \cdots g_2^{-1} g_1^{-1})$$

cumple $f \circ \overset{p \text{ veces}}{\cdots\cdots} \circ f(\vec{g}) = \vec{g}\ \ \forall \vec{g} \in \mathcal{G}$ y además $\exists \vec{g} \neq \vec{e}$ tal que $f(\vec{g}) = \vec{g}$. Concluir de esta última afirmación que *"si un primo, p, divide al orden de un grupo, existe algún elemento de orden p"*

<u>Nota</u>: Este resultado casi inverso al teorema de Lagrange se debe a Cauchy (1789-1857). Es sorprendente que un enunciado tan sencillo requiera una demostración tan difícil de entender.

Hoja 12

1) Comprobar que $\mathbb{Z}_{13}^*$ es cíclico.

2) Sabiendo que $\mathbb{Z}_{257}^*$ es cíclico, calcular cuántos subgrupos suyos tienen índice 64.

3) Descomponer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix}$ como producto de ciclos disjuntos y calcular su orden.

4) Hallar el orden de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ y calcular σ^{91}.

5) Escribir la permutación del ejercicio anterior como producto de trasposiciones y hallar su signo.

6) Hallar el orden y el signo de las permutaciones

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4 \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix} \in S_6 \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 2 & 1 \end{pmatrix} \in S_6$$

7) Sea $\sigma = (1,6,11,2,9,12)(3,8,4,7,10) \in S_{12}$. Hallar el orden de σ^{14}.

8) Sea $\sigma = (2,3,5)(4,6,7,8) \in S_4$. Escribir σ^2 como producto de ciclos disjuntos.

***9)** ¿Se cumple $S_n \cong \mathbb{Z}_2 \times A_n$?

10) Sean A, B los generadores habituales de un grupo diédrico ($A =$giro, $B =$simetría) demostrar que no existen $n_1, n_2, n_3, \ldots, n_{16} \in \mathbb{Z}^+$ tales que

$$A^{n_1} B A^{n_2} B A^{n_3} B \ldots A^{n_{16}} B = B$$

11) Sea G un grupo y sea $Z(G)$ el subgrupo de G formado por los elementos que conmutan todos los demás. Demostrar que $Z(G)$ es un subgrupo normal de G, y hallar $Z(G)$ si G es el grupo diédrico de 8 elementos.

12) Escribir $\mathbb{Z}_{15}^*$ y $\mathbb{Z}_{16}^*$ en la forma que asegura el teorema de estructura de grupos abelianos.

13) Demostrar que existe un homomorfismo $\phi : \mathbb{Z}_3 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_6 \times \mathbb{Z}_2$. ¿Puede ser ϕ monomorfismo?

3	2	1
4		8
5	6	7

14) Numerando las 20 piezas móviles del cubo de Rubik (hay 8 en la cara de arriba, otras 8 en la de abajo y 4 en la sección central), cada movimiento se puede considerar como una permutación de S_{20}. Además, girar una de las caras corresponde a un producto de dos 4-ciclos. Por ejemplo, si la cara de arriba está numerada como en la figura, girarla en sentido horario corresponde a $\sigma = (1,3,5,7)(2,4,6,8)$. Demostrar que es imposible intercambiar dos piezas dejando fijas el resto.

Miscelánea.

El concepto de grupo surgió históricamente con el estudio de la solución de las ecuaciones algebraicas. Este estudio es en realidad el origen del álgebra y tiene una larga tradición dentro de las Matemáticas que se remonta a los antiguos babilonios y que alcanzó su auge en el siglo XVI. La complicada notación utilizada en tiempos pasados, provocaba que los razonamientos fueran mucho más enrevesados que en la actualidad, por ello debe considerarse como un gran triunfo que los algebristas del siglo XVI descubrieran las fórmulas para resolver ecuaciones de tercer y cuarto grado. Para dar una idea de su complicación, diremos que las raíces de $x^3 + px + q = 0$ vienen dadas por

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Además hay ciertas condiciones para "elegir" las raíces cúbicas de los números (posiblemente complejos) que aparecen en el radicando. Todas las ecuaciones cúbicas se pueden reducir a la forma anterior dando lugar a una fórmula general más compleja. Esta complicación es todavía mayor al resolver la ecuación de cuarto grado.

Estas fórmulas datan del Renacimiento italiano, pero su historia es un tanto oscura. Parece que las ideas para resolver la ecuación cúbica se deben a S. del Ferro (aprox. 1465-1526), pero fueron publicadas por G. Cardano (1501-1576) en su libro "Ars Magna" (este "magno arte" es el álgebra). Por otra parte, N. Fontana (aprox. 1500-1557), llamado Tartaglia (tartamudo), afirmó que él mismo había comunicado la solución a Cardano quien prometió no divulgarla. Finalmente, la solución de la cuártica parece deberse a L. Ferrari (1522-1565).

Los matemáticos posteriores buscaron en vano una solución del mismo tipo para la ecuación de quinto grado, pero no lo consiguieron. En gran medida, en este intento apareció la teoría de grupos. N.H. Abel (1802-1829) demostró finalmente, usando propiedades del grupo S_5, que no existe ninguna fórmula para resolver la ecuación quíntica con radicales (P. Ruffini (1765-1822) lo demostró con anterioridad e independientemente pero de forma no muy rigurosa). Posteriormente, la estrecha relación entre las ecuaciones algebraicas y la teoría de grupos fue explicitada de una forma muy elegante, abstracta y general, por E. Galois (1811-1832) cuya vida aparece citada en muchos libros por estar plagada de vicisitudes: estuvo involucrado en problemas políticos, sus manuscritos fueron perdidos o rechazados, no pudo entrar en la universidad a la que optaba y el trabajo más importante que se conserva de él lo redactó y anotó la noche antes de celebrarse el duelo en el que moriría antes de cumplir los 21.

Si bien es cierto que Galois fue apenas valorado por sus contemporáneos (su trabajo se publicó 14 años después de su muerte); seguramente una visión romántica de su corta y azarosa vida lleva a veces en la actualidad a exagerar en el sentido contrario, exaltando la figura de Galois frente a la de otros matemáticos que trabajaron en el mismo tema.

> Los omnes, a las vegadas, con el grand afincamiento,
> otorgan lo que non deven, mudan su entendimiento;
> quando es fecho el daño, viene el arrepentimiento:
> çiega la muger seguida, non tiene seso nin tiento.
> *LBA, 865*

La llamada "Teoría de Galois" ha alcanzado unas dimensiones y abstracción considerables pero las ideas subyacentes son relativamente simples cuando uno conoce los fundamentos de la teoría de grupos. En primer lugar, nótese que los coeficientes de una ecuación algebraica son funciones simétricas de las raíces, por ejemplo, si las raíces de $x^3 + px + q = 0$ son x_1, x_2, x_3, entonces

$$x^3 + px + q = (x - x_1)(x - x_2)(x - x_3) \ \Rightarrow \ p = x_1x_2 + x_1x_3 + x_2x_3, \quad q = -x_1x_2x_3.$$

Como al cambiar x_1, x_2, x_3 por $x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}$ con $\sigma \in S_3$, p y q no varían, diremos que son funciones invariantes por S_3. Cada raíz por separado no tiene, en general, esta propiedad, así que en el proceso de extraer radicales para resolver la ecuación tenemos que ir perdiendo simetrías, esto es, las funciones que aparecen son invariantes por grupos cada vez más pequeños. Por ejemplo, algunos cálculos prueban que

$$\frac{q^2}{4}+\frac{p^3}{27}=-\frac{1}{108}(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$$

y por tanto $\sqrt{q^2/4+p^3/27}$ sólo es invariante por A_3 (permutaciones pares), mientras que

$$-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}=\frac{1}{27}(x_1+\zeta x_2+\zeta^2 x_3)^3 \quad \text{con } \zeta=\cos\frac{2\pi}{3}+i\operatorname{sen}\frac{2\pi}{3}$$

implica que la raíz cúbica de esta expresión no es invariante por nada distinto de la identidad.

Supongamos ahora que tenemos una fórmula general para resolver la ecuación de grado n y que $r=\sqrt[p]{A}$ es uno de los radicales más interiores (podemos suponer p primo porque $\sqrt[ab]{\ }=\sqrt[a]{\sqrt[b]{\ }}$), es decir, A es una función racional de los coeficientes y por tanto simétrica en las raíces $x_1,x_2,\ldots,x_n$; con lo cual, r^p es invariante por S_n. Consideremos el homomorfismo (pruébese que lo es)

$$\begin{aligned}\Phi: S_n &\longrightarrow \big(\mathbb{C}-\{0\},\cdot\big)\\ \sigma &\longrightarrow r\big(x_{\sigma(1)},x_{\sigma(2)},\ldots x_{\sigma(n)}\big)\big/r(x_1,x_2,\ldots,x_n).\end{aligned}$$

Nótese que $\sigma\in\operatorname{Nuc}\Phi$ si y sólo si r es invariante por σ. Si $\sqrt[p]{\ }$ ha roto algunas simetrías, hay elementos en la imagen distintos de 1; como además $\big(\Phi(\sigma)\big)^p=1$ (porque r^p es invariante por S_n), se deduce que la imagen de Φ está formada por las raíces de la unidad de índice p, esto es

$$\operatorname{Im}\Phi=\{1,\zeta,\zeta^2,\zeta^3,\ldots,\zeta^{p-1}\} \quad \text{con } \zeta=\cos\frac{2\pi}{p}+i\operatorname{sen}\frac{2\pi}{p}.$$

Como $\operatorname{Im}\Phi$ (con la multiplicación) es isomorfo a $\mathbb{Z}_p$, por el teorema del isomorfismo se tiene

$$S_n\big/\operatorname{Nuc}\Phi\cong\mathbb{Z}_p.$$

Recapitulemos todo lo hecho: Hemos partido de la expresión A que es invariante por $G_0=S_n$ y hemos demostrado que $\sqrt[p]{A}$ es invariante por $G_1=\operatorname{Nuc}\Phi$ y que si $G_1\underset{\neq}{\subset}G_0$ se debe tener $G_0/G_1\cong\mathbb{Z}_p$. Todo este proceso se puede repetir al añadir un nuevo radical "reduciendo" G_1 a G_2 con $G_1/G_2\cong\mathbb{Z}_{p'}$ y así sucesivamente hasta llegar a $\{\mathrm{Id}\}$ que corresponde a una expresión que no es invariante por nada y de la que podemos despejar las raíces. Todo esto queda resumido en el siguiente resultado:

Si la ecuación de grado n es soluble por radicales, existe una cadena de grupos

$$G_0=S_n\supset G_1\supset G_2\supset\ldots\supset G_m=\{\mathrm{Id}\}$$

tales que cada uno es normal en el anterior y $G_{i-1}/G_i\cong\mathbb{Z}_{p_i}$, $1\le i\le m$.

Para las ecuaciones de grados $n=2,3$ y 4, las cadenas son

$$S_2\supset\{\mathrm{Id}\},\quad S_3\supset A_3\supset\{\mathrm{Id}\},\quad S_4\supset A_4\supset\langle(1,2)(3,4),(2,3)(1,4)\rangle\supset\{\mathrm{Id}\};$$

pero no existe ninguna cadena similar en el caso $n=5$. La idea es que ésta debiera comenzar por $S_5\supset A_5$ y como A_5 no tiene ningún subrupo normal no trivial no podemos completar esta cadena, y por tanto no existe una solución con radicales para la ecuación quíntica general. Lo mismo ocurre siempre que $n\ge 5$.

La demostración de que A_5 (y en general A_n) no tiene subgrupos normales no triviales es un poco tediosa pero no excesivamente complicada. Esencialmente, se prueba que si $\sigma\in A_5$, $\sigma\neq\{\mathrm{Id}\}$, entonces $\{\tau^{-1}\sigma\tau\big/\tau\in A_5\}=A_5$ y por tanto no existe ningún $\{\mathrm{Id}\}\neq H\underset{\neq}{\subset}A_5$ tal que $\tau^{-1}H\tau=H$ para todo τ.

Además de la resolubilidad por radicales de ecuaciones algebraicas, una de las aplicaciones más bellas de la Teoría de Galois se refiere a la constructibilidad de los polígonos regulares.

Los antiguos griegos sabían construir con regla y compás polígonos regulares de, por ejemplo, 3, 4, 5, 6, 8, 10, 12 ó 15 lados, pero nunca consiguieron dar un método exacto para construir el polígono regular de, por ejemplo, 7 lados. Casi veinte siglos más tarde, P. de Fermat (1601-1665) se ocupaba de un tema totalmente distinto afirmando que los números $2^{2^n}+1$ con $n \in \mathbb{N}$ son todos primos. A pesar de que esto no es cierto en general, los primos de esta forma se llaman primos de Fermat. Más de 150 años después, C.F. Gauss (1777-1855), usando los rudimentos de lo que más tarde sería la Teoría de Galois, enunciaba el siguiente bellísimo resultado:

El polígono regular de n lados se puede construir con regla y compás si y sólo si $n = 2^k p_1 p_2 \dots p_r$ donde $k \in \mathbb{N}$ y $p_1, p_2, \dots p_r$ son primos de Fermat distintos.

Por ejemplo, el polígono regular de 771 lados es construible con regla y compás porque 771 se puede escribir como $2^0(2^{2^0}+1)(2^{2^3}+1)$.

Este asombroso resultado sugiere preguntarse qué tienen que ver los polígonos regulares (y su constructibilidad) con la solución de ecuaciones algebraicas o con la teoría de grupos. Dar una explicación a estas cuestiones sería demasiado extenso, por ello sólo diremos que las raíces de $x^n - 1$ están situadas (cuando las representamos como números complejos) en los vértices de un polígono regular de n lados y que ciertas funciones de estas raíces forma un grupo isomorfo a $\mathbb{Z}_n^*$ cuyo orden es una potencia de 2 para valores de n como los del resultado anterior.

En suma vos lo cuento por non vos detener:
do todo esto escriviese, en Toledo non ay papel;
en la obra de dentro ay tanto de fazer,
que, si lo dezir puedo, meresçía de bever.
LBA, 1269

5. Espacios Vectoriales

5.1. Espacios, subespacios, propiedades y ejemplos

En Física aparecen muchas veces magnitudes que no quedan bien determinadas por un solo número real, sino que para representarlas necesitamos su dirección y sentido. Se dice que estas magnitudes son vectoriales y vienen representadas por un vector.

El ejemplo más fácil y conocido son las fuerzas, cada fuerza se puede representar con una "flecha" (vector) cuya longitud indica el módulo de la fuerza. Si estas fuerzas se indican en un sistema de coordenadas cartesiano (situando el punto de aplicación en el origen), entonces la suma de fuerzas se traduce en la suma de puntos coordenada a coordenada

$$\begin{array}{ccccc} \uparrow & + & \rightarrow & = & \nearrow \\ (0,1) & + & (1,0) & = & (1,1) \end{array}$$

Las fuerzas no sólo se pueden sumar, sino también multiplicar por números reales, lo mismo ocurre con otras magnitudes físicas. Todo esto sugiere definir una estructura algebraica en la que podamos sumar y multiplicar por números, y que cuente con algunas propiedades básicas.

Definición: *Sea K un cuerpo. Se dice que E es un* espacio vectorial *sobre K si existe una operación, $+$, tal que $(E,+)$ es un grupo abeliano, y una aplicación $\cdot : K \times E \longrightarrow E$ (multiplicación por escalares). Además $+$ y $\cdot$ deben cumplir las propiedades*

$$\begin{aligned} &1)\ \vec{u},\vec{v}\in E,\ \lambda\in K,\ \Rightarrow\ \lambda\cdot(\vec{u}+\vec{v})=\lambda\cdot\vec{u}+\lambda\cdot\vec{v} \\ &2)\ \vec{u}\in E,\ \lambda,\mu\in K,\ \Rightarrow\ (\lambda+\mu)\cdot\vec{u}=\lambda\cdot\vec{u}+\mu\cdot\vec{u} \\ &3)\ \vec{u}\in E,\ \lambda,\mu\in K,\ \Rightarrow\ \lambda(\mu\cdot\vec{u})=(\lambda\mu)\cdot\vec{u} \\ &4)\ \vec{u}\in E\ \Rightarrow\ 1\cdot\vec{u}=\vec{u}. \end{aligned}$$

Nota: Normalmente se omite el símbolo $\cdot$ en la multiplicación por escalares. A los elementos de un espacio vectorial se les llama vectores y se suelen denotar por $\vec{u}$, $\vec{v}$, etc.

La definición de cualquier estructura algebraica sería una abstracción innecesaria si no existieran suficientes ejemplos que la justifiquen. Veamos a continuación algunos de ellos.

Ejemplo 1. El ejemplo prototípico de espacio vectorial es $\mathbb{R}^n$, $(n\in\mathbb{Z}^+)$. Éste es un espacio vectorial sobre $\mathbb{R}$ definido por

$$\mathbb{R}^n=\{(a_1,a_2,\ldots,a_n)\,/\,a_i\in\mathbb{R}\}$$

con la suma y multiplicación por escalares

$$
\begin{aligned}
&(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \\
&\lambda(a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n)
\end{aligned}
$$

Ejemplo 2. A partir de un cuerpo cualquiera, K, se puede definir un espacio vectorial sobre K de forma análoga al caso anterior. Por ejemplo, recuérdese que $\mathbb{Z}_p$ es un cuerpo, entonces $\mathbb{Z}_p^n$ es un espacio vectorial sobre $\mathbb{Z}_p$ definido por

$$\mathbb{Z}_p^n = \{(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \,/\, \overline{a_i} \in \mathbb{Z}_p\}.$$

Ejemplo 3. Las matrices $m \times n$ con coeficientes en un cuerpo K, forman un espacio vectorial que llamaremos $\mathcal{M}_{m\times n}(K)$

$$\mathcal{M}_{m\times n}(K) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \,/\, a_{ij} \in K,\ 1 \le i \le m,\ 1 \le j \le n \right\}.$$

Ejemplo 4. $K[x]$ es un espacio vectorial sobre K. (Recuérdese que $K[x]$ indica los polinomios con coeficientes en K, ejemplos de este tipo son $\mathbb{R}[x]$ y $\mathbb{C}[x]$).

Ejemplo 5. Una modificación del ejemplo anterior es

$$\mathbb{P}_n[x] = \{\text{Polinomios de } K[x] \text{ de grado} \le n\} \cup \{0\}.$$

Uno de los ejemplos más conocidos e interesante es

Ejemplo 6. Las soluciones $(x_1, x_2, \ldots, x_n)$ del sistema homogéneo

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0 \\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0 \\
\ldots \quad \ldots \quad \ldots \quad \ldots \quad & \ldots \quad \ldots \\
a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0
\end{aligned}
$$

con $a_{ij} \in K$, forman un espacio vectorial sobre K.

Una función se puede considerar como un vector de "infinitas coordenadas" formado por todos los valores que toma, por ello el ejemplo anterior está relacionado con el siguiente ejemplo con funciones. En algún sentido, derivar se puede traducir "infinitesimalmente" en hacer sumas y restas y multiplicar por números.

Ejemplo 7. Las soluciones, $y : \mathbb{R} \longrightarrow \mathbb{R}$, de

$$y'' + y = 0 \qquad \text{(ecuación del péndulo simple para oscilaciones pequeñas)}$$

forman un espacio vectorial sobre $\mathbb{R}$.

Esto puede ser útil para encontrar soluciones. Por ejemplo, si vemos "a ojo" que $y = \operatorname{sen} x$, $y = \cos x$ son soluciones, entonces la suma de ellas y producto por números reales también serán solución (por ser un espacio vectorial sobre $\mathbb{R}$), así pues, conseguimos toda una familia infinita de soluciones $y = \lambda \operatorname{sen} x + \mu \cos x$. De hecho se puede demostrar que éstas son todas las soluciones.

Intuitivamente, un subespacio es un espacio vectorial dentro de otro, pero casi es más fácil no intentar dar una definición en esa línea y utilizar en su lugar

DEFINICIÓN: *Sea V un espacio vectorial, decimos que $W \subset V$ es un* subespacio vectorial *de V si*

$$1)\ \vec{u}, \vec{v} \in W \ \Rightarrow\ \vec{u} + \vec{v} \in W \qquad 2)\ \vec{u} \in W,\ \lambda \in K \ \Rightarrow\ \lambda\vec{u} \in W.$$

Ejemplo 1.

$$W = \{(x, y, 0) \,/\, x, y \in \mathbb{R}\}$$

es un subespacio de $\mathbb{R}^3$.

Ejemplo 2.

$$W = \{(x, y, 1) \,/\, x, y \in \mathbb{R}\}$$

no es un subespacio de $\mathbb{R}^3$. Obsérvese, por ejemplo, que $(1, 1, 1) \in W$ pero $2 \cdot (1, 1, 1) = (2, 2, 2) \notin W$, lo que contradice la segunda propiedad.

Ejemplo 3.

$$W = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + y + z = 0,\ 2x - 3y - z = 0\}$$

es un subespacio de $\mathbb{R}^3$. También es un subespacio de

$$V = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + y + z = 0\}.$$

La conclusión de estos ejemplos debería ser que siempre que pongamos condiciones lineales y homogéneas en $\mathbb{R}^n$, obtenemos un subespacio. Esto está estrechamente relacionado con que el ejemplo 6 de la página anterior fuera un espacio vectorial.

Veamos otros ejemplos fuera de $\mathbb{R}^n$

Ejemplo 4.

$$\{P \in \mathbb{R}[x] \,/\, P'(1) = 0\}$$

es un subespacio de $\mathbb{R}[x]$. Comprobarlo se reduce a usar la linealidad de la derivada, es decir, $(P + Q)' = P' + Q'$ y $(\lambda P)' = \lambda P'$.

Ejemplo 5. $\mathbb{P}_n[x]$ es un subespacio de $K[x]$.

Ejemplo 6. Los polinomios de grado exactamente dos no forman un subespacio de $\mathbb{R}[x]$, ya que x^2+x+1 y $3x-x^2+5$ tienen grado exactamente dos pero su suma no.

DEFINICIÓN: *Si $\vec{v}, \vec{u_1}, \vec{u_2}, \ldots, \vec{u_n} \in V$, se dice que $\vec{v}$ es una combinación lineal de $\vec{u_1}$, $\vec{u_2}$, $\ldots$ $\vec{u_n}$ si existen $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ tales que*

$$\vec{v} = \lambda_1\vec{u_1} + \lambda_2\vec{u_2} + \ldots + \lambda_n\vec{u_n}.$$

Ejemplo 1. En $\mathbb{R}^2$ todo vector $\vec{u} = (x, y)$ es combinación lineal de $\vec{u_1} = (1, 0)$ y $\vec{u_2} = (0, 1)$, porque

$$\vec{u} = x\vec{u_1} + y\vec{u_2}.$$

Ejemplo 2. En $\mathbb{R}^3$, $(2, 5, 5)$ es combinación lineal de $(2, 1, -1)$ y $(0, 2, 3)$ porque

$$(2, 5, 5) = 1 \cdot (2, 1, -1) + 2 \cdot (0, 2, 3).$$

Ejemplo 3. En $\mathbb{R}^2$, $(2, 6)$ es combinación lineal de $(3, 9)$ porque $(2, 6) = \dfrac{2}{3}(3, 9)$.

Ejemplo 4. En un espacio vectorial, el elemento neutro de la suma, normalmente denotado por $\vec{0}$, es combinación lineal de cualquier vector, $\vec{v}$, porque $\vec{0} = 0 \cdot \vec{v}$ (ejercicio).

DEFINICIÓN: *Dado un subconjunto, C, de un espacio vectorial, se llama subespacio generado por C, y se denota por $\langle C\rangle$ o $\mathcal{L}(C)$, al conjunto formado por todas la combinaciones lineales de vectores de C.*

La propia notación sugiere

Proposición 1.1 : *Si $C \subset V$, $\langle C\rangle$ es un subespacio vectorial de V.*

Ejemplo 1. En $\mathbb{R}^2$

$$\langle(1, 0), (0, 1)\rangle = \{\lambda_1(1, 0) + \lambda_2(0, 1)\} = \mathbb{R}^2,$$

ya que en un ejemplo anterior habíamos visto que todo vector de $\mathbb{R}^2$ es una combinación lineal de $(1, 0)$ y $(0, 1)$.

Ejemplo 2. En $\mathbb{R}[x]$

$$\langle 1, (x-1)^2\rangle = \{\lambda_1 + \lambda_2(x-1)^2\}.$$

Algunas veces el conjunto C contiene información redundante, es decir, genera un subespacio utilizando más vectores de los que son necesarios. Veamos esto en un ejemplo

Ejemplo 3. Sea $C = \{(1, 1, 2), (0, 2, -1), (1, 3, 1)\} \subset \mathbb{R}^3$, entonces

$$\begin{aligned}\langle C\rangle &= \{\lambda(1, 1, 2) + \mu(0, 2, -1) + \nu(1, 3, 1)\}\\ &= \{(\lambda+\nu, \lambda+2\mu+3\nu, 2\lambda-\mu+\nu) \,/\, \lambda, \mu, \nu \in \mathbb{R}\}\end{aligned}$$

como $(1,3,1)$ es una combinación lineal de $(1,1,2)$ y $(0,2,-1)$, concretamente

$$(1,3,1) = (1,1,2) + (0,2,-1),$$

se tiene que el vector $(1,3,1)$ se puede omitir, es decir,

$$\langle C\rangle = \langle (1,1,2),(0,2,-1)\rangle.$$

La situación anterior sugiere que conviene definir el concepto de que en un conjunto haya alguna dependencia de unos vectores con otros.

DEFINICIÓN: *Se dice que un conjunto de vectores, C, es* <u>linealmente independiente</u> *si para cualquier subconjunto finito, $\{\vec{v_1},\vec{v_2},\ldots,\vec{v_n}\}\subset C$, la igualdad*

$$\lambda_1\vec{v_1} + \lambda_2\vec{v_2} + \ldots + \lambda_n\vec{v_n} = 0$$

sólo se satisface para $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$. En caso contrario se dice que C es <u>linealmente dependiente</u>.

<u>Nota</u>: Muchas veces se habla de que varios vectores son linealmente independientes (o dependientes), esto quiere decir que forman un conjunto linealmente independiente (o dependiente), en ese caso se puede tomar como subconjunto finito el formado por ellos mismos.

<u>Ejemplo 1</u>. Sea $C = \{x^2+1, x^2-1, x^2+x+1\}\subset\mathbb{R}[x]$. Comprobemos que C es un conjunto linealmente independiente y que $\langle C\rangle$ se puede describir de manera sencilla.

Si una combinación lineal de los elementos de C es el polinomio nulo

$$\lambda_1(x^2+1) + \lambda_2(x^2-1) + \lambda_3(x^2+x+1) = 0,$$

e igualando los coeficientes de términos del mismo grado se llega a

$$\left.\begin{aligned} \lambda_1+\lambda_2+\lambda_3 &= 0\\ \lambda_3 &= 0\\ \lambda_1-\lambda_2+\lambda_3 &= 0 \end{aligned}\right\} \Rightarrow\ \lambda_1=\lambda_2=\lambda_3=0.$$

Así que C es linealmente independiente. Veamos ahora cómo describir el subespacio generado por C de forma sencilla. Nótese que de la definición sólo se consigue

$$\langle C\rangle = \{\lambda_1(x^2+1) + \lambda_2(x^2-1) + \lambda_3(x^2+x+1) \,/\, \lambda_1,\lambda_2,\lambda_3\in\mathbb{R}\}.$$

Pero por otra parte

$$(x^2+1),(x^2-1)\in V \Rightarrow\ \frac{1}{2}(x^2+1) + \frac{-1}{2}(x^2-1) = 1\in V$$

$$\begin{aligned} (x^2+x+1),(x^2+1)\in V &\Rightarrow\ (x^2+x+1) + (-1)(x^2+1) = x\in V\\ (x^2+x+1),x,1\in V &\Rightarrow\ (x^2+x+1) + (-1)x + (-1)1 = x^2\in V, \end{aligned}$$

por tanto $1, x, x^2 \in \langle C \rangle$. Como $\mathbb{P}_2[x]$ está formado exatamente por todas combinaciones lineales de $1, x, x^2$, se tiene $\mathbb{P}_2[x] \subset \langle C \rangle$ y como es evidente $\langle C \rangle \subset \mathbb{P}_2[x]$ (porque los polinomios de C tienen grado menor o igual que dos) se tiene finalmente

$$\langle C \rangle = \mathbb{P}_2[x].$$

Ejemplo 2. Los vectores de $\mathbb{R}^3$, $(1,1,0), (2,1,1), (5,3,2)$ no son linealmente independientes. Porque escribiendo la combinación lineal

$$\lambda_1(1,1,0) + \lambda_2(2,1,1) + \lambda_3(5,3,2) = (0,0,0)$$

se llega la sistema

$$\left.\begin{aligned} \lambda_1 + 2\lambda_2 + 5\lambda_3 =& 0 \\ \lambda_1 + \lambda_2 + 3\lambda_3 =& 0 \\ \lambda_2 + 2\lambda_3 =& 0 \end{aligned}\right\} \Rightarrow \quad \begin{aligned} \lambda_2 =& -2\lambda_3 \\ \lambda_1 =& -\lambda_3 \end{aligned}$$

y como las soluciones dependen de un parámetro hay infinitas. Tomando por ejemplo $\lambda_3 = 1$, obtenemos $\lambda_1 = -1$ y $\lambda_2 = -2$ que corresponde a la combinación lineal

$$-1(1,1,0) - 2(2,1,1) + 1(5,3,2) = (0,0,0).$$

Para terminar esta sección veamos dos ejemplos un poco más difíciles

Ejemplo 3. Es fácil percatarse de que el conjunto $V = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$ es un espacio vectorial sobre $\mathbb{R}$ (las funciones se pueden sumar y multiplicar por números). Vamos a comprobar que el subconjunto de V dado por $C = \{x^2 - 3x, x^3 - 1, \operatorname{sen} x, \cos x\}$ es linealmente independiente. Para ello tenemos que probar que

$$\lambda_1(x^2 - 3x) + \lambda_2(x^3 - 1) + \lambda_3 \operatorname{sen} x + \lambda_4 \cos x = 0$$

sólo tiene la solución $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0$. Podríamos dar valores a la x y deducir varios sistemas de ecuaciones lineales que nos llevarían a esa solución, pero hagamos algo más ingenioso y breve:

$$\lambda_1(x^2 - 3x) + \lambda_2(x^3 - 1) = -\lambda_3 \operatorname{sen} x - \lambda_4 \cos x$$

implica que ambos términos son constantes, porque el de la derecha es una función acotada y el de la izquierda es un polinomio, y los únicos polinomios acotados son las constantes. Pero si el polinomio de la izquierda es constante debe ser $\lambda_1 = \lambda_2 = 0$ (obsérvense los términos de segundo y tercer grado). También se deduciría (despejando) que si λ_3 ó $\lambda_4 \neq 0$, $\operatorname{sen} x$ y $\cos x$ son uno múltiplo del otro para todo x, y eso es obviamente falso (tómese $x = 0$ y $x = \pi/2$).

Ejemplo 4. Es fácil comprobar que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$ es un espacio vectorial sobre

$K = \mathbb{Q}$. Veamos si el conjunto $C = \{1, \sqrt{2}\}$ es linealmente independiente.

$$\lambda_1 \cdot 1 + \lambda_2 \sqrt{2} = 0,\ \lambda_1, \lambda_2 \in \mathbb{Q} - \{0\} \ \Leftrightarrow\ \sqrt{2} = -\frac{\lambda_1}{\lambda_2}\ \lambda_1, \lambda_2 \in \mathbb{Q} - \{0\}.$$

Por tanto $C = \{1, \sqrt{2}\}$ es linealmente independiente si y sólo si $\sqrt{2}$ es un número racional. Si $\sqrt{2}$ fuera un número racional, digamos $\sqrt{2} = m/n$ con $m, n \in \mathbb{Z}^+$. Entonces podemos suponer que m o n es impar, porque si ambos fueran pares podríamos simplificar la fracción, pero

$$\sqrt{2} = \frac{m}{n} \ \Rightarrow\ 2m^2 = n^2 \ \Rightarrow\ n \text{ par } \Rightarrow\ n = 2k$$

$$\Rightarrow\ m^2 = 2k^2 \ \Rightarrow\ m \text{ par } .$$

con lo que se llega a una contradicción.

5.2. Base, dimensión, teorema de Steinitz, cambio de base

En los espacios vectoriales es conveniente considerar subconjuntos que generen todo el espacio y que tenga el mínimo número de vectores posibles. De alguna forma, el "tamaño" de estos conjuntos determina el tamaño del espacio vectorial.

Definición: *Se dice que un conjunto, B, es una* base *de un espacio vectorial V, si se cumple*

$$1)\ \langle B \rangle = V \qquad 2)\ B \text{ es linealmente independiente.}$$

A veces se indica la propiedad 1) diciendo que B es un sistema de generadores.

Ejemplo 1. $B = \{(1,0), (0,1)\}$ es una base de $\mathbb{R}^2$.

Ya habíamos comprobado que todo vector de $\mathbb{R}^2$ es combinación lineal de $(1,0)$ y $(0,1)$, por tanto se cumple 1). Por otra parte, es muy sencillo comprobar que estos vectores son linealmente independientes, así que también se cumple 2).

Ejemplo 2. $B = \{x^2+1, x^2-1, x^2+x+1\}$ es una base de $\mathbb{P}_2[x]$, porque ya habíamos comprobado en un ejemplo anterior que los elementos de B son linealmente independientes y generan todo $\mathbb{P}_2[x]$.

Ejemplo 3. $B = \{x^2+1, x^2-1, x^2+x+1\}$ es una base de $\mathbb{P}_2[x]$.

Por definición,

$$\mathbb{P}_2[x] = \{a + bx + cx^2 \,/\, a, b, c \in \mathbb{R}\},$$

así que todo elemento de $\mathbb{P}_2[x]$ es combinación lineal de 1, x y x^2, por tanto se cumple 1). De nuevo, verificar la independencia lineal es muy sencillo.

Ejemplo 4. $B = \{(1,1),(1,-1)\}$ es una base de $\mathbb{R}^2$.

Para saber si 1) es cierto tenemos que estudiar si

$$(x,y) = \lambda(1,1) + \mu(1,-1)$$

siempre tiene solución λ, μ, para cualquier $(x,y) \in \mathbb{R}^2$. Esto conduce al sistema

$$\left.\begin{aligned} \lambda + \mu &= x \\ \lambda - \mu &= y \end{aligned}\right\} \Leftrightarrow \ \lambda = \frac{x+y}{2}, \ \mu = \frac{x-y}{2}.$$

Como siempre hay solución, se cumple 1). Comprobar la independencia lineal de B nos lleva a considerar

$$(0,0) = \lambda(1,1) + \mu(1,-1),$$

que podemos resolver como antes obteniendo $\lambda = \nu = 0$.

Ejemplo 5. $B = \{(1,2,1),(1,0,1),(0,0,1)\}$ es una base de $\mathbb{R}^3$.

Como antes, la propiedad 1) nos lleva a estudiar si hay soluciones λ, μ, ν de

$$(x,y,z) = \lambda(1,2,1) + \mu(1,0,1) + \nu(0,0,1)$$

para cualquier $(x,y,z) \in \mathbb{R}^3$. Esta fórmula equivale al sistema

$$\left.\begin{aligned} \lambda + \mu \qquad &= x \\ 2\lambda \qquad\qquad &= y \\ \lambda + \mu + \nu &= z \end{aligned}\right\} \Leftrightarrow \ \lambda = \frac{y}{2}, \ \mu = \frac{2x-y}{2}, \ \nu = z - x.$$

La existencia de esta solución implica que B genera todo $\mathbb{R}^3$ y por tanto se cumple 1). La comprobación de la independencia lineal nos lleva al mismo sistema con $x = y = z = 0$ y por tanto la solución que se obtiene es $\lambda = \mu = \nu = 0$, y B es linealmente independiente.

Ejemplo 6. $B = \{(1,2,1),(1,0,1),(0,0,1),(2,2,3)\}$ no es una base de $\mathbb{R}^3$.

Estudiamos las soluciones $\lambda, \mu, \nu, \kappa$ de

$$(x,y,z) = \lambda(1,2,1) + \mu(1,0,1) + \nu(0,0,1) + \kappa(2,2,3).$$

Que equivale al sistema lineal

$$\left.\begin{aligned} \lambda + \mu \qquad + 2\kappa &= x \\ 2\lambda \qquad\qquad + 2\kappa &= y \\ \lambda + \mu + \nu + 3\kappa &= z \end{aligned}\right\} \Leftrightarrow \ \lambda = \frac{y-2\kappa}{2}, \ \mu = \frac{2x-y-2\kappa}{2}, \ \nu = z - x - \kappa.$$

donde κ es arbitrario. Esto implica que incluso hay un número infinito de soluciones al expresar un vector como combinación lineal de los elementos de B, en particular, se cumple 1). Por otra parte, es fácil comprobar que el razonamiento anterior implica que hay soluciones no triviales para

$$(0,0,0)=\lambda(1,2,1)+\mu(1,0,1)+\nu(0,0,1)+\kappa(2,2,3),$$

así pues B no es linealmente independiente y por tanto no es base.

Ejemplo 7. $B=\{(1,3,1),(1,1,1)\}$ no es una base de $\mathbb{R}^3$.

Si B fuera sistema de generadores, entonces

$$(x,y,z)=\lambda(1,3,1)+\mu(1,1,1)$$

tendría solución para cualquier $(x,y,z)\in\mathbb{R}^3$. Lo que implica

$$\left.\begin{aligned}\lambda+\mu&=x\\3\lambda+\mu&=y\\\lambda+\mu&=z\end{aligned}\right\}$$

Pero este sistema sólo puede tener solución cuando $x=z$ (obsérvense la primera y tercera ecuaciones), por tanto no todo vector está generado por B.

Ejemplo 8. Estudiar si $B=\{1,\operatorname{sen}x,x\}\subset\{f:\mathbb{R}\longrightarrow\mathbb{R}\}$ es una base de $\langle B\rangle$.

Nótese que, por definición, B es sistema de generadores, por tanto sólo hay que comprobar que es linealmente independiente. Esto equivale a probar que si λ,μ,ν cumplen

$$\lambda+\mu\operatorname{sen}x+\nu x=0$$

para todo x, entonces $\lambda=\mu=\nu=0$. hay varias maneras de demostrar esto. Quizá la más mecánica sea dar algunos valores adecuados a x y resolver el sistema de ecuaciones que resulta. Sin embargo es más corto y elegante proceder de la siguiente manera que me fue sugerida por un alumno:

Derivando sucesivas veces obtenemos

$$\begin{aligned}\lambda+\mu\operatorname{sen}x+\nu x&=0\\\mu\cos x+\nu&=0\\-\mu\operatorname{sen}x&=0\end{aligned}$$

La última ecuación implica $\mu=0$ y de las otras se deduce $\lambda=\nu=0$.

Antes de seguir, fijaremos nuestra atención en aquellos espacios vectoriales que tienen bases con un número finito de elementos.

DEFINICIÓN: *Se dice que un espacio vectorial tiene* dimensión finita *si tiene una base con un número finito de elementos. En caso contrario, se dice que tiene* dimensión infinita.

Observación: Si S es finito, entonces $V = \langle S \rangle \Rightarrow V$ es de dimensión finita (ejercicio).

En este curso nos centraremos en los espacios vectoriales de dimensión finita, pero queremos dejar claro que entender algunos fenómenos físicos requiere manejar espacios vectorial de dimensión infinita, muchos de ellos son subespacios del espacio de funciones reales.

Veamos algunos espacios vectoriales de dimensión finita y alguna de sus bases

Ejemplo 1. $B = \{(1,0,0,\ldots,0),(0,1,0,\ldots,0),(0,0,1,\ldots,0),\ldots,(0,0,0,\ldots,1)\}$ es una base de $\mathbb{R}^n$ que se suele llamar base canónica.

Ejemplo 2. Una base del espacio de matrices $\mathcal{M}_{n\times m}(K)$ viene dada por

$$B = \{\epsilon_{11}, \epsilon_{12}, \epsilon_{13}, \ldots \epsilon_{mn}\}$$

donde ϵ_{ij} es la matriz que cuyo coeficiente ij es uno y el resto son ceros. Por ejemplo, una base de $\mathcal{M}_{2\times 2}(\mathbb{R})$ es

$$B = \{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \}.$$

Ejemplo 3. Se dice que una matriz (a_{ij}) es simétrica si $a_{ij} = a_{ji}$. Una base del espacio de matrices simétricas $n \times n$, $\mathcal{S}_n(\mathbb{R})$, viene dada por

$$B = \{\epsilon_{11}, \epsilon_{22}, \epsilon_{33}, \ldots, \epsilon_{nn}, \epsilon_{12} + \epsilon_{21}, \epsilon_{13} + \epsilon_{31}, \ldots, \epsilon_{n-1\,n} + \epsilon_{n\,n-1}\}$$

donde ϵ_{ij} es como antes. Por ejemplo, una base de $\mathcal{S}_2(\mathbb{R})$ es

$$B = \{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}.$$

Ejemplo 4. El conjunto $B = \{1, x, x^2, x^3, \ldots, x^n\}$ es una base de $\mathbb{P}_n[x]$.

Como ya hemos comentado, nos centraremos en los espacios de dimensión finita, no obstante, antes de seguir veamos dos ejemplos de dimensión infinita.

Ejemplo . $\mathbb{R}[x]$ tiene dimensión infinita.

Un conjunto finito de polinomios $P_1, P_2, \ldots, P_n$ sólo puede generar polinomios que tengan grado menor o igual que el mayor de los grados de los P_i, así pues no se obtienen todos los de $\mathbb{R}[x]$.

Ejemplo . El espacio de todas las funciones reales, $\mathcal{F} = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$ tiene dimensión infinita (ejercicio).

Veamos ahora cómo calcular bases en algunos ejemplos prácticos.

Ejemplo 1. Hallar una base de $V = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + y + z = 0\}$.

Lo mejor en ejemplos de este tipo es expresar las condiciones que definen el subespacio en forma paramétrica, esto es, dependiendo de parámetros que pueden tomar valores arbitrarios. En nuestro caso, nótese que

$$\vec{v} \in V \;\Leftrightarrow\; \vec{v} = (-y - z, y, z)$$

donde y, z pueden tomar cualquier valor real. Por tanto

$$\begin{aligned} \vec{v} \in V \;&\Rightarrow\; \vec{v} = y(-1, 1, 0) + z(-1, 0, 1) \\ &\Rightarrow\; \vec{v} \in \langle(-1, 1, 0), (-1, 0, 1)\rangle \end{aligned}$$

lo que demuestra que $B = \{(-1, 1, 0), (-1, 0, 1)\}$ es sistema de generadores. Es fácil ver que B es también linealmente independiente, por tanto, es base.

Ejemplo 2. Hallar una base de $V = \{(x, y, z, t) \in \mathbb{R}^4 \,/\, x + y + z = 0,\ x + 3t = 0\}$.

Procediendo como antes, intentamos escribir las condiciones en términos de parámetros. Resolviendo

$$x + y + z = 0,\ x + 3t = 0 \;\Leftrightarrow\; x = -3t,\ y = 3t - z$$

donde t, z son arbitrarios. Por tanto

$$\vec{v} \in V \;\Leftrightarrow\; \vec{v} = (-3t, 3t - z, z, t).$$

De donde

$$\begin{aligned} \vec{v} \in V \;&\Rightarrow\; \vec{v} = z(0, -1, 1, 0) + t(-3, 3, 0, 1) \\ &\Rightarrow\; \vec{v} \in \langle(0, -1, 1, 0), (-3, 3, 0, 1)\rangle \end{aligned}$$

lo que demuestra que $B = \{(0, -1, 1, 0), (-3, 3, 0, 1)\}$ es sistema de generadores. De nuevo es fácil ver B es linealmente independiente y por tanto, base.

A continuación veremos un teorema del que deduciremos dos importantes corolarios.

Teorema 2.1 (de Steinitz): *Sea $B = \{\vec{u_1}, \vec{u_2}, \ldots, \vec{u_n}\}$ una base de un espacio vectorial V, y sean $\vec{v_1}$, $\vec{v_2}$, $\ldots$,$\vec{v_m}$, m vectores linealmente independientes ($m \leq n$), entonces existen m vectores de B que se pueden sustituir por $\vec{v_1}$, $\vec{v_2}$, $\ldots$,$\vec{v_m}$, obteniéndose una nueva base.*

A pesar de que el teorema sólo tiene interés teórico queremos dar un ejemplo para no mal interpretar su enunciado.

Ejemplo . Consideremos la base canónica de $\mathbb{R}^3$ $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ y el conjunto de vectores linealmente independientes $C = \{(0,1,0),(1,2,1)\}$. En la notación del teorema tenemos $n=3$, $m=2$ y

$$\vec{u_1} = (1,0,0), \qquad \vec{u_2} = (0,1,0), \qquad \vec{u_3} = (0,0,0)$$
$$\vec{v_1} = (0,1,0), \qquad \vec{v_2} = (1,2,1).$$

Nótese que $\vec{u_2}$ y $\vec{u_3}$ se pueden sustituir por $\vec{v_1}$ y $\vec{v_2}$ obteniendo la base de $\mathbb{R}^3$ dada por $B' = \{(1,0,0),(0,1,0),(1,2,1)\}$, pero si sustituimos $\vec{u_1}$ y $\vec{u_3}$ por $\vec{v_1}$ y $\vec{v_2}$ no obtenemos una base.

Corolario 2.2: *En un espacio de dimensión finita todas las bases tienen el mismo número de vectores.*

Dem.: Si B y B' son bases con $|B| < |B'|$, digamos $|B| = m$, $|B'| = n$, entonces, según el teorema podríamos forman una nueva base B'' tal que $B'' \supset B$ con $B'' \neq B$, pero como $\langle B\rangle$ es todo el espacio, esto implicaría que los vectores de $B'' - B$ dependen linealmente de los de B y por tanto B'' no es linealmente independiente. ■

Ahora llegamos a la anunciada definición del "tamaño" de un espacio vectorial.

Definición: *Se llama dimensión de un espacio vectorial (de dimensión finita) al cardinal de cualquiera de sus bases.*

Nota: Normalmente se completa la definición anterior diciendo que el espacio vectorial trivial $V = \{\vec{0}\}$ (el que sólo contiene al vector $\vec{0}$) tiene dimensión cero.

Anteriormente hemos dado bases de $\mathbb{R}^n$, $\mathcal{M}_{n\times m}(K)$, $\mathcal{S}_n(K)$ (las matrices simétricas $n\times n$) y de $\mathbb{P}_n[x]$. Contando los elementos de dichas bases obtenemos

$$\dim \mathbb{R}^n = n, \qquad \dim \mathcal{M}_{n\times m}(K) = nm, \qquad \dim \mathcal{S}_n(K) = \frac{n(n+1)}{2}, \qquad \dim \mathbb{P}_n[x] = n+1.$$

Estas fórmulas son de interés porque el siguiente corolario evita la comprobación de que una posible base es sistema de generadores si sabemos de antemano la dimensión del espacio vectorial.

Corolario 2.3: *En un espacio de dimensión n, cualesquiera n vectores linealmente independientes forman una base.*

Ejemplo 1. Estudiar si $B = \{(1,2,1),(1,2,0),(0,1,1)\}$ es una base de $\mathbb{R}^3$.

Según el corolario anterior basta ver que sus elementos son tres vectores linealmente independientes ($\dim \mathbb{R}^3 = 3$).

$$\lambda(1,2,1) + \mu(1,2,0) + \nu(0,1,1) = (0,0,0)$$

tiene solución única $\lambda = \mu = \nu = 0$

$$\left.\begin{array}{r}\lambda + \mu \quad\; = 0 \\ 2\lambda + 2\mu + \nu = 0 \\ \lambda \quad\; + \nu = z\end{array}\right\} \Leftrightarrow \lambda = \mu = \nu = 0.$$

Por tanto B es una base.

<u>Ejemplo 2</u>. Estudiar si

$$B = \{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \}$$

es una base de $\mathcal{S}_2(\mathbb{R})$.

De nuevo, como $\dim \mathcal{S}_3(\mathbb{R}) = \frac{3(3+1)}{2} = 3$, basta comprobar que los vectores de B son linealmente independientes, y esto se reduce a comprobar que el sistema

$$\lambda \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \mu \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} + \nu \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

tiene solución única $\lambda = \mu = \nu = 0$.

Ya sabemos que todo vector se puede escribir como combinación lineal de los elementos de una base. Los números que aparecen como coeficientes caracterizan al vector, por ello tiene sentido considerar la siguiente definicición

DEFINICIÓN: *Sea V un espacio vectorial de dimensión finita y $B = \{\vec{u_1}, \vec{u_2}, \dots, \vec{u_n}\}$ una de sus bases. Se dice que las <u>coordenadas</u> de cierto vector $\vec{v} \in V$ en la base B son $(\lambda_1, \lambda_2, \dots, \lambda_n)$, si*

$$\vec{v} = \lambda_1 \vec{u_1} + \lambda_2 \vec{u_2} + \ldots + \lambda_n \vec{u_n}.$$

<u>Nota</u>: Muchas veces se escribe (con el abuso de notación evidente) $\vec{v} = (\lambda_1, \lambda_2, \dots, \lambda_n)$. Pero cuando se use esta notación debe estar claro cuál es la base que estamos considerando. También es conveniente observar que las coordenadas dependen de la ordenación de los elementos de la base. Así pues, en rigor, las coordenadas no están sólo asociadas a la base, sino a la forma de ordenar sus elementos.

<u>Ejemplo 1</u>. Hallar las coordenadas de $\vec{v} = (19, -8) \in \mathbb{R}^2$ en la base canónica $B = \{(1, 0), (0, 1)\}$ y en $B' = \{(2, 1), (3, -2)\}$.

Es evidente que

$$\vec{v} = 19(1, 0) + (-8)(0, 1)$$

así que las coordenadas de $\vec{v}$ en B son $(19, -8)$. Para hallar las coordenadas con respecto a B' tenemos que resolver el sistema

$$\vec{v} = \lambda(2,1) + \mu(3,-2).$$

Algunos sencillos cálculos prueban $\lambda = 2$, $\mu = 5$, así pues, en la base B' se tiene $\vec{v} = (2,5)$.

Ejemplo 2. Hallar las coordenadas de $x^3 + x^2 - 1 \in \mathbb{P}_3[x]$ con respecto a la base $B = \{x^2 + x, x^3 - 3x^2 - x + 1, 1, 3x^2 - 1\}$.

Como antes, esto conduce a resolver

$$x^3 + x^2 - 1 = a(x^2 + x) + b(x^3 - 3x^2 - x + 1) + c + d(3x^2 - 1) \qquad a, b, c, d \in \mathbb{R}.$$

Comparando términos de igual grado se obtiene

$$\left.\begin{aligned} b =& 1 \\ a - 3b + 3d =& 1 \\ a - b =& 0 \\ b + c - d =& -1 \end{aligned}\right\} \Rightarrow \; b = 1, \; a = 1, \; c = -1, \; d = 1,$$

por tanto, las coordenadas son $(1, 1, -1, 1)$.

Como hemos indicado al comienzo del capítulo, el concepto de vector está fuertemente motivado por la Física. También dentro del contexto físico, podemos entender las coordenadas como números que “miden” un vector. Las diferentes bases están asociadas a diferentes maneras de “medir” los vectores. Un principio fundamental afirma que las leyes Físicas debieran ser esencialmente independientes de la forma de medir del observador, por ello tiene un gran interés saber transformar las coordenadas de un vector de una base a otra.

Con estas ideas en mente, analicemos con un poco más detalle el penúltimo ejemplo. Habíamos visto que

$$\vec{v} = (19, -8) \text{ en la base } B \text{ (canónica)}, \qquad \vec{v} = (2,5) \text{ en la base } B'.$$

La última afirmación significa que

$$\vec{v} = (19, -8) = \lambda(2,1) + \mu(3,-2). \qquad \text{con } \lambda = 2, \; \mu = 5.$$

Los valores de λ y μ se obtuvieron al resolver un sistema, que en forma matricial se puede escribir como

$$\begin{pmatrix} 19 \\ -8 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix}.$$

Obsérvese que las columnas de esta matriz son justamente las coordenadas de los vectores de B' en la base canónica, B.

Es fácil percatarse de que la situación es la misma en general, y por tanto se deduce el siguiente resultado

Proposición 2.4: *Sean B y $B' = \{\vec{b'_1}, \vec{b'_2}, \dots, \vec{b'_n}\}$ bases de V. Supongamos que las coordenadas de $\vec{v}$ y de $\vec{b'_j}$, $1 \le j \le n$, en la base B son respectivamente*

$$(v_1, v_2, \dots, v_n) \quad y \quad (b'_{1j}, b'_{2j}, b'_{3j}, \dots, b'_{nj})$$

entonces las coordenadas de $\vec{v}$ en B', $(v'_1, v'_2, \dots, v'_n)$, verifican

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} b'_{11} & b'_{12} & \dots\dots & b'_{1n} \\ b'_{21} & b'_{22} & \dots\dots & b'_{2n} \\ \dots & \dots & \dots\dots & \dots \\ b'_{n1} & b'_{n2} & \dots\dots & b'_{nn} \end{pmatrix} \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_n \end{pmatrix}.$$

<u>Observación</u>: Nótese que la matriz $\begin{pmatrix} b'_{ij} \end{pmatrix}$ está formada por las coordenadas de los vectores de B' en B colocadas en columna.

De la proposición anterior se deduce que cambiar de base es equivalente a multiplicar por una matriz. Para referirnos a esa matriz es conveniente considerar la siguiente definición

DEFINICIÓN: *Dadas dos bases B y B' de un espacio vectorial de dimensión n, se llama <u>matriz de cambio de base</u> de B' a B a la matriz, $M_{B'B} \in \mathcal{M}_{n\times n}(K)$, que al ser multiplicada por las coordenadas de un vector en la base B' produce las coordenadas en la base B.*

<u>Nota</u>: En la proposición anterior $M_{B'B} = \begin{pmatrix} b'_{ij} \end{pmatrix}$.

<u>Ejemplo</u> . Hallar una base, B, del subespacio $V = \{(x, y, z) \,/\, x + 2y + 2z = 0\}$. Demostrar que $B' = \{(4, -1, -1), (-8, 1, 3)\}$ es también una base, y hallar las matrices de cambio de base $M_{B'B}$ y $M_{BB'}$.

Para hallar una base de V escribimos las ecuaciones que definen el subespacio de forma paramétrica

$$\begin{aligned} \vec{v} \in V \; &\Leftrightarrow \vec{v} = (-2y - 2z, y, z) \quad \text{con } y, z \in \mathbb{R}. \\ &\Leftrightarrow \vec{v} = y(-2, 1, 0) + z(-2, 0, 1). \end{aligned}$$

Con esto hemos probado

$$V = \langle(-2,1,0),(-2,0,1)\rangle,$$

además como estos dos vectores son linealmente independientes, se tiene que

$$B = \{(-2,1,0),(-2,0,1)\}$$

es una base de V. Esto prueba que V tiene dimensión 2, entonces, por el Corolario 2.3, para comprobar que B' es base basta ver que los dos vectores que la forman son linealmente independientes y eso se reduce a un sencillo cálculo.

La matriz $M_{B'B}$ tiene dimensiones 2×2 y, como ya hemos comentado, está formada por las coordenadas de los vectores de B' escritas en columna, pero estas coordenadas deben estar expresadas respecto a la base B. Siguiendo la notación de la proposición, las coordenadas de $(4,-1,-1)$ son b'_{11} y b'_{21}. Por la definición de coordenadas

$$(4,-1,-1) = b'_{11}(-2,1,0) + b'_{21}(-2,0,1),$$

lo cual, resolviendo, implica $b'_{11} = -1$, $b'_{21} = -1$. De la misma manera las coordenadas de $(-8,1,3)$ respecto a B son $b'_{12} = 1$ y $b'_{22} = 3$, que son las soluciones del sistema

$$(-8,1,3) = b'_{12}(-2,1,0) + b'_{22}(-2,0,1).$$

Todo esto demuestra que la matriz de cambio de base de B' a B es

$$M_{B'B} = \begin{pmatrix} -1 & 1 \\ -1 & 3 \end{pmatrix}.$$

Es decir, si (x,y) son las coordenadas de un vector en la base B y (x',y') son las coordenadas de ese mismo vector en la base B', se tiene

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Por tanto, si quisiéramos expresar las coordenadas en B' en términos de las coordenadas en B, usaríamos

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix},$$

con esto hemos probado

$$M_{BB'} = \begin{pmatrix} -1 & 1 \\ -1 & 3 \end{pmatrix}^{-1}.$$

También podríamos haber hallado esta matriz repitiendo todo el procedimiento anterior intercambiando el papel de B y B', pero sería más largo.

No es difícil comprobar que la relación entre $M_{B'B}$ y $M_{BB'}$ de este ejemplo se generaliza a otros. Tampoco es muy difícil sospechar que como pasar de B a B'' directamente es equivalente a pasar de B a B' y después de B' a B'', las matrices de cambio de base involucradas deben estar relacionadas. Todo esto queda resumido en la siguiente proposición

Proposición 2.5 : *Sean B, B' y B'' bases de un espacio vectorial de dimensión finita, V, entonces*

$$i)\ M_{BB'} = M_{B'B}^{-1} \qquad ii)\ M_{BB''} = M_{B'B''}M_{BB'}.$$

<u>Ejemplo</u> . Para un observador, un proyectil describe la trayectoria $\vec{s}(t) = (t, 2t - t^2)$ en la base usual (la canónica). Calcular la trayectoria para un observador en una base girada 45^o en sentido positivo.

El problema se reduce a encontrar la matriz de cambio de base de B a B' donde B es base usual y B' es la otra. Es decir

$$B = \{(1,0),(0,1)\} \qquad B' = \{(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}), (-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})\}.$$

Las coordenadas de los vectores de la segunda base se obtienen fácilmente dibujando B' y utilizando que $\operatorname{sen} 45^o = \cos 45^o = \sqrt{2}/2$.

Sea $\vec{s}_1(t)$ la trayectoria observada desde B', es decir, las coordenadas de $\vec{s}(t)$ en B', entonces

$$\vec{s}(t) = \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{pmatrix} \vec{s}_1(t).$$

sustituyendo las coordenadas de $\vec{s}(t)$

$$\begin{pmatrix} t \\ 2t - t^2 \end{pmatrix} = \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{pmatrix} \vec{s}_1(t).$$

Calculando la matriz inversa se obtiene finalmente

$$\vec{s}_1(t) = \begin{pmatrix} \sqrt{2}/2 & \sqrt{2}/2 \\ -\sqrt{2}/2 & \sqrt{2}/2 \end{pmatrix} \begin{pmatrix} t \\ 2t - t^2 \end{pmatrix} = (\frac{\sqrt{2}}{2}(3t - t^2), \frac{\sqrt{2}}{2}(t - t^2)).$$

<u>Ejemplo</u> . Hallar una base, B, de $V = \{P \in \mathbb{P}_3[x] \,/\, P'(1) = 0\}$ y calcular las

coordenadas de $(x-1)^2$ en esa base. Hallar también las matrices de cambio de base de B a $B' = \{1, (x-1)^2, (x-1)^3\}$.

Obsérvese que

$$P = a + bx + cx^2 + dx^3 \text{ cumple } P'(1) = 0 \;\Leftrightarrow\; b + 2c + 3d = 0.$$

Despejando la variable b y suponiendo las otras parámetros que toman valores reales arbitrarios, se tiene

$$P \in V \;\Leftrightarrow\; P = a + c(-2x + x^2) + d(-3x + x^3).$$

Por tanto $B = \{1, -2x+x^2, -3x+x^3\}$ es un sistema de generadores. Como los elementos de B son linealmente independientes, se tiene que B es una base de V. Hallar las coordenadas $(\lambda_1, \lambda_2, \lambda_3)$ de $(x-1)^2$ con respecto a B, se reduce a resolver

$$(x-1)^2 = x^2 - 2x + 1 = \lambda_1 + \lambda_2(-2x + x^2) + \lambda_3(-3x + x^3).$$

Comparando los coeficientes de igual grado esto conduce al sistema

$$\begin{aligned} 1 &= \lambda_1 \\ -2 &= -2\lambda_2 - 3\lambda_3 \\ 0 &= \lambda_3 \end{aligned}$$

cuya solución $(\lambda_1, \lambda_2, \lambda_3) = (1, 1, 0)$ da las coordenadas buscadas.

La matriz $M_{BB'}$ tiene como columnas a las coordenadas de cada uno de los vectores de B con respecto a la base B', por ello nuestro primer objetivo es expresar 1, $-2x + x^2$ y $-3x + x^3$ como combinaciones lineales de 1, $(x-1)^2$, $(x-1)^3$. Para el primer elemento de B se tiene

$$\left.\begin{aligned} 1 =& \lambda \cdot 1 + \mu(x-1)^2 + \nu(x-1)^3 \\ =& \lambda \cdot 1 + \mu(x^2 - 2x + 1) + \nu(x^3 - 3x^2 + 3x - 1) \end{aligned}\right\} \Rightarrow \; (\lambda, \mu, \nu) = (1, 0, 0),$$

para el segundo

$$\left.\begin{aligned} -2x + x^2 =& \lambda \cdot 1 + \mu(x-1)^2 + \nu(x-1)^3 \\ =& \lambda \cdot 1 + \mu(x^2 - 2x + 1) + \nu(x^3 - 3x^2 + 3x - 1) \end{aligned}\right\} \Rightarrow \; (\lambda, \mu, \nu) = (-1, 1, 0),$$

y finalmente

$$\left.\begin{aligned} -3x + x^3 =& \lambda \cdot 1 + \mu(x-1)^2 + \nu(x-1)^3 \\ =& \lambda \cdot 1 + \mu(x^2 - 2x + 1) + \nu(x^3 - 3x^2 + 3x - 1) \end{aligned}\right\} \Rightarrow \; (\lambda, \mu, \nu) = (-2, 3, 1).$$

Por tanto,

$$M_{BB'} = \begin{pmatrix} 1 & -1 & -2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Para calcular $M_{B'B}$ basta invertir esta matriz, obteniéndose

$$M_{B'B} = M_{BB'}^{-1} = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Si todos nuestros razonamientos son correctos, las columnas de $M_{B'B}$ deberían dar las coordenadas de los vectores de B' en la base B. Comprobemos, por ejemplo, que el tercer vector de B', $(x-1)^3$, tiene como coordenadas $(-1,-3,1)$ en la base B. Esto se reduce al siguiente cálculo

$$(x-1)^3 = -1 \cdot 1 - 3(-2x + x^2) + 1 \cdot (-3x + x^3).$$

5.3. Suma e intersección de subespacios. Fórmula de Grassmann

Dados dos subespacios, V y W, de un espacio vectorial, podemos considerar el subespacio $V \cap W$ que está contenido en V y W; sin embargo, $V \cup W$ en general no es un subespacio. Por ejemplo, tomando

$$V = \{(x,y) \,/\, x = y\}, \qquad W = \{(x,y) \,/\, x = -y\} \subset \mathbb{R}^2,$$

se tendría

$$V \cup W = \{(x,y) \,/\, x = y \text{ ó } x = -y\} = \{(x,y) \,/\, x^2 = y^2\}$$

y esto no es un subespacio ya que $(1,-1) \in V \cup W$, $(1,1) \in V \cup W$, pero $(1,-1)+(1,1) = (2,0) \notin V \cup W$.

Por esta razón se define un nuevo subespacio, llamado suma, que es el menor (en el sentido de la inclusión) que contiene a $V \cup W$.

Definición: *Si V y W son subespacios de E, se llama* <u>suma de V y W</u>, *y se escribe $V+W$, a*

$$V + W = \{\vec{x} \,/\, \vec{x} = \vec{v} + \vec{w},\ \vec{v} \in V,\ \vec{w} \in W\}.$$

Lo expuesto hasta ahora se resume siguiente lema (ejercicio)

Lema 3.1 : *Si V y W son subespacios de E, $V \cap W$ y $V+W$ también lo son.*

<u>Observación</u>: Obsérvese que dos subespacios siempre se intersecan (nunca son disjuntos), ya que el vector $\vec{0}$ está contenido en todo subespacio

$$V \cap W = \{\vec{x} \,/\, \vec{x} \in V,\ \vec{x} \in W\} \supset \{\vec{0}\}.$$

Veamos cómo calcular $V \cap W$ y $V + W$ en algunos ejemplos.

Ejemplo 1. Hallar $V \cap W$ y $V + W$ describiendo alguna de sus bases, donde

$$V = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + y + z = 0\} \qquad W = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + y - z = 0\}.$$

Por definición

$$\begin{aligned} V \cap W =& \{(x, y, z) \in \mathbb{R}^3 \,/\, x + y + z = 0,\ x + y - z = 0\} \\ =& \{(x, y, z) \in \mathbb{R}^3 \,/\, x = -y,\ z = 0\}. \end{aligned}$$

Por tanto

$$\vec{v} \in V \cap W \ \Leftrightarrow\ \vec{v} = (-y, y, 0) = y(-1, 1, 0),$$

con lo cual, una base de $V \cap W$ es

$$B_{V\cap W} = \{(-1, 1, 0)\}.$$

Antes de calcular $V + W$, calculemos bases de V y W. No es difícil comprobar que

$$B_V = \{(-1, 1, 0), (-1, 0, 1)\} \qquad B_W = \{(-1, 1, 0), (1, 0, 1)\}$$

lo son. En particular, todo vector $\vec{v} \in V$ se escribe como

$$\vec{v} = \lambda(-1, 1, 0) + \mu(-1, 0, 1)$$

y todo vector $\vec{w} \in W$ se escribe como

$$\vec{w} = \lambda'(-1, 1, 0) + \mu'(1, 0, 1).$$

Por tanto, los elementos $\vec{v} + \vec{w}$ (los cuales constituyen $V + W$) son aquellos que admiten una expresión de la forma

$$\vec{v} + \vec{w} = \lambda(-1, 1, 0) + \mu(-1, 0, 1) + \lambda'(-1, 1, 0) + \mu'(1, 0, 1).$$

Con esto hemos probado

$$V + W = \langle(-1, 1, 0), (-1, 0, 1), (1, 0, 1)\rangle.$$

De hecho

$$B_{V+W} = \{(-1, 1, 0), (-1, 0, 1), (1, 0, 1)\}$$

es una base de $V + W$. Para comprobarlo sólo es necesario verificar que son linealmente independientes (ya hemos visto que generan), lo cual es cierto porque

$$\lambda(-1, 1, 0) + \mu(-1, 0, 1) + \nu(1, 0, 1) = (0, 0, 0)$$

equivale a

$$\left.\begin{aligned} -\lambda - \mu - \nu =& 0 \\ \lambda \qquad =& 0 \\ \mu + \nu =& 0 \end{aligned}\right\} \Rightarrow\ \lambda = \mu = \nu = 0.$$

Ejemplo 2. Dados

$$V = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + 3y + 2z = 0\} \qquad W = \{(x, y, z) \in \mathbb{R}^3 \,/\, 7x + 2z = 0\},$$

hallar $V \cap W$ y $V + W$.

Comencemos con $V \cap W$,

$$V \cap W = \{(x, y, z) \in \mathbb{R}^3 \,/\, x + 3y + 2z = 0,\ 7x + 2z = 0\}.$$

Despejando, podemos escribir estas dos condiciones como

$$V \cap W = \{(x, y, z) \in \mathbb{R}^3 \,/\, x = -2z/7,\ y = -4z/7\}.$$

Por tanto

$$\begin{aligned} V \cap W =& \{(-2z/7, -4z/7, z) \in \mathbb{R}^3\} \\ =& \langle(-2/7, -4/7, 1)\rangle = \langle(-2, -4, 7)\rangle. \end{aligned}$$

Obsérvese que para la última igualdad hemos usado que todo vector que sea combinación lineal de $(-2/7, -4/7, 1)$ (en este caso, proporcional a dicho vector), también lo es de $(-2, -4, 7)$. Una base de $V \cap W$ sería

$$B_{V \cap W} = \{(-2, -4, 7)\}.$$

Para calcular $V + W$, hallemos primero bases de V y W.

$$\begin{aligned} \vec{v} = (x, y, z) \in V \ \Leftrightarrow \vec{v} =& (-3y - 2z, y, z) \\ =& y(-3, 1, 0) + z(-2, 0, 1), \end{aligned}$$

por tanto estos vectores generan V. De la misma forma

$$\begin{aligned} \vec{w} = (x, y, z) \in w \ \Leftrightarrow \vec{W} =& (-2z/7, y, z) \\ =& y(0, 1, 0) + z(-2/7, 0, 1), \end{aligned}$$

lo que de nuevo produce un sistema de generadores. Es fácil comprobar que estos pares de vectores son linealmente independientes y por tanto tenemos las siguientes bases de V y W

$$B_V = \{(-3, 1, 0), (-2, 0, 1)\} \qquad B_W = \{(0, 1, 0), (-2/7, 0, 1)\}.$$

Cualquier vector de $V + W$ debe ser combinación lineal de éstos, es decir

$$V + W = \langle(-3, 1, 0), (-2, 0, 1), (0, 1, 0), (-2/7, 0, 1)\rangle.$$

A pesar de que estos vectores generan $V + W$, no pueden ser una base, porque $V + W \subset \mathbb{R}^3$ y en $\mathbb{R}^3$ hay a lo más $\dim \mathbb{R}^3 = 3$ vectores linealmente independientes. Variaciones de este mismo argumento, sirven para probar que si entre los generadores de $V + W$ hay tres linealmente independientes, debe cumplirse $V + W = \mathbb{R}^3$. Éste es el caso, ya que

$$\lambda_1(-3, 1, 0) + \lambda_2(-2, 0, 1) + \lambda_3(0, 1, 0) = (0, 0, 0)$$

tiene como única solución $\lambda_1 = \lambda_2 = \lambda_3 = 0$.

A continuación veremos cómo calcular $\dim(V + W)$ a partir de las dimensiones de V, W y $V \cap W$, sin necesidad de hallar una base. Antes de nada, recuérdese que en teoría de conjuntos los cardinales de A, B, $A \cup B$ y $A \cap B$ estaban relacionados por la fórmula

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Ya hemos mencionado que en la teoría de espacios vectoriales la suma juega un papel relacionado con la unión y la dimensión nos indica el "tamaño" de un espacio vectorial. Teniendo en mente estas analogías no debiera sorprender el siguiente resultado

Proposición 3.2 (Fórmula de Grassmann)**:** *Si V y W son subespacios de un espacio vectorial de dimensión finita, entonces*

$$dim\,(V + W) = dim\,V + dim\,W - dim\,(V \cap W).$$

Ejemplo 1. En los dos ejemplos anteriores se tiene

$$\begin{array}{ccccccc} \dim(V+W) & = & \dim V & + & \dim W & - & \dim(V \cap W) \\ 3 & = & 2 & + & 2 & - & 1 \end{array}$$

Obsérvese que como $V + W \subset \mathbb{R}^3$, este sencillo cálculo de la dimensión de $V + W$ permite concluir $V + W = \mathbb{R}^3$.

Ejemplo 2. Sea $V = \mathcal{S}_2(\mathbb{R})$ (matrices simétricas 2×2) y W el subespacio de matrices (a_{ij}) con $a_{11} = a_{21} = a_{22} = 0$.

Ya habíamos visto que $\dim \mathcal{S}_2(\mathbb{R}) = 3$. Por otra parte, como

$$W = \left\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\rangle,$$

se tiene $\dim W = 1$. Es evidente que $V \cap W$ sólo contiene a la matriz nula, por tanto

$$\dim(V + W) = 3 + 1 - 0 = 4.$$

Pero como $V + W \subset \mathcal{M}_{2\times 2}(\mathbb{R})$ y $\dim \mathcal{M}_{2\times 2}(\mathbb{R}) = 4$, esto es suficiente para concluir $V + W = \mathcal{M}_{2\times 2}(\mathbb{R})$.

Ejemplo 3. Sea V el subespacio de $\mathcal{M}_{2\times 2}(\mathbb{R})$ formado por las matrices antisimétricas, es decir, $(a_{ij}) \in V \Leftrightarrow a_{ij} = -a_{ji}$, y sea W como en el ejemplo anterior

$$V = \Big\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Big\rangle, \qquad W = \Big\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \Big\rangle.$$

Obsérvese también que el subespacio

$$U = \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \,/\, a = d = 0 \Big\}$$

cumple $V, W \subset U$; así pues, $V + W \subset U$ y $\dim(V + W) = \dim U = 2$ implica $U = V + W$.

Hoja 13

1) Comprobar en cada caso si el conjunto V es un espacio vectorial sobre el cuerpo K que se indica (*Sugerencia*: En caso afirmativo basta comprobar que son subespacios de algún espacio vectorial conocido).

i) $V = \{(x,y) \in \mathbb{R}^2 \,/\, x - y = 0\}$, $K = \mathbb{R}$.

ii) $V = \{(x,y) \in \mathbb{R}^2 \,/\, x^2 - y^2 = 0\}$, $K = \mathbb{R}$.

iii) $V = \{(x,y,z) \in \mathbb{C}^3 \,/\, x + y + z = 0\}$, $K = \mathbb{R}$.

iv) $V = \{(x,y,z) \in \mathbb{C}^3 \,/\, x + y + z = 0\}$, $K = \mathbb{C}$.

v) $V = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \,/\, a + b + c - 2d = 0 \right\}$, $K = \mathbb{R}$.

vi) $V = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \,/\, a^2 + b^2 + c^2 + 2ab + 2ac + 2bc = 0 \right\}$, $K = \mathbb{R}$.

vii) $V = \{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) \,/\, \det A = 0\}$, $K = \mathbb{R}$.

viii) $V = \{A \in \mathcal{M}_{3\times 3}(\mathbb{R}) \,/\, a_{11} + a_{22} + a_{33} = 0\}$, $K = \mathbb{R}$.

ix) $V = \{a + b\sqrt{2} \,/\, a, b \in \mathbb{Q}\}$, $K = \mathbb{Q}$.

x) $V = \{A \in \mathcal{M}_{m\times n}(\mathbb{R}) \,/\, AB = \mathbf{0}$ donde $B \in \mathcal{M}_{n\times l}$ es una matriz dada$\}$, $K = \mathbb{R}$.

xi) $V = \{$funciones reales continuas con un máximo absoluto en $x = 1\}$, $K = \mathbb{R}$.

xii) $V = \{f : [0,1] \longrightarrow \mathbb{C} \,/\, f(0) = 3f(1)\}$, $K = \mathbb{C}$.

2) Sea $\vec{0}$ el elemento neutro de un espacio vectorial, E, y sea $-\vec{u}$ el elemento inverso de $\vec{u} \in E$. Demostrar (usando las propiedades de espacio vectorial) que $0 \cdot \vec{u} = \vec{0}$ y que $(-1) \cdot \vec{u} = -\vec{u}$.

3) Estudiar para qué valores de a, $V = \{(x,y) \in \mathbb{R}^2 \,/\, x^2 + axy + y^2 = 0\}$ es un subespacio vectorial de $\mathbb{R}^2$. *Sugerencia*: Escribir $x^2 + axy + y^2$ como $(x - \alpha y)(x - \beta y)$.

4) Demostrar que las funciones (reales con dos derivadas continuas) que cumplen $y'' + y' + y = 0$ forman un espacio vectorial, V. Sabiendo que $y_1(x) = e^{-x/2}\cos(x\sqrt{3}/2)$ y $y_2(x) = e^{-x/2}\,\mathrm{sen}(x\sqrt{3}/2)$ pertenecen a V, hallar "muchos" elementos de V, y entre ellos uno que resuelva $y'' + y' + y = 0$, $y(0) = 1$, $y'(0) = 1$.

****5)** Sean $V_1 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,/\, a, b, c \in \mathbb{Q}\}$ y $V_2 = \left\{ \dfrac{a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}}{a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}} \,/\, a_i, b_i, c_i \in \mathbb{Q},\ a_2^2 + b_2^2 + c_2^2 \neq 0 \right\}$. Ambos son espacios vectoriales sobre $\mathbb{Q}$, demostrar que $V_1 = V_2$.

1) Decidir si los siguientes conjuntos son bases del espacio V que se indica

i) $B=\{(4,-1,1),\,(3,3,2)\},\;\; V=\{(x,y,z)\in\mathbb{R}^3\,\big/\,x+y-3z=0\}$.

ii) $B=\{(4,-1,1),\,(3,3,-2)\},\;\; V=\{(x,y,z)\in\mathbb{R}^3\,\big/\,x+y-3z=0\}$.

iii) $B=\{1,1+x,1+x+x^2,\dots,1+x+\ldots+x^n\},\;\; V=\mathbb{P}_n[x]$.

iv) $B=\Big\{\begin{pmatrix}2&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix},\begin{pmatrix}3&2\\2&2\end{pmatrix}\Big\}\;\; V=\mathcal{M}_{2\times 2}(\mathbb{R})$.

v) $B=\{\cos 2x,\cos 4x,\cos 8x\}\;\; V=\langle B\rangle$.

2) Hallar una base de los siguientes subespacios

i) $V=\{(x,y,z,t)\in\mathbb{R}^4\,\big/\,x+y=0,\; z+t=0\}$.

ii) $V=\{(x,y,z,t)\in\mathbb{R}^4\,\big/\,x+y+z=0,\; z+t=0,\; 2x-t=0\}$.

iii) $V=\{P\in\mathbb{P}_4[x]\,\big/\,x^2P''-2P=0\}$.

En los tres problemas siguientes, dados $a_i\in\mathbb{R}$, sea V el conjunto de funciones reales, y, con infinitas derivadas tales que

$$y^{n)}+a_{n-1}y^{n-1)}+a_{n-2}y^{n-2)}+\ldots+a_1y'+a_0y=0 \qquad y^{k)}=\text{ derivada de orden } k$$

3) Demostrar que $y\in V\Rightarrow y^{k)}\in V$, y que el sistema $C=\{y^{k)},y^{k+1)},\ldots y^{k+n)}\}$ es linealmente dependiente.

$*_*$**4)** Si $y\in V$ y $\exists x_0\in\mathbb{R}$ tal que $y(x_0)=y'(x_0)=\ldots y^{n-1)}(x_0)=0$, demostrar que $y=0$. *Indicación*: demostrar primero $y(x)=\int_{x_0}^{x}y^{n+k+1)}(t)(x-t)^{n+k}/(n+k)!\,dt$.

5) Suponiendo conocida la afirmación del problema anterior, demostrar $\dim V\le n$. (*Sugerencia*: Si $\dim V=m>n$, existirían λ_i no nulos tales que $F=\lambda_1y_1+\lambda_2y_2+\ldots+\lambda_my_m$ cumple $F(x_0)=F^{k)}(x_0)=0$, $k<n$). Nota: Se puede demostrar $\dim V=n$, pero no es fácil.

6) Sea $B=\{\operatorname{sen}x,\operatorname{sen}2x,\operatorname{sen}3x,\ldots\}$. Sabiendo que $\int_{-\pi}^{\pi}\operatorname{sen}nx\,\operatorname{sen}mx dx=0$, demostrar que cada subconjunto finito de B es linealmente independiente.

7) Si $f\in\langle B\rangle$ con $f=\lambda_1\operatorname{sen}x+\lambda_2\operatorname{sen}2x+\ldots+\lambda_n\operatorname{sen}nx$, demostrar que λ_k puede hallarse con la fórmula $\lambda_k=\frac{1}{\pi}\int_{-\pi}^{\pi}f(x)\operatorname{sen}kx\,dx$.

Curiosidades: B es "casi" una base de $V=\{f:[-\pi,\pi]\longrightarrow\mathbb{R}\,\big/\,\text{f impar y }\exists f''\}$, en el sentido de que toda función de V se aproxima por una combinación lineal suficientemente larga de B. Por ejemplo, si $f(x)=\frac{\pi}{2}2^{\cos x}\operatorname{sen}x$, hallando los λ_k con tu programa de integración favorito, se obtiene

$$\frac{\pi}{2}2^{\cos x}\operatorname{sen}x\approx 1.667\operatorname{sen}x+0.567\operatorname{sen}2x+0.097\operatorname{sen}3x+\ldots$$

Integrando entre 0 y $t=\operatorname{arc}\cos y$, se tiene (nótese $\cos t=y$, $\cos 2t=2y^2-1$, $\cos 3t=4y^3-3y$).

$$2^y\approx 0.990+1.061y+0.180(2y^2-1)+.020(4y^3-3y)+\ldots$$

Esta aproximación es, en general, mejor que Taylor y la usa (con más términos y pequeñas modificaciones) el ZX-Spectrum para calcular 2^x con $|x|<1/2$, lo que combinado con $2^{n+x}=2^n2^x$ y $e^x=2^{x\log_2 e}$ le sirve para hallar `EXP`$=e^x$ con $x\in\mathbb{R}$.

1) Hallar una base de $V=\{(x,y,z,t)\in\mathbb{R}^4\,/\,x+y-z=0,\ x+3y-2z+2t=0\}$ y hallar las coordenadas de $\vec{v}=(3,1,4,1)$ en dicha base.

2) Si $\vec{v}$ tiene coordenadas $(1,2,3)$ en la base B, hallar sus coordenadas en B'.
i) $B=\{(1,0,0),\ (0,1,0),\ (0,0,1)\}\subset\mathbb{R}^3,\ B'=\{(2,5,1),\ (-1,-2,-1),\ (0,-1,3)\}$.
ii) $B=\{(1,0,0),\ (0,1,0),\ (0,0,1)\}\subset\mathbb{R}^3,\ B'=\{(2,1,0),\ (0,1,1),\ (1,2,3)\}$.
iii) $B=\{1+x^2,\ x,\ x^2\}\subset\mathbb{P}_3,\ B'=\{1+x,\ x,\ 1+x^2\}$.
iv) $B=\{\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\}\subset S_2(\mathbb{R}),\ B'=\{\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix}\}$.

3) Si desde el centro del tiovivo las coordenadas de la caseta de helados son $(2,4)$, ¿cuáles serán cuando el tiovivo haya girado 60^o en sentido positivo?

4) Comprobar la fórmula $\dim(V+W)=\dim V+\dim W-\dim(V\cap W)$ para
i) $V=\{(x,y,z,t)\in\mathbb{R}^4\,/\,x+y+z=0\}$, $W=\{(x,y,z,t)\in\mathbb{R}^4\,/\,y+z+t=0\}$.
ii) $V=\{(x,y,z)\in\mathbb{R}^3\,/\,x-2y+z=0\}$, $W=\{(x,y,z)\in\mathbb{R}^3\,/\,2x+y-4z=0\}$.
iii) $V=$matrices simétricas 2×2, $W=$matrices antisimétricas 2×2 ($a_{ij}=-a_{ji}$).
iv) $V=\langle(2,1,0,1),(3,2,1,1)\rangle$, $W=\langle(0,1,2,1),(1,1,1,1),(1,2,3,2)\rangle$

5) La trayectoria unidimensional de una partícula se puede representar como un vector variable en $\mathbb{R}^2$, $\vec{w}=$ (espacio,tiempo). Sean (x,t) las coordenadas de $\vec{w}$ en B y (x',t') en B'. Leyes experimentales indujeron a Einstein a pensar que en todas las bases admisibles en Física (inerciales) la velocidad de la luz debe ser constante, esto es, $x^2-c^2t^2=0\Leftrightarrow {x'}^2-c^2{t'}^2=0$ con $c^2=9\cdot10^{16}$. Lo cual, tras algunas hipótesis físicas adicionales, implica $x^2-c^2t^2={x'}^2-c^2{t'}^2$ incluso si ambos valores no son cero.
i) Comprobar que los siguientes cambios de base verifican $x^2-c^2t^2={x'}^2-c^2{t'}^2$

$$\begin{pmatrix}x'\\t'\end{pmatrix}=M\begin{pmatrix}x\\t\end{pmatrix},\qquad M=\begin{pmatrix}\sqrt{1+\lambda^2c^{-2}}&\lambda\\\lambda c^{-2}&\sqrt{1+\lambda^2c^{-2}}\end{pmatrix}\qquad\text{con }\lambda\in\mathbb{R}$$

(de hecho son los únicos que además cumplen $x-ct=0,\ t\ge0,\Rightarrow\ x'-ct'=0,\ t'\ge0$).
ii) Se dice que B' tiene velocidad relativa v con respecto de B si $x=vt\Rightarrow x'=0$. Demostrar que en ese caso se tiene

$$\lambda=-v(1-v^2c^{-2})^{-1/2}\qquad M=(1-v^2c^{-2})^{-1/2}\begin{pmatrix}1&-v\\-vc^{-2}&1\end{pmatrix}$$

iii) Si una masa, m, está en reposo en B', esto es, $x'=0$, $t'=\tau$, hallar sus coordenadas en B. En Física a $p=m\,dx/d\tau$ se le llama momento lineal y a $E=\int v\,dp$ energía, comprobar que $p=mv(1-v^2c^{-2})^{-1/2}$, $E=mc^2(1-v^2c^{-2})^{-1/2}$ y deducir que si $v=0$ (masa en reposo en B y B'), $E=mc^2$.

6) Si $\alpha\in\mathbb{C}$, sea $\mathbb{P}_n[\alpha]=\{a_0+a_1\alpha+a_2\alpha^2+\ldots+a_n\alpha^n\,/\,a_i\in\mathbb{Q}\}$. Demostrar que $\dim\mathbb{P}_n[\alpha]=n+1\Leftrightarrow\{P\in\mathbb{P}_n[x]\cap\mathbb{Q}[x]\,/\,P(\alpha)=0\}=\{0\}$.

****7)** Demostrar que $\dim\mathbb{P}_n[e^{1/k}]\ge2$ para todo $k,n\in\mathbb{Z}^+$, $e=2'7182\ldots$

***8)** Dado V espacio vectorial, se define el conjunto de endomorfismos de V como $\mathrm{End}=\{f:V\longrightarrow V\,/\,f(\vec{x}+\vec{y})=f(\vec{x})+f(\vec{y}),\ f(\lambda\vec{x})=\lambda f(\vec{x})\}$. Demostrar que si $V=\mathbb{R}^{2n+1}$, $\{\vec{v}\,/\,\vec{v},\ f(\vec{v})$ son linealmente dependientes$\}\neq\{\vec{0}\}$ para cualquier $f\in$ END.

Miscelánea.

A pesar de que hoy en día es difícilmente imaginable la formulación de las leyes físicas más sencillas sin la notación vectorial, la aparición de los vectores es Física es relativamente tardía. Así, por ejemplo, fue J.C. Maxwell (1831-1879) uno de los primeros físicos en reconocer sus ventajas en su famoso "Treatise on Electricity and Magnetism" publicado en 1873.

El concepto de vector fue contemporáneo y compitió con el de cuaternión. Al igual que los números complejos son de la forma $a + bi$ donde i es un "número" que cumple $i^2 = -1$, los cuaterniones son de la forma $a + bi + cj + dk$ donde $i^2 = j^2 = k^2 = -1$ y satisfacen las reglas de multiplicación

$$i \cdot j = k, \quad j \cdot k = i, \quad k \cdot i = j, \quad j \cdot i = -k, \quad k \cdot j = -i, \quad i \cdot k = -j.$$

Los cuaterniones tienen gran importancia histórica en Matemáticas porque constituyen de los primeros ejemplos de estructura no conmutativa y dieron lugar a una visión abstracta del álgebra. Su creador, el físico y matemático W.R. Hamilton (1805-1865), estaba convencido de la relevancia que tendrían los cuaterniones en Física y dedicó una parte de su obra a formular diversas leyes con este lenguaje. Parte de su notación se conserva hoy en día, por ejemplo, fue Hamilton quien definió el operador nabla

$$\nabla = i\frac{\partial}{\partial x} + j\frac{\partial}{\partial y} + k\frac{\partial}{\partial z},$$

y también quien introdujo la palabra "vector".

Desde el punto de vista actual es más útil considerar sólo el vector formado por las tres últimas coordenadas del cuaternión. Ésta fue la línea seguida por H.G. Grassmann (1809-1877) quien creó, independientemente de Hamilton, parte del álgebra vectorial en tres dimensiones, definiendo el producto escalar, el producto vectorial, el producto mixto y otras operaciones. Pero su trabajo, publicado en 1844, era difícilmente comprensible y no fue demasiado conocido. Se considera que el triunfo de los vectores no ocurrió hasta la aparición en 1881 del libro de J.W. Gibbs (1839-1903) "Elements of Vector Analysis".

Los espacios vectoriales de dimensión infinita también desempeñan un lugar importante en la Física. Uno de los más conocidos es el subespacio generado por

$$B = \{1, \cos x, \cos 2x, \cos 3x, \dots, \operatorname{sen} x, \operatorname{sen} 2x, \operatorname{sen} 3x, \dots\}$$

dentro del espacio vectorial de funciones periódicas de periodo 2π. Los vectores (funciones) de B son linealmente independientes, ya que multiplicando por $\cos nx$ en

$$\sum_{n=0}^{N} \lambda_n \cos nx + \sum_{n=1}^{N} \mu_n \operatorname{sen} nx = 0,$$

e integrando el resultado entre 0 y 2π, se tiene $\lambda_n = 0$, y procediendo de la misma forma con $\operatorname{sen} nx$ se obtiene $\mu_n = 0$. Así pues, B es una base de $\langle B \rangle$. Esto no dejaría de ser más que una curiosidad de no ser porque siempre hay elementos de $\langle B \rangle$ arbitrariamente cerca de cualquier función periódica (de periodo 2π) con al menos dos derivadas. Es decir, para una función, f, con estas características

$$f(x) = \sum_{n=0}^{\infty} \lambda_n \cos nx + \sum_{n=1}^{\infty} \mu_n \operatorname{sen} nx$$

donde, procediendo como antes y usando que $\int_0^{2\pi} \cos^2 nx dx = \int_0^{2\pi} \operatorname{sen}^2 nx dx = \pi$ excepto si $n = 0$, los coeficientes vienen dados por

$$\lambda_n = \frac{1}{\pi}\int_0^{2\pi} f(x)\cos nx dx, \ (n \neq 0), \quad \mu_n = \frac{1}{\pi}\int_0^{2\pi} f(x)\sin nx dx, \quad \lambda_0 = \frac{1}{2\pi}\int_0^{2\pi} f(x) dx.$$

El anterior desarrollo en serie y los coeficientes λ_n, μ_n, se conocen con el nombre de *serie de Fourier* y *coeficientes de Fourier* en honor a J.B. Fourier (1768-1830) quien los usó en un famoso e importante trabajo acerca de la transmisión del calor. Sin embargo, el nombre no hace del todo justicia, ya que series similares y la fórmula para los coeficientes también habían sido introducidas con anterioridad en los trabajos (que seguramente desconocía Fourier) de L. Euler (1707-1783), D. Bernoulli (1700-1782) y otros. Por otra parte, ni Fourier ni sus predecesores fueron capaces de demostrar que realmente la serie de Fourier converge a la función de partida.

Pedro levanta la liebre e la mueve del covil,
non la sigue nin la toma, faz como cazador vil;
otro Pedro que la sigue e la corre más sotil
tómala: esto contesçe a caçadores mill.
LBA, 486

Para ver una aplicación de estas ideas en la línea que siguió Fourier, consideremos un anillo circular, unidimensional y aislado. Vamos a calcular cómo evolucionará su temperatura, $u(x,t)$, en función del ángulo, x, y del tiempo, t, sabiendo que inicialmente la temperatura en el punto de ángulo x es $f(x)$, esto es, que $u(x,0) = f(x)$.

Coonsiderando un pequeño intervalo $I = [x_1, x_2]$, el calor acumulado en I se pierde o gana a través de x_1 y x_2. Concretamente, si hay un cambio brusco de temperatura al atravesar x_1 y x_2 (esto es, si $\partial u/\partial x$ es grande en ellos) entonces se perderá o incrementará el calor acumulado en I muy rápido. Lo cual sugiere

$$\frac{d}{dt}\int_{x_1}^{x_2} u(x,t)dx = \frac{\partial u}{\partial x}(x_2,t) - \frac{\partial u}{\partial x}(x_1,t),$$

y derivando con respecto a x_2 se tiene

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}.$$

Ésta es la llamada *ecuación del calor*. Es fácil comprobar que $u_n(x,t) = e^{-n^2 t}\cos nx$ y $\tilde{u}_n(x,t) = e^{-n^2 t}\operatorname{sen} nx$ son soluciones, aunque en general no satisfacen nuestra hipótesis $u(x,0) = f(x)$. Como las soluciones forman un espacio vectorial, formalmente (olvidando cuestiones de convergencia) la "combinación lineal infinita"

$$u(x,t) = \sum_{n=0}^{\infty} \lambda_n e^{-n^2 t}\cos nx + \sum_{n=1}^{\infty} \mu_n e^{-n^2 t}\operatorname{sen} nx$$

también es solución. Escogiendo λ_n y μ_n como los coeficientes de Fourier de f, se tiene una solución a nuestro problema, ya que $u(x,0) = f(x)$. En la práctica se toman sólo unos cuantos términos de la serie para aproximar a $u(x,t)$. Obsérvese que $u(x,t) \to \lambda_0$ cuando $t \to \infty$, es decir, que como es lógico la temperatura tiende a la larga a igualarse en todos los puntos.

El llamado análisis de Fourier es también fundamental para entender la mecánica cuántica ya que, en ella, el concepto clásico de partícula perde su significado y se considera que una partícula viene dada, intuitivamente, por una superposición de ondas definida por la llamada función de onda, $\psi(x)$. Al igual que no es posible decir exactamente dónde está una onda sino sólo dónde es más o menos intensa (piénsese en una ola o en la cuerda de un violín), en el caso de las partículas la "intensidad" $|\psi(x)|^2$ indica una especie de probabilidad de detectar la partícula en x. Las frecuencias "predominantes" de las ondas que componen ψ están relacionadas con el momento de la partícula. Si ψ está muy localizada entonces debe estar compuesta por frecuencias muy altas. Ésta es la base del famoso *principio de incertidumbre* enunciado por W.K. Heisenberg (1901-1976).

Una exposición rigurosa de la mecánica cuántica es matemáticamente muy complicada (un libro bueno y divertido para aprender algo de electrodinámica cuántica sin nada de Matemáticas es "QED" de R. Feynman). Por ejemplo, las funciones de onda son elementos de cierto espacio vectorial de dimensión infinita y las magnitudes físicas "observables" son operadores que actúan sobre ellas. Sin duda éste no es el lugar adecuado para aprender de este tema.

En esto yerran mucho, que lo non pueden fazer;
de lo que fazer non pueden, non se deven entremeter:
si el çiego al çiego adiestra e quier traer,
en la foya entranbos dan e van a caer.
LBA, 1145

Estas notas fueron realizadas para el curso 1995/1996 de 1º de Ingeniería Informática de la U.A.M. y corregidas y ampliadas en el curso 1996/1997. Desde entonces han circulado libremente año tras año entre los estudiantes, dejándose copias en reprografía.

> Pues es de buen amor, enprestadlo de grado:
> no·l neguedes su nonbre ni·l dedes refertado,
> no·l dedes por dineros vendido nin alquilado,
> ca non ha grado nin graçias buen amor el comprado.
> *LBA, 1630*

Vista la difusión que han tenido, también podría decir yo que *Fizvos pequeño libro de testo,* [...] (*LBA, 1631*), y no se me ocurre nada mejor que terminar con las últimas estrofas restantes del Libro de Buen Amor. Aunque supongo que está claro, todas las citas en las misceláneas al final de cada capítulo están tomadas de él, concretamente de la magnífica edición de A. Blecua, Ed. Cátedra 1992.

> [...] por ende fago punto e çierro mi almario:
> séavos chica fabla, solaz e letüario.
> *LBA, 1632*

> Señores, hevos servido con poca sabidoría,
> por vos dar solaz a todos, fáblevos en juglería;
> yo un gualardón vos pido: que por Dios, en romería,
> digades un paternóster por mí e avemaría.
> *LBA, 1633*

Ahora con el generoso permiso que otorga Juan Ruiz en la *1629*, estropeo la *1634*

> Era de mill e novezientos e noventa e seis años,
> fue conpuesto el romançe por toller el estudio de daños,
> por fazer cosa, por grand orgullía, por estruir engaños
> e por mostrar a los moços fablas e saberes estraños.

Fernando Chamizo Lorente. Departamento de Matemáticas. Madrid a 22 de Enero del año 2002. U.A.M.