Contents

EL ASNO Y SU AMO
(Tomás de Iriarte)

"Siempre acostumbra a hacer el vulgo necio
de lo bueno y lo malo igual aprecio.
Yo le doy lo peor, que es lo que alaba."
De este modo sus yerros disculpaba
un escritor de farsas indecentes;
y un taimado poeta que lo oía,
le respondió en los términos siguientes:
"Al humilde Jumento
su dueño daba paja, y le decía:
Toma, pues que con esto estás contento.
Díjolo tantas veces, que ya un día
se enfadó el asno y replicó: Yo tomo
lo que me quieres dar; pero, hombre injusto,
¿piensas que sólo de la paja gusto?
Dame grano y verás si me lo como."

Sepa quien para el público trabaja
que tal vez a la plebe culpa en vano;
pues si en dándole paja, come paja,
siempre que le dan grano, come grano.

1 Nociones de lógica proposicional

Entenderemos por *proposición* toda expresión lingüística respecto de la cual puede decirse si es verdadera o falsa.

Por ejemplo, las oraciones:

3 *es un número primo*
7 *es un número par*

son proposiciones.

La verdad y la falsedad son los *valores de verdad* de una proposición. Si una proposición es verdadera, decimos que su valor de verdad es *verdad* (V), y si es falsa, decimos que su valor de verdad es *falsedad* (F).

Una proposición *simple* tiene un sujeto y un predicado, en el sentido gramatical. Por ejemplo,

El número 14 es divisible por 7
Boole fue un gran matemático del siglo pasado
El arroyo que cruza la ciudad desemboca en la ría

donde se ha subrayado el sujeto.

Vamos a representar a las proposiciones simples por letras mayúsculas A, B, C, ...

1.1 Conectivos

A través de expresiones como "o", "y", "no", "si ..., entonces", "si, y sólo si", llamadas *conectivos*, se generan proposiciones *compuestas* partiendo de proposiciones simples. Por ejemplo,

El número 14 *no es divisible por* 7.
Si llegamos temprano, saldremos a caminar.

Establecer el sentido y uso de estos términos es la tarea de una parte elemental de la lógica, llamada *lógica proposicional*.

Los símbolos que usaremos para denotar estos conectivos se dan en la siguiente tabla:

no A	$\sim A$
A y B	$A \wedge B$
A o B	$A \vee B$
si A entonces B	$A \Rightarrow B$
A si, y sólo si B	$A \Leftrightarrow B$

Vamos a estudiar *formas proposicionales*, más que proposiciones particulares. Para ello, usaremos las letras p, q, r, ... como *variables proposicionales* que representan proposiciones arbitrarias no especificadas, es decir las letras p, q, r, ... pueden ser sustituidas por proposiciones simples particulares cualesquiera. (Es importante tener en claro los diferentes usos de las letras p, q, r, ... y las letras A, B, C, ... Estas últimas son sólo nombres para proposiciones simples particulares).

Negación

Anteponiendo la palabra "no" se forma la *negación* de cualquier proposición (en el lenguaje ordinario se acostumbra colocarla con el verbo). Así, por ejemplo, la negación de la proposición:

2 *es un número primo*

es la proposición

2 *no es un número primo.*

Si la proposición A es verdadera su negación $\sim A$ es falsa y si la proposición A es falsa, su negación $\sim A$ es verdadera. Podemos describir esta situación por medio de una *tabla de verdad*.

p	$\sim p$
V	F
F	V

Conjunción

La unión de dos proposiciones por la palabra "y" se llama *conjunción* de proposiciones. Por ejemplo, la proposición

"3 *es un número impar y* 4 *es un número negativo*"

es la conjunción de las proposiciones

"3 *es un número impar*"

y

"4 *es un número negativo*".

Una conjunción de proposiciones es verdadera cuando ambas proposiciones lo son; pero si al menos una de las componentes es falsa, entonces toda la conjunción es falsa. Se tiene la siguiente tabla de verdad:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Disyunción

Con la unión de proposiciones por la palabra "o" se obtiene la *disyunción* de proposiciones. En el lenguaje corriente, la palabra "o" tiene, al menos, dos significados distintos. En el sentido **no excluyente** se expresa que al menos una de las dos proposiciones debe ser verdadera, aunque sin excluir la posibilidad de que ambas sean verdaderas. En el sentido **excluyente**, una disyunción afirma que una de las proposiciones es verdadera y la otra debe ser falsa. Por ejemplo, en el anuncio: "*Podrán ingresar al club los jóvenes que estudien en la UNS o que cursen el último año de la escuela secundaria*" la palabra "o" se usa en sentido no excluyente. En cambio, en la proposición: "*Pasaremos el verano en las sierras o en el mar*", la palabra "o" está usada en sentido excluyente. En Matemática, la palabra "o" se usa siempre en el sentido no excluyente.

La disyunción de dos proposiciones será verdadera cuando al menos una de ellas sea verdadera. Caso contrario, esto es, si ambas son falsas, la disyunción es falsa. La tabla de verdad de la disyunción es la siguiente:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Implicación

Si se combinan dos proposiciones por medio de las palabras "*si ..., entonces*" se obtiene una proposición compuesta llamada *implicación* o *condicional*. La proposición que sigue a la palabra "si" se llama *antecedente* y la introducida por la palabra "entonces" se llama *consecuente*.

Por ejemplo, en

Si x *es un número divisible por* 9, *entonces* x *es un número divisible por* 3,

el antecedente es

x *es un número divisible por* 9,

y el consecuente es

x *es un número divisible por* 3.

Una implicación es verdadera en los siguientes casos:

1. El antecedente y el consecuente son ambos verdaderos.
2. El antecedente es falso y el consecuente es verdadero.
3. El antecedente y el consecuente son ambos falsos.

Sólamente si el antecedente es verdadero y el consecuente es falso, la implicación es falsa.

La implicación tiene la siguiente tabla de verdad:

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Conviene aclarar que no es requisito que el antecedente y el consecuente estén relacionados entre sí en cuanto al contenido. Cualquier par de proposiciones pueden constituir una implicación. Así por ejemplo, la proposición "*Si* 5 *es un número primo, entonces París es la capital de Francia*", es una implicación lícita. Puede parecer raro, pero debe tenerse en cuenta que el principal interés es la deducción de métodos de demostración en Matemática, y es teóricamente útil que sea posible construir estas implicaciones.

Equivalencia

Otra expresión que aparece frecuentemente en Matemática es la frase "*si, y sólo si* ". Al unir dos proposiciones cualesquiera por medio de esta frase se obtiene una proposición compuesta que se llama *equivalencia* o *bicondicional*.

Por ejemplo,

x es un número par si y sólo si x^2 es un número par.

Una equivalencia es verdadera si sus miembros izquierdo y derecho son o bien ambos verdaderos o bien ambos falsos. En caso contrario la equivalencia es falsa. Se tiene entonces:

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Es claro que se pueden construir proposiciones compuestas de cualquier longitud a partir de proposiciones simples usando estos conectivos.

La siguiente definición es un ejemplo de una definición inductiva. Es una forma de definición muy común en Matemática.

Llamaremos *forma proposicional* a cualquier expresión en la que intervengan variables proposicionales y conectivos, construida según las siguientes reglas:
1) Toda variable proposicional es una forma proposicional.
2) Si $\mathcal{A}$ y $\mathcal{B}$ son formas proposicionales, entonces $\sim \mathcal{A}$, $\mathcal{A} \wedge \mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \Rightarrow \mathcal{B}$ y $\mathcal{A} \Leftrightarrow \mathcal{B}$ son formas proposicionales.

Ejemplos.

1. $(p \vee q) \Rightarrow (p \wedge r)$ es una forma proposicional.
2. $\sim p \vee q$ es una forma proposicional.
3. $p \Rightarrow (q \vee r)$ es una forma proposicional.

Vamos a construir las tablas de verdad para las formas proposicionales anteriores:

p	q	r	$p \vee q$	$p \wedge r$	$(p \vee q) \Rightarrow (p \wedge r)$
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	V	V	V
V	F	F	V	F	F
F	V	V	V	F	F
F	V	F	V	F	F
F	F	V	F	F	V
F	F	F	F	F	V

p	q	$\sim p$	$\sim p \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

p	q	r	$q \vee r$	$p \Rightarrow (q \vee r)$
V	V	V	V	V
V	V	F	V	V
V	F	V	V	V
V	F	F	F	F
F	V	V	V	V
F	V	F	V	V
F	F	V	V	V
F	F	F	F	V

Una forma proposicional es una *tautología* si toma el valor de verdad V para cualquier posible asignación de valor de verdad a las variables proposicionales que intervienen en ella.

Una forma proposicional es una *contradicción* si toma el valor de verdad F para cualquier posible asignación de valor de verdad a las variables proposicionales que intervienen en ella.

Ejemplos.

1. $(p \wedge q) \Rightarrow p$ es una tautología.
2. $p \wedge \sim p$ es una contradicción.
3. $p \vee \sim p$ es una tautología.

En efecto:

p	q	$p \wedge q$	$(p \wedge q) \Rightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

p	$\sim p$	$p \wedge \sim p$
V	F	F
F	V	F

p	$\sim p$	$p \vee \sim p$
V	F	V
F	V	V

Para verificar que una forma proposicional dada es una tautología, basta con construir su tabla de verdad. Dejamos como ejercicio verificar que las siguientes formas proposicionales, cuyo valor de verdad no es obvio sin la aplicación del método de las tablas de verdad, son tautologías:

1. $p \Rightarrow (q \Rightarrow p)$,
2. $\sim p \Rightarrow (p \Rightarrow q)$,
3. $(p \Rightarrow q) \vee (q \Rightarrow p)$.

Algunas tautologías reciben nombres especiales, por ser de uso muy frecuente. Se deja su verificación como ejercicio.

Identidad:	$p \Rightarrow p$, $p \Leftrightarrow p$
Ley de contradicción:	$\sim (p \wedge \sim p)$
Ley del tercero excluido:	$p \vee \sim p$
Ley de la doble negación:	$p \Leftrightarrow \sim\sim p$
Modus ponens:	$[(p \Rightarrow q) \wedge p] \Rightarrow q$
Modus tollens:	$[(p \Rightarrow q) \wedge \sim q] \Rightarrow \sim p$
Trasposición:	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
Simplificación:	$(p \wedge q) \Rightarrow p$
Adición:	$p \Rightarrow (p \vee q)$
Leyes de De Morgan:	$\sim (p \wedge q) \Leftrightarrow (\sim p \vee \sim q)$
	$\sim (p \vee q) \Leftrightarrow (\sim p \wedge \sim q)$
Transitividad:	$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$
Definición de la implicación:	$(p \Rightarrow q) \Leftrightarrow (\sim p \vee q)$

Se dice que una forma proposicional $\mathcal{A}$ *implica lógicamente* a una forma proposicional $\mathcal{B}$ si $\mathcal{A} \Rightarrow \mathcal{B}$ es una tautología. Se dice que $\mathcal{A}$ es *lógicamente equivalente* a $\mathcal{B}$ si $\mathcal{A} \Leftrightarrow \mathcal{B}$ es una tautología.

Ejemplos.

1. $p \wedge q$ implica lógicamente a p.
2. $\sim (p \wedge q)$ es lógicamente equivalente a $\sim p \vee \sim q$.
3. $\sim (p \vee q)$ es lógicamente equivalente a $\sim p \wedge \sim q$.

En efecto, verifiquemos los dos primeros casos.

p	q	$p \wedge q$	$(p \wedge q) \Rightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim (p \wedge q)$	$\sim p \vee \sim q$	$\sim (p \wedge q) \Leftrightarrow (\sim p \vee \sim q)$
V	V	F	F	V	F	F	V
V	F	F	V	F	V	V	V
F	V	V	F	F	V	V	V
F	F	V	V	F	V	V	V

1.2 Predicados y cuantificadores

Consideremos las siguientes proposiciones, en las que el sujeto está subrayado, y el resto es el predicado:

- *Jorge es un escritor.*
- *Mario toca muy bien el fagot.*
- *La ecuación* $x^2 + 1 = 0$ *no tiene solución en* $\mathbb{R}$.

Representemos los predicados por letras mayúsculas y los sujetos por letras minúsculas. Así, en los ejemplos anteriores tendríamos:

1. Sea E el predicado "es un escritor", j el sujeto "Jorge". Entonces la proposición "Jorge es un escritor" la simbolizamos $E(j)$. De la misma manera, si con l designamos al sujeto Luis, simbolizaríamos $E(l)$ la proposición "Luis es un escritor".
2. Sea F el predicado "toca muy bien el fagot". Entonces la proposición 2 se puede simbolizar $F(m)$, si con m designamos al sujeto Mario.
3. En este caso tenemos dos opciones, por ser el predicado una negación:
   (i) Si N significa "no tiene solución en $\mathbb{R}$" y e es "la ecuación $x^2 + 1 = 0$", la proposición 3 tendría la forma $N(e)$.
   (ii) Si R significa "tiene solución en $\mathbb{R}$", entonces la proposición tendría la forma $\sim R(e)$.

Consideremos ahora la siguiente proposición:

Todos los números naturales son positivos.

Más formalmente, podríamos escribir:

Para todo x, si x es un número natural, entonces x es positivo.

Ahora bien, si $N(x)$ indica "x es un número natural", y si $P(x)$ indica "x es positivo", podríamos escribir:

$$\textit{Para todo } x, \ N(x) \Rightarrow P(x).$$

La expresión "para todo" se llama un *cuantificador universal*, y se nota $(\forall x)$. Entonces tendríamos,

$$(\forall x)(N(x) \Rightarrow P(x)).$$

En forma análoga, la expresión "existe al menos un x tal que" se llama un *cuantificador existencial*, y se nota $(\exists x)$. Por ejemplo, la proposición

Existe un número primo x tal que x es impar

se traduce en:

$$(\exists x)(P(x) \wedge I(x)),$$

donde $P(x)$ es "x es primo", e $I(x)$ es "x es impar".

En general, si P es un predicado, se escribe $(\forall x)P(x)$ para indicar "todo objeto tiene la propiedad P", y $(\exists x)P(x)$ para indicar "existe al menos un objeto que tiene la propiedad P".

Ejemplos. Simbolizar:

1. *Todos los hombres merecen una oportunidad.*
   Si $H(x)$ es: x es un hombre, y $O(x)$ es : x merece una oportunidad, entonces la proposición se simboliza: $(\forall x)(H(x) \Rightarrow O(x))$.

2. *No todos los pájaros vuelan.*
   $\sim (\forall x)(P(x) \Rightarrow V(x))$, donde $P(x)$ es: x es un pájaro, y $V(x)$ es: x vuela.

3. *Todos los delfines son inteligentes.*
   $(\forall x)(D(x) \Rightarrow I(x))$, donde $D(x)$ es: x es un delfín, $I(x)$ es: x es inteligente.

4. *Algunos políticos no son honestos.*
   $(\exists x)(P(x) \wedge \sim H(x))$, donde $P(x)$ es: x es político, $H(x)$ es : x es honesto.

Existe una importante conexión entre los dos cuantificadores $(\forall x)$ y $(\exists x)$. Se puede ver intuitivamente que:

$$\begin{array}{lcl} \sim (\forall x)P(x) & \Leftrightarrow & (\exists x)(\sim P(x)) \\ \sim (\exists x)P(x) & \Leftrightarrow & (\forall x)(\sim P(x)) \end{array}$$

Analicemos estas equivalencias a la luz del ejemplo 4 anterior. Es claro que la proposición "Algunos políticos no son honestos", que hemos simbolizado

$$(\exists x)(P(x) \wedge \sim H(x))$$

es equivalente a la proposición "No todos los políticos son honestos", que podemos simbolizar

$$\sim (\forall x)(P(x) \Rightarrow H(x)).$$

De acuerdo a las reglas de la implicación, esto último es lo mismo que

$$\sim (\forall x)(\sim P(x) \vee H(x)),$$

lo cual equivale a

$$\sim (\forall x) \sim (P(x) \wedge \sim H(x)).$$

Se concluye entonces la equivalencia entre las dos proposiciones

$$(\exists x)(P(x) \wedge \sim H(x)) \quad \text{y} \quad \sim (\forall x) \sim (P(x) \wedge \sim H(x)),$$

esto es, $\sim (\exists x)(P(x) \wedge \sim H(x))$ es equivalente a $(\forall x) \sim (P(x) \wedge \sim H(x))$.

1.3 Ejercicios

1. Expresar simbólicamente las siguientes proposiciones compuestas.

   (a) La suma de dos números enteros es impar si y sólo si ambos números son pares o ambos números son impares.

   (b) Si no elegimos a A como presidente del partido, entonces perderemos las elecciones.

   (c) Ganaremos las elecciones, si A es elegido presidente del partido.

   (d) Si hay heladas y fuertes vientos, se arruinará la cosecha.

   (e) Si el asesino no ha dejado el país, entonces alguien lo está escondiendo.

   (f) El asesino ha dejado el país o alguien lo está escondiendo.

   (g) Este niño sabe leer, pero no escribe en absoluto.

   (h) Si y es entero entonces z no es real, suponiendo que x es un número racional.

   (i) 17 es un número primo, o es divisible por un número distinto de 17, -17, 1 y -1.

2. Construir la tabla de verdad de las siguientes formas proposicionales:

   (a) $\sim p \wedge \sim q$.

   (b) $\sim ((p \Rightarrow q) \Rightarrow (\sim (q \Rightarrow p)))$.

   (c) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.

3. ¿Cuáles de las siguientes formas proposicionales son tautologías?

   (a) $p \Rightarrow (q \Rightarrow p)$.

   (b) $(q \vee r) \Rightarrow (\sim r \Rightarrow q)$.

   (c) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \wedge \sim q) \vee r)$.

4. Indicar cuáles de los siguientes pares de formas proposicionales son lógicamente equivalentes.

   (a) $p \wedge q$; $\sim p \vee \sim q$.

   (b) $p \Rightarrow q$; $q \Rightarrow p$.

   (c) p; $p \wedge (q \vee \sim q)$.

   (d) $p \Rightarrow q$; $\sim q \Rightarrow \sim p$.

   (e) $(p \vee q) \wedge r$; $(p \wedge r) \vee (q \wedge r)$.

   (f) $(\sim p \wedge \sim q) \Rightarrow \sim r$; $r \Rightarrow (q \vee p)$.

   (g) $(\sim p \vee q) \Rightarrow r$; $(p \wedge \sim q) \vee r$.

5. Mostrar que la forma proposicional $(\sim p \Rightarrow q) \Rightarrow (p \Rightarrow \sim q)$ no es una tautología.

6. Traducir en símbolos:

   (a) No todo número primo es impar.

   (b) Existe un número entero que es divisible por 2 pero no es divisible por 4.

   (c) Ningún número es primo y compuesto.

   (d) Todo número real es racional o irracional.

   (e) Cualquier persona con constancia, puede aprender Matemática.

7. Traducir en símbolos:
   (i) sin usar cuantificadores existenciales. (ii) sin usar cuantificadores universales.
   (a) No todos los lobos viven en la montaña.
   (b) Algunos hombres son o inconscientes o perezosos.
   (c) Todo número real es negativo o posee una raíz cuadrada.
   (d) Ningún amante de la música puede no ir al concierto.

2 Conjuntos

En una serie de importantes publicaciones, un matemático alemán, Georg Cantor (1845 − 1918), formuló alrededor del año 1870 una teoría que ahora se conoce con el nombre de teoría de conjuntos. Esta teoría, muy resistida en sus comienzos, se ha transformado en una parte esencial de la moderna matemática. En efecto, las ideas de Cantor son aplicables a muchos problemas de diversas ramas de la Matemática, fuera de la teoría de conjuntos. Además, la teoría de conjuntos proporciona un marco uniforme en lo conceptual y en lo notacional dentro del cual se puede expresar toda la Matemática. Lo que sigue es una introducción intuitiva a la teoría de conjuntos.

Consideraremos como conceptos primitivos (no definidos) los de conjunto, elemento u objeto y pertenencia.

Generalmente designaremos a un conjunto con una letra latina mayúscula, y a los elementos que lo forman, con letras latinas minúsculas.

Para indicar que un elemento a pertenece a un conjunto A escribiremos $a \in A$. Si a no pertenece a A, escribiremos $a \notin A$.

Ejemplo. En este curso, con $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ indicaremos los conjuntos de números naturales, enteros, racionales, reales y complejos, respectivamente. Se tiene: $1 \in \mathbb{N}$, $\frac{1}{2} \notin \mathbb{N}$, $0 \in \mathbb{Z}$, $-7 \notin \mathbb{N}$, $9 \in \mathbb{N}$, $\sqrt{2} \in \mathbb{R}$, $\sqrt{2} \notin \mathbb{Q}$, $\sqrt{-1} \notin \mathbb{R}$, $1 + i \in \mathbb{C}$.

Un conjunto está bien definido, o bien determinado, cuando podemos precisar cuáles son sus elementos. Una forma de hacerlo es nombrar uno a uno todos los objetos que lo componen y encerrar esta lista entre llaves. Por ejemplo, si el conjunto A está formado por los elementos 1, 2, 3 y 4, podemos describir este conjunto escribiendo:

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

El orden en que escribimos los elementos es irrelevante, ya que un conjunto está completamente determinado por los objetos que lo componen. En consecuencia, $\{1, 2, 3, 4\} = \{2, 1, 3, 4\} = \{2, 1, 4, 3\} = \ldots$

Este método de describir un conjunto puede ser poco práctico o imposible en algunos casos, y deberemos usar otras formas de notación. Por ejemplo, $\{1, 2, 3, \ldots, 99, 100\}$ describe el conjunto de todos los números enteros positivos menores o iguales que 100.

Otras veces, para definir un conjunto indicamos una *propiedad común* a todos sus elementos y tal que *sólo sus elementos* la tengan. Así por ejemplo, los elementos del conjunto $A = \{1, 2, 3, 4\}$ pueden ser caracterizados como aquellos elementos x que cumplen la propiedad: $x \in \mathbb{N}$ y $x < 5$. Escribimos entonces:

$$A = \{x : x \in \mathbb{N} \text{ y } x < 5\}.$$

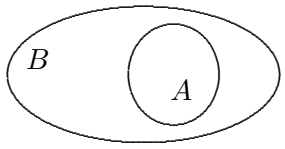
Ejemplos.

1. $A = \{x : x \in \mathbb{R} \text{ y } x > 0\}$ es el conjunto de los números reales positivos.
2. El conjunto de los números enteros pares puede escribirse $B = \{x : x \in \mathbb{Z} \text{ y } x \text{ es divisible por } 2\}$. También podemos escribir $B = \{x : x \in \mathbb{Z} \text{ y } x = 2k,\ k \in \mathbb{Z}\}$.
3. $C = \{x : x \in \mathbb{Z},\ x = 2k + 1,\ k \in \mathbb{Z}\}$ es el conjunto de los números enteros impares.
4. El conjunto $D = \{x : x \in \mathbb{N},\ x = 2k \text{ con } k \in \mathbb{N},\ x \text{ es múltiplo de } 7,\ x \leq 42\}$ tiene por elementos los números 14, 28 y 42.

2.1 Inclusión

Definición 2.1 *Dados dos conjuntos A y B, se dice que A está incluido en B, o que A es una parte de B, o que A es un subconjunto de B, si todo elemento de A pertenece a B. Se escribe $A \subseteq B$ o $B \supseteq A$.*

$$A \subseteq B \Leftrightarrow \text{ para todo } x \in A,\ x \in B.$$



Nota. Los dibujos que hemos utilizado para representar a los conjuntos A y B reciben el nombre de diagramas de Venn.

Cuando existe al menos un elemento que pertenece a A y no pertenece a B, la inclusión no se verifica, y escribiremos $A \not\subseteq B$.

Ejemplos.

1. Si $A = \{2, 4, 5\}$, $B = \{1, 2, 3, 4, 5\}$, $C = \{4, 6, 8\}$, y $D = \{3, 5, 7\}$, entonces $A \subseteq B$, $C \not\subseteq D$, $A \not\subseteq C$, $C \not\subseteq A$, $B \not\subseteq D$, $D \not\subseteq B$.

2. Si
   A es el conjunto de todos los divisores positivos de 12,
   B es el conjunto de todos los divisores positivos de 6,
   C es el conjunto de todos los divisores positivos de 4
   entonces $C \subseteq A$, $B \subseteq A$, $C \not\subseteq B$, $B \not\subseteq C$.

Propiedades de la inclusión

1. Reflexiva: $A \subseteq A$, para todo conjunto A.

2. Antisimétrica: Si $A \subseteq B$ y $B \subseteq A$ entonces $A = B$.

3. Transitiva: Si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$.

Por razones de conveniencia, introducimos un conjunto que carece de elementos, llamado el *conjunto vacío*. Lo simbolizamos por $\emptyset$ y puede definirse por cualquier propiedad que no sea verificada por ningún objeto. Por ejemplo, podríamos definir

$$\emptyset = \{x : x \neq x\} = \{x : x \in \mathbb{R},\ x^2 < 0\} = \{x : x \in \mathbb{N},\ 7 < x < 8\}.$$

Observación. El conjunto vacío está contenido en cualquier conjunto, es decir $\emptyset \subseteq A$, para todo conjunto A. En efecto, la implicación "$x \in \emptyset \Rightarrow x \in A$" es verdadera, pues su antecedente es falso.

Definición 2.2 *Se dice que el conjunto A es igual al conjunto B, si $A \subseteq B$ y $B \subseteq A$. Lo indicamos $A = B$*

Luego $A = B$ cuando todo elemento de A es un elemento de B y todo elemento de B es elemento de A, es decir, A y B tienen los mismos elementos.

La relación de inclusión no excluye la igualdad de los conjuntos. Si $A \subseteq B$ y además $A \neq B$, se dice que A es un subconjunto *propio* o una parte *propia* de B, o que A está contenido estrictamente en B. Lo notaremos $A \subset B$.

Ejemplos.

1. Sean $A = \{x : x \in \mathbb{N},\ 4 \leq 2 + 2x \leq 10\}$, $B = \{x : x \in \mathbb{N},\ 3 \leq 2 + x \leq 6\}$. Entonces $A = \{1, 2, 3, 4\}$ y $B = \{1, 2, 3, 4\}$. Luego $A = B$.

2. Veamos que los conjuntos $A = \{x : x \in \mathbb{R},\ x > 2\}$ y $B = \{x : x \in \mathbb{R},\ 3x - 4 > 2\}$ son iguales. Un procedimiento consiste en tomar un elemento cualquiera $x \in A$ y probar que $x \in B$, y recíprocamente, probar que todo elemento $x \in B$ verifica $x \in A$.

   En este caso, sea $x \in A$. Entonces $x \in \mathbb{R}$ y $x > 2$, lo que implica $3x > 6$, y de aquí se deduce $3x - 4 > 2$. Por lo tanto $x \in B$. Luego $A \subseteq B$.

   Recíprocamente, sea $x \in B$. Entonces $x \in \mathbb{R}$ y $3x - 4 > 2$, de donde resulta $3x > 6$, o sea, $x > 2$. Luego $x \in A$, y en consecuencia, $B \subseteq A$.

   Se ha probado entonces que $A = B$.

3. Sea A el conjunto de los números naturales pares y sea B el conjunto de los números naturales cuyo cuadrado es par. Veamos que $A = B$.

   En efecto, probemos en primer lugar que $A \subseteq B$. Sea $x \in A$; entonces existe $k \in \mathbb{N}$ tal que $x = 2k$. Luego $x^2 = (2k)^2 = 2(2k^2)$; entonces x^2 es par y por lo tanto $x \in B$. Hemos probado así que $A \subseteq B$.

   Probemos que $B \subseteq A$. Sea $y \in B$. Entonces y^2 es par. Queremos probar que $y \in A$, esto es, que y es par. Observemos en primer lugar que de la hipótesis resulta que $y \neq 1$. Si suponemos *por el absurdo* que y no es par, entonces y es de la forma $y = 2k + 1$, $k \in \mathbb{N}$. Pero en ese caso $y^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, que es impar, lo que contradice la hipótesis. En consecuencia y es par y por lo tanto $y \in A$, es decir $B \subseteq A$.

   Luego $A = B$.

Conjunto de partes de un conjunto

Dado un conjunto A, se puede considerar siempre el conjunto formado por los subconjuntos de A, el cual recibe el nombre de conjunto de las partes de A, y se indica $\mathcal{P}(A)$.

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

Observemos que $\mathcal{P}(A)$ nunca es vacío, pues como $\emptyset \subseteq A$ y $A \subseteq A$, entonces $\emptyset$ y A son elementos de $\mathcal{P}(A)$, es decir, $\emptyset \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$.

Ejemplo. Sea $A = \{a, b, c\}$. Los subconjuntos de A son:

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

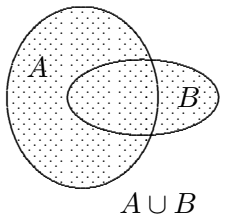
Entonces $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Observemos que en este ejemplo, el número de elementos de A es 3 y el de $\mathcal{P}(A)$ es $8 = 2^3$. Más generalmente, es posible probar (lo haremos más adelante) que si A es un conjunto con n elementos, entonces $\mathcal{P}(A)$ es un conjunto con 2^n elementos.

2.2 Unión de conjuntos

Definición 2.3 *Dados dos conjuntos A y B, se llama unión de A y B, y se indica $A \cup B$, al conjunto formado por todos los elementos que pertenecen a A o a B. En notación*

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



(Recordar que, en Matemática, el conectivo "o" se usa siempre en sentido no excluyente. En consecuencia, cuando decimos que un elemento está en A o en B no excluímos la posibilidad que esté en ambos conjuntos).

Ejemplo. Consideremos los conjuntos $A = \{x : x \in \mathbb{N},\ x \leq 4\} = \{1, 2, 3, 4\}$, y $B = \{x : x \in \mathbb{N},\ x \text{ es divisor de } 10\} = \{1, 2, 5, 10\}$. Entonces $A \cup B = \{1, 2, 3, 4, 5, 10\}$.

De la definición resulta que $A \subseteq A \cup B$ y $B \subseteq A \cup B$.

Propiedades de la unión.

1. Idempotente: $A \cup A = A$.
   Para demostrar la igualdad de los conjuntos $A \cup A$ y A hay que probar las dos inclusiones: (i) $A \cup A \subseteq A$ y (ii) $A \subseteq A \cup A$.

   Ya vimos que (ii) es consecuencia inmediata de la definición.

   Probemos (i), esto es que todo elemento de $A \cup A$ es un elemento de A. Sea $x \in A \cup A$. Entonces $x \in A$ ó $x \in A$, luego $x \in A$. Se tiene entonces $A \cup A \subseteq A$.

   De (i) y (ii) sigue la igualdad.

2. Conmutativa: $A \cup B = B \cup A$.
   Se demuestra de la misma manera que la propiedad anterior.

3. Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$.
   Debemos probar que:
   (a) $(A \cup B) \cup C \subseteq A \cup (B \cup C)$, y que
   (b) $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

   (a) Sea $x \in (A \cup B) \cup C \Rightarrow x \in (A \cup B)$ ó $x \in C \Rightarrow x \in A$ ó $x \in B$ ó $x \in C$. Luego $x \in A$ ó $x \in (B \cup C) \Rightarrow x \in A \cup (B \cup C)$. Entonces $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

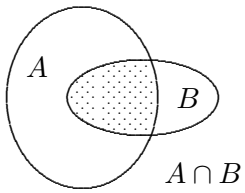
   (b) Sea $x \in A \cup (B \cup C) \Rightarrow x \in A$ ó $x \in (B \cup C) \Rightarrow x \in A$ ó $x \in B$ ó $x \in C \Rightarrow x \in (A \cup B)$ ó $x \in C \Rightarrow x \in (A \cup B) \cup C$. Entonces $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

   De (a) y (b) se tiene que $(A \cup B) \cup C = A \cup (B \cup C)$.

2.3 Intersección de conjuntos

Definición 2.4 *Dados dos conjuntos A y B, se llama intersección de A y B, y se indica $A \cap B$, al conjunto cuyos elementos son los elementos comunes a A y a B, es decir los elementos que pertenecen simultáneamente a los dos conjuntos.*

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



De la definición se desprende inmediatamente que $A \cap B \subseteq A$ y $A \cap B \subseteq B$.

Ejemplo. Consideremos los siguientes conjuntos: $A = \{x : x \in \mathbb{N},\ x \leq 4\} = \{1, 2, 3, 4\}$, y $B = \{x : x \in \mathbb{N},\ x \text{ es divisor de } 10\} = \{1, 2, 5, 10\}$. Entonces $A \cap B = \{1, 2\}$.

Si la intersección de dos conjuntos A y B es el conjunto vacío, se dice que A y B son *disjuntos*. Por ejemplo, el conjunto A de los números naturales pares y el conjunto B de los números naturales impares son disjuntos, ya que $A \cap B = \emptyset$.

Propiedades de la intersección.

1. Idempotente: $A \cap A = A$.
2. Conmutativa: $A \cap B = B \cap A$.
3. Asociativa: $(A \cap B) \cap C = A \cap (B \cap C)$.

La demostración de estas propiedades es análoga a la que hemos visto para las propiedades de la unión y quedan en consecuencia a cargo del alumno.

Teorema 2.5 $A \subseteq B \quad \Leftrightarrow \quad A \cup B = B$.

Demostración. Supongamos que $A \subseteq B$. Para probar que $A \cup B = B$, debemos probar que $B \subseteq A \cup B$ y que $A \cup B \subseteq B$. La primera inclusión es ya conocida. Para la segunda, sea $x \in A \cup B$, entonces $x \in A$ ó $x \in B$. Pero por hipótesis, $A \subseteq B$, luego $x \in B$, y se tiene entonces $A \cup B \subseteq B$. De lo anterior, $A \cup B = B$.

Para la recíproca, supongamos que $A \cup B = B$. Probemos que $A \subseteq B$. Sea $x \in A$. Entonces $x \in A \cup B$, y como por hipótesis $A \cup B = B$, se tiene que $x \in B$. Luego $A \subseteq B$. □

En forma análoga se prueba el siguiente

Teorema 2.6 $A \subseteq B \quad \Leftrightarrow \quad A \cap B = A$.

Las siguientes leyes se demuestran aplicando los dos teoremas anteriores.

Leyes de absorción

1. $A \cup (A \cap B) = A$.
   Como $A \cap B \subseteq A$, entonces por el teorema 1 resulta $A \cup (A \cap B) = A$.
2. $A \cap (A \cup B) = A$.
   Como $A \subseteq A \cup B$, entonces por el teorema 2 resulta $A \cap (A \cup B) = A$.

Leyes distributivas

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

Demostraremos sólo la primera, dejando la otra como ejercicio.

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
   Como se trata de probar una igualdad de conjuntos, debemos probar una doble inclusión.

   (a) $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
   Sea $x \in A \cup (B \cap C) \Rightarrow x \in A$ ó $x \in B \cap C$. Luego:
   Si $x \in A \Rightarrow x \in A \cup B$ y $x \in A \cup C$. Luego $x \in (A \cup B) \cap (A \cup C)$.
   Si $x \in B \cap C \Rightarrow x \in B$ y $x \in C$, luego $x \in A \cup B$ y $x \in A \cup C$. Luego $x \in (A \cup B) \cap (A \cup C)$.
   Es decir, en cualquier caso, $x \in (A \cup B) \cap (A \cup C)$. Entonces $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

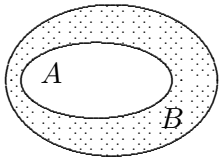
   (b) $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
   Sea $x \in (A \cup B) \cap (A \cup C) \Rightarrow x \in (A \cup B)$ y $x \in (A \cup C) \Rightarrow (x \in A$ o $x \in B)$ y $(x \in A$ o $x \in C)$.
   Si $x \in A \Rightarrow x \in A \cup (B \cap C)$. Si $x \notin A \Rightarrow x \in B$ y $x \in C$, de donde $x \in (B \cap C)$. Luego $x \in A \cup (B \cap C)$.
   Es decir, en cualquiera de los dos casos, tanto si $x \in A$ como si $x \notin A$, se cumple que $x \in A \cup (B \cap C)$. Luego $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

De (a) y (b) resulta: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

2.4 Complemento

Definición 2.7 *Dados dos conjuntos A y B, tales que $A \subseteq B$, se llama complemento de A relativo a B, y lo notamos $\mathcal{C}_B A$, al conjunto formado por todos los elementos de B que no pertenecen a A.*

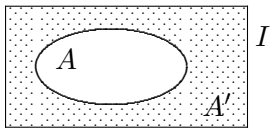
$$\mathcal{C}_B A = \{x : x \in B \text{ y } x \notin A\}.$$



Por ejemplo, si $B = \{2, 3, 5, 7, 11\}$ y $A = \{3, 7\}$ entonces $\mathcal{C}_B A = \{2, 5, 11\}$. Si $B = \mathbb{R}$ y $A = \{x : x \in \mathbb{R},\ x < 0\}$, entonces $\mathcal{C}_B A = \{x : x \in \mathbb{R},\ x \geq 0\}$

En general se considera un conjunto fijo I, respecto del cual se está desarrollando una teoría determinada, y entonces se trabaja siempre con subconjuntos de I y complementos relativos a I. Al conjunto I se lo llama *referencial* o *universal*, y el complemento de un subconjunto A de I, se lo indica simplemente A'.

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



Por ejemplo, si I es el conjunto de los números enteros, A el conjunto de los números enteros pares, entonces A' es el conjunto de los números enteros impares.

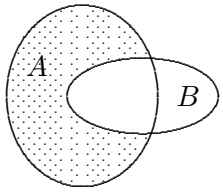
De la definición resulta en forma inmediata que:

1. $(A')' = A$, 2. $A \cup A' = I$ 3. $A \cap A' = \emptyset$, 4. $I' = \emptyset$ y 5. $\emptyset' = I$

2.5 Diferencia

Definición 2.8 *Dados dos conjuntos A y B, se llama diferencia entre A y B, en ese orden, al conjunto formado por los elementos que pertenecen a A y no pertenecen a B. Se nota $A - B$.*

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



Por ejemplo, Si $A = \{1, 2, 3, 4\}$ y $B = \{2, 4, 6, 8\}$, entonces $A - B = \{1, 3\}$ y $B - A = \{6, 8\}$.

Como casos particulares tenemos los siguientes:

- Si $A \subseteq B \Rightarrow A - B = \emptyset$ y $B - A = \mathcal{C}_B A$.
- Si $A = B \Rightarrow A - B = \emptyset$ y $B - A = \emptyset$.
- Si $A \cap B = \emptyset \Rightarrow A - B = A$ y $B - A = B$.

Observación. La siguiente propiedad es muy útil y resulta en forma inmediata de la definición de diferencia: $A - B = A \cap B'$.

Teorema 2.9 $A \subseteq B \Leftrightarrow B' \subseteq A'$.

Demostración. Supongamos que $A \subseteq B$ y probemos que $B' \subseteq A'$.
Sea $x \in B'$. Entonces $x \notin B$, y como por hipótesis $A \subseteq B$, entonces $x \notin A$, luego $x \in A'$. Luego $B' \subseteq A'$.

Supongamos ahora que $B' \subseteq A'$ y probemos que $A \subseteq B$.
Sea $x \in A$. Entonces $x \notin A'$, y como por hipótesis $B' \subseteq A'$, entonces $x \notin B'$, es decir $x \in B$. Luego $A \subseteq B$. □

Leyes de De Morgan.

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

Antes de demostrarlas, conviene tener presente que:

- $x \notin A \cup B$ significa que $x \notin A$ **y** $x \notin B$.
- $x \notin A \cap B$ significa que $x \notin A$ **o** $x \notin B$.

Demostración.

1. Para probar que $(A \cap B)' = A' \cup B'$ debemos probar: a) $A' \cup B' \subseteq (A \cap B)'$ y b) $(A \cap B)' \subseteq A' \cup B'$.
   a) Sea $x \in A' \cup B' \Rightarrow x \in A'$ ó $x \in B' \Rightarrow x \notin A$ ó $x \notin B \Rightarrow x \notin A \cap B \Rightarrow x \in (A \cap B)'$. Luego $A' \cup B' \subseteq (A \cap B)'$.
   b) Sea $x \in (A \cap B)' \Rightarrow x \notin A \cap B \Rightarrow x \notin A$ ó $x \notin B \Rightarrow x \in A'$ ó $x \in B' \Rightarrow x \in A' \cup B'$. Luego $(A \cap B)' \subseteq A' \cup B'$.

De a) y b) se tiene $(A \cap B)' = A' \cup B'$.

2. Para probar que $(A \cup B)' = A' \cap B'$ debemos probar:
   a) $(A \cup B)' \subseteq A' \cap B'$ y b) $A' \cap B' \subseteq (A \cup B)'$.

   a) Sea $x \in (A \cup B)' \Rightarrow x \notin A \cup B \Rightarrow x \notin A$ y $x \notin B \Rightarrow x \in A'$ y $x \in B' \Rightarrow x \in A' \cap B'$. Luego $(A \cup B) \subseteq A' \cap B'$.

   b) Sea $x \in A' \cap B' \Rightarrow x \in A'$ y $x \in B' \Rightarrow x \notin A$ y $x \notin B \Rightarrow x \notin A \cup B \Rightarrow x \in (A \cup B)'$. Luego $A' \cap B' \subseteq (A \cup B)'$.

   De a) y b) se tiene $(A \cup B)' = A' \cap B'$.

□

2.6 Producto cartesiano

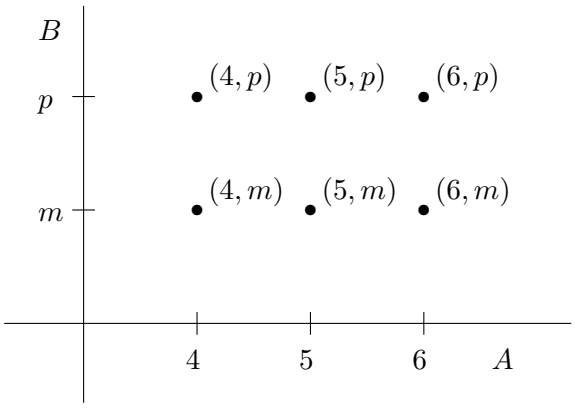
Dados dos conjuntos A y B, y objetos cualesquiera $a \in A$ y $b \in B$, consideraremos *pares ordenados* de primera coordenada a y segunda coordenada b, que notaremos (a, b). Dos pares ordenados (a, b) y (a', b') son iguales si y sólo si $a = a'$ y $b = b'$.

Definición 2.10 *Dados dos conjuntos A y B, llamamos producto cartesiano de A y B, y lo notamos $A \times B$, al conjunto formado por todos los pares ordenados (a, b), con $a \in A$ y $b \in B$. Es decir,*

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

Ejemplo. Si $A = \{4, 5, 6\}$ y $B = \{m, p\}$ entonces $A \times B = \{(4, m), (4, p), (5, m), (5, p), (6, m), (6, p)\}$ y $B \times A = \{(m, 4), (m, 5), (m, 6), (p, 4), (p, 5), (p, 6)\}$.

El producto cartesiano de A por B se suele representar en el plano considerando dos rectas perpendiculares. Los elementos de A se representan por puntos sobre la recta horizontal, y los elementos de B se representan por puntos sobre la recta vertical. Cada elemento (a, b) de $A \times B$ se representa por el punto del plano que se obtiene como intersección de rectas perpendiculares a los ejes por los puntos que corresponden a a y a b.



Al producto cartesiano $A \times A$ se lo nota A^2. Si $A \neq B$, entonces $A \times B \neq B \times A$.

2.7 Ejercicios

1. Determinar los elementos de los siguientes conjuntos:

   (a) $A = \{x : x \in \mathbb{N},\ 3 \leq x < 8\}$.

   (b) $A = \{x : x \in \mathbb{Z},\ x \text{ es múltiplo de } 3,\ -21 < x < 21\}$.

   (c) $A = \{x : x \in \mathbb{N},\ x \leq 5\}$.

   (d) $A = \{x : x \in \mathbb{N},\ 2 \leq x \leq 9\}$.

   (e) $A = \{x : x \in \mathbb{N},\ x = 2n + 1,\ n \in \mathbb{N}\}$.

   (f) $A = \{x : x \in \mathbb{N},\ x = 2n + 1,\ n \in \mathbb{N},\ n \geq 5\}$.

   (g) $A = \{x : x \in \mathbb{N},\ x \text{ es múltiplo de } 5,\ x < 40\}$.

   (h) $A = \{x : x \in \mathbb{Z},\ x^2 = 1\}$.

   (i) $A = \{x : x \in \mathbb{Z},\ -9 \leq x < 6\}$.

   (j) $A = \{x : x \in \mathbb{N},\ x \text{ es múltiplo de } 2,\ x^2 < 100\}$.

2. Definir simbólicamente los siguientes conjuntos:

   (a) Números naturales pares menores que 20.

   (b) Números enteros impares menores que 5.

   (c) Números reales positivos cuyo cuadrado es menor o igual que 2.

   (d) $\{12, 15, 18, 21, 24\}$.

3. Dados los siguientes conjuntos:

   $A = \{x : x \in \mathbb{N},\ 1 \leq x \leq 5\}$,
   $B = \{x : x \in \mathbb{N},\ 1 < x < 5\}$,
   $C = \{x : x \in \mathbb{N},\ x < 2\}$,
   $D = \{x : x \in \mathbb{N},\ 3x - 2 = 1\}$,

   completar con la relación $=$, $\subseteq$, $\supseteq$, $\in$ o $\notin$ que corresponda:

   (a) A ..... B (d) D ..... A (g) C ..... D

   (b) 1 ..... B (e) 1 ..... A (h) 5 ..... B

   (c) 0 ..... D (f) C ..... A (i) 2 C

4. Sean $V = \{d\}$, $W = \{c, d\}$, $X = \{a, b, c\}$, $Y = \{a, b\}$, $Z = \{a, b, d\}$.

   Indicar, justificando la respuesta, si las siguientes afirmaciones son verdaderas o falsas:

   (a) $Y \subseteq X$ (d) $V \supseteq X$ (g) $Z \supseteq V$

   (b) $X \neq Z$ (e) $W \not\supseteq V$ (h) $W \subseteq Y$

   (c) $V \not\subseteq Y$ (f) $X = W$ (i) $X \subseteq Z$

5. Dados los siguientes conjuntos, indicar en cada caso la cantidad de elementos del conjunto de partes: $A = \{a\}$, $B = \emptyset$, $C = \{1, 2, 3, 4, 5\}$.

6. Sea $A = \{a, b, c\}$. Decir si las siguientes afirmaciones son verdaderas o falsas: $\emptyset \subseteq A$, $\emptyset \in A$, $\emptyset \in \mathcal{P}(A)$, $\emptyset \subseteq \mathcal{P}(A)$, $\{a, b\} \in \mathcal{P}(A)$, $a \in \mathcal{P}(A)$, $\{a\} \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$, $A \in A$, $A \subseteq A$.

7. Los alumnos de una escuela pueden inscribirse para practicar alguno de estos deportes: fútbol, basquet y rugby. Escribir todas las posibilidades. ¿Cuántas son?

8. Dados los siguientes conjuntos: $I = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 4\}$, $C = \{2, 4, 5\}$, efectuar las operaciones que se indican y hacer los diagramas de Venn correspondientes:
   (a) $I \cap B$
   (b) $I \cup B$
   (c) $B \cup C$
   (d) $B \cap C$
   (e) $B - I$
   (f) $I - B$
   (g) $C - B$
   (h) $B - C$

9. (a) En cada uno de los siguientes casos, completar con $\subseteq$ o $\supseteq$, según corresponda:
   $A \cap B \ldots\ldots A, \quad A \cup B \ldots\ldots B, \quad A - B \ldots\ldots A, \quad A \cap B \ldots\ldots A \cup B.$
   (b) ¿En qué condiciones se cumple cada una de las siguientes igualdades?
   $A \cap B = A, \quad A \cup B = A, \quad A \cup B = A \cap B.$

10. Sean
    $A = \{x : x \in \mathbb{N},\ x < 20,\ x \text{ es múltiplo de } 2\}$,
    $B = \{x : x \in \mathbb{N},\ x \leq 10\}$,
    $C = \{x : x \in \mathbb{N},\ 10 < x < 20\}$,
    $D = \{x : x \in \mathbb{N},\ x < 20,\ x \text{ es múltiplo de } 5\}$,
    $I = \{x : x \in \mathbb{N},\ x < 20\}$, conjunto universal.

    Hallar:
    (a) $A \cap B$.
    (b) $A \cup B$.
    (c) $A \cap C$.
    (d) $A \cap (B \cup C)$ y $(A \cap B) \cup (A \cap C)$.
    (e) $A' \cup D'$ y $(A \cap D)'$.
    (f) $A' \cap D'$ y $(A \cup D)'$.
    (g) $B - C$.
    (h) $B - A$ y $B - (A \cap B)$.

11. Hacer un diagrama de Venn con tres conjuntos A, B y C de modo que A, B y C tengan las siguientes características:
    (a) $A \subseteq B, \quad C \subseteq B, \quad A \cap C = \emptyset$.
    (b) $A \subseteq B, \quad C \not\subseteq B, \quad A \cap C = \emptyset$.
    (c) $A \subseteq C, \quad A \neq C, \quad B \cap C = \emptyset$.
    (d) $A \subseteq (B \cap C), \quad B \subseteq C, \quad C \neq B, \quad A \neq C$.

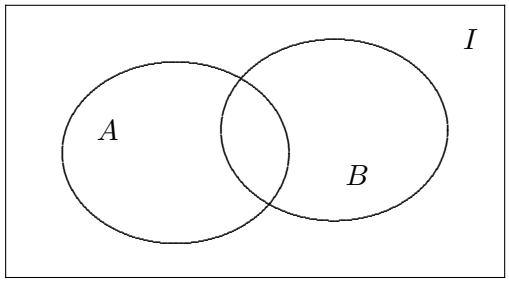
12. Demostrar las siguientes propiedades:
    (a) Si $A \subseteq C$ y $B \subseteq C$, entonces $A \cup B \subseteq C$.
    (b) Si $C \subseteq A$ y $C \subseteq B$, entonces $C \subseteq A \cap B$.
    (c) $A \subseteq B$ si y sólo si $A \cup (B - A) = B$
    (d) $A \cap B' = \emptyset$ si y sólo si $A \subseteq B$.
    (e) $A \subseteq B$ si y sólo si $B' \subseteq A'$.

13. Probar las siguientes igualdades por doble inclusión o por cálculo directo (propiedades):

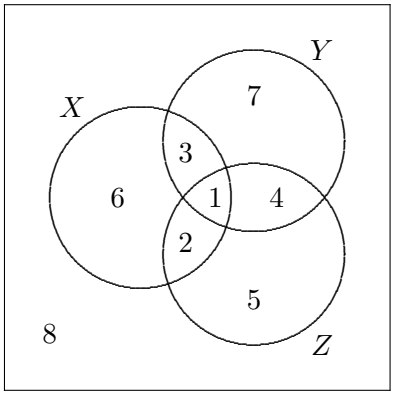
(a) $A - B = A - (A \cap B)$.
(b) $(A \cup B) - C = (A - C) \cup (B - C)$.
(c) $(A \cap B) - C = (A - C) \cap (B - C)$.
(d) $(A - B) - C = A - (B \cup C)$.
(e) $A - (B - C) = (A - B) \cup (A \cap C)$.
(f) $(A - B) - C \subseteq A - (B - C)$.
(g) $A \cup (B - C) = (A \cup B) - (C - A)$.
(h) $(A - B) - (A - C) = A \cap (C - B)$.
(i) $A - (B \cup C) = (A - B) \cap (A - C)$.
(j) $B - (A \cap C) = (B - A) \cup (B - C)$.
(k) $[(A \cup B)' \cup (A' - B)]' \cap (B - A)' = A$.

14. Verificar con un ejemplo que la unión no es distributiva con respecto a la diferencia.

15. Dados los conjuntos que se indican en el diagrama, determinar gráficamente:
    (a) $A \cup B$.
    (b) $A \cap B$.
    (c) $A - B$.
    (d) $B - A$.
    (e) A'.
    (f) B'.
    (g) $A' \cup B'$.
    (h) $A' \cap B'$.



16. Encontrar una expresión algebraica que determine exactamente cada uno de los ocho subconjuntos que figuran en el diagrama:



17. Sea A un conjunto con cinco elementos y B un conjunto con tres elementos. Decir cuáles de las siguientes afirmaciones pueden ser verdaderas, cuáles son necesariamente falsas y cuáles son necesariamente verdaderas:

(a) $A \cap B$ tiene exactamente 5 elementos.

(b) $A \cup B$ tiene exactamente 5 elementos.

(c) $A \cup B$ tiene exactamente 4 elementos.

(d) $A \cap B$ es un subconjunto de A.

(e) B es un subconjunto de A.

(f) $A \cup B$ no puede tener más de 8 elementos.

(g) $A \cap B$ tiene al menos un elemento.

(h) Si $A \cap B = \emptyset$ entonces $A \cup B = \emptyset$.

(i) Si $A \cap B$ tiene 3 elementos, entonces $B \subseteq A$.

18. Cien personas respondieron a un cuestionario formado por tres preguntas, cada pregunta debía contestarse por sí o por no, y una sola de estas respuestas era correcta. Si sabemos que:
8 personas contestaron bien las tres preguntas,
9 personas contestaron bien sólo la primera y la segunda,
11 personas contestaron bien sólo la primera y la tercera,
6 personas contestaron bien sólo la segunda y la tercera,
55 personas contestaron bien la primera, por lo menos,
32 personas contestaron bien la segunda, por lo menos,
49 personas contestaron bien la tercera, por lo menos,
¿Cuántas personas no contestaron ninguna pregunta?

19. De 73 alumnos del Conservatorio de Música, 52 saben tocar el clarinete, 25 saben tocar el fagot y 20 saben tocar el oboe. 17 saben tocar el clarinete y el fagot, 12 pueden tocar clarinete y oboe y 7 pueden tocar fagot y oboe. Sólamente uno sabe tocar los tres instrumentos. ¿Cuántos no saben tocar nunguno de los tres?

20. Dados los conjuntos $A = \{2, 3\}$, $B = \{x, y, z\}$ y $C = \{a\}$, hallar $A \times B$, $A \times C$, $B \times C$, $C \times A$, A^2 y C^3.

21. Si A es un conjunto con n elementos y B uno con m elementos, ¿cuántos elementos tienen $A \times B$ y $B \times A$?

22. Demostrar que cualquiera que sean A, B, C tres conjuntos no vacíos tales que $B \cap C \neq \emptyset$, se tiene $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

3 Relaciones binarias

En la vida diaria, por una relación entendemos un criterio que nos permite asociar ciertos objetos. Así por ejemplo, "es hijo de" es una relación entre personas, y cuando decimos que "Enrique es hijo de Fernando" se está afirmando algo sobre el par de personas (Enrique, Fernando). Lo hemos escrito de esta forma, porque es claro que se trata de un par ordenado, ya que si intercambiamos los nombres, la relación deja de cumplirse. Si tenemos entonces un conjunto A de personas, la relación "es hijo de" nos permite distinguir algunos pares de personas de otros: los pares formados por un hijo y su padre o madre, y todos los demás. Esto es, la relación dada nos permite distinguir un subconjunto R del producto cartesiano $A \times A$: R estará formado por los pares ordenados de personas (a, b), $a, b \in A$, tales que a es hijo de b.

Análogamente, la relación "estudia la misma carrera que" entre el conjunto A formado por los alumnos de esta Universidad puede caracterizarse dando un subconjunto R del producto cartesiano $A \times A$. Afirmar que dos alumnos a y b estudian la misma carrera equivale a decir que $(a, b) \in R$.

En Matemática la noción de relación es de mucha importancia. Definir una relación R es fijar una ley que permita decir para cada par de objetos a y b, cuándo a está en la relación R con b. Por ejemplo, si R es la relación $\leq$ entre números naturales, entonces $4R6$, o escrito de otra forma, $(4, 6) \in R$.

3.1 Definiciones

Definición 3.1 *Dados dos conjuntos A y B, una relación binaria R entre los elementos de A y los elementos de B (o en $A \times B$), es un subconjunto del producto cartesiano $A \times B$:*

$$R \subseteq A \times B.$$

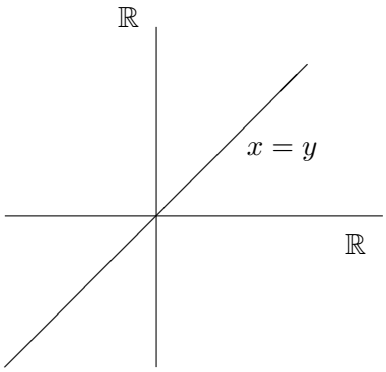
Se escribe aRb si $(a, b) \in R$. En particular, si $A = B$, entonces R se llama una relación binaria **en** A.

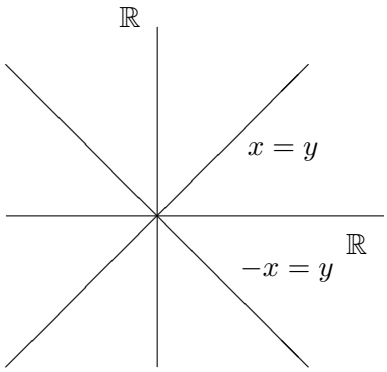
Ejemplos.

1. Si $A = \{10, 9, 7, 5\}$ y $B = \{6, 8, 15\}$, el conjunto $R = \{(x, y) \ : \ (x, y) \in A \times B, \ x > y\}$ $= \{(10, 6), (10, 8), (9, 6), (9, 8), (7, 6)\}$ es una relación binaria entre los elementos de A y los elementos de B.

2. Si $A = \{2, 3, 5\}$ y $B = \{4, 6, 8, 9\}$, el conjunto $R = \{(x, y) \ : \ (x, y) \in A \times B, \ x$ es divisor de $y\} = \{(2, 4), (2, 6), (2, 8), (3, 6), (3, 9)\}$ es una relación binaria en $A \times B$.

3. Sea $A = B = \mathbb{R}$ el conjunto de los números reales, y consideremos la relación S_1 definida por: $xS_1y \Leftrightarrow x = y$. S_1 es la relación $S_1 = \{(x, x) \ : \ x \in \mathbb{R}\}$ y su gráfico es la bisectriz del primer y tercer cuadrante. Sea $A = B = \mathbb{R}$, y consideremos la relación S_2 definida por: $xS_2y \Leftrightarrow x = y$ ó $x = -y$. S_2 es la relación $S_2 = \{(x, x) \ : \ x \in \mathbb{R}\} \cup \{(x, -x) \ : \ x \in \mathbb{R}\}$ y su gráfico es la bisectriz del primer y tercer cuadrante y la del segundo y cuarto cuadrante.





4. El conjunto $\emptyset$ y el conjunto total $A \times A$ son relaciones binarias en A.

Definición 3.2 *Dada una relación $R \subseteq A \times A$, diremos que R es reflexiva si aRa para todo $a \in A$. ($(a, a) \in R$ para todo $a \in A$).*

Ejemplos. Son reflexivas las siguientes relaciones:

1. Paralelismo: Sea A en conjunto de todas las rectas de un plano. Si $l_1, l_2 \in A$, $(l_1, l_2) \in R \Leftrightarrow l_1$ es paralela a l_2.
2. $A = \{1, 2, 3\}$, $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$.
3. La igualdad: Si $x, y \in A$ y R está definida por $(x, y) \in R \Leftrightarrow x = y$.
4. La relación "divide" en $\mathbb{N}$. Dados $a, b \in \mathbb{N}$ definimos la siguiente relación: $aRb \Leftrightarrow a$ divide a b, o sea, existe $k \in \mathbb{N}$ tal que $b = k \cdot a$. En lugar de aRb notaremos $a \mid b$. Esta relación es reflexiva: $a \mid a$, para todo $a \in \mathbb{N}$, pues $a = k \cdot a$ con $k = 1$.

Definición 3.3 *Diremos que una relación $R \subseteq A \times A$ es simétrica si se verifica que: Si aRb entonces bRa. ($(a, b) \in R \Rightarrow (b, a) \in R$).*

Ejemplos. Las siguientes relaciones son simétricas:

1. Perpendicularidad: Sea A en conjunto de todas las rectas de un plano. Si $l_1, l_2 \in A$, entonces $(l_1, l_2) \in R \Leftrightarrow l_1$ es perpendicular a l_2.
2. $A = \{a, b, c\}$, $R = \{(a, b), (a, c), (b, a), (c, a)\}$.
3. $A = \{1, 2, 3\}$, $R = \{(1, 1), (2, 3), (3, 2)\}$.

Definición 3.4 *Diremos que una relación $R \subseteq A \times A$ es antisimétrica si se verifica que:*
Si aRb y bRa entonces $a = b$. ($(a, b) \in R$ y $(b, a) \in R \Rightarrow a = b$).
Equivalentemente: Si $a \neq b$ entonces $a \not R\, b$ o bien $b \not R\, a$. ($a \neq b \Rightarrow (a, b) \notin R$ o bien $(b, a) \notin R$).

Ejemplos. Son antisimétricas:

1. La relación *divide* en los números naturales: $a, b \in \mathbb{N},\ a \mid b \ \Leftrightarrow\ b = k \cdot a,\ k \in \mathbb{N}$.
   Si $a \mid b$ y $b \mid a$ entonces $a = b$.
   En efecto, de $a \mid b$ resulta que existe $k \in \mathbb{N}$ tan que $b = k \cdot a$, y de $b \mid a$ se tiene que exuste $k' \in \mathbb{N}$ tal que $a = k' \cdot b$. Reemplazando obtenemos: $b = k \cdot k' \cdot b$, de donde $k \cdot k' = 1$, y como $k, k' \in \mathbb{N}$, entonces $k = k' = 1$. Luego $a = k' \cdot b = 1 \cdot b = b$.

2. La inclusión entre conjuntos: $X, Y \in \mathcal{P}(A)$, $(X, Y) \in R \ \Leftrightarrow\ X \subseteq Y$.

3. $A = \{1, 2, 3, 4\},\ R = \{(1, 1), (2, 3), (4, 4), (1, 4)\}$.

Nota: Otra expresión equivalente de la propiedad antisimétrica es la siguiente: Si $a \neq b$ y aRb entonces $b \not R\ a$. ($a \neq b$ y $(a, b) \in R\ \Rightarrow\ (b, a) \notin R$).

Definición 3.5 *Diremos que una relación $R \subseteq A \times A$ es transitiva, si se verifica que: Si aRb y bRc entonces aRc.* ($(a, b) \in R$ *y* $(b, c) \in R\ \Rightarrow\ (a, c) \in R$).

Ejemplos. Las siguientes relaciones son transitivas:

1. Paralelismo de rectas en el plano.

2. $A = \{1, 2, 3, 4\},\ R = \{(1, 2), (2, 4), (1, 4)\}$.

3. La relación *divide* en $\mathbb{N}$. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.
   De $a \mid b$ resulta que existe $k \in \mathbb{N}$ tal que $b = k \cdot a$. De $b \mid c$, existe $k' \in \mathbb{N}$ tal que $c = k' \cdot b$. Reemplazando se tiene: $c = k \cdot k' \cdot a$, de donde $c = k'' \cdot a$, $k'' \in \mathbb{N}$, y por lo tanto $a \mid c$.

Ejemplo. Hallar todas las relaciones sobre un conjunto con 2 elementos $A = \{a, b\}$. Estudiar sus propiedades.

Relación	Reflexiva	Simétrica	Antisimétrica	Transitiva
$\emptyset$	no	sí	sí	sí
$\{(a, a)\}$	no	sí	sí	sí
$\{(a, b)\}$	no	no	sí	sí
$\{(b, a)\}$	no	no	sí	sí
$\{(b, b)\}$	no	sí	sí	sí
$\{(a, a), (a, b)\}$	no	no	sí	sí
$\{(a, a), (b, a)\}$	no	no	sí	sí
$\{(a, a), (b, b)\}$	sí	sí	sí	sí
$\{(a, b), (b, a)\}$	no	sí	no	no
$\{(a, b), (b, b)\}$	no	no	sí	sí
$\{(b, a), (b, b)\}$	no	no	sí	sí
$\{(a, a), (a, b), (b, a)\}$	no	sí	no	no
$\{(a, a), (a, b), (b, b)\}$	sí	no	sí	sí
$\{(a, a), (b, a), (b, b)\}$	sí	no	sí	sí
$\{(a, b), (b, a), (b, b)\}$	no	sí	no	no
$A \times A$	sí	sí	no	sí

3.2 Relaciones de equivalencia

Definición 3.6 *Diremos que una relación R en A es de equivalencia si es reflexiva, simétrica y transitiva.*

Ejemplos.

1. Las siguientes expresiones, definidas sobre conjuntos adecuados, son relaciones de equivalencia:

   Tiene el mismo apellido que
   Es compatriota de
   Tiene tantas sílabas como
   Tiene la misma edad que
   Empieza con la misma letra que
   Estudia lo mismo que (suponiendo que ningún alumno estudia dos carreras)
   Tiene tantas cifras como

2. Sea $m \in \mathbb{Z}$ un entero fijo y sea R la siguiente relación: $(a, b) \in R \Leftrightarrow$ existe un entero k tal que $a - b = k \cdot m$. Veremos más adelante que R es una relación de equivalencia en $\mathbb{Z}$.

Partición de un conjunto

La noción de partición de un conjunto que definiremos a continuación, está ligada a la propiedad fundamental que tienen las relaciones de equivalencia.

Dado un conjunto A, diremos que una familia $\{A_i\}_{i \in I}$ de subconjuntos de A constituye una partición de A si:

1. $A_i \neq \emptyset$, para todo $i \in I$,
2. Si $i \neq j$ entonces $A_i \cap A_j = \emptyset$,
3. $\bigcup_{i \in I} A_i = A$,

donde $\bigcup_{i \in I} A_i = \{x : x \in A_i, \text{ para algún } i \in I\}$.

Es decir, todos los subconjuntos de la familia son no vacíos, son disjuntos dos a dos y su unión es A.

Ejemplos.

1. Sea $A = \{m, n, p, q, r\}$ y sean $A_1 = \{m\}$, $A_2 = \{n, p\}$ y $A_3 = \{q, r\}$. Es claro que la familia $\{A_i\}_{i=1,2,3}$ es una partición de A.
2. El conjunto de los números reales positivos, el conjunto de los números reales negativos y el cero, forman una partición de $\mathbb{R}$.
3. Si A es un conjunto no vacío, entonces $\{A\}$ es una partición de A, llamada *partición trivial*.
4. Si A es un conjunto no vacío, entonces $\{\{x\} : x \in A\}$ es una partición de A, llamada *partición identidad*.

Vamos a ver ahora que dada una relación de equivalencia sobre un conjunto A, queda determinada una partición de A por medio de subconjuntos llamados clases de equivalencia.

Partición inducida por una relación de equivalencia. Clases de equivalencia

Definición 3.7 *Dada una relación de equivalencia R definida en un conjunto A, llamaremos "clase de equivalencia de un elemento $x \in A$", al conjunto de todos los elementos de A que están en relación con x. Notaremos C_x.*

$$C_x = \{z \in A : zRx\}.$$

Observar que las clases de equivalencia de elementos de A son subconjuntos de A.

Propiedades de las clases de equivalencia

1. $C_x \neq \emptyset$, para todo $x \in A$. (Ninguna clase es vacía).
2. $C_x = C_y \Leftrightarrow xRy$.
3. $C_x \neq C_y \Rightarrow C_x \cap C_y = \emptyset$.

Demostración.

1. $C_x \neq \emptyset$, para todo $x \in A$.
   Se tiene que $x \in C_x$. Luego $C_x \neq \emptyset$.
2. $C_x = C_y \Leftrightarrow xRy$.
   Supongamos que xRy y probemos que $C_x = C_y$.
   a) Sea $z \in C_x \Rightarrow zRx$ y como por hipótesis xRy, entonces zRy, esto es, $z \in C_y$. Luego $C_x \subseteq C_y$.
   b) Sea $z \in C_y \Rightarrow zRy$ y como por hipótesis xRy, entonces por simetría yRx. Luego zRx, esto es, $z \in C_x$. Luego $C_y \subseteq C_x$.
   De a) y b) se tiene $C_x = C_y$.
   Para la recíproca, supongamos que $C_x = C_y$. Probemos que xRy.
   Como $x \in C_x$ y $C_x = C_y$, entonces $x \in C_y$, es decir, xRy.
3. $C_x \neq C_y \Rightarrow C_x \cap C_y = \emptyset$.
   Supongamos por el absurdo que $C_x \cap C_y \neq \emptyset$. Entonces existe $z \in C_x \cap C_y$, es decir $z \in C_x$ y $z \in C_y$. Entonces existe z tal que zRx y zRy. De aquí resulta xRy. Luego $C_x = C_y$. Contradicción.

□

En base a estas tres propiedades se tiene el siguiente teorema:

Teorema 3.8 *Toda relación de equivalencia definida en un conjunto A, determina una partición de A formada por las clases de equivalencia distintas.*

Demostración. En efecto, las clases de equivalencia **distintas** constituyen una partición del conjunto A, ya que, por 1, las clases no son vacías, y por 3, las clases de equivalencia distintas son disjuntas dos a dos. Además, como $x \in C_x$, la unión de las clases de equivalencia distintas es A. □

Conjunto cociente

Definición 3.9 *Se llama conjunto cociente al conjunto cuyos elementos son las clases de equivalencia distintas determinadas por una relación de equivalencia R definida en un conjunto A. Se nota A/R.*

Ejemplos

1. Si $A = \{a, b, c, d\}$ y $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a)\}$, entonces R es una relación de equivalencia cuyas clases son: $C_a = \{a, b\}$, $C_c = \{c\}$ y $C_d = \{d\}$. El conjunto cociente es el conjunto $A/R = \{C_a, C_c, C_d\}$.

2. Si A es un conjunto no vacío arbitrario y $R = \{(x, x) : x \in A\}$, entonces $C_x = \{x\}$, para todo $x \in A$, y por lo tanto $A/R = \{\{x\} : x \in A\}$.

Relación de equivalencia determinada por una partición

Vamos a ver ahora la recíproca del teorema anterior, es decir, que dada una partición de A se puede definir una relación de equivalencia de modo tal que las clases de equivalencia correspondientes coincidan con los subconjuntos de la partición dada.

Teorema 3.10 *Sea $\{A_i\}_{i\in I}$ una partición de un conjunto A. Sea R la relación definida en A por: $(x, y) \in R \Leftrightarrow$ existe $i \in I$ tal que $x \in A_i$ e $y \in A_i$. Entonces R es una relación de equivalencia y las clases de equivalencia correspondientes son los subconjuntos de la partición dada.*

Demostración. La relación definida R es claramente simétrica.

Que R es reflexiva es la condición 3 de la definición de partición, ya que si $x \in A$ existe un conjunto A_i de la partición tal $x \in A_i$.

Finalmente, probemos que R es transitiva: Si xRy e yRz, entonces existen conjuntos A_i y A_j de la partición tales que $x, y \in A_i$ e $y, z \in A_j$. En particular, $y \in A_i \cap A_j$, con lo que $A_i \cap A_j \neq \emptyset$. Luego por la condición 2 de la definición de partición, $A_i = A_j$. Luego se tiene que $x, z \in A_j$, de donde resulta xRz.

Por último, es claro que las clases de equivalencia determinadas por la relación R son los subconjuntos A_i de la partición. □

Congruencia módulo m

Un ejemplo muy importante de relación de equivalencia es la congruencia módulo m.

Definición 3.11 *Sea $\mathbb{Z}$ el conjunto de los números enteros y sea $m \in \mathbb{Z}$ fijo. Dos números enteros a y b se dicen congruentes módulo m, si y sólo si $a - b$ es un múltiplo de m. O sea,*

$$a \equiv b \pmod{m} \Leftrightarrow a - b = k \cdot m, \text{ con } k \in \mathbb{Z}.$$

Por ejemplo, $10 \equiv 2 \pmod 4$, $11 \equiv 25 \pmod 2$, $10 \equiv 13 \pmod 3$, $a \equiv b \pmod 0$ si y sólo si $a = b$, $a \equiv b \pmod 1$ para todo $a, b \in \mathbb{Z}$.

Teorema 3.12 *La relación de congruencia para un número entero fijo m, definida en el conjunto de los números enteros, es una relación de equivalencia.*

Demostración. En efecto, veamos que es reflexiva, simétrica y transitiva.

1. $a \equiv a \pmod m$, para todo $a \in \mathbb{Z}$, pues $a - a = 0 = 0 \cdot m$, y $0 \in \mathbb{Z}$.

2. Si $a \equiv b \pmod m$ entonces $b \equiv a \pmod m$.
   Si $a \equiv b \pmod m$ entonces $a - b = k \cdot m$. Multiplicando por -1 ambos miembros, se obtiene $b - a = -k \cdot m$; pero $k \in \mathbb{Z} \Rightarrow -k \in \mathbb{Z}$. Luego $b \equiv a \pmod m$.

3. Si $a \equiv b \pmod m$ y $b \equiv c \pmod m$ entonces $a \equiv c \pmod m$.
   Si $a \equiv b \pmod m$ entonces $a - b = k \cdot m$
   Si $b \equiv c \pmod m$ entonces $b - c = k' \cdot m$
   Sumando miembro a miembro se tiene: $a - c = (k + k') \cdot m$, esto es,
   $a - c = k'' \cdot m \Rightarrow a \equiv c \pmod m$.

□

Conviene observar que $a - b$ es un múltiplo de m si y sólo si $a - b$ es un múltiplo de $-m$, esto es, $a \equiv b \pmod m$ si y sólo si $a \equiv b \pmod{-m}$. En virtud de esto, convenimos en considerar en adelante sólamente la congruencia módulo m, con $m \geq 0$.

Como consecuencia del teorema anterior, la relación de congruencia módulo un entero fijo m particiona a $\mathbb{Z}$ en clases de equivalencia.

Por ejemplo, las clases de equivalencia determinadas por la congruencia módulo 3 son:
$\overline{0} = \{z \in \mathbb{Z} : z \equiv 0 \pmod 3\} = \{z \in \mathbb{Z} : z - 0 = k \cdot 3\} = \{z \in \mathbb{Z} : z = k \cdot 3 + 0\}$. Luego
$\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$ (múltiplos de 3).
$\overline{1} = \{z \in \mathbb{Z} : z \equiv 1 \pmod 3\} = \{z \in \mathbb{Z} : z - 1 = k \cdot 3\} = \{z \in \mathbb{Z} : z = k \cdot 3 + 1\}$. Luego
$\overline{1} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$ (múltiplos de 3, mas 1).
$\overline{2} = \{z \in \mathbb{Z} : z \equiv 2 \pmod 3\} = \{z \in \mathbb{Z} : z - 2 = k \cdot 3\} = \{z \in \mathbb{Z} : z = k \cdot 3 + 2\}$. Luego
$\overline{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$ (múltiplos de 3, mas 2).

Si calculamos la clase del 3, $\overline{3}$, veremos que coincide con la del 0. En general, si $m \neq 0$, la congruencia módulo m determina exactamente m clases de equivalencia; esto es una consecuencia del siguiente teorema:

Teorema 3.13 *Dos números enteros a y b son congruentes módulo m, con $m \neq 0$, si y sólo si dan el mismo resto al dividirlos por m.*

Demostración. Supongamos que $a \equiv b \pmod m$ y probemos que a y b dan el mismo resto al dividirlos por m.

Sean p y r el cociente y el resto, respectivamente, de dividir b por m. Entonces $b = p \cdot m + r$. Pero por hipótesis $a \equiv b \pmod m$, luego $a - b = k \cdot m$, esto es, $a = k \cdot m + b$. Remplazando b se tiene: $a = k \cdot m + p \cdot m + r = (k + p) \cdot m + r$, lo que significa que al dividir a por m el cociente es $k + p$ y el resto es r.

Recíprocamente, supongamos ahora que a y b dan el mismo resto al dividirlos por m. Probemos que $a \equiv b \pmod m$. Tenemos

$$\begin{array}{rcl} a & = & p \cdot m + r \\ b & = & p' \cdot m + r \\ \hline a - b & = & p \cdot m + r - p' \cdot m - r \\ a - b & = & (p - p') \cdot m \end{array}$$

Luego $a \equiv b \pmod m$. □

Los posibles restos al dividir un entero por m son 0, 1, 2, ..., $m - 1$, o sea, que mediante la congruencia módulo m se obtienen exactamente m clases de equivalencia, pues en una figuran todos los números que al dividirlos por m dan resto 0, en otra los que dan resto 1, ..., y en otra los que dan resto $m - 1$.

Como dijimos que el conjunto cociente es el conjunto de las clases de equivalencia, entonces el conjunto cociente de $\mathbb{Z}$ por esta relación de equivalencia tiene m elementos. Lo notamos

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Por ejemplo, si $m = 2$ entonces $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$.
Si $m = 4$, entonces $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.
Observación. Si $m = 1$, entonces existe única clase, la del 0, esto es, $\mathbb{Z}_1 = \{\overline{0}\}$.
Si $m = 0$, existen infinitas clases, pues cada entero forma una clase de equivalencia con un solo elemento.

3.3 Relaciones de orden

Definición 3.14 *Una relación binaria R definida en un conjunto A es de orden si es reflexiva, antisimétrica y transitiva.*

Ejemplos.

1. La relación menor o igual entre números reales.
2. La inclusión entre conjuntos.
3. Ya hemos visto que la relación "divide" en $\mathbb{N}$ es reflexiva, antisimétrica y transitiva, esto es, la relación "|" es una relación de orden en $\mathbb{N}$. Observar que la misma relación "|" definida sobre $\mathbb{Z}$ no es antisimétrica.

Conjuntos totalmente ordenados o cadenas

En lo que sigue, usaremos el signo "$\leq$" para designar una relación de orden arbitraria. Si $a \leq b$ leeremos "a precede a b".

Dada una relación de orden sobre A y elementos $a, b \in A$, puede ser que $a \not\leq b$ y $b \not\leq a$. Por ejemplo, si consideramos la relación "divide" en $\mathbb{N}$, entonces $3 \not| 4$ y $4 \not| 3$.

Se dice que a y b son *incomparables* si $a \not\leq b$ y $b \not\leq a$, y en este caso el orden es *parcial*.

En cambio, si para cualquiera que sean $a, b \in A$ se verifica que $a \leq b$ ó $b \leq a$, se dice que el conjunto A está *totalmente ordenado*. Por ejemplo el conjunto $\mathbb{N}$ con la relación "menor o igual" usual (el orden natural).

Veamos un ejemplo de un conjunto no totalmente ordenado. Sea $A = \{a, b\}$ y consideremos sobre el conjunto $\mathcal{P}(A)$ el orden dado por la relación de inclusión. $\mathcal{P}(A) = \{\{a\}, \{b\}, \{a, b\}, \emptyset\}$. Se tiene que $\{a\} \not\subseteq \{b\}$ y $\{b\} \not\subseteq \{a\}$.

Diagramas de Hasse

Los diagramas de Hasse sirven para visualizar gráficamente algunos conjuntos ordenados finitos.

Escribiremos $a < b$ para indicar que $a \leq b$ y $a \neq b$.

Definición 3.15 *Diremos que " b cubre a a" si $a < b$ y no existe c tal que $a < c$ y $c < b$.*

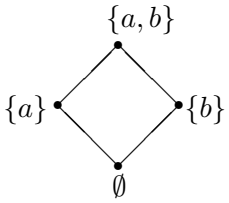
Construcción del diagrama.

(a) Cada elemento del conjunto se representa por un punto que se llama *afijo* de ese elemento.

(b) Si un elemento b cubre a a, el afijo de b se ubica a mayor altura que el de a y se unen con un segmento.

Ejemplos.

1. Sea $X = \{a, b\}$. Consideremos $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ ordenado por la relación de inclusión. Su diagrama de Hasse es:

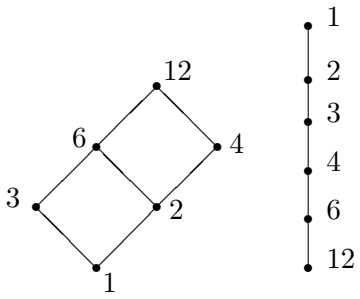


2. Sea X el conjunto de los divisores naturales de 12, ordenados por:

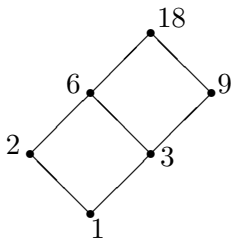
   (a) la relación "divide".

   (b) la relación "mayor o igual".

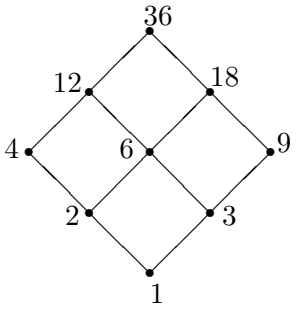
   Sus diagramas de Hasse son:



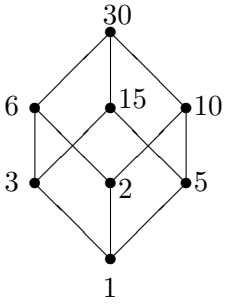
3. Sea B el conjunto de los divisores naturales de 18, $B = \{1, 2, 3, 6, 9, 18\}$, ordenado por la relación "divide". Su diagrama de Hasse es:

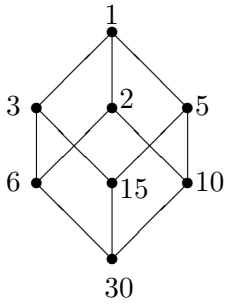


4. Sea C el conjunto de los divisores naturales de 36, $C = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, ordenado por la relación "divide". Su diagrama de Hasse es:



5. Sea D el conjunto de los divisores naturales de 30, $D = \{1, 2, 3, 5, 6, 10, 15, 30\}$, ordenado por la relación "divide" y por la relación "es múltiplo de". Sus diagramas de Hasse son:





Elementos distinguidos de un conjunto ordenado

Sea A un conjunto ordenado por la relación $\leq$.

(a) **Primer elemento.** Se dice que $x \in A$ es primer elemento de A si y sólo si $x \leq a$, para todo $a \in A$.

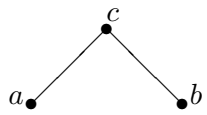
(b) **Último elemento.** Se dice que $u \in A$ es último elemento de A si y sólo si $a \leq u$, para todo $a \in A$.

(c) **Elementos minimales.** Se dice que $m \in A$ es un elemento minimal de A si y sólo si no existe ningún elemento que lo preceda propiamente esto es, si $x \in A$ es tal que $x \leq m$ entonces $x = m$.

(d) **Elementos maximales.** Se dice que $p \in A$ es un elemento maximal de A si y sólo si no existe ningún elemento que lo cubra, esto es, si $x \in A$ es tal que $p \leq x$ entonces $x = p$.

Ejemplos.

1. Sea $A = \{a, b, c\}$, $R = \{(a,a), (b,b), (c,c), (a,c), (b,c)\}$. Su diagrama de Hasse es:

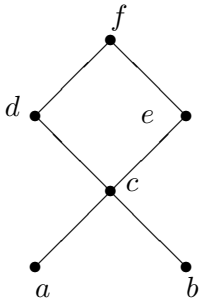


Primer elemento:	no tiene
Último elemento:	c
Elementos minimales:	a, b
Elementos maximales:	c

2. El conjunto $\mathbb{Z}$ ordenado por la relación $\leq$ habitual, no tiene ni primer ni último elemento.

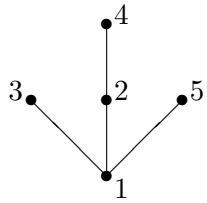
3. El conjunto $\mathbb{N}$ ordenado con el orden natural $\leq$ tiene primer elemento, el 1, no tiene último elemento, el 1 es también elemento minimal y no tiene elementos maximales.

4. Consideremos el conjunto ordenado que tiene el siguiente diagrama de Hasse:



Primer elemento:	no tiene
Último elemento:	f
Elementos minimales:	a, b
Elementos maximales:	f

5. El conjunto $A = \{1, 2, 3, 4, 5\}$ ordenado por la relación "divide".



Primer elemento:	1
Último elemento:	no tiene
Elementos minimales:	1
Elementos maximales:	$3, 4, 5$

De los ejemplos anteriores resulta que en un conjunto ordenado A, pueden no existir elementos maximales o minimales, y si existen, pueden no ser únicos.

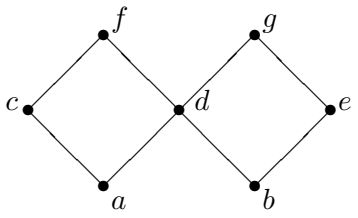
También puede suceder que no existan primer o último elemento, pero si existen, son únicos. En efecto, supongamos que existen dos primeros elementos x y x'. Entonces, por ser x primer elemento, debe ser $x \leq x'$. Pero por ser x' primer elemento, debe ser $x' \leq x$, de donde $x = x'$. Luego el primer elemento, si existe, es único. Un razonamiento análogo prueba que si existe último elemento, es único.

Definición 3.16 *Sea A un conjunto ordenado y notemos "$\leq$" la correspondiente relación de orden. Sea $X \subseteq A$. Diremos que:*

(a) *Un elemento $c \in A$ es cota inferior de X, si $c \leq x$ para todo $x \in X$.*

(b) *Un elemento $c \in A$ es cota superior de X si $x \leq c$ para todo $x \in X$.*

Ejemplo. Sea A el conjunto ordenado cuyo diagrama de Hasse es:



X	Cotas inferiores de X	Cotas superiores de X
$\{a, b\}$	No tiene	d, f, g
$\{f\}$	a, b, c, d, f	f
$\{d, e\}$	b	g
$\{c, g\}$	a	No tiene
$\{c, e\}$	No tiene	No tiene

Este ejemplo muestra que pueden existir o no cotas (inferiores o superiores); además, si existen, pueden no ser únicas. Si existen cotas (inferiores o superiores) de un conjunto X, éstas pueden pertenecer o no a X.

Definición 3.17 *Sea A un conjunto ordenado y $X \subseteq A$. Llamaremos ínfimo de X a la mayor (si existe) de las cotas inferiores de X. Llamaremos supremo de X a la menor (si existe) de las cotas superiores de X.*

Por ejemplo, si A es el conjunto ordenado del ejemplo anterior, entonces

Si $X = \{a, b\}$,	el ínfimo de X no existe,	el supremo de X es d
Si $X = \{f\}$,	el ínfimo de X es f,	el supremo de X es f
Si $X = \{d, e\}$,	el ínfimo de X es b,	el supremo de X es g
Si $X = \{c, g\}$,	el ínfimo de X es a,	el supremo de X no existe
Si $X = \{c, e\}$,	el ínfimo de X no existe,	el supremo de X no existe

Se observa, a partir de este ejemplo, que el ínfimo (supremo) de un conjunto X puede existir o no, y que, en caso de existir, puede pertenecer o no a X.

3.4 Ejercicios

1. Indicar, en cada caso, si la relación dada es reflexiva, simétrica, antisimétrica o transitiva.

   (a) $A = \{1, 2, 3\}$
   - i) $R = \{(1,1), (2,2), (3,3)\}$.
   - ii) $R = \{(1,2), (2,1), (1,3), (2,2)\}$.
   - iii) $R = A \times A$.
   - iv) $R = \{(1,1), (2,2), (1,3), (1,2), (2,3), (3,3)\}$.
   - v) $R = \emptyset$.

   (b) $A = \mathbb{Z}$, xRy si y sólo si $x - y$ es par.

   (c) $A = \mathbb{Z}^2$, $(a,b)R(c,d)$ si y sólo si $a \leq c$.

   (d) $A = \mathbb{Z}$, xRy si y sólo si $x \leq y$.

   (e) $A = \mathbb{N}$, xRy si y sólo si x divide a y.

   (f) $A = \mathbb{Z}$, xRy si y sólo si x divide a y.

   (g) $A = \mathbb{R}$, xRy si y sólo si $x^2 = y^2$.

2. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Graficar la relación

   $$R = \{(1,1), (1,3), (3,1), (3,3), (6,4), (4,6), (4,4), (6,6)\}$$

   dibujando 6 puntos en el plano que representen cada uno de los elementos de A y una flecha de a a b para cada $(a,b) \in R$. Viendo el gráfico, determinar si R es reflexiva, simétrica, antisimétrica o transitiva.

3. Sea R la relación definida sobre $\mathbb{Z}$ por nRn' si y sólo si $nn' > 0$. Probar que R es simétrica y transitiva pero no reflexiva.

4. Dar un ejemplo de una relación en $\mathbb{R}$ que

   (i) sea simétrica y antisimétrica.

   (ii) no sea ni simétrica ni antisimétrica.

   (iii) sea simétrica y transitiva pero no reflexiva.

   (iv) sea reflexiva y simétrica pero no transitiva.

   (v) sea de equivalencia y de orden.

5. El siguiente razonamiento parece probar que si una relación R es simétrica y transitiva, entonces R es reflexiva.
   Si aRb entonces bRa (propiedad simétrica).
   Pero aRb y bRa implican aRa (propiedad transitiva).
   Luego aRa, para todo a.
   ¿ Es correcto el razonamiento anterior ?

6. Indicar qué relaciones del ejercicio 1 son de equivalencia y cuáles son de orden. En el caso de las relaciones de equivalencia, hallar las clases de equivalencia y el conjunto cociente.

7. Averiguar si las siguientes relaciones son de equivalencia. Hallar las clases de equivalencia y el conjunto cociente, cuando corresponda.

(a) $A = \mathbb{Z}$, xRy si y sólo si $x + y$ es un número par.

(b) $A = \{1, 2, 3, 4\}$,

(i) $R = \{(1, 1), (2, 2), (1, 3), (3, 3), (2, 4), (4, 4), (4, 2), (3, 1)\}$.

(ii) $R = \{(1, 1), (2, 1), (3, 2), (2, 3)\}$.

(c) $A = \{x : x$ es estudiante de la UNS $\}$, xRy si y sólo si el apellido de x comienza con la misma letra que el apellido de y. (Suponer que para cada letra del abecedario, hay al menos un alumno cuyo apellido comienza con esa letra).

(d) $A = \mathbb{R} \times \mathbb{R}$, $(x, y)R(z, t)$ si y sólo si $x^2 + y^2 = z^2 + t^2$.

(e) $A = \mathbb{R} \times \mathbb{R}$, $(x, y)R(z, t)$ si y sólo si $x^2 = z^2$, $y^2 = t^2$.

8. Sea $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Determinar, en cada caso, si la familia de subconjuntos dados es una partición de X.

(a) $\{\{1, 3, 6\}, \{2, 8\}, \{5, 7, 9\}\}$.

(b) $\{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}, \{9\}\}$.

(c) $\{\{1, 2, 3, 4, 5, 6, 7, 8, 9\}\}$.

(d) $\{\{1, 5, 7\}, \{2, 4, 8, 9\}, \{3, 5, 6\}\}$.

(e) $\{\{2, 4, 5, 8\}, \{1, 9\}, \{3, 6, 7\}\}$.

9. Sea $A = \{a, b, c, d, e, f\}$. Dada la relación de equivalencia en A

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

hallar

(i) la clase de b.

(ii) la clase de c.

(iii) la clase de d.

(iv) la partición asociada a R.

10. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Hallar y graficar la relación de equivalencia en A asociada a la partición $\{\{1, 3\}, \{2, 6, 7\}, \{4, 8, 9, 10\}, \{5\}\}$.

11. Hallar todas las particiones del conjunto $A = \{1, 2, 3\}$. ¿ Cuántas relaciones de equivalencia pueden definirse en A ?

12. Calcular todas las posibles particiones de un conjunto con

(a) 3 elementos.

(b) 4 elementos.

13. Sea $A = \{1, 2, 3, 4, 5, 6\}$ y sea $\{\{1, 2, 3\}, \{4\}, \{5, 6\}\}$ una partición de A. Indicar la relación de equivalencia asociada a dicha partición.

14. Dar ejemplos de relaciones R sobre $A = \{1, 2, 3\}$ de modo que

(i) R sea simétrica y antisimétrica.

(ii) R no sea simétrica ni antisimétrica.

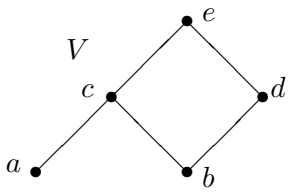
(iii) R sea reflexiva y no sea transitiva.

15. Sea A un conjunto y consideremos $\mathcal{P}(A)$ ordenado por la relación de inclusión. ¿Qué condiciones debe verificar A para que $\mathcal{P}(A)$ sea totalmente ordenado?

16. Completar con $<$, $>$ ó $\parallel$ (no comparables).

    (a) Sea $\mathbb{N}$ ordenado por la relación divide.
    (i) $2 \ldots 8$ (ii) $18 \ldots 24$ (iii) $9 \ldots 3$ (iv) $5 \ldots 15$.

    (b) Sea $V = \{a, b, c, d, e\}$ ordenado según el diagrama de la figura.



(i) $e \ldots b$ (ii) $c \ldots d$

(iii) $a \ldots e$ (iv) $d \ldots a$.

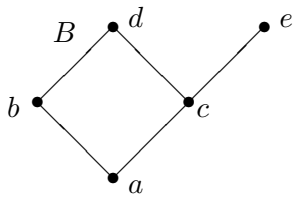
17. Sea $A = \mathbb{N}$. Probar que la relación xRy si y sólo si existe $z \in \mathbb{N} \cup \{0\}$ tal que $z + x = y$, es una relación de orden.

18. Dibujar el diagrama de Hasse correspondiente a cada uno de los siguientes conjuntos ordenados:

    (a) $A = \{2, 3, 4, 8, 9, 27, 45, 1215\}$, xRy si y sólo si $x|y$.
    (b) $A = \{1, 2, 3, 5, 7, 11\}$, xRy si y sólo si x es múltiplo de y.
    (c) $A = \{\{1\}, \{5\}, \{2, 3\}, \{1, 3\}, \{1, 3, 5\}, \emptyset\}$, XRY si y sólo si $X \supseteq Y$.
    (d) $\mathcal{P}(A)$, con la relación de inclusión, siendo:
        (i) $A = \emptyset$.
        (ii) A un conjunto con 2 elementos.
        (iii) A un conjunto con 3 elementos.

19. (a) Sea $A = \{1, 2, 3, 4\}$ y sea $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3), (1, 4), (2, 4)\}$ una relación de orden definida sobre A. Construir el diagrama de Hasse.

    (b) El diagrama de Hasse correspondiente al conjunto $B = \{a, b, c, d, e\}$ ordenado por la relación de orden R es el siguiente:



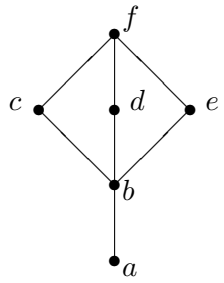
Definir la relación.

20. Para cada una de los conjuntos del ejercicio 18, hallar, si existen:

    (a) el primer elemento y el último elemento.
    (b) elementos maximales y elementos minimales.

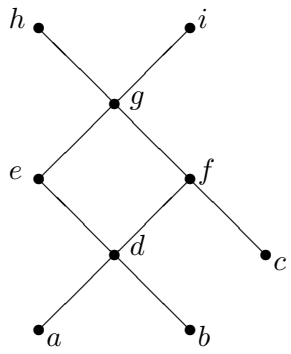
21. Indicar los elementos maximales y los elementos minimales de los conjuntos ordenados que se indican. Completar la tabla.

(a) A



X	Cotas inf.	Cotas sup.	Supremo	Ínfimo
$\{d, e\}$				
$\{b, f\}$				
$\{a, b, e\}$				
$\{c, d, f\}$				
$\{d, c\}$				
$\{a, c, e\}$				
$\{b\}$				

(b) A



X	Cotas inf.	Cotas sup.	Supremo	Ínfimo
$\{e, g, i\}$				
$\{c, d, f\}$				
$\{a, b, g\}$				
$\{d, e, h\}$				
$\{d, g\}$				
$\{c, e\}$				
$\{a, g\}$				

4 Funciones

Intuitivamente hablando, una función o aplicación de un conjunto A en un conjunto B es una correspondencia que permite asignar *a cada* elemento $a \in A$, un *único* elemento $b \in B$.

Formalizamos esta noción intuitiva mediante la siguiente definición:

Definición 4.1 *Dados dos conjuntos no vacíos A y B, una función o aplicación de A en B es una relación $f \subseteq A \times B$ tal que para todo $a \in A$, existe uno y sólo un elemento $b \in B$ tal que $(a, b) \in f$.*

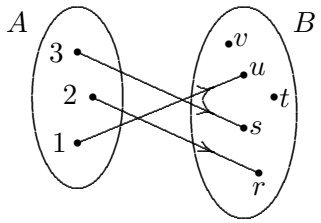
Por ejemplo, si $A = \{1, 2, 3\}$ y $B = \{r, s, t, u, v\}$, entonces la relación $f = \{(1, u), (2, r), (3, s)\}$ es una función.

Si f es una función de A en B, entonces escribiremos $b = f(a)$ para indicar que $(a, b) \in f$, y decimos que b es la *imagen* de a por f, o que b es el *valor* que toma f en a. Con esta notación escribiríamos, para el ejemplo anterior:

$$f(1) = u, \quad f(2) = r, \quad f(3) = s.$$

De la misma manera, para indicar que f es una aplicación de A en B, escribiremos preferentemente $f : A \to B$ ó $A \xrightarrow{f} B$.

Gráficos como el siguiente se usan frecuentemente para "visualizar" el comportamiento de las funciones.



Dada una función $f : A \to B$, el conjunto A se llama el *dominio* de f y B el *codominio*.

Nota. De la definición de función resulta que dadas dos funciones $f : A \to B$, $g : A \to B$, entonces $f = g$ si y sólo si $f(x) = g(x)$, para todo $x \in A$.

Imagen e imagen completa inversa

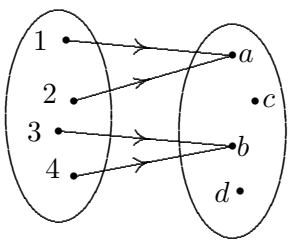
Para cada subconjunto $X \subseteq A$, se llama *imagen* de X por f al siguiente subconjunto de B: $f(X) = \{y \in B : \text{ existe } x \in X : y = f(x)\}$.

En particular, si $X = A$, la *imagen* de f (o rango de f) es $f(A) = Im(f) = \{y \in B : \text{ existe } x \in A : y = f(x)\}$.

En el ejemplo anterior, $Im(f) = \{r, s, u\}$.

Para cada subconjunto $Y \subseteq B$, se llama *imagen completa inversa* de Y por f al siguiente subconjunto de A: $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$.

Ejemplo. Sea f la función dada por el siguiente diagrama:



y consideremos $X_1 = \{2,4\}$, $X_2 = \{1,2,3\}$, $Y_1 = \{a,c\}$, $Y_2 = \{c,d\}$. Entonces

$$\begin{array}{rclcrcl} f(X_1) & = & \{a,b\} & & f(X_2) & = & \{a,b\} \\ f^{-1}(Y_1) & = & \{1,2\} & & f^{-1}(Y_2) & = & \emptyset \end{array}$$

4.1 Funciones inyectivas, epiyectivas y biyectivas

Definición 4.2 *Diremos que una función $f : A \to B$ es inyectiva, o que f es una función biunívoca, si elementos distintos en A tienen imágenes diferentes en B, esto es, si se verifica:*

$$x \neq x' \;\Rightarrow\; f(x) \neq f(x'),$$

o equivalentemente,

$$f(x) = f(x') \;\Rightarrow\; x = x'.$$

Ejemplos.

1. En la siguiente tabla figuran todas las funciones inyectivas de $A = \{a,b\}$ en $B = \{x,y,z\}$:

	f_1	f_2	f_3	f_4	f_5	f_6
a	x	x	y	y	z	z
b	y	z	x	z	x	y

2. La función lineal $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = mx + b$, donde m y b son números reales fijos, $m \neq 0$, es inyectiva. En efecto, si suponemos que $f(x) = f(x')$, entonces $mx + b = mx' + b$, de donde, $mx = mx'$, y como $m \neq 0$, se tiene $x = x'$.

3. La función $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$ no es inyectiva, ya que, por ejemplo, $f(-1) = f(1)$ y $1 \neq -1$.

Definición 4.3 *Diremos que una función $f : A \to B$ es epiyectiva, suryectiva, sobreyectiva, o que f es de A sobre B, si $Imf = B$, esto es, cualquiera que sea $y \in B$, existe un $x \in A$ tal que $f(x) = y$.*

Ejemplos.

1. Sea $A = \{1,2,3\}$ y $B = \{a,b\}$. En la siguiente tabla se exhiben todas las funciones epiyectivas de A en B:

	f_1	f_2	f_3	f_4	f_5	f_6
1	a	b	b	a	a	b
2	b	a	b	a	b	a
3	b	b	a	b	a	a

2. La función lineal $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = mx + b$, donde m y b son números reales fijos, $m \neq 0$, es epiyectiva. En efecto, sea $y \in \mathbb{R}$. Debemos hallar un $x \in \mathbb{R}$ tal que $f(x) = y$, esto es, tal que $mx + b = y$. El número x que se busca se obtiene resolviendo la ecuación anterior. Ese número es $x = \dfrac{1}{m}(y-b)$. Para este elemento se tiene: $f(x) = f(\dfrac{1}{m}(y-b)) = m \cdot \dfrac{1}{m}(y-b) + b = y$.

3. La función $f : \mathbb{N} \to \mathbb{N}$, definida por $f(x) = mx + b$, $m \neq 0$, no es suryectiva. En efecto, sea $y \in \mathbb{N}$. Debemos hallar un $x \in \mathbb{N}$ tal que $f(x) = y$, esto es, tal que $mx + b = y$. Pero del ejemplo anterior resulta que un tal x debe tener la forma: $x = \frac{1}{m}(y - b)$, que, en general, no es un número natural.

Definición 4.4 *Diremos que una aplicación $f : A \to B$ es biyectiva o que f es una correspondencia biunívoca de A sobre B si f es inyectiva y epiyectiva.*

Ejemplos.

1. Sean $A = \{1, 2, 3\}$ y $B = \{x, y, z\}$. Todas las funciones biyectivas de A en B están indicadas en la siguiente tabla:

	f_1	f_2	f_3	f_4	f_5	f_6
1	x	x	y	y	z	z
2	y	z	x	z	x	y
3	z	y	z	x	y	x

2. La aplicación $f : \mathbb{R} \to \mathbb{R}$, $f(x) = mx + b$, $m \neq 0$, es biyectiva.

3. La función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n + 1$ es inyectiva pero no epiyectiva.
En cambio $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(z) = z + 1$ es inyectiva y epiyectiva.

4. Sea A un conjunto cualquiera no vacío. Sea $I_A : A \to A$ la función definida por $I_A(x) = x$, para todo $x \in A$. Entonces I_A es biyectiva. I_A se llama la función *identidad* de A.

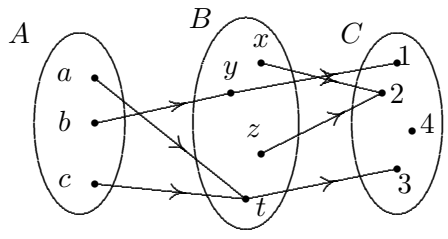
4.2 Composición de funciones

Definición 4.5 *Sean A, B, C conjuntos y sean $f : A \to B$ y $g : B \to C$ dos funciones. Se llama composición de f y g a la función, indicada con $g \circ f : A \to C$, definida por:*

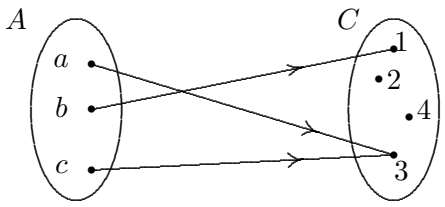
$$(g \circ f)(x) = g(f(x)), \text{ para todo } x \in A.$$

Ejemplos.

1. Sean $f : A \to B$ y $g : B \to C$ las siguientes funciones:



Entonces la función $g \circ f$ es:



2. Sea $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = 5x$ y $g : \mathbb{Z} \to \mathbb{Z}$ definida por $g(x) = x + 1$. Entonces $(g \circ f)(x) = g(f(x)) = g(5x) = 5x + 1$, y $(f \circ g)(x) = f(g(x)) = f(x + 1) = 5(x + 1)$.

3. Sea $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(x) = 4 - x$ y $g : \mathbb{Z} \to \mathbb{Q}$ definida por $g(x) = \dfrac{x}{2}$. Entonces $(g \circ f)(x) = g(f(x)) = g(4 - x) = \dfrac{4 - x}{2}$.
No es posible efectuar la composición $f \circ g$.

Proposición 4.6 *Sean A, B, C, D conjuntos y $f : A \to B$, $g : B \to C$, $h : C \to D$. Entonces vale la ley asociativa siguiente:*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Demostración. Debemos probar que $[h \circ (g \circ f)](x) = [(h \circ g) \circ f](x)$, para todo $x \in A$.
De la definición de composición se tiene:
$[h \circ (g \circ f)](x) = h[(g \circ f)(x)] = h[g(f(x))] = (h \circ g)(f(x)) = [(h \circ g) \circ f](x)$ □

Proposición 4.7 *Sea $f : A \to B$ una función. Entonces f es biyectiva si y sólo si existe una función $g : B \to A$ tal que $g \circ f = I_A$ y $f \circ g = I_B$.*

Demostración. Supongamos que $f : A \to B$ es biyectiva. En particular, f es suryectiva. Luego, si $y \in B$, existe $x \in A$ tal que $f(x) = y$. Además, por ser f inyectiva, ese x es único. Sea $g : B \to A$ la función que asigna a cada $y \in B$ el único $x \in A$ tal que $f(x) = y$, esto es, $g(y) = x$ si $f(x) = y$.

Resulta de la definición de g que $(g \circ f)(x) = g(f(x)) = x$, para todo $x \in A$ y $(f \circ g)(y) = f(g(y)) = y$, para todo $y \in B$. Luego

$$g \circ f = I_A \text{ y } f \circ g = I_B.$$

Supongamos ahora que $f : A \to B$ y existe una función $g : B \to A$ que satisface $g \circ f = I_A$ y $f \circ g = I_B$. Probemos que f es biyectiva.

(a) f es inyectiva.
Sean $x, x' \in A$ tales que $f(x) = f(x')$. Entonces
$x = I_A(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = I_A(x') = x'$.

(b) f es suryectiva.
Sea $y \in B$. Entonces $y = I_B(y) = (f \circ g)(y) = f(g(y))$.

La demostración del teorema está ahora completa. □

Observación. La aplicación g de la proposición anterior es biyectiva.

Definición 4.8 *Dada una función $f : A \to B$, se llama inversa de f a toda función $g : B \to A$ con las propiedades siguientes: $g \circ f = I_A$ y $f \circ g = I_B$.*

Según el teorema anterior, una función posee una inversa si y sólo si es biyectiva.

Proposición 4.9 *Si $f : A \to B$ posee una inversa, ésta es única.*

Demostración. Sean $g : B \to A$ y $g' : B \to A$ inversas de f. Entonces, como $f \circ g' = I_B$, se tiene $g = g \circ I_B = g \circ (f \circ g') = (g \circ f) \circ g' = I_A \circ g' = g'$. □

Notaremos a la función inversa de la función biyectiva $f : A \to B$, con $f^{-1} : B \to A$.

Ejemplos.

1. Sea $A = \{x, y, z, t\}$ y $B = \{1, 2, 3, 4\}$. Sea f la función definida por: $f(x) = 3$, $f(y) = 2$, $f(z) = 4$, $f(t) = 1$. Entonces f es biyectiva, y su función inversa es la función $f^{-1} : B \to A$ definida por: $f^{-1}(1) = t$, $f^{-1}(2) = y$, $f^{-1}(3) = x$, $f^{-1}(4) = z$.

2. Sea $f : \mathbb{R} \to \mathbb{R}$ la función lineal $f(x) = 3x - 1$. Llamemos y al elemento al cual va a parar x, es decir $y = 3x - 1$. Como f lleva x a y, la inversa debe aplicar y en x. Pero de $y = 3x - 1$ se deduce $x = \dfrac{y+1}{3}$, es decir, la inversa debe llevar y a $\dfrac{y+1}{3}$. Es decir, la inversa será la función $g : \mathbb{R} \to \mathbb{R}$ dada por
$$g(y) = \frac{y+1}{3},$$
o, lo que es lo mismo,
$$g(x) = \frac{x+1}{3}.$$
También escribimos, $f^{-1} : \mathbb{R} \to \mathbb{R}$, $f^{-1}(x) = \dfrac{x+1}{3}$.

Proposición 4.10 *Sean las funciones $f : A \to B$ y $g : B \to C$.*

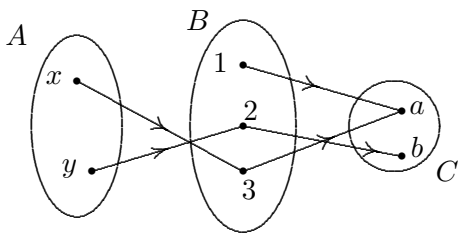
Si f y g son inyectivas	*entonces*	*$g \circ f$ es inyectiva.*
Si f y g son epiyectivas	*entonces*	*$g \circ f$ es epiyectiva.*
Si f y g son biyectivas	*entonces*	*$g \circ f$ es biyectiva.*

Demostración. Ejercicio. □

Proposición 4.11 *Si $f : A \to B$ y $g : B \to C$ son funciones biyectivas, entonces $f^{-1} \circ g^{-1} : C \to A$ es la inversa de $g \circ f$. (Es decir, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$).*

Demostración. $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g \circ f) = f^{-1} \circ (I_B \circ f) = f^{-1} \circ f = I_A$.
Análogamente, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = I_C$. □

Observación. Aunque la composición $g \circ f$ sea biyectiva, no necesariamente f y g lo son. Por ejemplo, en el diagrama siguiente



$g \circ f$ es biyectiva, pero ni f ni g lo son.

Sin embargo, valen las siguientes propiedades, cuya demostración se deja como ejercicio:

1. Si $g \circ f$ es epiyectiva, entonces g es epiyectiva.
2. Si $g \circ f$ es inyectiva, entonces f es inyectiva.

4.3 Relación de equivalencia asociada a una función

Una de las formas más frecuentes de definir una relación de equivalencia en un conjunto A que sea el dominio de una cierta función f, es considerar como equivalentes los puntos de A en los que f toma el mismo valor.

En efecto, sea dada una función $f : A \to B$. Si definimos $x \sim y \Leftrightarrow f(x) = f(y)$, para $x, y \in A$, entonces $\sim$ es una relación de equivalencia. La verificación es sencilla y se deja como ejercicio.

Así pues, toda función determina una relación de equivalencia en su dominio, de la que diremos que es *asociada* a la función.

Ejemplos.

1. Sea $m \geq 1$ un entero fijo y sea $r_m : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ la función que a cada $x \in \mathbb{Z}$ le asocia el resto r_m de dividir x por m.
   Entonces la relación de equivalencia $\sim$ asociada a la función r_m, es decir, la relación $x \sim y \Leftrightarrow r_m(x) = r_m(y)$, es la congruencia módulo m.

2. Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$.
   La relación de equivalencia asociada a f, es decir, la relación $x \sim y \Leftrightarrow x^2 = y^2$, es la que, si $x \neq 0$, $C_x = \{x, -x\}$, y $C_0 = \{0\}$.

Cabe ahora plantearse la siguiente pregunta: dado un conjunto A y una relación de equivalencia definida en A, ¿es posible encontrar una función f cuyo dominio sea A y tal que la relación de equivalencia asociada a f coincida con la dada? La noción de conjunto cociente, ya vista, y de *aplicación natural*, que definiremos a continuación, muestran que la respuesta es afirmativa.

Consideremos un conjunto A, sobre el cual está definida una relación de equivalencia R, y consideremos el conjunto cociente A/R. Indiquemos con $\overline{x}$ la clase de equivalencia que contiene al elemento $x \in A$. Cada $x \in A$ pertenece a una, y solamente una clase de equivalencia $\overline{x}$. Entonces la función $\pi : A \to A/R$, definida por $\pi(x) = \overline{x}$, para todo $x \in A$, está bien definida y se llama *aplicación natural* de A en A/R.

Ejemplo. Si R es la congruencia módulo 3 en $\mathbb{Z}$, tenemos la aplicación natural $\pi : \mathbb{Z} \to \mathbb{Z}_3$, $\pi(x) = \overline{x}$. Así, $\pi(0) = \overline{0}$, $\pi(4) = \overline{1}$, $\pi(2) = \overline{2}$, $\pi(8) = \overline{2}$, etc.

Proposición 4.12 *Sea A un conjunto y sea R una relación de equivalencia definida sobre A. Entonces la aplicación natural $\pi : A \to A/R$ es una función epiyectiva cuya relación de equivalencia asociada es R.*

Demostración. Probemos primero que π es epiyectiva. En efecto, si $\overline{x} \in A/R$, entonces tomando $x \in A$ es $\pi(x) = \overline{x}$.

Además, si notamos $\sim$ la relación de equivalencia asociada a π, entonces $x \sim y \Leftrightarrow \pi(x) = \pi(y) \Leftrightarrow \overline{x} = \overline{y} \Leftrightarrow xRy$, lo que prueba que la relación de equivalencia asociada a π coincide con la relación dada R. $\square$

4.4 Ejercicios

1. Sean $A = \{1, 2, 3, 4\}$ y $B = \{u, v, w, x, z\}$. Analizar si las siguientes relaciones son funciones de A en B. En caso afirmativo, hallar la imagen correspondiente.

   (a) $R = \{(1, u), (2, v), (1, x), (3, u), (4, u)\}$.

   (b) $R = \{(1, v), (3, u), (4, x)\}$.

   (c) $R = \{(1, w), (2, x), (3, u), (4, x)\}$.

   (d) $R = \{(1, v), (2, v), (3, v), (4, v)\}$.

   (e) $R = \{(1, z), (2, v), (3, w), (4, x)\}$.

2. Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2 - 3x + 2$. Hallar: $f(\sqrt[3]{2})$, $f(0)$, $f(x^2)$, $f(2x)$, $f(x+3)$, $f(-3)$, $f(x) + 3$, $f^{-1}(\{0\})$, $f^{-1}(\{-2\})$.

3. Dadas las siguientes funciones, hallar sus imágenes y averiguar si son inyectivas, epiyectivas o biyectivas.

   (a) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 3x + 1$.

   (b) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 3x + 1$.

   (c) $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) = 3x + 1$.

   (d) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 1$.

   (e) $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$, $f(x) = x^2$.

   (f) $f : \mathbb{R} \to \mathbb{R}^+$, $f(x) = x^2$, siendo $\mathbb{R}^+ = \{x : x \in \mathbb{R},\ x \geq 0\}$.

   (g) $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = x^2$.

   (h) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$.

   (i) $f : \mathbb{R}^* \to \mathbb{R}^*$, $f(x) = \dfrac{1}{x}$, siendo $\mathbb{R}^* = \{x : x \in \mathbb{R},\ x \neq 0\}$.

4. **Optativo.** Sea $f : A \to B$ una función, $X, X_1, X_2 \subseteq A$, $Y, Y_1, Y_2 \subseteq B$. Probar que:

   (a) $X_1 \subseteq X_2 \Rightarrow f(X_1) \subseteq f(X_2)$; $Y_1 \subseteq Y_2 \Rightarrow f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$.

   (b) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$; $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

   (c) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$; $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

   (d) $f(X_1 \cap X_2) = f(X_1) \cap f(X_2) \Leftrightarrow f$ es inyectiva.

   (e) $f^{-1}(Y') = [f^{-1}(Y)]'$.

   (f) $f(X') = [f(X)]' \Leftrightarrow f$ es biyectiva.

   (g) $f(X) = \emptyset \Leftrightarrow X = \emptyset$; $f^{-1}(Y) = \emptyset \Leftrightarrow Y \cap f(X) = \emptyset$.

   (h) $X \subseteq f^{-1}(f(X))$.

   (i) $X = f^{-1}(f(X)) \Leftrightarrow f$ es inyectiva.

   (j) $f(f^{-1}(Y)) \subseteq Y$.

   (k) $f(f^{-1}(Y)) = Y \Leftrightarrow f$ es suryectiva.

5. Sean $f : \mathbb{Z} \to \mathbb{Z}$ y $g : \mathbb{Z} \to \mathbb{Z}$ definidas por $f(x) = x + 1$ y $g(x) = 2x$. Probar que $f \circ g \neq g \circ f$.

6. Probar que la función $f : \mathbb{N} \to \mathbb{Z}$ definida por

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{si } n \text{ es par} \\ -\dfrac{n-1}{2} & \text{si } n \text{ es impar} \end{cases}$$

es biyectiva.

7. (a) Dadas
$$\begin{aligned} f : \mathbb{N} \to \mathbb{Q} \quad & \text{definida por} \quad f(x) = \frac{x+1}{x+2}, \\ g : \mathbb{Q} \to \mathbb{R} \quad & \text{definida por} \quad g(x) = x + \sqrt{2}, \\ h : \mathbb{R} \to \mathbb{R} \quad & \text{definida por} \quad h(x) = (x+1)^2, \\ k : \mathbb{R} \to \mathbb{R} \quad & \text{definida por} \quad k(x) = e^x, \\ t : \mathbb{N} \cup \{0\} \to \mathbb{R} \quad & \text{definida por} \quad t(x) = \frac{x+1}{x+2}, \end{aligned}$$
hallar $g \circ f$, $k \circ h$, $h \circ k$, $h \circ g$ y $k \circ t$. Calcular $(g \circ f)(1)$, $(k \circ h)(-1)$, $(h \circ k)(1)$, $(h \circ g)(2)$ y $(k \circ t)(0)$.

(b) ¿Se puede hacer $g \circ h$, $h \circ f$, $f \circ h$ y $f \circ g$?

8. Hallar la función inversa de las funciones que corresponda del ejercicio 3.

9. Para cada par de conjuntos A y B, y funciones $f : A \to B$, considerar la relación de equivalencia asociada a f y hallar las clases de equivalencia.

(a) $A = \{-3, -1, 0, 1, 3, 5, \sqrt{2}\}$, $B = \mathbb{Z}$, $f(x) = x^2 + 1$.

(b) $A = B = \mathbb{Z}$, $f(x) = 7x + 4$.

(c) $A = B = \mathbb{Z}$, $f(x) = -x^2 + 2$.

(d) $A = \mathbb{R}^2$, $B = \mathbb{R}$, $f((x, y)) = 2x + 3$.

(e) $A = B = \mathbb{R}^2$, $f((x, y)) = (-x, 2y)$.

5 Números reales

Los números naturales $1, 2, 3, \ldots$ aparecen ante la necesidad de contar los objetos de conjuntos finitos. Pero se necesita también medir longitudes, áreas, volúmenes, cantidad de energía, etc. Ya en la antigüedad los egipcios y los babilonios concibieron, alrededor del año 2000 A.C., una aritmética basada en los números racionales positivos. Es en tiempos de Pitágoras, alrededor del año 500 A.C., que los griegos descubrieron que existían segmentos imposibles de medir con los números racionales, es decir, que los números racionales no son suficientes para asignar a cada segmento una medida (racional), con lo que surge la necesidad de adoptar números irracionales, como $\sqrt{2}$.

Los números negativos fueron considerados como absurdos durante mucho tiempo, y sólo se manejaron libremente a partir del siglo XVII. Recién en el siglo XIX, Cantor, Dedekind y Weierstrass desarrollaron teorías rigurosas del número real. Cantor construyó los irracionales como sucesiones de racionales, Weierstrass los construyó como clases de racionales y Dedekind como cortaduras.

En todos los casos se parte de los números naturales, se define a partir de ellos el conjunto de los números enteros y, a partir de éstos, el conjunto de los números racionales. Finalmente, se definen los números reales a partir de los números racionales.

Una construcción de este tipo escapa a los alcances de un curso de elementos de álgebra. En su lugar, nosotros comenzaremos definiendo el conjunto de los números reales $\mathbb{R}$ por medio de las propiedades que sus elementos deben verificar. Es decir, vamos a enunciar como axiomas un conjunto de propiedades a partir de las cuales será posible probar cualquier otra propiedad de $\mathbb{R}$. Los otros conjuntos numéricos se definirán como subconjuntos particulares de $\mathbb{R}$.

5.1 El cuerpo ordenado de los números reales

El cuerpo ordenado de los números reales

Llamaremos *cuerpo ordenado real* a un sistema $(\mathbb{R}, +, \cdot, <)$ formado por:

(1) Un conjunto $\mathbb{R}$, cuyos elementos llamaremos *números reales*,

(2) Una operación binaria $+$, llamada *suma*, definida sobre $\mathbb{R}$, $a + b$ se lee "a más b",

(3) Una operación binaria $\cdot$, llamada *producto*, definida sobre $\mathbb{R}$, $a \cdot b$ se lee "a por b",

(4) Una relación binaria $<$, definida sobre $\mathbb{R}$, $a < b$ se lee "a menor que b",

de modo tal que, para todo $a, b, c \in \mathbb{R}$ se verifiquen las siguientes propiedades:

(S_1) $a + (b + c) = (a + b) + c$.

(S_2) $a + b = b + a$.

(S_3) Existe $0 \in \mathbb{R}$, llamado *cero*, tal que $0 + a = a$.

(S_4) Para cada $a \in \mathbb{R}$, existe $b \in \mathbb{R}$ llamado el *simétrico* de a, tal que $a + b = 0$.

(M_1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(M_2) $a \cdot b = b \cdot a$.

(M_3) Existe $1 \in \mathbb{R}$, llamado *uno*, $1 \neq 0$ que verifica $1 \cdot a = a$.

(M_4) Para cada $a \in \mathbb{R}$, $a \neq 0$, existe $c \in \mathbb{R}$, llamado el *inverso* de a tal que $a \cdot c = 1$.

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

(E_1) Para todo $a, b \in \mathbb{R}$ vale una y sólo una de las tres condiciones siguientes:

$$(i)\ a = b \qquad (ii)\ a < b \qquad (iii)\ b < a$$

(E_2) $a < b$ y $b < c \Rightarrow a < c$.

(E_3) $a < b \Rightarrow a + c < b + c$.

(E_4) $a < b$ y $0 < c \Rightarrow a \cdot c < b \cdot c$.

Para definir el cuerpo ordenado de los números reales resta enunciar el llamado Axioma de Completitud, lo que no haremos en este momento. Este Axioma, que no es necesario para probar las propiedades que enunciaremos más abajo, será objeto de estudio en el próximo parágrafo.

Para abreviar, designaremos al cuerpo ordenado real simplemente por $\mathbb{R}$.

Observación: Puede probarse que los elementos 0 y 1 denominados, respectivamente, *neutro aditivo* y *neutro multiplicativo*, son únicos. De la misma manera, son únicos el simétrico de cada elemento y el inverso de cada elemento distinto de cero.

Notaciones útiles

(1) Representaremos con $-a$ al simétrico de a. Entonces $-a$ es el único elemento de $\mathbb{R}$ que verifica $a + (-a) = 0$.

(2) Representaremos con a^{-1} al inverso de a. Entonces a^{-1} es el único elemento de $\mathbb{R}$ que verifica $a \cdot a^{-1} = 1$.

(3) Escribiremos $a - b$ para representar al elemento $a + (-b)$. Entonces, por definición, $a - b = a + (-b)$.

(4) Escribiremos $\frac{a}{b}$ para representar al elemento $a \cdot b^{-1}$. Entonces, por definición, $\frac{a}{b} = a \cdot b^{-1}$. El número real $\frac{a}{b}$ se llama el *cociente* de a por b. Como caso particular $a^{-1} = \frac{1}{a}$.

(5) Escribiremos $a \leq b$ y se lee "a es menor o igual que b", para indicar que vale alguna de las siguientes propiedades: $a = b$ ó $a < b$.

(6) Escribiremos $a > b$ para indicar que se verifica $b < a$ y se lee "a es mayor que b".

(7) Escribiremos $a \geq b$, y se lee "a es mayor o igual que b", para indicar que se verifica $b \leq a$. La relación $\leq$ es muy importante y está caracterizada por las siguientes propiedades:

(O_1) $a \leq a$.

(O_2) $a \leq b$ y $b \leq a \Rightarrow a = b$.

(O_3) $a \leq b$ y $b \leq c \Rightarrow a \leq c$.

(O_4) Dados $a, b \in \mathbb{R}$ entonces, $a \leq b$ ó $b \leq a$.

(8) Sea $a \in \mathbb{R}$, diremos que a es *positivo* si $a > 0$ y que a es *negativo* si $a < 0$.

(9) Escribiremos $a < b < c$ para indicar que $a < b$ y $b < c$. Análogamente escribiremos $a \leq b \leq c$ para indicar que $a \leq b$ y $b \leq c$.

(10) Teniendo en cuenta las propiedades de la suma y el producto escribiremos $a + b + c$ y $a \cdot b \cdot c$ en lugar de $a + (b + c)$ y $a \cdot (b \cdot c)$, respectivamente.

(11) Para simplificar, cuando no haya lugar a dudas, escribiremos $a\,b$ en lugar de $a \cdot b$.

Otras propiedades

De las propiedades anteriores se deducen las siguientes, algunas de cuyas demostraciones se incluyen, dejando las otras como ejercicio. Debe ponerse especial cuidado en no usar ninguna propiedad que no sea uno de los axiomas o que no haya sido probada previamente. Por un momento puede ser conveniente ignorar las propiedades que uno ya conoce de los números reales.

(P_1) $-(-a) = a$.

(P_2) $a + b = a + c \;\Rightarrow\; b = c$.

(P_3) $a\,b = a\,c \;,\; a \neq 0 \;\Rightarrow\; b = c$.

(P_4) $a \cdot 0 = 0$.
$a{\cdot}0 \overset{S_3}{=} a{\cdot}(0{+}0) \overset{D}{=} a{\cdot}0{+}a{\cdot}0,\ (1)\ ; a{\cdot}0 \overset{S_3}{=} a{\cdot}0{+}0,\ (2)$; de (1) y (2), $a{\cdot}0{+}a{\cdot}0 = a{\cdot}0{+}0 \overset{P_2}{\Rightarrow} a{\cdot}0 = 0$.

(P_5) $a\,b = 0 \;\Rightarrow\; a = 0$ ó $b = 0$.
Supongamos que $a \neq 0$. Entonces, por M_4, $a^{-1}(ab) = a^{-1}0$, esto es, $(a^{-1}a)b = 0$. Luego $1 \cdot b = b = 0$.

(P_6) $a\,(-b) = (-a)\,b = -(a\,b)$.
Probemos que $a(-b) = -(ab)$, es decir, que el simétrico de ab es $a(-b)$. Para esto basta probar que $ab + a(-b) = 0$. Y en efecto, $ab + a(-b) \overset{D}{=} a(b + (-b)) = 0$.
En forma análoga se prueba que $(-a)b = -(ab)$.

(P_7) $(-a)\,(-b) = a\,b$.
Aplicar P_6 dos veces.

(P_8) $(a^{-1})^{-1} = a\,,\ a \neq 0$.

(P_9) $(a\,b)^{-1} = a^{-1}\,b^{-1}\,,\ a \neq 0,\ b \neq 0$.

(P_{10}) $\dfrac{a}{b} = \dfrac{c}{d} \;\Leftrightarrow\; a\,d = b\,c,\ b \neq 0,\ d \neq 0$.

(P_{11}) $\dfrac{a}{b} = \dfrac{a\,c}{b\,c},\ c \neq 0\,,\ b \neq 0$.

(P_{12}) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a\,d + b\,c}{b\,d}\,,\ b \neq 0,\ d \neq 0$.
$\dfrac{a}{b} + \dfrac{c}{d} = ab^{-1} + cd^{-1} = add^{-1}b^{-1} + cbb^{-1}d^{-1} = adb^{-1}d^{-1} + cbb^{-1}d^{-1} = ad(bd)^{-1} + cb(bd)^{-1} = (ad + cb)(bd)^{-1} = \dfrac{a\,d + b\,c}{b\,d}$.

(P_{13}) $\dfrac{a}{b}\,\dfrac{c}{d} = \dfrac{a\,c}{b\,d}\,,\ b \neq 0,\ d \neq 0$.

(P_{14}) $\dfrac{-a}{b} = \dfrac{a}{-b} = -\dfrac{a}{b}\,,\ b \neq 0.$
Para probar que $\dfrac{-a}{b} = -\dfrac{a}{b}$ se debe probar que el simétrico de $\dfrac{a}{b}$ es $\dfrac{-a}{b}$. Es similar a P_6.

(P_{15}) $\dfrac{a}{b} \neq 0,\ b \neq 0 \ \Rightarrow\ \left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}\,.$

(P_{16}) $a < b$ y $c < d \ \Rightarrow\ a + c < b + d\,.$
De $a < b \overset{E_3}{\Rightarrow}\ a + c < b + c,$ y de $c < d \overset{E_3}{\Rightarrow}\ c + b < d + b.$ Luego, por E_2, $a + c < b + d.$

(P_{17}) $a + c < b + c \ \Rightarrow\ a < b\,.$
Sumar $-c$ a ambos miembros.

(P_{18}) $0 < a < b$ y $0 < c < d \ \Rightarrow\ a\,c < b\,d\,.$
Aplicar E_4.

(P_{19}) $a < b \ \Leftrightarrow\ -b < -a\,.$
Sumar $-b$ a ambos miembros, y luego $-a$.

(P_{20}) $0 < a \ \Leftrightarrow\ -a < 0\,.$
Es un caso particular de P_{19}.

(P_{21}) $a \neq 0 \ \Rightarrow\ a^2 > 0$ (El cuadrado de cualquier número no nulo es positivo).
Si $a > 0$, entonces $a \cdot a > a \cdot 0$, esto es $a^2 > 0$.
Si $a < 0$, entonces $-a > 0$, y por lo anterior, $(-a)(-a) > 0$, es decir, $a^2 > 0$.

(P_{22}) $0 < 1\,.$
Se tiene que $1 = 1^2$, luego $1 > 0$.

(P_{23}) $a < b,\ c < 0 \ \Rightarrow\ a\,c > b\,c.$
(Esta propiedad dice que si una desigualdad se multiplica miembro a miembro por un número negativo, se invierte el sentido de la desigualdad. Observar que el axioma E_4 afirma que si una desigualdad se multiplica miembro a miembro por un número positivo, no cambia el sentido de la misma).
Si $c < 0,\ -c > 0;$ de $a < b \overset{E_4}{\Rightarrow}\ a(-c) < b(-c)$, esto es, $-ac < -bc$, es decir, $ac > bc.$

(P_{24}) $a < 0 \ \Leftrightarrow\ \dfrac{1}{a} < 0\,.$
Si fuese $a^{-1} > 0$ entonces $aa^{-1} < 0$, de donde $1 < 0$, absurdo.

(P_{25}) $a > 0 \ \Leftrightarrow\ \dfrac{1}{a} > 0\,.$

(P_{26}) (1) $a\,b > 0 \ \Leftrightarrow\ a > 0$ y $b > 0$ ó $a < 0$ y $b < 0.$
(2) $a\,b < 0 \ \Leftrightarrow\ a > 0$ y $b < 0$ ó $a < 0$ y $b > 0.$
(3) $\dfrac{a}{b} > 0 \ \Leftrightarrow\ a > 0$ y $b > 0$ ó $a < 0$ y $b < 0.$
(4) $\dfrac{a}{b} < 0 \ \Leftrightarrow\ a > 0$ y $b < 0$ ó $a < 0$ y $b > 0.$

(P_{27}) $0 < a < b \ \Rightarrow\ 0 < \dfrac{1}{b} < \dfrac{1}{a}\,.$
Multiplicar por $a^{-1}b^{-1}$.

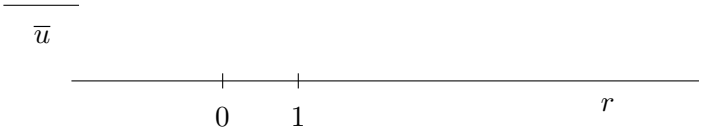
$(P_{28})\ a < b < 0 \Rightarrow \dfrac{1}{b} < \dfrac{1}{a} < 0\,.$

$(P_{29})\ 0 < a < b \Rightarrow a^2 < b^2\,.$

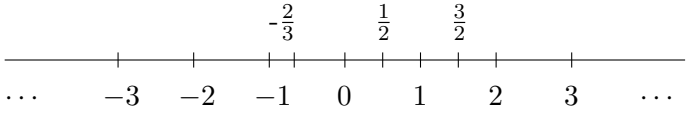
$(P_{30})\ a < b < 0 \Rightarrow b^2 < a^2\,.$

Representación geométrica de los números reales

Una idea intuitiva muy útil es la de representar al conjunto de los números reales sobre una recta. Consideremos una recta r, sobre la misma un punto O que llamaremos origen y al que asociamos el número 0, y una unidad de medida $\overline{u}$.



Con $\overline{u}$ ubicamos el 1. Es costumbre fijar el 1 a la derecha del 0. Entonces existe una correspondencia biyectiva entre números reales y puntos de r. Recíprocamente cada punto de la recta determina un número real.



Es usual designar con el mismo símbolo al número real y al punto de la recta que le corresponde.

Intervalos de números reales

Sean $a, b \in \mathbb{R},\ a < b$. Llamaremos, respectivamente, intervalo abierto, abierto-cerrado, cerrado-abierto y cerrado a los conjuntos siguientes:

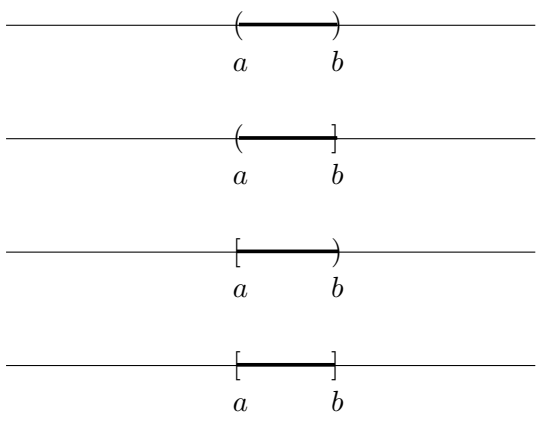
$(a\ ,\ b) = \{\ x \in \mathbb{R} : a < x < b\ \},$

$(a\ ,\ b] = \{\ x \in \mathbb{R} : a < x \leq b\ \},$

$[a\ ,\ b) = \{\ x \in \mathbb{R} : a \leq x < b\ \},$

$[a\ ,\ b] = \{\ x \in \mathbb{R} : a \leq x \leq b\ \}.$

Graficaremos los intervalos del siguiente modo:



En todos los casos los números a y b se llaman los extremos del intervalo.

Es cómodo, además, utilizar notaciones como

$$(-\infty\,,\,b\,] \;=\; \{\, x \in \mathbb{R} \,:\, x \le b\,\},\quad [\,a\,,\,+\infty) \;=\; \{\, x \in \mathbb{R} \,:\, x \ge a\,\},$$

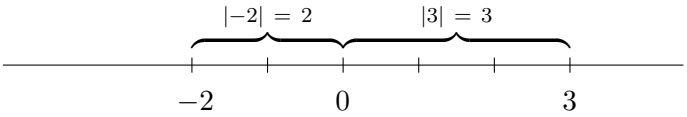
y sus correspondientes $(-\infty\,,\,b)$ y $(a\,,\,+\infty)$.

Valor Absoluto

Sea $x \in \mathbb{R}$. El valor absoluto de x (lo notamos $|x|$) se define como sigue:

$$|x| = \begin{cases} x & \text{si } x \ge 0 \\ -x & \text{si } x < 0 \end{cases}$$

Usando la representación de $\mathbb{R}$ en una recta, el valor absoluto de x tiene una sencilla interpretación geométrica: mide la distancia que hay entre x y 0.



Proposición 5.1 *El valor absoluto verifica las siguientes propiedades:*

(1) $|x| \ge 0$. *Además,* $|x| = 0 \Leftrightarrow x = 0$.

(2) $|-x| = |x|$.

(3) $-|x| \le x \le |x|$.

(4) *Si* $d \in \mathbb{R}$, $d > 0$, *entonces* $|x| \le d \;\Leftrightarrow\; -d \le x \le d$, *esto es,* $|x| \le d \;\Leftrightarrow\; x \in [-d, d]$.

(5) *Si* $d \in \mathbb{R}$, $d > 0$, *entonces* $|x| \ge d \;\Leftrightarrow\; x \le -d$ *ó* $x \ge d$, *o sea,* $|x| \ge d \;\Leftrightarrow\; x \in (-\infty, -d] \cup [d, +\infty)$.

(6) $|x + y| \le |x| + |y|$ (*Desigualdad triangular*).

(7) $|x - y| \ge |\,|x| - |y|\,|$.

(8) $|x \cdot y| = |x| \cdot |y|$.

(9) $\left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$, $y \ne 0$.

Demostración.

(1) Es una consecuencia inmediata de la definición.

(2) y (3) Ejercicio.

(4) Supongamos que $|x| \le d$. Es inmediato de la definición que $x \le |x|$. Luego, por transitividad resulta (i) $x \le d$.
Análogamente, de $-x \le |x|$ se tiene que $-x \le d$, y multiplicando por -1 miembro a miembro, se obtiene (ii) $-d \le x$.
De (i) y (ii) resulta $-d \le x \le d$.
Recíprocamente, supongamos que $-d \le x \le d$. Si $x \ge 0$, entonces $|x| = x \le d$. Si $x < 0$, entonces $|x| = -x$. De $-d \le x$ se tiene $-x \le d$, es decir $|x| \le d$.

(5) Es consecuencia de (4).

(6) Se tiene $-|x| \leq x \leq |x|$ y $-|y| \leq y \leq |y|$. Sumando miembro a miembro, $-(|x|+|y|) \leq x+y \leq |x|+|y|$, y por 4), $|x+y| \leq |x|+|y|$.

(7) Por (6), $|x| = |x-y+y| \leq |x-y|+|y|$, o sea, $|x|-|y| \leq |x-y|$ (i).
Análogamente se prueba que $|y|-|x| \leq |y-x|$ (ii).
Pero por 2), $|x-y| = |y-x|$, luego de (i) y (ii) resulta $-|x-y| \leq |x|-|y| \leq |x-y|$. Por 4), $||x|-|y|| \leq |x-y|$.

(8) Si $x=0$ ó $y=0$ entonces $0 = |xy| = |x||y|$.
Supongamos que $x \neq 0$ e $y \neq 0$.
Si $x>0$ e $y>0$, entonces $xy>0$. Luego $|xy| = xy = |x||y|$.
Si $x<0$ e $y<0$, entonces $xy>0$. Luego $|xy| = xy$, $|x| = -x$, $|y| = -y$. Como $(-x)(-y) = xy$, resulta $|xy| = |x||y|$.
Si $x<0$ e $y>0$, entonces $xy<0$. Luego $|xy| = -(xy) = (-x)y = |x||y|$.

(9) De $x = \dfrac{x}{y} \cdot y$, y usando (8), $|x| = \left|\dfrac{x}{y}\right| \cdot |y|$. Entonces $\left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$.

□

Observación Si x e y son dos números reales, la distancia entre x e y es $x-y$ si $x>y$, y es $y-x$ si $x<y$. Ahora bien

$$|x-y| = \begin{cases} x-y & \text{si } x-y \geq 0 \\ -(x-y) & \text{si } x-y<0 \end{cases} = \begin{cases} x-y & \text{si } x \geq y \\ y-x & \text{si } x<y \end{cases}$$

Entonces la distancia entre x e y es igual a $|x-y|$.

Ejemplos.

1. Describir el conjunto de números reales que verifican $|x-6| \leq 2$ como un intervalo.
   Por la propiedad 4), $|x-6| \leq 2$ equivale a $-2 \leq x-6 \leq 2$, esto es, $4 \leq x \leq 8$, o sea, $x \in [4,8]$.

2. Describir el intervalo $(5,10)$ por medio de una inecuación con valor absoluto.
   Sea x_0 el punto medio del intervalo $(5,10)$, esto es, $x_0 = \dfrac{5+10}{2} = \dfrac{15}{2}$. Entonces $x \in (5,10)$ si y sólo si la distancia de x a x_0 es menor que la distancia de 10 a x_0, esto es, $x \in (5,10)$ si y sólo si $|x - \dfrac{15}{2}| < |10 - \dfrac{15}{2}| = \dfrac{5}{2}$. (Observar que la distancia de 5 a x_0 es también $\dfrac{5}{2}$).

3. Supongamos que queremos resolver la inecuación $|2\,x+1| < 2$.
   Utilizando la propiedad 4) de valor absoluto obtenemos:
   $|2\,x+1| < 2 \;\Leftrightarrow\; -2 < 2\,x+1 < 2 \;\Leftrightarrow -3 < 2\,x < 1 \;\Leftrightarrow\; -\dfrac{3}{2} < x < \dfrac{1}{2}$.
   Luego $S = \left\{ x \in \mathbb{R} : -\dfrac{3}{2} < x < \dfrac{1}{2} \right\} = \left(-\dfrac{3}{2}, \dfrac{1}{2} \right)$.

4. Para resolver la inecuación $|x-2| < \dfrac{x}{2}$, usaremos la definición de valor absoluto.
   Si $x-2 \geq 0$, $|x-2| = x-2$, luego $|x-2| < \dfrac{x}{2} \;\Leftrightarrow\; x-2 < \dfrac{x}{2} \;\Leftrightarrow\; x - \dfrac{x}{2} < 2 \;\Leftrightarrow$
   $\dfrac{x}{2} < 2 \;\Leftrightarrow\; x < 4$.

Sea $S_1 = \{x \in \mathbb{R} : x - 2 \geq 0 \text{ y } x < 4\} = [2, 4)$.
Si $x - 2 < 0$, $|x-2| = -(x-2)$, luego $|x-2| < \frac{x}{2} \Leftrightarrow -(x-2) < \frac{x}{2} \Leftrightarrow -x - \frac{x}{2} < -2 \Leftrightarrow \frac{3}{2}x > 2 \Leftrightarrow x > \frac{4}{3}$.
Sea $S_2 = \{x \in \mathbb{R} : x - 2 < 0 \text{ y } x > \frac{4}{3}\} = (\frac{4}{3}, 2)$.
Entonces $S = (\frac{4}{3}, 2) \cup [2, 4) = (\frac{4}{3}, 4)$.

5. Resolver la ecuación $|3\,x - 4| = \frac{1}{2}$.

   Supongamos que $3\,x - 4 \geq 0$, esto es, $x \geq \frac{4}{3}$.
   Entonces $|3\,x - 4| = 3\,x - 4$, luego $|3\,x - 4| = \frac{1}{2} \Leftrightarrow 3\,x - 4 = \frac{1}{2} \Leftrightarrow 3\,x = \frac{1}{2} + 4 \Leftrightarrow x = \frac{3}{2}$.
   Supongamos ahora que $3\,x - 4 < 0$, es decir, $x < \frac{4}{3}$.
   Entonces $|3\,x - 4| = -(3\,x - 4)$, luego $|3\,x - 4| = \frac{1}{2} \Leftrightarrow -(3\,x - 4) = \frac{1}{2} \Leftrightarrow -3\,x + 4 = \frac{1}{2} \Leftrightarrow x = \frac{7}{6}$.
   Luego las dos soluciones son $x = \frac{3}{2}$ y $x = \frac{7}{6}$.

6. Resolver la inecuación $|1 - 3x| < 2$.
   Como $|1 - 3x| = |3x - 1|$, la desigualdad anterior es equivalente a $|3x - 1| < 2$.
   Ahora usamos la propiedad 4).
   $|3x - 1| < 2 \Leftrightarrow -2 < 3x - 1 < 2 \Leftrightarrow -1 < 3x < 3 \Leftrightarrow -\frac{1}{3} < x < 1$.
   Luego la solución es $S = \{x \in \mathbb{R} : -\frac{1}{3} < x < 1\} = (-\frac{1}{3}, 1)$.

7. Resolver la inecuación $\frac{1}{|2 + 3\,x|} < 1$.
   La inecuación $\frac{1}{|2 + 3\,x|} < 1$ es equivalente a la inecuación $|2 + 3\,x| > 1$, para $x \neq -\frac{2}{3}$. Para resolver esta última inecuación es conveniente hallar los x que no la verifican, es decir, resolver la inecuación $|2 + 3\,x| \leq 1$. La solución que se obtenga es justamente el conjunto de números reales que no son solución de la inecuación original. Descartamos esa solución y nos quedamos con el complemento. Resolvemos, entonces la inecuación $|2 + 3\,x| \leq 1$.
   $|2 + 3\,x| \leq 1 \Leftrightarrow -1 \leq 2 + 3x \leq 1 \Leftrightarrow -3 \leq 3x \leq -1 \Leftrightarrow -1 \leq x \leq -\frac{1}{3}$. Luego la solución de la desigualdad $|2 + 3\,x| \leq 1$ es el conjunto de números reales del intervalo $[-1, -\frac{1}{3}]$.
   La solución de la desigualdad original es entonces $S = (-\infty, -1) \cup (-\frac{1}{3}, +\infty)$.

Ejercicio. Resolver la desigualdad $|x + 1| - |3\,x + 7| > 0$.
Sugerencia: considerar los siguientes casos: $x < -\frac{7}{3}$, $-\frac{7}{3} \leq x < -1$, y $x \geq -1$.

5.2 Números naturales

Vamos a comenzar ahora a distinguir ciertos subconjuntos de los números reales: el conjunto de los números naturales $\mathbb{N}$, el conjunto de los números enteros $\mathbb{Z}$ y el conjunto de los números racionales $\mathbb{Q}$.

En el conjunto de los números reales hay dos elementos distinguidos: el 0 y el 1. Si sumamos el 0 con el 0 obtenemos el mismo número, pero no sucede lo mismo si sumamos el 1. Si sumamos 1 a un número real a obtenemos el número real $a+1$, que es distinto de a, y se llama el *siguiente* de a. Por ejemplo, $1+1 \neq 1$ (porque $1 \neq 0$) y lo denotamos con 2; $2+1=3$, $2 \neq 3$, $3 \neq 1$, y así siguiendo. De esta manera es cómo aparecen *intuitivamente* todos los *números naturales*. Para dar una definición formal de número natural, introducimos el concepto de conjunto inductivo.

Definición 5.2 *Un subconjunto A de $\mathbb{R}$ se dice inductivo si verifica las siguientes propiedades:*

1. $1 \in A$.
2. *Si $x \in A$, entonces $x+1 \in A$.*

Ejemplos.

1. $\mathbb{R}$ es inductivo.
2. $\mathbb{R}^+ = \{x : x \in \mathbb{R} : x \geq 0\}$ es un conjunto inductivo.
3. $A = \{1, 2, 3\}$ no es un conjunto inductivo.
4. $\emptyset$ no es inductivo.

Definición 5.3 *El conjunto de los números naturales es el subconjunto de $\mathbb{R}$, que designaremos con $\mathbb{N}$, definido por las siguientes reglas:*

N1. $\mathbb{N}$ *es inductivo.*

N2. *Si A es un subconjunto inductivo de $\mathbb{R}$, entonces $\mathbb{N} \subseteq A$.*

Es decir, $\mathbb{N}$ es el menor subconjunto inductivo de $\mathbb{R}$ (en el sentido de la inclusión). En particular, como los números reales positivos forman un subconjunto inductivo, los números naturales son positivos.

Considerando los símbolos:
$2 = 1+1$,
$3 = 2+1 = 1+1+1$,
$4 = 3+1 = 1+1+1+1$,
$\vdots$
tenemos entonces: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$.

Principio de inducción

Teorema 5.4 (Principio de Inducción). *Si S es un subconjunto de $\mathbb{N}$ tal que:*

1. $1 \in S$.

2. *Si* $n \in S$ *entonces* $n+1 \in S$,

entonces $S = \mathbb{N}$.

Demostración. Por 1) y 2), S es inductivo, con lo que $\mathbb{N} \subseteq S$. Pero como S es un subconjunto de $\mathbb{N}$, $S \subseteq \mathbb{N}$. Luego $S = \mathbb{N}$. □

El Principio de Inducción es equivalente al siguiente criterio de demostración, llamado *método de demostración por inducción o recurrencia*:

Teorema 5.5 (Criterio de demostración.)
Sea $P(n)$ *una proposición relativa al número natural* n *y supongamos que:*

1. $P(1)$ *es verdadera.*

2. *Para todo* $k \in \mathbb{N}$, *si* $P(k)$ *es verdadera, entonces* $P(k+1)$ *es verdadera.*

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

Veamos que los Teoremas 5.4 y 5.5 son equivalentes. En efecto, el Teorema 5.5 se deduce del Principio de Inducción, ya que si $S = \{n \in \mathbb{N} : P(n) \text{ es verdadera }\}$, entonces S verifica las condiciones 1 y 2 del teorema, y por consiguiente, $S = \mathbb{N}$.

Recíprocamente, el Principio de Inducción es una consecuencia del Teorema 5.5, ya que si ahora S es un subconjunto de $\mathbb{N}$ que verifica 1 y 2 del teorema y consideramos la proposición $P(n)$: "$n \in S$", entonces, por el criterio, $P(n)$ es verdadera para todo $n \in \mathbb{N}$, esto es, para todo $n \in \mathbb{N}$, $n \in S$. Luego $S = \mathbb{N}$.

Ejemplos.

1. Probar que la proposición $P(n)$: $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$ es verdadera para todo $n \in \mathbb{N}$.
   (La proposición se lee: "La suma de los n primeros números naturales es igual a $\dfrac{n(n+1)}{2}$".

   (a) **Probemos** que $P(1)$ es verdadera: $1 = \dfrac{1 \cdot (1+1)}{2}$

   (b) **Supongamos** que $P(k)$ es verdadera:
   $$1 + 2 + \cdots + k = \frac{k(k+1)}{2} \qquad \text{Hipótesis Inductiva (HI)}$$
   (La suposición según la cual $P(k)$ es verdadera, se conoce con el nombre de *hipótesis inductiva* (HI)).

   (c) **Probemos** que $P(k+1)$ es verdadera:
   $$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)[(k+1)+1]}{2},$$
   esto es,
   $$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

$$\begin{aligned} 1+2+\cdots+k+(k+1) &\overset{\text{(HI)}}{=} \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Es muy conocida (aunque apócrifa) la siguiente anécdota de la historia de la matemática referida al ejemplo 1. Carl Friedrich Gauss (1777-1855), uno de los más grandes matemáticos de todos los tiempos, estaba en la escuela primaria cuando su maestro le dió a la clase la tarea de hallar la suma de todos los enteros de 1 a 1000, esperando tener un buen rato de descanso mientras sus alumnos estaban trabajando. Para su sorpresa, Gauss le alcanzó la respuesta casi inmediatamente. Su solución era muy simple: sumando el primer término con el último se obtiene $1+1000 = 1001$; sumando el segundo término con el anteúltimo se obtiene $2+999 = 1001$; sumando el tercero... etc. ; estas sumas siempre dan 1001. La última suma es $500+501 = 1001$. Luego se obtienen 500 veces 1001, es decir, 500500, o lo que es lo mismo $\frac{1000}{2} \cdot 1001$.

2. Probar que la proposición $P(n)$: $1+3+5+\cdots+(2n-1) = n^2$ es verdadera para todo $n \in \mathbb{N}$.

   (a) **Probemos** que vale para $n = 1$: $\quad 2 \cdot 1 - 1 = 1^2$.

   (b) **Supongamos** que vale para $n = k$:

   $$1+3+5+\cdots+(2k-1) = k^2 \qquad \text{Hipótesis Inductiva (HI)}$$

   (c) **Probemos** que vale para $n = k+1$:

   $$1+3+5+\cdots+(2k-1)+[2(k+1)-1] = (k+1)^2$$

   $$\begin{aligned} 1+3+5+\cdots+(2k-1)+[2(k+1)-1] &\overset{\text{(HI)}}{=} k^2+[2(k+1)-1] \\ &= k^2+2k+2-1 \\ &= k^2+2k+1 \\ &= (k+1)^2. \end{aligned}$$

3. La proposición $P(n) : 1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2\,n+1)}{6}$ es verdadera para todo $n \in \mathbb{N}$.

   (a) Si $n = 1$, $1^2 = 1 = \frac{1(1+1)(2.1+1)}{6}$, por lo tanto $P(1)$ es verdadera.

   (b) Supongamos que la proposición es verdadera para $n = k$ y probemos que lo es para $n = k+1$.

   Es decir, supongamos que

   $$1^2+2^2+\cdots+k^2 = \frac{k(k+1)(2\,k+1)}{6} \qquad \text{Hipótesis Inductiva (HI)}$$

   (c) Probemos que

   $$1^2+2^2+\cdots+k^2+(k+1)^2 = \frac{(k+1)(k+2)(2\,k+3)}{6}.$$

$$1^2+2^2+\cdots+k^2+(k+1)^2 \overset{HI}{=} \frac{k(k+1)(2\,k+1)}{6}+(k+1)^2 = \frac{k(k+1)(2\,k+1)+6(k+1)^2}{6} =$$
$$\frac{(k+1)}{6}[k(2\,k+1)+6(k+1)] = \frac{(k+1)}{6}(2\,k^2+7\,k+6) = \frac{(k+1)}{6}(2\,k^2+4\,k+3\,k+6) =$$
$$\frac{(k+1)}{6}\,[2\,k(k+2)+3(k+2)] = \frac{(k+1)}{6}(k+2)(2\,k+3).$$

Concluimos entonces que $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

4. Para todo $n \in \mathbb{N}$, es $n \geq 1$.
   Consideremos la proposición $P(n)$: "$n \geq 1$, para todo $n \in \mathbb{N}$ ".
   Es claro que $P(1)$ es verdadera.
   Supongamos que $P(k)$ es verdadera, es decir, $k \geq 1$.
   Probemos que $P(k+1)$ es verdadera, es decir, probemos que $k+1 \geq 1$. Pero de $k \geq 1$ resulta $k+1 \overset{E3}{\geq} 1+1 > 1+0 = 1$.

5. Probemos por inducción que $2^n > n$, para todo $n \in \mathbb{N}$.

   (a) Si $n = 1$, $2^1 = 2 > 1$. Luego $P(1)$ es verdadera.

   (b) Supongamos que $P(k)$ es verdadera, esto es, $2^k > k$. (HI)

   (c) Probemos que $P(k+1)$ es verdadera, o sea, $2^{k+1} > k+1$.
   $2^{k+1} = 2 \cdot 2^k \overset{HI}{>} 2\,k = k+k \geq k+1$, luego $2^{k+1} > k+1$.

   Por lo tanto la proposición $P(n) : 2^n > n$ es verdadera para todo $n \in \mathbb{N}$.

6. Usemos el Principio de Inducción para probar que para todo $n \in \mathbb{N}$, n^2+n es un número par.

   (a) Si $n = 1$, $1^2+1 = 2 = 2.1$ luego $P(1)$ es verdadera.

   (b) Supongamos que $k^2+k = 2\,s$, $s \in \mathbb{N}$, o sea un número par

   (c) Probemos la paridad de $(k+1)^2+(k+1)$.
   $(k+1)^2+(k+1) = k^2+2\,k+1+k+1 = k^2+k+2(k+1) \overset{HI}{=} 2\,s+2(k+1) = 2(s+k+1)$, que es un número par, ya que $t = s+k+1$ es un natural.

   Resulta entonces que la proposición $P(n)$: "n^2+n es un número par" es verdadera para todo $n \in \mathbb{N}$.

7. Probar que si $a \in \mathbb{R}$, entonces $\displaystyle\sum_{i=0}^{n-1} a^i = \frac{a^n-1}{a-1}$.

Observación: El Principio de Inducción admite una pequeña modificación, de gran utilidad para probar la validez de algunas propiedades:
Sea n_0 un número natural cualquiera, y supongamos que para cada número natural $n \geq n_0$, se verifican las siguientes condiciones, para una proposición dada $P(n)$:

1. *$P(n_0)$ es verdadera.*

2. *Si $P(k)$ es verdadera, $k \geq n_0$, entonces $P(k+1)$ es verdadera.*

Entonces $P(n)$ es verdadera para todo natural $n \geq n_0$.

Dejamos la demostración a cargo del lector, con la siguiente sugerencia:
considerar $S = \{1, 2, 3, \ldots, n_0 - 1\} \cup \{n \in \mathbb{N} : P(n) \text{ es verdadera } \}$ y probar que S es inductivo.

Ejemplos.

1. Probar que si $n \geq 3$, $n^2 > 2n + 1$.
   (a) Claramente, la propiedad vale para $n = 3$.
   (b) Supongamos que la propiedad vale para $n = k$, esto es, supongamos que $k^2 > 2k + 1$.
   (c) Probemos que vale para $n = k + 1$, es decir, probemos que $(k + 1)^2 > 2(k + 1) + 1$.
   $(k + 1)^2 = k^2 + 2k + 1 \overset{HI}{>} 2k + 1 + 2k + 1 = 2(k + 1) + 2k > 2(k + 1) + 1$.
2. Probar como ejercicio que si $n \geq 4$, $2^n \geq n^2$.

Usaremos ahora el Principio de Inducción para probar algunas propiedades de los números naturales.

Teorema 5.6 $\mathbb{N}$ *es cerrado con respecto a la suma y a la multiplicación.*

(a) *Si* $a, b \in \mathbb{N}$, *entonces* $a + b \in \mathbb{N}$.

(b) *Si* $a, b \in \mathbb{N}$, *entonces* $a \cdot b \in \mathbb{N}$.

Demostración. (a) Sea $a \in \mathbb{N}$. Sea $S = \{b : b \in \mathbb{N} \text{ y } a + b \in \mathbb{N}\}$. Veamos que S es inductivo.
1. $1 \in S$. En efecto, como $a \in \mathbb{N}$, entonces $a + 1 \in \mathbb{N}$, por lo tanto $1 \in S$.
2. Veamos que si $b \in S$, entonces $b+1 \in S$. De $b \in S$ resulta $a+b \in \mathbb{N}$. Pero entonces $(a+b)+1 \in \mathbb{N}$, esto es, $a + (b + 1) \in \mathbb{N}$. Luego $b + 1 \in S$.
Luego $S = \mathbb{N}$, es decir, $a+b \in \mathbb{N}$ cualquiera que sea $b \in \mathbb{N}$. Como a es arbitrario resulta que $a+b \in \mathbb{N}$ cualquiera que sean $a, b \in \mathbb{N}$.
(b) Queda como ejercicio. □

Las siguientes propiedades se demuestran también usando el Principio de Inducción. Se aconseja al lector intentar demostrarlas por su cuenta, y sólo acudir a la demostración que aquí se incluye, después de haber realizado algún esfuerzo por obtener la propia.

Propiedades.

1. Para todo $n \in \mathbb{N}$, o bien $n = 1$, o bien $n - 1 \in \mathbb{N}$.
   Sea $P(n)$: "Para todo $n \in \mathbb{N}$, o bien $n = 1$, o bien $n - 1 \in \mathbb{N}$ ".
   Es claro que $P(1)$ es verdadera.
   Supongamos que $P(k)$ es verdadera, es decir, $k = 1$ ó $k - 1 \in \mathbb{N}$.
   Probemos que $P(k + 1)$ es verdadera, es decir, probemos que $k + 1 = 1$ ó que $k + 1 \in \mathbb{N}$.
   Si $k = 1$ en la HI, entonces $P(k + 1) = P(2)$, que es verdadera porque $2 - 1 = 1 \in \mathbb{N}$.
   Si $k - 1 \in \mathbb{N}$ en la HI, entonces $P(k + 1)$ es verdadera ya que $(k + 1) - 1 = (k - 1) + 1 \in \mathbb{N}$ pues es suma de dos números naturales.
2. Si $m, n \in \mathbb{N}$ y $n < m$, entonces $m - n \in \mathbb{N}$. Considerar $P(n)$: "Para todo $m \in \mathbb{N}$, si $n < m$ entonces $m - n \in \mathbb{N}$ ".
   $P(1)$ es verdadera, por el ejercicio anterior. Suponemos que $P(k)$ es verdadera, esto es, si $k < m$,

entonces $m-k \in \mathbb{N}$. Debemos probar que $P(k+1)$ es verdadera, esto es, si $k+1<m$ entonces $m-(k+1) \in \mathbb{N}$. Pero como $k \geq 1$, de $k+1<m$ resulta que $m \geq 2$. En particular, $m \neq 1$. Por lo anterior, $m-1 \in \mathbb{N}$. Pero $k+1<m \Leftrightarrow k<m-1 \overset{HI}{\Rightarrow} (m-1)-k \in \mathbb{N}$, o sea, $m-k-1 \in \mathbb{N} \Rightarrow m-(k+1) \in \mathbb{N}$.

3. Si $m, n \in \mathbb{N}$ y $n<m$, entonces $n+1 \leq m$ (Entre n y $n+1$ no hay ningún número natural). De $n<m$, por 3), es $m-n \in \mathbb{N}$, pero por 1), $1 \leq m-n$, o sea $n+1 \leq m$.

Principio de Buena Ordenación

Un subconjunto A de $\mathbb{R}$ se dice *bien ordenado* si todo subconjunto no vacío de A tiene primer elemento.

El Principio de Buena Ordenación establece que $\mathbb{N}$ es bien ordenado. Para apreciar la importancia de esta propiedad de los números naturales, conviene observar que $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ no la verifican. Así por ejemplo, el conjunto $\{-1,-2,-3,\ldots,-n.\ldots\} \subseteq \mathbb{Z}$ no tiene primer elemento, pues $-(n+1)<-n$ para todo n. Análogamente, el conjunto $\{1,1/2,1/3,\ldots,1/n,\ldots\} \subseteq \mathbb{Q}$ no tiene primer elemento, pues $1/(n+1)<1/n$.

Teorema 5.7 (Principio de Buena Ordenación). *$\mathbb{N}$ es un conjunto bien ordenado.*

Demostración. Consideremos la siguiente proposición $P(n)$: "Si $A \subseteq \mathbb{N}$ y A contiene un elemento que es menor o igual que n, entonces A tiene primer elemento".

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

1. $P(1)$ es verdadera. En efecto, sea $A \subseteq \mathbb{N}$ y supongamos que A contiene un elemento $t \leq 1$. Como siempre $1 \leq t$, debe ser $t=1$. Entonces $1 \in A$, y 1 es el primer elemento de A.

2. Supongamos que $P(k)$ es verdadera y probemos que $P(k+1)$ es verdadera. Sea $A \subseteq \mathbb{N}$ y supongamos que A contiene un número $t \leq k+1$. Si A no contiene ningún número estrictamente menor que $k+1$, entonces $k+1$ es el primer elemento de A. Si A contiene un número $s<k+1$, entonces, como entre k y $k+1$ no hay ningún número natural, $s \leq k$, esto es, A contiene un número $\leq k$. Por la hipótesis inductiva, A tiene primer elemento.

□

El teorema anterior se probó a partir del Principio de Inducción. En realidad, el Principio de Buena Ordenación es equivalente al Principio de Inducción.

En efecto, supongamos que vale el Principio de Buena Ordenación. Sea $P(n)$ una proposición tal que:

1. $P(1)$ es verdadera.

2. Si $P(k)$ es verdadera, entonces $P(k+1)$ es verdadera.

Queremos probar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Supongamos lo contrario, esto es, que existe al menos un número natural n para el cual $P(n)$ es falsa.

Sea $A=\{n \in \mathbb{N} : P(n) \text{ es falsa }\}$. Por lo anterior, A es un subconjunto de $\mathbb{N}$ no vacío, y por el Principio de Buena Ordenación, A tiene primer elemento n_0.

Es claro que $n_0 \neq 1$, pues $P(1)$ es verdadera.

Además, $n_0 - 1$ no pertenece a A, luego $P(n_0 - 1)$ es verdadera. Pero de 2, para $k = n_0 - 1$, como $P(k)$ es verdadera, $P(k+1)$ es verdadera, es decir, $P((n_0 - 1) + 1)$ es verdadera, esto es, $P(n_0)$ es verdadera, lo que es una contradicción. Esta contradicción provino de suponer que existía un número natural n tal que $P(n)$ es falsa. Luego $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Como una aplicación del Principio de Buena Ordenación, vamos a ver una variante del principio de inducción utilizada con mucha frecuencia en las demostraciones. Mediante esta segunda forma, para probar que una proposición $P(n)$ es verdadera para todo número natural, basta probar que es verdadera para 1, y, suponiéndola verdadera para todos los números naturales menores que n $(n > 1)$, probarla para n.

Teorema 5.8 (**Segunda forma del Principio de Inducción**).
Sea $P(n)$ una proposición sobre el número natural n y supongamos que:

a) *$P(1)$ es verdadera.*

b) *Para todo $n \in \mathbb{N}$, $n > 1$, si $P(k)$ es verdadera para todo $k < n$, entonces $P(n)$ es verdadera.*

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

Demostración. Sea $H = \{n \in \mathbb{N} : P(n) \text{ es verdadera } \}$ y probemos que $H = \mathbb{N}$.

Por la definición de H, se verifican las siguientes condiciones:

1. $1 \in H$.

2. Para todo $n \in \mathbb{N}$, $n > 1$, si $k \in H$ para todo $k < n$, entonces $n \in H$.

Supongamos que $H \neq \mathbb{N}$. Por lo tanto, como $H \subseteq \mathbb{N}$, es $\mathbb{N} - H = H' \neq \emptyset$.

Por el Principio de Buena Ordenación, H' posee primer elemento j. Por la misma definición de j, es claro que $j > 1$, ya que $1 \in H$, y si $k < j$, entonces $k \in H$.

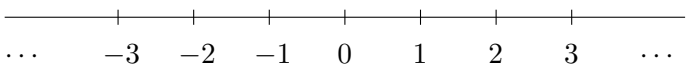
Luego, por 2), $j \in H$, lo cual es un absurdo, pues $j \in H'$. El absurdo provino de suponer que $H \neq \mathbb{N}$. Luego el teorema queda probado. □

5.3 Números enteros

Daremos en este momento solamente una introducción a los números enteros, dejando para el capítulo siguiente el estudio de sus propiedades más importantes.

Si X es un subconjunto de $\mathbb{R}$, notaremos $X^- = \{-x : x \in X\}$.
Llamaremos *número entero* a todo elemento del conjunto $\mathbb{Z} = \mathbb{N}^- \cup \{0\} \cup \mathbb{N}$.
Entonces $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

A los números enteros los representamos como sigue:



Proposición 5.9 *Si $x, y \in \mathbb{Z}$ entonces $x + y \in \mathbb{Z}$, $x \cdot y \in \mathbb{Z}$ y $x - y \in \mathbb{Z}$.*

Demostración. Indiquemos cómo probar que $x+y \in \mathbb{Z}$.
Si $x=0$ ó $y=0$, la propiedad es inmediata.
Supongamos entonces que $x \neq 0$ e $y \neq 0$. Si $x>0$ e $y>0$, entonces $x,y \in \mathbb{N}$, y es claro que $x+y \in \mathbb{N}$. Si $x<0$ e $y<0$, entonces $x=-n$, $y=-m$, $n,m \in \mathbb{N}$. Luego $x+y=-n+(-m)=-(n+m) \in \mathbb{N}^- \subseteq \mathbb{Z}$.
Dejamos los casos restantes, así como las otras dos propiedades, como ejercicio. □

5.4 Números racionales

Llamaremos *número racional* a todo número real de la forma $\frac{a}{b}$, con $a, b \in \mathbb{Z}$, $b \neq 0$.
Designaremos con $\mathbb{Q}$ al conjunto de todos los números racionales.

Para representar los números racionales se puede proceder de la siguiente manera:

Para representar el racional positivo $\frac{a}{b}$ se divide al segmento $\overline{u}$ en b segmentos iguales y luego se transporta uno de ellos a veces a partir del origen sobre la semirrecta que contiene al 1. El racional negativo $-\frac{a}{b}$ está representado por el simétrico del anterior respecto al origen.
Representemos geométricamente al racional $\frac{5}{3}$.

Proposición 5.10 *Si $x, y \in \mathbb{Q}$ entonces $x+y \in \mathbb{Q}$, $x \cdot y \in \mathbb{Q}$, $x-y \in \mathbb{Q}$ y $\frac{x}{y} \in \mathbb{Q}$ $(y \neq 0)$.*

Demostración. Ejercicio (ver propiedades P12 a P15). □

Observemos que todo número entero m es un número racional, ya que $m=\frac{m}{1}$. Entonces tenemos las inclusiones:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

A partir de la proposición anterior podemos probar la sencilla pero importante propiedad de que entre dos números racionales existe siempre otro número racional:

Proposición 5.11 *Si $a, b \in \mathbb{Q}$ y $a<b$, entonces $\frac{a+b}{2}$ es un número racional, y se tiene:*

$$a < \frac{a+b}{2} < b.$$

Demostración. De la proposición anterior resulta que $\frac{a+b}{2}$ es racional.
Como $a<b$ se tiene: $a+a<a+b$, esto es, $2a<a+b$, se donde $a<\frac{a+b}{2}$.
Análogamente, $a+b<b+b$, esto es, $a+b<2b$, se donde $\frac{a+b}{2}<b$. □

Es claro que reiterando el procedimiento indicado en la proposición anterior, se obtiene que entre dos racionales a y b hay infinitos racionales.

5.5 Propiedad de completitud

Sea A un subconjunto cualquiera de números reales, es decir, $A \subseteq \mathbb{R}$. Recordemos las nociones de *cota superior* y *supremo* que fueron introducidas en el parágrafo correspondiente a relaciones de orden.

Un número real c se dice *cota superior* de A si $a \leq c$, para todo $a \in A$.

Por ejemplo, si $A = (a, b)$, donde $a < b$, entonces los números b, $b+1$, $b+0.5$, ..., $b+\epsilon$, donde ϵ es un número real no negativo, son cotas superiores de A. Estos mismos números son cotas superiores de $A = [a, b]$.

En términos de la representación de los números reales en una recta, que un número c sea cota superior de un conjunto $A \subseteq \mathbb{R}$ significa que c está *a la derecha* del conjunto A.

Si A tiene una cota superior, A se dice *acotado superiormente*.

Si $A \subseteq \mathbb{R}$, un número real c se dice *supremo* de A, y escribimos $c = Sup\ A$, si c es una cota superior de A y además, es la menor de las cotas superiores de A.

Por ejemplo, $Sup\ (a, b) = b$, $Sup\ [a, b] = b$. Observemos que en el caso $A = (a, b)$, el supremo no pertenece a A, mientras que en el caso $A = [a, b]$, el supremo pertenece a A. En general, el supremo puede o no pertenecer al conjunto.

Enunciamos ahora el Axioma de Completitud de los números reales. Esta es la última de las propiedades básicas de los números reales, que juntamente con las de cuerpo ordenado ya enunciadas, caracteriza a los números reales como un cuerpo ordenado completo.

Axioma de Completitud. *Si A es un subconjunto no vacío de $\mathbb{R}$, acotado superiormente, entonces existe $c = Sup\ A$.*

Observación: Sea $Inf\ A$ el ínfimo de un subconjunto $A \subseteq \mathbb{R}$ (Recordemos que el ínfimo de A es la mayor de las cotas inferiores de A). Entonces, el axioma de completitud puede enunciarse equivalentemente de la siguiente manera: *Si A es un subconjunto no vacío de $\mathbb{R}$, acotado inferiormente, entonces existe $d = Inf\ A$.* Es decir, se puede probar esta propiedad a partir del Axioma de Completitud. Y además, si aceptamos esta propiedad entonces es posible probar el Axioma de Completitud.

Observación. El conjunto vacío está acotado superior e inferiormente, pero no tiene ínfimo ni supremo. En efecto, todo número real es cota superior e inferior de $\emptyset$.

Consecuencias del Axioma de Completitud.

La primera propiedad que vamos a enunciar como consecuencia del Axioma de Completitud se refiere al hecho, intuitivamente obvio, de que existen números naturales tan grandes como uno quiera.

Teorema 5.12 (Principio de Arquímedes, o propiedad arquimediana). *Para todo número real a, existe un número natural n tal que $n > a$.*

Demostración. Supongamos por el absurdo que el Principio no vale. Entonces existe $a \in \mathbb{R}$ tal que $n \leq a$ para todo $n \in \mathbb{N}$.

Esto significa que a es una cota superior para $\mathbb{N}$. Como $\mathbb{N} \neq \emptyset$, por el Axioma de Completitud, existe $a^* = Sup\ \mathbb{N}$.

Si $a^* = n$ para algún n, entonces $a^* = n < n + 1$, lo cual es absurdo. Luego $n < a^*$ para todo $n \in \mathbb{N}$.

Como $n + 1 \in \mathbb{N}$, entonces también $n + 1 < a^*$, esto es, $n < a^* - 1$ cualquiera que sea $n \in \mathbb{N}$, lo cual es un absurdo, pues a^* es el supremo. El absurdo provino de suponer que $\mathbb{N}$ estaba acotado. Luego vale la propiedad arquimediana. □

Corolario 5.13 *Sean $a, b \in \mathbb{R}$ tales que $a > 0$. Entonces existe un número natural n tal que $n \cdot a > b$.*

Demostración. Si $a = b$, se verifica para todo $n > 1$. Si $a > b$, se verifica para todo $n \in \mathbb{N}$. Si $a < b$, como $\frac{b}{a} \in \mathbb{R}$, por el Principio de Arquímedes, existe un $n \in \mathbb{N}$ tal que $n > \frac{b}{a}$. Como $a > 0$, $n \cdot a > b$. □

El siguiente corolario prueba que $\mathbb{Q}$ es denso en $\mathbb{R}$, es decir, que entre dos números reales siempre hay un número racional.

Corolario 5.14 (*Densidad de $\mathbb{Q}$ en $\mathbb{R}$*). *Sean $a, b \in \mathbb{R}$, $a < b$. Entonces existe $t \in \mathbb{Q}$, con $a < t < b$.*

Demostración. Sin pérdida de generalidad, podemos suponer que $0 \leq a$.

Si $a = 0$, entonces tenemos $0 < b$. Como $0 < 1$, sea $n \in \mathbb{N}$ tal que $1 < n \cdot b$. Se tiene así $0 < \frac{1}{n} < b$. Como $\frac{1}{n} \in \mathbb{Q}$, $\frac{1}{n}$ es el racional buscado.

Supongamos ahora que $0 < a$. Como $a < b$, $b - a > 0$. De $b - a > 0$ y $1 > 0$, por Corolario 1, existe $n \in \mathbb{N}$ tal que $n(b - a) > 1$, esto es, $\frac{1}{n} < b - a$. (1)

Como $na \in \mathbb{R}$, por el Principio de Arquímedes, el conjunto

$$A = \{t \in \mathbb{N} : n \cdot a < t\}$$

es no vacío. Por el Principio de Buena Ordenación, A tiene primer elemento m. Entonces, $m \in \mathbb{N}$, $na < m$ y m es el menor número natural con esta propiedad, esto es, $m - 1 \leq na$. (2)

Veamos que $a < \frac{m}{n} < b$. De $m > na$ resulta $\frac{m}{n} > a$. Además, aplicando (1) y (2),

$$\frac{m}{n} = \frac{m-1}{n} + \frac{1}{n} \leq \frac{na}{n} + \frac{1}{n} < a + (b - a) = b$$

.

Luego $r = \frac{m}{n} \in \mathbb{Q}$ es el racional buscado. □

Una última consecuencia de la propiedad de completitud es la existencia de raíces n-ésimas de cualquier número real positivo, para todo $n \in \mathbb{N}$. Para su demostración remitimos al lector a Gentile, Notas de Algebra I, Eudeba.

Teorema 5.15 *Sea a un número real positivo y sea n un número natural. Entonces existe un único número positivo b tal que $b^n = a$. Se nota $b = \sqrt[n]{a}$, y decimos que b es la raíz n-ésima de a.*

En base al teorema anterior, podemos asegurar, por ejemplo, la existencia de $\sqrt{2}$. Vamos a probar que $\sqrt{2}$ no es racional.

Supongamos que $\sqrt{2}$ es racional, esto es, existen números enteros a y b, $b \neq 0$, tales que:

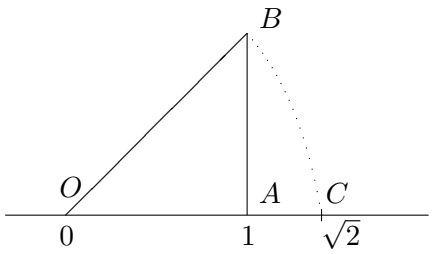
$$\sqrt{2} = \frac{a}{b},$$

es decir, existen dos enteros a y b tales que $\left(\frac{a}{b}\right)^2 = 2$. Podemos suponer que $\frac{a}{b}$ es una fracción irreducible, esto es, a y b no poseen factores comunes propios.

De lo anterior resulta $a^2 = 2\,b^2$, lo que implica que a^2 es par, esto es, a es par. $(*)$
Tenemos que $a = 2\,c$ y entonces $4\,c^2 = 2\,b^2$, es decir, $2\,c^2 = b^2$. Razonando como antes obtenemos que b^2 es par concluyendo que b es par. $(**)$

$(*)$ y $(**)$ contradicen la hipótesis sobre la irreducibilidad de la fracción $\dfrac{a}{b}$.

Podemos entonces determinar sobre la recta un punto que no representa a un racional.



Habiendo asegurado la existencia de raíces n-ésimas de números reales no negativos, podemos probar la siguiente propiedad del valor absoluto de un número real:

$$\sqrt{x^2} = |x|.$$

Observemos, en primer lugar, que $x^2 \geq 0$, y por lo tanto, x^2 tiene una única raíz cuadrada no negativa.

Si $x \geq 0$, es claro que $\sqrt{x^2} = x$.

Si $x < 0$, entonces $-x > 0$, o sea, $-x$ es positivo. Además, $(-x)^2 = (-x)(-x) = xx = x^2$. Luego, si $x < 0$, $\sqrt{x^2} = -x$.

En resumen,

$$\sqrt{x^2} = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

Luego $\sqrt{x^2} = |x|$.

Veamos que $\mathbb{Q}$ no verifica la propiedad de completitud, es decir, que $\mathbb{Q}$ **no es completo**. Esto significa que existen conjuntos de números racionales no vacíos acotados superiormente que no tienen supremo en $\mathbb{Q}$. El típico ejemplo está dado en el siguiente teorema:

Teorema 5.16 *$\mathbb{Q}$ no es completo.*

Demostración. Consideremos el conjunto $A = \{x \in \mathbb{Q} : x^2 < 2\}$. Claramente $A \neq \emptyset$ y es acotado superiormente. Veamos que no existe supremo de A en Q. Supongamos por el absurdo que $b = Sup\ A \in \mathbb{Q}$.

1. No puede ser $b^2 = 2$, porque $b \in \mathbb{Q}$.
2. Supongamos que $b^2 < 2$. Sea $t = 2 - b^2 > 0$, y sea h un número racional tal que $0 < h < 1$. Entonces $(b+h)^2 = b^2 + 2hb + h^2 < b^2 + 2hb + h = b^2 + h(2b+1) < b^2 + h(b^2 + 2b + 1) = b^2 + h(b+1)^2 = 2 - t + h(b+1)^2$. Luego, tomando $h < \dfrac{t}{(b+1)^2}$ (y $0 < h < 1$) resulta $(b+h)^2 < 2 - t + h(b+1)^2 < 2 - t + \dfrac{t}{(b+1)^2} \cdot (b+1)^2 = 2 - t + t = 2$, es decir, $(b+h)^2 < 2$, y en consecuencia, $b + h \in A$ y $b + h > b$, lo cual es imposible, pues $b = Sup\ A$.

3. Supongamos que $b^2 > 2$. Sea $t = b^2 - 2 > 0$, y sea h un número racional tal que $0 < h < 1$. Entonces $(b-h)^2 = b^2 - 2hb + h^2 > b^2 - 2hb - h = b^2 - h(2b+1) > b^2 - h(b^2+2b+1) = b^2 - h(b+1)^2 = t + 2 - h(b+1)^2$. Luego, tomando $h < \dfrac{t}{(b+1)^2}$ (y $0 < h < 1$) resulta $(b-h)^2 > t + 2 - h(b+1)^2 > t + 2 - \dfrac{t}{(b+1)^2} \cdot (b+1)^2 = t + 2 - t = 2$, es decir, $(b-h)^2 > 2$, y en consecuencia, $b - h \notin A$. Ahora, como $b = Sup\ A$, existe $d \in A$ tal que $b - h < d$, luego $(b-h)^2 < d^2 < 2$, o sea, $(b-h)^2 < 2$. Absurdo.

Luego hemos probado que si $b = Sup\ A$ y $b \in \mathbb{Q}$ entonces $b^2 \neq 2$, $b^2 \not> 2$ y $b^2 \not< 2$. Luego no existe b racional tal que $b = SupA$. □

Llamaremos **número irracional** a todo número real que no es racional. Si designamos con $\mathbb{I}$ al conjunto de todos los números irracionales, entonces $\mathbb{I} = \{x \in \mathbb{R} : x \notin \mathbb{Q}\} = \mathbb{R} - \mathbb{Q}$.

Potencia de un número real

Potencia natural

Sean $x \in \mathbb{R}$ y $n \in \mathbb{N}$. Definimos la potencia n-ésima de x de la siguiente manera:

(PN1) $x^1 = x$.

(PN2) $x^{n+1} = x^n \cdot x$.

Ejemplo: $x^2 = x \cdot x$, $\quad x^3 = x^2 \cdot x = x \cdot x \cdot x$.

Propiedades.

Sean $a, b \in \mathbb{R}$ y $m, n \in \mathbb{N}$, entonces se verifican las siguientes propiedades:

(1) $a^{n+m} = a^n \cdot a^m$.
Consideremos la siguiente proposición:

$$P(n): \ a^{n+m} = a^n \cdot a^m, \text{ para todo } m \in \mathbb{N}.$$

(Se suele decir en casos como este que se está haciendo *inducción sobre* n.)
$P(1)$ es verdadera, ya que $a^{m+1} = a^m \cdot a = a^m \cdot a^1$.
Supongamos que $P(k)$ es verdadera, esto es, $a^{m+k} = a^m \cdot a^k$, para todo $m \in \mathbb{N}$.
Veamos que $P(k+1)$ es verdadera, esto es, que $a^{m+(k+1)} = a^m \cdot a^{k+1}$.
$a^{m+(k+1)} = a^{(m+k)+1} = a^{m+k} \cdot a = (a^m \cdot a^k) \cdot a = a^m \cdot (a^k \cdot a) = a^m \cdot a^{k+1}$.

(2) $a^{m \cdot n} = (a^m)^n$.
Ejercicio. Considerar $P(n)$: "$a^{m \cdot n} = (a^m)^n$, para todo $m \in \mathbb{N}$ ".

(3) $(a \cdot b)^n = a^n \cdot b^n$.

(4) $\left(\dfrac{a}{b}\right)^n = \dfrac{a^n}{b^n}$, $b \neq 0$.

Potencia entera

Si $x \in \mathbb{R} - \{0\}$ y $k \in \mathbb{Z}$; $k \leq 0$, la definición de potencia natural se extiende a exponente entero como sigue:

(PE1) $x^0 = 1$.

(PE2) $x^k = \dfrac{1}{x^{-k}} = \left(x^{-1}\right)^{-k}$, $k \neq 0$.

Ejemplo: $x^{-2} = \dfrac{1}{x^2}$ y $x^{-3} = \dfrac{1}{x^3}$.

Propiedades de la raíz n-ésima de un número real no negativo

Algunas propiedades de la potenciación se trasladan a la radicación:
Sean $a, b \in \mathbb{R}$, $a \geq 0$, $b \geq 0$, $n, m, s \in \mathbb{N}$, entonces se verifican:

(1) $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$.
En efecto, de $\left(\sqrt[n]{a} \cdot \sqrt[n]{b}\right)^n = (\sqrt[n]{a})^n \cdot \left(\sqrt[n]{b}\right)^n = ab$, resulta que $\sqrt[n]{a} \cdot \sqrt[n]{b}$ es un número positivo que elevado a la n es igual a ab. Por la unicidad de la raíz n-ésima, resulta la propiedad.

(2) $\sqrt[m]{a^n} = (\sqrt[m]{a})^n$.
$\left[(\sqrt[m]{a})^n\right]^m = (\sqrt[m]{a})^{n \cdot m} = (\sqrt[m]{a})^{m \cdot n} = \left[(\sqrt[m]{a})^m\right]^n = a^n$. Luego $\sqrt[m]{a^n} = (\sqrt[m]{a})^n$.

(3) $\sqrt[m]{\sqrt[n]{a}} = \sqrt[m \cdot n]{a}$.
$\left(\sqrt[m]{\sqrt[n]{a}}\right)^{m \cdot n} = \left[\left(\sqrt[m]{\sqrt[n]{a}}\right)^m\right]^n = [\sqrt[n]{a}]^n = a$, de donde se tiene la propiedad.

(4) $\sqrt[m \cdot s]{a^{n \cdot s}} = \sqrt[m]{a^n}$.

Raíz n-ésima impar de un número real

Si n es un número natural impar $(n = 2\,k - 1,\ k \in \mathbb{N})$, entonces la definición de raíz n-ésima de un número real no negativo puede ser extendida a todos los números reales, pues se verifica que:

Si $a \in \mathbb{R}$ y n es un número natural impar entonces existe un único $b \in \mathbb{R}$ tal que $b^n = a$. Si $a < 0$, se tiene que $b < 0$. El número b se denomina la raíz n-ésima de a y lo notaremos, como antes, $\sqrt[n]{a}$.

Raíz n-ésima par negativa de un número real positivo

Sea $a > 0$ y n un número natural par ($n = 2\,k$, $k \in \mathbb{N}$), entonces existe un único $d < 0$ que satisface $d^n = a$. Diremos que d es la raíz n-ésima negativa de a y la notaremos $-\sqrt[n]{a}$.
Como antes, si $n = 2$, escribiremos $-\sqrt{a}$ en lugar de $-\sqrt[2]{a}$. De los expuesto resulta que si $a > 0$ y n es un número natural par existen dos únicos números reales, uno positivo y el otro negativo, tales que al calcular su potencia n-ésima obtenemos a.

Potencia de exponente racional de un número real no negativo

Sea $\mathbb{R}^+ = \{\ x \in \mathbb{R} : x \geq 0\ \}$ el conjunto de los reales no negativos, $x \in \mathbb{R}^+$ y $r = \frac{m}{n} \in \mathbb{Q}$.
Definimos la potencia r-ésima de x de la siguiente manera:

(PQ1) Si $x \neq 0$ entonces $x^0 = 1$.

(PQ2) Si $r = \frac{m}{n} > 0$, $m > 0$, $n > 0$, entonces $x^r = x^{\frac{m}{n}} = \sqrt[n]{x^m}$.

(PQ3) Si $r < 0$ y $x \neq 0$ entonces $x^r = \dfrac{1}{x^{-r}}$.

Conviene hacer una observación. El número racional r se puede escribir de muchas maneras (infinitas) como cociente de enteros: $r = \frac{m}{n} = \frac{m'}{n'}$. No es difícil probar, usando las propiedades de la radicación, que la definición dada no depende de la forma de representar r.

Sean $x, y \in \mathbb{R}^+$, $r, s \in \mathbb{Q}$. Entonces se verifican las siguientes propiedades:

(1) $x^{r+s} = x^r \cdot x^s$.

(2) $x^{r \cdot s} = (x^r)^s$.

(3) $(x \cdot y)^r = x^r \cdot y^r$.

(4) $\left(\frac{x}{y}\right)^r = \frac{x^r}{y^r}$, $y \neq 0$.

Para probar estas propiedades, basta escribir $r = \frac{m}{n}$, $s = \frac{p}{q}$ y aplicar las propiedades ya conocidas.

También se puede definir la *potencia de exponente real* de un número real no negativo. Este es un punto delicado de la teoría del número real, que no abordaremos aquí. Digamos, solamente a título informativo, que todo número real positivo se puede aproximar tanto como se quiera por números racionales $r > 0$, y entonces se define la potencia a^x (con $a > 0$) por medio de sus aproximaciones a^r. Así por ejemplo, $\sqrt{2}$ puede aproximarse por los números racionales 1, $1,4$, $1,41$ $1,414$, $1,4142$, etc. Entonces las potencias de exponente racional a^1, $a^{1,4}$, $a^{1,41}$ $a^{1,414}$, $a^{1,4142}$, etc. son aproximaciones a la potencia de exponente real $a^{\sqrt{2}}$.

5.6 Ejercicios

1. Determinar, justificando la respuesta, cuáles de las siguientes afirmaciones son verdaderas y cuáles son falsas:

   Si $x < a < 0$ entonces :

   (i) $x^2 < a\,x < 0$.

   (ii) $x^2 > a\,x > a^2$.

   (iii) $x^2 > a\,x$ y $a\,x < 0$.

2. Demostrar las siguientes afirmaciones:

   (i) Si $b > 0$, entonces $a - b < a < a + b$.

   (ii) Si $0 < a < 1$, entonces $a^2 < a$.

   (iii) Si a y b son positivos y $a^2 < b^2$, entonces $a < b$.
   (Sugerencia: utilizar la igualdad $b^2 - a^2 = (b + a)(b - a)$).

   (iv) $(a + b)^2 = a^2 + b^2$ si y sólo si $a = 0$ ó $b = 0$.

3. Mostrar que si $x \in \mathbb{R}$ y $x > 0$ entonces $\dfrac{1}{x} + x \geq 2$. (Ayuda: $(x - 1)^2 \geq 0$).

4. La expresión $\dfrac{a^2 - b^2}{a\,b} - \dfrac{a\,b - b^2}{a\,b - a^2}$ simplificada es :

   (i) $\dfrac{a}{b}$ (ii) a^2 (iii) $\dfrac{a^2 - 2\,b^2}{a\,b}$ (iv) $a - 2\,b$

   ¿ o ninguna de las anteriores ?

5. (a) Hallar los valores $x \in \mathbb{R}$ que satisfacen las siguientes ecuaciones y verificar las soluciones.

   (i) $4\,(x + 3) - 3\,(2\,x - 5) = 6 - x - 2\,(3 - x)$ (ii) $\dfrac{(x + 1)\,(x^2 - 1)}{x - 1} = 0$

   (iii) $\dfrac{1}{x - 1} + \dfrac{2}{x - 3} = \dfrac{3\,x - 5}{(x - 1)\,(x - 3)}$ (iv) $\dfrac{2\,x^2 - 2\,x^3 + 8}{x^2} + 2\,x = 2$

   b) Resolver las siguientes inecuaciones:

   (i) $\dfrac{x + 1}{4} < \dfrac{5}{2} - \dfrac{1 - 2\,x}{3}$ (ii) $\dfrac{6 - 5\,x}{5} + \dfrac{3\,x - 1}{2} > 5 - x$

   (iii) $4\,x - 3 \leq 4\,(x - 7)$ (iv) $4\,x - 2 \leq 4\,(x + 1)$

6. Hallar los valores reales de x que verifican simultáneamente las dos inecuaciones:

   (a) $\begin{cases} x \geq 0 \\ 3\,x - 2 < 0 \end{cases}$ (b) $\begin{cases} x \geq 4 \\ -x + 2 \leq \dfrac{1}{2} \end{cases}$ (c) $\begin{cases} x - 1 < 2\,x + 3 \\ 4 - 2\,x > x + 1 \end{cases}$

7. Resolver las siguientes inecuaciones:

(a) $(x+1)(2x+3) < 0$ (b) $\dfrac{1}{x-1} \geq 1$ (c) $\dfrac{3}{x+4} + \dfrac{1}{x-4} \geq 0$

(d) $x^3(x-1) \leq 0$ (e) $-2(3x+1)(2x-3) > 0$ (f) $x^2 + 3x < 0$

(g) $\dfrac{x+2}{5-x} - 1 \geq 0$

8. Resolver las siguientes desigualdades, donde $b > 0$:
   (i) $|x-a| < b$ (ii) $|x-a| > b$.
   Dar una interpretación geométrica de las soluciones.

9. Resolver las siguientes ecuaciones y desigualdades:
   (a) $|3x-4| = \dfrac{1}{2}$ (b) $2 \cdot |4-3x| \leq 1$
   (c) $|x-3| > -1$ (d) $-2 \cdot |2x+1| < -4$
   (e) $||x+1|+2| = 2$ (f) $|x| + x^3 = 0$
   (g) $|x-2| < \dfrac{x}{2}$ (h) $(x+1) \cdot (|x|-1) = -\dfrac{1}{4}$
   (i) $|x-1| - |x| = 2$ (j) $-3 \cdot (x-2)^2 + 5 > 0$

10. Escribir las siguientes desigualdades en términos de valor absoluto:
    (a) $x^2 + 5x > 0$
    (b) $x^2 - 2x < 0$
    (c) $x^2 - x - 2 > 0$
    (d) $x^2 + 5x + 7 < 0$

11. Expresar en términos de valor absoluto:
    (a) $x \in (-3, 3)$
    (b) $x \in (2, 6)$
    (c) $x \in [-4, 8]$

12. Encontrar el primer elemento de los siguientes subconjuntos de $\mathbb{N}$:
    (a) $A = \{n \in \mathbb{N} : n > 2\}$ (b) $B = \{n \in \mathbb{N} : n^2 \geq 20\}$
    (c) $C = \{n \in \mathbb{N} : n^2 + n > 10\}$ (d) $D = \{n \in \mathbb{N} : n \neq 1, 2, 4, 8\}$

13. En cada uno de los siguientes casos, decir si el conjunto X tiene una cota inferior. Si tiene una cota inferior, hallar su primer elemento.
    (a) $X = \{x : x \in \mathbb{Z}, x^2 \leq 16\}$
    (b) $X = \{x : x \in \mathbb{Z}, x = 2k, \text{ para algún } k \in \mathbb{Z}\}$
    (c) $X = \{x : x \in \mathbb{Z}, x^2 \leq 100x\}$

14. Demostrar, usando el principio de inducción, que para todo $n \in \mathbb{N}$:
    (a) $1 + t + t^2 + \ldots + t^{n-1} = \dfrac{t^n - 1}{t-1}, \quad t \in \mathbb{R},\ t \neq 1.$
    (b) $1 + 3 + 5 + \ldots + (2n-1) = n^2.$

(c) $1 + 2 + 4 + \ldots + 2^{n-1} = 2^n - 1$.

(d) $1 + \dfrac{1}{2} + \dfrac{1}{4} + \ldots + \dfrac{1}{2^{n-1}} = 2 - 2^{1-n}$.

(e) $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \dfrac{1}{3 \cdot 4} + \ldots + \dfrac{1}{n \cdot (n+1)} = \dfrac{n}{n+1}$.

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

(g) $4(1^3 + 2^3 + 3^3 + \ldots + n^3) = n^2(n+1)^2$.

(h) $\dfrac{1}{3} + \dfrac{2}{3^2} + \dfrac{2^2}{3^3} + \ldots + \dfrac{2^{n-1}}{3^n} = 1 - \left(\dfrac{2}{3}\right)^n$.

(i) $1 + 2 \cdot 3 + 3 \cdot 3^2 + \ldots + n \cdot 3^{n-1} = \dfrac{1 + (2n-1) \cdot 3^n}{4}$.

(j) $\dfrac{1}{2} + 2 + 6 + \ldots + n \cdot 2^{n-2} = \dfrac{1 + (n-1) \cdot 2^n}{2}$.

Para los incisos (b) y (c), indicar el cuarto término de la suma y verificar la igualdad para $n = 4$.

15. Reescribir cada una de las siguientes sumas usando el símbolo de sumatoria:

(i) $1 + 2 + 3 + 4 + \cdots + 100$

(ii) $1 + 2 + 4 + 8 + 16 + \cdots + 1024$

(iii) $1 + (-4) + 9 + (-16) + 25 + \cdots + (-144)$

(iv) $1 + 9 + 25 + 49 + \cdots + 441$

16. Probar que las siguientes igualdades son verdaderas para todo $n \in \mathbb{N}$.

(i) $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$

(ii) $\displaystyle\sum_{i=1}^{n} (-1)^{i+1} \cdot i^2 = \frac{(-1)^{n+1} n(n+1)}{2}$

(iii) $\displaystyle\sum_{i=1}^{n} (2i+1) \cdot 3^{i-1} = n \cdot 3^n$

(iv) $\displaystyle\sum_{i=1}^{n} \frac{i \cdot 2^i}{(i+1)(i+2)} = \frac{2^{n+1}}{n+2} - 1$

17. Probar por inducción que para todo $n \in \mathbb{N}$ se verifican las siguientes desigualdades:

(a) $n < 2^n$.

(b) $3^n \geq 1 + 2^n$.

(c) $n^2 \geq n$.

18. Probar, usando el principio de inducción, que para todo $n \in \mathbb{N}$:

(a) $4^n - 1$ es múltiplo de 3.

(b) $n^2 + n$ es múltiplo de 2.

(c) $6^n - 1$ es múltiplo de 5.

(d) $10^n - 1$ es múltiplo de 9.

(e) $n^3 + 5\,n$ es múltiplo de 6.

(f) $n^3 + 2n$ es divisible por 3.

(g) $n^2 + (n+1)^2$ no es divisible por 2.

(h) Si $b \in \mathbb{R}$ y $b + 1 > 0$, entonces $(1+b)^n \geq 1 + nb$.

19. Demostrar que cualquier conjunto con n elementos contiene 2^n subconjuntos.

20. Demostrar que la suma de los ángulos interiores de un polígono convexo de $n+2$ lados es $n \cdot 180°$.

21. (a) Sea $P(n) : 2 + 5 + 8 + \cdots + (3n-1) = \dfrac{(3n+4)(n-1)}{2}$.

Probar que si $P(n)$ es válida para $n = k$ entonces es válida para $n = k+1$. Sin embargo, la fórmula es falsa para todo n. ¿Por qué?

(b) Idem para $P(n) : 1 + 5n = 7 + 5n$.

22. Sea $P(n)$ la proposición sobre el número natural n definida de la siguiente manera:

$P(1) = 2$

$P(n) : 2 + 2 \cdot 2! + 3 \cdot 3! + \ldots + n \cdot n! = (n+1)!$, si $n > 1$.

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

23. Para cada uno de los siguientes subconjuntos numéricos:

(i) Decir si es acotado superiormente o inferiormente, y en tal caso, indicar dos cotas superiores y dos cotas inferiores.

(ii) En el caso que el conjunto sea acotado superiormente (inferiormente) determinar el supremo (ínfimo) e indicar si pertenece o no al subconjunto numérico en cuestión.

(iii) Decir si tienen primer o último elemento.

(a) $\{x \in \mathbb{R} : -2 < x \leq 9\}$ (b) $\{x \in \mathbb{Z} : -2 < x \leq 9\}$

(c) $\{x \in \mathbb{R} : x < x^2\}$ (d) $\{x \in \mathbb{Z} : x < 2x\}$

(e) $\{x \in \mathbb{Q} : x < \dfrac{x}{2}\}$ (f) $\{x \in \mathbb{Q} : x = \dfrac{1}{n},\ n \in \mathbb{N}\}$

24. Analizar la validez de las siguientes proposiciones:

(a) Si n es un número natural y a un número real no natural entonces $n + a$ no es natural.

(b) Si m es un entero y a un número real no entero entonces $m + a$ no es entero.

25. Probar que:

(a) $\sqrt{3}$, $\sqrt[3]{2}$ y $\sqrt{2} + \sqrt{5}$ son irracionales.

(b) Si r es racional y t irracional entonces $r + t$ y $r\,t$ son irracionales ($r \neq 0$ en el segundo caso).

26. Encontrar dos números irracionales cuya suma sea racional. En forma análoga para la diferencia, el producto y el cociente.
¿Es cerrado el conjunto de los números irracionales respecto a la suma y al producto?

27. Demostrar que :

(a) Si a es irracional entonces $-a$ y a^{-1} son irracionales.

(b) Si a es irracional y $a > 0$ entonces $\sqrt{a}$ es irracional.

(c) Si $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$ y $\sqrt{a\,b}$ es irracional entonces $\sqrt{a} - \sqrt{b}$ es irracional.

28. Resolver :

(a) $\sqrt{10 - 3\sqrt[4]{\frac{1}{100}}}\,\sqrt{10 + 3\sqrt[4]{\frac{1}{100}}}$

(b) $\dfrac{\sqrt{a}}{\sqrt[3]{x^2}}\,\dfrac{\sqrt[3]{x}}{\sqrt{2\,a}}$

(c) $\left(\sqrt{3} - \dfrac{\sqrt{12}}{2} - \dfrac{2}{3}\sqrt{27} + \dfrac{5}{12}\sqrt{48}\right)\sqrt{3}$

(d) $\left(\dfrac{4}{9}\right)^{\frac{3}{4}}\,\left(\dfrac{4}{9}\right)^{-1}\,\left(\dfrac{4}{9}\right)^{\frac{1}{4}}$

(e) $3^{\frac{1}{2}}\;\;3^{-2}\;\;3^{\frac{2}{5}}\;\;3$

(f) $\left(\dfrac{9}{16}\right)^{-3} : \left(\dfrac{9}{16}\right)^{-\frac{5}{2}}$

(g) $\left(a^{-\frac{1}{2}} + b^{-\frac{1}{2}}\right)\,\left(a^{-\frac{1}{2}} - b^{-\frac{1}{2}}\right)$

(h) $\left[\left(\dfrac{1}{125}\right)^{\frac{3}{2}}\right]^{\frac{4}{9}}$

(i) $\left[\left(\dfrac{1}{100}\right)^{\frac{5}{4}}\right]^{-2}\,\left[\left(\dfrac{1}{100}\right)^{-\frac{3}{4}}\right]^{-\frac{3}{4}}$

(j) $\left[\left(\dfrac{1}{16}\right)^{3}\right]^{-\frac{1}{4}}$

29. Escribir bajo la forma de una potencia de x las siguientes expresiones:

(a) $x^{-2}\sqrt[3]{x^2\sqrt{x^{-7}}}$

(b) $\dfrac{x^{-\frac{1}{4}}\sqrt{x}}{\sqrt[3]{x\sqrt{x}}}$

30. (a) La expresión $\dfrac{2^{n+4} - 2\,\cdot\,2^n}{2\,\cdot\,2^{n+3}}$ simplificada es :

(i) $2^{n+1} - \dfrac{1}{8}$ (ii) -2^{n+1} (iii) $1 - 2^n$ (iv) $\dfrac{7}{8}$ ó (v) $\dfrac{7}{4}$?

(b) $2^{-(2k+1)} - 2^{-(2k-1)} + 2^{-2k}$ es igual a:

(i) 2^{-2k} (ii) $2^{-(2k-1)}$ ó (iii) $-2^{-(2k+1)}$?

(c) $\dfrac{1^{4n-1}}{5^{-1} + 3^{-1}}$ es igual a :

(i) $\dfrac{4n-1}{8}$ (ii) 8 (iii) $\dfrac{15}{2}$ (iv) $\dfrac{15}{8}$ ó v) $\dfrac{1}{8}$?

(d) $\sqrt{\dfrac{4}{3}} - \sqrt{\dfrac{3}{4}}$ es igual a:

(i) $\dfrac{\sqrt{3}}{6}$ (ii) $-\dfrac{\sqrt{3}}{6}$ (iii) $\dfrac{5}{6}\,\sqrt{3}$ ó iv) 1 ?

31. Calcular:

(a) $\dfrac{2^{2^n}}{2}$ (b) $\dfrac{2^{2^n}}{2^{2^m}}$ (c) $\left(2^{2^n}\right)^2$

(d) $2^{2^n}+2^{2^n}$ (e) $\left[\sqrt[3]{\sqrt[6]{a^9}}\ \right]^4\ \left[\sqrt[6]{\sqrt[3]{a^9}}\ \right]^4$

32. Indicar cuáles de la siguientes afirmaciones son verdaderas y cuáles son falsas, justificando las respuestas :

(a) $3\cdot 2^k+5\cdot 2^k=5^k+7^k$ (b) $3\cdot 2^k+5\cdot 2^k=6^k+10^k$ (c) $3\cdot 2^k+5\cdot 2^k=2^{k+3}$

6 Divisibilidad de enteros

En este capítulo estudiaremos propiedades de los números enteros. Esta área de la Matemática, conocida como *teoría de números*, es una de las más antiguas: nació hace más de 2500 años, con el comienzo de la matemática griega. Se podría pensar que después de tantos años de investigación se debería conocer todo acerca de la teoría de los números. Sin embargo, eso no es así: existen aún problemas de muy simple y natural formulación cuya respuesta aún no se conoce. Y hay algunos cuya solución se ha obtenido recién en los últimos años. Mencionemos sólo dos de los más famosos: la *conjetura de Goldbach* ("todo número par mayor que 2 puede ser escrito como suma de dos números primos," por ejemplo, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, etc.), el *último teorema de Fermat* ("no existen números naturales n, x, y, z tal que $n > 2$ y $x^n + y^n = z^n$"). En junio de 1993, *Andrew Wiles*, profesor de Princeton, anunció durante una conferencia en Cambridge que había probado la llamada *conjetura de Shimura-Taniyama*, de la cual el último teorema de Fermat es una consecuencia.

Comenzamos recordando la definición de la relación "divide".

Definición 6.1 *Sean* $a, b \in \mathbb{Z}$. *Se dice que* a *divide a* b, *y escribimos* $a \mid b$ *(con una barra vertical), si existe* $k \in \mathbb{Z}$ *tal que* $b = a \cdot k$.

En este caso diremos también que a *es un factor* de b, que b *es divisible* por a ó que b *es múltiplo* de a .

Si a no divide a b escribimos $a \nmid b$.

Ejemplo. $3 \mid 12$, $8 \mid 32$, $2 \mid -2$, $-3 \mid 9$, $7 \mid 49$, $5 \nmid 3$, $11 \nmid 35$.

Propiedades de la relación divide. Las siguientes propiedades se prueban en forma inmediata a partir de la definición:

Para todo $a, b, c \in \mathbb{Z}$ se tiene:

(1) $a \mid a$.

(2) Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

(3) $a \mid 0$.

(4) Si $c \mid a$ y $c \mid b$ entonces $c \mid ax + by$, $x, y \in \mathbb{Z}$.

(5) Si $a \mid b$ entonces $a \mid -b$, $-a \mid b$ y $-a \mid -b$.

(6) Si $a \mid b$ entonces $ac \mid bc$.

(7) Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$.

(8) $a \mid b$ y $b \mid a \Longleftrightarrow |a| = |b|$.

Observaciones.

(1) $c \mid a + b$ no implica que $c \mid a$ ó $c \mid b$. Por ejemplo, $6 \mid 4 + 8$, pero $6 \nmid 4$ y $6 \nmid 8$.

(2) Sin embargo, si $c \mid a + b$ y se sabe que $c \mid a$ entonces $c \mid b$ (pues $c \mid (a + b) - a$).

(3) Si $c \mid a$, entonces $c \mid k \cdot a$ para todo $a \in \mathbb{Z}$.

(4) Si $c \mid a$, entonces $c \mid a^2$ y $c \mid a^n$ para todo $n \in \mathbb{N}$.

Ejercicio. Decir si son verdaderas o falsas las siguientes proposiciones. Justificar.

(a) Si un número es divisible por 4 entonces es divisible por 2.

(b) Si un número es divisible por 2 entonces es divisible por 4.

(b) Si un número es divisible por 4 entonces no es divisible por 8.

(c) Si un número no es divisible por 4 entonces no es divisible por 8.

(d) Si un número es divisible por 15 entonces no es divisible ni por 3 ni por 5.

(e) Si un número es divisible por 6 entonces es divisible por 2 ó por 3.

(f) Si un número es divisible por 2 ó por 3 entonces es divisible por 6.

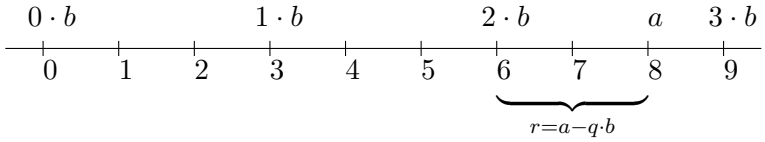
6.1 Algoritmo de la división entera

Teorema 6.2 (Algoritmo de la división entera). *Dados dos enteros a y b, $b \neq 0$ existen enteros q y r, llamados respectivamente el cociente y el resto de dividir a por b, unívocamente determinados tales que:*

$$a = b \cdot q + r \quad con \quad 0 \leq r < |b|.$$

Antes de demostrar el resultado anterior, vamos a dar una interpretación geométrica del mismo.

Sean $a, b \in \mathbb{Z}$, $b > 0$. Representamos en el eje real a los múltiplos de b, es decir los enteros de la forma $q \cdot b$, donde $q \in \mathbb{Z}$. La idea consiste en encuadrar a a entre dos múltiplos consecutivos de b, es decir $a \in [\, q \cdot b, (q+1)b\,)$, para algún $q \in \mathbb{Z}$. En el gráfico consideramos el caso $a = 8$, $b = 3$.



Por lo tanto, tomando $r = a - q \cdot b$ se tiene $a = b \cdot q + r$, con $0 \leq r < b$.

Demostración. Comencemos por probar la existencia de los números q y r. Supongamos primero que $b > 0$. Consideremos el conjunto

$$A = \{x : x = a - b \cdot q,\ x \geq 0,\ q \in \mathbb{Z}\}.$$

$A \neq \emptyset$, ya que si tomamos $q = -|a|$, entonces $a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$. Luego, por el Principio de Buena Ordenación, A posee primer elemento $r = a - bq$. Veamos que este número r satisface las relaciones $0 \leq r < b$.

Que $0 \leq r$ es obvio, pues $r \in A$. Si fuese $r \geq b$ entonces tendríamos $0 \leq r - b = a - b(q+1)$, de donde resulta que $r - b \in A$, con $r - b < r$. Absurdo.

Supongamos ahora que $b < 0$. Entonces $-b > 0$, y por lo anterior, existen enteros q y r tales que

$$a = q(-b) + r, \quad \text{y} \quad 0 \leq r < -b.$$

Luego, como $|b| = -b$,

$$a = (-q)b + r, \quad \text{y} \quad 0 \leq r < |b|.$$

Probemos ahora la unicidad de los números q y r. Supongamos que existen enteros q, q', r, r', tales que

$$a = qb + r = q'b + r', \quad \text{con } 0 \leq r < |b|,\ 0 \leq r' < |b|.$$

Entonces, $(q - q')b = r' - r$, de donde, tomando valores absolutos, $|q - q'| \cdot |b| = |r' - r| < |b|$, por lo anterior.

Si fuese $r \neq r'$, entonces sería $|r - r'| \neq 0$ y $|q - q'| \neq 0$. De donde,

$$|b| \leq |q - q'| \cdot |b| = |r' - r|, \text{ lo cual es absurdo.}$$

□

Ejemplos.

1. Determinar el cociente y el resto en cada uno de los siguientes casos:

Si $a = 305$	y	$b = 13$	entonces	$q = 23$	y	$r = 6$	:	$305 = 23 \cdot 13 + 6$
Si $a = -12$	y	$b = -7$	entonces	$q = 2$	y	$r = 2$	:	$-12 = 2 \cdot (-7) + 2$
Si $a = -21$	y	$b = 5$	entonces	$q = -5$	y	$r = 4$	:	$-21 = (-5) \cdot 5 + 4$
Si $a = 5$	y	$b = 8$	entonces	$q = 0$	y	$r = 5$	:	$5 = 0 \cdot 8 + 5$
Si $a = 36$	y	$b = -5$	entonces	$q = -7$	y	$r = 1$	:	$36 = (-7) \cdot (-5) + 1$

2. Hallar el cociente y el resto de la división de $a = n^2 + 5$ por $b = n + 2$ $(n \in \mathbb{N})$.

   - Si $2 < n \leq 7$, $0 \leq 7 - n < n + 2$, y $n^2 + 5 = (n - 1)(n + 2) + (7 - n)$. En este caso $q = n - 1$ y $r = 7 - n$.
   - Si $n > 7$, entonces $n^2 + 5 = (n - 2)(n + 2) + 9$, y entonces $q = n - 2$ y $r = 9$.
   - Para $n = 1$, $q = 2$ y $r = 0$, y para $n = 2$, $q = 2$ y $r = 1$.

3. El resto de la división de a por 18 es 5. Hallar:

   (i) El resto de dividir $a^2 - 3a + 11$ por 18.
   De $a = q \cdot 18 + 5$, $a^2 = q_1 \cdot 18 + 25 = q_1' \cdot 18 + 7$. Además, $-3a = q_2 \cdot 18 - 15 = q_2 \cdot 18 - 15 + 18 - 18 = q_2' \cdot 18 + 3$. Por último, $11 = 0 \cdot 18 + 11$. Luego $a^2 - 3a + 11 = q_3 \cdot 18 + 7 + 3 + 11 = q_3' \cdot 18 + 3$.

   (ii) El resto de dividir a por 3.
   $a = q \cdot 18 + 5 = q \cdot 6 \cdot 3 + 3 + 2 = q_1 \cdot 3 + 2$.

Ejercicio. Si el resto de dividir un entero a por 5 es 3, calcular el resto de la división por 5 de: $3a$, $-a$, $2a + 5$, $-a + 2$, $5a + 2$, a^2, a^3.

6.2 Máximo común divisor y algoritmo de Euclides

Sea $a \in \mathbb{Z}$ y sea $D(a) = \{ c \in \mathbb{Z} :\ c \mid a\}$. Es claro que $D(a) = D(-a)$, para todo $a \in \mathbb{Z}$ y si $a \neq 0$, $D(a)$ es un conjunto finito.

Sean a, b dos enteros, y supongamos que al menos uno de ellos es distinto de cero. Indiquemos $D(a, b)$ el conjunto de todos los divisores comunes de a y b, es decir,

$$D(a, b) = \{c \in \mathbb{Z} : c \mid a \text{ y } c \mid b\}.$$

Es claro que $D(a,b) \neq \emptyset$, y como $D(a,b) = D(a) \cap D(b)$, se tiene que $D(a,b)$ es finito.

El mayor de todos los elementos de $D(a,b)$ se llama el *máximo común divisor* de a y b, y se nota (a,b).

Observemos que (a,b) es un entero positivo pues: $c \in D(a,b) \Leftrightarrow -c \in D(a,b)$.

Ejemplo. $(75,-12) = 3$, $(4,6) = 2$, $(3,2) = 1$, $(15,25) = 5$.

Observación: $(a,b) = (b,a) = (-a,b) = (a,-b) = (-a,-b)$.

La siguiente sencilla propiedad es la base del llamado ALGORITMO DE EUCLIDES, el cual es un procedimiento para hallar el máximo común divisor de dos números enteros no simultáneamente nulos.

Proposición 6.3 *Si a y b son enteros, $b \neq 0$ y r es el resto de dividir a por b entonces $D(a,b) = D(b,r)$.*

Demostración. Sea q el cociente y r el resto de dividir a por b:

$$a = bq + r, \quad 0 \leq r < |b| \ ; \ \text{esto es} \quad r = a - bq.$$

De la propiedad (4) de la relación divide, resulta fácilmente que $D(a,b) = D(b,r)$. □

Corolario 6.4 $(a,b) = (b,r)$.

Observación: Si $b \mid a$ y $b \neq 0$, entonces $r = 0$, y por lo tanto, $(a,b) = (b,0) = |b|$.

Ejemplo. Hallemos el máximo común divisor de 216 y 80. Como $216 = 2 \cdot 80 + 56$, entonces $(216,80) = (80,56)$. Reiterando el procedimiento obtenemos:

$$(216,80) = (80,56) = (56,24) = (24,8) = 8.$$

El ejemplo anterior ilustra el procedimiento que se utiliza para hallar el máximo común divisor de dos números no simultáneamente nulos. Lo exponemos a continuación en forma general.

Algoritmo de Euclides (Existencia del máximo común divisor)

Sean a y b dos enteros no simultáneamente nulos. Como $(a,b) = (a,-b)$, podemos suponer sin pérdida de generalidad que $b > 0$.

Sea r_1 el resto de dividir a por b. Si $r_1 = 0$ entonces $b \mid a$ y entonces $(a,b) = |b| = b$. Si $r_1 \neq 0$ por divisiones sucesivas obtenemos:

$$\begin{array}{lcll}
a & = & b \cdot q_1 + r_1 & 0 < r_1 < b \\
b & = & r_1 \cdot q_2 + r_2 & 0 < r_2 < r_1 \\
r_1 & = & r_2 \cdot q_3 + r_3 & 0 < r_3 < r_2 \\
 & \vdots & & \vdots \\
r_{n-2} & = & r_{n-1} \cdot q_n + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} & = & r_n \cdot q_{n+1} &
\end{array}$$

donde, como $b > r_1 > r_2 > \cdots \geq 0$, al cabo de un número finito de divisiones se obtiene un resto nulo, es decir,

$$r_{n-1} = r_n \cdot q_{n+1}.$$

(de lo contrario habría infinitos enteros positivos menores que b).

Veamos que $r_n = (a, b)$. En efecto, como $r_n \mid r_{n-1}$, aplicando el corolario anterior reiteradamente obtenemos:

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \cdots = (r_2, r_3) = (r_1, r_2) = (b, r_1) = (a, b).$$

Este algoritmo se puede esquematizar mediante la siguiente tabla:

	q_1	q_2	q_3			q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots\cdots\cdots$	r_{n-3}	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3			r_{n-1}	r_n	0	

El último resto no nulo es el máximo común divisor. Si el resto es cero en la primera división, es decir, si a es un múltiplo de b, entonces $(a, b) = b$ (estamos suponiendo que $b > 0$). En este caso convenimos en que el último resto no nulo es b.

Vamos a probar ahora una importante consecuencia del algoritmo de Euclides.

Teorema 6.5 *Dados $a, b \in \mathbb{Z}$, $b \neq 0$, existen enteros x e y tales que $(a, b) = xa + yb$.*

Demostración. Supongamos de nuevo, sin pérdida de generalidad, que $b > 0$.

Si $r_1 = 0$, entonces $(a, b) = b = 0 \cdot a + 1 \cdot b$.

Si $r_1 \neq 0$, probemos que cada resto r_k es de la forma $r_k = x_k \cdot a + y_k \cdot b$, $x_k, y_k \in \mathbb{Z}$.

De $a = q_1 b + r_1$ obtenemos

$$r_1 = a - q_1 b = 1 \cdot a + (-q_1) \cdot b = x_1 \cdot a + y_1 \cdot b, \text{ donde } x_1 = 1 \text{ e } y_1 = -q_1.$$

De $b = q_2 r_1 + r_2$ obtenemos

$$r_2 = b - q_2 r_1 = b - q_2(x_1 a + y_1 b) = (-q_2 x_1) \cdot a + (1 - q_2 y_1) \cdot b = x_2 a + y_2 b$$

Supongamos que todos los restos, hasta r_k inclusive, son de la forma indicada. En particular,

$$r_{k-1} = x_{k-1} \cdot a + y_{k-1} \cdot b, \quad r_k = a x_k + b y_k.$$

De $r_{k-1} = q_{k+1} r_k + r_{k+1}$ resulta

$$\begin{aligned} r_{k+1} = r_{k-1} - q_{k+1} r_k &= (x_{k-1} a + y_{k-1} b) - q_{k+1}(x_k a + y_k b) \\ &= \underbrace{(x_{k-1} - q_{k+1} x_k)}_{x_{k+1}} a + \underbrace{(y_{k-1} - q_{k+1} y_k)}_{y_{k+1}} b \\ &= x_{k+1} a + y_{k+1} b \end{aligned}$$

Esto prueba que reiterando el razonamiento, podemos llegar a la igualdad

$$r_n = x_n a + y_n b,$$

es decir, como $r_n = (a, b)$,

$$(a, b) = x_n a + y_n b.$$

□

Observaciones:

1. De $(a, b) = xa + yb$ resulta que si $d \in D(a, b)$, entonces $d \mid (a, b)$.
2. Los enteros x e y del teorema anterior no son únicos. Por ejemplo, si $a = 1$ y $b = 1$, $(1, 1) = 1 = (-1) \cdot 1 + 2 \cdot 1 = 0 \cdot 1 + 1 \cdot 1 = 4 \cdot 1 + (-3) \cdot 1 = \cdots$
3. Como $(a, b) = (-a, b) = (a, -b) = (-a, -b)$, para calcular el máximo común divisor de dos números enteros a y b, podemos aplicar el algoritmo directamente a los números $|a|$ y $|b|$.

Ejemplos.

1. Si $a = 134$ y $b = 18$ tenemos:

	7	2	4
134	18	8	2
8	2	0	

Por lo tanto, $d = 2 = (134, 18)$.

Expresémoslo como combinación lineal de 134 y 18 .

$$\begin{aligned} 134 &= 18 \cdot 7 + 8 \\ 18 &= 8 \cdot 2 + 2 \\ 2 &= 18 - 8 \cdot 2 = 18 - (134 - 18 \cdot 7) \cdot 2 = (-2) \cdot 134 + 15 \cdot 18 = 134\, x + 18\, y. \end{aligned}$$

2. Sean $a = 2137$ y $b = -623$.

	3	2	3	12	2	3
2137	623	268	87	7	3	1
268	87	7	3	1	0	

Luego $(2137, -623) = 1$.

Hallemos números enteros x, y tales que $1 = x \cdot 2137 + y \cdot (-623)$.

$$\begin{aligned} 2137 &= 3 \cdot 623 + 268 \\ 623 &= 2 \cdot 268 + 87 \\ 268 &= 3 \cdot 87 + 7 \\ 87 &= 12 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

Luego, despejando los restos:

$$\begin{aligned}
268 &= 2137 - 3 \cdot 623 \\
87 &= 623 - 2 \cdot 268 = 623 - 2 \cdot (2137 - 3 \cdot 623) = -2 \cdot 2137 + 7 \cdot 623 \\
7 &= 268 - 3 \cdot 87 = 2137 - 3 \cdot 623 - 3 \cdot (-2 \cdot 2137 + 7 \cdot 623) = 7 \cdot 2137 - 24 \cdot 623 \\
3 &= 87 - 12 \cdot 7 = -2 \cdot 2137 + 7 \cdot 623 - 12 \cdot (7 \cdot 2137 - 24 \cdot 623) = -86 \cdot 2137 + 295 \cdot 623 \\
1 &= 7 - 2 \cdot 3 = 7 \cdot 2137 - 24 \cdot 623 - 2 \cdot (-86 \cdot 2137 + 295 \cdot 623) = 179 \cdot 2137 - 614 \cdot 623
\end{aligned}$$

Luego el máximo común divisor se escribe: $1 = 179 \cdot 2137 + 614 \cdot (-623)$.

Vamos a dar ahora otra definición equivalente de máximo común divisor de dos enteros, que puede ser en ciertos casos más conveniente.

Proposición 6.6 *Dados dos enteros a y b no simultáneamente nulos, un entero positivo d es el máximo común divisor de a y b si y sólo si d verifica las siguientes propiedades:*

1. $d \mid a$ *y* $d \mid b$.
2. *Si d' es un entero tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.*

Demostración. Supongamos que $d = (a, b)$. Entonces es claro que d verifica 1. Además, como $d = xa + yb$, con $x, y \in \mathbb{Z}$, si d' es un entero tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid xa + yb$, esto es, $d' \mid d$. Luego d verifica 2.

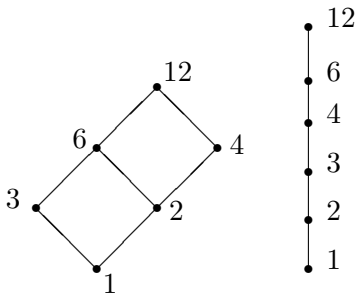
Recíprocamente, supongamos que d es un entero positivo que verifica 1 y 2. Por 1, d es un divisor común de a y b. Por 2, d es el mayor de los divisores comunes. En efecto, si d' es un divisor común de a y b, entonces $d' \mid d$, luego por la propiedad 7, $|d'| \leq d$, o sea, $d' \leq d$. Luego $d = (a, b)$. □

La proposición anterior nos permite dar también la siguiente definición de máximo común divisor:

Dados dos enteros a y b no simultáneamente nulos, un entero positivo d se llama *máximo común divisor* de a y b si d verifica las siguientes propiedades:

1. $d \mid a$ y $d \mid b$.
2. Si d' es un entero tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

Nota: Sobre el conjunto de los divisores positivos comunes a a y a b, podemos considerar dos relaciones de orden diferentes: el orden dado por la relacion divide $\mid$ y el orden natural $\leq$. La Proposición 6.6 asegura que el máximo común divisor de a y b es el último elemento en ambas ordenaciones. Así por ejemplo, el conjunto de los divisores positivos comunes de 24 y 36 es $\{1, 2, 3, 4, 6, 12\}$. Ordenando este conjunto por las relaciones "$\mid$" y "$\leq$" se tienen respectivamente los siguientes diagramas:



En ambos casos el último elemento es 12, que es el máximo común divisor de 24 y 36.

Definición 6.7 *Dos enteros* a *y* b *se dicen relativamente primos o coprimos si* $(a,b)=1$.

Ejemplo. $(2,3)=1$, $(5,8)=1$, $(6,35)=1$.

Proposición 6.8 (Euclides). *Sean* $a,b,c\in\mathbb{Z}$. *Si* $c\mid a\cdot b$ *y* $(a,c)=1$ *entonces* $c\mid b$.

Demostración. Si $(a,c)=1$ entonces $1=a\,x+c\,y$; $x,y\in\mathbb{Z}$. Luego $b=a\,b\,x+b\,c\,y$. Como $c\mid a\cdot b$ resulta $a\cdot b=c\cdot t$ y por lo tanto $b=c\,t\,x+b\,c\,y=c\underbrace{(t\,x+b\,y)}_{\in\mathbb{Z}}$ entonces $c\mid b$. □

Proposición 6.9 *Si* $a\mid n$ *y* $b\mid n$ *y* $(a,b)=1$, *entonces* $a\cdot b\mid n$.

Demostración. En efecto, si $a\mid n$, $n=k\cdot a$, $k\in\mathbb{Z}$. Si $b\mid n$, entonces $b\mid k\cdot a$. Como $(a,b)=1$, de la proposición anterior resulta $b\mid k$. Luego $k=k'\cdot b$, $k'\in\mathbb{Z}$. Reemplazando resulta $n=k'\cdot b\cdot a$, es decir, $a\cdot b\mid n$. □

Esta propiedad no vale si $(a,b)\neq 1$. Mostrar un contraejemplo.

Ecuaciones diofánticas.

Alrededor del siglo III (D.C.), el matemático griego Diofanto consideró ecuaciones de las cuales sólamente interesaban las soluciones enteras. Hay muchos problemas prácticos que se resuelven por ecuaciones donde las soluciones no enteras no tienen interpretación razonable (pensar por ejemplo cómo medir 8 litros de agua usando dos recipientes de 5 y 7 litros cada uno; esto da origen a la ecuación $5x+7y=8$). Una ecuación en una o más incógnitas con *coeficientes enteros* en la que interesa hallar solamente las *soluciones enteras* se llama una *ecuación diofántica*. La más simple es la ecuación lineal diofántica con dos incógnitas

$$ax+by=c,$$

donde a, b, $c\in\mathbb{Z}$, y se desean hallar números enteros x e y que la satisfagan. Vamos a probar ahora que la condición necesaria y suficiente para que la ecuación diofántica $ax+by=c$ tenga al menos una solución (entera) es que el máximo común divisor de a y b sea un divisor de c.

Proposición 6.10 *Sean* a, b, $c\in\mathbb{Z}$, a *y* b *no simultáneamente nulos. Entonces existen enteros* x, y *tales que* $a\,x+b\,y=c\iff(a,b)\mid c$.

Demostración. ($\Rightarrow$) Como $(a,b)\mid a$ y $(a,b)\mid b$ entonces $a=(a,b)t$ y $b=(a,b)t'$; $t,t'\in\mathbb{Z}$.
Tenemos que:
$c=a\,x+b\,y=(a,b)t\,x+(a,b)t'\,y=(a,b)(t\,x+t'\,y)=(a,b)s,\ s\in\mathbb{Z}\Longrightarrow(a,b)\mid c$.

($\Leftarrow$) Como $(a,b)\mid c$ entonces $c=(a,b)t=(a\,s+b\,s')t=a(s\,t)+b(s'\,t)$, por lo tanto $x=s\,t$, $y=s'\,t$ son los enteros buscados. □

Corolario 6.11 $(a,b)=1\iff a\,x+b\,y=1$, *para algún* $x,y\in\mathbb{Z}$.

Demostración. Si $(a,b)=1$, entonces existen enteros x e y tales que $xa+yb=1$. Para la recíproca, supongamos que existen enteros x e y tales que $xa+yb=1$. Si $d=(a,b)$, entonces, por Proposición 6.10, $d\mid 1$. Luego $d=1$, y por lo tanto $(a,b)=1$. □

Ejemplo. Hallemos una solución entera de la ecuación $129x-27y=21$. Calculemos en primer lugar el máximo común divisor entre 129 y -27.

	4	1	3	2
129	27	21	6	3
21	6	3	0	

Se tiene que $(129, -27) = 3$. Como $3 \mid 21$, la ecuación dada tiene solución. Para hallarla expresamos a 3 como combinación lineal de 129 y -27.

De $129 = 4 \cdot 27 + 21$, $27 = 1 \cdot 21 + 6$, $21 = 3 \cdot 6 + 3$, obtenemos:

$3 = 21 - 3 \cdot 6 = 21 - 3 \cdot (27 - 21) = 5 \cdot 21 - 3 \cdot 27 = 4 \cdot (129 - 4 \cdot 27) - 3 \cdot 27 = 4 \cdot 129 - 19 \cdot 27$, esto es, $3 = 4 \cdot 129 + 19 \cdot (-27)$. Multiplicando ambos miembros por 7 se tiene $21 = 28 \cdot 129 + 133 \cdot (-27)$. Por lo tanto, $x = 28$, $y = 133$ es una solución (entera) de la ecuación diofántica $129x - 27y = 21$.

Observación. Si la ecuación diofántica $ax + by = c$ tiene una solución (x_0, y_0), entonces todas las soluciones de esta ecuación están dadas por los pares de enteros (x, y) tales que

$$\begin{cases} x = x_0 + t \cdot b \\ y = y_0 - t \cdot a \end{cases}, \quad t \in \mathbb{Z} \qquad (*)$$

En efecto, es fácil ver que cualquier par de enteros de la forma $(*)$ satisface la ecuación, ya que $a(x_0 + t \cdot b) + b(y_0 - t \cdot a) = ax_0 + by_0 = c$.

Recíprocamente, supongamos que el par (x, y) es una solución de la ecuación $ax + by = c$. Podemos suponer que a y b son relativamente primos, porque si así no fuera, dividiríamos ambos miembros de la ecuación por el máximo común divisor de a y b. Como por hipótesis $ax_0 + by_0 = c$, restando las relaciones $ax + by = c$ y $ax_0 + by_0 = c$, obtenemos

$$a(x - x_0) + b(y - y_0) = 0,$$

o lo que es equivalente,

$$a(x - x_0) = b(y_0 - y). \qquad (**)$$

Por lo tanto, $a \mid b(y_0 - y)$, y como $(a, b) = 1$, $a \mid y_0 - y$, mientras que de la misma manera, $b \mid x - x_0$. Luego $y_0 - y = a \cdot t$ y $x - x_0 = b \cdot s$. Sustituyendo en $(**)$ se obtiene $abs = bat$, de donde $t = s$. Por consiguiente, debe ser $x = x_0 + t \cdot b$ e $y = y_0 - t \cdot a$, donde $t \in \mathbb{Z}$.

Geométricamente, la ecuación $ax + by = c$ representa una recta en el plano, y la solución diofántica consiste en hallar todos los puntos de coordenadas enteras que pertenecen a dicha recta.

Mínimo Común Múltiplo

Dado un número entero a, sea $M(a)$ el conjunto de todos los múltiplos no negativos de a. Así por ejemplo, $M(3) = \{0, 3, 6, 9, \ldots\}$, $M(0) = \{0\}$, $M(1) = \mathbb{N} \cup \{0\}$. Es claro que $M(a) \neq \emptyset$.

Sean a y b dos enteros y notemos $M(a, b)$ el conjunto de todos los múltiplos no negativos comunes de a y b. Es claro que $M(a, b) = M(a) \cap M(b)$. Vamos a probar el siguiente

Teorema 6.12 *Si a y b son dos enteros, entonces existe $m \in M(a, b)$ tal que si $c \in M(a, b)$, entonces $m \mid c$.*

Demostración. Si $a = b = 0$, $M(a,b) = \{0\}$ y $m = 0$ verifica el teorema. Supongamos que a y b no son simultáneamente nulos. Sean s y t tales que $a = (a,b) \cdot s$; $b = (a,b) \cdot t$. Se tiene que $(s,t) = 1$.

Sea

$$m = a \cdot t = (a,b) \cdot s \cdot t = b \cdot s.$$

Es claro que $m \in M(a,b)$.

Sea $c \in M(a,b)$, $c = a \cdot h$; $c = b \cdot k$, $h, k \in \mathbb{Z}$. Entonces $(a,b) \cdot s \cdot h = (a,b) \cdot t \cdot k$, de donde $s \cdot h = t \cdot k$.

Luego $s \mid t \cdot k$, y como $(s,t) = 1$, resulta $s \mid k$, es decir, $k = s \cdot l$. Por consiguiente, $c = b \cdot k = b \cdot s \cdot l = m \cdot l$. Luego $m \mid c$. □

El número m del teorema se llama el *mínimo común múltiplo* de los enteros a y b, y se nota $[a,b]$.

Observemos que de la demostración del teorema anterior resulta un procedimiento para calcular el mínimo común múltiplo de a y b no simultáneamente nulos, a saber,

$$[a,b] = \frac{|\, a \cdot b \,|}{(a,b)}.$$

Ejemplo. Calculemos el mínimo común múltiplo de 216 y 80.

	2	1	2	3
216	80	56	24	8
56	24	8	0	

Entonces $(216,80) = 8$ y por lo consiguiente $[216,80] = \dfrac{216 \cdot 80}{8} = 2160$.

6.3 Números primos

Si $a \in \mathbb{Z}$, a es divisible por $a, -a, 1, -1$, que se denominan los *divisores triviales* de a. Si a posee otro divisor, éste se llama un *divisor propio.*

Definición 6.13 *Un entero $a \neq 0, 1, -1$ se dice* **primo** *si sus únicos divisores son los triviales.*

Lo anterior es equivalente a decir que un entero es primo si posee *exactamente* 4 divisores.

Ejemplo. 2, 3, 5, 7, 11, 101 son números primos.

Si un entero $a \neq 0, \pm 1$ no es primo, se dice *compuesto.*

Teorema 6.14 *Todo número entero a distinto de 0, 1 y -1 admite por lo menos un divisor primo positivo.*

Demostración. Sea m el menor entero mayor que 1 que divide a a. Veamos que m es primo. Si m no fuera primo existiría $k \in \mathbb{Z}$ tal que $1 < k < m$ y $k \mid m$. Como $m \mid a$, resulta $k \mid a$, lo que contradice la definición de m. □

La siguiente propiedad ya era conocida por los antiguos griegos.

Teorema 6.15 (Euclides). *Existen infinitos números primos.*

Demostración. Basta efectuar la demostración para primos positivos. Supongamos por el absurdo que hay sólo un número finito de primos positivos. Notamos a los primos $p_1, p_2, \ldots, p_k$. Sea $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$. Entonces, como $n > 1$, existe un primo positivo p tal que $p \mid n$. Por la hipótesis se tiene que $p = p_i$ para algún i, $1 \leq i \leq k$. Como $p_i \mid p_1 \cdot p_2 \cdot \cdots \cdot p_i \cdot \cdots \cdot p_k$, entonces $p_i \mid n - p_1 \cdot p_2 \cdot \cdots \cdot p_k = 1$ lo que implica que $p_i = 1$. Absurdo, pues p_i es un número primo. □

Ejercicio. El teorema anterior también se puede demostrar de la siguiente manera. Los detalles se dejan como ejercicio. Para probar que hay infinitos primos basta probar que para todo número natural n, hay un primo $p > n$. Considerar el número $n! + 1$ ($n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1$, y se lee el factorial de n) y sea p cualquier divisor primo de $n! + 1$. Probar que $p > n$. Si fuera $p \leq n$, entonces $p | n!$. Como $p | n! + 1$, entonces p es un divisor de la diferencia, lo cual es imposible.

Nota. Un problema importante de la Aritmética es el de determinar cómo están distribuidos los números primos en la sucesión natural $1, 2, 3, \ldots$ Enseguida se observan grandes irregularidades. Por ejemplo, los números

$$k! + 2, \quad k! + 3, \quad k! + 4, \ldots, \quad k! + k, \quad k > 1,$$

son $k - 1$ números compuestos. En efecto, $k! + 2$ es divisible por 2, $k! + 3$ es divisible por 3, $\ldots$, $k! + k$ es divisible por k. Esto significa que en la sucesión de los números primos existen "lagunas" tan grandes como se desee.

Observación: Dado un número primo p y un entero a, o bien $(p, a) = 1$, o bien $p \mid a$.

Ejercicio. (La regla de oro de la Aritmética, según Gentile). Si p es primo y $p \mid a \cdot b$ entonces $p \mid a$ ó $p \mid b$. Esta propiedad no vale si p no es primo. (Dar el correspondiente contraejemplo).

Ejemplos.

1. Probar que si $n \in \mathbb{Z}$, entonces $2n + 1$ y $\frac{1}{2}n(n+1)$ son coprimos.
   Sea $d = (2n + 1, \frac{1}{2}n(n+1))$. Supongamos que $d \neq 1$ y sea p un primo que divide a d. Entonces $p \mid 2n + 1$ y $p \mid \frac{1}{2}n(n+1)$, esto es, $p \mid 2n + 1$ y $p \mid n(n+1)$. De $p \mid n(n+1)$, como p es primo resulta que $p \mid n$ ó $p \mid n + 1$. Luego se tiene,
   $p \mid 2n + 1$ y $p \mid n$, en cuyo caso $p \mid 1$, lo cual es imposible, ó
   $p \mid 2n + 1$ y $p \mid n + 1$, que conduce a la misma contradicción.
   Luego $d = 1$

2. Probar que si $(a, b) = 1$ y $n + 2$ es un número primo, entonces $(a + b, a^2 + b^2 - nab)$ es 1 ó $n + 2$.
   Sea $d = (a + b, a^2 + b^2 - nab)$ y supongamos que $d \neq 1$. Sea p un número primo tal que $p \mid d$. Entonces $p \mid a + b$ y $p \mid a^2 + b^2 - nab = (a + b)^2 - 2ab - nab = (a + b)^2 - ab(n + 2)$. Luego $p \mid ab(n + 2)$. Como p es primo, $p \mid ab$ ó $p \mid n + 2$, esto es, $p \mid ab$ ó $p = n + 2$ dado que $n + 2$ es primo.
   Si suponemos que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$, pero como $p \mid a + b$, entonces p divide a ambos, lo cual no es posible porque $(a, b) = 1$.
   Luego $p = n + 2$, esto es, el único primo que divide a d es $n + 2$. Puede verse que $(n + 2)^2$ no divide a d, y en consecuencia, $d = n + 2$.

Teorema 6.16 (Teorema Fundamental de la Aritmética). *Todo número entero a distinto de $0, 1, -1$, o bien es un número primo, o bien se puede escribir como ± 1 por un producto de números primos positivos. Esta representación de un entero como producto de primos es única, salvo el orden de los factores.*

Demostración. Es suficiente probar el Teorema para el caso $a > 1$. Sea A el conjunto de todos los números enteros positivos que no verifican el Teorema, esto es, no son primos y no pueden representarse como producto de números primos. Queremos probar que $A = \emptyset$. Supongamos por el absurdo que $A \neq \emptyset$. Por el Principio de Buena Ordenación, A tiene primer elemento m. Sea p un divisor primo positivo de m. Se tiene $m = pk$, con $1 < k < m$, de donde resulta que $k \notin A$. Entonces el número k o bien es primo, o bien es producto de números primos. En ambos casos se obtiene una contradicción.

Probemos ahora la unicidad. De nuevo usaremos el Principio de Buena Ordenación. Supongamos por el absurdo que existen enteros positivos que se pueden expresar como producto de números primos de dos formas diferentes. Sea m el menor de tales números. Entonces

$$m = p_1 p_2 \cdot \cdots \cdot p_r = q_1 q_2 \cdot \cdots \cdot q_t. \quad (1)$$

De $p_1 \mid q_1 q_2 \cdots q_t$ resulta que $p_1 \mid q_i$ para algún i. Reordenando los factores si fuera necesario, podemos suponer que $p_1 \mid q_1$. De donde resulta $p_1 = q_1$. Cancelando este factor en (1) resulta

$$n = p_2 \cdot \cdots \cdot p_r = q_2 \cdot \cdots \cdot q_t.$$

El número n es un entero positivo menor que m y se expresa de dos formas diferentes como producto de números primos, lo cual contradice la definición de m. El absurdo provino de suponer la existencia de enteros positivos que se pueden expresar como producto de números primos de dos formas diferentes. □

Agrupando los factores primos iguales entre sí en la representación $a = p_1 p_2 \cdot \cdots \cdot p_r$, podemos escribir

$$a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

donde ahora los primos $p_1, p_2, \ldots, p_s$ son distintos dos a dos, $e_i \in \mathbb{N}$, $1 \leq i \leq s$. Por ejemplo,

$$11760 = 2^4 \cdot 3 \cdot 5 \cdot 7^2, \quad 11880 = 2^3 \cdot 3^3 \cdot 5 \cdot 11.$$

Nota. El primer enunciado claro del Teorema Fundamental de la Aritmética fue hecho por Gauss (1777–1855) en sus Disquisitiones Arithmeticae en 1801.

Ejemplos.

1. Un número $a \neq 0, 1, -1$ es un cuadrado si y sólo si en su descomposición en factores primos, cada primo aparece un número par de veces.
   Basta probarlo cuando $a > 1$. Supongamos que a es un cuadrado. Entonces $a = m^2$, $m \in \mathbb{Z}$, $m > 1$. Sea $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s}$, p_i primos distintos, $e_i > 0$. Entonces la factorización de a es $a = m^2 = (p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s})^2 = p_1^{2e_1} \cdot p_2^{2e_2} \cdot \cdots \cdot p_s^{2e_s}$, y cada primo aparece un número par de veces.

   Recíprocamente, supongamos que en la descomposición de a en factores primos, cada primo figura un número par de veces. Entonces

   $$a = p_1^{2e_1} \cdot p_2^{2e_2} \cdot \cdots \cdot p_s^{2e_s} = (p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s})^2 .$$

   Luego a es un cuadrado.

2. No existen números enteros a y b no nulos tales que $3a^2 = b^2$.
   Es claro que si $b = 1$, la igualdad anterior no se verifica. Supongamos $b \neq 1$. Por el ejemplo anterior, en la descomposición de $3a^2$, el primo 3 aparece un número impar de veces, mientras que en la descomposición de b^2 aparece un número par de veces. Por la unicidad de la factorización, se tiene que la igualdad $3a^2 = b^2$ no se verifica si a y b son no nulos.

3. Probar que $\sqrt{2}$ es irracional usando el Teorema Fundamental de la Aritmética.
   Si $\sqrt{2} \in \mathbb{Q}$, entonces $\sqrt{2} = a/b$, $a, b \in \mathbb{N}$. Entonces $a^2 = 2b^2$. Sea e la potencia de 2 que aparece en la factorización de a, f la potencia de 2 que aparece en la factorización de b. Entonces de $a^2 = 2b^2$ se tiene $2e = 2f + 1$, lo cual es imposible pues $2e$ es par y $2f + 1$ es impar.

4. Probar que $(100)^{1/3}$ es irracional.
   Si 100 fuese un cubo, entonces $b^3 = a^3 100 = a^3 2^2 5^2$. Usar la unicidad de la factorización.

5. La siguiente propiedad es inmediata: $(a, b) = 1$ si y sólo si los primos que aparecen en la representación de a son distintos de los primos que aparecen en la representación de b.

6. Si a y b son enteros no negativos tales que $(a, b) = 1$ y $a \cdot b$ es un cuadrado, entonces a y b son cuadrados.
   Si $a \cdot b = 0$, entonces, como $(a, b) = 1$ y a y b son no negativos, debe ser $a = 1$ y $b = 0$, ó $a = 0$ y $b = 1$, y la propiedad vale.
   Si $a \cdot b \geq 1$, entonces $a \geq 1$ y $b \geq 1$. Si $a = 1$, entonces $a \cdot b = b$ y se verifica la propiedad. Análogamente si $b = 1$.
   Supongamos $a > 1$ y $b > 1$. Consideremos las descomposiciones de a y b:

   $$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s} \quad ; \quad b = q_1^{f_1} \cdot q_2^{f_2} \cdot \cdots \cdot q_r^{f_r} .$$

   Como $(a, b) = 1$, los primos p_i son distintos de los primos q_j. Entonces

   $$a \cdot b = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s} \cdot q_1^{f_1} \cdot q_2^{f_2} \cdot \cdots \cdot q_r^{f_r},$$

   donde todos los p_i son distintos entre sí, los q_j son distintos entre sí, y los p_i son distintos de los q_j. Como por hipótesis $a \cdot b$ es un cuadrado, cada primo figura un número par de veces. Luego los exponentes e_i y los f_i son pares. En consecuencia, a y b son cuadrados.

Es conocido el procedimiento para hallar efectivamente los factores primos de un número n: se divide n por los números primos menores que n. El siguiente teorema proporciona una simplificación para encontrar esos factores, ya que bastará con probar con los números primos menores o iguales que $\sqrt{n}$.

Teorema 6.17 *Sea $n \in \mathbb{Z}$, $n > 1$. Si n no es primo entonces existe un primo p tal que $p \mid n$ y $p \leq \sqrt{n}$.*

Demostración. Sea $n \in \mathbb{Z}$, $n > 1$. Si n no es primo entonces $n = a \cdot b$, a, b divisores propios, luego $1 < a \leq b < n$. Como $a > 0$ y $a \leq b$ entonces $a^2 \leq a \cdot b = n$. Esto implica que $a = |a| = \sqrt{a^2} \leq \sqrt{n}$. Como $a > 1$, existe un primo positivo p tal que $p \mid a$. Entonces $p \mid n$, y como $p \leq a$, se tiene que $p \leq a \leq \sqrt{n}$. □

Supongamos que se han encontrado todos los divisores primos de n que son menores o iguales que $\sqrt{n}$: $p_1, p_2, \ldots, p_s$. Si $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s}$, ya se tiene la factorización de n. Si no,

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s} \cdot b, \text{ con } p_i \nmid b,\ b \neq 1.$$

Veamos que b es primo. En efecto, por el teorema anterior, si b no es primo, admite un divisor primo menor o igual que $\sqrt{b}$. Pero como $\sqrt{b} \leq \sqrt{n}$, este primo es uno de los primos $p_1, p_2, \ldots, p_s$. Absurdo.
Luego, o bien $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s}$, $p_i \leq \sqrt{n}$, o bien $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s} \cdot b$, $p_i \leq \sqrt{n}$, b primo.

Ejemplos.

1. Sea $a = 271$. Como $\sqrt{271} = 16, \ldots,$ consideremos los primos menores o iguales que 16 : 2, 3, 5, 7, 11, 13. Los mismos no dividen a 271, por lo tanto 271 es primo.

2. Consideremos $a = 1001$. $\sqrt{1001} = 31, \ldots$. Sean $p = 2$, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, los primos menores o iguales que 31. Como $7 \mid 1001$ entonces 1001 no es primo.

3. Probar que 2003 y 467 son primos. ¿ Es 4031 primo ?

Nota. El teorema anterior nos permite construir la llamada "Criba de Eratóstenes" (Eratóstenes de Cirene (278–194 a.C.)) para determinar todos los primos menores que un número dado n. Para ello se escriben los números naturales entre 2 y n en su orden natural. Para cada primo $p \leq \sqrt{n}$, se tachan en esa lista todos los múltiplos de p mayores que p. Al terminar, los números no tachados son los primos menores que n.

Construyamos una tabla de todos los números primos menores que 100.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Entonces, los números primos menores que 100 son:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

6.4 Divisores de un número entero

Sea $a \in \mathbb{Z}$, como el conjunto de divisores de a coincide con el conjunto de divisores de $-a$, consideramos el caso $a \geq 0$.
Si $a = 0$, $D(a) = \mathbb{Z}$. Si $a = 1$, $D(a) = \{\pm 1\}$.

Teorema 6.18 *Sea* $a > 1$, *y sea* $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s}$, p_i *primos positivos distintos,* $e_i \in \mathbb{N}$, $1 \leq i \leq s$. *Sea* $b \in \mathbb{Z}$, $b > 0$, *entonces* $b \mid a \iff b = p_1^{t_1} \cdot p_2^{t_2} \cdot \cdots \cdot p_s^{t_s}$, $0 \leq t_i \leq e_i \,; 1 \leq i \leq s$.

Demostración. Es claro que si $b = p_1^{t_1} \cdot p_2^{t_2} \cdot \cdots \cdot p_s^{t_s}$, $0 \leq t_i \leq e_i \,; 1 \leq i \leq s$, entonces $b \mid a$.

Veamos la recíproca. Los únicos divisores primos de a son los números $p_1, p_2 \ldots, p_s$, en virtud de la unicidad de la descomposición en factores primos. Luego, si $b \mid a$, cualquier divisor primo de b es uno de los números $p_1, p_2, \ldots, p_s$. Luego $b = p_1^{t_1} \cdot p_2^{t_2} \cdot \cdots \cdot p_s^{t_s}$, $t_i \geq 0$, $t_i \in \mathbb{Z}$.

Además, de $b \mid a$ se tiene $a = bc$ donde, por el mismo razonamiento, $c = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_s^{r_s}$, $r_i \geq 0$, $r_i \in \mathbb{Z}$. Entonces

$$a = bc = p_1^{t_1 + r_1} \cdot p_2^{t_2 + r_2} \cdot \cdots \cdot p_s^{t_s + r_s},$$

de donde resulta $e_i = t_i + r_i$, $1 \leq i \leq s$, por la unicidad de la factorización, y por lo tanto, $0 \leq t_i \leq e_i \,; 1 \leq i \leq s$. □

Hallados los divisores positivos de a, todos sus divisores se obtienen calculando los simétricos de los anteriores.

Ejemplo. Sea $a = 75 = 3^1 \cdot 5^2$. Los divisores positivos de a son: $3^0 \cdot 5^0 = 1$, $3^0 \cdot 5^1 = 5$, $3^0 \cdot 5^2 = 25$, $3^1 \cdot 5^0 = 3$, $3^1 \cdot 5^1 = 15$, $3^1 \cdot 5^2 = 75$.

Si $a > 1$, $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s}$ y con $d(a)$ notamos al número de los divisores positivos de a, resulta en forma inmediata del teorema anterior que: $d(a) = (e_1 + 1) \cdot (e_2 + 1) \cdot \cdots \cdot (e_s + 1)$.

Ejemplos

1. Sea $a = 84 = 3^1 \cdot 2^2 \cdot 7^1$. Se tiene entonces que $d(a) = (1+1) \cdot (2+1) \cdot (1+1) = 12$ y por lo tanto a posee 12 divisores positivos y en consecuencia 24 divisores.
   ¿Cuántos divisores positivos tiene el número 92? Como $92 = 2^2 \cdot 23$, entonces $d(92) = (2+1) \cdot (1+1) = 6$.

2. Hallemos el menor natural a que posee exactamente 42 divisores. En este caso, a tiene 21 divisores positivos, esto es, $d(a) = 21 = 21 \cdot 1 = 3 \cdot 7 = (e_1 + 1) \cdot (e_2 + 1)$. Se tienen entonces dos posibilidades:
   $a = p^{20}$, p primo ó $a = p^2 \cdot q^6$; p, q primos distintos. Como busco el menor natural posible, considero los primos menores (2 y 3) obteniendo como posibles valores de a a los siguientes: $a = 2^{20}$, $a = 3^2 \cdot 2^6$ ó $a = 2^2 \cdot 3^6$. Un fácil cálculo nos indica que $a = 3^2 \cdot 2^6$ es el natural buscado.

3. ¿Cuál es el menor entero positivo que admite exactamente 15 divisores positivos? Como $15 = 1 \cdot 15 = 3 \cdot 5 = (e_1+1)(e_2+1)$, entonces el número a buscado será de la forma $a = p_1^{e_1} \cdot p_2^{e_2}$, con $e_1 = 2, e_2 = 4$, ó $e_1 = 0, e_2 = 14$. Es decir, $a = p^{14}$ ó $a = p_1^2 \cdot p_2^4$. Como buscamos el menor a, elegimos los primos más chicos posibles. Luego a puede ser: 2^{14}, $2^2 \cdot 3^4$ ó $3^2 \cdot 2^4$. El número más chico es $3^2 \cdot 2^4 = 144$.

4. Probar que $6 \mid n^3 - n$.
Como $6 = 2 \cdot 3$, basta demostrar que $2 \mid n^3 - n$ y $3 \mid n^3 - n$. (Recordar que si $a \mid n$ y $b \mid n$ y $(a,b) = 1$, entonces $a \cdot b \mid n$).
$n^3 - n = n(n^2-1) = n(n+1)(n-1)$.
Si n es par, entonces $2 \mid n$, y en consecuencia, $2 \mid n^3 - n$. Si n es impar, entonces $2 \mid n-1$ y entonces $2 | n^3 - n$.
Por otro lado, como $n-1$, n, $n+1$ son tres enteros consecutivos, entonces uno de ellos es múltiplo de 3. Luego $3 \mid n(n+1)(n-1) = n^3 - n$.
Luego $2 \cdot 3 = 6 \mid n^3 - n$.

Corolario 6.19 *Si* $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_s^{e_s}$ *y* $b = p_1^{t_1} \cdot p_2^{t_2} \cdot \cdots \cdot p_s^{t_s}$, $e_i \geq 0$, $t_i \geq 0$, *entonces*

$$(a,b) = p_1^{m_1} \cdot p_2^{m_2} \cdot \cdots \cdot p_s^{m_s}$$

y

$$[a,b] = p_1^{M_1} \cdot p_2^{M_2} \cdot \cdots \cdot p_s^{M_s},$$

donde m_i *y* M_i *representan, respectivamente, el menor y el mayor de los números* e_i *y* t_i.

Demostración. Es inmediata. □

Ejemplo. De $280 = 2^3 \cdot 5 \cdot 7$ y $693 = 3^2 \cdot 7 \cdot 11$ podemos escribir

$$\begin{aligned} 280 &= 2^3 \cdot 3^0 \cdot 5 \cdot 7 \cdot 11^0 \\ 693 &= 2^0 \cdot 3^2 \cdot 5^0 \cdot 7 \cdot 11. \end{aligned}$$

Luego

$$\begin{aligned} (280, 693) &= 2^0 \cdot 3^0 \cdot 5^0 \cdot 7 \cdot 11^0 = 7 \\ [280, 693] &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27720. \end{aligned}$$

6.5 Una aplicación del algoritmo de la división. Representación en distintas bases

Un problema, que es consecuencia inmediata del algoritmo de la división, es el de representar cualquier número entero positivo en una base $b > 1$.

El sistema de numeración que habitualmente usamos para representar los números enteros es el llamado sistema decimal (o sistema en base 10), que utiliza los símbolos $0, 1, 2, 3, 4, 5, 6, 7, 8$ y 9, y que consiste en expresar cualquier número entero en términos de potencias de 10. Así por ejemplo,

$$7231 = 7 \cdot 1000 + 2 \cdot 100 + 3 \cdot 10 + 1 = 7 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 1$$

Sin embargo, la elección del número 10 es completamente arbitraria, y un desarrollo análogo puede llevarse a cabo tomando en lugar de 10 un número entero cualquiera $b > 1$. Por ejemplo, $74 = 2 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3^1 + 2$, $74 = 2202_{(3)}$.

Comencemos con el siguiente ejemplo. Consideremos el número 2234 y hagamos sucesivas divisiones por 5.

2234	5				
23	446	5			
34	46	89	5		
$\underline{4}$	$\underline{1}$	39	17	5	
		$\underline{4}$	$\underline{2}$	**3**	5
				$\underline{3}$	0

Consideremos los restos, en el siguiente orden: $\underline{3}$, $\underline{2}$, $\underline{4}$, $\underline{1}$, $\underline{4}$.

Observemos que:

$$2234 = 446 \cdot 5 + 4 \quad (1)$$
$$446 = 89 \cdot 5 + 1 \quad (2)$$
$$89 = 17 \cdot 5 + 4 \quad (3)$$
$$17 = 3 \cdot 5 + 2 \quad (4)$$

Entonces $2234 \overset{(1)}{=} 446 \cdot 5 + 4 \overset{(2)}{=} (89 \cdot 5 + 1) \cdot 5 + 4 = 89 \cdot 5^2 + 1 \cdot 5 + 4 \overset{(3)}{=} (17 \cdot 5 + 4) \cdot 5^2 + 1 \cdot 5 + 4 = 17 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5 + 4 \overset{(4)}{=} (3 \cdot 5 + 2) \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5 + 4 = 3 \cdot 5^4 + 2 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5 + 4$, esto es,

$$2234 = \underline{3} \cdot 5^4 + \underline{2} \cdot 5^3 + \underline{4} \cdot 5^2 + \underline{1} \cdot 5 + \underline{4}.$$

Los restos obtenidos en las divisiones sucesivas son los coeficientes del desarrollo de 2234 en potencias de 5. Por la unicidad del algoritmo de la división, estos restos están unívocamente determinados, y podemos en consecuencia decir que los números 3, 2, 4, 1, 4 representan a 2234 en la base 5. En notación,

$$2234 = 32414_{(5)}.$$

Lo anterior se formaliza en el siguiente

Teorema 6.20 *Sea $b \in \mathbb{N}$, $b > 1$. Para todo entero $a > 0$, existen únicos enteros $a_0, a_1, \ldots, a_n$, con $0 \leq a_i < b$, $i = 0, 1, \ldots, n$ y $a_n > 0$ tales que*

$$a = a_n b^n + \cdots + a_2 b^2 + a_1 b + a_0.$$

Escribimos $a = a_n \ldots a_2 a_1 a_{0(b)}$, ó $a = a_n \ldots a_2 a_1 a_0$, si no hay riesgo de confusión. Los coeficientes a_i se llaman las cifras y b se llama la base de la representación.

Demostración. Vamos a probarlo haciendo inducción sobre a.
Si $a = 1$, entonces $1 = 0 \cdot b + 1$, y entonces $1 = 1_{(b)}$.

Supongamos que el teorema vale (existencia y unicidad) para todo entero positivo menor que k, y probemos que vale para k.

Por el algoritmo de la división, $k = q \cdot b + r$, con $0 \leq r < b$. Podemos suponer que $k > b$, pues caso contrario, $k = 0 \cdot b + k$, si $k < b$, y $k = 1 \cdot b + 0$, si $k = b$.

De $k > b$, debe ser $q > 0$, y como $b > 1$, se tiene $q < q \cdot b \leq q \cdot b + r = k$. Entonces, por la hipótesis inductiva, el teorema vale para q, esto es, $q = a_0 + a_1 \cdot b + \cdots + a_t \cdot b^t$, $0 \leq a_i < b$, y entonces $k = q \cdot b + r = a_0 \cdot b + a_1 \cdot b^2 + \cdots + a_t \cdot b^{t+1} + r$, que es el desarrollo de k.

Probemos la unicidad. Si

$$a_0 + a_1 \cdot b + \cdots + a_t \cdot b^t = c_0 + c_1 \cdot b + \cdots + c_s \cdot b^s, \quad 0 \leq a_i,\ c_i < b,$$

entonces $a_0 + (a_1 + \cdots + a_t \cdot b^{t-1}) \cdot b = c_0 + (c_1 + \cdots + c_s \cdot b^{s-1}) \cdot b$. Como $0 \leq a_0 < b$ y $0 \leq c_0 < b$, por la unicidad en el algoritmo de la división, $a_0 = c_0$, y $a_1 + \cdots + a_t \cdot b^{t-1} = c_1 + \cdots + c_s \cdot b^{s-1}$, y por la hipótesis inductiva, $t = s$ y $a_1 = c_1, \ \ldots\ , \ a_t = c_t$. □

Si a es negativo, entonces el desarrollo de a se obtiene anteponiendo un signo menos al desarrollo de $|\, a \,|$.

En la práctica, para representar el entero a en la base b, hallamos la división entera de a por b: $a = q \cdot b + a_0$. Dividiendo q por b obtenemos un resto a_1 y un cociente q_1; dividiendo q_1 por b obtenemos un resto a_2 y un cociente q_2, etc. Continuando con este procedimiento llegamos finalmente al cociente $q_{n-1} < b$, $q_{n-1} = a_n$. La representación de a en la base b es entonces $a = a_n a_{n-1} \ldots a_0{}_{(b)}$.

$$\begin{array}{lll}
a & | & b \\
\cline{2-3}
a_0 & q & | \ b \\
\cline{3-3}
 & a_1 & q_1 \quad | \ b \\
\cline{4-4}
 & & a_2 \quad q_2 \quad \ldots \\
 & & \qquad\qquad \ldots \\
 & & \qquad\qquad\quad \ldots \\
 & & \qquad\qquad\quad\ q_{n-2} \ | \ b \\
\cline{5-5}
 & & \qquad\qquad\quad\ a_{n-1} \quad q_{n-1} \quad | \ b \\
\cline{6-6}
 & & \qquad\qquad\qquad\qquad\ a_n = q_{n-1} \quad 0
\end{array}$$

Ejemplo. Representar el número 1517 en las bases 3 y 7.

$1517 = 505 \cdot 3 + \underline{2}$, $505 = 168 \cdot 3 + \underline{1}$, $168 = 56 \cdot 3 + \underline{0}$, $56 = 18 \cdot 3 + \underline{2}$, $18 = 6 \cdot 3 + \underline{0}$, $6 = 2 \cdot 3 + \underline{0}$, $2 = 0 \cdot 3 + \underline{2}$.

Luego,

$$1517 = 2002012_{(3)}.$$

Por otro lado, $1517 = 216 \cdot 7 + \underline{5}$, $216 = 30 \cdot 7 + \underline{6}$, $30 = 4 \cdot 7 + \underline{2}$, $4 = 0 \cdot 7 + \underline{4}$.

Luego,

$$1517 = 4265_{(7)}.$$

Las cifras en base 3 son $0, 1, 2$, y en base 7 son $0, 1, 2, 3, 4, 5, 6$. Para representar números en base mayor que 10 se agregan nuevos símbolos a los dígitos $0, 1, 2, \ldots, 8, 9$ para completar las cifras faltantes. Así por ejemplo, para representar un número en base 12 necesitamos agregar dos símbolos, por ejemplo α y β, para representar las cifras diez y once.

Ejemplo. Representar 3307 en base 12.
Haciendo divisiones sucesivas por 12, obtenemos:

$$3307 = 275 \cdot 12 + \underline{7}, \;\; 275 = 22 \cdot 12 + \underline{11}, \;\; 22 = 1 \cdot 12 + \underline{10}, \;\; 1 = 0 \cdot 12 + \underline{1}.$$

Luego las cifras de la representación de 3307 en base 12 son:

$$1 \quad ; \quad \alpha = 10 \quad ; \quad \beta = 11 \quad ; \quad 7.$$

Luego

$$3307 = 1\alpha\beta 7_{(12)}.$$

Si $b = 10$, la representación en base b es la representación llamada decimal, si $b = 2$ es la representación binaria y si $b = 8$, es la octal. Así, $3307 = 3307_{(10)} = 3 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10 + 7$.

Ejemplo. Usando la representación decimal, probar que un número entero es divisible por 2 (por 5) si y sólo si la cifra de sus unidades es múltiplo de 2 (de 5).

Escribamos $a = a_n a_{n-1} \cdots a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots a_1 10 + a_0$. Todos los términos de la expresión anterior, salvo eventualmente a_0, son múltiplos de 2. Luego podemos escribir $a = t \cdot 2 + a_0$. Luego

$$2 \mid a \;\Leftrightarrow\; 2 \mid a_0.$$

De la misma manera todos los términos, salvo eventualmente a_0, son múltiplos de 5. De donde $a = s \cdot 5 + a_0$. Luego

$$5 \mid a \;\Leftrightarrow\; 5 \mid a_0.$$

Observar que la representación del número b en la base b es 10, ya que $b = 1 \cdot b + 0$.

Las operaciones de suma, resta, multiplicación y división de números enteros expresados en una base b, se efectúan esencialmente de la misma forma que en la base decimal.

Ejemplos.

1. Sumar $2543_{(6)}$ y $5323_{(6)}$.

   Para efectuar la suma conviene tener presente que:

   $$6 = 10_{(6)} \;;\; 7 = 11_{(6)} \;;\; 8 = 12_{(6)} \;;\; 9 = 13_{(6)} \;;\; 10 = 14_{(6)} \;;\; 11 = 15_{(6)},$$

   y que, en base 6, las tablas para la suma y el producto son:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	10
2	2	3	4	5	10	11
3	3	4	5	10	11	12
4	4	5	10	11	12	13
5	5	10	11	12	13	14

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

   Luego

$$\begin{array}{r} 2543 \\ +\ 5323 \\ \hline 12310 \end{array}$$

Como en el caso decimal, el procedimiento ha sido el siguiente: (lo que sigue está escrito en base 6):

$$\begin{array}{rll} 3+3=10\ ; & \text{escribimos el } 0 \text{ y llevamos } 1. \\ 1 \text{ (que nos llevábamos)} \ +4+2=11\ ; & \text{escribimos el } 1 \text{ y llevamos } 1. \\ 1+5+3=13\ ; & \text{escribimos el } 3 \text{ y llevamos } 1, \text{ etc.} \end{array}$$

2. Multiplicar $4354_{(6)}$ por $342_{(6)}$.

$$\begin{array}{r} 4354 \\ \times\ 342 \\ \hline 13152 \\ 30344 \\ 21550 \\ \hline 2520032 \end{array}$$

3. Calcular $132003_{(5)} - 41134_{(5)}$.

$$\begin{array}{r} 132003 \\ -\ 41134 \\ \hline 40314 \end{array}$$

6.6 Ejercicios

1. ¿ Cuáles de las siguientes relaciones son verdaderas ?
   $2 \mid 2$, $3 \mid 17$, $-7 \mid 14$, $17 \mid 135$, $4 \mid 2$, $-23 \mid -117$, $3481 \mid 437289$.

2. Si a, b, c, d indican números enteros arbitrarios, decidir cuáles de las siguientes proposiciones son verdaderas y cuáles son falsas, justificando la respuesta:

   (a) Si $10 \mid a$ entonces $5 \mid a$.
   (b) Si $14 \nmid a$ entonces $7 \nmid a$.
   (c) Si $15 \mid a$, entonces $3 \mid a$.
   (d) Si $2 \mid a$ ó $7 \mid a$, entonces $14 \mid a$.
   (e) Si $3 \nmid a$, entonces $6 \nmid a$.
   (f) Si $a + b$ es par entonces a es par ó b es par.
   (g) Si $a + b$ es par entonces a y b poseen la misma paridad.
   (h) Si $a \mid b + c$ entonces $a \mid b$ ó $a \mid c$.
   (i) Si $a \mid a + b$ entonces $a \mid b$.
   (j) Si $a \mid b \cdot c$ entonces $a \mid b$ ó $a \mid c$.
   (k) Si $a \mid c$ y $b \mid c$, entonces $a \cdot b \mid c$.
   (l) Si $a^2 \mid b^3$ entonces $a \mid b$.
   (m) Si $c = a\,x + b\,y$; x , $y \in \mathbb{Z}$, $d \mid b$ y $d \nmid a$ entonces $d \nmid c$.

3. Calcular el cociente y el resto de la división de a por b en los siguientes casos:
   $a = 423$, $b = 7$; $a = 0$, $b = 2^{353}$; $a = -25$, $b = 6$; $a = 132$, $b = -89$; $a = -101$, $b = -23$.

4. Probar que en cualquier conjunto de 79 enteros debe existir por lo menos un par cuya diferencia es divisible por 78.

5. Probar que si los restos de dividir $a, b \in \mathbb{Z}$ por $m \in \mathbb{N}$ son 1, entonces el resto de dividir ab por m es también 1.

6. Probar que el resto de dividir el cuadrado de un número impar por 8 es 1.

7. Probar que la suma de los cuadrados de dos números naturales consecutivos tiene resto 1 al dividirla por 4.

8. Probar que si $a, b \in \mathbb{Z}$, $a^2 + b^2$ es múltiplo que 3 si y sólo si a y b son múltiplos de 3. ¿ Es cierto que si $a^3 + b^3$ es múltiplo de 3 entonces a y b son múltiplos de 3 ?

9. (a) ¿ Cuántos enteros entre 1 y 100 son divisibles por 9 ?
   (b) ¿ Cuántos enteros entre 25 y 250 son divisibles por 11 ?

10. Sean a, $b \in \mathbb{Z}$. Probar que:

    (a) Si $b \mid a$ y $a \mid b$, entonces $a = b$ ó $a = -b$.
    (b) Si $a \mid b + c$ y $a \mid b$, entonces $a \mid c$.
    (c) Deducir de (b) que si $a \mid a + c$, entonces $a \mid c$.

11. Hallar, utilizando el algoritmo de Euclides, el máximo común divisor de a y b y expresarlo como combinación lineal de ellos, siendo:

    (a) $a = 901,\ b = 1219.$
    (b) $a = -24,\ b = -6.$
    (c) $a = -330,\ b = 42.$
    (d) $a = 13,\ b = 101.$
    (e) $a = -187,\ b = -1219.$
    (f) $a = -42,\ b = 300.$

12. ¿Existe $x \in \mathbb{Z}$ tal que $15 \mid 3x + 77$?

13. Sea S el conjunto de todos los números que son suma de los cuadrados de tres enteros consecutivos. Decir si las siguientes afirmaciones son verdaderas o falsas, justificando la respuesta:

    (a) Ningún elemento de S es par.
    (b) Ningún elemento de S es divisible por 3 y alguno de ellos es divisible por 11.
    (c) Ningún elemento de S es divisible por 3 ni por 5.

14. Decir cuál es el máximo común divisor de los enteros a y b tales que:

    (a) $3a + 5b = 6$, a y b no son coprimos y $(a, 3) = 1$.
    (b) $7a + 5b = 8$ y a es impar.
    (c) $9\,a + 7\,b = 15$, si a y b no son coprimos y $(b, 5) = 1$.
    (d) $23\,a + 55\,b = 22$, b es impar y $(b, 11) = 1$.

15. Probar que para cualquier número natural n, $(n, n + 1) = 1$.

16. (a) Hallar, si existe, una solución entera de las siguientes ecuaciones:
        (i) $36\,x + 30\,y = 54$
        (ii) $8\,x + 3\,y = 27$
        (iii) $3\,x + 83\,y = -4$
        (iv) $12\,x + 6\,y = 1.$
        (v) $175x + 12y = 20.$
        (vi) $12x + 44y = 240.$

    (b) Hallar dos fracciones con denominadores 11 y 13, tales que su suma sea $\dfrac{67}{143}$.

17. (a) ¿ Cómo se puede poner un litro de agua en un recipiente si se dispone de dos jarros que tienen capacidad para 7 y 9 litros respectivamente ?

    (b) Se dispone de un reloj de arena de 6 minutos y de otro de 11 minutos. ¿ Cómo se pueden medir 13 minutos ?

18. Probar que si a y b son enteros no simultáneamente nulos:

    (a) $(0, b) = \mid b \mid$.
    (b) $(a, b) = \mid a \mid \Leftrightarrow\ a \mid b$.
    (c) Si $c \in \mathbb{Z},\ c > 0,$ entonces $(a \cdot c, b \cdot c) = (a, b) \cdot c.$

(d) Probar que si existen enteros x e y tales que $xa + yb = 1$, entonces $(a, b) = 1$.

(e) Usar (d) para probar que si $d = (a, b)$, entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

19. ¿Cuántos de los 100 primeros números naturales son divisibles por 2, 3, 4 y 5?

20. (a) Probar que entre m enteros consecutivos hay exactamente uno que es divisible por m.

(b) Sean $m > n > 1$ números naturales. Probar que existe t, $n \leq t < m$, tal que $m - n \mid t$.

21. Sea $a \neq 1$ un número natural con la siguiente propiedad: para todo b, c, si $a \mid bc$ y $a \nmid b$ entonces $a \mid c$. Probar que a debe ser primo.

22. Hallar todos los primos p tales que $100 \leq p \leq 120$.

23. Demostrar que para todo $a \in \mathbb{Z}$:

(a) $a \cdot (a + 1)$ es divisible por 2.

(b) $(a^2 - 1) \cdot a$ es divisible por 3.

(c) $a \cdot (a^4 - 1)$ es múltiplo de 5.

(d) $a \cdot (a^6 - 1)$ es múltiplo de 7.

(e) Si a es impar, entonces $a \cdot (a^4 - 1)$ es divisible por 240.

(f) $7a^3 - 7a$ es divisible por 42.

24. Probar que si p es un número primo, $p \geq 5$, entonces $24 \mid p^2 - 1$.

25. (a) Hallar la descomposición en factores primos de los siguientes números enteros:
880, -9180, 16758, 14703, 1988^2, $(12 \cdot 15)^2 \cdot 16 \cdot 30^3$.

(b) Determinar si existen enteros no nulos a y b que satisfagan:
(i) $5a^2 = 7b^2$. (ii) $a^2 = 8b^2$.
(iii) $a^2 = 180$. (iv) $a^4 = 850b^{10}$.
(v) $a^3 = b^2$, $a \neq 1$, $b \neq 1$.

(c) Usar las técnicas del inciso (b) para demostrar que los siguientes números son irracionales:
(i) $\sqrt{10}$ (ii) $\sqrt[3]{2}$ (iii) $\sqrt[8]{8/11}$.

26. Mostrar que si n es un natural mayor que 1 y p es un primo positivo entonces $\sqrt[n]{p}$ no es racional.

27. Hallar el menor entero positivo x para el cual $1260 \cdot x$ es un cubo.

28. Decir si son verdaderas o falsas las siguientes proposiciones sobre números enteros, justificando la respuesta:

(a) Un número es divisible por 6 si y sólo si es divisible por 2 y por 3.

(b) Si p es primo, $p \mid a$ y $p \mid a^2 + b^2$, entonces $p \mid b$.

(c) Si p es primo, $p \mid a$ y $p \mid a^2 + 6b^2$, entonces $p \mid b$.

29. Probar que:

(a) Los números 2^h y $2^h + 7^k$ son relativamente primos, para todo $h, k \in \mathbb{N}$.

(b) $(18, 35 + 12a) = 1$, para todo $a \in \mathbb{Z}$.

(c) Si $a, b \in \mathbb{Z}$, $(a, b) = 1$, entonces $(2a + b, 3a + b) = 1$.

(d) Si $(a, b) = 1$ y $(b, 5) = 1$ entonces $(b^2, b^3 + 5a^2) = 1$.

30. Sean a y b dos enteros relativamente primos. Demostrar que:

(a) a^m y b^n son relativamente primos, para todo $m, n \in \mathbb{Z}$, $m \geq 0$, $n \geq 0$.

(b) $a + b$ y $a \cdot b$ son relativamente primos.

(c) $(a + b, a - b)$ es 1 ó 2.

31. Probar que los números 983 y 3931 son primos.

32. (a) Determinar el número de divisores positivos de 36, 52, 39 y 72. Hallarlos.

(b) Indicar la forma de todos los números naturales con exactamente 10 divisores positivos.

(c) Hallar el menor natural con exactamente 10 divisores positivos.

33. (a) Escribir todos los divisores comunes a 500 y 280.

(b) ¿Cuál es el menor entero positivo que posee exactamente 30 divisores?

(c) ¿De cuántas maneras se puede escribir 7800 como producto de *dos* enteros positivos?

(d) Hallar los divisores positivos de p^8, siendo p un número primo cualquiera. Calcular la suma de dichos divisores, si $p = 4057$.

34. Hallar el mínimo común múltiplo de los siguientes pares de números enteros a y b:
(a) $a = 6500$, $b = 175$ (b) $a = 126$, $b = 1470$ (c) $a = 500$, $b = 280$

35. Hallar todos los pares de enteros a y b positivos tales que:

(a) $(a, b) = 98$ y $[a, b] = 1470$.

(b) $(a, b) = 36$ y $[a, b] = 756$.

36. (a) Convertir los siguientes enteros decimales al sistema binario y al octal :
64; 16; 32768; 1000.

(b) Los siguientes números enteros están escritos en sistema binario, representarlos en el sistema decimal :
101; 1011; 10011101011.

(c) Representar en el sistema decimal, los enteros que en el sistema octal se escriben :
10; 64; 777; 6432.

37. (a) Escribir en las bases 2, 5 y 12, los números que en base 10 se escriben :
15; 642; 1108.

(b) Verificar que las expresiones $1447_{(8)}$, $1100100111_{(2)}$, $2(13)8_{(17)}$, representan al mismo número entero.

(c) Representar en base 2 y en base 7 el número entero que en base 3 se escribe 200112.

38. (a) Hallar la representación binaria de los dígitos 1, 2, 3, 4, 5, 6, 7.

(b) Hallar la representación binaria y octal de los enteros decimales : 121 y 242 .

(c) Deducir a partir de a) y b) una forma sencilla de convertir enteros binarios en octales.

39. (i) Efectuar las siguientes operaciones en el sistema binario :

(a)	$1010 + 0011$	(b)	$1111 + 0011$
(c)	1001×110	(d)	1011×1100
(e)	$11001 - 101$	(f)	$10011 - 1010$

(ii) Efectuar las siguientes operaciones en base 8 :

(a)	$3432 + 1367$	(b)	356×45
(c)	$4357 - 421$		

40. Si $N = 11000_{(2)}$, hallar $N - 1$ en base 2.

41. Mostrar que $10_{(b)} \times 10_{(b)} = 100_{(b)}$.

42. Determinar, si existe, una base b en la cual $31 \times 12 = 402$.

43. Determinar el valor de x para que $n = 342x_{(6)}$ sea divisible por 5.

44. Supongamos que los números en el siguiente problema se escriben en base b. Si Juan compra un automóvil en 440 unidades monetarias y paga con 1000, recibe 340 de vuelto. Hallar el valor de b.

45. Un almacenero tiene una balanza de platillos y seis pesas distintas, y puede pesar cualquier peso entero de 1 a 63 kilogramos inclusive.

(a) Indicar cuáles son las pesas.

(b) Decir cómo pesar un peso de $53\ Kg$ y uno de $27\ Kg$.

7 Números complejos

Las sucesivas ampliaciones de los conjuntos numéricos son motivadas por la necesidad de encontrar soluciones a determinadas ecuaciones, o poder realizar ciertas operaciones. Por ejemplo, ampliamos el conjunto $\mathbb{N}$ de los números naturales al conjunto de los números enteros para poder resolver ecuaciones como $x+2=1$, o lo que es lo mismo, para poder *restar*. En el conjunto $\mathbb{Z}$ no podemos resolver una ecuación como $3x=1$, es decir, no podemos *dividir*, y para ello lo ampliamos al conjunto $\mathbb{Q}$ de los números racionales. De la misma manera, no podemos resolver en $\mathbb{Q}$ una ecuación como $x^2-2=0$, mientras que sí es posible resolverla en $\mathbb{R}$. Pero no toda ecuación es resoluble en $\mathbb{R}$. Por ejemplo, la ecuación $x^2+1=0$ no tiene solución real, ya que $x^2 \neq -1$, para todo número real x.

La ampliación del conjunto de los números reales al conjunto de los números complejos tiene por objetivo obtener un sistema numérico en el cual toda ecuación con coeficientes reales o complejos tenga solución. Este resultado se conoce con el nombre de Teorema Fundamental del Algebra.

7.1 Definición y propiedades

Definición 7.1 *Sea $\mathbb{C}=\mathbb{R}\times\mathbb{R}$ el conjunto de todos los pares ordenados (a,b) de números reales sobre el cual definimos las operaciones siguientes:*

1. **Suma:** *Dados (a,b) y $(c,d)\in\mathbb{C}$, $(a,b)+(c,d)=(a+c,b+d)$.*
2. **Producto:** *Dados (a,b) y $(c,d)\in\mathbb{C}$, $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$.*

El conjunto $\mathbb{C}=\{(a,b):a,\ b\in\mathbb{R}\}$, junto con las operaciones de suma y producto definidas, recibe el nombre de conjunto de los números complejos.

Propiedades.

(S_1) $(z+u)+w=z+(u+w)$, para todo z, u, $w\in\mathbb{C}$.

(S_2) $z+w=w+z$, para todo z, $w\in\mathbb{C}$.

(S_3) Existe un único elemento $\mathbf{0}=(0,0)\in\mathbb{C}$, tal que $z+\mathbf{0}=z$, para todo $z\in\mathbb{C}$.

(S_4) Para cada $z=(a,b)\in\mathbb{C}$, existe un único elemento $-z=(-a,-b)$ tal que $z+(-z)=\mathbf{0}$.

(M_1) $(z\cdot u)\cdot w=z\cdot(u\cdot w)$, para todo z, u, $w\in\mathbb{C}$.

(M_2) $z\cdot w=w\cdot z$, para todo z, $w\in\mathbb{C}$.

(M_3) Existe un único elemento $\mathbf{1}=(1,0)\in\mathbb{C}$, tal que $z\cdot\mathbf{1}=z$, para todo $z\in\mathbb{C}$.

(M_4) Para cada $z=(a,b)\in\mathbb{C}$, $z\neq\mathbf{0}$, existe un único elemento $z^{-1}=(\dfrac{a}{a^2+b^2}\ ,\ \dfrac{-b}{a^2+b^2})$ tal que $z\cdot z^{-1}=\mathbf{1}$

(D) $z\cdot(u+w)=z\cdot u+z\cdot w$, para todo z, u, $w\in\mathbb{C}$.

La función $f:\mathbb{R}\to\mathbb{C}$ definida por: $f(a)=(a,0)$, para todo $a\in\mathbb{R}$, es inyectiva, como es inmediato de verificar. Además verifica que $f(a+b)=f(a)+f(b)$ y $f(a\cdot b)=f(a)\cdot f(b)$, para todo a, $b\in\mathbb{R}$, es decir, preserva las operaciones de suma y multiplicación. En efecto,

$$f(a+b)=(a+b,0)=(a,0)+(b,0)=f(a)+f(b),$$

$$f(a \cdot b) = (a \cdot b, 0) = (a, 0) \cdot (b, 0) = f(a) \cdot f(b).$$

Esto significa que los números de la forma $(a, 0)$ se comportan, respecto de las operaciones de suma y multiplicación, como los números reales a. Esto permite identificar el complejo $(a, 0)$ con el número real a.

Observaciones:

1. Dado $z = (a, b)$, diremos que a es la **parte real** y b la **parte imaginaria** de z. Sin embargo, debemos notar que tanto a como b son reales. Escribimos $a = Re\ z$, $b = Im\ z$.

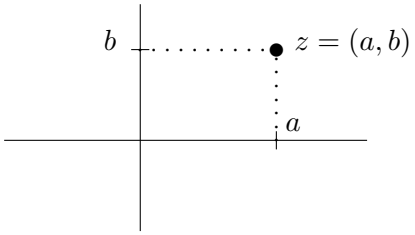
2. Si identificamos al número real x con el complejo $(x, 0)$, o sea, de parte imaginaria nula, es lo mismo hablar en $\mathbb{R}$ de x, que hablar en $\mathbb{C}$ del número $(x, 0)$.
   De aquí resulta que podemos considerar a $\mathbb{R}$ como un subconjunto de $\mathbb{C}$, identificando el número real x con el número complejo $(x, 0)$.

3. Si $b = 0$, entonces $(a, 0)$ se llama complejo real.
   Si $a = 0$ y $b \neq 0$, entonces $(0, b)$ se llama imaginario puro.

Representación geométrica de los números complejos

Teniendo en cuenta que los números complejos se han definido como pares ordenados de números reales, es natural representarlos en un sistema de coordenadas cartesianas ortogonales.

Sabemos que todo punto $P(a, b)$ del plano está determinado por dos números reales a y b que son la abscisa y la ordenada respectivamente de P. Entonces, a cada número complejo $z = (a, b)$ le corresponde un punto del plano de abscisa a y ordenada b, y recíprocamente, a cada punto $P(a, b)$ del plano le corresponde el número complejo $z = (a, b)$ de parte real a y de parte imaginaria b. El punto P correspondiente al número complejo z se llama *afijo* de z.



Si z es un complejo real, entonces su afijo está sobre el eje de las abscisas, que por esta razón se llama eje real. Si z es imaginario puro, entonces su afijo está sobre el eje de las ordenadas, que recibe el nombre de eje imaginario.

Unidad Imaginaria

Veamos ahora que en $\mathbb{C}$ tiene solución la ecuación $x^2 + 1 = 0$, o sea, $x^2 = -1$, y que la solución está dada por el número complejo $(0, 1)$.

Recordemos que la unidad real 1 la podemos escribir como el número complejo $(1, 0)$. Por otro lado, si $x = (0, 1)$, se tiene:

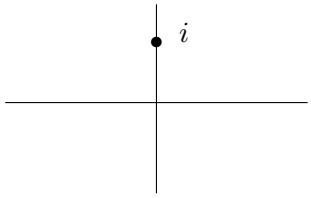
$$\begin{aligned} x^2 &= (0,1) \cdot (0,1) \\ x^2 &= (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) \\ x^2 &= (-1, 0) \end{aligned}$$

Entonces, si en la ecuación $x^2 + 1 = 0$ reemplazamos $x = (0, 1)$, se tiene:

$$(-1, 0) + (1, 0) = (0, 0),$$

es decir, que $x = (0, 1)$ es solución de la ecuación. Esto motiva la siguiente definición.

Definición 7.2 *El número complejo* $(0, 1)$ *recibe el nombre de unidad imaginaria y se nota* $i = (0, 1)$.



Por lo que acabamos de probar, $i^2 = -1$.

Nota 1. Observemos que las operaciones de suma y multiplicación en $\mathbb{C}$ satisfacen las mismas propiedades (S_1) a (S_4), (M_1) a (M_4) y (D) que satisfacen la suma y la multiplicación en el cuerpo de los números reales, por lo que también $\mathbb{C}$, con esas operaciones, es un cuerpo. Sin embargo, a diferencia de $\mathbb{R}$, $\mathbb{C}$ no es un cuerpo ordenado, en el sentido que no es posible definir en $\mathbb{C}$ un orden " $<$" que cumpla las propiedades (E_1) a (E_4) que hacen de $\mathbb{R}$ un cuerpo ordenado. En efecto, si existiese un tal orden, como $i = (0, 1) \neq (0, 0)$, es decir, $i \neq \mathbf{0}$, debería ser

$$0 < i \quad \text{ó} \quad i < 0.$$

Supongamos que $0 < i$. Entonces, por (E_4), $0 \cdot i < i \cdot i$, o sea, $0 < i^2 = -1$. Una contradicción.

Una contradicción similar obtenemos si suponemos que $i < 0$.

Nota 2. El cuerpo $\mathbb{C}$ se obtuvo haciendo el producto cartesiano $\mathbb{R} \times \mathbb{R}$ y definiendo en él las operaciones

$$(a, b) + (a', b') = (a + a', b + b'),$$
$$(a, b) \cdot (a', b') = (aa' - bb', ab' + ba').$$

Si ahora consideramos en forma similar $\mathbb{C} \times \mathbb{C}$ y sobre este producto cartesiano definimos de la misma forma una suma y un producto, no se obtendrá un cuerpo, pues no se verificará la propiedad (M_4). Puede probarse que, en general, si K es un cuerpo, entonces $K \times K$, con las operaciones indicadas, es un cuerpo si y sólo si la ecuación $x^2 + 1 = 0$ no admite solución en K. Al respecto recomendamos al lector la estimulante lectura del libro Notas de Algebra I, de E. Gentile.

Forma binómica.

Vamos a ver ahora que todo número complejo $z = (a, b)$ puede escribirse en la forma $a + bi$.

Es claro que $(a, b) = (a, 0) + (0, b)$. Pero $(0, b)$ puede escribirse $(0, b) = (b, 0) \cdot (0, 1)$, pues $(b, 0) \cdot (0, 1) = (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (0, b)$. Entonces reemplazando, es

$$(a, b) = (a, 0) + (b, 0) \cdot (0, 1)$$

Luego, identificando $(a, 0)$ con a y $(b, 0)$ con b,

$$(a, b) = a + b\, i.$$

La forma binómica nos permite aplicar para la suma y el producto de números complejos todas las propiedades válidas en $\mathbb{R}$, con sólo tener en cuenta que $i^2 = -1$.

Ejemplo: Sean $z = a + bi$ y $z' = c + di$. Entonces

(a) Suma: $z + z' = (a + b\,i) + (c + d\,i) = (a + c) + (b + d)\,i$

(b) Diferencia: $z - z' = (a + b\,i) - (c + d\,i) = (a - c) + (b - d)\,i$

(c) Producto: $z \cdot z' = (a + b\,i) \cdot (c + d\,i) = (ac - bd) + (ad + bc)\,i$

(d) Cociente: $\dfrac{z}{z'} = \dfrac{a + b\,i}{c + d\,i}, \quad z' \neq 0.$

Para transformar el divisor complejo en un divisor real, se multiplica numerador y denominador por $c - d\,i$ (que luego veremos se llama el conjugado de z'), y se obtiene:

$$\frac{z}{z'} = \frac{(a + b\,i)(c - d\,i)}{(c + d\,i)(c - d\,i)} = \frac{(ac + bd) + (bc - ad)\,i}{c^2 + d^2}$$

Observación: Teniendo en cuenta que la división es la operación inversa de la multiplicación, también podría haber efectuado la división z/z' multiplicando a z por el inverso de z':

$$\frac{z}{z'} = z \cdot z'^{-1} = (a + b\,i) \cdot \left(\frac{c}{c^2 + d^2} - \frac{d}{c^2 + d^2}\,i \right) = \frac{(ac + bd) + (bc - ad)\,i}{c^2 + d^2}$$

Ejemplos: Si $z = 3 + 5\,i$ y $z' = 2 - i$, entonces

(a) $(3 + 5\,i) + (2 - i) = 5 + 4\,i$

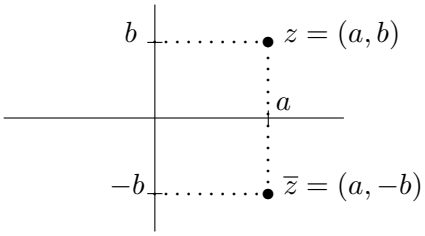
(b) $(3 + 5\,i) - (2 - i) = 1 + 6\,i$

(c) $(3 + 5\,i) \cdot (2 - i) = 11 + 7\,i$

(d) $\dfrac{3 + 5\,i}{2 - i} = \dfrac{(3 + 5\,i)(2 + i)}{(2 - i)(2 + i)} = \dfrac{1 + 13\,i}{5} = \dfrac{1}{5} + \dfrac{13}{5}\,i$

Conjugado de un número complejo

Definición 7.3 *Dado el número complejo $z = (a, b)$ (ó $z = a + b\,i$), llamaremos* **conjugado** *de z al número complejo $\overline{z} = (a, -b)$ (ó $\overline{z} = a - b\,i$).*



Ejemplos:

Si	$z = (-3, 5)$	entonces	$\overline{z} = (-3, -5)$
Si	$z' = 7 + 3\,i$	entonces	$\overline{z'} = 7 - 3\,i$
Si	$v = -2\,i$	entonces	$\overline{v} = +2\,i$
Si	$w = (4, 0)$	entonces	$\overline{w} = (4, 0)$
Si	$u = -5$	entonces	$\overline{u} = -5$

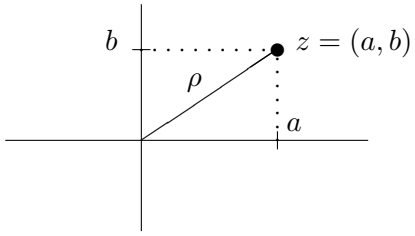
Propiedades del conjugado

Las siguientes propiedades del conjugado de un número complejo, son de fácil demostración. Sea $z = a + b\,i$. Entonces:

1. $\overline{\overline{z}} = z$.
2. $z + \overline{z} = 2\ Re\ z$ (O sea, $z + \overline{z} = 2a$).
3. $z - \overline{z} = 2\ Im\ z\ i$ (O sea, $z - \overline{z} = 2b\ i$).
4. $z \cdot \overline{z} = a^2 + b^2$.
5. $z = \overline{z} \Leftrightarrow z$ es real.
6. $z = -\overline{z} \Leftrightarrow z$ es imaginario puro, ó $z = 0$.
7. $\overline{z + z'} = \overline{z} + \overline{z'}$.
8. $\overline{z - z'} = \overline{z} - \overline{z'}$.
9. $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$.
10. $\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z'}}$, si $z' \neq 0$.

Módulo de un número complejo

Definición 7.4 *Dado un número complejo $z = a + b\ i$, se llama* módulo *de z al número real, positivo o nulo, $\rho = \sqrt{a^2 + b^2}$. Lo notaremos $\rho = |z|$.*



Esta definición tiene sentido, ya que si $z \neq 0$, entonces $a^2 + b^2$ es un número real positivo y $|z|$ es la raíz cuadrada aritmética de ese número (o sea, la única raíz real positiva). Si $z = 0$, entonces $|z| = 0$.

El módulo de $z = (a, b)$ es la longitud del segmento que une el origen y el punto $P(a, b)$.

Ejemplos.

Si $z = 5 + 3\ i$, entonces $|z| = \sqrt{5^2 + 3^2} = \sqrt{25 + 9} = \sqrt{34}$
Si $v = 4 - 3\ i$, entonces $|v| = \sqrt{16 + 9} = \sqrt{25} = 5$.

Observación: Si z es un número real, entonces el módulo de z coincide con el valor absoluto.

Propiedades del módulo:

Sea $z = a + b\ i$. Entonces:

1. $|z| \geq 0$. Evidente por la definición de módulo.
   $|z| = 0 \Leftrightarrow z = 0$.
2. $|z| \geq a$ y $|z| \geq b$.
   $|a|^2 = a^2$, luego $|a|^2 \leq a^2 + b^2 = |z|^2$, de donde, por ser $|a|$ y $|z|$ no negativos, $|a| \leq |z|$. Como $a \in \mathbb{R}$, $a \leq |a|$, luego $a \leq |z|$, o sea $|z| \geq a$.
   Análogamente se prueba que $|z| \geq b$.
3. $|z|^2 = z \cdot \overline{z}$.
   En efecto, $|z| = \sqrt{a^2 + b^2}$, luego $|z|^2 = a^2 + b^2 = z \cdot \overline{z}$.

4. $|z| = |\overline{z}| = |-z|$.
$\sqrt{a^2+b^2} = \sqrt{a^2+(-b)^2} = \sqrt{(-a)^2+(-b)^2}$.

5. $|z \cdot z'| = |z| \cdot |z'|$.
Usando la propiedad 3, se tiene: $|z \cdot z'|^2 = (z \cdot z')(\overline{z \cdot z'}) = (z \cdot \overline{z})(z' \cdot \overline{z'}) = |z|^2 \cdot |z'|^2$.

6. $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$, si $z' \neq 0$.
Podemos escribir $z = z' \cdot \frac{z}{z'}$, luego $|z| = \left|z' \cdot \frac{z}{z'}\right|$, luego $|z| = |z'| \cdot \left|\frac{z}{z'}\right|$, de donde $\frac{|z|}{|z'|} = \left|\frac{z}{z'}\right|$.

7. $|z+z'| \leq |z| + |z'|$.
Calculemos:

$$\begin{aligned} |z+z'|^2 &= (z+z')\overline{(z+z')}, \text{ (por propiedad 3)} \\ &= (z+z')(\overline{z}+\overline{z'}) \text{ (conjugado de la suma)} \\ &= z\overline{z} + z\overline{z'} + z'\overline{z} + z'\overline{z'}, \text{ esto es,} \\ &= |z|^2 + z\overline{z'} + z'\overline{z} + \left|z'\right|^2. \ (*) \end{aligned}$$

Si observamos el segundo y el tercer término de la última expresión se ve que son complejos conjugados. En efecto, $\overline{z\overline{z'}} = \overline{z}\overline{\overline{z'}} = \overline{z}z'$, y la suma de dos complejos conjugados es el duplo de la parte real. Luego

$$z\overline{z'} + \overline{z}z' = 2\ Re\ (z\overline{z}'). \quad (1)$$

Sabemos que la parte real es menor o igual que el módulo, luego

$$Re\ (z\overline{z'}) \leq |z\overline{z'}|$$

$$2\ Re\ (z\overline{z'}) \leq 2(|z\overline{z'}|),$$

y como $\left|\overline{z'}\right| = |z'|$, entonces

$$2\ Re\ (z\overline{z'}) \leq 2|z||z'|. \quad (2)$$

Reemplazando (1) en (*),

$$|z+z'|^2 = |z|^2 + 2\ Re\ (z\overline{z'}) + |z'|^2. \quad (3)$$

Sumando (2) y (3),

$$|z+z'|^2 + 2\ Re\ (z\overline{z'}) \leq |z|^2 + 2\ Re\ (z\overline{z'}) + |z'|^2 + 2|z||z'|.$$

$$|z+z'|^2 \leq \left(|z| + |z'|\right)^2.$$

Como las bases son no negativas resulta

$$|z+z'| \leq |z| + |z'|.$$

que es lo que queríamos probar.

8. $||z| - |z'|| \leq |z - z'|$.
Para probar esta propiedad, pensemos que $|z| - |z'|$ es un número real a y recordemos que:

$$|a| \leq x \Leftrightarrow -x \leq a \leq x, \text{ si } x \geq 0.$$

De acuerdo a esto, probar que

$$|\underbrace{|z| - |z'|}_{a}| \leq \underbrace{|z - z'|}_{x}$$

es equivalente a probar que

$$-|z - z'| \leq |z| - |z'| \leq |z - z'|.$$

Escribamos z y z' de la siguiente forma: $z = z' + (z - z')$, $z' = z + (z' - z)$. Aplicando módulo se tiene: $|z| = |z' + (z - z')|$, pero por la propiedad anterior es $|z| \leq |z'| + |z - z'|$, de donde

$$|z| - |z'| \leq |z - z'|. \quad (1)$$

De la misma manera,
$|z'| = |z + (z' - z)|$, luego $|z'| \leq |z| + |z' - z|$, de donde $|z'| - |z| \leq |z' - z|$.
Pero $|z' - z| = |z - z'|$
Luego

$$|z'| - |z| \leq |z - z'|$$

Multiplicando por -1,

$$-(|z'| - |z|) \geq -|z - z'|,$$

luego

$$|z| - |z'| \geq -|z - z'|,$$

esto es,

$$-|z - z'| \leq |z| - |z'|. \quad (2)$$

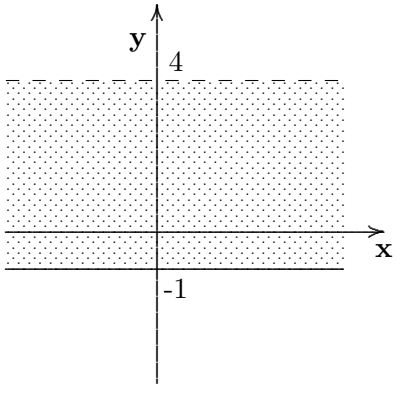
Luego de (1) y (2) resulta

$$-|z - z'| \leq |z| - |z'| \leq |z - z'|$$

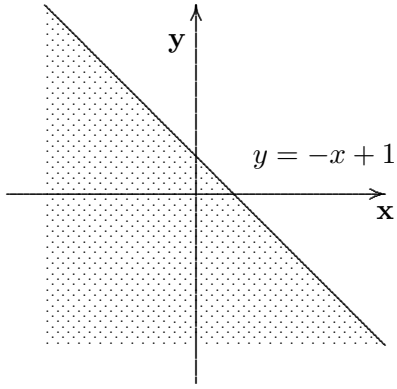
que es lo que queríamos probar.

Ejemplos

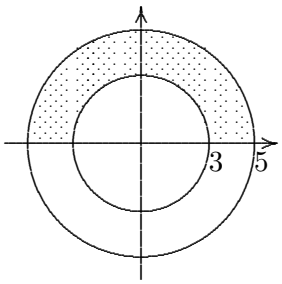
1. Representemos en el plano complejo la región determinada por los $z \in \mathbb{C}$ tales que:
   i) $-1 \leq Im\, z < 4$



   ii) $Im\, z + Re\, z \leq 1$



2. Representar en el plano complejo la región determinada por los $z \in \mathbb{C}$ tales que $3 \leq |z| \leq 5$ y $Im\ z \geq 0$:



Argumento de un número complejo

Definición 7.5 *Dado un número complejo $z = a + bi$, $z \neq 0$, se llama* **argumento** *de z, al ángulo formado por el semieje real positivo y el segmento $\overline{OP}$, y a menos de un múltiplo entero de 2π, tomándose como sentido positivo el sentido antihorario.*

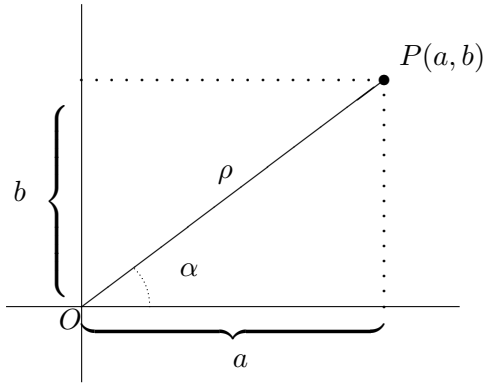
Si α es el argumento de z, también serán argumento de z los ángulos de la forma: $\alpha + 2k\pi$, con $k \in \mathbb{Z}$, o sea, que los valores que toma "argumento de z" son:

$$\ldots,\ \alpha - 3 \cdot 2\pi,\ \alpha - 2 \cdot 2\pi,\ \alpha - 2\pi,\ \alpha,\ \alpha + 2\pi,\ \alpha + 2 \cdot 2\pi,\ \ldots$$

Llamaremos **argumento principal** de z, al argumento de z comprendido entre 0 y 2π, es decir, que α es el argumento principal de z si $0 \leq \alpha < 2\pi$. Para indicar que α es el argumento de z, escribiremos $\alpha = \arg z$.

Expresión polar o trigonométrica de un número complejo

Vimos que al número complejo $z = a+bi$ le corresponde el punto $P(a, b)$ del plano. Entonces, si $z \neq 0$ y consideramos el segmento $\overline{OP}$ y el ángulo que dicho segmento forma con el semieje real positivo, se pueden establecer las siguientes relaciones:



$$\operatorname{sen}\alpha = \frac{b}{\rho} \Rightarrow b = \rho \cdot \operatorname{sen}\alpha$$

$$\cos\alpha = \frac{a}{\rho} \Rightarrow a = \rho \cdot \cos\alpha$$

Entonces

$$\begin{aligned} z = a + bi &= \rho \cdot \cos\alpha + \rho \cdot \operatorname{sen}\alpha \cdot i \\ z = a + bi &= \rho(\cos\alpha + i\operatorname{sen}\alpha) \end{aligned}$$

que se acostumbra escribir

$$z = a + bi \quad = \quad \rho \cdot \operatorname{cis} \alpha$$

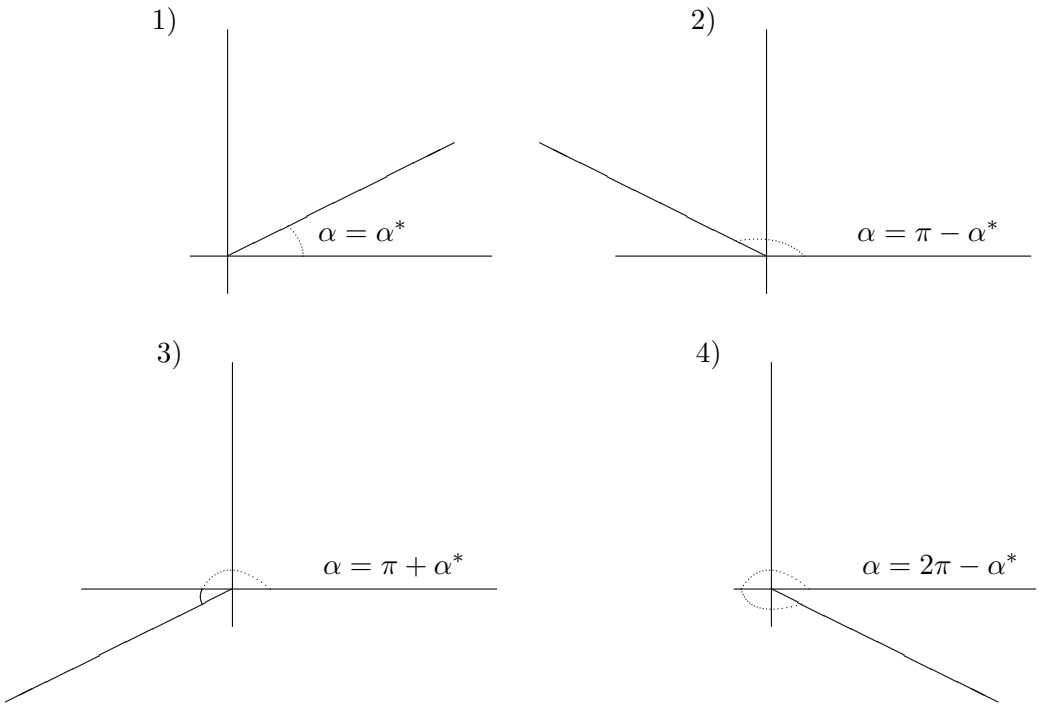
Esta forma de escribir los números complejos se llama **forma polar o trigonométrica** y suele abreviarse también: $z = \rho_\alpha$.

Observando la figura resulta que:

$$\rho = \sqrt{a^2 + b^2} = |z| \quad \text{y} \quad \tan \alpha = \frac{b}{a}\,, \quad \text{esto es,} \quad \alpha = \arctan \frac{b}{a}.$$

En la práctica, para calcular α, puede ser conveniente determinar primero un ángulo del primer cuadrante α^*, haciendo $\alpha^* = \arctan \dfrac{|b|}{|a|}$, y para determinar el cuadrante al cual pertenece α, se considera el signo de a y de b.

1. Si $a > 0$ y $b > 0$, entonces α pertenece al primer cuadrante y entonces $\alpha = \alpha^*$.
2. Si $a < 0$ y $b > 0$, entonces α pertenece al segundo cuadrante y entonces $\alpha = \pi - \alpha^*$.
3. Si $a < 0$ y $b < 0$, entonces α pertenece al tercer cuadrante y entonces $\alpha = \pi + \alpha^*$.
4. Si $a > 0$ y $b < 0$, entonces α pertenece al cuarto cuadrante y entonces $\alpha = 2\pi - \alpha^*$.



Ejemplo. Escribir en forma polar el complejo $z = 2 - 2i$.

En este caso $a = 2$ y $b = -2$. Luego $\rho = \sqrt{a^2 + b^2} = 2\sqrt{2}$. Por otro lado, $\tan \alpha^* = \dfrac{|b|}{|a|} = \dfrac{2}{2} = 1$, luego $\alpha^* = \arctan 1 = \dfrac{\pi}{4}$.

Como $a > 0$ y $b < 0$, entonces α pertenece al cuarto cuadrante. Luego $\alpha = 2\pi - \alpha^*$. Esto es, $\alpha = 7\,\frac{\pi}{4}$. Entonces $z = 2\sqrt{2} \cdot \text{cis}\ 7\,\frac{\pi}{4}$.

Recíprocamente, si tenemos un número complejo escrito en forma trigonométrica $z = \rho \cdot \text{cis}\ \alpha$, podemos pasarlo a la forma binómica calculando los valores de sen α y $\cos\alpha$.

Ejemplo. Sea $z = 2 \cdot \text{cis}\,\frac{\pi}{6}$. Como $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$ y $\text{sen}\,\frac{\pi}{6} = \frac{1}{2}$, entonces $z = 2 \cdot \left(\frac{\sqrt{3}}{2} + i\,\frac{1}{2}\right) = \sqrt{3} + i$.

Observaciones

1. El argumento de $z = (0, 0)$ no está definido.
2. El número complejo z es real positivo $\Leftrightarrow$ su argumento principal es $\alpha = 0$. Por ejemplo, $3 = 3 \cdot \text{cis}\ 0$.
3. El número complejo z es real negativo $\Leftrightarrow$ su argumento principal es $\alpha = \pi$. Así, $-2 = 2 \cdot \text{cis}\ \pi$.
4. El número complejo z es imaginario puro $\Leftrightarrow$ su argumento principal es $\alpha = \frac{\pi}{2}$ ó $\alpha = 3\,\frac{\pi}{2}$. Por ejemplo, $i = \text{cis}\,\frac{\pi}{2}$, $-i = \text{cis}\,\frac{3\pi}{2}$.

7.2 Operaciones en forma polar

Producto de números complejos en forma polar

Teorema 7.6 *Si $z = \rho\ \text{cis}\ \alpha$ y $z' = \rho'\ \text{cis}\ \alpha'$, entonces $z \cdot z' = \rho\rho'\text{cis}\ (\alpha + \alpha')$*

Demostración.

$$\begin{aligned}
z \cdot z' &= \rho\ \text{cis}\ \alpha\ \rho'\text{cis}\ \alpha' \\
&= (\rho\ \cos\alpha + \rho\ i\text{sen}\ \alpha)(\rho'\ \cos\alpha' + \rho'\ i\ \text{sen}\ \alpha') \\
&= \rho\ \cos\alpha\rho'\ \cos\alpha' + \rho\ \cos\alpha\rho'\ i\ \text{sen}\ \alpha' + \rho\ i\ \text{sen}\ \alpha\rho'\ \cos\alpha' + \rho\ \rho'\ i^2\ \text{sen}\ \alpha\ \text{sen}\ \alpha' \\
&= \rho\rho'[(\cos\alpha\ \cos\alpha' - \text{sen}\ \alpha\ \text{sen}\ \alpha') + i(\cos\alpha\ \text{sen}\ \alpha' + \text{sen}\ \alpha\ \cos\alpha')] \\
&= \rho\rho'[\cos(\alpha + \alpha') + i\ \text{sen}\ (\alpha + \alpha')] \\
&= \rho\rho'\ \text{cis}\ (\alpha + \alpha').
\end{aligned}$$

□

Es decir, el producto de dos complejos expresados en forma trigonométrica es otro complejo cuyo módulo es el producto de los módulos y cuyo argumento es la suma de los argumentos de los complejos dados.

Ejemplo. Si $z = 2\ \text{cis}\,\frac{\pi}{6}$ y $z' = 3\ \text{cis}\,\frac{\pi}{4}$, entonces $z \cdot z' = 2 \cdot 3\ \text{cis}\,\left(\frac{\pi}{6} + \frac{\pi}{4}\right)$, $z \cdot z' = 6 \cdot\ \text{cis}\ 5\,\frac{\pi}{12}$

Cociente de números complejos en forma polar

Sea $z = \rho \text{ cis } \alpha$ y $z' = \rho' \text{ cis } \alpha' \neq 0$ ($\Leftrightarrow \rho' \neq 0$). Queremos hallar $\frac{z}{z'} = z'' = \rho'' \text{ cis } \alpha''$. Entonces tenemos que hallar ρ'' y α''.

De $\frac{z}{z'} = \frac{\rho \text{ cis } \alpha}{\rho' \text{ cis } \alpha'} = \rho'' \text{ cis } \alpha''$ resulta:
$\rho \text{ cis } \alpha = \rho'' \text{ cis } \alpha'' \cdot \rho' \text{ cis } \alpha' \Rightarrow \rho \text{ cis } \alpha = \rho'' \cdot \rho' \text{ cis } (\alpha'' + \alpha') \Rightarrow \rho = \rho'' \cdot \rho'$ y $\alpha = \alpha'' + \alpha' + 2k\pi$, con $k \in \mathbb{Z}$.
De donde

$$\rho'' = \frac{\rho}{\rho'} \quad \text{y} \quad \alpha'' = \alpha - \alpha' - 2k\pi, \ k \in \mathbb{Z}.$$

Luego

$$\frac{z}{z'} = \frac{\rho}{\rho'} \text{ cis } (\alpha - \alpha').$$

Es decir, el cociente de dos números complejos expresados en forma polar es otro número complejo cuyo módulo es el cociente de los módulos y cuyo argumento es la diferencia de los argumentos de los complejos dados.

Ejemplo: Sean $z = 3 \text{ cis } \frac{\pi}{4}$ y $z' = 2 \text{ cis } \frac{\pi}{2}$. Entonces $\frac{z}{z'} = \frac{3}{2} \text{ cis } (\frac{\pi}{4} - \frac{\pi}{2})$, $\frac{z}{z'} = \frac{3}{2} \text{ cis } (-\frac{\pi}{4})$.
Luego $\frac{z}{z'} = \frac{3}{2} \text{ cis } 7\ \frac{\pi}{4}$.

Potenciación de números complejos

Definimos primero potencia de números complejos para exponente natural. Definimos por recurrencia:

$$\begin{aligned} z^1 &= z \\ z^{n+1} &= z^n \cdot z^1 \end{aligned}$$

Ahora definimos potencia para $z \neq 0$ y para exponente entero de la siguiente forma:

$$\begin{aligned} z^0 &= 1 \\ z^n &= \left(z^{-1}\right)^{-n} \text{ para } n \in \mathbb{Z},\ n < 0 \end{aligned}$$

Fórmula de De Moivre (1667-1754)

La fórmula de De Moivre se usa para calcular la potencia **entera** de un número complejo expresado en forma trigonométrica.

Teorema 7.7 *Sea $z \in \mathbb{C}$, $z = \rho(\cos\alpha + i \text{ sen } \alpha)$. Entonces para todo $n \in \mathbb{Z}$, es:*

$$z^n = [\rho(\cos\alpha + i \text{ sen } \alpha)]^n = \rho^n(\cos n\alpha + i \text{ sen } n\alpha).$$

Demostración. Por inducción se demuestra que vale para $n \in \mathbb{N}$ y luego se prueba que vale para todo $n \in \mathbb{Z}$.

a) Probemos que la fórmula vale para exponente natural, o sea, que

$$(\rho \text{ cis } \alpha)^n = \rho^n \text{ cis } n\alpha, \ \text{ para todo } n \in \mathbb{N}.$$

1. Probemos que vale para $n = 1$, es decir, que

$$(\rho \text{ cis } \alpha)^1 = \rho^1 \text{ cis } 1\alpha,$$

lo cual es evidentemente cierto.

2. Supongamos que vale para $n = k$, es decir, que

$$(\rho \text{ cis } \alpha)^k = \rho^k \text{ cis } k\alpha.$$

3. Probemos que vale para $n = k + 1$, o sea, que

$$(\rho \text{ cis } \alpha)^{k+1} = \rho^{k+1} \text{ cis } (k+1)\alpha.$$

$(\rho \text{ cis } \alpha)^{k+1} = (\rho \text{ cis } \alpha)^k \ \rho \text{ cis } \alpha = \rho^k \text{ cis } k\alpha \ \rho \text{ cis } \alpha = \rho^{k+1} \text{ cis } (k\alpha + \alpha) = \rho^{k+1} \text{ cis } (k+1)\alpha$. Por lo tanto, vale para $n = k + 1$.

En consecuencia, por el principio de inducción, es válida para todo número natural.

b) Probemos ahora que vale para $n = 0$, esto es, que

$$(\rho \text{ cis } \alpha)^0 = \rho^0 \text{ cis } 0\alpha$$

Pero $(\rho \text{ cis } \alpha)^0 = 1$ y $\rho^0 \text{ cis } 0\alpha = 1(1 + 0) = 1$.

c) Probemos finalmente que vale para exponentes negativos, es decir, que

$$(\rho \text{ cis } \alpha)^n = \rho^n \text{ cis } n\alpha, \text{ si } n \in \mathbb{Z},\ n < 0.$$

Por definición de potencia de exponente negativo,

$$(\rho \operatorname{cis} \alpha)^n = [(\rho \operatorname{cis} \alpha)^{-1}]^{-n} = \frac{1}{(\rho \text{ cis } \alpha)^{-n}} = (\text{ya que } -n \text{ es un número natural}) = \frac{1}{\rho^{-n} \text{ cis } (-n)\alpha} =$$

$$\frac{\rho^n}{\text{cis } (-n)\alpha} = \frac{\rho^n}{\cos n\alpha - i \text{ sen } n\alpha} = \frac{\rho^n(\cos n\alpha + i \text{ sen } n\alpha)}{(\cos n\alpha - i \text{ sen } n\alpha)(\cos n\alpha + i \text{ sen } n\alpha)} = \frac{\rho^n(\cos n\alpha + i \text{ sen } n\alpha)}{\cos^2 n\alpha + \text{sen }^2 n\alpha} =$$

$$\frac{\rho^n(\text{cis } n\alpha)}{1} = \rho^n \text{ cis } n\alpha, \text{ que es lo que queríamos probar.}$$

□

Ejemplos.

(a) Sea $z = \sqrt{2} \operatorname{cis} 3\,\frac{\pi}{4}$. Calcular z^{16}.

$$z^{16} = \left(\sqrt{2}\right)^{16} \text{ cis } 16 \cdot 3\,\frac{\pi}{4} = 2^8(\cos 0 + i \text{ sen } 0) = 256.$$

(b) Sea $z = (1 - i)$. Hallar z^{10}.

$$z = \sqrt{2} \operatorname{cis} 7\,\frac{\pi}{4} \Rightarrow z^{10} = \left(\sqrt{2}\right)^{10} \text{ cis } 10 \cdot 7\,\frac{\pi}{4} = 2^5 \operatorname{cis} 3\,\frac{\pi}{2} = 32(0 + i(-1)) = -32i.$$

Radicación de números complejos

Dado un número complejo z y $n \in \mathbb{N}$, llamaremos raíz n-ésima de z a todo número complejo w tal que $w^n = z$. Notaremos con $\sqrt[n]{z}$ al conjunto de todas las raíces n-ésimas de z.

Se plantea entonces el problema de averiguar si dado un número complejo z, existe siempre alguna raíz n-ésima de z, y se demuestra el siguiente teorema.

Teorema 7.8 *Dado un número complejo $z = \rho \operatorname{cis} \alpha$, y $n \in \mathbb{N}$, existen exactamente n raíces n-ésimas de z, que son de la forma*

$$r_k = \sqrt[n]{\rho} \operatorname{cis} \frac{\alpha + 2k\pi}{n}, \quad \textit{con } k = 0, 1, 2, 3, \ldots, n-1.$$

Demostración. Si $w = |w| \cdot \operatorname{cis} \theta$ es una raíz n-ésima de z, entonces $w^n = z$, esto es,

$$|w|^n \cdot \operatorname{cis} n \cdot \theta = z = \rho \cdot \operatorname{cis} \alpha.$$

Luego

$$|w|^n = \rho \qquad \text{y} \qquad n \cdot \theta = \alpha + 2k\pi, \quad k \in \mathbb{Z}.$$

Luego

$$|w| = \sqrt[n]{\rho} \qquad \text{y} \qquad \theta = \frac{\alpha + 2k\pi}{n}, \quad k \in \mathbb{Z}.$$

Se tiene entonces que el módulo de w está unívocamente determinado: es la raíz aritmética del módulo de z. Pero no ocurre lo mismo con el argumento, pues en su expresión aparece un número k que puede tomar cualquier valor entero.

Cuando k toma los valores 0, 1, 2, ..., $n-1$, se obtienen los siguientes argumentos:

$$\frac{\alpha}{n}, \quad \frac{\alpha + 2\pi}{n}, \quad \frac{\alpha + 2 \cdot 2\pi}{n}, \quad \ldots\ldots, \quad \frac{\alpha + (n-1) \cdot 2\pi}{n}.$$

Los n números complejos

$$w_k = \sqrt[n]{\rho} \cdot \operatorname{cis} \frac{a + 2k\pi}{n}, \quad 0 \leq k \leq n-1$$

son todos distintos. En efecto, $w_k \neq w_{k'}$, o lo que es lo mismo, $\dfrac{w_k}{w_{k'}} \neq 1$, ya que su argumento

$$\frac{\alpha + 2k\pi}{n} - \frac{\alpha + 2k'\pi}{n} = \frac{2(k-k')\pi}{n} = \frac{k-k'}{n} \cdot 2\pi$$

no es un múltiplo de 2π, pues $0 < |k - k'| < n$.

Por otro lado, si k toma valores distintos de 0, 1, ..., $n-1$, se obtienen ángulos que difieren de los dados en múltiplos de 2π, y por lo tanto la correspondiente raíz coincide con una de las indicadas. □

Observación. Si $z = 0$, la única raíz n-ésima de z es $w = 0$.

Ejemplo. Hallar las raíces cúbicas de $z = -1 + i$.
De $z = -1 + i$, se tiene $\rho = \sqrt{2}$ y $\alpha^* = \dfrac{\pi}{4}$, luego $\alpha = \pi - \dfrac{\pi}{4}$, esto es, $\alpha = 3\,\dfrac{\pi}{4}$.
Luego $z = \sqrt{2} \operatorname{cis} 3\,\dfrac{\pi}{4}$. Entonces

$$\sqrt[3]{z} = \sqrt[3]{\sqrt{2} \operatorname{cis} 3\,\frac{\pi}{4}} = \sqrt[3]{\sqrt{2}} \operatorname{cis} \frac{3\,\dfrac{\pi}{4} + 2k\pi}{3}, \quad \text{con } k = 0, 1, 2.$$

Para $k=0$, $\quad r_0=\sqrt[6]{2}\ \text{cis}\ \dfrac{3\,\dfrac{\pi}{4}}{3}$, $\quad$ luego $r_0=\sqrt[6]{2}\ \text{cis}\ \dfrac{\pi}{4}$.

Para $k=1$, $\quad r_1=\sqrt[6]{2}\ \text{cis}\ \dfrac{3\,\dfrac{\pi}{4}+2\pi}{3}$, $\quad$ luego $r_1=\sqrt[6]{2}\ \text{cis}\ \dfrac{11\pi}{12}$.

Para $k=2$, $\quad r_2=\sqrt[6]{2}\ \text{cis}\ \dfrac{3\,\dfrac{\pi}{4}+4\pi}{3}$, $\quad$ luego $r_2=\sqrt[6]{2}\ \text{cis}\ \dfrac{19\pi}{12}$.

Representación geométrica de las raíces.

Dado $z\in\mathbb{C}$, $z\neq 0$, y $n\in\mathbb{N}$, vimos que las raíces n-ésimas de z son de la forma $r_k=\sqrt[n]{\rho}\ \text{cis}\ \dfrac{\alpha+2k\pi}{n}$, con $k=0,1,\ldots,n-1$. Entonces resulta que todas las raíces tienen el mismo módulo $\sqrt[n]{\rho}$, y sus argumentos principales son de la forma:

$$\frac{\alpha}{n},\quad \frac{\alpha}{n}+\frac{2\pi}{n},\quad \frac{\alpha}{n}+\frac{2\cdot 2\pi}{n},\ldots,\quad \frac{\alpha}{n}+\frac{(n-1)2\pi}{n}.$$

Como todas las raíces n-ésimas tienen el mismo módulo, entonces los afijos de las n raíces n-ésimas equidistan del origen de coordenadas, es decir, se encuentran sobre la circunferencia de centro en el origen y radio $\sqrt[n]{\rho}$.

El argumento de r_0 es $\dfrac{\alpha}{n}$.

Observemos que el argumento principal de r_1 se obtiene sumándole al anterior $\dfrac{2\pi}{n}$, y así sucesivamente, el argumento principal de cada raíz se obtiene sumándole al anterior $\dfrac{2\pi}{n}$. Como $\dfrac{2\pi}{n}$ es el número que resulta al dividir la circunferencia en n partes iguales, entonces los afijos de las n raíces n-ésimas de z $(n>2)$ son los vértices de un polígono regular de n lados inscripto en la circunferencia con centro en el origen y radio $\sqrt[n]{\rho}$.

Ejemplo. Hallar $\sqrt[4]{-1+\sqrt{3}\,i}$, y representar las raíces.

En este caso, $\rho=2$, $\alpha^*=\dfrac{\pi}{3}\Rightarrow\alpha=\pi-\dfrac{\pi}{3}\Rightarrow\alpha=2\,\dfrac{\pi}{3}$. Luego $z=2\ \text{cis}\ 2\dfrac{\pi}{3}$. Entonces

$$\sqrt[4]{-1+\sqrt{3}\,i}=\sqrt[4]{2}\cdot\text{cis}\ \frac{2\frac{\pi}{3}+2k\pi}{4}\ ,\ \text{con } k=0,1,2,3.$$

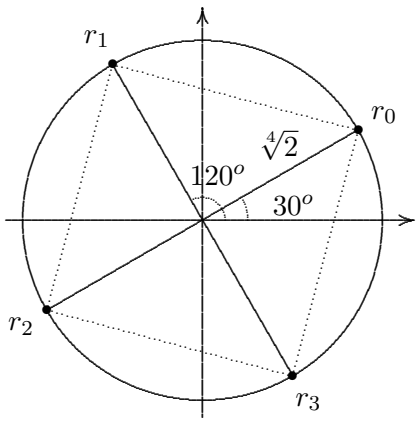
Se tiene entonces

$k=0;\ r_0=\sqrt[4]{2}\ \text{cis}\ \dfrac{\pi}{6}=\sqrt[4]{2}\ \left(\dfrac{\sqrt{3}}{2}+\dfrac{1}{2}i\right)$

$k=1;\ r_1=\sqrt[4]{2}\ \text{cis}\ 2\,\dfrac{\pi}{3}=\sqrt[4]{2}\ \left(-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i\right)$

$k=2;\ r_2=\sqrt[4]{2}\ \text{cis}\ 7\,\dfrac{\pi}{6}=\sqrt[4]{2}\ \left(-\dfrac{\sqrt{3}}{2}-\dfrac{1}{2}i\right)$

$k=3;\ r_3=\sqrt[4]{2}\ \text{cis}\ 5\,\dfrac{\pi}{3}=\sqrt[4]{2}\ \left(\dfrac{1}{2}-\dfrac{\sqrt{3}}{2}i\right)$



7.3 Raíces de la unidad

Sea el número complejo $z = 1$. Entonces $\rho = 1$ y $\alpha = 0$, y por lo tanto, las raíces n-ésimas de 1 están dadas por:

$$\sqrt[n]{1 \text{ cis } 0^\circ} = \sqrt[n]{1} \text{ cis } \frac{2k\pi}{n}, \text{ con } k = 0, 1, \cdots, n-1.$$

Una de las raíces n-ésimas de 1 es 1, que se obtiene para $k = 0$. Se puede observar que, si n es un número par, existen dos raíces reales que son $+1$ y -1, y si n es impar existe una sola raíz real, que es 1. Geométricamente, los afijos de las n raíces n-ésimas de la unidad, son los vértices de un polígono regular de n lados inscripto en una circunferencia de radio 1.

Ejemplo. Las cuatro raíces cuartas de 1 son:

$$\begin{aligned} r_0 &= \sqrt[4]{1} \text{ cis } 0^\circ = 1(1 + 0i) = 1, \\ r_1 &= \sqrt[4]{1} \text{ cis } 90^\circ = 1(0 + 1i) = i, \\ r_2 &= \sqrt[4]{1} \text{ cis } 180^\circ = 1(-1 + 0i) = -1, \\ r_3 &= \sqrt[4]{1} \text{ cis } 270^\circ = 1(0 + (-1)i) = -i. \end{aligned}$$

Observación: Dado un número $z \in \mathbb{C}$, todas sus raíces n-ésimas se obtienen multiplicando una cualquiera de ellas por cada una de las n raíces n-ésimas de la unidad, más precisamente, sea w una raíz n-ésima de z y sean u_1, u_2, ..., u_n las n raíces n-ésimas de 1. Entonces los números complejos

$$w \cdot u_1, \;\; w \cdot u_2, \;\; \ldots\ldots, w \cdot u_n$$

son las n raíces n-ésimas de z.

En efecto, si $z = 0$, entonces el resultado es trivial. Si $z \neq 0$, entonces

$$(w \cdot u_i)^n = w^n \cdot u_i^n = z \cdot 1 = z, \;\; 1 \leq i \leq n,$$

luego los números $w \cdot u_i$ son raíces n-ésimas de z. Además son todos distintos, pues si $w \cdot u_i = w \cdot u_j$, entonces $u_i = u_j$, pues $w \neq 0$.

Ejemplos.

1. Sabemos que las cuatro raíces cuartas de la unidad son: $r_0 = 1$, $r_1 = i$, $r_2 = -1$, $r_3 = -i$. Entonces, las raíces cuartas de un número $z \in \mathbb{C}$ se pueden determinar multiplicando una raíz cuarta de z por las cuatro raíces cuartas de 1. Por un ejemplo anterior sabemos que las raíces cuartas de $z = -1 + \sqrt{3}\, i$ son:

   $$w_0 = \sqrt[4]{2} \text{ cis } \frac{\pi}{6}, \;\; w_1 = \sqrt[4]{2} \text{ cis } 2\,\frac{\pi}{3}, \;\; w_2 = \sqrt[4]{2} \text{ cis } 7\,\frac{\pi}{6}, \;\; w_3 = \sqrt[4]{2} \text{ cis } 5\,\frac{\pi}{3}.$$

   Entonces, si tomamos una de ellas, por ejemplo, w_0, y la multiplicamos por r_0, r_1, r_2, r_3, obtenemos las cuatro raíces cuartas de z.
   En efecto: $w_0 = \sqrt[4]{2} \text{ cis } \frac{\pi}{6} = \sqrt[4]{2}\, \left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right)$.
   $w_0 \cdot r_0 = \sqrt[4]{2}\, \left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) \cdot 1 = \sqrt[4]{2}\, \left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right)$.

$$w_0 \cdot r_1 = \sqrt[4]{2}\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)\cdot i = \sqrt[4]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right).$$
$$w_0 \cdot r_2 = \sqrt[4]{2}\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)\cdot (-1) = \sqrt[4]{2}\left(-\frac{\sqrt{3}}{2}-\frac{1}{2}i\right).$$
$$w_0 \cdot r_3 = \sqrt[4]{2}\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)\cdot (-i) = \sqrt[4]{2}\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right).$$

2. Hallar las raíces cuartas de $z = 81$.
   Una raíz cuarta de 81 es 3. Luego todas las raíces son:

$$\begin{array}{rcrcr} 3\cdot r_0 & = & 3\cdot 1 & = & 3 \\ 3\cdot r_1 & = & 3\cdot i & = & 3i \\ 3\cdot r_2 & = & 3\cdot (-1) & = & -3 \\ 3\cdot r_3 & = & 3\cdot (-i) & = & -3i \end{array}$$

   Las cuatro raíces cuartas de 81 son: 3, -3, $3i$, $-3i$.

Sea $n \in \mathbb{N}$, n fijo, y sea G_n el conjunto de las raíces n-ésimas de la unidad. Se tiene el siguiente resultado cuya demostración se deja como ejercicio:

Teorema 7.9 *G_n es cerrado con respecto a la multiplicación. Además, si $u \in G_n$, $u^{-1} \in G_n$ y $u^k \in G_n$ para todo $k \in \mathbb{N}$.*

Raíces primitivas de la unidad

Consideremos el siguiente ejemplo: las raíces cuartas de la unidad son 1, i, -1 y $-i$. De estas cuatro raíces se observa que dos de ellas, 1 y -1, son tales que elevándolas a exponentes naturales **menores** que 4 también se obtiene la unidad. Por ejemplo: $1^1 = 1$, $1^2 = 1$, $1^3 = 1$, $(-1)^2 = 1$.

Sin embargo, las otras dos raíces, i y $-i$, son tales que el menor exponente natural al cual hay que elevarlas para obtener la unidad es 4, ya que: $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ y $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$.

Esta clasificación de las raíces cuartas de 1 nos lleva a la siguiente definición.

Definición 7.10 *Se llaman raíces primitivas de n-ésimo orden de la unidad, a aquellas raíces n-ésimas de la unidad que no son raíces de la unidad de un orden menor que n. Es decir, si ϵ es una raíz primitiva de n-ésimo orden de la unidad, entonces $\epsilon^n = 1$ y no existe $k \in \mathbb{N}$ tal que $k < n$ y $\epsilon^k = 1$.*

Ejemplo. En las raíces cuartas de 1, i y $-i$ son raíces primitivas de cuarto orden, 1 es raíz primitiva de primer orden y -1 es raíz primitiva de orden 2.

El siguiente teorema nos da una forma de calcular las raíces primitivas.

Teorema 7.11 *Las raíces n-ésimas primitivas de la unidad se obtienen dando a k en la fórmula*

$$u = \cos\frac{2k\pi}{n} + i\,\operatorname{sen}\frac{2k\pi}{n}$$

valores relativamente primos con n y menores que n.

Demostración. Sea u una raíz n-ésima de 1. Entonces

$$u = \cos\frac{2k\pi}{n} + i \operatorname{sen}\frac{2k\pi}{n}\,, \quad 0 \le k \le n-1.$$

Luego

$$u^h = \cos\frac{2kh\pi}{n} + i \operatorname{sen}\frac{2kh\pi}{n}.$$

Entonces, u es raíz de orden h de 1 (esto es, $u^h = 1$) $\Leftrightarrow$ $\dfrac{2kh\pi}{n}$ es múltiplo de 2π $\Leftrightarrow$ $n|kh$.
Ahora bien,

(i) Si $(k,n) = 1$, entonces $n|h$. Luego el menor valor posible de h es n, esto es, u es raíz primitiva de orden n.

(ii) Si $(k,n) = d \neq 1$, sean $k' = \dfrac{k}{d}$ y $n' = \dfrac{n}{d}$. Entonces $u = \cos\dfrac{2k'\pi}{n'} + i \operatorname{sen}\dfrac{2k'\pi}{n'}$, y como $(k',n') = 1$, entonces, por (i), u es una raíz primitiva de orden $n' < n$.

□

De este último teorema resulta que para un orden n determinado, hay tantas raíces primitivas de ese orden, como números relativamente primos con n y menores que n. Este número se llama el indicador de Euler de n, y se indica $\varphi(n)$. Si n es un número primo, entonces todas las raíces n-ésimas de la unidad son primitivas de ese orden, excepto 1 (que se obtiene para $k = 0$).

Conociendo una raíz primitiva de n-ésimo orden de la unidad, se pueden hallar todas las raíces n-ésimas de la unidad:

Teorema 7.12 *Sea u una raíz n-ésima de 1. u es una raíz n-ésima primitiva si y sólo si u^0, u, u^2, …, u^{n-1} son todas las raíces n-ésimas de 1.*

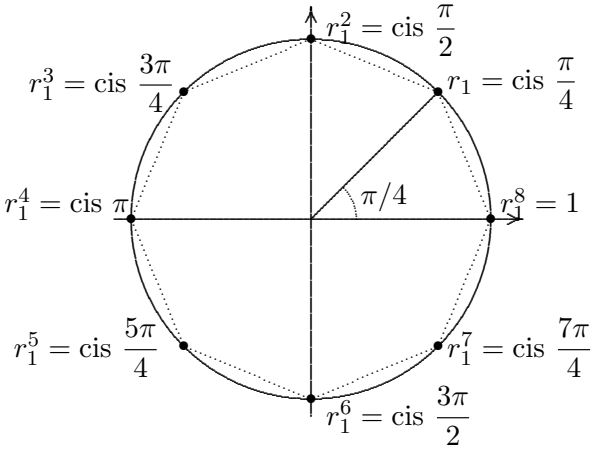
Demostración. Es claro que los números $1, u, u^2, \ldots, u^{n-1}$ son raíces n-ésimas de 1, pues G_n es cerrado por potencias naturales. Además, son distintos, pues si fuese $u^r = u^s$ con $0 \le r < s \le n-1$, sería $u^{s-r} = 1$. Pero $0 < s - r < n$, lo que contradice la hipótesis de que u es raíz primitiva de orden n.
Luego $1 = u^0, u, u^2, \ldots, u^{n-1}$ son todas las raíces n-ésimas de 1.
Recíprocamente, si u es tal que $1 = u^0, u, u^2, \ldots, u^{n-1}$ son todas las raíces n-ésimas de 1, entonces u es raíz n-ésima primitiva ya que $u^n = 1$ y n es el menor exponente natural con esa propiedad. □

Ejemplo: Calcular las raíces primitivas de la unidad de octavo orden.
Debemos dar a k los valores 1, 3, 5 y 7 en la fórmula

$$\cos\frac{2k\pi}{8} + i \operatorname{sen}\frac{2k\pi}{8}.$$

Entonces:

$$\begin{aligned}
&\text{Si } k=1, \quad r_1 = \operatorname{cis}\frac{2\pi}{8}, \quad \text{o bien, } r_1 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\
&\text{Si } k=3, \quad r_3 = \operatorname{cis}\frac{3\pi}{4}, \quad \text{o bien, } r_3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\
&\text{Si } k=5, \quad r_5 = \operatorname{cis}\frac{5\pi}{4}, \quad \text{o bien, } r_5 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\
&\text{Si } k=7, \quad r_7 = \operatorname{cis}\frac{7\pi}{4}, \quad \text{o bien, } r_7 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i
\end{aligned}$$


$r_1^2 = \text{cis } \frac{\pi}{2}$
$r_1^3 = \text{cis } \frac{3\pi}{4}$
$r_1 = \text{cis } \frac{\pi}{4}$
$r_1^4 = \text{cis } \pi$
$\pi/4$
$r_1^8 = 1$
$r_1^5 = \text{cis } \frac{5\pi}{4}$
$r_1^7 = \text{cis } \frac{7\pi}{4}$
$r_1^6 = \text{cis } \frac{3\pi}{2}$

7.4 Ejercicios

1. (a) Escribir en la forma $a + b\,i$ los siguientes números complejos:
   $(0, -\frac{1}{2})$, $(\sqrt{3}, 0)$, $(-1, 1)$, $(0, 0)$.
   (b) Escribir en la forma (a, b) los siguientes números complejos:
   $-3 + i$, 2 , $-i$, $\frac{1}{2} - \frac{\sqrt{3}}{2}\,i$.
   (c) Escribir en la forma $a + b\,i$ los siguientes números complejos:
   $(2 + 5\,i) + (3 - i) + \frac{1}{2}\,i$, $(3 - 5\,i) - (7 - 2\,i) + (1 - 3\,i)$,
   $(2 - 3\,i) \cdot (-2 + 5\,i) \cdot i$, $2\,i \cdot (\frac{1}{3} + 7\,i) - (1 - 2\,i) \cdot (3 + 4\,i)$.

2. Calcular:
   (a) $i^{14} - i^{9} + 3\,i^{5} - i^{3} + 1$.
   (b) $i^{18} - 3\,i^{7} + i^{2}\,(1 - i^{4}) - (-i)^{26}$.

3. Hallar la parte real e imaginaria de :
   i , 3 , $-2\,i$, $\frac{1}{i}$, $\frac{1}{1-i}$, $\frac{1-i}{3-i}$, $\frac{1}{1+i} + \frac{1}{1-i}$, $\frac{1+i}{1-i}$.

4. Hallar los módulos y los conjugados de los siguientes números complejos:
   (a) $-\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$
   (b) $\frac{2}{1 - \sqrt{2}\,i}$
   (c) $\frac{1}{i} + i$
   (d) $|1 - i| + i$

5. Probar las siguientes relaciones:
   (a) $z + \overline{z} = 2\ Re\ z$
   (b) $z - \overline{z} = 2\ Im\ z\ i$
   (c) $z = \overline{z} \ \Leftrightarrow\ Im\ z = 0$
   (d) $\overline{z} = -z \ \Leftrightarrow\ Re\ z = 0$
   (e) $Re\ z = Re\ \overline{z}$
   (f) $Im\ \overline{z} = -Im\ z$
   (g) $z \cdot \overline{z} = |z|^2$

6. (a) Hallar todos los números complejos z, tales que
   (i) $-z + i = -i + 3$
   (ii) $(-1 + i) \cdot z - (1 - i) = 2 + 3\ i$
   (b) Hallar los números complejos z, w tales que $z + w = 6$ y $z - w = 2\,i$.

7. (a) ¿Para qué valores reales de x e y se satisfacen las siguientes igualdades?
   (i) $2x - y\ i = 4y - 6 - 4\ i$
   (ii) $x\ i + y\ i = 4\ i + 5x$
   (b) ¿Para qué valores reales de x, z es un número real?
   (i) $z = 1 - (x - 2)10\ i$

(ii) $z = (-4 + 3\,i) + (2x + 1)\,i$

8. Probar que:

   (a) $|z| = 1 \Leftrightarrow z^{-1} = \overline{z}$.

   (b) $z + \dfrac{1}{z} \in \mathbb{R} \Leftrightarrow Im\, z = 0$ ó $|z| = 1$.

   (c) Si $z + w \in \mathbb{R}$ y $z \cdot w \in \mathbb{R}$ entonces $z, w \in \mathbb{R}$ ó $z = \overline{w}$.

   (d) Si $|z| = 1$ entonces $|z - w| = |1 - w \cdot \overline{z}|$. (Sugerencia: escribir $|z - w| = |z - w| \cdot |\overline{z}|$).

9. Hallar la forma binómica de:

   (a) $z = 2_{\,\frac{\pi}{3}}$ (b) $z = 1_{\,\frac{\pi}{4}}$

   (c) $z = \sqrt{3}_{-\frac{\pi}{2}}$ (d) $z = \dfrac{1}{2}(\cos\dfrac{2}{3}\,\pi + i\,\mathrm{sen}\,\dfrac{2}{3}\,\pi)$

   (e) $z = 2\,(\cos\dfrac{7}{6}\,\pi + i\,\mathrm{sen}\,\dfrac{7}{6}\,\pi)$

10. Hallar la forma polar de:

    (a) $-1 + i$ (b) -17

    (c) $-i$ (d) $i^{15} - 1$

    (e) $\mathrm{sen}\,\dfrac{\pi}{6} + i\,\mathrm{sen}\,\dfrac{\pi}{3}$ (f) $\dfrac{1}{2} - i\,\mathrm{sen}\,\dfrac{\pi}{3}$

    (g) $(2 + 2\,i)^{-1}$ (h) $\mathrm{sen}\,\alpha + i\,\mathrm{sen}\,\alpha, \quad \pi < \alpha < 2\,\pi$

    (i) $\dfrac{1}{2}\,(\cos\dfrac{11}{3}\pi - i\,\mathrm{sen}\,\dfrac{13}{3}\,\pi)$

11. Calcular, pasando previamente a forma polar y expresar el resultado en forma binómica.

    (a) $(1 + \sqrt{3}\,i)(-3\,i)$ (b) $(-\sqrt{3} - i)(-\dfrac{\sqrt{3}}{2} + \dfrac{1}{2}\,i)$

    (c) $\dfrac{-1 + \sqrt{3}\,i}{-3\,i}$ (d) $\dfrac{\frac{1}{2} - \frac{1}{2}\,i}{-3 + 3\,i}$

12. Calcular: $(1 - i)^{53}$, $(-\sqrt{3} + i)^{103}$, $(-1 + i)^{-57}$.

13. Calcular, representar en el plano complejo y expresar en forma binómica:

    (a) $\sqrt[4]{-1 - \sqrt{3}\,i}$ (b) $\sqrt[3]{-8}$

    (c) $\sqrt[3]{-i}$. (d) $\sqrt[6]{1}$

14. Hallar los números complejos z que verifiquen:

(a) $-i\,z^3 + i\,z - 5\,i\,(1-i)^2 = -\dfrac{z}{i} - 10\,i.$

(b) $(-i\,z - 10)\,i = 6\,i\,(1+i)^2 + 2.$

(c) $z^4 = -z^2$

(d) $z^{-3} = z$

(e) $2z^4 + 162 = 0$

15. Representar en el plano complejo la región determinada por los $z \in \mathbb{C}$ tales que:

(a) $Re\,z \leq 1$ (b) $Im\,z \leq -2$ (c) $|Re\,z| < 1$

(d) $|z|^2 = 1$ (e) $|z|^2 \leq 4$ (f) $|z|^2 > 16$

(g) $4 \leq |z|^2 < 7$ (h) $Re\,(z^2) = 0$ (i) $z^2 = (\overline{z})^2$

(j) $|z+1| = |z-2|$ (k) $|Re\,z| < 2$ y $|Im\,z| < 2$ (l) $|z|^2 \leq 9$ y $-2 < Im\,z \leq 1$

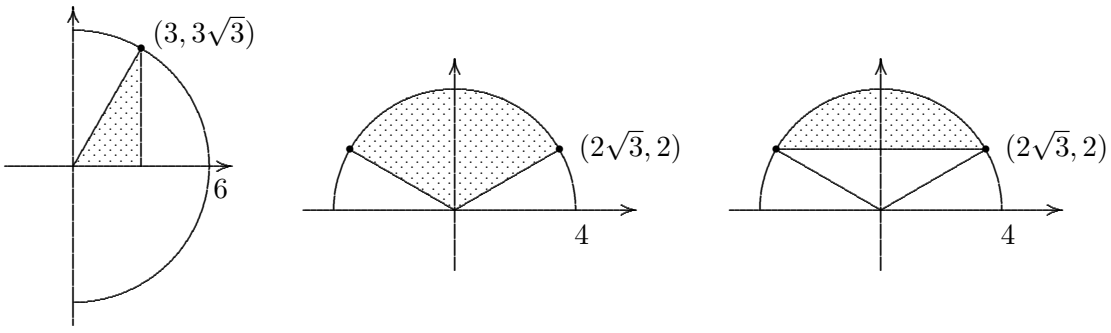
16. Para cada una de las condiciones siguientes, representar la región del plano complejo que caracterizan:

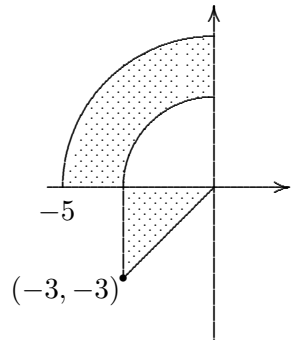
(a) $z + Re\,(\overline{z}) \cdot z = i$ (b) $arg\,z = \dfrac{\pi}{4}$ (c) $\dfrac{\pi}{4} < arg\,z < \dfrac{5}{4}\,\pi$ ó $Im\,z = 1$

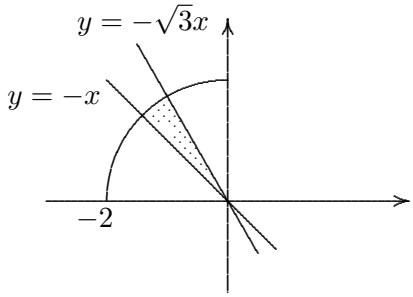
(d) $arg\,z^3 = 3\pi$ (e) $arg\,z = \pi$ y $|z| < 1$ (f) $|z-i| = |z+2|$

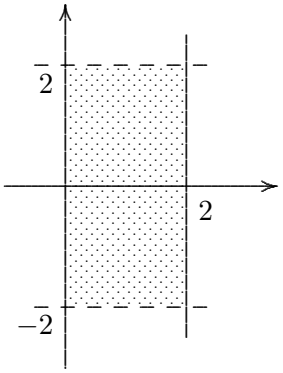
(g) $|z-i| = 1$ y $arg\,z = \dfrac{\pi}{2}$ (h) $|z| \leq 2$ y $Re\,z \geq 0$ (i) $3 \leq |z|$

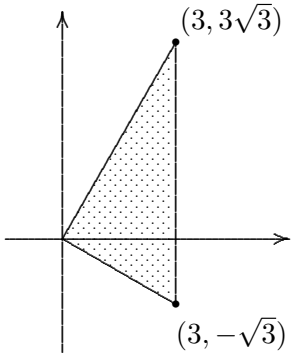
17. Escribir las condiciones que deben verificar los $z \in \mathbb{C}$ para que pertenezcan a la región indicada:

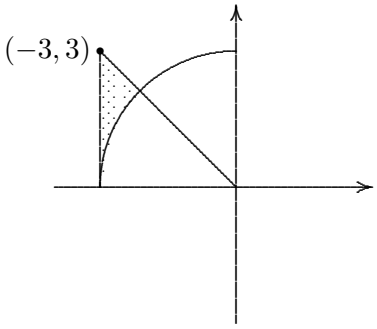


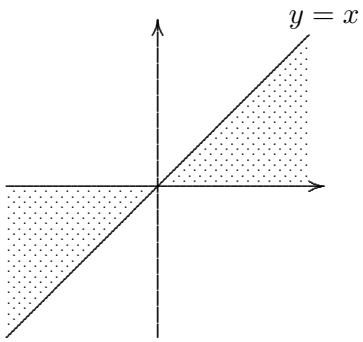












18. Calcular las raíces de la unidad de orden 3, 5, 6 y 7, y representarlas geométricamente. Indicar en cada caso las que son primitivas de cada orden.

19. Hallar las raíces primitivas de la unidad de orden 8, 15 y 18.

20. Demostrar que para cada $n \in \mathbb{N}$, el conjunto G_n de las raíces n-ésimas de la unidad tiene las siguientes propiedades:

    (a) G_n es cerrado con respecto a la multiplicación, es decir, si u, $v \in G_n$, entonces $u \cdot v \in G_n$.

    (b) $1 \in G_n$.

    (c) Si $u \in G_n$, entonces $u^{-1} \in G_n$.

    (d) Si $u \in G_n$, entonces $\overline{u} \in G_n$.

    (e) Si $\epsilon \in G_n$ es una raíz primitiva de orden n de la unidad, entonces $G_n = \{1, \epsilon, \epsilon^2, \ldots, \epsilon^{n-1}\}$.

(f) La suma de las n raíces n-ésimas de la unidad, $n > 1$, es 0, y su producto es 1 ó -1, según sea n impar o par.

(g) Hallar $G_2 \cap G_4$. Probar que en general $G_n \cap G_m = G_{(n,m)}$. Deducir que $G_n \subseteq G_m$ si y sólo si $n \mid m$.

21. Sabiendo que u es una raíz de la unidad de orden n, demostrar las siguientes igualdades:

(a) $u(u^{n-1} + u^{3n-1}) - u^{-n} = 1$

(b) $u^2(u^{n-1} - (3u)^{n-2}) + \dfrac{3^n}{9} = u$

22. (a) Demostrar que si r es una raíz de orden n de un número complejo z y $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ son las raíces n-ésimas de la unidad, entonces $r \cdot \epsilon_1, r \cdot \epsilon_2, \ldots, r \cdot \epsilon_n$ son las raíces n-ésimas de z.

(b) ¿Qué se puede decir sobre la suma y el producto de las raíces n-ésimas, $n > 1$, de un número complejo $z \neq 0$?

23. (a) Probar que $-\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}\, i$ es una raíz de la unidad de orden 8. Decir si es raíz primitiva de dicho orden. En caso afirmativo, hallar todas las raíces de orden 8, a partir de la dada.

(b) Usando los resultados obtenidos en el inciso (a), resolver la ecuación $X^8 - 256 = 0$.

(c) Resolver la ecuación $X^3 + 27 = 0$ utilizando las raíces cúbicas de 1.

8 Polinomios

8.1 Definiciones

La definición de polinomio no es sencilla de dar dentro de los niveles de este curso. Por su claridad y, al mismo tiempo rigurosidad, adoptaremos la presentación dada por E. Gentile en su libro "Anillo de Polinomios". Conviene, sin embargo, que el alumno recuerde la noción que ya posee de polinomio y omita en una primera lectura la definición formal que aquí presentamos en las páginas que siguen.

Comenzaremos por introducir el concepto de sucesión.

En esta sección, K representará el cuerpo de los números racionales, el de los números reales o el de los números complejos.

Una *sucesión de elementos de* K es una función $f : \mathbb{N} \cup \{0\} \to K$.

Ejemplos.

$$f : \mathbb{N} \cup \{0\} \to K \quad , \quad f(n) = \frac{1}{n+1}$$
$$f : \mathbb{N} \cup \{0\} \to K \quad , \quad f(n) = n^2 + 1$$

Una sucesión queda determinada por los valores que ella asume, es decir, por los números $a_0 = f(0)$, $a_1 = f(1)$, $a_2 = f(2)$, ..., $a_n = f(n)$, ... Por lo tanto, dar una sucesión $f : \mathbb{N} \cup \{0\} \to K$ es equivalente a dar ordenadamente los números $a_0 = f(0)$, $a_1 = f(1)$, $a_2 = f(2)$, ..., $a_n = f(n)$, ... Se escribe entonces simplemente

$$a = (a_0, a_1, a_2, \ldots, a_n, \ldots).$$

Así por ejemplo, dar la sucesión $f : \mathbb{N} \cup \{0\} \to K$, $f(n) = \dfrac{1}{n+1}$, es equivalente a dar la expresión

$$(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n+1}, \ldots).$$

Los números a_i de la sucesión $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ se llaman los *coeficientes* de la sucesión.

Si a y b son sucesiones, $a = (a_0, a_1, a_2, \ldots, a_n, \ldots)$, $b = (b_0, b_1, b_2, \ldots, b_n, \ldots)$, entonces $a = b$ si y sólo si $a_i = b_i$ para todo $i \in \mathbb{N} \cup \{0\}$.

Observar que las sucesiones $a = (a_0, a_1, a_2, \ldots, a_n, \ldots)$ y $b = (0, 0, 0, \ldots, 0, \ldots)$ son iguales si y sólo si $a_i = 0$ para todo $i \in \mathbb{N} \cup \{0\}$.

Vamos a considerar ahora sólamente aquellas sucesiones tales que todos sus coeficientes son cero desde un índice en adelante.

La notación utilizada para designar el siguiente conjunto se verá justificada más adelante.

Sea $K[X] = \{a = (a_0, a_1, a_2, \ldots, a_n, \ldots),\ a_i \in K :$ existe $m \in \mathbb{N}$ tal que $a_i = 0$ si $i > m\}$.

Ejemplo. Son elementos de $K[X]$

(a) $a = (0, 0, 0, \ldots, 0, \ldots)$; $a_i = 0$ para todo $i \in \mathbb{N} \cup \{0\}$.
(b) $a = (1, 0, 0, \ldots, 0, \ldots)$; $a_0 = 1$, $a_i = 0$ si $i \geq 1$.
(c) $a = (0, 1, 0, \ldots, 0, \ldots)$; $a_0 = 0$, $a_1 = 1$, $a_i = 0$ si $i \geq 2$.
(d) $a = (0, 0, 1, \ldots, 0, \ldots)$; $a_0 = a_1 = 0$, $a_2 = 1$, $a_i = 0$ si $i \geq 3$.

Vamos a definir una *suma* en $K[X]$.

Definición 8.1 *Sean* $a,\ b \in K[X]$, $a = (a_0, a_1, a_2, \ldots, a_n, \ldots)$, $b = (b_0, b_1, b_2, \ldots, b_n, \ldots)$. *Definimos*

$$a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, \ldots),$$

esto es, $a + b$ *es la sucesión cuyo coeficiente* i*-ésimo es* $(a + b)_i = a_i + b_i$.

Observaciones.

1. Es claro que si $a,\ b \in K[X]$, entonces $a + b \in K[X]$.
2. La suma definida en $K[X]$ tiene las siguientes propiedades:
   (a) Es asociativa. En efecto, si $a,\ b,\ c \in K[X]$, el coeficiente i-ésimo de $(a + b) + c$ es $((a + b) + c)_i = (a + b)_i + c_i = (a_i + b_i) + c_i \overset{(*)}{=} a_i + (b_i + c_i) = a_i + (b + c)_i = (a + (b + c))_i$, que es el coeficiente i-ésimo de $a + (b + c)$. Luego $(a + b) + c = a + (b + c)$.
   La igualdad $(*)$ vale porque $a_i,\ b_i,\ c_i \in K$, donde vale la propiedad asociativa.
   (b) Es conmutativa. Ejercicio.
   (c) Admite elemento neutro: $0 = (0, 0, 0, \ldots, 0, \ldots)$.
   (d) Todo elemento $a = (a_0, a_1, a_2, \ldots, a_n, \ldots)$ admite un opuesto $-a = (-a_0, -a_1, -a_2, \ldots, -a_n, \ldots)$.

Ahora vamos a definir un *producto* en $K[X]$.

Previamente vamos a definir el producto de un elemento de K por un elemento de $K[X]$, para obtener una representación de los elementos de $K[X]$ que nos permita operar con sencillez.

Definición 8.2 *Sea* $k \in K$, $a = (a_0, a_1, a_2, \ldots, a_n, \ldots) \in K[X]$. *Entonces definimos*

$$k \cdot a = (ka_0, ka_1, ka_2, \ldots, ka_n, \ldots),$$

esto es, $k \cdot a$ *es la sucesión cuyo coeficiente* i*-ésimo es* $(k \cdot a)_i = ka_i$.

Se prueba sin dificultad que este producto tiene las siguientes propiedades:

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

(b) $(k_1 + k_2) \cdot a = k_1 \cdot a + k_2 \cdot a$

(c) $(k_1 k_2) \cdot a = k_1 \cdot (k_2 \cdot a)$

(d) $1 \cdot a = a$

donde $k,\ k_1,\ k_2 \in K$, $a,\ b \in K[X]$.

Vamos a destacar ahora algunas sucesiones particulares de $K[X]$:

$$\begin{aligned}
X_0 &= (1, 0, 0, 0, \ldots) \\
X_1 &= (0, 1, 0, 0, \ldots) \\
X_2 &= (0, 0, 1, 0, \ldots) \\
&\vdots \quad\quad \vdots \\
X_i &= (0, \ldots, 0, 1, 0, \ldots),\ x_i = 1,\ x_j = 0 \ \text{ si } \ j \neq i.
\end{aligned}$$

Si $a = (a_0, a_1, a_2, \ldots, a_n, \ldots) \in K[X]$ y suponemos que $a_i = 0$ para $i > n$, entonces a puede escribirse:

$$\begin{aligned} a &= a_0 \cdot (1,0,0,0,\ldots) + a_1 \cdot (0,1,0,0,\ldots) + a_2 \cdot (0,0,1,0,\ldots) + \cdots + a_n \cdot (0,\ldots,\underbrace{1}_{n+1},\ldots) \\ &= a_0 \cdot X_0 + a_1 \cdot X_1 + a_2 X_2 + \cdots + a_n \cdot X_n. \end{aligned}$$

Entonces, todo elemento $a \in K[X]$ se puede representar como una *combinación lineal* finita de las sucesiones X_0, X_1, X_2, …, X_i, …, con coeficientes en K.

Para definir un producto en $K[X]$, basta definirlo para los elementos X_0, X_1, X_2, …, X_i, …, y extenderlo a todos los elementos de $K[X]$ por medio de la propiedad distributiva.

Definición 8.3 $X_i \cdot X_j = X_{i+j}$.

Observaciones.

(a) El producto anterior es conmutativo y asociativo, como se verifica sin dificultad.

(b) $X_0 \cdot X_i = X_i$, para todo i.

(c) $X_1^2 = X_1 \cdot X_1 = X_2$, $X_1^3 = X_3$, …, $X_1^n = X_n$, para todo n.

Entonces, si convenimos en notar $X_1^0 = X_0 = 1$ (neutro del producto) y $X_1^1 = X_1 = X$, la expresión de un elemento cualquiera en $K[X]$ es:

$$a_0 \cdot 1 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n$$

Es costumbre identificar $a \cdot 1 = a \cdot X_0 = a$, y entonces la expresión de un elemento de $K[X]$ es

$$a_0 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n = a_0 + a_1 X + a_2 X^2 + \cdots + a_n \cdot X^n, \quad a_i \in K.$$

Con esta representación, el producto de elementos de $K[X]$ se efectúa teniendo en cuenta las definiciones $(a_i \cdot X^i) \cdot (b_j \cdot X^j) = a_i b_j \cdot X^{i+j}$ y la propiedad distributiva.

Ejemplos.

1. La suma de dos elementos de $K[X]$ se efectúa de la siguiente manera:
   - $f_1(X) = X^2 + X + 1$,
     $f_2(X) = 2X^3 + 1$,
     $f_1(X) + f_2(X) = 2X^3 + X^2 + X + 2$.
   - $f_1(X) = 3X^3 + X + 2$,
     $f_2(X) = -3X^3 + X^2$,
     $f_1(X) + f_2(X) = X^2 + X + 2$.
2. Para efectuar el producto $(X^4 - 2X^3 + X - 2) \cdot (X^2 + X - 1)$, procedemos de la siguiente manera:

$$\begin{array}{r} X^4 - 2X^3 \quad + X - 2 \\ \hline X^2 + X - 1 \\ \hline -X^4 + 2X^3 \quad - X + 2 \\ X^5 - 2X^4 \quad + X^2 - 2X \\ X^6 - 2X^5 \quad + X^3 - 2X^2 \\ \hline X^6 - X^5 - 3X^4 + 3X^3 - X^2 - 3X + 2 \end{array}$$

Los elementos de $K[X]$ se llaman *polinomios* en X con coeficientes en K. El elemento X se llama *indeterminada*.

Grado de un polinomio

En adelante denotaremos los elementos de $K[X]$ con $a(X)$, $f(X)$, $g(X)$, $p(X)$, ... , o bien a, f, g, p, ...

Sea $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$. Si $f(X) \neq 0$, entonces algún coeficiente es no nulo.

Definición 8.4 *Se llama grado de un polinomio no nulo $f(X)$, y se nota $gr\ f(X)$, al mayor índice i tal que $a_i \neq 0$.*

Al polinomio nulo no se le atribuye grado.

Si $gr\ f(X) = n$, diremos que a_nX^n es el *término principal* de $f(X)$, y que a_n es el *coeficiente principal*. $f(X)$ se dice *mónico* si $a_n = 1$.

Ejemplos.

1. $gr\ (3 + X^2 - 2X^3 - X^5) = 5$
2. $gr\ f(X) = 0$ si y sólo si $f(X) = k \in K$, $k \neq 0$, esto es, los polinomios de grado cero son las constantes no nulas.

Resulta claramente de la definición de suma de polinomios que **el grado del polinomio suma** es menor o igual que el máximo de los grados de los polinomios dados. En símbolos, si $f(X)$, $g(X)$ y $f(X) + g(X)$ no son nulos,

$$gr\ (f(X) + g(X)) \leq máx\ \{gr\ f(X), gr\ g(X)\}.$$

En el caso en que $gr\ f(X) = gr\ g(X) = n$ y $a_n = -b_n$, se tiene que $gr\ (f(X) + g(X)) < n$.

Para **el grado del producto** de dos polinomios, vale la siguiente propiedad, para $f(X) \neq 0$ y $g(X) \neq 0$:

$$gr\ (f(X) \cdot g(X)) = gr\ f(X) + gr\ g(X).$$

En efecto, supongamos que $gr\ f(X) = n$ y $gr\ g(X) = m$, $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_n \cdot X^n$ $(a_n \neq 0)$, $g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_m \cdot X^m$ $(b_m \neq 0)$.
Entonces $f(X) \cdot g(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + a_nb_m \cdot X^{n+m}$, es decir, el coeficiente c_k de X^k se obtiene como la suma de todos los productos posibles a_ib_j tales que $i + j = k$. Para $k > n + m$, debe ser $i + j > n + m$, de donde $i > n$ ó $j > m$, luego $a_i = 0$ ó $b_j = 0$, y por lo tanto, $c_k = 0$.
Por último, $c_{n+m} = a_nb_m$, que es distinto de cero porque $a_n \neq 0$ y $b_m \neq 0$.
Luego $gr\ (f(X) \cdot g(X)) = n + m = gr\ f(X) + gr\ g(X)$.

Observación. Los únicos polinomios inversibles con respecto a la multiplicación son las constantes no nulas. En efecto, si un polinomio $f(X)$ tiene inverso $g(X)$, es decir, si $f(X) \cdot g(X) = 1$, entonces $gr\ f(X) + gr\ g(X) = 0$, de donde $gr\ f(X) = gr\ g(X) = 0$, y por lo tanto, $f(X)$ y $g(X)$ son constantes no nulas.

Ejercicios.

1. Sean $f(X)$ y $g(X)$ dos polinomios tales que $f(X) \cdot g(X) = 0$. Demostrar que $f(X) = 0$ ó $g(X) = 0$. (Se sugiere comparar los grados)
2. Si $f(X) \cdot h(X) = g(X) \cdot h(X)$ y $h(X) \neq 0$, entonces $f(X) = g(X)$. La recíproca es clara.

8.2 Divisibilidad

Teorema 8.5 (Algoritmo de la división). *Dados dos polinomios $f(X)$ y $g(X) \in K[X]$, con $g(X)$ no nulo, existen dos únicos polinomios $q(X)$ y $r(X) \in K[X]$, llamados cociente y resto respectivamente de dividir $f(X)$ por $g(X)$, tal que $f(X) = q(X)g(X) + r(X)$, donde $gr\ r(X) < gr\ g(X)$ ó $r(X) = 0$.*

Demostración. Probemos la existencia de los polinomios $q(X)$ y $r(X)$.

1. Supongamos que $f(X) = p(X) \cdot g(X)$, para algún $p(X) \in K[X]$. En ese caso bastará tomar $q(X) = p(X)$ y $r(X) = 0$.

2. Supongamos ahora que $f(X) \neq p(X) \cdot g(X)$, para todo $p(X) \in K[X]$. Consideremos el siguiente conjunto de polinomios:

$$H = \{f(X) - p(X) \cdot g(X) : p(X) \in K[X]\}.$$

El polinomio nulo $0 \notin H$, y por el Principio de Buena Ordenación, considerando los grados de los polinomios de H, existe en H al menos un polinomio, digamos $r(X)$, de *grado mínimo*, o sea, $r(X) \in H$ y si $t(X) \in H$, $gr\ r(X) \leq gr\ t(X)$.

$$r(X) = f(X) - q(X) \cdot g(X), \quad \text{para un cierto } q(X) \in K[X].$$

Entonces

$$f(X) = q(X) \cdot g(X) + r(X).$$

Veamos que $gr\ r(X) < gr\ g(X)$. Supongamos por el absurdo que $gr\ r(X) \geq gr\ g(X)$.
Escribamos

$$g(X) = b_0 + b_1X + \cdots + b_nX^n \ ; \quad r(X) = r_0 + r_1X + \cdots + r_sX^s \ , \quad s \geq n.$$

Entonces el polinomio

$$r'(X) = r(X) - \frac{r_s}{b_n}X^{s-n} \cdot g(X)$$

es diferencia de dos polinomios de grado s y con el mismo coeficiente principal. Luego $r'(X)$ es cero ó $gr\ r'(X) < gr\ r(X)$.
Reemplazando de tiene

$$r'(X) = f(X) - q(X) \cdot g(X) - \frac{r_s}{b_n}X^{s-n} \cdot g(X) = f(X) - \left(q(X) + \frac{r_s}{b_n} \cdot X^{s-n}\right) \cdot g(X).$$

Entonces $r'(X) \in H$.
Pero como $0 \notin H$ se tiene que $r'(X)$ tiene grado menor que $r(X)$, una contradicción que provino de suponer que $gr\ r(X) \geq gr\ g(X)$. Por lo tanto, $gr\ r(X) < gr\ g(X)$.
Probemos la unicidad del cociente y el resto.
Supongamos que

$$f(X) = q(X) \cdot g(X) + r(X), \text{ con } r(X) = 0 \ \text{ ó } \ gr\ r(X) < gr\ g(X)$$

y también

$$f(X) = q'(X) \cdot g(X) + r'(X), \text{ con } r'(X) = 0 \ \text{ ó } \ gr\ r'(X) < gr\ g(X).$$

Debemos probar que $r(X) = r'(X)$ y $q(X) = q'(X)$.
Restando ambas expresiones resulta

$$0 = \big(q(X) - q'(X)\big) \cdot g(X) + \big(r(X) - r'(X)\big),$$

o sea,

$$r(X) - r'(X) = \big(q'(X) - q(X)\big) \cdot g(X).$$

Razonando por el absurdo, si $r(X) - r'(X)$ fuese distinto de cero, entonces $q'(X) - q(X)$ sería distinto de cero. Luego

$$gr\ \big(r(X) - r'(X)\big) = gr\ \big(q'(X) - q(X)\big) + gr\ g(X) \geq gr\ g(X).$$

Pero por otro lado,

$$gr\ \big(r(X) - r'(X)\big) \leq máx\ \{gr\ r(X), gr\ r'(X)\} < gr\ g(X),$$

pues ambos grados son menores que el grado de $g(X)$.
Hemos obtenido entonces una contradicción, y por lo tanto debe ser $r(X) - r'(X) = 0$, o sea, $r(X) = r'(X)$.
Como $0 = (q'(X) - q(X)) \cdot g(X)$ y $g(X) \neq 0$, resulta $q'(X) - q(X) = 0$, esto es, $q'(X) = q(X)$.

□

Ejemplo. Sean $f(X) = X^4 - 3X^2 + 1$ y $g(X) = X^2 - 2X$.

$$\begin{array}{r|l} X^4 + 0X^3 - 3X^2 + 0X + 1 & X^2 - 2X \\ \cline{2-2} X^4 - 2X^3 & X^2 + 2X + 1 \\ \cline{1-1} \quad 2X^3 - 3X^2 & \\ \quad 2X^3 - 4X^2 & \\ \cline{1-1} \qquad\quad X^2 + 0X & \\ \qquad\quad X^2 - 2X & \\ \cline{1-1} \qquad\qquad\ \ 2X + 1 & \end{array}$$

Entonces $q(X) = X^2 + 2X + 1$ y $r(X) = 2X + 1$.

Luego $X^4 - 3X^2 + 1 = (X^2 + 2X + 1)(X^2 - 2X) + (2X + 1)$.

El algoritmo utilizado en el ejemplo anterior se puede simplificar cuando se trata de dividir un polinomio $f(X)$ por otro de la forma $X - a$. Es la llamada *Regla de Ruffini*, que ejemplificamos a continuación.

Ejemplos.

1) $f(X) = X^3 - 2X + 1$, $g(X) = X - 2$

	1	0	−2	1
2		2	4	4
	1	2	2	5

Luego $q(X) = X^2 + 2X + 2$, $r(X) = 5$.

2) $f(X) = 3X^4 + 2X^2 + X - 3$, $g(X) = X + 3$

	3	0	2	1	-3
-3		-9	27	-87	258
	3	-9	29	-86	255

Luego $q(X) = 3X^3 - 9X^2 + 29X - 86$, $r(X) = 255$.

Vamos a ver ahora que es posible desarrollar una teoría de la divisibilidad en $K[X]$ semejante a la dada en $\mathbb{Z}$, incluyendo un teorema fundamental de la aritmética. Omitiremos en algunos casos los detalles por ser análogos a los ya vistos para $\mathbb{Z}$.

Definición 8.6 *Dados dos polinomios $f(X), g(X) \in K[X]$, se dice que $f(X)$ divide a $g(X)$ si existe un polinomio $h(X) \in K[X]$ tal que $g(X) = h(X) \cdot f(X)$. Se escribe $f|g$.*

Ejemplo. $f(X) = X - 1$ divide a $g(X) = X^3 - X^2 + X - 1$, pues $X^3 - X^2 + X - 1 = (X^2 + 1) \cdot (X - 1)$.

Propiedades.

1. Si $f \neq 0$, entonces $f|g$ si y sólo si el resto de dividir $g(X)$ por $f(X)$ es cero.
   En efecto, si $f|g$, existe $h(X)$ tal que $g(X) = h(X) \cdot f(X)$. Si $q(X)$ y $r(X)$ son el cociente y el resto de la división de $g(X)$ por $f(X)$, entonces tenemos

   $$g(X) = h(X) \cdot f(X) + 0 \quad \text{y} \quad g(X) = q(X) \cdot f(X) + r(X).$$

   Por la unicidad del cociente y el resto, debe ser $h(X) = q(X)$ y $r(X) = 0$.
   Recíprocamente, si el resto de la división es cero, entonces $g(X) = q(X) \cdot f(X) + 0$, o sea, $g(X) = q(X) \cdot f(X)$, luego $f|g$.

2. $f|0$ para todo $f(X) \in K[X]$, pues $0 = 0 \cdot f(X)$.

3. $f|f$ para todo $f(X) \in K[X]$, pues $f(X) = 1 \cdot f(X)$. Más generalmente, $f|k \cdot f$, para todo $k \in K$.

4. Si $a \in K$, $a \neq 0$, y $f(X) \in K[X]$, entonces $a|f$.
   En efecto, si $f(X) = a_0 + a_1 X + \cdots + a_n X^n$, entonces podemos escribir

   $$f(X) = \left(\frac{a_0}{a} + \frac{a_1}{a} X + \cdots + \frac{a_n}{a} X^n\right) \cdot a.$$

5. Si $f|g$ y $g|h$, entonces $f|h$.

6. Si $f|g$ y $f|h$, entonces $f|p \cdot g + q \cdot h$ para todo $p(X), q(X) \in K[X]$.

7. Si $f|g$ y $g(X) \neq 0$, entonces $gr\ f(X) \leq gr\ g(X)$.
   De $f|g$, $g(X) = h(X) \cdot f(X)$, y por lo tanto, $gr\ g(X) = gr\ h(X) + gr\ f(X) \geq gr\ f(X)$.

8. $f|g$ y $g|f$ si y sólo si $f(X)$ y $g(X)$ difieren en una constante no nula, esto es, $f = k \cdot g$, con $k \in K$, $k \neq 0$.
   En efecto, de $f|g$ y $g|f$ existen polinomios $h(X)$ y $h'(X)$ tales que $g(X) = h(X) \cdot f(X)$ y $f(X) = h'(X) \cdot g(X)$. Entonces

$$f(X) = h'(X) \cdot h(X) \cdot f(X).$$

   Si $f(X) \neq 0$, razonando sobre los grados, se obtiene que $h'(X)$ y $h(X)$ son constantes. Si $f(X) = 0$, entonces también $g(X) = 0$, y vale la propiedad.
   Recíprocamente, supongamos que $f(X)$ y $g(X)$ difieren en una constante no nula, esto es, $f(X) = k \cdot g(X)$, $k \in K$, $k \neq 0$. Entonces $g|f$. Por otro lado, se tiene que $g(X) = k^{-1} \cdot f(X)$, esto es $f|g$.

Definición 8.7 *Dados dos polinomios $f = f(X)$ y $g = g(X)$, un polinomio $d = d(X)$ se llama un máximo común divisor de $f(X)$ y $g(X)$ si se verifica que:*

1. *$d|f$ y $d|g$.*

2. *Si $d'(X)$ es un polinomio tal que $d'|f$ y $d'|g$, entonces $d'|d$.*

Notaremos $d = (f, g)$.

Si $d(X)$ y $d'(X)$ son dos m.c.d. de $f(X)$ y $g(X)$, por la propiedad 8, $d(X)$ y $d'(X)$ difieren en una constante. Si se considera el m.c.d. mónico, entonces el m.c.d. es *único*.

Análogamente a lo que sucede en $\mathbb{Z}$, es posible aplicar el algoritmo de Euclides para calcular el máximo común divisor de dos polinomios $f(X)$ y $g(X)$.

Omitiremos la demostración de la siguiente propiedad por ser la misma que la de la correspondiente propiedad en $\mathbb{Z}$:

Algoritmo de Euclides. Dados dos polinomios no nulos $f(X)$ y $g(X)$, para hallar el máximo común divisor se hacen divisiones sucesivas de acuerdo al esquema visto para números enteros. Como los grados de los restos que se van obteniendo son estrictamente decrecientes, el procedimiento termina al cabo de un número finito de pasos. El último resto no nulo es un máximo común divisor.

Ejemplo. Hallar el m.c.d. de los polinomios $f(X) = X^4 - 3X^3 + 5X^2 - 9X + 6$ y $g(X) = X^3 + 4X^2 + 3X + 12$.

	$X - 7$	X+4
$X^4 - 3X^3 + 5X^2 - 9X + 6$	$X^3 + 4X^2 + 3X + 12$	$X^2 + 3$
$X^4 + 4X^3 + 3X^2 + 12X$	$X^3 \quad + 3X$	
$-7X^3 + 2X^2 - 21X + 6$	$4X^2 \quad + 12$	
$-7X^3 - 28X^2 - 21X - 84$	$4X^2 \quad + 12$	
$30X^2 + 90$	0	
$X^2 + 3$		

Observar que es conveniente simplificar la expresión de cada resto antes de continuar con las divisiones sucesivas. El último resto no nulo es X^2+3. Luego $(f,g)=X^2+3$.

También puede probarse que existen polinomios $s(X)$ y $t(X)$ tales que

$$d(X)=s(X)\cdot f(X)+t(X)\cdot g(X).$$

Si alguno de los dos polinomios es cero, digamos $g(X)=0$, entonces $(f,0)=f$ y $f(X)=1\cdot f(X)+1\cdot 0$.

Ejercicio. Hallar el m.c.d. de $f(X)=6X^4-3X^3+11X^2-15X+1$ y $g(X)=6X^3+14X-8$.

Polinomios irreducibles

Un problema importante en el estudio de la divisibilidad en $K[X]$ es el de determinar los polinomios *irreducibles*.

Definición 8.8 *Un polinomio no constante $f(X)\in K[X]$ se dice irreducible o primo en $K[X]$ si no se puede expresar como producto de dos polinomios no constantes de $K[X]$. (Equivalentemente, si los únicos divisores de $f(X)$ en $K[X]$ son las constantes no nulas y los polinomios $k\cdot f(X)$, $k\in K$, $k\neq 0$.)*

Ejemplos.

1. X^2-2 no es irreducible en $\mathbb{R}[X]$, ya que $X^2-2=(X-\sqrt{2})(X+\sqrt{2})$.
2. X^2-2 es irreducible en $\mathbb{Q}[X]$, pues caso contrario sería producto de dos polinomios mónicos de grado 1: $X^2-2=(X+a)(X+b)$, $a,b\in\mathbb{Q}$. Luego $X^2-2=X^2+(a+b)X+ab$. De donde $ab=-2$ y $a+b=0$. De aquí resulta $a=\sqrt{2}$ y $b=-\sqrt{2}$, que no son racionales.
3. Todo polinomio de grado 1 en $K[X]$ es irreducible.

Definición 8.9 *Dos polinomios $f(X)$ y $g(X)$ se dicen relativamente primos si $(f,g)=1$.*

Mencionemos los siguientes resultados fundamentales cuya demostración omitimos, pues es igual a la vista en $\mathbb{Z}$:

Sean $f(X)$, $g(X)$ y $h(X)\in K[X]$. Entonces:

1. Si $f|g\cdot h$ y $(f,g)=1$, entonces $f|h$.
   En particular, si $f|g\cdot h$ y f es irreducible, entonces $f|g$ ó $f|h$.
2. Si $f|h$, $g|h$ y $(f,g)=1$, entonces $f\cdot g|h$.

Teorema 8.10 (El Teorema Fundamental de la Aritmética en K[X]). *Todo elemento $f(X)\in K[X]$ no constante, puede escribirse en la forma:*

$$f=k\cdot p_1^{e_1}\cdot p_2^{e_2}\cdot\cdots\cdot p_s^{e_s},$$

donde $k\in K$, p_i son polinomios irreducibles mónicos distintos en $K[X]$ y $e_i\in\mathbb{N}$. Esta factorización es única salvo el orden de los factores.

Demostración. Para probar la existencia de la factorización, haremos inducción sobre $n = gr\ f(X)$. Si $n = 1$, entonces $f(X) = a_0 + a_1X$. Entonces $f(X) = a_1\left(\frac{a_0}{a_1} + X\right)$, y el polinomio $p_1(X) = \frac{a_0}{a_1} + X$ es irreducible mónico en $K[X]$.
Sea $n > 1$ y supongamos que la factorización existe para todo polinomio no constante de grado menor que n. Veamos que $f(X)$ puede factorizarse en la forma indicada.
Si $f(X)$ es irreducible y si a_n es su coeficiente principal, entonces $f(X) = a_n\left(\frac{1}{a_n} \cdot f(X)\right)$. Como el polinomio $\frac{1}{a_n} \cdot f(X)$ es irreducible mónico en $K[X]$, se tiene la factorización buscada.
Si $f(X)$ no es irreducible, entonces $f(X) = g(X) \cdot h(X)$, $g(X)$, $h(X) \in K[X]$ no constantes y $gr\ g(X) < gr\ f(X)$, $gr\ h(X) < gr\ f(X)$. Por la hipótesis inductiva, $g(X)$ y $h(X)$ se pueden expresar como producto de una constante por polinomios irreducibles mónicos, y por lo tanto, lo mismo sucede con $f(X)$.
Hemos probado entonces la existencia de la descomposición.
La unicidad se prueba de la misma forma que en el Teorema Fundamental de la Aritmética para los números enteros.
Si aparecen factores irreducibles repetidos, se agrupan en forma de potencias y se obtiene la expresión del enunciado. □

Ejemplo. El polinomio $f(X) = X^8 - 4X^6 + 2X^4 + 4X^2 - 3$ se factoriza

$$\begin{aligned} f(X) &= (X^2+1)(X^2-3)(X-1)^2(X+1)^2, \text{ en } \mathbb{Q}[X], \\ f(X) &= (X^2+1)(X-\sqrt{3})(X+\sqrt{3})(X-1)^2(X+1)^2, \text{ en } \mathbb{R}[X], \\ f(X) &= (X-i)(X+i)(X-\sqrt{3})(X+\sqrt{3})(X-1)^2(X+1)^2, \text{ en } \mathbb{C}[X]. \end{aligned}$$

8.3 Raíces

Especialización o valor numérico.

Sea $a \in K$ y $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$. Se llama *especialización* o *valor numérico* de f en a al número

$$f(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n.$$

Ejemplo. Sea $f(X) = X^2 + 2X - 1$. Entonces $f(2) = 7$, $f(-1) = -2$, $f(0) = -1$.

Teorema 8.11 (Teorema del resto, o Teorema de Bézout). *El resto de dividir un polinomio $f(X)$ por otro de la forma $X - a$ es $f(a)$, es decir, es el valor del polinomio en a.*

Demostración. Sean $q(X)$ y $r(X)$ el cociente y el resto de dividir $f(X)$ por $X - a$. Entonces

$$f(X) = q(X) \cdot (X - a) + r(X), \tag{5}$$

donde $r(X) = 0$ ó $gr\ r(X) < gr\ (X - a) = 1$, esto es, $r(X) = 0$ ó $gr\ r(X) = 0$. En ambos casos el resto es una constante. Luego $r(X) = r$, y en (5) es $f(a) = q(a) \cdot (a - a) + r$, luego $f(a) = r$. □

Definición 8.12 *Dado un polinomio $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, diremos que un número a es una* **raíz** *de $f(X)$, si $f(a) = 0$, es decir si $a_na^n + a_{n-1}a^{n-1} + \cdots + a_1a + a_0 = 0$.*

Corolario 8.13 (*del Teorema del Resto*) *Un número a es raíz de un polinomio $f(X)$ si y sólo si $f(X)$ es divisible por $X-a$.*

Demostración. a es raíz de $f(X) \Leftrightarrow f(a)=0$. Como $f(a)$ es el resto de dividir $f(X)$ por $X-a$, entonces $f(a)=0$ si y sólo si el resto de dividir $f(X)$ por $X-a$ es cero, y esto es equivalente a decir que $f(X)$ es divisible por $X-a$. □

Ejemplo. Verificar que 3 es raíz de $f(X)=X^3-X^2-5X-3$.
Para ello basta ver que el resto de dividir $f(X)$ por $X-3$ es cero. Aplicando la regla de Ruffini:

	1	−1	−5	−3
3		3	6	3
	1	2	1	0

Entonces $r(X)=0$, luego 3 es raíz.

Observación. A partir del Corolario del Teorema del Resto, si $f(X)$ es un polinomio de grado n y conocemos una raíz a de $f(X)$, entonces existe un polinomio $g(X)$ tal que $f(X)=(X-a)\cdot g(X)$. Si b es una raíz de $g(X)$, entonces $f(b)=(b-a)\cdot g(b)=0$, es decir, b también raíz de $f(X)$. Esto es, las restantes raíces de $f(X)$ son las raíces de $g(X)$, que es un polinomio de un grado menor que el grado de $f(X)$.

Raíces múltiples

Si a es raíz de un polinomio $f(X)$, sabemos que $f(X)$ es divisible por $X-a$. Puede suceder que $f(X)$ sea también divisible por $(X-a)^2$ y no lo sea por $(X-a)^3$; en ese caso diremos que a es una raíz doble (o una raíz múltiple de orden 2). En general, si k es el mayor número natural tal que $f(X)$ es divisible por $(X-a)^k$, diremos que a es una raíz múltiple de orden k. El orden de multiplicidad de una raíz se puede hallar aplicando la regla de Ruffini.

Ejemplo. Verificar que 2 es una raíz del polinomio $f(X)=X^5-6X^4+11X^3-2X^2-12X+8$, y hallar su orden de multiplicidad. (Debemos hacer divisiones sucesivas por $X-2$ hasta que el resto no dé cero).

	1	−6	11	−2	−12	8
2		2	−8	6	8	−8
	1	−4	3	4	−4	0
2		2	−4	−2	4	
	1	−2	−1	2	0	
2		2	0	−2		
	1	0	−1	0		
2		2	4			
	1	2	$3 \neq 0$			

El orden de multiplicidad es 3.

Si conocemos una raíz de $f(X)$, es siempre conveniente calcular su orden de multiplicidad para obtener un polinomio de menor grado cuyas raíces son también raíces de $f(X)$. Así, en el ejemplo anterior, 2 es raíz múltiple de orden 3 de $f(X)=X^5-6X^4+11X^3-2X^2-12X+8$, y se tiene que

$f(X) = (X-2)^3 \cdot (X^2-1)$. Luego las restantes raíces de $f(X)$ son las raíces de X^2-1, es decir, 1 y -1.

Introducimos a continuación la noción de *polinomio derivado* con el fin de determinar criterios que permitan decidir si una raíz dada de un polinomio es simple o múltiple.

Definición 8.14 *Sea* $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0 \in K[X]$. *Se llama polinomio derivado de* f *al polinomio* $f' = f'(X) = n\,a_n\,X^{n-1} + (n-1)\,a_{n-1}\,X^{n-2} + \cdots + 2\,a_2\,X + a_1$.

Ejemplos.

1. Si $f(X) = X^3, \quad f'(X) = 3X^2$.
2. Si $f(X) = 3X^5 + 4X^4 - 2X^3 + X^2 - 2X + 1, \quad f'(X) = 15X^4 + 16X^3 - 6X^2 + 2X - 2$.

Propiedades.

1. Si f es constante, entonces $f' = 0$.
   Resulta de la definición.
2. $(f+g)' = f' + g'$.
   La demostración es inmediata.
3. $(f \cdot g)' = f' \cdot g + f \cdot g'$.
   Por la propiedad 2, es suficiente probar la propiedad para polinomios de la forma $f(X) = a \cdot X^i$, $g(X) = b \cdot X^j$, $a, b \in K$.
   $(f \cdot g)' = (a \cdot X^i \cdot b \cdot X^j)' = (a \cdot bX^{i+j})' = (i+j)a \cdot b \cdot X^{i+j-1} = ia \cdot X^{i-1} \cdot b \cdot X^j + a \cdot X^i \cdot jb \cdot X^{j-1} = (a \cdot X^i)' \cdot b \cdot X^j + a \cdot X^i \cdot (b \cdot X^j)' = f' \cdot g + f \cdot g'$.

Definimos ahora por recurrencia polinomios derivados de orden superior:

$$\begin{aligned} f^{(1)}(X) &= f'(X) \\ f^{(n+1)}(X) &= \left(f^{(n)}(X)\right)', \quad n \in \mathbb{N} \end{aligned}$$

Por conveniencia, definimos también $f^{(0)}(X) = f(X)$.

4 Si $f(X) = a_n\,X^n + a_{n-1}\,X^{n-1} + \cdots + a_2\,X^2 + a_1\,X + a_0$, entonces $f^{(n)}(X) = n! \cdot a_n$. En particular, si f tiene grado n, $f^{(n)}(X) \neq 0$.

5 Si f tiene grado n, $f^{(i)}(X) = 0$, si $i > n$.

Teorema 8.15 *Si* a *es una raíz de un polinomio* $f(X)$, *entonces* a *es una raíz múltiple de orden* k, $k > 1$, *de* $f(X)$ *si y sólo si* a *es una raíz múltiple de orden* $k-1$ *de* $f'(X)$.

Demostración. Sea a una raíz múltiple de orden k de $f(X)$, $k > 1$. Entonces $f(X) = (X-a)^k \cdot g(X)$, donde $X - a \nmid g(X)$. Luego $f'(X) = k \cdot (X-a)^{k-1} \cdot g(X) + (X-a)^k \cdot g'(X) = (X-a)^{k-1}[k \cdot g(X) + (X-a) \cdot g'(X)] = (X-a)^{k-1} \cdot h(X)$.
Como $X - a \nmid g(X)$, entonces $X - a \nmid h(X)$. Luego $k-1$ es el mayor exponente tal que $(X-a)^{k-1} | f'(X)$.
Luego a es una raíz de $f'(X)$ de orden de multiplicidad $k-1$.

Para la recíproca, supongamos que a es una raíz de $f(X)$ tal que a es raíz de $f'(X)$ de orden de multiplicidad $k-1$. Sea s el mayor exponente tal que $(X-a)^s | f(X)$. Entonces $s \geq 1$ y $f(X) = (X-a)^s \cdot g(X)$, con $X - a \not| \ g(X)$.
Entonces $f'(X) = s \cdot (X-a)^{s-1} \cdot g(X) + (X-a)^s \cdot g'(X) = (X-a)^{s-1}[s \cdot g(X) + (X-a) \cdot g'(X)] = (X-a)^{s-1} \cdot h(X)$.
Como $X - a \not| \ g(X)$ entonces $X - a \not| \ h(X)$, y por lo tanto $s-1$ es el mayor exponente tal que $(X-a)^{s-1} | f'(X)$. Como a es una raíz de $f'(X)$ de orden de multiplicidad $k-1$, resulta que $s - 1 = k - 1$, esto es, $s = k$. Luego a es una raíz de $f(X)$ de orden de multiplicidad k. □

Corolario 8.16 *Un número a es raíz múltiple de orden k, $k > 0$, de $f(X)$ si y sólo si $f(a) = f'(a) = \cdots = f^{(k-1)}(a) = 0$ y $f^{(k)}(a) \neq 0$.*

Demostración. Por el teorema anterior, se tienen las siguientes equivalencias:
- a es raíz múltiple de orden k de $f(X)$, $k > 0$.
- $f(a) = 0$ y a es raíz múltiple de orden $k-1$ de $f'(X)$.
- $f(a) = f'(a) = 0$ y a es raíz múltiple de orden $k-2$ de $f^{(2)}(X)$.
- $f(a) = f'(a) = f^{(2)}(a) = 0$ y a es raíz múltiple de orden $k-3$ de $f^{(3)}(X)$.

. . . . . .
- $f(a) = f'(a) = f^{(2)}(a) = \cdots = f^{(k-1)}(a) = 0$ y $f^{(k)}(a) \neq 0$. □

El orden de multiplicidad de una raíz a de un polinomio $f(X)$ es, entonces, igual al orden de la derivada de $f(X)$ de menor orden que no se anula en a.

Conviene observar que en la demostración del corolario anterior se usó implícitamente un argumento inductivo que podría ser formalizado en la manera habitual.

Ejemplo. Calcular el orden de multiplicidad de la raíz 1 del polinomio $f(X) = X^4 - X^3 - 3X^2 + 5X - 2$.
$f'(X) = 4X^3 - 3X^2 - 6X + 5$ y $f'(1) = 0$.
$f^{(2)}(X) = 12X^2 - 6X - 6$ y $f^{(2)}(1) = 0$.
$f^{(3)}(X) = 24X - 6$ y $f^{(3)}(1) = 18 \neq 0$.
Luego 1 es una raíz múltiple de orden 3.

Ejercicio. Un número $a \in K$ es raíz múltiple de $f(X)$ si y sólo si a es raíz del máximo común divisor de $f(X)$ y $f'(X)$.

Como consecuencia del ejercicio anterior se tiene que las raíces de $f(X)$ que *no son simples* son las raíces del máximo común divisor de $f(X)$ y $f'(X)$. Luego para determinar las raíces múltiples de un polinomio $f(X)$ basta calcular las raíces de $(f(X), f'(X))$. En particular, un polinomio $f(X)$ tiene todas sus raíces simples si y sólo si $(f(X), f'(X)) = 1$.

Teorema 8.17 *Si $f(X) \in K[X]$ es un polinomio de grado $n \geq 1$, entonces $f(X)$ tiene a lo sumo n raíces en K.*

Demostración. La demostración la hacemos por inducción sobre el grado del polinomio.

Si gr $f(X) = 1$, entonces $f(X) = a_1 X + a_0$, y su única raíz es $X = -\dfrac{a_0}{a_1}$.
Supongamos que el teorema vale para todos los polinomios de grado $n-1$.
Sea $f(X)$ un polinomio de grado n.
Si $f(X)$ no tiene ninguna raíz, no hay nada que demostrar.
Si $f(X)$ tiene una raíz a, entonces, por el corolario del Teorema del resto, es $f(X) = (X-a) \cdot q(X)$,

con gr $q(X) = n-1$. De aquí resulta que toda raíz de $q(X)$ es raíz de $f(X)$, y recíprocamente, una raíz de $f(X)$ es a ó una raíz de $q(X)$, por lo tanto, las raíces de $f(X)$ son a y las raíces de $q(X)$. Pero $q(X)$ tiene a lo sumo $n-1$ raíces en K (por la hipótesis de inducción), luego $f(X)$ tiene a lo sumo n raíces en K. □

Teorema 8.18 (Teorema Fundamental del Algebra). *Todo polinomio no constante con coeficientes en $\mathbb{C}$, tiene por lo menos una raíz en $\mathbb{C}$.*

Nota. La demostración de este teorema no puede hacerse en este curso, pues necesita algunos elementos de funciones de variable compleja. La primera demostración fue hecha por Gauss a principios del siglo pasado.

Veamos ahora que este Teorema implica que todo polinomio de grado n con coeficientes en $\mathbb{C}$, tiene exactamente n raíces en $\mathbb{C}$ (contando cada raíz tantas veces como su orden de multiplicidad).

En efecto, si $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, $a_n \neq 0$, por el Teorema Fundamental, $f(X)$ tiene una raíz, digamos c_1 en $\mathbb{C}$. Luego

$$f(X) = (X - c_1) \cdot q_1(X), \text{ con gr } q_1(X) = n-1.$$

Pero por el Teorema Fundamental, $q_1(X)$ tiene una raíz c_2 en $\mathbb{C}$. Luego

$$q_1(X) = (X - c_2) \cdot q_2(X), \text{ con gr } q_2(X) = n-2.$$

Entonces

$$f(X) = (X - c_1) \cdot (X - c_2) \cdot q_2(X).$$

Reiterando el procedimiento, al cabo de n pasos es:

$$f(X) = (X - c_1) \cdot (X - c_2) \cdot (X - c_3) \cdot \cdots \cdot (X - c_n) \cdot a_n$$

y $f(X)$ tiene raíces c_1, c_2, …, c_n, o sea, exactamente n raíces en $\mathbb{C}$.

Corolario 8.19 *Los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de primer grado.*

Demostración. Resulta de la demostración del Teorema anterior que todo polinomio $f(X)$ no constante es el producto de su coeficiente principal por polinomios $X - c_1$, $X - c_2$, …, $X - c_n$, donde c_1, c_2, …, c_n son las raíces de $f(X)$ en $\mathbb{C}$. Como todo polinomio de grado 1 es irreducible, esta es la factorización de $f(X)$ en factores irreducibles en $\mathbb{C}[X]$. De aquí resulta fácilmente el Corolario. □

Teorema 8.20 *Si z es una raíz compleja de un polinomio $f(X)$* **con coeficientes reales**, *entonces $\overline{z}$ también es raíz de $f(X)$. Además, z y $\overline{z}$ tienen el mismo orden de multiplicidad.*

Demostración. (Recordar que $\overline{z} \cdot \overline{z'} = \overline{z \cdot z'}$, $\overline{z} + \overline{z'} = \overline{z + z'}$ y $z = \overline{z} \Leftrightarrow z$ es real).

Sea $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, con $a_i \in \mathbb{R}$. Entonces $\overline{a_i} = a_i$ (porque a_i es un número real y por lo tanto es igual a su conjugado). Entonces

$$\begin{aligned}
f(\overline{z}) &= a_n\overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1\overline{z} + a_0 \\
&= \overline{a_n}\overline{z^n} + \overline{a_{n-1}}\overline{z^{n-1}} + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} \\
&= \overline{a_nz^n} + \overline{a_{n-1}z^{n-1}} + \cdots + \overline{a_1z} + \overline{a_0} \\
&= \overline{a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0} \\
&= \overline{f(z)}.
\end{aligned}$$

Luego $f(\overline{z}) = \overline{f(z)}$.

Si z es raíz de $f(X)$, entonces, por definición de raíz, es $f(z) = 0$, luego, tomando conjugados en ambos miembros, es $\overline{f(z)} = \overline{0}$, pero $\overline{0} = 0$, luego $\overline{f(z)} = 0$, y como $\overline{f(z)} = f(\overline{z})$, resulta $f(\overline{z}) = 0$, luego $\overline{z}$ es raíz de $f(X)$.

Veamos que z y $\overline{z}$ tienen el mismo orden de multiplicidad. Supongamos que el orden de multiplicidad de z es k y el orden de multiplicidad de $\overline{z}$ es k', y supongamos que $k > k'$.

Observemos que $(X - z)(X - \overline{z}) = (X - (a + b\ i))\,(X - (a - b\ i)) = X^2 - 2aX + (a^2 + b^2)$.

Se tiene que $f(X)$ es divisible por $(X-z)^{k'}$ y por $(X-\overline{z})^{k'}$, esto es, es divisible por $((X - z)(X - \overline{z}))^{k'} = \left(X^2 - 2aX + (a^2 + b^2)\right)^{k'}$ que tiene coeficientes reales. Luego $f(X) = \left(X^2 - 2aX + (a^2 + b^2)\right)^{k'} \cdot g(X)$, con $g(X) \in \mathbb{R}[X]$.

Ahora, z es raíz de $g(X)$ de orden de multiplicidad $k - k' > 0$ y $g(X)$ tiene coeficientes reales. Pero $\overline{z}$ no es raíz de $g(X)$. Contradicción. □

Ejemplos.

1. Hallar todas las raíces de $f(X)$ sabiendo que -3 es raíz múltiple.

$$f(X) = X^5 + 10X^4 + 34X^3 + 36X^2 - 27X - 54.$$

	1	10	34	36	-27	-54
-3		-3	-21	-39	9	54
	1	7	13	-3	-18	0
-3		-3	-12	-3	18	
	1	4	1	-6	0	
-3		-3	-3	6		
	1	1	-2	0		
-3		-3	6			
	1	-2	$4 \neq 0$			

Luego -3 es raíz múltiple de orden 3, y se tiene que

$$f(X) = (X + 3)^3 \cdot (X^2 + X - 2).$$

Las restantes raíces de $f(X)$ son las raíces de $X^2 + X - 2$, que son 1 y -2.

2. Idem para $f(X) = X^4 - 2X^3 - 3X^2 + 10X - 10$, sabiendo que $1 + i$ es una raíz del mismo.
Como $1 + i$ es raíz de $f(X)$ y $f(X)$ tiene coeficientes reales, también lo es $1 - i$. Además, puede verse que ambas tienen orden de multiplicidad 1. Entonces

	1	-2	-3	10	-10
$1 + i$		$1 + i$	-2	$-5 - 5\ i$	10
	1	$-1 + i$	-5	$5 - 5\ i$	0
$1 - i$		$1 - i$	0	$-5 + 5\ i$	
	1	0	-5	0	

Entonces

$$f(X) = (X - (1 + i)) \cdot (X - (1 - i)) \cdot (X^2 - 5) = (X^2 - 2X + 2) \cdot (X^2 - 5)$$

y las restantes raíces de $f(X)$ son las raíces de $X^2 - 5$, esto es, $\sqrt{5}$ y $-\sqrt{5}$.

Observación. Del Teorema anterior resulta que si $f(X)$ es un polinomio con coeficientes reales y si $z = a + b\,i$ es raíz de $f(X)$, entonces $f(X)$ es divisible por $X - z$ y por $X - \overline{z}$. Entonces $f(X)$ es divisible por

$$(X - z) \cdot (X - \overline{z}) = X^2 - (z + \overline{z})X + z \cdot \overline{z} = X^2 - 2aX + (a^2 + b^2) = X^2 + pX + q$$

que es un polinomio con coeficientes reales tal que $p^2 - 4q < 0$, como se verifica sin dificultad. Entonces, si $f(X)$ es no constante, $c_1, c_2, \ldots, c_r$ son todas sus raíces reales y $z_1, \overline{z_1}, z_2, \overline{z_2}, \ldots, z_s, \overline{z_s}$, son todas sus raíces complejas $(r + 2s = n)$, entonces $f(X)$ se descompone en factores irreducibles en $\mathbb{R}[X]$ en la forma

$$f(X) = a_n(X - c_1)\ldots(X - c_r)(X^2 + p_1X + q_1)\ldots(X^2 + p_sX + q_s)$$

Corolario 8.21 *En $\mathbb{R}[X]$, los únicos polinomios irreducibles son los de grado 1 y los de segundo grado de la forma $a(X^2 + bX + c)$, con $b^2 - 4c < 0$.*

Demostración. Es consecuencia inmediata de la observación anterior. □

Corolario 8.22 *Todo polinomio con coeficientes reales de grado impar tiene por lo menos una raíz real.*

Demostración. Es consecuencia inmediata de la observación anterior. □

Relación entre las raíces de un polinomio y sus coeficientes

Sea $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ y sean $c_1, c_2, \ldots, c_n$ sus raíces en $\mathbb{C}$. O sea $f(X) = a_n \cdot (X - c_1) \cdot (X - c_2) \cdot \cdots \cdot (X - c_n)$ en $\mathbb{C}[X]$.

Vamos a establecer relaciones entre los coeficientes a_i de $f(X)$ y sus raíces.

De

$$\begin{aligned} f(X) &= a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \\ &= a_n \cdot (X - c_1) \cdot (X - c_2) \cdot \cdots \cdot (X - c_n) \\ &= a_nX^n - a_n(c_1 + c_2 + \cdots + c_n)X^{n-1} + a_n(c_1c_2 + c_1c_3 + \cdots + \\ &\quad c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n)X^{n-2} - \cdots + (-1)^n a_n c_1 c_2 \cdots c_n \end{aligned}$$

se siguen las identidades, denominadas *relaciones de Vieta.*

$$\begin{aligned} -\frac{a_{n-1}}{a_n} &= c_1 + c_2 + \cdots + c_n \\ \frac{a_{n-2}}{a_n} &= c_1c_2 + \cdots + c_{n-1}c_n \\ \vdots &\quad \vdots \\ (-1)^n\frac{a_0}{a_n} &= c_1 \cdot c_2 \cdot \cdots \cdot c_n \end{aligned}$$

Las expresiones $c_1 + c_2 + \cdots + c_n,\ c_1c_2 + \cdots + c_{n-1}c_n,\ \ldots,\ c_1 \cdot c_2 \cdot \cdots \cdot c_n,$ se llaman los *polinomios simétricos elementales* en $c_1, c_2, \ldots, c_n$.

Ejemplo. Calcular las raíces a, b, c del polinomio $f(X) = X^3 - \sqrt{5}X^2 - 2X + 2\sqrt{5}$, sabiendo que $a + b = 0$.

Ejemplo. (Gentile) Sea $a \in \mathbb{Q}$, $a \neq 0$. Encontrar un polinomio mónico de grado 4 en $\mathbb{Q}[X]$ que tenga a, $-a$, $\frac{1}{a}$, $-\frac{1}{a}$ por raíces.

Sea $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$. Tenemos que determinar los coeficientes a_i.

$$\begin{aligned} -a_3 &= a + (-a) + \frac{1}{a} + \left(-\frac{1}{a}\right) = 0 \\ a_2 &= -a^2 + 1 - 1 - 1 + 1 - \frac{1}{a^2} \\ -a_1 &= -a + a - \frac{1}{a} + \frac{1}{a} = 0 \\ a_0 &= 1 \end{aligned}$$

Luego

$$f(X) = x^4 - \left(\frac{a^4+1}{a^2}\right) X^2 + 1$$

Ejercicios. 1.- El polinomio $f(X) = X^2 + pX + q$ tiene la propiedad de que la suma de sus raíces es $p + q$ y el producto es $p \cdot q$. Hallar p y q.
2.- La suma de dos raíces del polinomio $f(X) = 2X^3 - X^2 - 7X + \lambda$ es 1. Hallar λ y las raíces de $f(X)$.

8.4 Cálculo de las raíces de un polinomio

Consideraremos ahora el problema del cálculo de las raíces de un polinomio.

Es muy simple calcular la raíz de un polinomio de grado 1, y para polinomios de grado 2 es muy conocida la fórmula que permite calcular sus raíces. También existen fórmulas generales para calcular las raíces de polinomios de grados 3 y 4, aunque no creemos razonable incluirlas aquí. Se dice que las ecuaciones de grado menor que 5 admiten resolubilidad por *radicales* porque pueden resolverse mediante fórmulas que involucran las operaciones de suma, producto y extracción de raíces.

El problema de la resolución general de la ecuación de grado n por radicales ha sido de gran importancia en la historia de la Matemática y su estudio ha sido el motivador de gran parte de la matemática actual. Se puede demostrar que no es posible obtener una fórmula general que involucre sólamente operaciones de suma, producto y extracción de raíces n-ésimas y que permita calcular las raíces de un polinomio de grado mayor o igual que 5. La solución de este problema se debe a Evaristo Galois ($1811 - 1832$).

1. Acotación de las raíces reales de un polinomio con coeficientes reales

Teorema 8.23 (Regla de Laguerre-Thibault.) *Sea $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, $a_i \in \mathbb{R}$, con $a_n > 0$. Si al dividir $f(X)$ por $X - a$, con $a \geq 0$, todos los coeficientes del cociente, y el resto, son no negativos, entonces a es una cota superior de las raíces reales de $f(X)$.*

Demostración. Por el teorema del resto es $f(X) = (X - a) \cdot q(X) + f(a)$. Si todos los coeficientes de $q(X)$ son no negativos, y $f(a)$ es también no negativo, es claro que si $b > a$, entonces $f(b) > 0$, luego, por definición de raíz, si $b > a$, b no puede ser raíz de $f(X)$, o sea, que todas las raíces reales de $f(X)$ son menores o iguales que a. Luego a es una cota superior de las raíces de $f(X)$. □

Para hallar una cota inferior, se procede de la siguiente forma: se considera el polinomio $f(-X)$ y por el procedimiento anterior se calcula una cota superior l de las raíces de $f(-X)$, entonces $-l$ es una cota inferior de las raíces de $f(X)$.

Ejemplo. Acotar las raíces reales de $f(X) = X^3 - 3X^2 + 5X + 4$.
Dividimos por $X - 1$, $X - 2$, $X - 3$, ..., hasta que el resto y todos los coeficientes del cociente sean no negativos.

	1	−3	5	4
3		3	0	15
	1	0	5	19

Luego 3 es una cota superior de las raíces reales de $f(X)$.

Para hallar la cota inferior hacemos $f(-X) = -X^3 - 3X^2 - 5X + 4$, pero como el coeficiente principal debe ser positivo, consideramos $-f(-X) = X^3 + 3X^2 + 5X - 4$ y hallamos la cota superior de sus raíces.

	1	3	5	−4
1		1	4	9
	1	4	9	5

Luego 1 es cota superior de las raíces reales de $f(-X)$, luego -1 es cota inferior de las raíces reales de $f(X)$.

Por lo tanto, las raíces reales del polinomio $f(X)$ están todas en el intervalo $[-1, 3]$.

2. Número de las raíces reales positivas y negativas de un polinomio con coeficientes reales

Daremos sin demostración la siguiente:

Regla de Descartes. El número de raíces reales positivas de un polinomio $f(X)$ con coeficientes reales, contadas tantas veces como su orden de multiplicidad, es *menor o igual* que el número de variaciones de signo de los coeficientes de $f(X)$, y difiere del mismo en un número par.

Lo mismo vale para el número de raíces reales negativas: es *menor o igual* que el número de variaciones de signo de los coeficientes de $f(-X)$ y difiere del mismo en un número par.

Ejemplo. Hallar el número de raíces reales positivas y negativas de

$$f(X) = X^4 - 3X^3 - 5X^2 + 7X - 3.$$

Como en los coeficientes de $f(X)$ hay tres variaciones de signo, el número de raíces reales positivas de $f(X)$ es 3 ó 1.

Por otro lado, $f(-X) = X^4 + 3X^3 - 5X^2 - 7X - 3$, y este polinomio tiene una sola variación de signo en sus coeficientes. Entonces el número de raíces reales negativas es 1.

3. Raíces racionales de un polinomio con coeficientes racionales.

Consideremos la siguiente ecuación: $2X^3 + \frac{1}{2}X^2 + \frac{1}{3}X + 2 = 0$.

Si la multiplicamos por el m.c.m. de los denominadores, o sea, por 6, es: $12X^3 + 3X^2 + 2X + 12 = 0$, que es una ecuación con coeficientes enteros que tiene las mismas raíces que la anterior. Es decir, cuando tenemos un polinomio con coeficientes racionales, lo podemos transformar en un polinomio con coeficientes enteros que tiene las mismas raíces, multiplicándolo por el m.c.m. de los denominadores.

Teorema 8.24 (de Gauss). *Si un número racional $\frac{p}{q}$, con p y q relativamente primos, es raíz de un polinomio $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ con coeficientes enteros, entonces $p|a_0$ y $q|a_n$.*

Demostración. Como $\frac{p}{q}$ es raíz de $f(X)$ tenemos:

$$f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0.$$

Luego

$$f\left(\frac{p}{q}\right) = a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1\frac{p}{q} + a_0 = 0.$$

Multiplicando por q^n se tiene:

$$a_np^n + a_{n-1}p^{n-1}\cdot q + \cdots + a_1p\cdot q^{n-1} + a_0\cdot q^n = 0.$$

Luego

$$a_np^n + a_{n-1}p^{n-1}\cdot q + \cdots + a_1p\cdot q^{n-1} = -a_0\cdot q^n,$$

esto es,

$$p\cdot(a_np^{n-1} + a_{n-1}p^{n-2}\cdot q + \cdots + a_1\cdot q^{n-1}) = -a_0\cdot q^n.$$

Luego $p|a_0\cdot q^n$, pero como p y q son relativamente primos, entonces $p|a_0$.
Análogamente se demuestra que $q|a_n$. □

Ejemplo. Calcular las raíces racionales de $X^3 + \frac{1}{2}X^2 - \frac{7}{2}X - 3$.
Es lo mismo que calcular las raíces racionales de $2X^3 + X^2 - 7X - 6$. Éstas son de la forma $\frac{p}{q}$, donde $p|-6$ y $q|2$.

$$p:\ \pm1,\ \pm2,\ \pm3,\ \pm6;\ q:\ \pm1,\ \pm2.$$

Luego las posibles raíces racionales son:

$$\frac{\pm1}{\pm1},\ \frac{\pm2}{\pm1},\ \frac{\pm3}{\pm1},\ \frac{\pm6}{\pm1},\ \frac{\pm1}{\pm2},\ \frac{\pm2}{\pm2},\ \frac{\pm3}{\pm2},\ \frac{\pm6}{\pm2},$$

o sea,

$$1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 6,\ -6,\ \frac{1}{2},\ -\frac{1}{2},\ \frac{3}{2},\ -\frac{3}{2}.$$

Reemplazando en $f(X)$ o aplicando la regla de Ruffini, se ve que las raíces racionales son: -1, 2 y $-\frac{3}{2}$.

En resumen: Dado un polinomio no constante $f(X)$, el procedimiento para hallar las raíces de $f(X)$ es el siguiente:

1. Se acotan las raíces reales.
2. Se determina el número de raíces reales positivas y negativas.
3. Se determinan las raíces racionales.
4. Una vez determinada una raíz de $f(X)$, se analiza su orden de multiplicidad y se obtiene un polinomio de menor grado que $f(X)$ cuyas raíces son también raíces de $f(X)$.

Ejercicios.

1. Sea $f(X) = 6X^4 + 17X^3 + 8X^2 - 5X - 2$. Verificar que -3 es una cota inferior para las raíces reales de $f(X)$ y 1 es una cota superior. Verificar que el número de raíces reales positivas es 1 y que el número de raíces reales negativas es 3 ó 1. Las raíces son: $\frac{1}{2}$, $-\frac{1}{3}$, -1, -2.

2. Sea $f(X) = 2X^3 + X^2 - 5X + 2$. Verificar que las raíces reales están en el intervalo $[-2, 2]$. El número de raíces reales positivas es 2 ó 0. El número de raíces reales negativas es 1. Las posibles raíces racionales son ± 1, ± 2, $\pm\frac{1}{2}$. Las raíces son: 1, -2 y $\frac{1}{2}$.

4. El Teorema de Bolzano-Weierstrass.

El siguiente teorema juega un papel importante en la localización de las raíces de un polinomio con coeficientes reales.

Teorema 8.25 (Bolzano-Weierstrass). *Sea $f(X) \in \mathbb{R}[X]$ y sean $a, b \in \mathbb{R}$, $a < b$. Si $f(b)$ y $f(a)$ son no nulos y tienen diferente signo, entonces existe un número $c \in (a, b)$ tal que $f(c) = 0$.*

Ejemplos.

1. Vamos a localizar las raíces reales del polinomio $f(X) = X^4 - 2X^3 + X^2 - 1$. Calculemos los valores $f(a)$ para algunos números enteros a.

   $f(-1) = 3$ (positivo) $\quad f(0) = -1$ (negativo) $\quad f(1) = -1$ (negativo) $\quad f(2) = 3$ (positivo)

   Luego f tiene una raíz en el intervalo $(-1, 0)$ y otra en el intervalo $(1, 2)$. Si nos interesa podemos subdividir estos intervalos y localizar las raíces en los subintervalos correspondientes. El método utilizado repetidamente puede ser muy efectivo utilizando una calculadora. Así, $[-1, 0] = [-1, -0, 5] \cup [-0, 5\ ; 0]$. Como $f(-0, 5) = 0, 5$, la raíz se encuentra en el intervalo $[-0, 5\ ; 0]$. Repetimos el proceso al intervalo $[-0, 5\ ; 0]$.

   Una observación directa del polinomio nos muestra que $f(a) > 0$ para todo $a < -1$, y que $f(a) > 0$ para todo $a > 2$. Es decir, no hay otros cambios de signo en los valores de $f(a)$ más que los indicados. En consecuencia, $f(X)$ tiene dos raíces reales.

2. (Gentile) Calcular las raíces del polinomio $f(X) = X^3 - 3X - 1$.

   Calculemos los valores $f(a)$ para algunos números enteros a.

   $f(-2) = -3$ (negativo) $\quad f(-1) = 1$ (positivo) $\quad f(0) = -1$ (negativo)
   $f(1) = -3$ (negativo) $\quad f(2) = 1$ (positivo)

   De lo anterior concluimos que f tiene una raíz (real) en el intervalo $(-2, -1)$, otra en el intervalo $(-1, 0)$ y otra en el intervalo $(1, 2)$. Vamos a aproximar la raíz que se encuentra en el intervalo $(1, 2)$ mediante sucesivas subdivisiones de este intervalo. En este momento es indispensable el uso de una calculadora. Llamemos c a esa raíz.

$f(1,8) = -0,568$ (negativo)	$f(2) = 1$ (positivo) ,	luego $c \in (1,8\ ;2)$
$f(1,8) = -0,568$	$f(1,9) = 0,159$,	luego $c \in (1,8\ ;1,9)$
$f(1,87) = -0,070797$	$f(1,88) = 0,004672$,	luego $c \in (1,87\ ;1,88)$
$f(1,879) = -0,0029256$	$f(1,880) = 0,0046720$,	luego $c \in (1,879\ ;1,880)$
$f(1,8793) = -0,0006475$	$f(1,8894) = 0,0001121$,	luego $c \in (1,8793\ ;1,8794)$
$f(1,87938) = -0,0000398$	$f(1,87939) = 0,0000361$,	luego $c \in (1,87938\ ;1,87939)$
$f(1,879385) = -0,0000018$	$f(1,879386) = 0,0000058$,	luego $c \in (1,879385\ ;1,879386)$
$f(1,8793852) = -0,0000003$	$f(1,8793853) = 0,0000004$	

Luego $c \cong 1,879385$ con todas sus cifras exactas.

8.5 Ejercicios

1. Efectuar en $\mathbb{R}[X]$:
   (a) $(X^2 - 3\,X + 3)\,(X^2 + 3\,X + 3)$,
   (b) $(X^2 + 2\,X - 1)^2$,
   (c) $(X^3 + X^2 - X - 1)\,(X^2 - 2\,X + 1) + \dfrac{3}{2}\,X + 2$.

2. Dados $f(X) = 3\,X^5 - 2\,X^3 + X^2 - 5\,X - 1$ y $g(X) = 2\,X^4 - 3\,X^2 - X + 5 \in \mathbb{R}[X]$, determinar:
   (a) $gr[f(X) + g(X)^3]$.
   (b) $gr[f(X) - X^3\,g(X)]$.
   (c) El coeficiente principal de $f(X)^3 + g(X)^2$.
   (d) El término independiente de $f(X)^5 - 7\,(X - 2)\,g(X)^2$.
   (e) El coeficiente de X^5 en $f(X)\,g(X)$.

3. Hallar un polinomio cuyo cuadrado es $X^4 - 2\,X^3 + c\,X^2 - 30\,X + d$ y calcular los valores reales de c y d .

4. Determinar $a, b \in \mathbb{R}$ de modo tal que $f(X) = g(X)$.
   (a) $f(X) = 6X^2 + aX + b\,, \quad g(X) = (3X - 1)\,(2X + 1)$.
   (b) $f(X) = a\,(X^2 - X - 2) + b\,(X - 1) + \dfrac{5}{2}\,(X^2 - 3X + 4)\,, \quad g(X) = 3X^2 + 2X - 1$.
   (c) $f(X) = a\,(X^2 + X + 3) + b\,(X^2 - 2X + 1) + \dfrac{7}{16}\,(X^2 - 3)\,, \quad g(X) = 2X - 1$.

5. Hallar el cociente y el resto de la división de:
   (a) $2\,X^4 - 3\,X^3 + 4\,X^2 - 5\,X + 6 \quad$ por $\quad X^2 - 3\,X + 1$,
   (b) $X^2 + X + 1 \quad$ por $\quad X^3 + 2$,
   (c) $-4\,X^3 + X^2 \quad$ por $\quad X^2 + X + 3$.

6. Calcular el valor numérico de los siguientes polinomios, en los valores de a indicados:
   (a) $f(X) = X^4 - 2X^3 + X + 1\,, \quad a = 0$.
   (b) $f(X) = \sqrt{2}\,X^2 - \dfrac{\sqrt{8}}{5}\,X\,, \quad a = \sqrt{2}$.
   (c) $f(X) = 2X^5 - 7X^3 - 10X^2 + 2X + 7\,, \quad a = -1$.

7. (a) Aplicando la regla de Ruffini hallar el cociente y el resto de dividir:
   (i) $X^4 + 2\,X^3 - 3\,X^2 - 4\,X + 1 \quad$ por $\quad X + 1$,
   (ii) $X^5 \quad$ por $\quad X - 2$,
   (iii) $X^3 + X \quad$ por $\quad X + \dfrac{1}{2}$.

(b) Dados $f(X) = 2\,X^5 - X^4 + 3\,X^3 - \dfrac{1}{3}$, $g(X) = 3\,X^7 - X^6 + 2\,X^2$ y

$s(X) = X^9 - X^8 + 5\,X^7 + \dfrac{1}{2}\,X^6 + 1$ hallar: $f(-2)$, $g(\dfrac{1}{3})$, $s(-1)$ y $s(i)$.

8. Aplicar el teorema del resto y hallar las condiciones para que $X^n \pm a^n$ sea divisible por $X \pm a$, $a \in \mathbb{R}$, $a \neq 0$.

9. $f(X) = 3\,X^3 - 9\,X^2 + k\,X - 12$ es divisible por $X - 3$. Determinar cuál de los siguientes polinomios es factor de $f(X)$:

   (i) $3\,X^2 - X + 4$ (ii) $3\,X^2 - 4$ (iii) $3X^2 + 4$ (iv) $3\,X - 4$ (v) $3\,X + 4$.

10. Determinar los valores reales de a y b de modo que:

    (a) Al dividir $f(X) = 6\,X^2 + a\,X + b$ por $g(X) = 3\,X - 2$, el resto es cero y el cociente $q(X) = 2\,X - 1$.
    (b) $2\,X^2 + a\,X + 3$ sea divisible por $2\,X - 5$,
    (c) $X^2 + a\,X + 4$ dé el mismo resto al dividirlo por $X + 2$ y $X - 2$.

11. Hallar el m.c.d. (mónico) de los siguientes pares de polinomios:

    (a) $f(X) = X^3 - 1$, $g(X) = X^4 + X^3 + 2X^2 + X + 1$.
    (b) $f(X) = X^3 - 1$, $g(X) = X^4 + 1$.

    Expresarlo en la forma $d(X) = s(X) \cdot f(X) + t(X) \cdot g(X)$.

12. Hallar las raíces de los siguientes polinomios:

    (a) $3\,X^4 - X^2 - 2$ (b) $X^4 + 4\,X^2 + 4$
    (c) $2\,X^2 - X - 3$ (d) $X^5 + i\,X^3 + X^3$
    (e) $X^2 - 2\sqrt{2}\,X + 3$ (f) $X^6 + 2\,X^4 + X^2$
    (g) $X^2 + (5 + 2\,i)\,X + 5 + 5\,i$

13. Determinar el orden de multiplicidad de la raíz indicada:

    (a) 1 en $(X^2 - 1)(X^3 - 1)$,
    (b) 0 en $X^3\,(X^3 - 2\,X^2 + X)$,
    (c) -1 en $(X^2 - 1)(X^3 + 1)$,
    (d) -2 en $X^4 + 2\,X^3 + 4X^2 + 8\,X$,
    (e) 5 en $X^4 - 4.5\,X^3 + 6.5^2\,X^2 - 4.5^3\,X + 5^4$.

14. Hallar las raíces de los siguientes polinomios:

    (a) $X^5 + 6\,X^4 + 15\,X^3 + 26\,X^2 + 36\,X + 24$ sabiendo que $\alpha = -2$ es una raíz múltiple.
    (b) Idem para $8\,X^4 - 4\,X^3 - 10\,X^2 + 9\,X - 2$ y $\alpha = \dfrac{1}{2}$.
    (c) $X^5 + X^3 + (1 - i)\,X^2 + (1 - i)$ sabiendo que $X^2 + 1$ es factor de dicho polinomio.
    (d) $i\,X^2 - X + i$.
    (e) $X^4 + 2X^2 + 4$.

15. Determinar el menor valor entero k para el cual $f(X) = 2X \cdot (kX - 4) - X^2 + 6$ no posea raíces reales.

16. 1 es raíz múltiple del polinomio $f(X) = X^6 - 6X + 5$. ¿ Cuál es su orden de multiplicidad ? ¿ Tiene $f(X)$ otras raíces múltiples ?

17. Si 2 es raíz de orden 3 de un polinomio $f(X)$ que no tiene otras raíces múltiples, hallar (f, f').

18. Mostrar que $X^7 + X^5 + X^3 + 1$ no posee raíces múltiples en $\mathbb{R}$.

19. Hallar el valor de a para el cual $X^7 - aX^6 + aX - 1$ tenga a 1 como raíz triple.

20. Expresar el polinomio $f(X) = X^6 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{C}[X]$.

21. Si $-6i$ es una raíz múltiple de orden 5 de un polinomio $f(X) \in \mathbb{R}[X]$, ¿ cuáles son sus restantes raíces si $gr\ f(X) = 11$ y su término independiente es nulo ? Si $f(X)$ es mónico, escribirlo como producto de irreducibles en $\mathbb{R}[X]$.

22. Si $f(X) = 8(X^2 - 2)^4(X - 3)^2(X - 5\ i)^7(X + 5\ i)^7$, hallar la descomposición de $f(X)$ en irreducibles mónicos en $\mathbb{R}[X]$.

23. Hallar las raíces de $f(X) = 2\,X^7 + 10\,X^5 - 4\,X^4 - 66\,X^3 - 32\,X^2 + 54\,X + 36$ sabiendo que $-3\ i$ y -1 son raíces. Descomponer el polinomio en producto de irreducibles sobre $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

24. Hallar las raíces de $X^4 - 3X^3 + 5X^2 - 27X - 36$ sabiendo que tiene una raíz imaginaria pura.

25. ¿ Son válidas las siguientes afirmaciones ?

    (a) Si $X^3 + 7X - 6\ i$ tiene a $\ i\ $ como raíz, entonces $-i$ es otra raíz.

    (b) Si $X^3 + (1 - 2\sqrt{3})X^2 + (5 - 2\sqrt{3})X + 5$ tiene a $\sqrt{3} - \sqrt{2}\ i$ como raíz, entonces $\sqrt{3} + \sqrt{2}\ i$ es otra raíz.

    (c) Si $X^4 + (1 - 2\sqrt{2})X^3 + (4 - 2\sqrt{2})X^2 + (3 - 4\sqrt{2})X + 1$ tiene a $-1 + \sqrt{2}$ como raíz, entonces $-1 - \sqrt{2}$ es otra raíz.

26. (a) Si $\epsilon = \cos\dfrac{2\pi}{n} + i\ \text{sen}\ \dfrac{2\pi}{n}$, demostrar que:
    $X^{n-1} + X^{n-2} + \cdots + X + 1 = (X - \epsilon)(X - \epsilon^2)\cdots(X - \epsilon^{n-1})$.

    (b) Si ϵ es una raíz primitiva de la unidad de orden n, probar que:
    $n = (1 - \epsilon)(1 - \epsilon^2)\cdots(1 - \epsilon^{n-1})$.

    (c) Hallar todas las raíces del polinomio $X^n + X^{n-1} + \cdots + X + 1$.

27. (a) Sea $f(X) \in \mathbb{Q}[X]$ un polinomio de tercer grado. Probar que $f(X)$ es reducible en $\mathbb{Q}[X]$ si y sólo si $f(X)$ posee una raíz en $\mathbb{Q}$. Todo polinomio de tercer grado en $\mathbb{R}[X]$ es reducible. Dar ejemplos de polinomios de tercer grado en $\mathbb{Q}[X]$ irreducibles.

    (b) Dar ejemplos que prueben que la siguiente afirmación es falsa:
    "Si $f(X) \in \mathbb{Q}[X]$ no tiene ninguna raíz en $\mathbb{Q}$, entonces es irreducible sobre $\mathbb{Q}$".

    (c) Analizar la validez de la siguiente proposición: "Si $f(X) \in \mathbb{R}[X]$ no tiene ninguna raíz en $\mathbb{R}$, entonces es irreducible en $\mathbb{R}[X]$".

    (d) Demostrar que los irreducibles en $\mathbb{R}[X]$ son los polinomios de primer grado y los de segundo grado con discriminante negativo, y los irreducibles en $\mathbb{C}[X]$ son los polinomios de primer grado.

28. Encontrar un polinomio a coeficientes reales de grado mínimo que posea las siguientes raíces:

    (a) $1\ ,\ -2\ ,\ -\dfrac{1}{3}\ ,$

    (b) 1 raíz triple , $2\,i\ ,$

    (c) $0,\ -\dfrac{1}{2}\ ,\ \dfrac{1}{2}\ ,\ -3$ raíz doble ,

    (d) 0 raíz doble , $1-i\ ,\ \sqrt{2}\ .$

29. Hallar las raíces racionales, en caso de existir, de los siguientes polinomios:

    (a) $X^3 - 6\,X^2 + 15\,X - 14,$

    (b) $X^5 - 7\,X^3 - 12\,X^2 + 6\,X + 36\ ,$

    (c) $X^4 - 2\,X^3 - 8\,X^2 + 13\,X - 24\ ,$

    (d) $2\,X^3 - 2\,X - 12\ ,$

30. Acotar las raíces reales de los siguientes polinomios:

    (a) $X^3 - X + 4$

    (b) $X^3 - 7X - 7$

    (c) $X^7 + X^2 + 1$

    (d) $X^4 + 2X^3 - X^2 - 1$

31. (a) Analizar, utilizando la regla de Descartes, las raíces de los siguientes polinomios:

        (i) $X^5 - 8X + 6$

        (ii) $X^5 - 6X^2 + 3$

        (iii) $X^3 - 3X + 1$

    (b) Determinar exactamente el número de raíces reales positivas, negativas y complejas de los polinomios de a).

32. Calcular las raíces del polinomio $X^7 - \dfrac{4}{3}\,X^6 - \dfrac{11}{9}\,X^5 + \dfrac{52}{9}\,X^4 - 5\,X^3 - \dfrac{16}{3}\,X^2 - X,$ sabiendo que $\alpha = 1 + \sqrt{2}\,i$ es raíz. Factorizarlo sobre $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

33. Hallar todas las raíces del polinomio $f(X) = 5X^7 - 2X^6 - 10X^5 + 4X^4 - 15X^3 + 6X^2$.

34. Hallar las raíces del polinomio $f(X) = X^5 + 12X^4 + 57X^3 + 134X^2 + 156X + 72$ sabiendo que admite raíces múltiples.

35. Sea $f(X) = X^6 - 3X^5 - 6X^3 - X + 8$. Determinar cuál de las siguientes afirmaciones es válida. Justificar las respuestas.

    (a) $f(X)$ no tiene raíces reales.

    (b) $f(X)$ tiene exactamente dos raíces reales negativas distintas.

    (c) $f(X)$ tiene una raíz real negativa.

    (d) $f(X)$ no posee raíces reales negativas, pero posee al menos una raíz real positiva.

36. Hallar el valor de a, sabiendo que la suma de dos raíces del polinomio $2X^3 - X^2 - 7X + a$ es 1.

37. Hallar

    (i) la suma,

    (ii) la suma de los cuadrados,

    (iii) el producto,

    (iv) la suma de los inversos,

    de las raíces de los siguientes polinomios, sin calcularlas:

    (a) $X^3 + 3\,X - 1$.

    (b) $X^9 - 1$.

    (c) $X^4 + X^3 + X + 1$.

    (d) $X^n - 1$.

9 Cálculo combinatorio y binomio de Newton

9.1 Cálculo combinatorio

Consideremos los siguientes problemas:

- Una casa de electrodomésticos tiene 4 marcas diferentes de heladeras, y en cada marca, tiene tres tamaños diferentes. ¿Cuántas clases de heladeras tiene ese comercio para ofrecer a sus clientes? La respuesta se obtiene multiplicando $4 \cdot 3$, ya que hay 4 heladeras chicas, 4 medianas, y 4 grandes, esto es,
$$4 + 4 + 4 = 4 \cdot 3 = 12.$$

- ¿De cuántas maneras se pueden formar palabras de tres letras con las letras a, b, c, d, e, sin repetir ninguna letra?
Consideremos el primero de los tres lugares:

  a __ __ , b __ __ , c __ __ , d __ __ , e __ __

  Es claro que hay 5 elecciones posibles para llenar el primer lugar. Una vez hecha la elección de la primera letra, hay 4 elecciones posibles para la segunda, y la tercera se puede elegir de 3 formas diferentes. Se tienen entonces
$$5 \cdot 4 \cdot 3 = 60$$
  palabras posibles.

Estos ejemplos ilustran el llamado

Principio de multiplicación. *Si un evento puede ocurrir en m formas y un segundo evento puede ocurrir en n formas, el número de formas en las que pueden ocurrir ambos es $m \cdot n$.*

Factoriales

Dado un número entero $n \geq 0$, se llama factorial de n, y se nota $n!$, al número definido de la siguiente manera:

$$\begin{aligned} 0! &= 1 \\ n! &= n \cdot (n-1)! \text{ si } n > 0. \end{aligned}$$

Ejemplos.

1. $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1$.
   $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$.
2. $\dfrac{(n+1)!}{n!} = \dfrac{(n+1) \cdot n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1}{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1} = (n+1)$.
3. $\dfrac{(n+2)!}{(n-1)!} = \dfrac{(n+2) \cdot (n+1) \cdot n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1}{(n-1) \cdot (n-2) \cdot \cdots \cdot 3 \cdot 2 \cdot 1} = (n+2) \cdot (n+1) \cdot n$.
4. $\dfrac{n!}{(n-r)!} = n \cdot (n-1) \cdot \cdots \cdot (n-r+1)$.

En los párrafos que siguen, se tendrán m objetos distintos, entre los cuales se seleccionará un subconjunto formado por n de esos m objetos. Analizaremos diferentes casos, que dependerán de si el *orden* de la elección es importante y de si se permiten elementos *repetidos*.

Variaciones

Dados m elementos distintos, una variación de orden n de m elementos ($n \leq m$), es una selección *ordenada* formada por n de esos m objetos.

Es decir, una variación de m elementos de orden n (ó de m elementos tomados de a n) es una selección de n objetos *distintos* entre los m dados, en la que importa el *orden* en que se eligen.

Indicaremos con V_m^n el número de variaciones de m objetos de orden n.

Teorema 9.1 $\quad V_m^n = \dfrac{m!}{(m-n)!}$.

Demostración. Probaremos la fórmula por inducción.
Si $n = 1$, el número de variaciones de m elementos tomados de a 1 es m. Entonces $V_m^1 = m = \dfrac{m!}{(m-1)!}$.
Supongamos que la fórmula vale para $n-1$, es decir,

$$V_m^{n-1} = \frac{m!}{(m-n+1)!}.$$

Las variaciones de orden n pueden hallarse de la siguiente manera: a cada variación de orden $n-1$, se le agrega (por ejemplo, a la derecha) uno de los $m-(n-1) = m-n+1$ objetos que no figuran en esa variación.
Entonces cada variación de orden $n-1$ da origen a $m-n+1$ variaciones de orden n. Luego

$$V_m^n = V_m^{n-1} \cdot (m-n+1) = \frac{m!}{(m-n+1)!} \cdot (m-n+1) = \frac{m!}{(m-n)!}.$$

□

Ejemplos.

1. ¿De cuántas maneras se pueden formar palabras de 3 letras con las letras a, b, c, d, e, sin repetir ninguna?
   Cada palabra es una variación de 5 objetos tomados de a 3. Luego la respuesta es:

$$V_5^3 = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 5 \cdot 4 \cdot 3 = 60.$$

2. (a) ¿Cuántos números de 3 cifras distintas pueden formarse con los dígitos 1, 3, 5, 7 y 9?

$$V_5^3 = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 5 \cdot 4 \cdot 3 = 60.$$

   (b) ¿Cuántos de ellos empiezan con 1?

$$V_4^2 = \frac{4!}{(4-2)!} = \frac{4!}{2!} = 4 \cdot 3 = 12.$$

(c) ¿Cuántos terminan con 37?

$$V_3^1 = \frac{3!}{(3-1)!} = \frac{3!}{2!} = 3.$$

3. Se desea hacer una apuesta en una carrera de caballos seleccionando los 3 caballos que ocuparán los 3 primeros puestos al finalizar la carrera. Si en ella participan 9 caballos ¿De cuántas formas se pueden elegir los 3 primeros caballos?

$$V_9^3 = \frac{9!}{(9-3)!} = \frac{9!}{6!} = 9 \cdot 8 \cdot 7 = 504.$$

4. Un candidato debe visitar 8 ciudades antes de las elecciones. Sin embargo, sólo dispone de tiempo para visitar 3 de ellas. ¿Entre cuántos itinerarios diferentes tiene para elegir?

$$V_8^3 = \frac{8!}{(8-3)!} = \frac{8!}{5!} = 8 \cdot 7 \cdot 6 = 336.$$

5. ¿Cuántos números naturales menores que 1000 tienen dígitos diferentes?
El problema puede separarse en tres casos:

(i) Números con un dígito: $V_9^1 = 9$.

(ii) Números con dos dígitos: $V_{10}^2 - V_9^1 = 81$.

(iii) Números con tres dígitos: $V_{10}^3 - V_9^2 = 648$.

Luego hay $9 + 81 + 648 = 738$ números menores que 1000 con dígitos diferentes.

El ejemplo anterior ilustra el **principio de adición**: *si los eventos a ser contados están separados en casos, el número total de eventos es la suma de los números de los distintos casos.*

Si $n = m$, las variaciones de m objetos tomados de a m se llaman *permutaciones* de orden m, y se nota P_m. Entonces

$$P_m = V_m^m = m!$$

Ejemplo. ¿De cuántas maneras se pueden sentar 5 personas en una fila de 5 asientos?

$$P_5 = 5! = 120$$

Variaciones con repetición

Dados m objetos o elementos distintos, se llama *variación con repetición* de orden n de esos m objetos a toda sucesión formada por n (no necesariamente distintos) de los m objetos dados.

En este caso, no es necesario que $n \leq m$.

Notaremos $V_m^{'n}$ al número de variaciones con repetición de m objetos tomados de a n.

Teorema 9.2

$$V_m^{'n} = m^n.$$

Demostración. Haremos inducción sobre n.
Si $n = 1$ es claro que $V_m^{'1} = m = m^1$.
Sea $n > 1$ y supongamos que la fórmula vale para $n - 1$. Probémosla para n.
El razonamiento es similar al de la demostración del teorema anterior. Cada variación con repetición de orden $n - 1$ da origen a m variaciones con repetición de orden n agregando a la derecha cada uno de los m elementos disponibles. Luego

$$V_m^{'n} = V_m^{'n-1} \cdot m = m^{n-1} \cdot m = m^n.$$

□

Ejemplos.

1. ¿Cuántas patentes de automóvil de seis símbolos puede haber si cada patente comienza con 3 letras y termina con 3 dígitos ?
   Tanto las letras como los dígitos pueden repetirse. Como hay 27 letras en el alfabeto y 10 dígitos, tenemos
   $$V_{27}^{'3} \cdot V_{10}^{'3} = 27^3 \cdot 10^3$$

2. ¿De cuántos códigos de tres dígitos dispone una compañía telefónica, si no hay restricciones para los dígitos? ¿Cuántos, si el primer dígito no puede ser 0?

   $$V_{10}^{'3} = 10^3 = 1000, \qquad V_{10}^{'3} - V_{10}^{'2} = 10^3 - 10^2 = 900.$$

3. Determinar la cantidad de posibles números de siete dígitos si los tres primeros no pueden ser cero y

   (a) puede emplearse cualquier dígito para el resto de los lugares.

   $$V_9^{'3} \cdot V_{10}^{'4}$$

   (b) todos los dígitos tienen que ser impares.

   $$V_5^{'7}$$

   (c) el primer dígito tiene que ser impar e ir alternándose entre pares e impares.

   $$V_5^{'4} \cdot 4 \cdot V_5^{'2}$$

   (d) no puede repetirse ningún dígito.

   $$V_{10}^7 - 3 \cdot V_9^6 \quad \text{ó} \quad V_9^3 \cdot V_7^4$$

Combinaciones

Dado un conjunto A con m elementos, se llama *combinación* de orden n $(n \leq m)$ de esos m elementos a todo subconjunto de A con n elementos.

En una combinación no se permiten repeticiones, pero no interesa el orden de los objetos.

El número de combinaciones de m objetos tomados de a n se nota C_m^n.

Ejemplo. Calculemos C_4^3. Según la definición, C_4^3 es el número de subconjuntos con 3 elementos de un conjunto con 4 elementos. Sea entonces $A = \{x, y, z, t\}$. Los subconjuntos de A con 3 elementos son:

$$\{x, y, z\}, \quad \{x, y, t\}, \quad \{x, z, t\}, \quad \{y, z, t\}.$$

Luego $C_4^3 = 4$.

Teorema 9.3

$$C_m^n = \frac{V_m^n}{P_n} = \frac{m!}{n! \cdot (m-n)!}.$$

Demostración. Si A tiene m elementos, cada subconjunto de n elementos de A puede ser ordenado de $n!$ maneras distintas. Luego,

$$V_m^n = n! \cdot C_m^n = P_n \cdot C_m^n,$$

o sea,

$$C_m^n = \frac{V_m^n}{P_n} = \frac{m!}{n!(m-n)!}.$$

□

Ejemplos.

1. (a) ¿Cuántas comisiones de 5 personas se pueden formar a partir de un grupo de 4 mujeres y 5 hombres?

$$C_9^5 = \frac{9!}{5!(9-5)!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} = 126.$$

   (b) ¿Cuántas de las comisiones anteriores están formadas por 3 mujeres y 2 hombres?

$$C_4^3 \cdot C_5^2 = \frac{4!}{3!(4-3)!} \cdot \frac{5!}{2!(5-2)!} = 4 \cdot \frac{5 \cdot 4}{2} = 40.$$

2. Una encuesta consta de 7 preguntas, de las cuales el encuestado debe contestar 4 y omitir 3, a su elección. ¿De cuántas maneras puede hacer la elección?

$$C_7^4 = \frac{7!}{4!(7-4)!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35.$$

3. El Consejo Departamental de cualquier Departamento Académico de la UNS consta de 12 miembros: 6 profesores, 2 graduados y 4 alumnos. ¿De cuántas maneras se puede formar una comisión de 6 miembros si:

   (a) debe estar integrada por al menos 2 profesores, al menos 1 graduado y al menos 2 alumnos?

   Las posibilidades son:
   2 P, 1 G, 3 A
   2 P, 2 G, 2 A
   3 P, 1 G, 2 A

   Calculando cada número por separado y luego sumando, obtenemos:

$$C_6^2 \cdot C_2^1 \cdot C_4^3 + C_6^2 \cdot C_2^2 \cdot C_4^2 + C_6^3 \cdot C_2^1 \cdot C_4^2.$$

(b) la única condición es que al menos uno de los 6 sea un profesor?
Los diferentes casos son: 1 P, 5 entre G y A
2 P, 4 entre G y A
⋮ ⋮ ⋮ ⋮
Entonces la respuesta es:

$$C_6^1 \cdot C_6^5 + C_6^2 \cdot C_6^4 + \cdots + C_6^5 \cdot C_6^1 + C_6^6.$$

4. ¿De cuántas maneras puede un socio de un Club emitir su voto para elegir una terna de Presidente, Vicepresidente y Secretario, si hay 4 candidatos para Presidente, 3 para Vicepresidente y 5 para Secretario si puede dejar a lo sumo uno de los cargos en blanco?
Los siguientes términos corresponden respectivamente a: ningún cargo en blanco, el cargo de Secretario en blanco, el cargo de Vicepresidente en blanco, el cargo de Presidente en blanco:

$$C_4^1 \cdot C_3^1 \cdot C_5^1 + C_4^1 \cdot C_3^1 + C_4^1 \cdot C_5^1 + C_3^1 \cdot C_5^1.$$

La siguiente propiedad es inmediata:

$$C_m^n = C_m^{m-n}.$$

En efecto, para cada elección de n objetos, queda determinado un conjunto de $m-n$ objetos, los objetos no seleccionados. Luego el número de maneras de elegir n objetos es el mismo que el número de formas de elegir $m-n$ objetos.

Ejercicio. Probar la propiedad anterior usando que $C_m^n = \dfrac{m!}{n! \cdot (m-n)!}$.

Consideremos ahora el siguiente problema: ¿De cuántas maneras es posible sentar n personas a una mesa redonda? (Se considera que dos ordenamientos de personas en una mesa redonda son iguales si cada uno tiene a las mismas personas a la derecha y a la izquierda en ambos ordenamientos).
Teniendo en cuenta que cada posible ordenamiento de esas n personas no cambia si cada una de esas personas se mueve, por ejemplo, un lugar a su derecha, dos lugares a su derecha, etc., podemos fijar una persona en uno de los lugares y ordenar las otras alrededor de la mesa. Entonces se tendrán $(n-1)(n-2)(n-3) \cdot \cdots \cdot 3 \cdot 2 \cdot 1 = (n-1)!$ posibles ordenamientos.

Ejemplos.

1. ¿De cuántas maneras se pueden sentar 5 personas a una mesa redonda? ¿Y si dos personas están enemistadas y no deben ocupar asientos adyacentes?

$$P_4 = 4! = 24\ , \quad P_4 - 2 \cdot P_3 = 12.$$

2. ¿Cuántas pulseras de 14 perlas se pueden fabricar con 14 perlas diferentes?

$$\frac{P_{13}}{2} = \frac{13!}{2}.$$

3. ¿De cuántas maneras se pueden sentar 4 hombres y 4 mujeres alrededor de una mesa redonda, si no debe haber dos hombres juntos?

$$P_3 \cdot P_4.$$

Combinaciones con repetición

Consideremos el siguiente ejemplo: ¿Cuántos grupos de 2 letras se pueden formar con las letras a, b, c, d si se pueden repetir letras?

$$aa,\ ab,\ ac,\ ad,\ bb,\ bc,\ bd,\ cc,\ cd,\ dd.$$

El número de combinaciones con repetición de m objetos tomados de a n se notará C'^{n}_{m}.

La fórmula siguiente reduce el cálculo del número de combinaciones con repetición al caso de conbinaciones sin repetición.

Teorema 9.4

$$C'^{n}_{m} = C^{n}_{m+n-1}.$$

Demostración. Sean $a_1, a_2, \ldots, a_m$ m objetos. Sean $c_1, c_2, \ldots, c_{m+n-1}$ $m+n-1$ objetos distintos. Sea $a_{i_1}a_{i_2}\ldots a_{i_n}$ una combinación con repetición de los m objetos tomados de a n, y supongamos que los índices están ordenados de menor a mayor. A cada combinación con repetición

$$a_{i_1}a_{i_2}\ldots a_{i_n}$$

le vamos a asociar la siguiente combinación (sin repetición) de orden n formada con los elementos c_1, c_2, …, c_{m+n-1}:

$$c_{i_1}c_{i_2+1}c_{i_3+2}\ldots c_{i_n+n-1}.$$

(Sumamos 0, 1, 2, …, $n-1$ a los subíndices i_1, i_2, i_3, …, i_n, respectivamente).
Recíprocamente, cada combinación de los $m+n-1$ objetos c_1, c_2, …, c_{m+n-1} tomados de a n determina una combinación de a_1, a_2, …, a_m restando 0, 1, … , $n-1$ unidades a los subíndices.
Luego

$$C'^{n}_{m} = C^{n}_{m+n-1}.$$

□

Así, por ejemplo, $C'^{2}_{4} = C^{2}_{5} = \dfrac{5!}{2!\cdot 3!} = 10.$

Ejemplo. Un automóvil tiene 8 sistemas básicos. Se efectúa una prueba con 5 automóviles similares para determinar qué sistema falla primero. ¿Cuántos resultados son posibles? (El orden en el que se prueban los automóviles es irrelevante).

$$C'^{5}_{8} = C^{5}_{12} = \frac{12!}{5!\cdot 7!} = 792.$$

Permutaciones con repetición

Supongamos que tenemos 4 anillos marrones, 1 anillo blanco y 1 anillo verde, y queremos saber cuántas ordenaciones distinguibles se pueden hacer con esos 6 anillos.
Con estos 6 anillos se pueden formar 6! ordenaciones, aunque es claro que varias de ellas tendrán la misma apariencia. Así por ejemplo, una ordenación como $MBMMVM$ es una de las 4! ordenaciones indistinguibles que se obtienen al permutar entre sí los 4 anillos marrones. En consecuencia, se debe dividir por 4! el número total de ordenaciones, esto es, el número de permutaciones distinguibles es

$$\frac{6!}{4!} = 30.$$

Este resultado vale en general: dado un conjunto con m elementos, entre los cuales hay k_1 elementos iguales entre sí, k_2 elementos iguales entre sí, ... , k_r elementos iguales entre sí, el número de *permutaciones distinguibles* de esos m elementos es:

$$P_m^{k_1,k_2,\ldots,k_r} = \frac{m!}{k_1! \cdot k_2! \cdot \cdots \cdot k_r!}$$

Ejemplos.

1. ¿De cuántas maneras diferentes es posible escribir las letras de la palabra *Mississippi*? ¿Y las letras de la palabra *Abracadabra*?

$$P_{11}^{4,4,2} = \frac{11!}{4! \cdot 4! \cdot 2!}, \quad P_{11}^{5,2,2} = \frac{11!}{5! \cdot 2! \cdot 2!}.$$

2. ¿En cuántas formas puede un profesor asignar 6 calificaciones A, 5 calificaciones B, 7 C, 3 D y 1 F en un grupo de 22 alumnos?

$$P_{22}^{6,5,7,3}$$

3. ¿De cuántas maneras pueden dividirse 9 mujeres en 3 grupos de 2, 3 y 4 mujeres para habitar los cuartos rojo, verde y azul, respectivamente?

$$P_9^{2,3,4}$$

4. ¿De cuántas maneras puede un equipo de fútbol ganar 7 partidos, perder 2 y empatar otros 2 si van a efectuar 11 partidos?

$$P_{11}^{7,2,2}$$

5. ¿Cuántas señales diferentes se pueden hacer con 6 banderas, utilizando 3 banderas blancas, 2 banderas rojas y 1 bandera azul?

$$P_6^{3,2}$$

6. ¿De cuántas maneras diferentes puede ser escrito a^3b^4 sin utilizar exponentes? Sugerencia: una manera es *aaabbbb*.

$$P_7^{3,4}$$

9.2 El desarrollo binomial

El desarrollo binomial es una fórmula que permite calcular cualquier potencia entera positiva de un binomio. Esta fórmula se conoce con el nombre de *binomio de Newton* (Isaac Newton, 1642 - 1727) aunque ya era conocida por Tartaglia, matemático italiano del siglo XVI.

Antes de indicar el desarrollo de $(a+b)^n$, introducimos los *números combinatorios*:

Los números de la forma $\dfrac{m!}{n!(m-n)!}$, $m, n \in \mathbb{Z}$, $0 \leq n \leq m$, se llaman **números combinatorios**. Se utiliza la siguiente notación:

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}.$$

m se llama el *numerador* y n el *denominador*.

La siguiente importante propiedad de los números combinatorios ya fue probada (recordar que $C_m^n = C_m^{m-n}$):

$$\binom{m}{n} = \binom{m}{m-n}.$$

Otra propiedad útil de estos números es la siguiente:

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}.$$

En efecto,

$$\begin{aligned}
\binom{m-1}{n-1} + \binom{m-1}{n} &= \frac{(m-1)!}{(n-1)!\,[m-1-(n-1)]!} + \frac{(m-1)!}{n!(m-1-n)!} \\
&= \frac{(m-1)!}{(n-1)!(m-n)!} + \frac{(m-1)!}{n!(m-n-1)!} \\
&= \frac{n\cdot(m-1)! + (m-n)\cdot(m-1)!}{n!\cdot(m-n)!} \\
&= \frac{m\cdot(m-1)!}{n!\cdot(m-n)!} \\
&= \frac{m!}{n!\cdot(m-n)!}.
\end{aligned}$$

Veamos ahora el desarrollo binomial.

Si desarrollamos algunas de las primeras potencias de $a+b$, obtenemos

$$\begin{aligned}
(a+b)^1 &= a+b \\
(a+b)^2 &= a^2+2ab+b^2 \\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3 \\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4
\end{aligned}$$

que podemos escribir:

$$\begin{aligned}
(a+b)^1 &= \binom{1}{0}a + \binom{1}{1}b \\
(a+b)^2 &= \binom{2}{0}a^2 + \binom{2}{1}ab + \binom{2}{2}b^2 \\
(a+b)^3 &= \binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3 \\
(a+b)^4 &= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4.
\end{aligned}$$

En general, se tiene:

Teorema 9.5

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.\end{aligned}$$

Demostración. Haremos la demostración por inducción sobre n.
La fórmula es claramente válida para $n = 1$.
Sea $n > 1$ y supongamos que la fórmula vale para $n-1$. Probémosla para n.

$$\begin{aligned}(a+b)^n &= (a+b)\cdot(a+b)^{n-1} = (a+b)\cdot\sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-1-k}b^k \\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=0}^{n-1}\binom{n-1}{k}a^{n-1-k}b^{k+1} \\ &= \binom{n-1}{0}a^n + \sum_{k=1}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=0}^{n-2}\binom{n-1}{k}a^{n-1-k}b^{k+1} + \binom{n-1}{n-1}b^n.\end{aligned}$$

Haciendo $t = k+1$ en la segunda sumatoria, se tiene $k = t-1$ y si $0 \le k \le n-2$, entonces $1 \le t \le n-1$. Entonces esa suma puede escribirse

$$\sum_{t=1}^{n-1}\binom{n-1}{t-1}a^{n-t}b^t,$$

que podemos igualmente notar, cambiando el nombre de la variable,

$$\sum_{k=1}^{n-1}\binom{n-1}{k-1}a^{n-k}b^k.$$

Entonces

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n + \sum_{k=1}^{n-1}\binom{n-1}{k}a^{n-k}b^k + \sum_{k=1}^{n-1}\binom{n-1}{k-1}a^{n-k}b^k + \binom{n}{n}b^n \\ &= \binom{n}{0}a^n + \sum_{k=1}^{n-1}\left[\binom{n-1}{k} + \binom{n-1}{k-1}\right]a^{n-k}b^k + \binom{n}{n}b^n \\ &= \binom{n}{0}a^n + \sum_{k=1}^{n-1}\binom{n}{k}a^{n-k}b^k + \binom{n}{n}b^n \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.\end{aligned}$$

□

El triángulo de Pascal

La disposición triangular de números que se da a continuación recibe el nombre de *triángulo de Pascal* (o de Tartaglia). Cada linea está formada por los coeficientes binomiales del desarrollo de $(a+b)^n$, para $n = 0,\ 1,\ 2,\ \ldots$ Exceptuando los extremos, cada número es la suma de los números que están arriba de él.

$n=0$						1					
$n=1$					1		1				
$n=2$				1		2		1			
$n=3$			1		3		3		1		
$n=4$		1		4		6		4		1	
$n=5$	1		5		10		10		5		1
$n=6$	1	6		15		20		15		6	1
...	...	...	...	...	...	...	...	...	...	...	...

La relación $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ justifica la regla de formación de la tabla anterior.

Ejemplos.

1. Desarrollar $(2a+b)^4$.

$$\begin{aligned}(2a+b)^4 &= \sum_{k=0}^{4}\binom{4}{k}(2a)^{4-k}b^k \\ &= \binom{4}{0}(2a)^4 + \binom{4}{1}(2a)^3 b + \binom{4}{2}(2a)^2 b^2 + \binom{4}{3}2ab^3 + \binom{4}{4}b^4.\end{aligned}$$

   Reemplazando los coeficientes $\binom{4}{k}$ según la linea que corresponde a $n=4$ en el triángulo de Pascal y resolviendo, resulta

$$(2a+b)^4 = 16a^4 + 32a^3b + 24a^2b^2 + 8ab^3 + b^4.$$

2. Hallar los primeros 2 términos del desarrollo de $(2x-5y)^5$ en potencias decrecientes de x.
   Los dos primeros términos del desarrollo de $(2x-5y)^5$ son $\binom{5}{0}(2x)^5$ y $\binom{5}{1}(2x)^4\cdot(-5y)$, esto es, $32x^5$ y $-400x^4y$.

3. Hallar el sexto término del desarrollo de $(\frac{1}{2}x-2y)^8$ en potencias decrecientes de x.
   El sexto término se obtiene para $k=5$ en la expresión

$$\sum_{k=0}^{8}\binom{8}{k}\left(\frac{1}{2}x\right)^{8-k}(-2y)^k.$$

   El sexto término es, entonces,

$$\binom{8}{5}\left(\frac{1}{2}x\right)^3(-2y)^5 = -224x^3y^5.$$

4. **Criterio de divisibilidad por** 11. Un número entero es múltiplo de 11 si la suma algebraica alternada de sus cifras es múltiplo de 11.
   Escribamos

$$a = a_n a_{n-1}\ldots a_1 a_0 = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_1 10 + a_0$$

$$= a_n(11-1)^n + a_{n-1}(11-1)^{n-1} + \ldots + a_1(11-1) + a_0$$

$$= a_n \sum_{k=0}^{n} \binom{n}{k} 11^{n-k} \cdot (-1)^k + a_{n-1} \sum_{k=0}^{n-1} \binom{n-1}{k} 11^{n-1-k} \cdot (-1)^k + \ldots + a_1(11-1) + a_0.$$

Todos los términos de $\sum_{k=0}^{n} \binom{n}{k} 11^{n-k} \cdot (-1)^k$ son múltiplos de 11, excepto el que corresponde a $k = n$, y lo mismo sucede con las otras sumas. Luego, agrupando, podemos escribir

$$a = 11 \cdot t + (-1)^n a_n + (-1)^{n-1} a_{n-1} + \ldots + (-1)a_1 + a_0.$$

Luego $\quad 11 \mid a \;\Leftrightarrow\; 11 \mid a_0 - a_1 + a_2 - \ldots + (-1)^n a_n.$

Así por ejemplo, 35486 en múltiplo de 11, ya que $6 - 8 + 4 - 5 + 3 = 0$, que es múltiplo de 11.

5. **Criterio de divisibilidad por 3.** Un número entero es múltiplo de 3 si la suma de sus cifras es múltiplo de 3.
Escribamos

$$a = a_n a_{n-1} \ldots a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$$

$$= a_n(9+1)^n + a_{n-1}(9+1)^{n-1} + \ldots + a_1(9+1) + a_0$$

$$= a_n \sum_{k=0}^{n} \binom{n}{k} 9^{n-k} \cdot 1^k + a_{n-1} \sum_{k=0}^{n-1} \binom{n-1}{k} 9^{n-1-k} \cdot 1^k + \ldots + a_1(9+1) + a_0.$$

Con el mismo razonamiento del ejemplo anterior, podemos escribir

$$a = 9 \cdot t + a_n + a_{n-1} + \ldots + a_1 + a_0.$$

Luego $\quad 3 \mid a \;\Leftrightarrow\; 3 \mid a_0 + a_1 + a_2 + \ldots + a_n.$

Ejercicios.

1. Probar que $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.
2. Probar que $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$.
3. Probar que el número de subconjuntos de un conjunto con n elementos es 2^n.

9.3 Las permutaciones como transformaciones

Dado un conjunto con n elementos, que, sin pérdida de generalidad, podemos notar $A_n = \{1, 2, \ldots, n\}$, vamos a considerar las $n!$ permutaciones de esos n elementos.

Dar una permutación de esos n elementos equivale a reordenarlos:

$$k_1, k_2, \ldots, k_n,$$

donde cada elemento k_i es uno de los elementos $1, 2, \ldots, n$, y para $i \neq j$, $k_i \neq k_j$. Podemos asociar, entonces, a cada permutación del conjunto A_n, la función $\sigma : A_n \to A_n$ tal que $\sigma(i) = k_i$, que es una función biyectiva que suele representarse en la forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ k_1 & k_2 & k_3 & \ldots & k_n \end{pmatrix}$$

Recíprocamente, toda función biyectiva σ de A_n en A_n, que podemos representar en la forma anterior, define una permutación de A_n.

Ejemplo. Sea $n = 3$. Todas las permutaciones de A_3 las podemos representar por las siguientes biyecciones:

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Pensando a las permutaciones como funciones biyectivas, podemos hablar de la *composición* de permutaciones y de la permutación *inversa* de una permutación.

Así, en el ejemplo anterior, $\alpha \circ \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\delta^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \gamma$.

Definición 9.6 *Llamaremos trasposición a una permutación que intercambia dos números y deja fijos los demás.*

Ejemplos.

1. $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ es una trasposición de A_3.
2. $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$ es una trasposición de A_5.
3. $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ es una trasposición de A_4.

Para indicar una trasposición se adopta una notación más sencilla, que consiste en escribir entre paréntesis sólo los dos números que se intercambian entre sí, ignorando el resto. Así, las tres trasposiciones del ejemplo anterior se escriben:

$$\alpha = (2\ 3), \quad \beta = (3\ 4), \quad \gamma = (1\ 3).$$

Si σ es una trasposición que intercambia los números k_i y k_j, entonces notaremos $\sigma = (k_i\ k_j)$.

Observemos que la inversa de una trasposición σ es la misma trasposición σ, como resulta en forma inmediata de la definición.

Vamos a probar ahora el siguiente importante resultado:

Teorema 9.7 *Toda permutación de A_n, $n \geq 2$, se puede expresar como una composición de trasposiciones.*

Demostración. Vamos a hacer la demostración por inducción sobre n.
Para $n = 2$, la propiedad vale porque en I_2 hay solamente dos permutaciones: $\iota = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ y $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. σ ya es una trasposición, mientras que $\iota = \sigma \circ \sigma$.
Supongamos que el teorema vale para $n = k$, $(k \geq 2)$, esto es, cualquier permutación de k elementos se puede expresar como una composición de trasposiciones.
Probemos que vale para $k+1$. Sea σ una permutación de $k+1$ elementos. Analicemos el tranformado del elemento $k+1$ por medio de σ, es decir, $\sigma(k+1)$. Si $\sigma(k+1) = k+1$, entonces σ deja fijo el elemento $k+1$, y puede, por consiguiente, ser considerada como una permutación de k elementos, que por la hipótesis inductiva, es una composición de trasposiciones. Supongamos ahora que $\sigma(k+1) = j$, con $j \neq k+1$. Consideremos la trasposición τ definida por $\tau = (j \;\; k+1)$. Entonces $(\tau \circ \sigma)(k+1) = \tau(\sigma(k+1)) = k+1$, y por lo tanto $\tau \circ \sigma$ es una permutación de k elementos. Por hipótesis inductiva,

$$\tau \circ \sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$$

donde las τ_i son trasposiciones.
Luego

$$\sigma = \tau^{-1} \circ \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$$

que es una composición de trasposiciones, como queríamos probar. □

Ejemplo.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 1 & 2 \end{pmatrix} = (1\ 5)(2\ 6)(2\ 3) = (1\ 5)(1\ 4)(1\ 4)(2\ 6)(2\ 3).$$

Definición 9.8 *Una permutación σ de A_n se dice un ciclo de longitud r si σ deja fijos $n-r$ elementos de A_n y a los r restantes los permuta de la siguienta forma: $\sigma(k_1) = k_2$, $\sigma(k_2) = k_3$, $\ldots$, $\sigma(k_{r-1}) = k_r$, $\sigma(k_r) = k_1$.*

Notaremos $\sigma = (k_1\ k_2\ k_3\ \ldots k_{r-1}\ k_r)$.

Es claro que toda trasposición es un ciclo de longitud dos.

Ejemplos.

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 3 & 5 & 1 \end{pmatrix}$ es un ciclo de longitud 4, que escribimos $(1\ 4\ 3\ 6)$.

2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 4 & 5 \end{pmatrix}$ es un ciclo de longitud 5, que escribimos $(2\ 3\ 6\ 5\ 4)$.

Dos permutaciones σ y τ de A_n se dicen *disjuntas* si el conjunto de elementos que mueve σ es disjunto del conjunto de elementos que mueve τ.

Si consideramos el ejemplo $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 4 & 6 \end{pmatrix}$, resulta que

$$\sigma = (1\ 5\ 4)(2\ 3),$$

es decir, σ se escribe como una composición de ciclos disjuntos. En particular, el hecho de ser disjuntos hace que se puedan conmutar al hacer la composición, esto es,

$$\sigma = (1\ 5\ 4)(2\ 3) = (2\ 3)(1\ 5\ 4).$$

Este ejemplo ilustra el siguiente resultado:

Toda permutación de A_n, distinta de la permutación identidad, se puede escribir como una composición de ciclos disjuntos de longitud ≥ 2. Esta descomposición es única, salvo por el orden en que se haga la composición.

Permutaciones pares e impares

Dada una permutación σ de A_n,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ k_1 & k_2 & k_3 & \dots & k_n \end{pmatrix}$$

se dice que dos elementos k_i y k_j forman *inversión* si $i < j$ pero $k_i > k_j$.

Por ejemplo, en la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$$

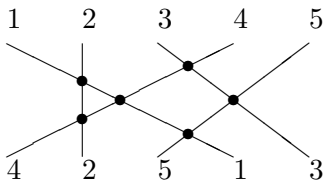
forman inversión 4 y 2, 4 y 1, 4 y 3, 2 y 1, 5 y 1, 5 y 3. Esta permutación presenta 6 inversiones.

El número de inversiones de una permutación se obtiene comparando cada número de la fila de abajo con los que le siguen.

Hay una forma muy simple de contar el número de inversiones de una permutación. Si unimos con un segmento cada número de la primera fila con el mismo número de la segunda, entonces se tiene que dos segmentos correspondientes a dos números distintos se cortan solamente si esos números no están en su orden natural en la segunda fila, es decir esos números forman una inversión. Por lo tanto, para contar el número de inversiones de una permutación, basta contar el número de intersecciones de esos segmentos.

Ejemplo. Hallemos el número de inversiones de la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$$



Hay 6 puntos de intersección. Luego la permutación dada presenta 6 inversiones.

Definición 9.9 *Una permutación se dice de clase par si el número de sus inversiones es par, y se dice de clase impar si el número de sus inversiones es impar.*

El método gráfico dado para determinar el número de inversiones de una permutación, puede utilizarse para probar las siguientes propiedades:

1. Toda trasposición es una permutación impar.

2. La composición de una permutación cualquiera con una trasposición cambia la paridad de la permutación, esto es, si σ es una permutación par y τ es una trasposición, $\sigma \circ \tau$ es impar, y si σ es impar, $\sigma \circ \tau$ es par.

Teorema 9.10 *Dada una permutación σ de A_n, el número de factores de una expresión cualquiera de σ como composición de trasposiciones tiene la misma paridad que el número de inversiones de la permutación dada.*

Demostración. Sea s el número de inversiones de la permutación σ y sea $\sigma = \tau_r \circ \cdots \circ \tau_2 \circ \tau_1$ una expresión de σ como composición de trasposiciones. Podemos pensar que comenzamos con la permutación identidad, y cada vez que se aplica una trasposición τ_i, se intercambian entre sí dos elementos de la segunda fila. Al cabo de este proceso se habrán producido r cambios de clase de esa permutación. Entonces la paridad de r debe coincidir con la de s. □

Ejemplo. Vimos que la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ presenta 6 inversiones, y es, en consecuencia, par. Una expresión de σ como composición de trasposiciones es $\sigma = (1\ 4)(3\ 5)$.

9.4 Ejercicios

1. Calcular: $V_5^3,\ V_7'^2,\ P_6,\ P_7^{2,3},\ C_7^3,\ C_{10}^6$.

2. (a) ¿Cuántos números de 4 cifras pueden escribirse con los dígitos 1, 2, 3, 5, 7, 8 y 9 de modo que no haya cifras repetidas en cada número? Rta.: 840
   ¿Cuántos son múltiplos de 2? Rta.: 240
   ¿En cuántos figuran sólo cifras impares? Rta.: 120
   ¿Cuántos son números menores que 7.000? Rta.: 480
   (b) Resolver el mismo problema si se admiten números con cifras repetidas.
   Rta.: 2.401, 686, 625, 1.372

3. (a) ¿Cuántos números de 4 cifras pueden formarse con los dígitos 1, 2, 3, 4? Rta: 256
   (b) ¿Cuántos números pares de 4 cifras pueden formarse con los dígitos 1, 2, 3, 4? Rta: 128
   (c) ¿Cuántos números de 4 cifras distintas pueden formarse con los dígitos 1, 2, 3, 4? Rta: 24
   (d) ¿Cuántos números de 5 cifras, capicúas, pueden formarse con los dígitos 1, 2, 3, 4, 5, 6, 7, 8? Rta: 512

4. Si en un colectivo hay 10 asientos vacíos, ¿de cuántas formas pueden sentarse 7 personas? Rta: 604.800

5. (a) ¿Cuántas palabras de cuatro letras (no repetidas) se pueden formar con las letras de la palabra GRUPO? Rta: 120
   (b) ¿En cuántas figura la letra G? Rta: 96
   (c) ¿En cuántas palabras las vocales ocupan los dos primeros lugares y las consonantes los dos últimos? Rta: 12
   (d) De las palabras del inciso a), ¿cuántas terminan en R? Rta: 24

6. ¿Cuántos números de cuatro dígitos, múltiplos de 4, se obtienen utilizando los dígitos 1, 2, 3, 4, 5, con y sin repetición de los mismos? Rta.: 125, 24

   Recordemos que un número entero $abcd$ es múltiplo de 4 si y sólo si el entero cd es múltiplo de 4. Si los dígitos no se repiten las posibilidades son:

   _ _ 3 2 , _ _ 1 2 , _ _ 5 2 , _ _ 2 4.

   Se tiene entonces que $N = 4.V_3^2 = 4.3.2 = 24$.

   Si se permiten repeticiones se tienen las siguientes posibilidades :
   _ _ 3 2 _ _ 1 2 , _ _ 5 2 , _ _ 2 4 , _ _ 4 4.

   Por lo tanto $N = 5.V_5'^2 = 5.25 = 125$.

7. ¿De cuántas formas pueden fotografiarse 6 chicas y 7 chicos puestos en hilera de manera tal que nunca aparezcan juntas dos personas del mismo sexo? Rta: 3.628.800
   ¿Y si tenemos 7 chicas y 7 chicos? Rta: 50.803.200

8. (a) ¿Cuántos polinomios de 5º grado se pueden escribir con los dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9? Rta: 900.000
   b) ¿Cuántos del inciso (a) son mónicos y con término independiente primo? Rta: 40.000

c) ¿En cuántos del inciso (a) 0 es raíz simple ?, ¿ y doble? Rta: 81.000; 8.100

9. En una Universidad en la que hay 18 carreras distintas, 5 hermanos decidieron inscribirse de modo que no haya dos anotados en la misma carrera.

   (a) ¿De cuántas maneras pueden hacerlo? Rta.: 1.028.160

   (b) ¿De cuántas, si uno de ellos no quiere estudiar ingeniería civil? Rta.: 971.040

10. ¿De cuántas formas se pueden sentar 8 personas alrededor de una mesa circular? Rta: 5.040

11. ¿ Cuántas pulseras podemos confeccionar con 8 perlas distintas ? Rta: 2.520

12. Sea A un conjunto con 5 elementos y B uno con 9 elementos.
    ¿Cuántas funciones se pueden definir de A en B? Rta.: 59.049
    ¿Cuántas inyectivas? Rta.: 15.120
    En general, ¿cuántas funciones se pueden definir de un conjunto A con n elementos en uno B con m elementos? ¿Cuántas funciones inyectivas, si $n \leq m$? Si $n = m$, ¿cuántas biyecciones hay de A sobre B?

13. ¿Cuántas banderas se pueden hacer con 3 bandas verticales con los colores rojo, blanco, azul y verde?
    La pregunta equivale a determinar el número de aplicaciones de un conjunto de 3 elementos (bandas) en un conjunto de 4 elementos (colores). Se tienen entonces $4^3 = 64$ banderas distintas.

14. ¿Cuántas posiciones hacen falta para hacer (al menos) un millón de llaves diferentes? Las llaves se construyen haciendo incisiones de profundidad variable en distintas posiciones. Supongamos que hay 8 profundidades posibles.
    Sea m el número de posiciones. Queremos que la cantidad de funciones del conjunto $\{1, 2, \ldots, m\}$ en $\{1, 2, \ldots, 8\}$ sea mayor que 10^6. Ahora bien,

    $$2^8 = 256, \text{ luego } 2^8 \cdot 4 > 10^3, \text{ esto es, } 2^{10} > 10^3. \text{ Entonces } 2^{20} > 10^6, \text{ y } 2^{21} = 8^7 > 10^6,$$

    luego hacen falta 7 posiciones.

15. ¿De cuántas maneras es posible alinear 13 signos + y 8 signos − sin que haya dos signos − juntos? Rta.: 3.003

16. ¿Cuántos enteros positivos de 5 cifras hay que utilizan sólo los dígitos 1, 2 y 3, y usan por lo menos una vez cada uno de los dígitos mencionados? Rta: 150

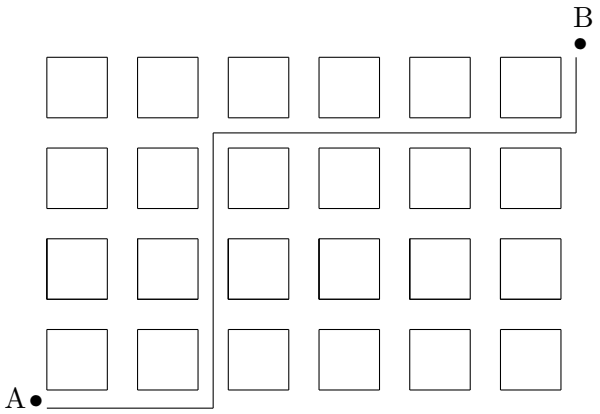
17. ¿De cuántas formas se pueden permutar las letras de la palabra PARALELISMO?, ¿y sin cambiar el orden relativo de las vocales? Rta: 9.979.200; 166.320

18. En un edificio que tiene 8 pisos viajan en el ascensor 5 personas.

    (a) ¿De cuántas maneras diferentes pueden bajarse esas 5 personas? Rta.: 32.768

    (b) ¿De cuántas si no bajan 2 en el mismo piso? Rta.: 6.720

19. ¿Entre cuántas rutas puede optar un alumno para ir a la U.N.S. (ubicada en B) desde su casa (ubicada en A) sabiendo que utiliza caminos de longitud mínima? Rta: 210



20. ¿Cuántas diagonales tiene un triángulo?, ¿cuántas un cuadrado?, ¿y un octógono?. Determinar el número $D(n)$ de las diagonales de un polígono regular de n lados.

    Rta: $D(n) = \dfrac{n\,(n-3)}{2}$

21. Sobre una mesa hay 13 libros distintos: 5 tienen tapas rojas, 5 azules y 3 verdes. ¿De cuántas formas distintas pueden ser colocados en un estante si:

    (a) Se desea que los de un color estén juntos? Rta.: 518.400

    (b) Se desea que los de un color estén juntos, los rojos están numerados por tomos y se respeta la numeración? Rta.: 4320

    Los 5 libros rojos se ubican juntos en un estante de 5! formas, los azules de 5! formas, y los verdes de 3! maneras. Si además consideramos la posición relativa de los colores se tiene que el número buscado es $N = P_3 \,.\, P_5 \,.\, P_5 \,.\, P_3 = 3!\,.\,5!\,.\,5!\,.\,3! = 518.400$.
    Para la solución del inciso (b) basta con no permutar los libros rojos. Obtenemos entonces $N = P_3 \,.\, P_5 \,.\, P_3 = 3!\,.\,5!\,.\,3! = 4.320$.

22. ¿Cuántas palabras de 5 letras no repetidas pueden formarse con las letras F, L, O, R, E, N, C, I y A de modo que aparezcan en ellas 2 vocales y 3 consonantes ? Rta.: 7200

23. ¿Cuántos equipos de fútbol de pueden formar con 18 jugadores? Rta.: $\binom{18}{11}$

24. ¿Cuántos equipos de fútbol se pueden formar con 1 arquero, 4 defensores, 4 mediocampistas y 2 atacantes si hay 3 arqueros, 6 defensores, 5 mediocampistas y 4 atacantes? Rta.: 1350

25. ¿Cuántos paralelogramos hay determinados por 8 restas paralelas y 6 paralelas (no paralelas a las anteriores)? Rta.: 420

26. De un conjunto de 7 payasos, 5 malabaristas y 4 magos:

    (a) ¿De cuántas maneras se puede seleccionar un conjunto de 5 personas de modo que lo integren 2 payasos, 2 malabaristas y un mago? Rta: 840

    (b) ¿De cuántas maneras se puede seleccionar un conjunto de 5 personas si deben integrarlo a lo sumo 3 payasos y por lo menos 2 magos? Rta: 1.596

27. Una mujer tiene 11 amistades.

    (a) ¿De cuántas formas puede invitar a 5 de ellas a comer? Rta: 462

(b) ¿De cuántas maneras si dos de las amistades son marido y mujer, y si asisten lo hacen juntos? Rta: 210

(c) ¿De cuántas maneras si dos de ellas no se hablan y no asistirán juntas? Rta: 378

28. En un plano hay 12 puntos no alineados de a tres, excepto 5 que lo están. Calcular:

(a) El número de rectas que determinan. Rta: 57

(b) El número de triángulos que poseen un lado sobre la recta determinada por los cinco puntos alineados. Rta: 70

(c) El número de triángulos que forman. Rta: 210

29. Una baraja de 40 cartas tiene cuatro palos, en cada uno de los cuales hay 10 cartas numeradas 1, 2, ..., 9, 10. Calcular el número de formas en que se pueden elegir 5 cartas de modo que resulten:

(a) Cinco cartas de un palo. Rta: 1.008

(b) Cinco cartas consecutivas de un palo. Rta: 24

(c) Cinco cartas numeradas consecutivamente. Rta: 6.144

(d) Cuatro cartas de las cinco con los mismos números. Rta: 360

30. Determinar el valor de n para el cual:

(a) $3\binom{n}{4} = 5\binom{n-1}{5}$. Rta: 10

(b) $6\,V_5^2 - V_n^2 = (P_5 - 93)\,n$. Rta: 4

(c) $\binom{5}{n} = \binom{5}{n^2-1}$. Rta: 2

31. Demostrar que:

(a) $\binom{n}{1} + 6\binom{n}{2} + 6\binom{n}{3} = n^3$.

(b) $\binom{n}{k}\binom{n-k}{p-k} = \binom{p}{k}\binom{n}{p}$.

32. Al utilizar la fórmula del binomio :

(i) ¿Qué se deduce si $a = b = 1$?

(ii) Si $b = -a = 1$, ¿qué fórmula se obtiene?

(iii) Probar, usando (i) y (ii) que:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^{n-1}.$$

$$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}.$$

33. Hallar el 5º término del desarrollo en potencias crecientes de x de $(a\,x+5\,y^2)^5$. Rta: $25\,a^4\,x^4\,y^2$

34. Hallar los coeficientes a y b en el desarrollo $(1-4x)^8 = 1 + a\,x + b\,x^2 + \cdots$.

    Rta: $a = -32$; $b = 448$

35. Hallar el coeficiente de x^4 en el desarrollo $\left(x + \dfrac{1}{2\,x}\right)^{10}$. Rta.: 15

    $$\left(x + \frac{1}{2\,x}\right)^{10} = \sum_{k=0}^{10} \binom{10}{k} x^k \left(\frac{1}{2\,x}\right)^{10-k} = \sum_{k=0}^{10} \binom{10}{k} x^{2k-10}\,\frac{1}{2^{10-k}}.$$

    Si $2k - 10 = 4$ entonces $k = 7$, y por lo tanto $\binom{10}{7}\dfrac{1}{2^3} = 15$ es el coeficiente buscado. ¿Cuál es el coeficiente de x^8 en el mismo desarrollo?

36. Hallar el coeficiente de:

    (i) $x^3\,y^6$ en el desarrollo de $(x+y)^9$. Rta: 84

    (ii) x^n en el desarrollo $(x^2 + 2\,x)^n$. Rta: 2^n

37. Hallar el exponente del binomio $\left(\dfrac{3}{x^2} - 2\,x^3\right)^n$, sabiendo que el undécimo término del desarrollo es un polinomio de grado 10. Rta: 20

38. En el desarrollo de $\left(x\sqrt{x} + \dfrac{1}{x^4}\right)^n$ el coeficiente del tercer término es mayor que el coeficiente del segundo término en 44 unidades. Hallar el término que no contiene x. Rta: 165

10 Sistemas de ecuaciones lineales, matrices y determinantes

10.1 Matrices

Una **matriz** $m \times n$ (o de orden $m \times n$) es un cuadro de números con m filas (horizontales) y n columnas (verticales):

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Si $m = n$, A se dice una *matriz cuadrada* de orden n. El número a_{ij} es el elemento de la matriz que está en la fila i y en la columna j.

A veces usaremos la notación $A = (a_{ij})$, $1 \leq i \leq m$, $1 \leq j \leq n$, para designar una matriz de orden $m \times n$.

Si $n = 1$, la matriz tiene una sola columna y se llama *matriz columna*. De la misma manera, si $m = 1$, la matriz tiene una sola fila y se llama *matriz fila*.

Dos matrices $m \times n$, $A = (a_{ij})$ y $B = (b_{ij})$, son *iguales* si $a_{ij} = b_{ij}$ para todos los valores posibles de los subíndices i y j.

Definición 10.1 *La suma de dos matrices A y B de orden $m \times n$ es otra matriz $m \times n$ que se obtiene sumando los elementos correspondientes de A y B. En símbolos, si $A = (a_{ij})$ y $B = (b_{ij})$, entonces $A + B = (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$.*

Ejemplo. Si $A = \begin{pmatrix} -2 & 1 & 4 \\ 2 & -3 & 5 \end{pmatrix}$ y $B = \begin{pmatrix} 6 & 3 & 0 \\ -2 & 0 & -7 \end{pmatrix}$,

entonces $A + B = \begin{pmatrix} -2+6 & 1+3 & 4+0 \\ 2-2 & -3+0 & 5-7 \end{pmatrix} = \begin{pmatrix} 4 & 4 & 4 \\ 0 & -3 & -2 \end{pmatrix}$.

Propiedades

Sean A, B, C matrices $m \times n$. Entonces :

(S_1) $(A + B) + C = A + (B + C)$.

(S_2) $A + B = B + A$.

(S_3) La matriz de orden $m \times n$, $0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$ es tal que $0 + A = A + 0 = A$ para toda matriz de orden $m \times n$ A.

(S_4) Dada $A = (a_{ij})$, la matriz $B = (-a_{ij})$ es tal que $A + B = 0$.

Definición 10.2 *El producto de un número real k y la matriz A es la matriz $k \cdot A$ que se obtiene multiplicando por el número k cada uno de los elementos de A. En símbolos,*

$$k \cdot A = k \cdot (a_{ij}) = (k a_{ij}).$$

En estos casos es costumbre llamar *escalares* a los números reales, y la operación anterior se denomina *multiplicación por un escalar.*

Ejemplo. Si $A = \begin{pmatrix} 0 & 1 & -5 \\ 2 & -3 & 2 \end{pmatrix}$, entonces $3 \cdot A = \begin{pmatrix} 0 & 3 & -15 \\ 6 & -9 & 6 \end{pmatrix}$

Propiedades

Sean A, B matrices de orden $m \times n$ y λ, λ' números complejos. Entonces:

(1) $\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B$.

(2) $(\lambda + \lambda') \cdot A = \lambda \cdot A + \lambda' \cdot A$.

(3) $(\lambda\, \lambda') \cdot A = \lambda \cdot (\lambda' \cdot A)$.

(4) $1 \cdot A = A$.

Definición 10.3 *Sea A una matriz $m \times n$, y sea B una matriz $n \times p$. El producto de A y B es la matriz $A \cdot B$ de orden $m \times p$ definida por:*

$$A \cdot B = (c_{ij}),$$

donde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{t=1}^{n} a_{it}b_{tj}.$$

Es decir, para obtener el elemento c_{ij} de $A \cdot B$ se multiplica cada elemento de la fila i de A por el correspondiente elemento de la columna j de B, y luego se suman esos productos.

Ejemplos.

1. Si $A = \begin{pmatrix} 1 & 4 \\ -3 & 2 \end{pmatrix}$ y $B = \begin{pmatrix} 5 & -1 & 3 \\ 0 & 2 & -2 \end{pmatrix}$ entonces $A \cdot B = \begin{pmatrix} 5 & 7 & -5 \\ -15 & 7 & -13 \end{pmatrix}$.
   Observemos que en este ejemplo no es posible efectuar el producto $B \cdot A$.

2. Si $A = \begin{pmatrix} 3 & -2 \\ 1 & 4 \end{pmatrix}$ y $B = \begin{pmatrix} 5 & 1 \\ -6 & 3 \end{pmatrix}$ entonces
   $A \cdot B = \begin{pmatrix} 27 & -3 \\ -19 & 13 \end{pmatrix}$ y $B \cdot A = \begin{pmatrix} 16 & -6 \\ -15 & 24 \end{pmatrix}$.
   En este ejemplo, ambos productos $A \cdot B$ y $B \cdot A$ pueden efectuarse; sin embargo, $A \cdot B \neq B \cdot A$.

Propiedades Siempre que el producto pueda efectuarse, se verifican

(M_1) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.

(M_2) $A \cdot (B + C) = A \cdot B + A \cdot C$, $\quad (B + C) \cdot A = B \cdot A + C \cdot A$.

(M_3) Se llama matriz identidad de orden n a una matriz $n \times n$ en la que $a_{ii} = 1$ para todo i, $1 \leq i \leq n$, y $a_{ij} = 0$ si $i \neq j$. Se nota I ó I_n.

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$ es tal que $A \cdot I_n = I_n \cdot A = A$, para toda matriz A de orden n.

(M_4) $(\lambda \cdot A) \cdot B = A \cdot (\lambda \cdot B) = \lambda \cdot (A \cdot B)$.

Observación: Sean $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Entonces

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad B \cdot A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} .$$

De lo anterior se deduce que:

1. El producto de matrices no es, en general, conmutativo.
2. El producto puede ser nulo sin que ninguno de los factores lo sea.

Si A es una matriz $m \times n$, la *diagonal principal* de A está formada por los elementos a_{ii}, $1 \leq i \leq min\{m, n\}$.

Se llama *matriz traspuesta* de la matriz A, y se nota A^T, a la matriz que se obtiene al intercambiar las filas y las columnas de A. Es decir, si $A = (a_{ij})$, entonces $A^T = (b_{ij})$, con $b_{ij} = a_{ji}$.

Si A es $m \times n$, entonces A^T es $n \times m$.

Si $A = A^T$, entonces A se dice *simétrica*.

Ejemplo. La matriz traspuesta de la matriz $A = \begin{pmatrix} -1 & 2 & 5 \\ -2 & 3 & -7 \end{pmatrix}$ es la matriz $A^T = \begin{pmatrix} -1 & -2 \\ 2 & 3 \\ 5 & -7 \end{pmatrix}$.

Propiedades

(1) $(A^T)^T = A$.

(2) $(A + B)^T = A^T + B^T$.

(3) $(\lambda \cdot A)^T = \lambda \cdot A^T$; $\lambda \in \mathbb{C}$.

(4) $(A \cdot B)^T = B^T \cdot A^T$, si el producto $A \cdot B$ está definido.

10.2 Matrices y sistemas de ecuaciones

Consideremos un sistema de dos ecuaciones lineales con dos incógnitas:

$$\begin{cases} ax + by = e \\ cx + dy = f \end{cases}$$

(El nombre de lineales, que también se utiliza para mayor número de incógnitas, se debe a que las ecuaciones del tipo $ax + by = e$ se representan en el plano por una recta.)

Un par ordenado de números (x_0, y_0) se llama *solución* del sistema si al reemplazar x por x_0 e y por y_0 se satisfacen ambas ecuaciones. Geométricamente, esto sucede cuando el punto (x_0, y_0) es el punto de intersección de las rectas r_1 y r_2, de ecuación $ax + by = e$ y $cx + dy = f$, respectivamente.

Hay tres posibilidades para el conjunto de soluciones:

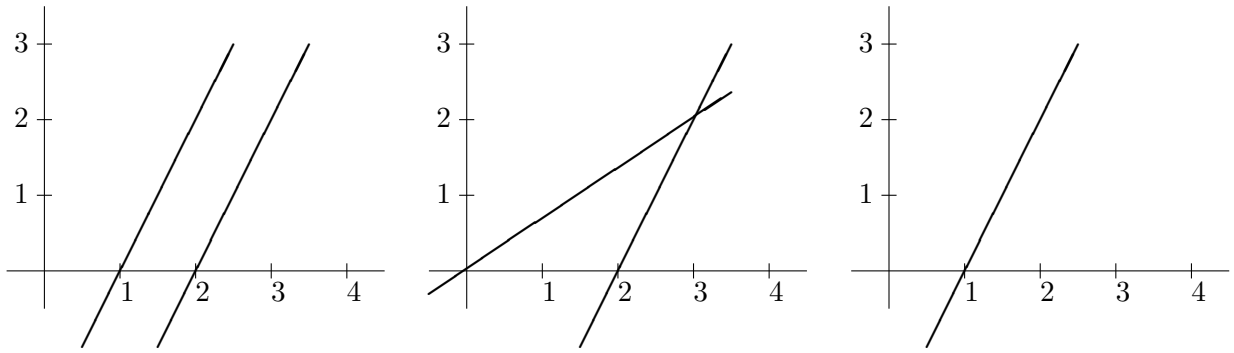
1. Puede ser vacío, es decir, las rectas r_1 y r_2 no se cortan. Decimos entonces que el sistema es *incompatible*.

2. Tiene exactamente un punto. Geométricamente significa que las rectas se cortan. Decimos que el sistema es *compatible determinado.*

3. Contiene infinitos puntos, es decir, r_1 y r_2 son coincidentes. En este caso decimos que el sistema es *compatible indeterminado.*

Ejemplos.

$$\begin{cases} 2x - y = 2 \\ 2x - y = 4 \end{cases} \qquad \begin{cases} 2x - 3y = 0 \\ 2x - y = 4 \end{cases} \qquad \begin{cases} 2x - y = 2 \\ 4x - 2y = 4 \end{cases}$$



Las tres posibilidades anteriores son las únicas, es decir, no puede haber un sistema con exactamente dos soluciones, exactamente tres soluciones, etc. Esto es claro en el caso de dos ecuaciones con dos incógnitas porque dos puntos determinan una recta, pero también es válido para un número mayor de ecuaciones y de incógnitas.

Para resolver un sistema de dos ecuaciones lineales con dos incógnitas se acostumbra usar alguno de estos tres métodos: 1. Sustitución. 2. Igualación. 3. Eliminación.

Ejemplo. Resolver el siguiente sistema de ecuaciones lineales:

$$\begin{cases} 3x - 2y = 50 \\ 2x + 4y = 140 \end{cases}$$

Sustitución. Despejamos una de las incógnitas, por ejemplo y, en una de las ecuaciones y la reemplazamos en la otra.
De la primera ecuación, $y = -25 + \frac{3}{2}x$. Reemplazando en la segunda ecuación, $2x + 4(-25 + \frac{3}{2}x) = 140$.
Resolviendo obtenemos $x = 30$, y sustituyendo este valor en $y = -25 + \frac{3}{2}x$ resulta $y = -25 + 45 = 20$.
Luego la solución es el par ordenado $(30, 20)$.

Igualación. Despejamos una misma incógnita de ambas ecuaciones e igualamos las expresiones obtenidas.
De la primera ecuación, $y = -25 + \frac{3}{2}x$, y de la segunda, $y = 35 - \frac{1}{2}x$. Luego $-25 + \frac{3}{2}x = 35 - \frac{1}{2}x$.
De aquí se obtiene $x = 30$, y entonces $y = 35 - \frac{1}{2} \cdot 30 = 20$.

Eliminación. Se elimina una incógnita, multiplicando cada ecuación por el coeficiente de esa incógnita en la otra ecuación, y luego restando ambas ecuaciones.

En el ejemplo, supongamos que queremos eliminar la incógnita x. Multiplicamos la primera ecuación por 2 y la segunda por 3 y luego restamos:

$$\begin{array}{rcrcr} 6x & - & 4y & = & 100 \\ 6x & + & 12y & = & 420 \\ \hline & & -16y & = & -320 \end{array}$$

Luego $y = 20$. Para determinar x se sustituye $y = 20$ en cualquiera de las ecuaciones, y se resuelve, obteniendo $x = 30$.

Método de eliminación de Gauss

Nos proponemos indicar un método que nos permita resolver sistemas de m ecuaciones lineales con n incógnitas, m y n arbitrarios. Tal sistema puede escribirse:

$$\left\{\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}\right. \qquad (1)$$

donde los números (reales o complejos) a_{ij}, $1 \leq j \leq n$, $1 \leq i \leq m$, son los coeficientes, y los números (reales o complejos) b_1, b_2, ..., b_m son los términos independientes.

Un sistema de n números $k_1, k_2, \ldots, k_n$, es una **solución** del sistema de ecuaciones lineales (1), si cada una de las ecuaciones del mismo se convierte en una identidad después de haber sustituido en ellas las incógnitas x_i por los correspondientes valores k_i, $i = 1, 2, \ldots, n$.

Un sistema de ecuaciones puede no tener solución y entonces se denomina **incompatible**.

Las definiciones de sistema compatible (determinado e indeterminado) e incompatible vistas anteriormente se aplican también al caso general. Si el sistema de ecuaciones lineales tiene solución se denomina **compatible**. Se dice que un sistema compatible es **determinado** si posee solución única, e **indeterminado** si tiene más de una solución.

Nota: Si $b_1 = b_2 = \cdots = b_m = 0$ el sistema (1) se dice **homogéneo** y siempre es compatible, pues $(0, 0, \ldots, 0)$ es solución del mismo.

Un problema de la teoría de los sistemas de ecuaciones lineales consiste en la elaboración de métodos que permitan establecer si un sistema dado es compatible o no, y en caso de ser compatible, indicar el número de soluciones y señalar un método para hallarlas a todas.

Si se aplica a un sistema de ecuaciones lineales alguna de las tres operaciones que se indican a continuación, se obtiene un nuevo sistema *equivalente* al dado, en el sentido que ambos sistemas tienen las mismas soluciones:

(I) Intercambiar dos ecuaciones entre sí.

(II) Reemplazar una ecuación por la que se obtiene multiplicándola por una constante distinta de cero.

(III) Reemplazar una ecuación por la que se obtiene sumando a dicha ecuación otra ecuación multiplicada por una constante.

En el sistema (1) podemos suponer sin pérdida de generalidad que $a_{11} \neq 0$.

Por ejemplo, dado el sistema

$$\left\{\begin{array}{rcrcrcl} 2x & + & 3y & - & z & = & 1 \\ x & + & 4y & - & z & = & 4 \\ 3x & + & y & + & 2z & = & 5 \end{array}\right. ,$$

si intercambiamos la primera y segunda ecuación, obtenemos el siguiente sistema equivalente:

$$\left\{\begin{array}{rcrcrcl} x & + & 4y & - & z & = & 4 \\ 2x & + & 3y & - & z & = & 1 \\ 3x & + & y & + & 2z & = & 5 \end{array}\right. .$$

Si ahora reemplazamos:

- la segunda ecuación por la suma de la segunda y la primera multiplicada por (-2), y
- la tercera ecuación por la suma de la tercera mas la primera multiplicada por (-3),

obtenemos el siguiente sistema equivalente:

$$\left\{\begin{array}{rcrcrcr} x & + & 4y & - & z & = & 4 \\ & & -5y & + & z & = & -7 \\ & & -11y & + & 5z & = & -7 \end{array}\right. .$$

Multiplicando ahora la segunda ecuación por $-\dfrac{1}{5}$:

$$\left\{\begin{array}{rcrcrcr} x & + & 4y & - & z & = & 4 \\ & & y & - & \frac{1}{5}z & = & \frac{7}{5} \\ & & -11y & + & 5z & = & -7 \end{array}\right. .$$

Reemplazando la tercera ecuación por la suma de la tercera y 11 veces la segunda:

$$\left\{\begin{array}{rcrcrcr} x & + & 4y & - & z & = & 4 \\ & & y & - & \frac{1}{5}z & = & \frac{7}{5} \\ & & & & \frac{14}{5}z & = & \frac{42}{5} \end{array}\right. .$$

Este último sistema es equivalente al primero y puede resolverse en forma muy sencilla. El resultado es $z = 3$, $y = 2$ y $x = -1$; esto es, la solución es el conjunto $S = \{(-1, 2, 3)\}$.

La matriz cuyos elementos son los coeficientes de un sistema de ecuaciones lineales dado, se llama *matriz de los coeficientes*. Se llama *matriz del sistema* a la matriz

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix} .$$

Podemos aplicar a las filas de la matriz del sistema las mismas operaciones que se aplicaron a las ecuaciones. Aplicadas a la matriz reciben el nombre de *operaciones elementales*.

Traducidas en términos de la matriz del sistema, estas operaciones son:

1. Intercambiar dos filas de la matriz.
2. Reemplazar una fila por la que se obtiene al multiplicarla por un número distinto de cero.
3. Reemplazar una fila por la que se obtiene al sumarle a esa fila otra fila previamente multiplicada por un número.

Estas operaciones elementales transforman la matriz del sistema en otra matriz que corresponde a un sistema de ecuaciones equivalente al dado.

La aplicación de las operaciones elementales tiene por objetivo obtener una matriz que tenga:

- Ceros debajo de la diagonal principal.
- Unos en la diagonal principal (eventualmente puede aparecer algún cero).

Este procedimiento se llama el *método de eliminación de Gauss* (Karl Friedrich Gauss, 1777–1855).

Ejemplo. Resolver el siguiente sistema de ecuaciones lineales:

$$\left\{\begin{array}{rcrcrcr} x & + & y & + & z & = & 2 \\ 2x & + & 5y & + & 3z & = & 1 \\ 3x & - & y & - & 2z & = & -1 \end{array}\right.$$

Comenzamos considerando la matriz del sistema. Las operaciones elementales que se efectúan se indican usando F_i para indicar la fila i.

$$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 2 & 5 & 3 & 1 \\ 3 & -1 & -2 & -1 \end{pmatrix} \xrightarrow{F_2-2F_1\,:\,F_2;\ F_3-3F_1\,:\,F_3} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 3 & 1 & -3 \\ 0 & -4 & -5 & -7 \end{pmatrix} \xrightarrow{(1/3)F_2\,:\,F_2}$$

$$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 1 & 1/3 & -1 \\ 0 & -4 & -5 & -7 \end{pmatrix} \xrightarrow{F_3+4F_2\,:\,F_3} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 1 & 1/3 & -1 \\ 0 & 0 & -11/3 & -11 \end{pmatrix} \xrightarrow{-(3/11)F_3\,:\,F_3} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 1 & 1/3 & -1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

Esta última matriz representa el sistema

$$\left\{\begin{array}{rcrcrcr} x & + & y & + & z & = & 2 \\ & & y & + & (1/3)z & = & -1 \\ & & & & z & = & 3 \end{array}\right.$$

cuya solución es $(1, -2, 3)$

Si durante la aplicación del método de eliminación de Gauss alguna de las matrices intermedias tiene una fila con todos los elementos nulos excepto el último, es decir, una fila de la forma

$$0 \quad 0 \quad \cdots \quad 0 \quad b, \quad \text{con} \quad b \neq 0,$$

entonces el sistema es *incompatible*, ya que esa fila corresponde a una ecuación

$$0x_1 + 0x_2 + \cdots + 0x_n = b$$

que no tiene solución.

Si alguna de las matrices tiene una fila con todos los elementos nulos (incluyendo el último), esa fila simplemente se elimina.

Si en la última matriz el número de filas r es igual al número de incógnitas n, entonces el sistema es *compatible determinado*. Si $r < n$, hay $n - r$ incógnitas a las cuales se les puede dar valores arbitrarios y calcular en función de ellos los valores de las otras incógnitas. En ese caso el sistema es *compatible indeterminado*.

Ejemplos.

1. Resolver

$$\left\{\begin{array}{rcrcrcr} x & - & 2y & + & 3z & = & 10 \\ 2x & - & 3y & - & z & = & 8 \\ 5x & - & 9y & + & 8z & = & 20 \end{array}\right.$$

$$\left(\begin{array}{rrrr} 1 & -2 & 3 & 10 \\ 2 & -3 & -1 & 8 \\ 5 & -9 & 8 & 20 \end{array}\right) \longrightarrow \left(\begin{array}{rrrr} 1 & -2 & 3 & 10 \\ 0 & 1 & -7 & -12 \\ 0 & 1 & -7 & -30 \end{array}\right) \longrightarrow \left(\begin{array}{rrrr} 1 & -2 & 3 & 10 \\ 0 & 1 & -7 & -12 \\ 0 & 0 & 0 & -18 \end{array}\right)$$

El sistema es incompatible.

2. Resolver

$$\left\{\begin{array}{rcrcrcr} x & - & 2y & + & 3z & = & 10 \\ 2x & - & 3y & - & z & = & 8 \\ 4x & - & 7y & + & 5z & = & 28 \end{array}\right.$$

$$\left(\begin{array}{rrrr} 1 & -2 & 3 & 10 \\ 2 & -3 & -1 & 8 \\ 4 & -7 & 5 & 28 \end{array}\right) \longrightarrow \left(\begin{array}{rrrr} 1 & -2 & 3 & 10 \\ 0 & 1 & -7 & -12 \\ 0 & 1 & -7 & -12 \end{array}\right) \longrightarrow \left(\begin{array}{rrrr} 1 & -2 & 3 & 10 \\ 0 & 1 & -7 & -12 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

El sistema asociado es

$$\left\{\begin{array}{rcrcrcr} x & - & 2y & + & 3z & = & 10 \\ & & y & - & 7z & = & -12 \end{array}\right.$$

Resolviendo la segunda ecuación y reemplazando en la primera se obtiene $x = 11z - 14$, $y = 7z - 12$, z arbitrario. El sistema es *compatible indeterminado* y el conjunto de soluciones es

$$S = \{(11k - 14,\ 7k - 12,\ k),\ \text{con } k \in \mathbb{R}\}.$$

3. Resolver

$$\left\{\begin{array}{rcrcrcrcr} x & + & 3y & + & z & & & = & 1 \\ 2x & + & 7y & + & z & - & u & = & -1 \\ 3x & - & 2y & & & + & 4u & = & 8 \\ -x & + & y & - & 3z & - & u & = & -6 \end{array}\right.$$

$$\left(\begin{array}{rrrrr} 1 & 3 & 1 & 0 & 1 \\ 2 & 7 & 1 & -1 & -1 \\ 3 & -2 & 0 & 4 & 8 \\ -1 & 1 & -3 & -1 & -6 \end{array}\right) \longrightarrow \left(\begin{array}{rrrrr} 1 & 3 & 1 & 0 & 1 \\ 0 & 1 & -1 & -1 & -3 \\ 0 & -11 & -3 & 4 & 5 \\ 0 & 4 & -2 & -1 & -5 \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{rrrrr} 1 & 3 & 1 & 0 & 1 \\ 0 & 1 & -1 & -1 & -3 \\ 0 & 0 & -14 & -7 & -28 \\ 0 & 0 & 2 & 3 & 7 \end{array}\right) \longrightarrow \left(\begin{array}{rrrrr} 1 & 3 & 1 & 0 & 1 \\ 0 & 1 & -1 & -1 & -3 \\ 0 & 0 & 1 & \frac{1}{2} & 2 \\ 0 & 0 & 2 & 3 & 7 \end{array}\right) \longrightarrow \left(\begin{array}{rrrrr} 1 & 3 & 1 & 0 & 1 \\ 0 & 1 & -1 & -1 & -3 \\ 0 & 0 & 1 & \frac{1}{2} & 2 \\ 0 & 0 & 0 & 2 & 3 \end{array}\right)$$

El sistema asociado es

$$\begin{cases} x + 3y + z = 1 \\ y - z - u = -3 \\ z + \frac{1}{2}u = 2 \\ 2u = 3 \end{cases}$$

Entonces, $u = \frac{3}{2}$, $z = \frac{5}{4}$, $y = -\frac{1}{4}$ y $x = \frac{1}{2}$.

El sistema es *compatible determinado*, con única solución $\left(\frac{1}{2}, -\frac{1}{4}, \frac{5}{4}, \frac{3}{2}\right)$.

10.3 Determinantes

Determinantes de segundo y tercer orden

Dada una matriz cuadrada de 2×2, $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, el valor de su determinante se define como

$$\det A = |A| = a_{11}a_{22} - a_{12}a_{21}.$$

Ejemplo. Si $A = \begin{pmatrix} 3 & 2 \\ -1 & 2 \end{pmatrix}$, entonces $|A| = 3 \cdot 2 - (-1) \cdot 2 = 8$.

Consideremos ahora una matriz cuadrada de tercer orden

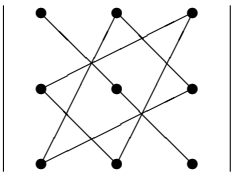
$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Entonces el determinante de A se define como

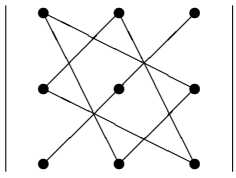
$$\det A = |A| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

donde cada término consta de un producto de tres factores, uno de cada fila y uno de cada columna. Si a cada término le asociamos la permutación σ de $\{1, 2, 3\}$ determinada por los subíndices (por ejemplo, al término $a_{11}a_{23}a_{32}$ le asociamos $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ entonces se asigna a ese término el signo $(-1)^s$, donde s es el número de inversiones de la permutación σ.

Para obtener rápidamente el valor de $\det A$, puede aplicarse la siguiente regla práctica, llamada regla de Sarrus:



Signo +



Signo −

Ejemplo.

$$\begin{vmatrix} 2 & -4 & -5 \\ 1 & 0 & 4 \\ 2 & 3 & -6 \end{vmatrix} = 2 \cdot 0 \cdot (-6) + (-4) \cdot 4 \cdot 2 + 1 \cdot 3 \cdot (-5) - ((-5) \cdot 0 \cdot 2 + (-4) \cdot 1 \cdot (-6) + 4 \cdot 3 \cdot 2) = -95.$$

Determinantes de orden n

Sea dada una matriz cuadrada de orden n,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Consideremos todos los productos posibles de n elementos de esta matriz de modo que en cada producto haya un factor de cada fila y uno de cada columna, o sea, productos de la forma

$$a_{1\alpha_1} a_{2\alpha_2} \cdots a_{n\alpha_n}$$

donde los subíndices α_1, α_2, ..., α_n forman una permutación de los números 1, 2 , ..., n. Hay $n!$ productos de esta forma.

A cada producto de este tipo se le adjunta un signo + ó un signo − según que la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

sea de clase par o impar, respectivamente, esto es, se considera el número

$$(-1)^s a_{1\alpha_1} a_{2\alpha_2} \cdots a_{n\alpha_n},$$

donde s es el número de inversiones de σ.

Definición 10.4 *Se llama determinante de la matriz cuadrada A a la suma de los $n!$ productos de la forma $(-1)^s a_{1\alpha_1} a_{2\alpha_2} \cdots a_{n\alpha_n}$. Se nota* det A *ó* $|A|$.

$$\det A = |A| = \sum (-1)^s a_{1\alpha_1} a_{2\alpha_2} \cdots a_{n\alpha_n}.$$

det A *se dice un determinante de orden n.*

Ejemplo. Calcular

$$\begin{vmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & -1 & 1 \\ 3 & -1 & 0 & 2 \end{vmatrix}$$

Los productos que no se anulan son: $a_{11} \cdot a_{23} \cdot a_{32} \cdot a_{44}$ y $a_{11} \cdot a_{23} \cdot a_{34} \cdot a_{42}$, además el número de inversiones de 1324 es 1 y el número de inversiones de 1342 es 2, luego,

$$\det A = (-1)^1 \cdot a_{11} \cdot a_{23} \cdot a_{32} \cdot a_{44} + (-1)^2 \cdot a_{11} \cdot a_{23} \cdot a_{34} \cdot a_{42} = -(-1) \cdot 1 \cdot 1 \cdot 2 + (-1) \cdot 1 \cdot 1 \cdot (-1) = 2 + 1 = 3.$$

Para $n = 2$, si $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $\det A = (-1)^0 \cdot a_{11} \cdot a_{22} + (-1)^1 \cdot a_{12} \cdot a_{21} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$.

Para $n = 3$, si $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, $\det A = (-1)^0 \cdot a_{11} \cdot a_{22} \cdot a_{33} + (-1)^1 \cdot a_{11} \cdot a_{23} \cdot a_{32} +$

$+(-1)^2 \cdot a_{12} \cdot a_{23} \cdot a_{31} + (-1)^1 \cdot a_{12} \cdot a_{21} \cdot a_{33} + (-1)^2 \cdot a_{13} \cdot a_{21} \cdot a_{32} + (-1)^3 \cdot a_{13} \cdot a_{22} \cdot a_{31} = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33} - a_{13} \cdot a_{22} \cdot a_{31}$, resultado que puede obtenerse aplicando la regla de Sarrus para el cálculo de determinantes de orden 3.

Es fácil convencerse de que la definición de determinante es completamente ineficiente para calcular determinantes de orden n, incluso para valores de n no muy grandes, por lo que es necesario establecer algunas propiedades de los determinantes que faciliten su cálculo.

El caso más simple de cálculo de un determinante es el caso del determinante de una matriz *triangular* ($A = (a_{ij})$ es triangular superior si $a_{ij} = 0$ cuando $i > j$; es triangular inferior si $a_{ij} = 0$ cuando $i < j$ y triangular, si es triangular superior o triangular inferior):

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

Todos los términos del determinante se anulan excepto el formado por el producto de los elementos de la diagonal principal, luego

$$\det A = a_{11}a_{22}\cdots a_{nn}.$$

Vamos a ver ahora algunas propiedades elementales de los determinantes que serán de utilidad para hallar métodos para calcularlos.

Propiedad 10.5 *El determinante de una matriz coincide con el determinante de su traspuesta. Es decir,* $\det A = \det A^T$.

Demostración. Los términos de $\det A$ son de la forma

$$(-1)^s a_{1\alpha_1}a_{2\alpha_2}\cdots a_{n\alpha_n}$$

donde s es el número de inversiones de la permutación $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$.
Pero $A^T = (b_{ij})$, donde $b_{ij} = a_{ji}$. Entonces $a_{1\alpha_1}a_{2\alpha_2}\cdots a_{n\alpha_n} = b_{\alpha_1 1}b_{\alpha_2 2}\cdots b_{\alpha_n n}$, y como la permutación asociada al término $b_{\alpha_1 1}b_{\alpha_2 2}\cdots b_{\alpha_n n}$ es σ^{-1}, que tiene la misma paridad que σ, entonces el signo que le corresponde a $b_{\alpha_1 1}b_{\alpha_2 2}\cdots b_{\alpha_n n}$ es $(-1)^s$, es decir

$$(-1)^s a_{1\alpha_1}a_{2\alpha_2}\cdots a_{n\alpha_n} = (-1)^s b_{\alpha_1 1}b_{\alpha_2 2}\cdots b_{\alpha_n n}$$

es también un término de $\det A^T$. De la misma manera, todo término de $\det A^T$ es un término de $\det A$.
Luego $\det A = \det A^T$. □

De la Propiedad 1 se deduce que a toda propiedad de un determinante relativa a las columnas le corresponde una análoga para las filas, y recíprocamente, puesto que las columnas (filas) de una matriz son las filas (columnas) de la matriz traspuesta. En lo que sigue indicaremos las propiedades de los determinantes únicamente para las columnas pero sabemos, por lo anterior, que para las filas valen propiedades análogas.

Propiedad 10.6 *Si una de las columnas de la matriz A está constituida por ceros, entonces* $\det A = 0$.

Demostración. Supongamos que la columna i-ésima está formada por ceros. Todos los términos del determinante contienen un factor de la columna i-ésima. Luego todos los términos del determinante son cero, y por lo tanto, $\det A = 0$. □

Propiedad 10.7 *Si A' es la matriz que se obtiene de la matriz A intercambiando dos columnas, entonces* $\det A' = -\det A$.

Demostración. Supongamos que $a_{1\alpha_1}a_{2\alpha_2}\cdots a_{n\alpha_n}$ figura en un término de $\det A$. La permutación asociada es $\sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_i & \cdots & \alpha_j & \cdots & \alpha_n \end{pmatrix}$. Entonces ese mismo producto figura también en un término de $\det A'$, pero con permutación asociada $\sigma' = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_j & \cdots & \alpha_i & \cdots & \alpha_n \end{pmatrix}$, que tiene paridad contraria que σ. Luego todos los términos de $\det A'$ coinciden con los términos de $\det A$, pero con signos contrarios, es decir, $\det A' = -\det A$. □

Propiedad 10.8 *Si A es una matriz con dos columnas iguales, entonces* $\det A = 0$.

Demostración. En efecto, intercambiando las dos columnas iguales, por un lado $\det A$ no varía, y por otro lado cambia de signo. Luego $\det A = -\det A$. De donde $\det A = 0$. □

Propiedad 10.9 *Si A' es la matriz que se obtiene multiplicando todos los elementos de una columna de la matriz A por un número k, entonces* $\det A' = k \cdot \det A$.

Demostración. Supongamos que se ha multiplicado por k la columna i-ésima. Como cada término del determinante contiene exactamente un elemento de la columna i-ésima, entonces todo término ha sido nultiplicado por k, esto es $\det A$ queda multiplicado por k. □

Ejemplo.

$$\begin{vmatrix} 1/2 & 0 & -1 \\ 3/2 & 1 & -2 \\ 1/2 & 1 & -1 \end{vmatrix} = \frac{1}{2} \cdot \begin{vmatrix} 1 & 0 & -1 \\ 3 & 1 & -2 \\ 1 & 1 & -1 \end{vmatrix}.$$

Propiedad 10.10 *Si A es una matriz que tiene dos columnas proporcionales, entonces* $\det A = 0$.

Demostración. Supongamos que la columna j-ésima es k veces la columna i-ésima. Sacando afuera del determinante ese factor k (propiedad anterior) queda un determinante de una matriz con dos columnas iguales, que es cero. □

Propiedad 10.11 *Si $A = (a_{ij})$ y la columna r-ésima se puede expresar $a_{ir} = b_{ir} + c_{ir}$, $1 \le i \le n$, entonces* $\det A = \det B + \det C$ *donde B y C coinciden con A salvo en la columna r-ésima, en la que B tiene los elementos b_{ir} y C tiene los elementos c_{ir}, $1 \le i \le n$.*

Ejemplo.

$$\begin{vmatrix} a_{11} & b_{12}+c_{12} & a_{13} \\ a_{21} & b_{22}+c_{22} & a_{23} \\ a_{31} & b_{32}+c_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & b_{12} & a_{13} \\ a_{21} & b_{22} & a_{23} \\ a_{31} & b_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & c_{12} & a_{13} \\ a_{21} & c_{22} & a_{23} \\ a_{31} & c_{32} & a_{33} \end{vmatrix}.$$

Demostración. En cada producto $a_{1\alpha_1}a_{2\alpha_2}\cdots a_{n\alpha_n}$ de det A, algún $\alpha_i = r$. Luego

$$a_{1\alpha_1}a_{2\alpha_2}\cdots a_{i\alpha_i}\cdots a_{n\alpha_n} = a_{1\alpha_1}a_{2\alpha_2}\cdots(b_{ir}+c_{ir})\cdots a_{n\alpha_n} = a_{1\alpha_1}a_{2\alpha_2}\cdots b_{ir}\cdots a_{n\alpha_n}+a_{1\alpha_1}a_{2\alpha_2}\cdots c_{ir}\cdots a_{n\alpha_n}.$$

Como a cada nuevo término le corresponde el mismo signo que a $a_{1\alpha_1}a_{2\alpha_2}\cdots a_{n\alpha_n}$, agrupando se tiene la descomposición det $A = \det B + \det C$. □

Sea A una matriz de orden n, si indicamos con $C_1, C_2, \ldots, C_n$ las columnas de A, diremos que la columna C_i es combinación lineal de las columnas C_j y C_k, con $1 \leq j, k \leq n$, si existen números α, β tales que $C_i = \alpha \cdot C_j + \beta \cdot C_k$.

Ejemplo

(a) En $\begin{pmatrix} 1 & 5 & 7 \\ -2 & 1 & -3 \\ 3 & 0 & 6 \end{pmatrix}$, $C_3 = 2 \cdot C_1 + C_2$. (b) En $\begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}$, $C_2 = 0 \cdot C_1$.

(c) En $\begin{pmatrix} 1 & 0 & -2 & 3 \\ 2 & 1 & -4 & -1 \end{pmatrix}$, $C_3 = -2 \cdot C_1$.

Propiedad 10.12 *Si en una matriz A una columna es combinación lineal de otras, entonces* det $A = 0$.

Demostración. Supongamos, por ejemplo, que la columna j-ésima es combinación lineal de las columnas j_1, j_2, ..., j_s. Entonces todo elemento de la columna j es una suma de s términos. Por la propiedad anterior, det A es una suma de s determinantes, en cada uno de los cuales la j-ésima columna es proporcional a una de las otras columnas. Por la propiedad 6, resulta que cada uno de esos determinantes es cero. Luego det $A = 0$. □

Propiedad 10.13 *Si A' es la matriz que se obtiene al sumar a una columna de una matriz A una combinación lineal de otras columnas de A, entonces* det $A' =$ det A.

Ejemplo.

Si $A = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & -2 \\ 3 & 1 & -3 \end{pmatrix}$, reemplazando C_3 por $2 \cdot C_1 + C_3$ se obtiene $A' = \begin{pmatrix} 2 & 0 & 3 \\ 0 & 1 & -2 \\ 3 & 1 & 3 \end{pmatrix}$.

Entonces det $A =$ det A'.

Demostración. Supongamos que a la columna j-ésima se le suma una combinación lineal de las columnas j_1, j_2, ..., j_s. Entonces todo elemento de esa columna es de la forma

$$c_j + \sum_{i=1}^{s} k_i c_{j_i}.$$

Entonces por la propiedad 7, det A es suma de $s+1$ determinantes, el primero de los cuales coincide con det A, y los otros son cero porque cada uno contiene dos columnas proporcionales. □

Cálculo de determinantes

De las propiedades anteriores resulta que si se pasa de una matriz A a otra matriz por medio de una operación elemental, entonces

(I) El determinante cambia de signo si se intercambian dos columnas (filas).

(II) El determinante queda multiplicado por un escalar no nulo si se reemplaza una columna (fila) por un múltiplo no nulo de esa columna (fila).

(III) El determinante no varía si a una columna (fila) se le suma un múltiplo de otra.

Por consiguiente, un método para calcular el determinante de una matriz A consiste en transformar A en una matriz A' triangular, cuyo determinante es de cálculo inmediato. Según lo anterior, det A y det A' diferirán a lo sumo en un escalar.

Ejemplo

$$\begin{vmatrix} 0 & 3 & 2 \\ 1 & -6 & 6 \\ 5 & 9 & 1 \end{vmatrix} = \quad C_1 \leftrightarrow C_2 \quad - \begin{vmatrix} 3 & 0 & 2 \\ -6 & 1 & 6 \\ 9 & 5 & 1 \end{vmatrix} = \quad \tfrac{1}{3}.C_1 \to C_1$$

$$= -3. \begin{vmatrix} 1 & 0 & 2 \\ -2 & 1 & 6 \\ 3 & 5 & 1 \end{vmatrix} = \quad -2.C_1 + C_3 \to C_3 \quad -3. \begin{vmatrix} 1 & 0 & 0 \\ -2 & 1 & 10 \\ 3 & 5 & -5 \end{vmatrix} = \quad -10.C_2 + C_3 \to C_3$$

$$= -3. \begin{vmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 3 & 5 & -55 \end{vmatrix} = \quad (-3) \cdot (-55) = 165$$

Desarrollo de un determinante por los elementos de una línea (fila o columna).

Dada una matriz $A = (a_{ij})$ se llama **menor complementario** del elemento a_{ij} y se nota M_{ij} al determinante de la matriz que se obtiene a partir de A suprimiendo la i-ésima fila y la j-ésima columna.
Se llama **complemento algebraico o cofactor** del elemento a_{ij} de A al número $(-1)^{i+j} \cdot M_{ij}$.

Lema 10.14 *Sea a_{ij} un elemento cualquiera de una matriz cuadrada A. Si en $D = \det A$ agrupamos todos los términos que contienen a a_{ij} y escribimos $D = a_{ij} \cdot A_{ij} + (\text{términos que no contienen a } a_{ij})$, entonces A_{ij} es el complemento algebraico del elemento a_{ij}, esto es $A_{ij} = (-1)^{i+j} \cdot M_{ij}$.*

Demostración. Probemos primero el lema para el elemento a_{11}. Cada término donde figura el elemento a_{11} tiene la forma

$$(-1)^s \cdot a_{11} a_{2\alpha_2} \cdots a_{n\alpha_n},$$

donde s es el número de inversiones de la permutación de orden n $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$.
Pero es claro que la permutación σ y la permutación de orden $n-1$ $\sigma' = \begin{pmatrix} 2 & 3 & \cdots & n \\ \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix}$ tienen el mismo número de inversiones, luego el producto

$$(-1)^s \cdot a_{2\alpha_2} \cdots a_{n\alpha_n}$$

es un término del determinante M_{11}.
Recíprocamente, si a cada término del determinante M_{11} lo multiplicamos por a_{11} obtenemos un término de det A. Luego det $A = a_{11}M_{11} + (\text{términos que no contienen a } a_{11})$.
Consideremos ahora un elemento a_{ij} arbitrario. Hagamos $i-1$ intercambios de filas y $j-1$ intercambios

de columnas para llevar el elemento a_{ij} al lugar $(1,1)$. Si D' es el nuevo determinante así obtenido, entonces

$$\det A = (-1)^{(i-1)+(j-1)} \cdot D' = (-1)^{i+j} \cdot D' = (-1)^{i+j}[a_{ij}M_{ij} + (\text{términos que no contienen a } a_{ij})]$$

$$= a_{ij} \cdot (-1)^{i+j} \cdot M_{ij} + \cdots = a_{ij} \cdot A_{ij} + \cdots$$

donde $A_{ij} = (-1)^{i+j}M_{ij}$, es decir, A_{ij} es el complemento algebraico de a_{ij}. □

Teorema 10.15 *El determinante de una matriz $A = (a_{ij})$ es igual a la suma de los elementos de una línea (fila o columna) multiplicados cada uno de ellos por sus respectivos complementos algebraicos.*

Así, $\det A = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + \cdots + a_{in} \cdot A_{in}$ es el desarrollo de $\det A$ por los elementos de la i-ésima fila y $\det A = a_{1j} \cdot A_{1j} + a_{2j} \cdot A_{2j} + \cdots + a_{nj} \cdot A_{nj}$ es el desarrollo de $\det A$ por los elementos de la j-ésima columna.

Demostración. Una vez elegida una fila, por ejemplo, la fila i, podemos agrupar los términos de $\det A$ que contienen a a_{i1}, los términos de $\det A$ que contienen a a_{i2}, etc. Por el Lema anterior se tiene que

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}.$$

El mismo razonamiento si se elige una columna j. □

Corolario 10.16 *Si $A = (a_{ij})$, la suma de los elementos de una fila (columna) multiplicados cada uno de ellos por los complementos algebraicos de los elementos correspondientes de otra fila (columna) distinta es cero.*

Es decir, $a_{s1} \cdot A_{t1} + a_{s2} \cdot A_{t2} + \cdots + a_{sn} \cdot A_{tn} = 0$ y $a_{1s} \cdot A_{1t} + a_{2s} \cdot A_{2t} + \cdots + a_{ns} \cdot A_{nt} = 0$, si $s \neq t$.

Demostración. En efecto, $a_{s1} \cdot A_{t1} + a_{s2} \cdot A_{t2} + \cdots + a_{sn} \cdot A_{tn}$ es el desarrollo del determinante de la matriz que se obtiene reemplazando en A la fila t por la fila s. Esta matriz tiene dos filas iguales, y por consiguiente, su determinante es cero. □

Ejemplo. Calculemos el siguiente determinante **desarrollándolo por los elementos de una línea**. Para aplicar este método resulta conveniente que la fila o columna elegida tenga la mayor cantidad de ceros posible.

$$\begin{vmatrix} 2 & -1 & 0 & 5 \\ 0 & 2 & 3 & 1 \\ 1 & 0 & -1 & 4 \\ 2 & 1 & -2 & 8 \end{vmatrix} = (-1)^{1+1} \cdot 2 \cdot \begin{vmatrix} 2 & 3 & 1 \\ 0 & -1 & 4 \\ 1 & -2 & 8 \end{vmatrix} + (-1)^{1+2} \cdot (-1) \cdot \begin{vmatrix} 0 & 3 & 1 \\ 1 & -1 & 4 \\ 2 & -2 & 8 \end{vmatrix} +$$

$$+(-1)^{1+3} \cdot 0 \cdot \begin{vmatrix} 0 & 2 & 1 \\ 1 & 0 & 4 \\ 2 & 1 & 8 \end{vmatrix} + (-1)^{1+4} \cdot 5 \cdot \begin{vmatrix} 0 & 2 & 3 \\ 1 & 0 & -1 \\ 2 & 1 & -2 \end{vmatrix} = 2 \cdot 13 + 0 + 0 + (-5) \cdot 3 = 11.$$

Si una matriz $A = (a_{ij})$ de orden n tiene iguales a cero los elementos de una línea, excepto uno de ellos, el cálculo de su determinante se reduce, desarrollando por los elementos de esa línea al cálculo de un determinante de orden $n-1$. *Por lo tanto, antes de calcular* $\det A$ *conviene, aplicando operaciones elementales a las filas y/o columnas de A, hacer cero todos los elementos de una fila o columna excepto uno, reiterando este procedimiento hasta reducir el cálculo al de un determinante de orden 3 ó 2.*

Ejemplo.

$$\begin{vmatrix} 3 & 5 & -2 & 6 \\ 1 & 2 & -1 & 1 \\ 2 & 4 & 1 & 5 \\ 3 & 7 & 5 & 3 \end{vmatrix} = \begin{matrix} -3\cdot F_2 + F_1 \to F_1 \\ -2\cdot F_2 + F_3 \to F_3 \\ -3\cdot F_2 + F_4 \to F_4 \end{matrix} = \begin{vmatrix} 0 & -1 & 1 & 3 \\ 1 & 2 & -1 & 1 \\ 0 & 0 & 3 & 3 \\ 0 & 1 & 8 & 0 \end{vmatrix} = (-1)^{2+1}\cdot 1 \cdot \begin{vmatrix} -1 & 1 & 3 \\ 0 & 3 & 3 \\ 1 & 8 & 0 \end{vmatrix} =$$

$$F_1 + F_3 \to F_1 = -\begin{vmatrix} 0 & 9 & 3 \\ 0 & 3 & 3 \\ 1 & 8 & 0 \end{vmatrix} = -(-1)^{3+1}\cdot 1 \cdot \begin{vmatrix} 9 & 3 \\ 3 & 3 \end{vmatrix} = -18.$$

Algunas propiedades más de los determinantes

Propiedad 10.17 *Si A es una matriz de orden n y α es un número entonces* $\det(\alpha\cdot A) = \alpha^n \cdot \det A$.

Propiedad 10.18 *El determinante de un producto de matrices es el producto de los determinantes de cada una de ellas, es decir, si A y B son matrices cuadradas del mismo orden, entonces* $\det(A\cdot B) = \det A \cdot \det B$.

Matriz Inversa

Si A es una matriz de orden n y si existe una matriz B tal que $A\cdot B = B\cdot A = I_n$, donde I_n es la matriz unidad de orden n, entonces A se dice **inversible** y B se llama la **inversa** de A.

Es fácil ver que si existe una matriz B en esas condiciones, es única. Se escribe $B = A^{-1}$.

No toda matriz tiene inversa. Por ejemplo, si $A = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$ no existe ninguna matriz B tal que $A\cdot B = B\cdot A = I_n$.

En efecto, sea $B = \begin{pmatrix} x & y \\ z & u \end{pmatrix}$. Entonces si fuese $A\cdot B = I_n$, $\begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}\cdot\begin{pmatrix} x & y \\ z & u \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, o sea,

$$\begin{pmatrix} 2\,x + z & 2\,y + u \\ 2\,x + z & 2\,y + u \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

de donde resulta

$$\begin{cases} 2\,x + z = 1 \\ 2\,x + z = 0 \\ 2\,y + u = 0 \\ 2\,y + u = 1 \end{cases}$$

que es un sistema incompatible.

Puede probarse que si A es una matriz cuadrada de orden n, entonces $A\cdot B = I_n$ equivale a $B\cdot A = I_n$.

Definición 10.19 *Si $A = (a_{ij})$ es una matriz de orden n, definimos la* **matriz adjunta** *de A, y la notamos $AdjA$, de la siguiente manera: $AdjA = (A_{ij})$ donde A_{ij} es el complemento algebraico del elemento a_{ij}.*

$$AdjA = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n1} & \cdots & A_{nn} \end{pmatrix}$$

Ejemplo.

Si $A = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 3 \\ 1 & -1 & 0 \end{pmatrix}$, $AdjA = \begin{pmatrix} 3 & 3 & -1 \\ -2 & -2 & 0 \\ -5 & -3 & 1 \end{pmatrix}$.

Teorema 10.20 *Sea A una matriz de orden n. Entonces A es inversible si y sólo si* $\det A \neq 0$. *En ese caso,*

$$A^{-1} = \frac{(Adj\ A)^T}{\det A}.$$

Demostración. Veamos que $A \cdot (Adj\ A)^T = (Adj\ A)^T \cdot A = \det A \cdot I_n$. Si $A \cdot (AdjA)^T = (c_{ij})$ entonces $c_{ij} = a_{i1} \cdot A_{j1} + a_{i2} \cdot A_{j2} + \cdots + a_{in} \cdot A_{jn}$, donde A_{jk} es el complemento algebraico del elemento a_{jk}. Por lo tanto, según el teorema 10.15 y su corolario, resulta:

$$c_{ij} = \begin{cases} \det A & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j \end{cases}.$$

Luego, $A \cdot (AdjA)^T = \begin{pmatrix} \det A & 0 & \cdots & 0 \\ 0 & \det A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \det A \end{pmatrix} = \det A \,.\, I_n.$

Análogamente se prueba que $(AdjA)^T \cdot A = \det A \ \cdot \ I_n$. Por lo tanto, si $\det A \neq 0$,

$$A \cdot \frac{(AdjA)^T}{\det A} = \frac{(AdjA)^T}{\det A} \cdot A = I_n$$

y, por consiguiente,

$$A^{-1} = \frac{(AdjA)^T}{\det A}.$$

Recíprocamente, supongamos que A es inversible. Entonces existe una matriz A^{-1} tal que $A \cdot A^{-1} = I_n$. Por la Propiedad 11,

$$\det A \cdot \det (A^{-1}) = \det I_n.$$

Pero $\det I_n = 1$. Luego $\det A \cdot \det (A^{-1}) \neq 0$. De donde $\det A \neq 0$. $\square$

Ejemplo. Averiguar si la matriz A es inversible. En caso afirmativo hallar su inversa.

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 3 \\ 1 & -1 & 0 \end{pmatrix}$$

Como $\det A = -2 \neq 0$, A es inversible. Su inversa es

$$A^{-1} = \frac{(AdjA)^T}{\det A} = \frac{\begin{pmatrix} 3 & -2 & -5 \\ 3 & -2 & -3 \\ -1 & 0 & 1 \end{pmatrix}}{-2} = \begin{pmatrix} -3/2 & 1 & 5/2 \\ -3/2 & 1 & 3/2 \\ 1/2 & 0 & -1/2 \end{pmatrix}$$

Cálculo de la inversa de una matriz aplicando operaciones elementales

Vamos a describir a continuación otro método para hallar la inversa de una matriz A. La justificación de este procedimiento está contenida esencialmente en el siguiente ejemplo.

Sea $A = \begin{pmatrix} 3 & -1 \\ 2 & 1 \end{pmatrix}$. Queremos hallar una matriz $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ tal que $A \cdot B = I$, esto es,

$$\begin{pmatrix} 3 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 3x - z & 3y - t \\ 2x + z & 2y + t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hallar la matriz B es equivalente a resolver los sistemas de ecuaciones

$$\begin{cases} 3x - z = 1 \\ 2x + z = 0 \end{cases} \qquad \begin{cases} 3y - t = 0 \\ 2y + t = 1 \end{cases}$$

con matrices asociadas

$$\left(\begin{array}{cc|c} 3 & -1 & 1 \\ 2 & 1 & 0 \end{array}\right) \qquad \left(\begin{array}{cc|c} 3 & -1 & 0 \\ 2 & 1 & 1 \end{array}\right)$$

En estos dos sistemas se observa que:

- En el primer sistema aparecen sólo las incógnitas de la primera columna de B, y en el segundo, las de la segunda columna de B.
- La matriz de los coeficientes en ambos sistemas es la matriz A.

Podemos entonces resolver ambos sistemas simultáneamente escribiendo:

$$\left(\begin{array}{cc|cc} 3 & -1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right). \qquad (*)$$

Triangulando, se tiene:

$$(1/3) \cdot F_1 \qquad \left(\begin{array}{cc|cc} 1 & -1/3 & 1/3 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right)$$

$$(-2) \cdot F_1 + F_2 \qquad \left(\begin{array}{cc|cc} 1 & -1/3 & 1/3 & 0 \\ 0 & 5/3 & -2/3 & 1 \end{array}\right)$$

$$(3/5) \cdot F_2 \qquad \left(\begin{array}{cc|cc} 1 & -1/3 & 1/3 & 0 \\ 0 & 1 & -2/5 & 3/5 \end{array}\right)$$

$$(1/3) \cdot F_2 + F_1 \qquad \left(\begin{array}{cc|cc} 1 & 0 & 1/5 & 1/5 \\ 0 & 1 & -2/5 & 3/5 \end{array}\right)$$

que equivale a:

$$\left(\begin{array}{cc|c} 1 & 0 & 1/5 \\ 0 & 1 & -2/5 \end{array}\right) \qquad \left(\begin{array}{cc|c} 1 & 0 & 1/5 \\ 0 & 1 & 3/5 \end{array}\right)$$

1de donde $x = 1/5$, $z = -2/5$, $y = 1/5$, $t = 3/5$, esto es,

$$B = \begin{pmatrix} 1/5 & 1/5 \\ -2/5 & 3/5 \end{pmatrix}$$

Verificación:

$$A \cdot B = \begin{pmatrix} 3 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1/5 & 1/5 \\ -2/5 & 3/5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Observar que $(*)$ se formó escribiendo la matriz A a la izquierda y la matriz identidad a la derecha, y se aplicaron operaciones elementales hasta obtener la matriz identidad en las dos columnas de la izquierda. En general, dada una matriz A de orden n, si aplicando un número finito de operaciones elementales $E_1,\ E_2,\ \ldots, E_k$ sobre sus filas se puede obtener la matriz unidad de orden n, entonces la matriz A es inversible y para calcular su inversa basta aplicar a la matriz unidad de orden n las mismas operaciones elementales $E_1,\ E_2,\ \ldots, E_k$ y en el mismo orden. Si al aplicar operaciones elementales por filas a la matriz A, tratando de obtener la matriz unidad, se obtiene una fila nula, entonces A no es inversible.

Ejemplo. Decir si la matriz A es o no inversible, y en caso afirmativo, hallar su inversa:

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \\ 4 & -1 & 5 \end{pmatrix}$$

$$\begin{array}{rc|c}
 & \left(\begin{array}{ccc} 1 & -1 & 2 \\ 3 & 0 & 1 \\ 4 & -1 & 5 \end{array}\right) & \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \\
\begin{array}{r} -3F_1 + F_2 \to F_2 \\ -4F_1 + F_3 \to F_3 \end{array} & \left(\begin{array}{ccc} 1 & -1 & 2 \\ 0 & 3 & -5 \\ 0 & 3 & -3 \end{array}\right) & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -4 & 0 & 1 \end{array}\right) \\
\frac{1}{3}F_2 \to F_2 & \left(\begin{array}{ccc} 1 & -1 & 2 \\ 0 & 1 & -5/3 \\ 0 & 3 & -3 \end{array}\right) & \left(\begin{array}{ccc} 1 & 0 & 0 \\ -1 & 1/3 & 0 \\ -4 & 0 & 1 \end{array}\right) \\
\begin{array}{r} F_2 + F_1 \to F_1 \\ -3F_2 + F_3 \to F_3 \end{array} & \left(\begin{array}{ccc} 1 & 0 & 1/3 \\ 0 & 1 & -5/3 \\ 0 & 0 & 2 \end{array}\right) & \left(\begin{array}{ccc} 0 & 1/3 & 0 \\ -1 & 1/3 & 0 \\ -1 & -1 & 1 \end{array}\right) \\
\frac{1}{2}F_3 \to F_3 & \left(\begin{array}{ccc} 1 & 0 & 1/3 \\ 0 & 1 & -5/3 \\ 0 & 0 & 1 \end{array}\right) & \left(\begin{array}{ccc} 0 & 1/3 & 0 \\ -1 & 1/3 & 0 \\ -1/2 & -1/2 & 1/2 \end{array}\right) \\
\begin{array}{r} -\frac{1}{3}F_3 + F_1 \to F_1 \\ \frac{5}{3}F_3 + F_2 \to F_2 \end{array} & \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) & \left(\begin{array}{ccc} 1/6 & 1/2 & -1/6 \\ -11/6 & -1/2 & 5/6 \\ -1/2 & -1/2 & 1/2 \end{array}\right)
\end{array}$$

Verificación:

$$\begin{pmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \\ 4 & -1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1/6 & 1/2 & -1/6 \\ -11/6 & -1/2 & 5/6 \\ -1/2 & -1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

10.4 Característica de una matriz

Sea $A = (a_{ij})$ una matriz $n \times m$. Una *submatriz* de A es una matriz construída tomando la intersección de ciertas filas y columnas de A. Por ejemplo,

$$\begin{pmatrix} 1 & -1 & 3 \\ 4 & -1 & 2 \end{pmatrix} \text{ es una submatriz de } \begin{pmatrix} 1 & -1 & 2 & 3 \\ 3 & 0 & 1 & 4 \\ 4 & -1 & 5 & 2 \end{pmatrix}.$$

Se llama *menor de A de orden k* al determinante de cualquier submatriz B de A de orden $k \times k$.

Definición 10.21 *La* CARACTERÍSTICA *(o* RANGO*) de una matriz A $n \times m$ es el número entero k = Car A definido por la siguiente condición: existe un menor de A de orden k no nulo, y no existe ningún menor de A de orden mayor que k no nulo. La matriz de un tal menor de orden k se llama* submatriz principal. *También el* menor *se llama* principal.

Ejemplos.

$$\text{Car} \begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 2 & 2 & 0 \end{pmatrix} = 2 \quad ; \text{Car} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} = 3$$

$$\text{Car} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \end{pmatrix} = 1 \quad ; \text{Car} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = 1$$

Observación. Si en la matriz A hay un menor de orden k no nulo y todos los menores de orden $k+1$ son nulos, entonces Car $A = k$. En efecto, cualquier menor de orden $k+2$ será también cero (desarrollarlo por los elementos de una fila o columna). De la misma manera, los menores de orden $k+3$, $k+4$, ... son nulos.

Sea A una matriz de orden $n \times m$. Si indicamos con $C_1, C_2, \ldots, C_m$ las columnas de A, diremos que la columna C_i es combinación lineal de las columnas C_j y C_k, con $1 \leq j, k \leq m$, si existen números α, β tales que $C_i = \alpha \cdot C_j + \beta \cdot C_k$. En forma análoga se define una combinación lineal de un número cualquiera de columnas, y una combinación lineal de dos o más filas.

Lema 10.22 *Sea $A = (a_{ij})$ una matriz de orden n. Si Car $A = n - 1$, entonces una columna (fila) de A es combinación lineal de las columnas (filas) de una submatriz principal cualquiera de A.*

Demostración. Vamos a suponer sin pérdida de generalidad que

$$\alpha = det \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,n-1} \end{pmatrix} \neq 0.$$

Por hipótesis, det $A = 0$, luego por Corolario 10.16

$$\begin{array}{ccccccccccccc} a_{11}A_{n1} & + & a_{12}A_{n2} & + & \cdots & + & a_{1n}A_{nn} & = & 0 \\ a_{21}A_{n1} & + & a_{22}A_{n2} & + & \cdots & + & a_{2n}A_{nn} & = & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1}A_{n1} & + & a_{n2}A_{n2} & + & \cdots & + & a_{nn}A_{nn} & = & \det A & = & 0 \end{array}$$

Luego, como $A_{nn} = \alpha \neq 0$, resulta

$$\begin{aligned} a_{1n} &= -\frac{A_{n1}}{\alpha}a_{11} - \frac{A_{n2}}{\alpha}a_{12} - \cdots - \frac{A_{n,n-1}}{\alpha}a_{1,n-1} \\ a_{2n} &= -\frac{A_{n1}}{\alpha}a_{21} - \frac{A_{n2}}{\alpha}a_{12} - \cdots - \frac{A_{n,n-1}}{\alpha}a_{2,n-1} \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ a_{nn} &= -\frac{A_{n1}}{\alpha}a_{n1} - \frac{A_{n2}}{\alpha}a_{n2} - \cdots - \frac{A_{n,n-1}}{\alpha}a_{n,n-1} \end{aligned}$$

Es decir,

$$C_n = -\frac{A_{n1}}{\alpha}C_1 - \frac{A_{n2}}{\alpha}C_2 - \cdots - \frac{A_{n,n-1}}{\alpha}C_{n-1}.$$

Una demostración similar vale para filas en lugar de columnas □

Proposición 10.23 *Todas las columnas (filas) de una matriz $n \times m$ son combinación lineal de las columnas (filas) de una submatriz principal.*

Demostración. Supongamos, sin pérdida de generalidad, que las primeras k filas y las primeras k columnas de la matriz $A = (a_{ij})$ de orden $n \times m$ forman una submatriz $M = (m_{ij})$ principal.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & \cdots & a_{1s} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2k} & \cdots & a_{2s} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} & \cdots & a_{ks} & \cdots & a_{km} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rk} & \cdots & a_{rs} & \cdots & a_{rm} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nk} & \cdots & a_{ns} & \cdots & a_{nm} \end{pmatrix}$$

Elijamos una fila, digamos r, y una columna, digamos s, de A, y formemos la siguiente matriz ampliada de M:

$$N = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{1s} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} & a_{ks} \\ a_{r1} & a_{r2} & \cdots & a_{rk} & a_{rs} \end{pmatrix}$$

Como M es una submatriz principal, se tiene que $\det M \neq 0$ y $\det N = 0$. Entonces, por el lemma anterior, la columna C_s de N es combinación lineal de las columnas de M, o sea, existen $\lambda_1, \lambda_2, \ldots, \lambda_k \in R$ tales que

$$\begin{cases} \lambda_1 a_{11} + \lambda_2 a_{12} + \cdots + \lambda_k a_{1k} = a_{1s} \\ \lambda_1 a_{21} + \lambda_2 a_{22} + \cdots + \lambda_k a_{2k} = a_{2s} \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\quad \vdots \\ \lambda_1 a_{k1} + \lambda_2 a_{k2} + \cdots + \lambda_k a_{kk} = a_{ks} \\ \lambda_1 a_{r1} + \lambda_2 a_{r2} + \cdots + \lambda_k a_{rk} = a_{rs} \end{cases}$$

Las k primeras ecuaciones de este sistema se pueden escribir $M\lambda = d_s$, donde

$$\lambda = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_k \end{pmatrix} \quad , \quad d_s = \begin{pmatrix} a_{1s} \\ a_{2s} \\ \vdots \\ a_{ks} \end{pmatrix},$$

de donde $\lambda = M^{-1} d_s$.

Luego la matriz λ (de orden $n \times 1$) está determinada por d_s y no depende de r. En consecuencia, cualquier columna C_s, $1 \leq s \leq m$, de A es combinación lineal con coeficientes $\lambda_1, \lambda_2, \ldots, \lambda_k$ de las columnas $C_2, C_2, \ldots, C_k$.

En forma análoga se prueba para las filas de A. □

Proposición 10.24 *Sea A una matriz y sea B la matriz obtenida de A al sumar a una fila (columna) de A una combinación lineal de las demás. Sean $i_1, i_2, \ldots, i_k$ y $j_1, j_2, \ldots, j_k$ filas y columnas respectivamente de una matriz principal de A. Entonces $i_1, i_2, \ldots, i_k$ y $j_1, j_2, \ldots, j_k$ son filas y columnas de una matriz principal de B. En particular, A y B tienen la misma característica.*

Demostración. Todas las filas (columnas) de A son combinación lineal de las filas $i_1, i_2, \ldots, i_k$ (columnas $j_1, j_2, \ldots, j_k$) de A, y lo mismo para B. Como el determinante de una matriz no varía al sumar a una fila (columna) una combinación lineal de otras, resulta que A y B tienen la misma característica. □

La proposición anterior permite calcular Car A por el método de triangulación de Gauss. En efecto, la triangulación de A se logra sumando a filas de A combinaciones lineales de otras filas de A. Luego las filas $i_1, i_2, \ldots, i_k$ y columnas $j_1, j_2, \ldots, j_k$ de A corresponden a una matriz principal si y sólo si lo son de una matriz principal de la matriz triangulada. En esta última se detectan de inmediato tales $i_1, i_2, \ldots, i_k$ y $j_1, j_2, \ldots, j_k$.

Ejemplo.

$$A = \begin{pmatrix} 1 & 2 & 0 & -1 & 1 & 1 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 1 \\ 1 & -2 & -2 & 1 & -1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & -1 & 1 & 1 \\ 0 & -1 & 2 & 1 & -1 & -1 \\ 0 & -5 & 0 & 3 & -3 & -2 \\ 0 & -4 & -2 & 2 & -2 & -1 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 2 & 0 & -1 & 1 & 1 \\ 0 & -1 & 2 & 1 & -1 & -1 \\ 0 & 0 & -10 & -2 & 2 & 3 \\ 0 & 0 & -10 & -2 & 2 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & -1 & 1 & 1 \\ 0 & -1 & 2 & 1 & -1 & -1 \\ 0 & 0 & -10 & -2 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

La característica de la última matriz es evidentemente 3. Luego, como se ha obtenido por el proceso de triangulación, todas las anteriores, incluyendo A, tienen característica 3.

Resolución de sistemas lineales por determinantes. Regla de Cramer

Como aplicación del Teorema 10.15, vamos a probar que si el determinante de la matriz de los coeficientes de un sistema de n ecuaciones lineales con n incógnitas es distinto de cero, entonces el sistema tiene una única solución. Además vamos a dar una fórmula que expresa la solución única del sistema en función de los coeficientes y de los términos independientes.

Un sistema de n ecuaciones y n incógnitas

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

puede escribirse en forma matricial como sigue:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

es decir, puede escribirse $A \cdot X = B$, donde $A = (a_{ij})$ es la matriz de orden $n \times n$ de los coeficientes del sistema, $X = (x_i)$ es la matriz de orden $n \times 1$ de las incógnitas y $B = (b_i)$ es la matriz de orden $n \times 1$ de los términos independientes.

Teorema 10.25 (Regla de Cramer). *Si* $\det A \neq 0$*, el sistema* $A \cdot X = B$ *es compatible determinado, y la única solución del sistema está dada por*

$$x_i = \frac{\begin{vmatrix} a_{11} & a_{12} & \dots & b_1 & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & b_2 & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & b_n & \dots & a_{nn} \end{vmatrix}}{\det A},$$

donde b_1*,* b_2*, ...,* b_n *son los elementos de la* i*-ésima columna.*

Demostración. Si $\det A \neq 0$, entonces A es inversible. Entonces una solución del sistema $A \cdot X = B$ es $X = A^{-1} \cdot B$, ya que

$$A \cdot (A^{-1} \cdot B) = (A \cdot A^{-1}) \cdot B = B.$$

Además, esta solución es única, pues si Z es solución del sistema, se tiene $A \cdot Z = B$, de donde $A^{-1} \cdot A \cdot Z = A^{-1} \cdot B$, esto es, $Z = A^{-1} \cdot B$.

De $X = A^{-1} \cdot B$, y teniendo en cuenta que $A^{-1} = \dfrac{(Adj\,A)^T}{\det A}$, resulta:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \frac{1}{\det A} \cdot \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \frac{1}{\det A} \cdot \begin{pmatrix} A_{11}\,b_1 + A_{21}\,b_2 + \cdots + A_{n1}\,b_n \\ A_{12}\,b_1 + A_{22}\,b_2 + \cdots + A_{n2}\,b_n \\ \\ A_{1n}\,b_1 + A_{2n}\,b_2 + \cdots + A_{nn}\,b_n \end{pmatrix}.$$

Luego, para cada $i = 1, 2, \ldots, n$ se verifica

$$x_i = \frac{A_{1i}\, b_1 + A_{2i}\, b_2 + \cdots + A_{ni}\, b_n}{\det A},$$

es decir,

$$x_i = \frac{\begin{vmatrix} a_{11} & a_{12} & \ldots & b_1 & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & b_2 & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix}}{\det A}.$$

□

Ejemplo. Verificar si los siguientes sistemas son compatibles determinados, y en caso afirmativo, hallar la solución aplicando la regla de Cramer.

(a) $\left\{ \begin{array}{rcrcrcr} 2x & - & 6y & & & = & 3 \\ x & - & 3y & + & z & = & 2 \\ & & 2y & - & 3z & = & -1 \end{array} \right.$

(b) $\left\{ \begin{array}{rcrcrcrcr} x & - & y & & & + & u & = & 0 \\ 2x & & & - & z & + & 3u & = & 4 \\ & & 5y & - & z & - & u & = & 1 \\ 3x & + & 4y & - & 2z & + & 3u & = & 5 \end{array} \right.$

(a) $A = \begin{pmatrix} 2 & -6 & 0 \\ 1 & -3 & 1 \\ 0 & 2 & -3 \end{pmatrix}$

Como $\det A = -4 \neq 0$, el sistema es compatible determinado. La solución es:

$$x = \frac{\begin{vmatrix} 3 & -6 & 0 \\ 2 & -3 & 1 \\ -1 & 2 & -3 \end{vmatrix}}{-4} = \frac{9}{4}\,, \quad y = \frac{\begin{vmatrix} 2 & 3 & 0 \\ 1 & 2 & 1 \\ 0 & -1 & -3 \end{vmatrix}}{-4} = \frac{1}{4}\,, \quad z = \frac{\begin{vmatrix} 2 & -6 & 3 \\ 1 & -3 & 2 \\ 0 & 2 & -1 \end{vmatrix}}{-4} = \frac{1}{2}$$

(b) $A = \begin{pmatrix} 1 & -1 & 0 & 1 \\ 2 & 0 & -1 & 3 \\ 0 & 5 & -1 & -1 \\ 3 & 4 & -2 & 3 \end{pmatrix}$

En este caso, $\det A = 0$, luego el sistema no puede resolverse por la regla de Cramer.

La expresión matricial de la solución es útil para diversos fines. Sin embargo hay que enfatizar que, para un sistema genérico dado, el método de Gauss es más rápido a los efectos del cálculo numérico.

Consideremos ahora el caso general de un sistema lineal de n ecuaciones y m incógnitas

$$\left\{ \begin{array}{rcrcrcrcr} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1m}x_m & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2m}x_m & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{nm}x_m & = & b_n \end{array} \right.$$

Si A es la matriz de orden $n \times m$ de los coeficientes, X es la matriz $n \times 1$ de las incógnitas y B es la matriz $n \times 1$ de los términos independientes, el sistema puede escribirse en forma matricial

$AX = B$. Notemos (A, B) a la matriz que resulta de agregar a la matriz A la columna de los términos independientes:

$$(A,B) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} & b_1 \\ a_{21} & a_{22} & \dots & a_{2m} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} & b_m \end{pmatrix}$$

Teorema 10.26 *(***Teorema de Rouché-Frobenius o de Kroenecker-Capelli***) El sistema lineal $AX = B$ es compatible si y sólo si la característica de la matriz A de los coeficientes y la característica de la matriz ampliada (A, B) coinciden. Sea M una submatriz principal de A, con filas $i_1, i_2, \dots, i_k$ y columnas $j_1, j_2, \dots, j_k$. Sea A' la matriz obtenida de A eliminando las filas distintas de $i_1, i_2, \dots, i_k$, y sea B' la matriz obtenida de B eliminando los elementos (filas) distintos de $i_1, i_2, \dots, i_k$. Entonces el sistema $AX = B$ es equivalente (esto es, tiene las mismas soluciones) al sistema $A'X = B'$.*

Antes de ver la demostración de esta proposición veamos el siguiente ejemplo.

Ejemplo. Consideremos el sistema

$$\begin{cases} x_1 + 2x_2 + 3x_3 + x_5 = 0 \\ 2x_1 + 2x_2 + 3x_3 - 2x_4 = 1 \\ -x_1 + 2x_4 + x_5 = -1 \\ 2x_2 + 3x_3 + 2x_4 + 2x_5 = -1 \end{cases}$$

La matriz de los coeficientes y la matriz ampliada son respectivamente

$$A = \begin{pmatrix} 1 & 2 & 3 & 0 & 1 \\ 2 & 2 & 3 & -2 & 0 \\ -1 & 0 & 0 & 2 & 1 \\ 0 & 2 & 3 & 2 & 2 \end{pmatrix} \quad y \quad (A,B) = \begin{pmatrix} 1 & 2 & 3 & 0 & 1 & 0 \\ 2 & 2 & 3 & -2 & 0 & 1 \\ -1 & 0 & 0 & 2 & 1 & -1 \\ 0 & 2 & 3 & 2 & 2 & -1 \end{pmatrix}.$$

Ambas tienen característica 2. Las filas 1 y 3, y las columnas 1 y 2 corresponden a la submatriz principal

$$M = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}$$

en ambas matrices. Luego el sistema es compatible.
Las matrices A' y B' de la proposición son

$$A = \begin{pmatrix} 1 & 2 & 3 & 0 & 1 \\ -1 & 0 & 0 & 2 & 1 \end{pmatrix}, \qquad B' = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

El sistema dado $AX = B$ es equivalente al sistema $A'X = B'$, que es

$$\begin{cases} x_1 - 2x_2 + 3x_3 + x_5 = 0 \\ -x_1 + 2x_4 + x_5 = -1 \end{cases}$$

La matriz A' tiene submatriz principal M. Pasando al segundo miembro las incógnitas que no figuran en M resulta

$$\begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -3x_3 - x_5 \\ -x_5 - 1 \end{pmatrix}$$

Como la inversa de $M = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}$ es $M^{-1} = \begin{pmatrix} 0 & -1 \\ 1/2 & 1/2 \end{pmatrix}$, resulta

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1/2 & 1/2 \end{pmatrix} \begin{pmatrix} -3x_3 - x_5 \\ -x_5 - 1 \end{pmatrix} = \begin{pmatrix} 2x_4 + x_5 + 1 \\ -3/2x_3 - x_4 - x_5 - 1/2 \end{pmatrix},$$

esto es,

$$x_1 = 2x_4 + x_5 + 1; \qquad x_2 = (-3/2)x_3 - x_4 - x_5 - 1/2.$$

La solución general es entonces

$$(2x_4 + x_5 + 1, (-3/2)x_3 - x_4 - x_5 - 1/2, x_3, x_4, x_5).$$

Demostración. El procedimiento indicado en el ejemplo es general: siempre pueden pasarse al segundo miembro las incógnitas cuyos coeficientes no están en M, y luego despejar las restantes, multiplicando por M^{-1}. Esto prueba que si la característica de la matriz de los coeficientes y la de la matriz ampliada son iguales el sistema tiene solución. Recíprocamente, si el sistema tiene solución, entonces B es combinación lineal de las columnas de A, por lo cual la característica de A y la de (A, B) son iguales. □

Proposición 10.27 *Si el sistema $AX = B$ es compatible, entonces si la característica r de A es igual al número m de columnas de A, (número de incógnitas), la solución es única. Si $r < m$, el sistema tiene infinitas soluciones.*

Demostración. Siguiendo el procedimiento indicado en la proposición anterior, es claro que si el número de incógnitas (número de columnas de A) es mayor que la característica de A, entonces pueden pasarse incógnitas al segundo miembro, dando lugar a infinitas soluciones. □

Ejercicio. Resolver el siguiente sistema aplicando el Teorema de Rouché-Frobenius.

$$\begin{cases} x_1 - x_2 - x_3 + x_4 = 1 \\ 2x_1 + 2x_2 - 3x_3 + 6x_4 - x_5 = -1 \\ x_1 + 2x_2 - x_3 + 4x_4 = 1 \\ 3x_1 + x_2 - 4x_3 + 7x_4 - x_5 = 0 \end{cases}$$

La matriz de los coeficientes y la matriz ampliada son respectivamente

$$A = \begin{pmatrix} 1 & -1 & -1 & 1 & 0 \\ 2 & 2 & -3 & 6 & -1 \\ 1 & 2 & -1 & 4 & 0 \\ 3 & 1 & -4 & 7 & -1 \end{pmatrix} \qquad y \qquad (A, B) = \begin{pmatrix} 1 & -1 & -1 & 1 & 0 & 1 \\ 2 & 2 & -3 & 6 & -1 & -1 \\ 1 & 2 & -1 & 4 & 0 & 1 \\ 3 & 1 & -4 & 7 & -1 & 0 \end{pmatrix}.$$

Se puede ver que el rango de A y el rango de (A, B) es 3, con matriz principal

$$M = \begin{pmatrix} 1 & -1 & -1 \\ 2 & 2 & -3 \\ 1 & 2 & -1 \end{pmatrix}.$$

Por el teorema de Rouché-Frobenius el sistema es compatible indeterminado. La solución del sistema dado se lleva al sistema

$$\begin{pmatrix} x_1 - x_2 - x_3 = 1 - x_4 \\ 2x_1 + 2x_2 - 3x_3 = -1 - 6x_4 + x_5 \\ x_1 + 2x_2 - x_3 = 1 - 4x_4 \end{pmatrix}.$$

La matriz de los coeficientes de este nuevo sistema es la matriz M, con $\det M = 3$, y el sistema puede escribirse matricialmente

$$M \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & - & x_4 & & \\ -1 & - & 6x_4 & + & x_5 \\ 1 & - & 4x_4 & & \end{pmatrix},$$

y como

$$M^{-1} = 1/3 \begin{pmatrix} 4 & -3 & 5 \\ -1 & 0 & 1 \\ 2 & -3 & 4 \end{pmatrix},$$

resulta

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 1/3 \begin{pmatrix} 4 & -3 & 5 \\ -1 & 0 & 1 \\ 2 & -3 & 4 \end{pmatrix} \begin{pmatrix} 1 & - & x_4 & & \\ -1 & - & 6x_4 & + & x_5 \\ 1 & - & 4x_4 & & \end{pmatrix}.$$

Haciendo $x_4 = \lambda$ y $x_5 = \mu$ se tiene:

$$x_1 = 4 - 2\lambda - \mu, \quad x_2 = -\lambda, \quad x_3 = 3 - \mu.$$

La solución general puede escribirse $\quad (4 - 2\lambda - \mu, -\lambda, 3 - \mu, \lambda, \mu)$.

Sistemas lineales homogéneos

Si en la matriz $B = (b_i)$ de los términos independientes, es $b_i = 0$ para todo i, se dice que el sistema es *homogéneo*. A partir del Teorema de Rouché-Frobenius se tiene que un sistema homogéneo siempre en compatible, pues al agregar la columna B no se modifica el rango de la matriz de los coeficientes. Una solución evidente es $x_1 = x_2 = \ldots = x_m = 0$, llamada *solución trivial*.

El siguiente teorema es evidente.

Teorema 10.28 *Un sistema homogéneo tiene soluciones no triviales si y sólo si el rango r de la matriz A de los coeficientes es menor que el número m de incógnitas. Si el sistema tiene igual número de ecuaciones que de incógnitas ($n = m$) entonces el sistema tiene soluciones no triviales si y sólo si $\det A = 0$.*

10.5 Ejercicios

1. Resolver y clasificar los siguientes sistemas de ecuaciones lineales. Si el sistema es compatible indeterminado, hallar además una solución particular del mismo.

(a) $\begin{cases} x+3y+5z=1 \\ 4x+3y+2z=1 \\ 3x+6y+9z=2 \end{cases}$ (b) $\begin{cases} 2x-y+3z=4 \\ 3x-2y+2z=3 \\ 5x-3y=2 \end{cases}$

(c) $\begin{cases} 2x+7y+3z+t=6 \\ 3x+5y+2z+2t=4 \\ 9x+4y+z+7t=2 \end{cases}$ (d) $\begin{cases} 3x+2y+2z+2t=2 \\ 2x+3y+2z+5t=3 \\ 9x+y+4z-5t=1 \\ 7x+y+6z-t=7 \\ 2x+2y+3z+4t=5 \end{cases}$

(e) $\begin{cases} x+3y+z=11 \\ x+2y-3z=4 \\ 2x+5y-4z=13 \\ 2x+6y+2z=22 \end{cases}$ (f) $\begin{cases} x+y-z=0 \\ 2x+4y-z=0 \\ -x+y+2z=0 \end{cases}$

2. Hallar el valor de λ para el cual los siguientes sistemas son compatibles determinados, indeterminados ó incompatibles:

(a) $\begin{cases} x+2y-3z=4 \\ 3x-y+5z=2 \\ 4x+y+(\lambda^2-14)z=\lambda+2 \end{cases}$ (b) $\begin{cases} 2x+5y+z+3t=2 \\ 4x+6y+3z+5t=4 \\ 4x+14y+z+7t=4 \\ 2x-3y+3z+\lambda t=7 \end{cases}$

3. Determinar, si existen, $x, y, z \in \mathbb{R}$ que verifiquen simultáneamente:

(a) $\begin{cases} x=1+2\lambda \\ y=-1-4\lambda \\ z=-2+2\lambda \end{cases}, \ \lambda \in \mathbb{R}$ $\begin{cases} x=3-\gamma \\ y=-6+3\gamma \\ z=-2+\gamma \end{cases}, \ \gamma \in \mathbb{R}$

(b) $\begin{cases} x=1+\lambda \\ y=2-\lambda \\ z=-3+3\lambda \end{cases}, \ \lambda \in \mathbb{R}$ $\begin{cases} x=2+2\gamma \\ y=-2+2\gamma \\ z=1-2\gamma \end{cases}, \ \gamma \in \mathbb{R}.$

4. Construir matrices que cumplan las siguientes condiciones:

(a) $A=(a_{ij})$ de orden 2 tal que $a_{ij}=i^2-2j+1$.

(b) $B=(b_{ij})$ de orden 3 tal que $b_{ij}-b_{ji}=0$ si $i \neq j$, $b_{ij}=0$ si $i=j$.

(c) $C=(c_{ij})$ de orden 2 tal que $c_{ij}=\begin{cases} 0 & \text{si } i+j=3 \\ 2 & \text{si } i+j \neq 3 \end{cases}$.

(d) $D=(d_{ij})$ de orden 4 tal que $d_{ij}=\begin{cases} i-j & \text{si } i>j \\ 0 & \text{si } i<j \\ -2j & \text{si } i=j \end{cases}$.

(e) $E = (e_{ij})$ de orden 3 tal que $e_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ \sqrt{j} & \text{si } i = j \end{cases}$.

5. Resolver, si es posible, las siguientes ecuaciones matriciales:

(a) $\begin{pmatrix} a+b & -a \\ a+b & b+c \end{pmatrix} + \begin{pmatrix} 0 & -b \\ b+2c & 0 \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ 1 & -2 \end{pmatrix}$.

(b) $\begin{pmatrix} d & c \\ a-c & a+b \end{pmatrix} + \begin{pmatrix} 0 & -d \\ 2d & c-d \end{pmatrix} = \begin{pmatrix} 2 & 4 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

(c) $\begin{pmatrix} a+2b & 11 \\ 2a & 2a+6b \end{pmatrix} + \begin{pmatrix} -3c & 0 \\ 5b-4c & 2c \end{pmatrix} = \begin{pmatrix} 4 & a+3b+c \\ 13 & 22 \end{pmatrix}$.

6. Efectuar los siguientes productos entre matrices:

(a) $\begin{pmatrix} 3 & -2 \\ 5 & -4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & -3 & 2 \\ 3 & -4 & 1 \\ 2 & -5 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 5 & 6 \\ 1 & 2 & 5 \\ 1 & 3 & 2 \end{pmatrix}$ (c) $\begin{pmatrix} 2 & -1 \\ 0 & 1 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 1 \end{pmatrix}$

7. Sean $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.
Calcular: $A \cdot B - B \cdot A$, $B \cdot C - C \cdot B$ y $A \cdot C - C \cdot A$.

8. (a) Sea $A = \begin{pmatrix} 2 & -1 \\ 3 & -2 \end{pmatrix}$, calcular:

(i) A^2 y A^3.

(ii) A^n, $n \in \mathbb{N}$.

(b) Idem para $A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ y $A = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$.

9. Dar ejemplos de matrices no nulas A y B de orden 2 que verifiquen:

(a) $A^2 = A$, $A \neq I_2$.

(b) $A^n = 0$, para algún $n \in \mathbb{N}$.

(c) $A \cdot B + B \cdot A = I_2$.

10. Dada la matriz $A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 4 \end{pmatrix}$, hallar una matriz B tal que se puedan efectuar los productos $A \cdot B$ y $B \cdot A$. ¿De qué órdenes son estos productos?

11. Sean A y B matrices cuadradas de orden n. Mostrar que:

(a) En general, $A \cdot B \neq B \cdot A$.

(b) Si $A \cdot B \neq B \cdot A$ entonces $(A+B)^2 \neq A^2 + B^2 + 2A \cdot B$ y $A^2 - B^2 \neq (A+B) \cdot (A-B)$.

(c) En general, si $A \cdot B = 0$ no necesariamente $A = 0$ ó $B = 0$.

(d) Si $A = \lambda \cdot I_n$ entonces $A \cdot B = B \cdot A$ para toda matriz B de orden n.

12. Hallar, si es posible, una matriz A tal que:

(a) $7 \cdot A - 2 \cdot \begin{pmatrix} 1 & 5 & 3 \\ 3 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & -3 & 8 \\ 0 & -2 & 2 \end{pmatrix} + \begin{pmatrix} 5 & 0 & 7 \\ 1 & -1 & 3 \end{pmatrix}$.

(b) $A \cdot \begin{pmatrix} 3 & -6 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & -6 \\ -1 & 2 \end{pmatrix} \cdot A = I_2$.

(c) $A \cdot \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \cdot A = I_2$.

13. Una matriz cuadrada $a = (a_{ij})$ se dice diagonal si $a_{ij} = 0$ cuando $i \neq j$. Decidir la verdad o falsedad de las siguientes afirmaciones justificando su respuesta.

Si A, B, C son matrices cuadradas de orden n se tiene:

(a) $[2 \cdot A^T \cdot (3 \cdot B) \cdot C]^T = 6 \cdot (B \cdot C)^T \cdot A$.

(b) $(2 \cdot A + B \cdot C)^T = 2 \cdot A^T + B \cdot C$, donde B y C son matrices diagonales.

(c) $(A \cdot B^T \cdot C - A)^T = (C^T \cdot B - I_n) \cdot A^T$.

(d) $\left((A^T)^2\right)^T = A^2$.

(e) Si A y B son matrices diagonales, entonces $A^2 - B^2 = (A-B) \cdot (A+B)$.

14. Una matriz cuadrada $A = (a_{ij})$ se dice simétrica si $a_{ij} = a_{ji}$, para todo i, j. Mostrar que:

(a) Si A es una matriz $m \times n$ entonces el producto $A \cdot A^T$ está definido y es una matriz simétrica .

(b) La suma de matrices simétricas es una matriz simétrica.

(c) El producto de dos matrices simétricas es una matriz simétrica, si las matrices conmutan.

15. Calcular:

(a) $\begin{vmatrix} 2 & 1 \\ 3 & -5 \end{vmatrix}$ (b) $\begin{vmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \\ -1 & 3 & 0 \end{vmatrix}$ (c) $\begin{vmatrix} 2 & 0 & 1 \\ -1 & 3 & 1 \\ 0 & 1 & -2 \end{vmatrix}$.

16. Hallar los valores de x tales que $det\, A = 0$.

(a) $A = \begin{pmatrix} x-1 & -2 \\ 1 & x-4 \end{pmatrix}$ (b) $A = \begin{pmatrix} x-6 & 0 & 0 \\ 0 & x & -1 \\ 0 & 4 & x-4 \end{pmatrix}$ (c) $A = \begin{pmatrix} 1 & 3 & x \\ 4 & 5 & -1 \\ 2 & -1 & 5 \end{pmatrix}$

17. Si $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & m \end{pmatrix}$ y $det\, A = 5$ decir, sin calcular los determinantes, por qué valen las

siguientes igualdades:

(a) $\begin{vmatrix} d & e & f \\ g & h & m \\ a & b & c \end{vmatrix} = 5$ (b) $\begin{vmatrix} -a & -b & -c \\ 2\,d & 2\,e & 2\,f \\ -g & -h & -m \end{vmatrix} = 10$

(c) $\begin{vmatrix} a+d & b+e & c+f \\ d & e & f \\ g & h & m \end{vmatrix} = 5$ (d) $\begin{vmatrix} a & b & c \\ d-3\,a & e-3\,b & f-3\,c \\ 2g & 2h & 2m \end{vmatrix} = 10$

18. Calcular, desarrollando por los elementos de la fila ó columna con más ceros, el siguiente determinante

$$\begin{vmatrix} 1 & -1 & 2 & 3 \\ -1 & 0 & 1 & 0 \\ 2 & 1 & -2 & -1 \\ 5 & 1 & 1 & 3 \end{vmatrix}$$

19. Calcular el determinante del ejercicio anterior, llevando previamente a la forma triangular.

20. Calcular los siguientes determinantes haciendo previamente todos los elementos de una fila o columna cero excepto uno y desarrollando luego por esa línea.

(a) $\begin{vmatrix} 1 & -1 & 2 \\ 0 & 1 & 3 \\ -1 & 1 & 1 \end{vmatrix}$ (b) $\begin{vmatrix} 1 & 2 & -1 & 3 \\ 0 & 1 & -1 & 2 \\ 2 & -1 & 5 & 0 \\ 0 & 1 & 1 & 1 \end{vmatrix}$ (c) $\begin{vmatrix} 1 & -1 & 2 & 1 & 3 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & 1 & 1 & -1 & 2 \\ 0 & 1 & -1 & 3 & 0 \\ 1 & -1 & 1 & 1 & 1 \end{vmatrix}$

21. Si A es una matriz de orden 3 y $\det A = 2$, hallar $\det(\frac{1}{2} \cdot A)$ y $\det(A \cdot A^t)$.

22. ¿ Es cierto que $\det(A+B) = \det A + \det B$? Justificar la respuesta.

23. Dadas las siguientes matrices decir si son o no inversibles, y en caso afirmativo, hallar su inversa:

(a) $\begin{pmatrix} 1 & -1 & 2 \\ 3 & 0 & 1 \\ 4 & -1 & 5 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & -1 & 1 & 2 \\ 0 & 0 & -1 & 3 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & -1 & 0 \\ 3 & 1 & 4 \\ 0 & 1 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 1 & -1 & 2 \\ 3 & 1 & -2 & 5 \\ 4 & 1 & -1 & 10 \end{pmatrix}$

24. Sean A y B matrices cuadradas de orden n. Probar que:

(a) Si A y B son matrices inversibles, entonces $A \cdot B$ también lo es y $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

(b) Si A es inversible, entonces $\det B = \det(A^{-1} \cdot B \cdot A)$.

25. Si A es una matriz de orden 3 y $\det A = 3$, hallar $\det(A^{-1})$, $\det(5 \cdot A^{-1})$ y $\det(5 \cdot A)^{-1}$.

26. Verificar si los siguientes sistemas son compatibles determinados, y en caso afirmativo, hallar la solución aplicando la regla de Cramer.

(a) $\begin{cases} x+3\,y+5\,z=1 \\ 4\,x+3\,y+2\,z=1 \\ 3\,x+6\,y+9\,z=2 \end{cases}$ (b) $\begin{cases} 2\,x-\ y+3\,z=4 \\ 3\,x-2\,y+2\,z=3 \\ 5\,x-3\,y\ \ \ \ =2 \end{cases}$

(c) $\begin{cases} 2\,x-6\,y=\ \ 3 \\ x-3\,y+z=\ \ 2 \\ 2\,y-3\,z=-1 \end{cases}$ (d) $\begin{cases} x-y+u=\ \ 0 \\ 2\,x-z+3\,u=\ \ 4 \\ 5\,y-z-u=\ \ 1 \\ 3\,x+4\,y-2\,z+3\,u=\ \ 5 \end{cases}$

27. Analizar la compatibilidad de los siguientes sistemas de ecuaciones lineales utilizando el teorema de Rouché-Frobenius. Resolver.

(a) $\begin{cases} -5x+4y-7z=\ \ 1 \\ -5x-2y+3z=-2 \\ \ \ 5x-4y+6z=-1 \end{cases}$ (b) $\begin{cases} x+2y-2z-t=\ \ 1 \\ 2x-2y-2z-3t=-1 \\ 2x-2y-z-5t=\ \ 9 \\ -3x+y-z+2t=\ \ 0 \end{cases}$

(c) $\begin{cases} x+2y-5z=-5 \\ 3x-2y+z=\ \ 9 \end{cases}$ (d) $\begin{cases} 3x+iy-z-6t=\ \ 2 \\ (1-i)x+y+iz-2(1-i)t=-2i \\ -x+2y+4iz+4t=-6i \end{cases}$

28. Para qué valores de λ tiene soluciones no triviales el sistema

$$\begin{cases} x+y+z+t=0 \\ x+\lambda y+z+t=0 \\ x+y+\lambda z+t=0 \\ x+y+z+\lambda t=0 \end{cases}$$

11 Ejercicios de repaso

1. Sean A, B y C los conjuntos: $A = \{\{7,8,9\},\{3,6\},\{5\}\}$; $B = \{7,8,9,3,6,5\}$; $C = \{\{7\},\{8\},\{9\},\{3\},\{6\},\{5\}\}$.

   Completar con la relación: $\subseteq$, $\supseteq$, $\in$ ó $\notin$ según corresponda:

   (i) $\{3,6\}$ ..... A
   (ii) $\{\{6\},\{5\}\}$ ..... $\{\{9\},\{6\},\{5\}\}$
   (iii) $\{3,6\}$ ..... B
   (iv) $\{7,8\}$ C
   (v) A ..... $\{\{7,8,9\}\}$

2. Verificar, por cálculo directo, las siguientes igualdades:

   (a) $[(A \cup B)' \cup (A' - B)]' \cap (B - A)' = A$.
   (b) $(B - A)' \cap [(A' - B) \cup (A \cup B)']' = A$.
   (c) $[(D \cap F)' - E']' \cap [(D' \cup F')' \cup E] = D \cap F$.
   (d) $[(X - Y)' \cup Z] \cap [(X \cap Z) - Y]' = X' \cup Y$.

3. ¿Cuántos elementos puede tener la unión de un conjunto con 5 elementos y otro con 9 elementos?. ¿Y la intersección?

4. Sean A y B dos conjuntos.

   (a) Si A tiene 5 elementos y $A \cap B$ tiene 3 elementos, determinar cuáles de las siguientes afirmaciones pueden ser verdaderas, cuáles son necesariamente falsas y cuáles necesariamente verdaderas.

      (i) A es un subconjunto de B.
      (ii) $A \cup B$ tiene 5 elementos.
      (iii) B tiene exactamente 2 elementos.
      (iv) Si $A \cup B$ tiene 5 elementos, entonces B tiene 3 elementos.
      (v) $\mathcal{P}(A)$ tiene exactamente cuatro elementos.
      (vi) B no es vacío.
      (vii) Si $B \subseteq A$ entonces B tiene 2 elementos.

   (b) Si B tiene tres elementos y $A \cup B$ tiene cinco elementos, determinar cuáles de las siguientes afirmaciones pueden ser verdaderas, cuáles son necesariamente falsas y cuáles necesariamente verdaderas.

      (i) $A \cap B$ tiene exactamente tres elementos.
      (ii) A es vacío.
      (iii) $\mathcal{P}(B)$ tiene exactamente ocho elementos.
      (iv) A tiene exactamente dos elementos.
      (v) Si $B \subseteq A$ entonces $A \cap B$ tiene más de tres elementos.

5. (a) Demostrar que si $D \subseteq E'$ y $F \subseteq G$ entonces $D \cup F \subseteq (D - E) \cup (F \cap G)$.
   (b) Demostrar que si $X \subseteq T$ y $Z' \subseteq Y$ entonces $X - Z \subseteq Y \cap (T \cup Z')$.

6. Demostrar que si $A \cap X = A \cap Y$ y $A \cup X = A \cup Y$, entonces $X = Y$.

7. Se llama *diferencia simétrica* de los conjuntos A y B al conjunto $A\Delta B = (A - B) \cup (B - A)$. Determinar cuáles de las siguientes afirmaciones son verdaderas cualesquiera sean los conjuntos A, B y C y cuáles no. Para las que sean verdaderas, dar una demostración, para las otras dar un contraejemplo.

   (i) $A \cup (B \cap C) = (A \cup B) \cap C$
   (ii) $A\Delta B \subseteq (A\Delta C) \cup (B\Delta C)$
   (iii) Si $C \subseteq A$ entonces $B \cap C \subseteq (A\Delta B)'$
   (iv) $A\Delta B = \emptyset$ si y sólo si $A = B$
   (v) $(A\Delta B) - C = (A - C)\Delta(B - C)$
   (vi) $A\Delta\emptyset = A$
   (vii) $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$
   (viii) $A - (B - C) = (A - B) \cup (A \cap C)$
   (ix) $A - (A\Delta B) = A \cap B$
   (x) $(A \cap C) - B = (A - B) \cap C$
   (xi) Si $A \subseteq B$ entonces $A\Delta B = B \cap A'$
   (xii) Si $A \cap C = \emptyset$ entonces $A \cap (B\Delta C) = A \cap B$

8. (a) Sea $A = \mathbb{R} \times \mathbb{R}$ y sea R la relación definida por: $(x, y)R(z, t)$ si y sólo si $x \leq z$ e $y \leq t$. Indicar si R es reflexiva, simétrica, antisimétrica y transitiva.
   (b) Dados el conjunto $Y = \{a, b, c, d\}$ y la relación de equivalencia definida por:

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

   hallar las clases de equivalencia y el conjunto cociente determinado por R.

9. (a) Sea $A = \mathbb{Z} \times \mathbb{Z}$ y sea R la relación definida por: $(a, b)R(c, d)$ si y sólo si a divide a c. Indicar si R es reflexiva, simétrica, antisimétrica y transitiva.
   (b) Dados el conjunto $A = \{1, 2, 3, 4\}$ y la relación de equivalencia definida por:

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

   hallar las clases de equivalencia y el conjunto cociente determinado por R.

10. (a) Sea $A = \mathbb{R} \times \mathbb{R}$ y sea R la relación definida por: $(x, y)R(z, t)$ si y sólo si $x^2 = z^2$. Indicar si R es reflexiva, simétrica, antisimétrica y transitiva.
    (b) Dados el conjunto $X = \{a, b, c, d, e\}$ y la relación de equivalencia definida por:

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

    hallar las clases de equivalencia y el conjunto cociente determinado por R.

11. Sea $A = \mathbb{R} \times \mathbb{R}$ y sea R la relación definida por: $(x, y)R(u, v)$ si y sólo si $(x^2, y) = (u^2, v)$.

    (a) Demostrar que R es una relación de equivalencia, calcular las clases de equivalencia, dar ejemplos y graficar. Hallar el conjunto cociente.
    (b) Indicar si las siguientes proposiciones son verdaderas o falsas, justificando las respuestas:

(i) $(2,3)$ pertenece a la clase del $(-2,-3)$.

(ii) El conjunto $I = \{(x,y) \in \mathbb{R}^2 : y = 0, x \geq 0\}$ contiene un elemento y uno solo de cada clase de equivalencia.

(iii) $C_{(0,3)}$ tiene 2 elementos.

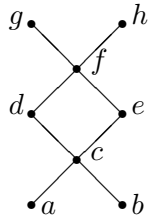
(c) ¿ Cuántos elementos tiene $C_{(0,y)}$, $y \in \mathbb{R}$?

12. Dibujar el diagrama de Hasse correspondiente al conjunto $A = \{10, 9, 5, 3, 2, 1\}$ ordenado por la relación: xRy si y sólo si x es múltiplo de y. Indicar, si existe, el primer elemento, el último elemento, los elementos maximales y los elementos minimales de A.

13. Dibujar el diagrama de Hasse correspondiente al conjunto $A = \{2, 3, 4, 5, 15, 60\}$ ordenado por la relación: xRy si y sólo si x divide a y.

Indicar, si existe, el primer elemento, el último elemento, los elementos maximales y los elementos minimales de A.

14. Sea B el conjunto ordenado cuyo diagrama de Hasse es:



Hallar, si existen, las cotas inferiores, las cotas superiores, el supremo y el ínfimo de los conjuntos $X_1 = \{a, b, d\}$, $X_2 = \{d, e\}$, $X_3 = \{a, e, g\}$, $X_4 = \{e, g, h\}$, $X_5 = \{c, f\}$, $X_6 = \{d, g\}$.

15. (a) Determinar si R es una función de A en B en los casos

(i) $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$, $R = \{(1,a),(2,a),(3,d),(4,b),(5,c)\}$

(ii) $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$, $R = \{(1,a),(2,a),(3,a),(4,b),(5,c),(3,d)\}$

(iii) $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$, $R = \{(1,a),(2,a),(3,d),(4,b)\}$

(iv) $A = \{1,2,3\}$, $B = \{a,b,c,d,e\}$, $R = \{(1,a),(2,a),(3,e)\}$

(v) $A = \mathbb{N}$, $B = \mathbb{R}$, $R = \{(a,b) \in \mathbb{N} \times \mathbb{R} : a = 2b - 3\}$

(vi) $A = \mathbb{R}$, $B = \mathbb{N}$, $R = \{(a,b) \in \mathbb{R} \times \mathbb{N} : a = 2b - 3\}$

(vii) $A = \mathbb{Z}$, $B = \mathbb{Z}$, $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a + b$ es divisible por $5\}$

(viii) $A = \mathbb{N}$, $B = \mathbb{N}$, $R = \{(a,b) \in \mathbb{N} \times \mathbb{N} : b = a^2\}$

(b) Para cada una de las relaciones de A en B definidas en (a) que sean funciones, hallar la imagen y determinar si es inyectiva, sobreyectiva o biyectiva.

16. (a) Averiguar si la función f es inyectiva, epiyectiva o biyectiva. Justificar las respuestas.

(i) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 5\,x - 3$.

(ii) $f : \mathbb{R} \to \mathbb{R}^+$, $f(x) = 6\,x^2$. $\quad (\mathbb{R}^+ = \{x : x \in \mathbb{R},\, x \geq 0\})$.

(iii) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 5\,x^3 - 3$.

(iv) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 8$.

(b) Hallar la función inversa de la función g.

(i) $g : \mathbb{R}^+ \to \mathbb{R}^+$, definida por $g(x) = \dfrac{1}{4}x^2$.

(ii) $g : \mathbb{R} \to \mathbb{R}$, definida por $g(x) = 8x^3 + 2$.

(iii) $g : \mathbb{R}^+ \to \mathbb{R}^+$, definida por $g(x) = 9\,x^2$.

(iv) $g : \mathbb{R} \to \mathbb{R}$, definida por $g(x) = x^3 - 6$.

(c) Dadas la funciones f y g, hallar $g \circ f$ y calcular $(g \circ f)(-1)$.

(i) $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^3$ y $g : \mathbb{R} \to \mathbb{R}$, definida por $g(x) = \dfrac{5x}{x^2+1}$.

(ii) $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = 2\,x - 1$ y $g : \mathbb{R} \to \mathbb{R}$, definida por $g(x) = (x+6)^3$.

(iii) $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^3 - 1$ y $g : \mathbb{R} \to \mathbb{R}$, definida por $g(x) = (-x-1)^2$.

(iv) $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x + 2$ y $g : \mathbb{R} \to \mathbb{R}$, definida por $g(x) = (-3\,x + 4)^2$.

17. Determinar si las siguientes funciones son inyectivas, sobreyectivas o biyectivas. Para las que sean biyectivas, hallar la inversa y para las que no sean biyectivas, hallar la imagen.

(i) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 12x^3 - 5$

(ii) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 12x^2 - 5$

(iii) $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x + y$

(iv) $f : \mathbb{R} \to \mathbb{R}^3$, $f(x) = (2x, x^2, x - 7)$

(v) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \begin{cases} 2x & \text{si } x < 6 \\ x + 6 & \text{si } x \geq 6 \end{cases}$

(vi) $f : \mathbb{N} \to \mathbb{N}$, $f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ n + 1 & \text{si } n \text{ es impar} \end{cases}$

(vii) $f : \mathbb{N} \to \mathbb{N}$, $f(n) = \begin{cases} n - 1 & \text{si } n \text{ es par} \\ 2n & \text{si } n \text{ es impar} \end{cases}$

(viii) $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(a, b) = 3a - 2b$

(ix) $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = \begin{cases} a + 1 & \text{si } a \text{ es par} \\ a - 1 & \text{si } a \text{ es impar} \end{cases}$

18. (a) Dadas las funciones

$$f : \mathbb{N} \to \mathbb{N}, \quad f(n) = \begin{cases} \frac{n^2}{2} & \text{si } n \text{ es divisible por 6} \\ 3n + 1 & \text{en otro caso} \end{cases} \; ; \; g : \mathbb{N}\times\mathbb{N} \to \mathbb{N}, \quad g(n, m) = n(m+1)$$

calcular $(f \circ g)(3, 4)$, $(f \circ g)(2, 5)$ y $(f \circ g)(3, 2)$.

(b) Dadas las funciones

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \begin{cases} x^2 & \text{si } n \leq 7 \\ 2x - 1 & \text{si } x > 7 \end{cases} \; ; \qquad g : \mathbb{N} \to \mathbb{R}, \quad g(n) = \sqrt{n}$$

hallar todos los $n \in \mathbb{N}$ tal que

(i) $(f \circ g)(n) = 13$

(ii) $(f \circ g)(n) = 15$

19. Hallar $f \circ g$ en los casos

(i) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x^2 - 18$, $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x + 3$

(ii) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 3$, $g : \mathbb{R} \to \mathbb{R}$, $g(x) = 2x^2 - 18$

(iii) $f : \mathbb{N} \to \mathbb{N}$, $f(n) = \begin{cases} n - 2 & \text{si } n \text{ es divisible por 4} \\ n - 1 & \text{en otro caso} \end{cases}$, $g : \mathbb{N} \to \mathbb{N}$, $g(n) = 4n$

(iv) $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \quad f(x) = (x + 5, 3x), \quad g : \mathbb{N} \to \mathbb{R}, \quad g(n) = \sqrt{n}$

20. Hallar dos funciones $f : \mathbb{N} \to \mathbb{N}$ y $g : \mathbb{N} \to \mathbb{N}$ tales que $f \circ g = id_{\mathbb{N}}$ y $g \circ f \neq id_{\mathbb{N}}$, donde $id_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ denota la función identidad.

21. (a) Probar que una función $f : A \to B$ es inyectiva si y sólo si para todo $y \in B$, si $f^{-1}(\{y\}) \neq \emptyset$, entonces $f^{-1}(\{y\})$ tiene un elemento.

    (b) Sea $f : E \to F$ y $X \subseteq E$ e $Y \subseteq E$. Probar que si f es inyectiva entonces $f(X \cap Y) = f(X) \cap f(Y)$.

22. (a) Describir el intervalo $(4, 9)$ por medio de una desigualdad utilizando valor absoluto.

    (b) Idem para el conjunto $(-\infty, -2] \cup [4, +\infty)$.

    (c) Resolver las siguientes desigualdades y expresar la solución utilizando valor absoluto:
    (i) $x^2 + 5x > 0$, (ii) $x^2 - 2x < 0$, (iii) $x^2 - x - 2 > 0$, (iv) $x^2 + 5x + 7 < 0$.

    (d) Resolver las siguientes desigualdades:

    (i) $\dfrac{x}{x^2 + 4} > 0$, (ii) $\dfrac{x + 1}{x - 3} > 0$,

    (iii) $\dfrac{x}{x^2 - 4} \geq 0$, (iv) $\dfrac{x^2 - 1}{x^2 - 3x} < 0$.

23. (a) Determinar el conjunto de soluciones de la siguiente inecuación. Expresarlo en forma de intervalo.

$$x + 4 \leq 2x^2 - x - 4.$$

    (b) Resolver la siguiente ecuación y verificar la solución:

$$\frac{x - 5}{2} + \frac{2x - 1}{2 + 3x} = \frac{5x - 1}{10} - \frac{7}{5}.$$

24. Sean $a, b \in \mathbb{R}$ tales que $0 < a < b$. Demostrar que:

    (a) $0 < \dfrac{1}{b} < \dfrac{1}{a}$.

    (b) $a^2 < b^2$.

25. Sean $a, b \in \mathbb{R}$ tales que $a < b < 0$. Demostrar que:

    (a) $\dfrac{1}{b} < \dfrac{1}{a} < 0$.

    (b) $b^2 < a^2$.

26. Sea $A = \{x \in \mathbb{R} : (|2x - 3| - 1)(x + 3) \leq 0\}$.

    (a) Representar gráficamente el conjunto A.

    (b) ¿ Es acotado inferiormente ?

    (c) Indicar una cota superior y hallar el supremo de A.

27. Decir si A es acotado superior y/o inferiormente. En caso afirmativo dar dos cotas superiores y/o inferiores. ¿ Tiene primer y/o último elemento ?

    (a) $A = \left\{ x \in R \ : \ \dfrac{3 - | \, x - 1 \, |}{x - 1} \ \geq \ 2 \right\}$

(b) $A = \left\{ x \in R \ : \ \dfrac{2}{1-x} \ < \ \dfrac{x+1}{2} \right\}$

(c) $A = \left\{ x \in R \ : \ \dfrac{3}{2-x} \ < \ \dfrac{x+2}{3} \right\}$

28. (a) Dado el conjunto $A = \left\{ x \in \mathbb{R} \ : \ x + 3 - \dfrac{9x}{2x+3} \ \geq \ 0 \right\}$.
Decir si A es acotado inferiormente. En caso afirmativo indicar el ínfimo de dicho conjunto. ¿ Tiene A primer elemento? Justificar.

(b) Hallar, si existen, los valores reales de x para los cuáles se verifique :

(i) $| -x-1| \ + \ |x+2| \ > \ 5$

(ii) $\dfrac{2-3x}{|\,3-2x\,|} \ \geq \ 1$

(iii) $\dfrac{3-4x}{|\,4-3x\,|} \ \geq \ 1$

(iv) $\left| x + \dfrac{1}{2} \right| \geq -2x + 3$

(v) $\left| x + \dfrac{3}{2} \right| \geq 5 - 2x$

29. Decir si las siguientes afirmaciones son verdaderas o falsas. Justificar la respuesta, con demostración o contraejemplo, según corresponda:

(a) $\sqrt{(x-3)^2} = x - 3 \quad , \quad x \in \mathbb{R}$.

(b) Si q es un número racional tal que $2 \cdot q^2 \in \mathbb{N}$ entonces $q \in \mathbb{N}$.

(c) Si $y < b < 0$ entonces $y^2 > b \cdot y > b^2$.

(d) $\sqrt{x^2 - 6x + 9} + \sqrt{x^2 + 6x + 9} = -2x$, $\forall\, x \in R$, $x < -3$.

(e) Si $x \in R$, $y > 0$, entonces $x - y < x + y$.

30. (a) Probar que cualquiera que sea $x \in \mathbb{R}$, $x \neq 0$ se verifica que $\dfrac{|\,x - |x|\,|}{x} \leq 0$.

(b) Si $a,\ b \in \mathbb{R}$, ¿es cierto que $a^2 = b^2 \implies a^5 = b^5$?

(c) Sean $x,\ y \in \mathbb{R},\ x \neq 0,\ y \neq 0$ tales que $x + y = 1$. Probar que

$$\left(\frac{1}{x} - 1 \right) \cdot \left(\frac{1}{y} - 1 \right) = 1 \ .$$

31. (a) Hallar, si existen, los valores reales de x para los cuales se verifique:

$$|2\,x + \frac{1}{2}| \geq -x + 3.$$

(b) Dado el conjunto $A = \{x \in \mathbb{R} : 1 - \dfrac{x-1}{3+x} \geq 0\}$, decir si A es acotado inferiormente. En caso afirmativo, indicar el ínfimo. ¿ Tiene A primer elemento ? Justificar la respuesta.

32. Decir si las siguientes proposiciones son verdaderas o falsas. Justificar las respuestas, con demostración o contraejemplo, según corresponda.

(a) Si a y b son números irracionales y $a+b$ es racional, entonces $2\,a-b$ es irracional.

(b) Si $a<b$ implica $a\,c<b\,c$ para todo a, b, $c\in\mathbb{R}$.

(c) La única solución de la ecuación $|x-1|-|x|=0$ es $x=\dfrac{1}{2}$.

33. Demostrar, aplicando el principio de inducción:

(a) $2^n\geq 1+n$, para todo $n\geq 1$.
$(2^{k+1}=2^k\cdot 2\geq(1+k)\cdot 2=2+2k>1+(k+1))$.

(b) $3^{2n}-1$ es divisible por 8, para todo $n\geq 1$.
$(3^{2(k+1)}-1=3^{2k}\cdot 3^2-1=3^{2k}\cdot 3^2-3^2+3^2-1=3^2(3^{2k}-1)+(3^2-1)=3^2(3^{2k}-1)+8)$.

(c) $2n^3-3n^2+n+31\geq 0$.

(d) $n!\geq 2^n$, para todo $n\geq 4$.

34. Demostrar, aplicando el principio de inducción, que las siguientes igualdades y propiedades valen para todo $n\in\mathbb{N}$: Indicar el cuarto término y hallar la suma de los seis primeros sumandos.

(a) $\left(2-\dfrac{1}{2}\right)+\left(2-\dfrac{2}{2^2}\right)+\cdots+\left(2-\dfrac{n}{2^n}\right)=(2n-2)+\dfrac{n+2}{2^n}$.

(b) $\left(\dfrac{1}{2}-1\right)+\left(\dfrac{1}{2}-3\right)+\left(\dfrac{1}{2}-3^2\right)+\ldots+\left(\dfrac{1}{2}-3^{n-1}\right)=\dfrac{n+1-3^n}{2}$.

(c) $\left(\dfrac{1}{3}-1\right)+\left(\dfrac{1}{3}-2\right)+\left(\dfrac{1}{3}-2^2\right)+\ldots+\left(\dfrac{1}{3}-2^{n-1}\right)=\dfrac{n}{3}-(2^n-1)$.

(d) $3+9+\ldots+3^n=\dfrac{3(3^n-1)}{2}$

(e) $(-1)^1+(-1)^2+(-1)^3+\cdots+(-1)^n=\dfrac{(-1)^n-1}{2}$

(f) $1\cdot 2+3\cdot 4+5\cdot 6+\ldots+(2n-1)\cdot 2n=\dfrac{n(n+1)(4n-1)}{3}$

(g) $1+4+7+\ldots+(3n-2)=\dfrac{n(3n-1)}{2}$

(h) $5+9+13+\ldots+(4n+1)=n(2n+3)$

(i) $3+7+11+\ldots+(4n-1)=n(2n+1)$

(j) $2+6+18+\ldots+2\cdot 3^{n-1}=3^n-1$

(k) $\dfrac{1}{2}+\dfrac{1}{4}+\dfrac{1}{8}+\ldots+\left(\dfrac{1}{2}\right)^n=1-\left(\dfrac{1}{2}\right)^n$

(l) $7+7^2+7^3+\ldots+7^n=\dfrac{7(7^n-1)}{6}$

(m) $1^3+2^3+3^3+\ldots+n^3=\left(\dfrac{n(n+1)}{2}\right)^2$

(n) $\left(1+\dfrac{1}{1}\right)\cdot\left(1+\dfrac{1}{2}\right)\cdot\left(1+\dfrac{1}{3}\right)\cdot\ldots\cdot\left(1+\dfrac{1}{n}\right)=n+1$

(o) $3^{2n+1}+1$ es divisible por 4

(p) $2^{3n}-1$ es divisible por 7

(q) 5^n-1 es divisible por 4

(r) $4^{2n} - 1$ es divisible por 3

(s) $(5 - \frac{1}{2}) + (5 - \frac{2}{2^2}) + \ldots + (5 - \frac{n}{2^n}) = (5\,n - 2) + \frac{n+2}{2^n}$

(t) $\frac{1}{6} + \frac{5}{6^2} + \frac{5^2}{6^3} + \cdots + \frac{5^{n-1}}{6^n} = 1 - \left(\frac{5}{6}\right)^n$

(u) $1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1}\, n^2 = (-1)^{n-1}\, \frac{n\,(n+1)}{2}$

(v) $\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}$

(w) Probar que si $2 + 5 + 8 + \ldots + (3n-1) = \frac{(3n+4)(n+1)}{2}$ es válida para $n = k$, entonces es válida para $n = k + 1$. Sin enbargo, la fórmula no vale.

(x) $1 \cdot 2 + 2 \cdot 3 + \ldots + (n-1) \cdot n = \frac{(n-1) \cdot n \cdot (n+1)}{3}$

(y) $1^2 - 2^2 + 3^2 - 4^2 + \cdots + (2n-1)^2 - (2n)^2 = -n \cdot (2n+1)$.

(z) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2 \cdot (2n^2 - 1)$.

(α) $1 + 2\left(\frac{1}{2}\right) + 3\left(\frac{1}{2}\right)^2 + \ldots + n\left(\frac{1}{2}\right)^{n-1} = 4 - \frac{n+2}{2^{n-1}}$

35. Con n tres y n cuatros, $n \geq 2$, formamos los números $A_n = 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}$ y $B_n = 4^{4^{\cdot^{\cdot^{\cdot^{4}}}}}$. Probar por inducción que $A_n > 2B_{n-1}$. En particular, $A_n > B_{n-1}$.

36. Con 8 cincos y 5 ochos formamos los números $5^{5^{\cdot^{\cdot^{\cdot^{5}}}}}$ y $8^{8^{\cdot^{\cdot^{\cdot^{8}}}}}$. ¿Cuál de los dos números es el mayor? (Tomar A_n la potencia con n cincos y B_n la potencia con n ochos y probar por inducción que $A_n > 2B_{n-3}$, $n \geq 4$).

37. La siguiente demostración por inducción parece probar la siguiente afirmación:
Todo conjunto de n rectas, $n \geq 2$, en el plano no paralelas dos a dos se cortan en un punto.
Como esto es claramente falso, ¿dónde está el error ?

Demostración. La afirmación es verdadera para $n = 2$, ya que suponemos que no son paralelas.
Supongamos que es verdadera para cualquier conjunto de $n - 1$ rectas. Sea $L = \{a, b, c, d, \ldots\}$ un conjunto de n rectas en el plano, no paralelas dos a dos. Si suprimimos la recta c nos queda un conjunto L' de $n-1$ rectas no paralelas dos a dos. Por la hipótesis inductiva, existe un punto P por el que pasan todas las rectas de S'. En particular, P es el punto de intersección de a y b. Ahora reintegramos c y eliminamos la recta d para obtener un conjunto S'' con $n - 1$ rectas. Usando de nuevo la hipótesis de inducción, todas estas rectas se cortan en un punto P'. Razonando como antes, P' debe ser el punto de intersección de a y b. En consecuencia $P = P'$. Pero entonces c pasa por P (por la elección de P) y por lo tanto todas las n rectas pasan por P. □

38. Hallar el cociente y el resto de dividir $a = n + 3$ por $b = n^2 + 1$ ($n \in \mathbb{N}$). (Ayuda: Observar que si $n \geq 3$, $n^2 + 1 > n^2 \geq 3n > n + 3$).

39. Si el resto de la división de a por 18 es 5, hallar:

(i) El resto de dividir $4a + 1$ por 9.

(ii) El resto de dividir $a^2 + 7$ por 36.

(iii) El resto de dividir $7a^2 + 12$ por 28.

(iv) El resto de dividir $1 - 3a$ por 27.

40. (a) Hallar, utilizando el algoritmo de Euclides, el máximo común divisor de -187 y 77. Expresarlo como combinación lineal de ellos.

(b) ¿ Cuál es la condición necesaria y suficiente para que la ecuación $-187x + 77y = 22$ tenga solución entera ? En caso de ser posible, hallar una de ellas.

(c) Demostrar que si $n \in \mathbb{N}$, n impar, entonces $n(n^4 - 1)$ es divisible por 120.

41. Decidir la verdad o falsedad de las siguientes afirmaciones. Justificar la respuesta.

(a) Si el producto de dos números enteros es par entonces uno de los dos números es par.

(b) Un número es primo si y solo si es impar.

(c) Si $a \mid b \cdot c$ entonces $a \mid b$ ó $a \mid c$.

(d) Si $a \mid b$ y $a \mid c$ entonces $a \mid b + c$.

(e) Si $b \in Z$ y $5 \mid b^4$ entonces $5 \mid b^2 + 10$.

42. (a) Decir cuál es el m.c.d. de dos enteros a y b tales que $9\,a + 42\,b = 18$, si no son relativamente primos y uno de ellos no es divisible por 3.

(b) Demostrar que si n es un número entero par , entonces $11\,n^3 - 44\,n$ es divisible por 264.

(c) Demostrar que si n es un número entero entonces $n^6 - n^4$ es divisible por 12.

43. Hallar los enteros a y b sabiendo que al dividirlos por su máximo común divisor se obtienen cocientes 20 y 17 respectivamente y que la suma de su máximo común divisor y su mínimo común múltiplo es igual a 3410.

44. Decidir la verdad o falsedad de las siguientes afirmaciones. Justificar la respuesta.

(a) Si un número entero es divisible por 21 entonces es divisible por 7.

(b) Si $a\,, b \in Z$ y $a \mid b^2$ entonces $a \mid b$.

(c) Si $u\,, v \in Z$, $7\,u + 8\,v = 10$, v impar y $(u, 5) = 1$ entonces u y v son relativamente primos.

45. (a) Probar que todo número primo $p > 3$ es de la forma $p = 6n + 1$ ó $p = 6n + 5$, $n \in \mathbb{Z}$.

(b) Probar que si p es un número primo, $p > 3$, el resto de dividir p^2 por 12 es 1.

46. Probar que si $2^n - 1$ es primo, entonces n es primo (Ayuda: tener en cuenta que $a^n - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{n-1})$).

47. Un problema abierto es saber si existen infinitas parejas de números primos de la forma n, $n+2$. Por ejemplo, 3 y 5, 5 y 7, 29 y 31, etc. Probar que no existen infinitas ternas de primos de la forma n, $n + 2$, $n + 4$. (Ayuda: considerar la división de n por 3).

48. Probar que para todo entero positivo n existe un primo p tal que $n < p < n!$. (Observar que existe un primo p tal que $p \mid n! - 1$).

49. Un número natural se dice *perfecto* si es la suma de sus divisores positivos propios. Por ejemplo, $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$. Probar que si 2^{n-1} es primo, entonces $2^{n-1} \cdot (2^n - 1)$ es perfecto.

50. Decidir la verdad o falsedad de las siguientes afirmaciones. Justificar las respuestas, con demostración o contraejemplo, según corresponda.

    (a) Si el producto de dos números enteros es un cuadrado entonces uno de ellos es un cuadrado.

    (b) Si $a \mid b^2$ entonces $a^2 \mid b^2$, para todo entero a, b.

    (c) Si $a \mid b^3$ entonces $a^3 \mid b^3$, para todo entero a, b.

    (d) Si a, b son números irracionales y $a + b$ es racional entonces $a - b$ es irracional.

    (e) Si el resto de dividir a un número entero a por 9 es 4, entonces el resto de dividir a $8a - 1$ por 9 es 4.

    (f) Si $7 \mid b^5$ entonces $7 \mid (b^3 + 21a)$.

    (g) Si a y b son números enteros, uno de ellos impar, entonces $2 \mid a - b$ si y sólo si $2 \mid a^3 - b^3$.

51. Probar que la suma de 4 enteros consecutivos no es un cuadrado.

52. (i) Probar que $3 \mid a^2 + b^2$ si y sólo si $3 \mid a$ y $3 \mid b$.

    (ii) Probar que $7 \mid a^2 + b^2$ si y sólo si $7 \mid a$ y $7 \mid b$.

    (iii) Probar que $5 \mid a^2 + b^2$ si y sólo si $5 \mid a - 2b$ y $5 \mid a - 3b$.

    (iv) Probar que no vale que si $5 \mid a^2 + b^2$ entonces $5 \mid a$ ó $5 \mid b$.

53. Probar que cualesquiera que sean $a, b, c \in \mathbb{Z}$, $a^2 + b^2 + c^2 + 1$ no es divisible por 8.

54. (a) ¿ Cómo son los divisores de 22^{6081} ?

    (b) Determinar el número de divisores de $14^3 \cdot 18^2$ y de $3 \cdot 28^4$.

    (c) Probar que si a, b, $d \in Z$, $a \neq 0$, y $a^2 = d \cdot b^2$, entonces d es un cuadrado en Z.

    (d) Sea a un entero par. Probar que $2a^2 + 16a - 2$ no es un cuadrado.

    (e) Hallar el menor número natural impar que tiene exactamente 6 divisores positivos.

    (f) Hallar el menor natural n, tal que $1200 \cdot n$ es un cubo.

    (g) ¿ Cuántos divisores tiene el número 648 ?

    (h) Hallar la suma de los divisores positivos de $2^4 \cdot 5^{123}$ y de $7^{435} \cdot 8^{23}$.

55. Hallar el menor entero positivo n tal que $\dfrac{n}{2}$ es un cuadrado y $\dfrac{n}{3}$ es un cubo.

56. Sea $2\mathbb{N}$ el conjunto de los números naturales pares. Diremos que un número a en $2\mathbb{N}$ es irreducible si no existen números $b, c \in 2\mathbb{N}$ tal que $a = bc$.

    (i) Probar que si n es un número impar, entonces $2n \in 2\mathbb{N}$ y es irreducible. Recíprocamente, todo número irreducible en $2\mathbb{N}$ es de la forma $2k$, k impar.

    (ii) Probar que todo número $a \in 2\mathbb{N}$ se factoriza en un producto de irreducibles en $2\mathbb{N}$.

    (iii) Probar que esta factorización no es única.

    (iv) Probar que la propiedad "si p es irreducible y $p \mid ab$, entonces $p \mid a$ ó $p \mid b$" no vale en $2\mathbb{N}$.

57. (a) Determinar el valor de b sabiendo que $13_{(b)} \times 15_{(b)} = 243_{(b)}$, y hallar en base 10 el número x tal que $x_{(b)} = 13_{(b)} + 15_{(b)}$.

    (b) Idem para $12_{(b)} \times 13_{(b)} = 211_{(b)}$, y $x_{(b)} = 12_{(b)} + 13_{(b)}$.

    (c) Idem para $13_{(b)} \times 14_{(b)} = 230_{(b)}$, y $x_{(b)} = 13_{(b)} + 14_{(b)}$.

58. Determinar justificando la respuesta, si el número $c = 3211_{(4)}$ es primo.

59. (a) Sea $n \in \mathbb{N}$, $n \geq 5$. Hallar $(10^n, 96)$.
    (b) Indicar el número de divisores positivos de 96.
    (c) Determinar la base b tal que $[14_{(b)}]^2 = 232_{(b)}$.

60. (a) (i) Demostrar que para todo $m \in \mathbb{Z}$, $2^2 \mid m^2(m^2-1)$ y $3 \mid m^2(m^2-1)$.
    (ii) De (i) deducir que $12 \mid m^2(m^2-1)$. Justificar la respuesta.
    (b) Hallar todos los pares de números enteros positivos a y b tales que $(a,b) = 20$ y $[a,b] = 120$.

61. (a) Si a y b son números enteros tales que $(a,b) = 1$ y $(a,3) = 1$, demostrar que $9\,a$ y $a + 3\,b$ son relativamente primos.
    (b) Hallar dos fracciones con denominador 11 y 13 tales que su suma sea $\dfrac{67}{143}$.
    (c) Demostrar que la suma de dos números naturales consecutivos y la suma de sus cuadrados, son números relativamente primos.

62. (a) Probar que para todo $a \in \mathbb{Z}:\ a(a^4-1)$ es múltiplo de 5.
    (b) Si a y b son dos enteros relativamente primos, probar que $(a, a+b) = 1$.

63. (a) Demostrar que $11a^7 - 891a^3$ es divisible por 440.
    (b) Deducir cuál es el máximo común divisor de u y v sabiendo que $56u - 84v = 28$.

64. (a) Si a y b son dos números enteros tales que $(a,b) = 1$ y $(a,6) = 2$, demostrar que la fracción $\dfrac{9a}{a+3b}$ es irreducible.
    (b) Demostrar que si a y b son dos enteros tales que $(a,b) = 1$ y $a \mid b \cdot c$, entonces $a \mid c$.

65. (a) Hallar todos los enteros no nulos a y b tales que $770a^4 = b^5$.
    (b) Decir cuáles son todos los números enteros que se pueden escribir en la forma $82x + 24y$, x, $y \in Z$. ¿28 se puede escribir así? ¿Por qué?

66. Para qué números naturales n se tiene que $n+1 \mid n^2+1$? (Se sabe que $n+1 \mid n^2-1$).

67. Hallar todos los números enteros $a \neq 3$ para los cuales $a-3 \mid a^3-3$ (expresar $a^3 - 27 = (a-3)(a^2+3a+9)$).

68. Probar que para todo $a \in \mathbb{Z}$, si a es impar entonces $(a^3-a)(a^2-9)$ es divisible por 80.

69. Probar que si k es impar y $n \in \mathbb{N}$, $2^{n+2} \mid k^{2^n} - 1$ (inducción sobre n).

70. Probar que $56 \mid 13^{2n} + 28n^2 - 84n - 1$ (Ayuda: Probar primero por inducción que $7 \mid 13^{2n} - 1$ y $7 \mid 13^{2n} - 1$).

71. Usar el principio de inducción para probar que
    (a) $n^2 + 3n$ es divisible por 2.
    (b) $n^3 + 3n^2 + 2n$ es divisible por 6.

72. Hallar $(2n+1, 9n+4)$, $n \in \mathbb{N}$.

73. Hallar $(2n-1, 9n+4)$, $n \in \mathbb{N}$.

Solución. Sea $d = (2n-1, 9n+4)$. Entonces $d|2n-1$ y $d|9n+4$. Luego $d|18n-9$ y $d|18n+8$, y por lo tanto, $d|17$. En consecuencia, $d = 1$ ó $d = 17$.

¿ Para qué valores de n es $d = 1$ y para qué valores $d = 17$?

Observemos que si $17|2n-1$, entonces $17|9n+4$. En efecto, si $17|2n-1$, entonces $2n-1 = 17k'$, con k' impar, es decir, $2n-1 = 17(2k+1) = 17 \cdot 2k + 17$, con $k \in \mathbb{N} \cup \{0\}$. Luego $n = 17k+9$. Entonces $9n+4 = 9(17k+9)+4 = 17(9k+5)$.

Entonces, basta averiguar cuándo $17|2n-1$. Pero siguiendo la cuenta anterior, es fácil ver que $17|2n-1$ si y sólo si $n = 17k+9$, $k \in \mathbb{N} \cup \{0\}$.

En conclusión, $d = 17$ para $n = 17k+9$, $k \in \mathbb{N} \cup \{0\}$, y $d = 1$ para los restantes valores de n.

74. Hallar $(36n+3, 90n+6)$, $n \in \mathbb{N}$.

75. Hallar $(2n+3, n+7)$, $n \in \mathbb{N}$.

76. (a) Hallar $(a+b, ab)$, para a, b enteros relativamente primos.

(b) Dados dos enteros a, b cualesquiera, hallar $(a+b, [a,b])$ (aplicar (a) a $x = \dfrac{a}{(a,b)}$, $y = \dfrac{b}{(a,b)}$).

(c) Probar que si $(a,b) = 1$ y ab es un cuadrado, entonces a es un cuadrado y b es un cuadrado.

77. (a) Si $(a,b) = p^3$, p primo, ¿ cuánto vale (a^2, b^2) ?. (Rta.: p^6)

(b) Si $(a,b) = 8$, ¿ cuáles son los posibles valores de (a^3, b^4) ?. (Rta.: 8^3 y 8^4)

78. Decir si son verdaderas o falsas. En cada caso probar la propiedad o dar un contraejemplo.

(a) Si $(a,b) = d$ entonces $(a, mb) = md$.

(b) Si $a \mid bc$ y $a \nmid b$, entonces $a \mid c$.

(c) Si $(a,b) = d$, entonces $(a^3, b^3) = d^3$.

79. Probar que si $(a,b) = 1$ y $c \mid a$, entonces $(c,b) = 1$.

80. Probar que si $a \mid bc$ y $(a,b) \mid c$, entonces $a \mid c^2$.

81. Determinar, justificando la respuesta, si el número $c = 3211_{(4)}$ es primo.

82. (a) Utilizando propiedades de números complejos, representar la región determinada por:

$$z \cdot \overline{z} \leq \left|-2\sqrt{3} + 2\,i\right|, \ |Im\, z| \leq 1 \quad \text{y} \quad \pi \leq arg(\, z \cdot (150 + 150\,i)) \leq \frac{7}{4}\pi.$$

¿Pertenecen a la región los números $-1 - \dfrac{1}{\sqrt{3}}\,i$ y $-\dfrac{1}{\sqrt{3}} + i$? Justificar.

(b) Sean $z_1 = -1 - \sqrt{3}\,i$ y $z_2 = -1 + \sqrt{3}\,i$. Hallar $n \in \mathbb{N}$ tal que $\left(\dfrac{z_1}{z_2}\right)^n$ sea un número real positivo.

83. Representar en el plano complejo el siguiente conjunto :

$$A = \left\{ z \in C \ : \ \frac{\pi}{3} \leq arg\ \frac{z}{i} \leq \frac{7}{6}\,\pi \quad \mathbf{y} \quad |z|^2 < 16 \right\}.$$

84. Representar en el plano complejo la región determinada por

$$\left|\left(-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}\ i\right)^{18}\cdot(-2+5\ i)^2\cdot z\right| \leq \left|\frac{87}{-3i}\right| \quad \text{y} \quad -\frac{5}{3}\pi < arg\ \frac{1}{\left(-\sqrt{3}-i\right)z} \leq -\frac{3}{2}\pi$$

85. (a) Demostrar, por inducción, que la siguiente igualdad vale para todo $n \in N$:

$$(1+i)^n = 2^{\frac{n}{2}}\ (cos\ \frac{n\,\pi}{4} + i\ sen\ \frac{n\,\pi}{4}).$$

(b) Utilizando propiedades del módulo de números complejos, representar en el plano complejo el conjunto :

$$A = \left\{ z \in C\ :\ \left|\frac{(-\sqrt{3}+i)^6\cdot z^2}{64\ i}\right| \leq 4\ \text{ y }\ |\ Im\ z\ | < 1 \right\}.$$

86. (a) Sea $z \in C$ tal que $|z| = 5$ y $arg\ z = \frac{5}{6}\,\pi$. Hallar, aplicando propiedades, el módulo y el argumento principal de:

$$z\cdot\left(\frac{\sqrt{3}-i}{-1+i}\right)^{50}.$$

(b) Hallar todos los valores de $z \in C$ tales que: $z^5 = (5\,i^{23} - 3\,i^{-23})\cdot z^2$.
Expresarlos en forma binómica y representarlos en el plano complejo.

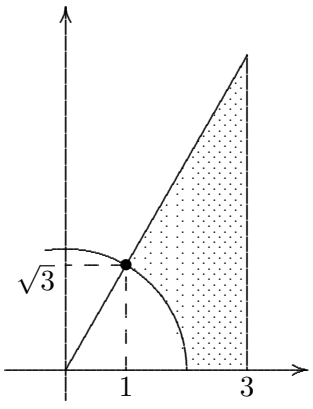
87. Verificar que $\epsilon = cos\ \frac{8}{15}\,\pi + i\ sen\ \frac{8}{15}\ \pi$ es raíz primitiva de la unidad de orden 15.
¿Como se obtiene el conjunto G_{15} a partir de ϵ ?

88. (a) Sea $\varepsilon = cos\ \frac{2}{3}\pi + i\,sen\ \frac{2}{3}\pi$ una raíz primitiva de la unidad de orden 3.
(i) Hallar, a partir de ε, todas las raíces de la unidad de orden 3.
(ii) Hallar el módulo y el argumento principal de $[\varepsilon\,(1-\sqrt{3}\ i)]^{22}$

(b) Hallar los valores de $z \in \mathbb{C}$ que verifiquen la siguiente igualdad,

$$z^4 = \frac{2-2\sqrt{3}\ i}{-1+\sqrt{3}\ i}.$$

(c) Indicar las condiciones que verifican los $z \in \mathbb{C}$ para que pertenezcan a la región indicada.



89. (a) Sea $\epsilon = 1cis(\frac{2}{3}\pi)$ una raíz primitiva de orden 3 de la unidad. Obtener a partir de ϵ las raíces cúbicas de la unidad.

    (b) Utilizando el inciso (a) resolver la ecuación $x^3 + 27 = 0$. Expresar el resultado en forma binómica y representar gráficamente.

90. (a) Sea $\varepsilon = cos\ \frac{\pi}{3} + i\, sen\ \frac{\pi}{3}$ una raíz primitiva de la unidad de orden 6.

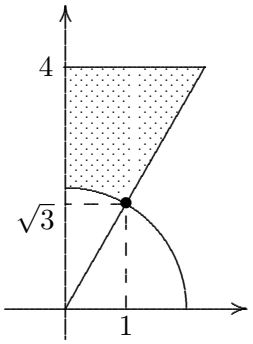
    (i) Hallar, a partir de ε, todas las raíces de la unidad de orden 6.

    (ii) Hallar el módulo y el argumento principal de $[\varepsilon\,(-\sqrt{3}+\,i)]^{29}$

    (b) Hallar los valores de $z \in \mathbb{C}$ que verifiquen la siguiente igualdad,

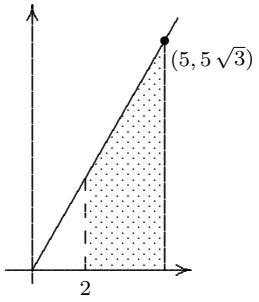
$$z^3 = \frac{3\sqrt{3} - 3\,i}{-\sqrt{3} + \,i}.$$

    (c) Indicar las condiciones que verifican los $z \in \mathbb{C}$ para que pertenezcan a la región indicada.

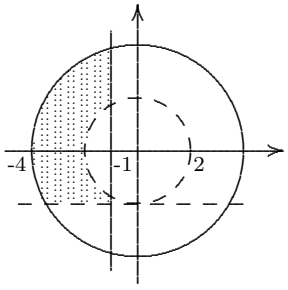


91. Escribir las condiciones que deben verificar los $z \in \mathbb{C}$ para que pertenezcan a la región indicada en cada caso.

(a)



(b)



92. Resolver las siguientes ecuaciones.

    (a) $(1-i)^8\, z = (2\,i - 1)\, z^2$.

    (b) $|4 + 3\,i|\, z - (1 + 2\,i)(1 - i) = i\, z + 3 + i^{347}$.

93. Sea $z = \dfrac{1}{3i}(i^{35} - 2i^{-35})$. Hallar $\sqrt[4]{z}$ y representar gráficamente.

94. Representar en el plano complejo la región determinada por los $z \in \mathbb{C}$ tales que:

$$\text{(a)} \begin{cases} |z| \leq 3 \\ -3 \leq Im\, z < 1 \\ |arg\, z| \leq \dfrac{\pi}{2} \end{cases}, \qquad \text{(b)} \begin{cases} Re\, z \leq 0 \\ z \cdot Re\, z + Im\,(\overline{z}) = 4 \end{cases}.$$

95. (a) Hallar los números complejos z que verifiquen:

$$-8\,i^{-10} - \frac{-3+5\,i}{5+3\,i}\,z = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\,i\right)^{22} z + i^{65}\,z^3.$$

(b) Representar en el plano complejo la región determinada por los $z \in \mathbb{C}$ tales que:

$$|z| \geq 5;\ \frac{\pi}{4} < arg\, z \leq \frac{3}{2}\pi;\ Re\, z > -6.$$

96. Hallar los números complejos z que verifiquen

(a) $(2-i)\cdot z - z^4 = \left(\dfrac{7-i}{3+i}\right)\cdot z - 256$

(b) $z^2\cdot(1-i) = \dfrac{-8}{z}\cdot(1+i)$

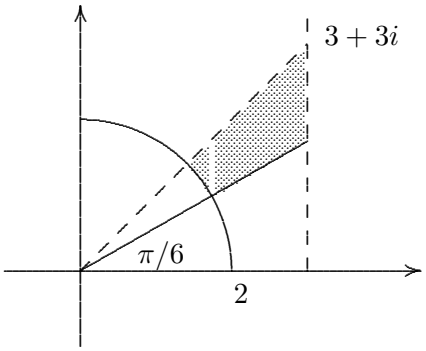
97. (a) Demostrar que si u es raíz n-ésima de la unidad, se verifica:

$$u(u^{n-1} - \overline{u}) + \frac{1}{32}(1-\sqrt{3}i)^9 u + \overline{u}(\overline{u}^{n-1} - u) - 16i^{70}u = 0$$

(b) Sea $z = \dfrac{i^{24} + i^{-24}}{2i}$. Hallar y representar en el plano complejo $\sqrt[4]{z}$.

98. (a) Hallar el conjugado de $1 + \dfrac{i}{1 + \dfrac{i}{1+i}}$

(b) Representar analíticamente



99. Decir si las siguientes afirmaciones son verdaderas o falsas. Justificar la respuesta.

(a) Si u es raíz n-ésima de la unidad entonces $\overline{u}$ es raíz n-ésima de la unidad.

(b) Si v es raíz n-ésima de la unidad entonces $v\cdot(v^{n-1} - \overline{v}) = 1$.

(c) $w = cos\ 8/15\,\pi + i\, sen\, 8/15\,\pi$ es raíz primitiva de la unidad de orden 15.

100. (a) Sea $z = 1 - \dfrac{i}{1+i}$. Determinar la parte real y la parte imaginaria de:

i) $i^{50}\cdot z - \overline{z}$. ii) $z^{10} - i$.

(b) Hallar todos los valores $\omega \in C$ tales que: $\omega\cdot(i - Im\,\overline{\omega}) = 5i$.

(c) Probar que $\epsilon^{100} = -1$, cualquiera sea ϵ raíz primitiva de la unidad de orden 200.

101. Resolver las siguientes ecuaciones.

(a) $\left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\,i\right)^{30} - i^{239}\,z^3 = cos\,\frac{\pi}{6} + i\,sen\,\frac{23}{6}\pi.$

(b) $(1+2\,i)(2-3\,i)\,z - 4_\pi = 3\,z + |3-4\,i|.$

102. (a) Sabiendo que u es raíz $n-$ésima de la unidad, verificar que:

$$u(u^{n-1} - \overline{u}) + \overline{u}(\overline{u}^{n-1} - u) - u(i^{70} + u^{n-1}) = u - 1.$$

(b) Hallar todos los valores de $z \in \mathbb{C}$ que verifiquen la igualdad dada a continuación. Representarlos en el plano complejo:

$$i\,z^3 = \frac{\sqrt{3}}{2}\,i - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}\,i\right)^{14}$$

(c) Indicar el número de raíces primitivas de la unidad de orden 14.

103. Determinar todos los números complejos z que verifican

$$\frac{(1-i)^8 + 2\cdot z^2}{i\cdot z^2} + \frac{3+i}{1-i} = 1 + i^9\cdot z^2$$

104. Determinar y representar en el plano todos los $z \in C$ tales que

$$-\pi/4 \le arg(zi^{46} + iz) \le \pi/2 \quad \text{y} \quad (-1/2)Re\ z \le 1/2 + Im\ z$$

105. (a) Hallar todos los valores de $z \in C$ que verifican

$$i^3\left(\frac{z^3}{i} + 2\right) = (1+i)^4\cdot 2i + 6$$

(b) Probar que si $|z| = 1$, entonces $|z - w| = |1 - w\cdot\overline{z}|$, para todo $w \in C$.

106. (a) Hallar los valores de $z \in \mathbb{C}$ que verifiquen la siguiente igualdad y representarlos en el plano complejo.

$$(1-i)^{10} + z^5 = 32 - 32\ i^{29}.$$

(b) Representar en el plano complejo la siguiente región:

$$|z| < 4, \quad \frac{\pi}{6} < arg\,z \le \frac{2}{3}\pi, \quad Re\,z \le 1.$$

(c) ¿ Es cierto que el número de raíces primitivas de la unidad de orden 14 es 6 ? ¿ Por qué ?

107. (a) Sea $f(X) = X^3 - a\,X^2 + b\,X - 1$. Sabiendo que 1 es raíz de $f(X)$, determinar los coeficientes a y b de modo que estos valores sean las restantes raíces de $f(X)$.

(b) Decir si las siguientes afirmaciones son verdaderas o falsas. Justificar la respuesta.

i) $f(X) = (X^2+1)\cdot(X^2-5)$ es irreducible en $Q[X]$.

ii) $T(X) = X^3 + 3$ es irreducible en $Q[X]$.

108. Hallar un polinomio $f(X)$ de grado 3, con coeficiente principal 3, tal que $f(0) = 5$ y al dividirlo por $X^2 - 2X + 1$ tenga resto $2X - 1$.

109. (a) Determinar los coeficientes a y b de modo que el resto de dividir a $X^3 + bX + a$ por $X^2 + 3X + 1$ sea $3X + 2$.

(b) Hallar las raíces de $f(X) = (X^5 - 8X^4 + 21X^3 - 14X^2 - 20X + 24)(X^2 - 1)$, sabiendo que 2 es raíz múltiple.

¿ Es -1 raíz múltiple ? ¿ Y 1 ?

110. (a) Hallar un polinomio de grado 2 tal que $f(1) = \frac{1}{2}$, $f(-1) = \frac{-15}{2}$, $f(2) = 3$.

(b) Calcular las raíces a, b, c del polinomio $f(X) = X^3 - \sqrt{5}X^2 - 2X + 2\sqrt{5}$, sabiendo que $a + b = 0$.

111. (a) Determinar los coeficientes a y b de modo que el resto de dividir a $X^3 + 2X^2 + aX + b$ por $X^2 + 4X + 1$ sea $7X + 1$.

(b) Hallar las raíces de $f(X) = (X^5 - 4X^4 + 4X^3 + 2X^2 - 5X + 2)(X^2 - 4)$, sabiendo que 1 es raíz múltiple.

¿ Es 2 raíz múltiple ? ¿ Y -2 ?

112. Dados los siguientes polinomios $f(X)$ y la raíz a de $f(X)$, indicar, aplicando la regla de Ruffini, el orden de multiplicidad de a. Hallar todas las raices de $f(X)$.

(a) $P(X) = X^5 - 4X^4 + 3X^3 + 4X^2 - 4X, \quad a = 2.$

(b) $P(X) = X^5 - 2X^4 - 3X^3 + 8X^2 - 4X, \quad a = 1.$

(c) $P(X) = X^5 - 2X^4 - 3X^3 + 8X^2 - 4X, \quad a = 1.$

113. (a) Hallar el valor de a para que el polinomio $f(X) = X^4 - 4aX^3 + 4aX - 1$ sea divisible por $(X - 1)^2$.

(b) Sea $g(X) = 3\,(X^2 - 4)^2\,(X^2 + 9)\,(2X^2 - 6)^2\,(X - 1)$.

(i) Indicar el grado y el coeficiente principal de $g(x)$.

(ii) Escribir al polinomio $g(x)$ como producto de polinomios irreducibles mónicos en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

114. Sean $f(X) \in \mathbb{R}[X]$ y z una raíz compleja de f. Demostrar que z y $\overline{z}$ tienen el mismo orden de multiplicidad. (Sugerencia: si $z = a + b\,i$, entonces $(X - z)(X - \overline{z}) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$).

115. Indicar si las siguientes afirmaciones son verdaderas o falsas, justificando las respuestas y sin realizar cálculos:

(a) Si la descomposición de $f(X)$ en polinomios irreducibles mónicos en $\mathbb{C}[X]$ es

$$(X + 1)^2(X - \sqrt{2})(X - i)^2(X - 3),$$

entonces $f(X)$ tiene coeficientes reales.

(b) El polinomio $X^3 - X^2 + 1$ es irreducible en $\mathbb{R}[X]$.

116. Si $-2i$ es raíz de orden tres y 2 es raíz simple de un polinomio $f(X) \in \mathbb{R}[X]$, ¿Cuáles son sus restantes raíces si el grado de $f(X)$ es 9 y sus términos lineal e independiente son nulos?

117. Sea $f(X) = X^9 - 3X^5 + 2X^2 - X + 12$. Sin calcular las raíces de $f(X)$, determinar la veracidad o falsedad de las siguientes afirmaciones, justificando las respuestas:

(a) $f(X)$ no posee raíces reales.

(b) $f(X)$ tiene exactamente una raíz real negativa.

(c) $f(X)$ tiene exactamente tres raíces complejas no reales.

(d) $f(X)$ tiene por lo menos cuatro raíces complejas no reales.

118. Decir si las siguientes afirmaciones son verdaderas o falsas:

(a) $1/3$ es raíz de $f(X) = X^{1800} - X^{150} + 4$.

(b) El polinomio $f(X) = X^{1700} - 3X^{150} + 1$ tiene raíces reales.

119. (a) Hallar las raíces de $f(X) = 3X^8 - X^7 + 6X^6 - 2X^5 - 15X^4 + 5X^3 - 18X^2 + 6X$ sabiendo que $\sqrt{3}\,i$ y $\dfrac{1}{3}$ son raíces de $f(X)$.
Descomponer a $f(X)$ en producto de polinomios irreducibles mónicos sobre $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$.

(b) Determinar los coeficientes p, q de modo que $X^3 + pX + q$ sea divisible por $X^2 - 4X + 1$.

120. Determinar para qué valor de k, $g(X)$ divide a $f(X)$, si $f(X) = -X^4 + 4X^3 - kX^2 + 7X - 6$ y $g(X) = X - 2$.

121. Expresar los siguientes polinomios como producto de polinomios irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$, sucesivamente:

(a) $X^2 - 1$ (b) $X^2 + 1$
(c) $X^2 - 4X + 2$ (d) $X^3 - 3X$
(e) $X^4 - 4$ (f) $3X^4 + 4X^2$
(g) $X^2 + X + 1$ (h) $aX^2 + bX + c$

122. Si $f(X) = 8(X^4 - 4)^4(X - 3)^2(X - 5i)^7(X + 5i)^7$, hallar la descomposición de $f(X)$ en producto de polinomios irreducibles mónicos sobre $\mathbb{R}$.

123. (a) Sea $f(X) \in \mathbb{Q}[X]$ un polinomio de tercer grado. Probar que $f(X)$ es reducible en $\mathbb{Q}[X]$ si y sólo si $f(X)$ posee una raíz en $\mathbb{Q}$. Todo polinomio de tercer grado en $\mathbb{R}[X]$ es reducible. Dar ejemplos de polinomios de tercer grado en $\mathbb{Q}[X]$ irreducibles.

(b) La siguiente afirmación es falsa: "Si $f(X) \in \mathbb{Q}[X]$ no tiene ninguna raíz en $\mathbb{Q}$ entonces es irreducible". Dar un contraejemplo.

(c) Demostrar que los polinomios de $\mathbb{R}[X]$ irreducibles en $\mathbb{R}[X]$ son de primer y segundo grado (con discriminante negativo), y que los polinomios irreducibles de $\mathbb{C}[X]$ son los de primer grado.

124. Sabiendo que $1 + \sqrt{2}i$ es raíz del polinomio $X^7 - \dfrac{4}{3}X^6 - \dfrac{11}{9}X^5 + \dfrac{52}{9}X^4 - 5X^3 - \dfrac{16}{3}X^2 - X$, factorizarlo sobre $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

125. (a) Hallar un intervalo (a, b) en el cual se encuentren todas las raíces reales de

$$g(X) = 6\,X^4 + 7\,X^3 - 21\,X^2 - 21\,X + 9.$$

(b) Dado $f(X) = \left(X^2 - 2\,X + 3\right)\left(X^6 + \dfrac{7}{6}\,X^5 - \dfrac{7}{2}\,X^4 - \dfrac{7}{2}\,X^3 + \dfrac{3}{2}\,X^2\right)$.

(i) Sin hacer cálculos, indicar cuáles son las raíces de $X^2 - 2X + 3$, sabiendo que $1 - \sqrt{2}\,i$ es raíz. Justificar la respuesta.

(ii) Hallar todas las raíces de $f(X)$. (Ayuda: considerar el inciso (a)).

126. Indicar si las siguientes afirmaciones son verdaderas o falsas. Justificar las respuestas.

(a) El polinomio $f(X) = X^2 - 2$ es irreducible sobre $\mathbb{R}$.

(b) Si v es una raíz $n-$ésima de la unidad, entonces $v^{n-1}(v-1) = 1 - \overline{v}$.

(c) Si $f(X), g(X) \in \mathbb{R}[X]$ y $gr[f(X)] = gr[g(X)] = 3$ entonces $gr[f(X) + g(X)] = 3$.

127. Sea $f(X)$ un polinomio mónico en $\mathbb{R}[X]$ de grado mínimo que tiene a $-2i$ como raíz doble y a 0, $\sqrt{2}$ y $-\sqrt{2}$ como raíces simples. Expresar $f(X)$ factorizado en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

128. (a) Sabiendo que el resto de dividir a $X^3 + 2X^2 - 4X + 8$ por $X^2 - k$ es un polinomio de grado 0, hallar el valor de $k \in \mathbb{Z}$ y el resto.

(b) Sean $f(X)$, $g(X) \in \mathbb{R}[X]$ tales que: $gr\, f(X) = 4$, $-2\,i$ es raiz doble de $f(X)$ y $g(X) = a\,(X^4 - X^2 + 2) + 2\,b\,(X^2 - 1) - c\,(X^4 - 2)$.
Determinar los valores de a, b, $c \in \mathbb{Q}$ para los cuales $f(X) = g(X)$.

129. (a) Acotar las raíces reales del polinomio

$$g(X) = 6X^4 - 7X^3 - 21X^2 + 21X + 9.$$

Indicar cuántas raíces reales negativas posee exactamente este polinomio.

(b) Sin hacer cálculos, indicar cuáles son las raíces de $X^2 - 2X + 2$, sabiendo que $1 + i$ es raiz. Justificar la respuesta.

(c) Hallar todas las raíces de

$$f(X) = (X^2 - 2X + 2)\left(X^4 - \frac{7}{6}X^3 - \frac{7}{2}X^2 + \frac{7}{2}X + \frac{3}{2}\right)$$

(d) Descomponer a $f(X)$ en producto de irreducibles mónicos sobre $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

(e) Determinar los coeficientes a, b de modo que $X^4 + 2X^3 - 3X^2 + aX + b$ sea divisible por $X^2 - 2$.

130. Sea el polinomio: $f(X) = X^6 - \frac{13}{6}X^5 - \frac{53}{6}X^4 + \frac{23}{6}X^3 + \frac{55}{6}X^2 - \frac{5}{3}X - \frac{4}{3}$.

(a) Acotar las raíces reales de $f(X)$.

(b) Hallar todas las raíces de $f(X)$.

131. Sea el polinomio: $f(X) = X^6 + \frac{7}{6}X^5 - 7X^4 - \frac{7}{3}X^3 + 7X^2 + \frac{7}{6}X - 1$.

(a) Determinar un intervalo real en el cual se encuentren todas las raíces reales de $f(X)$.

(b) Hallar todas las raíces de $f(X)$.

132. Hallar todas las raíces del polinomio:

$f(X) = X^7 - \frac{1}{5}X^6 - 2X^5 + \frac{2}{5}X^4 - 13X^3 + \frac{13}{5}X^2 - 10X + 2$,

sabiendo que $\sqrt{2}\,i$ es raíz del mismo.

Escribir a $f(X)$ como producto de polinomios irreducibles mónicos en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

133. Hallar todas las raíces de $f(X) = 9\ X^5 - 6\ X^4 + (1+18i)\ X^3 - 12i\ X^2 + 2i\ X$, sabiendo que admite como factor a $X^2 + 2i$.

134. Sean $f(X) = X^5 - X^2 + iX^2$ y $g(X) = X^6 + 4X^4 - 3X^2 - 18$. Hallar las raíces de $f(X) \cdot g(X)$ sabiendo que $X - \sqrt{3}i$ es factor de $g(X)$. Indicar el orden de multiplicidad de cada una de las raíces.

135. (a) Sabiendo que un polinomio mónico de quinto grado $p(X)$ es tal que $p(0) = 12$ y que $p(X)$ tiene una raíz doble igual a 2, una simple igual a 3 y otra simple igual a 1, decir cuál es la quinta raíz, justificando la respuesta.

(b) Probar que si $p(X)$ es un polinomio con coeficientes reales y z es una raíz compleja de $p(X)$, entonces $\overline{z}$ es también raíz de $p(X)$.

136. Hallar el resto de la división del polinomio $f(X) = X + X^3 + X^9 + X^{27} + X^{81} + X^{243}$ por
(a) $X - 1$. (b) $X^2 - 1$.
(Usar el algoritmo de la división y reemplazar X por 1 y -1).

137. ¿ Para qué número natural n, 0 es una raíz de $f(X) = (X+1)^n + (X-1)^n - 2$? ¿Cuál es su multiplicidad ?

138. Probar que si $f(X)$ y $g(X)$ son polinomios de grado $\leq n$ y tales que para $n+1$ elementos distintos $c_0, c_1, \ldots, c_n$ se tiene que $f(c_i) = g(c_i)$, $i = 0, 1, \ldots, n$, entonces $f(X) = g(X)$.
(Sugerencia: Considerar el polinomio $h(X) = f(X) - g(X)$).

139. Probar que si el polinomio $f(X) = X^3 + pX + q$, $p, q \in \mathbb{R}$, $q \neq 0$, tiene 3 raíces reales entonces $p < 0$.

140. Las raíces c_1, c_2, c_3 del polinomio $f(X) = X^3 + pX + q$ satisfacen $c_3 = \dfrac{1}{c_1} + \dfrac{1}{c_2}$. ¿Qué condición satisfacen los coeficientes p y q ?

141. ¿Qué relación satisfacen los coeficientes del polinomio $f(X) = X^3 + pX^2 + qX + r$ si una de sus raíces es igual a la suma de las otras dos.

142. Sean c_1, c_2, c_3 las raíces del polinomio $f(X) = X^3 + pX^2 + qX + r$. Hallar un polinomio $g(X)$ que tenga raíces c_1c_2, c_1c_3, c_2c_3, y un polinomio $h(X)$ que tenga raíces $c_1 + c_2$, $c_1 + c_3$, $c_2 + c_3$.

143. Sean los dígitos 0, 1, 2, 3, 4, 5, 6.

(a) ¿ Cuántos conjuntos con 4 elementos pueden obtenerse ?

(b) ¿ Cuántos polinomios de 4° grado pueden formarse ?

(c) ¿ Cuántos polinomios de 4° grado con coeficientes distintos pueden formarse ?

(d) ¿ En cuántos de los polinomios hallados en c), el 0 es raíz simple ?

144. (a) En el desarrollo en potencias decrecientes de x de $\left(x - \dfrac{1}{5}\right)^n$ la suma de los coeficientes de los tres primeros términos es $\dfrac{4}{5}$. Hallar n.

(b) Hallar $m \in \mathbb{N}$ tal que $\dfrac{1}{2}\ V_m^2 + 3m = V_{m+1}^2 - 9$.

145. (a) Hallar todos los valores de $m \in \mathbb{N}$ tales que $\dfrac{1}{2} \cdot V_{m-3}^2 + \dfrac{1}{3} \cdot V_{m-1}^2 = \dfrac{8}{5} \cdot C_{m-2}^{m-4}$

(b) Sea $(z+w)^8$ desarrollado en potencias crecientes de z. Sean $c, d > 0$ tales que $c - d = 1$. Hallar los valores de c y d sabiendo que cuando $z = d$ y $w = c$ el cuarto término es igual al quinto.

146. Indicar la respuesta correcta. Justificar.

(a) ¿ Cuántos números de 5 cifras se pueden formar con los dígitos: 1,2,3,4,5,6,7,8,9, de manera que figuren 2 cifras pares, 3 cifras impares y no haya cifras repetidas?

720	1440	7200

(b) ¿ En cuántos figura el 2 ?

180	3600	21600

(c) ¿Cuántos terminan en 3?

144	864	1032

147. ¿ Cuántas palabras de 4 letras que empiecen con A pueden formarse con las letras de la palabra CASITA ? ¿ Y que empiecen con C ?

148. ¿ De cuántas formas puede una persona ponerse 3 anillos distintos en los dedos de una mano (sin contar el pulgar) ?

149. En un plano hay 3 rectas paralelas que son cortadas por otras 4 paralelas entre sí. ¿ Cuántos paralelogramos se forman ?

150. (a) Un estudiante tiene que resolver 10 problemas de los 13 planteados en un examen. ¿De cuántas formas puede hacerlo si:
(i) tiene que resolver los dos primeros problemas ?
(ii) tiene que resolver por lo menos 3 de los 5 primeros problemas ?

(b) Hallar el exponente del binomio $\left(3\,a^3 - \dfrac{1}{a^2}\right)^n$, sabiendo que el grado del octavo término es 10.

151. (a) Hallar el coeficiente de x^{41} en el desarrollo de $\left(\dfrac{1}{2}b^3y^{-1}x^{-2} - b^2y^4x^3\right)^{17}$.

(b) Hallar $m \in \mathbb{N}$ tal que $\begin{pmatrix} m \\ m-2 \end{pmatrix} + \begin{pmatrix} m \\ m-1 \end{pmatrix} = 28$.

152. En una repisa se colocan 5 discos de rock, 4 de tango y 6 de música clásica.

(a) ¿ De cuántas maneras se pueden ubicar ?
(b) ¿ De cuántas si los de rock deben estar juntos ?
(c) ¿ De cuántas maneras se pueden seleccionar dos de cada clase para una fiesta ?
(e) ¿ De cuántas si para la fiesta solo se puede llevar dos discos y deben ser de distinta clase ?

153. (a) Hallar el término que no contiene x en el desarrollo de: $\left(-\dfrac{1}{5}x^{-3} + 3y^2\sqrt{x}\right)^{28}$.

(b) Hallar $m \in \mathbb{N}$ para el cual: $C_m^3 = \dfrac{5}{3}C_m^5$.

154. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(a) ¿Cuántos boletos capicúas de 6 cifras se pueden formar con los números del conjunto A?

(b) ¿Cuántos números de 4 cifras diferentes, mayores que 2000 y menores que 6000 se pueden obtener con los dígitos del conjunto A?

(c) ¿De cuántas formas se pueden elegir 3 números distintos del conjunto A de modo que la suma de los 3 sea impar?

155. (a) Con los números 0 y 1, ¿Cuántas sucesiones de 9 elementos se pueden formar con la condición que contengan 5 unos y 4 ceros?

(b) ¿Cuántas contienen unos en los lugares pares?

(c) ¿Cuántas son capicúas?

156. (a) Calcular el coeficiente de x^{-24} en el desarrollo de $\left(\frac{1}{4}a^2x^3 - x^{-4}\right)^{13}$. Indicar en qué término aparece.

(b) Demostrar que $(n-7)\binom{n}{n-7} = 8\binom{n}{8}$.

(c) ¿Cuántos números entre 1200 y 3522 pueden formarse con los dígitos 1, 2, 3, 4, 5, 6 y 7 sin repetir dígitos?

157. ?De cuántas formas diferentes pueden ordenarse las letras de la palabra UNIVERSITARIAS de modo que no haya dos consonantes juntas ?

158. (a) En el desarrollo de $\left(x^2 + x^{-\frac{1}{3}}\right)^n$ el coeficiente del cuarto término es mayor que el coeficiente del tercer término en 14 unidades. Hallar el término que no contiene a x.

(b) ¿Cuántos polinomios diferentes de sexto grado se pueden escribir de modo que sus coeficientes pertenezcan al conjunto $A = \{0, 1, 2, 4, 6\}$? ¿Cuántos tales que $p(0) = 4$? ¿Cuántos que admitan a x^3 como factor?

159. (a) ¿ Cuántos números de 4 cifras pueden formarse con los dígitos: 1, 2, 4, 5, 7, 8, 9, de modo que no haya cifras repetidas en cada número ?

(b) ¿ Cuántos de los números hallados en (a) son pares ?

(c) ¿ En cuántos de los números hallados en (a) aparecen 2 cifras pares y 2 impares ?

160. Demostrar por inducción que:

(a) $1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2} + 3 \cdot \binom{n}{3} + \cdots + n \cdot \binom{n}{n} = n \cdot 2^{n-1}$.
(Ayuda: $k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$, (probarlo)).

(b) $-1 \cdot \binom{n}{1} - 2 \cdot \binom{n}{2} + 3 \cdot \binom{n}{3} - \cdots + (-1)^{n+1} \cdot n \cdot \binom{n}{n} = 0$ para todo $n \geq 2$.

(c) $\frac{1}{1} \cdot \binom{n}{0} + \frac{1}{2} \cdot \binom{n}{1} + \frac{1}{3} \cdot \binom{n}{2} + \cdots + \frac{1}{n+1} \cdot \binom{n}{n} = \frac{2^{n+1} - 1}{n+1}$.
(Ayuda: $\frac{1}{k+1} \cdot \binom{n}{k} = \frac{1}{n+1} \cdot \binom{n+1}{k+1}$, (probarlo)).

(d) $\binom{5}{0} + \binom{6}{1} + \binom{7}{2} + \cdots\cdots\cdots + \binom{5+n}{n} = \binom{5+n+1}{n}$ para todo $n \in \mathbb{N}$.

161. Probar que para todo $n \in \mathbb{N}$, $3^n \mid 2^{3^n} + 1$ (Inducción y binomio de Newton).

162. Probar que $9 \mid 4^n + 15n - 1$ (desarrollar $(3+1)^n$, o probarlo por inducción).

163. Probar que $64 \mid 3^{2n+3} + 40n - 27$ (desarrollar $(4-1)^n$, o probarlo por inducción).

164. Probar que $n^2 \mid (n+1)^n - 1$ (desarrollar $(n+1)^n$).

165. Probar que si a y b son números enteros, entonces $(a+b)^n = ka + b^n$, $k \in \mathbb{Z}$, para todo $n \in \mathbb{N}$.

166. (a) Probar que si r y s son enteros tales que $s \mid r$, y p es un primo tal que $p \mid r$ y $p \nmid s$, entonces $p \mid \frac{r}{s}$. (Escribir $r = st$).

(b) Deducir que $\binom{p}{i}$ es divisible por p para todo i, $1 \leq i \leq p-1$.

167. Indicar si las siguientes afirmaciones son verdaderas o falsas. Justificar las respuestas.

(a) El polinomio $f(X) = X^3 - 20X^2 - 4X + 80$ no tiene raíces reales.
(b) Si A y B son matrices de orden n, entonces $(9 \cdot A^2 + B^T \cdot A)^T - (3 \cdot A^T)^2 = A^T \cdot B$.
(c) Sean A, B matrices cuadradas de orden 2. Si $A \cdot B = 0$ entonces $(A+B)^2 = A^2 + B^2$.

168. Decir si las siguientes afirmaciones son verdaderas o falsas. Justificar las respuestas.

(a) El polinomio $f(X) = X^4 - 3X^3 - X^2 - 2X + 1$ no tiene raíces reales.
(b) Si A y B son matrices de orden 4 y A es inversible, entonces $det(4A^tBA^{-1})^2 = 4^8 \cdot detB$.
(c) El cuarto término del desarrollo de $(\frac{1}{2}a^3 - \frac{1}{3}a^{-5})^{10}$ es $-\frac{5}{144}a^6$.

169. Dadas las matrices $A = \begin{pmatrix} 1 & -2 & 3 \\ 2 & -3 & -1 \\ 4 & -7 & 5 \end{pmatrix}$ y $C = (10 \quad 8 \quad 28)$, hallar utilizando el método de eliminación de Gauss, una matriz B tal que: $A \cdot B = C^T$.

170. (a) Sea $A = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 7 \end{pmatrix}$, $B = (b_{i,j})$ una matriz cuadrada de orden 3 tal que $b_{i,j} = \begin{cases} i-j & \text{si } i < j \\ 1 & \text{si } i = j \\ i+j & \text{si } i > j \end{cases}$ y $C = (c_{i,j})$ una matriz de orden 2×3 tal que $c_{i,j} = \begin{cases} 0 & \text{si } i+j = 3 \\ 1 & \text{si } i+j \neq 3 \end{cases}$

(i) Indicar las matrices B y C.
(ii) Calcular $A^T \cdot C - 2 \cdot B$.

(b) Sean A, B matrices cuadradas de orden 3, A matriz simétrica. Probar que $(2 \cdot A \cdot (8 \cdot B^T))^T \cdot B \cdot A = (4 \cdot B \cdot A)^2$.

171. Resolver, aplicando el método de eliminación de Gauss, los siguientes sistemas de ecuaciones lineales. Clasificarlos. Si tienen más de una solución, indicar una solución particular. Indicar en cada caso la operación elemental usada.

$$\begin{cases} 2x + y + 3z - 7t = 5 \\ y - z + t = -3 \\ x + 3y - 3t = 1 \\ -7y + 3z + t = -3 \end{cases} \qquad \begin{cases} 2x + y - 5z + 6u = 1 \\ x + y - 2z + 3u = 2 \\ y + u = 1 \\ 3x - 2y - 7z + 5u = -1 \end{cases}$$

172. Determinar el valor de λ para el cual el siguiente sistema sea compatible y resolverlo. En caso de ser indeterminado, indicar la solución general.

$$\left\{\begin{array}{rcrcrcrcr} x & + & 2y & - & z & + & 4t & = & 2 \\ 3x & + & 5y & & & + & 13t & = & 7 \\ 2x & - & y & + & z & + & t & = & -3 \\ x & + & 7y & - & 4z & + & 11t & = & \lambda \end{array}\right.$$

173. Dado el siguiente sistema de ecuaciones

$$\left\{\begin{array}{rcrcrcrcr} x & & & - & z & + & w & = & 1 \\ -2x & + & y & + & z & - & 3w & = & -2 \\ x & + & y & - & 2z & & & = & 1 \\ & & & & & & (k-2)\cdot(k-1)w & = & (k-1) \end{array}\right.$$

(a) Analizar para qué valores de k el sistema es
(i) Compatible determinado, (ii) Compatible indeterminado, (iii) Incompatible

(b) Eligiendo un valor de k para que el sistema sea compatible indeterminado, hallar la solución general y una solución particular.

174. (a) Dada la matriz cuadrada de orden 2 A inversible, hallar una matriz inversible B de orden 2 tal que:

$$[A^T.(2.B)]^T.(2.B^{-1}.A)^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}^{-1}.B$$

(b) Dada la matriz $A = \begin{pmatrix} x & -1 & 0 \\ 0 & 1 & 2 \\ -1 & x & x^2 \end{pmatrix} - \begin{pmatrix} 0 & -1 & 1 \\ -1 & 1-x & -1 \\ -2 & x & x(1+x) \end{pmatrix}$, calcular $detA$ y hallar los valores de x para los cuales la matriz A no es inversible.

175. (a) Hallar una raíz primitiva de orden 6 de la unidad, y a partir de ella, hallar todas las raíces de orden 6 de la unidad.

(b) Triangulando previamente la matriz A, hallar $z = det\ A$, y usando las raíces halladas en (a), calcular $\sqrt[6]{z}$, siendo

$$A = \begin{pmatrix} 1 & -2 & 1 \\ i & -(1+i) & 0 \\ 1 & 2i & 1 \end{pmatrix}$$

176. (a) ¿Cuántas matrices de la forma

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}$$

se pueden escribir con los números 5, 7, -1, -2, -4 ?

(b) ¿ En cuántas de ellas su determinante es un entero positivo ?

177. Dados los números -1, 1, -3, 5 y 9,

(a) ¿Cuántas matrices de la forma

$$\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

se pueden escribir con esos números ?

(b) ¿ En cuántas de ellas su determinante es 9 ?

178. (a) ¿ Cuántas matrices simétricas de orden 3 se pueden escribir con los dígitos 1, 2, 3, 5, 6 y 9?

(b) ¿ En cuántas de ellas es $a_{13} = 5$?

(c) ¿ En cuántas el producto de los elementos de la diagonal principal es igual a 30 ?

179. Hallar, si existe, una matriz B tal que $A^T \cdot B = C$, siendo

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 6 & 3 & 9 \\ -2 & -1 & -3 \\ 6 & 2 & 3 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 18 \\ 7 \\ 15 \end{pmatrix}.$$

¿ Es única B ?

180. (a) Si A, B son matrices cuadradas de orden 3, $detA = 2$ y $detB = \dfrac{1}{2}$, hallar

$$det\left(((2.B \cdot A^T)^T)^2 \cdot A^{-1}\right) \frac{1}{2}(det\, B)^2 - \left(det(A^{-1} \cdot (A^{-1} \cdot B)^{-1} \cdot B)\right)^{-1}.$$

(b) Dada la matriz $C = \begin{pmatrix} 7 & x & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 3\,x \end{pmatrix}$, hallar los valores de x para los cuales C sea inversible.

181. Determinar el valor de λ para el cual el siguiente sistema sea compatible y resolverlo.

$$\begin{cases} x & +2y & -z & = 2 \\ 3x & +5y & & = 7 \\ 2x & -y & +z & = -3 \\ x & +7y & -4z & = \lambda \end{cases}$$

182. Hallar todos los valores de $z \in C$ tales que

$$\begin{vmatrix} 3z-1 & -1 & 2 & 1 \\ z^2 & z^2 & 1 & -1 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 1 & -1 \end{vmatrix} = 3i.$$

183. Si la matriz de un sistema es

$$\begin{pmatrix} 1 & 2 & \text{-1} & 5 \\ 0 & 1 & \text{-2} & -2+b \\ 0 & 0 & a^2-4 & -1+b \end{pmatrix},$$

clasificar las diferentes posibilidades para el conjunto solución en términos de a y b.

Para algún par de valores a, b que hacen que el sistema sea compatible indeterminado, dar la solución general y una particular.

184. Sin desarrollar el determinante, demostrar que

$$\begin{vmatrix} 1 & 6 & 9 \\ 1 & 9 & 5 \\ 1 & 4 & 3 \end{vmatrix}$$

es múltiplo de 13. (Observar que los números 169, 195 y 143 son múltiplos de 13).

185. Demostrar, aplicando propiedades de los determinantes que

$$(i) \begin{vmatrix} x & y & x+y \\ y & x+y & x \\ x+y & x & y \end{vmatrix} = 2(x+y) \begin{vmatrix} 1 & 1 & 1 \\ y & x+y & x \\ x+y & x & y \end{vmatrix} \quad (ii) \begin{vmatrix} \text{sen}^2 x & \cos 2x & \cos^2 x \\ \text{sen}^2 y & \cos 2y & \cos^2 y \\ 1 & 0 & 1 \end{vmatrix} = 0$$

(Recordar que $\cos 2x = \cos^2 x - \text{sen}^2 x$)

186. Elegir en cada inciso la **única** opción correcta.

(1) El conjunto solución de la inecuación $\dfrac{1}{x-1} > 1$ es ...
(a) $(-\infty, 2)$ (b) $(-\infty, 1) \cup (1, 2)$ (c) $(1, 2)$ (d) $\mathbb{R} - \{1\}$.

(2) La ecuación $|2 + |x - 2|| = 3$ tiene ...
(a) una solución (b) dos soluciones (c) ninguna solución (d) cuatro soluciones.

(3) El conjugado de $\sqrt{2} - \sqrt{3} + i$ es ...
(a) $-\sqrt{2} + \sqrt{3} + i$ (b) $\sqrt{2} - \sqrt{3} - i$ (c) $\sqrt{2} + \sqrt{3} - i$ (d) $-\sqrt{2} - \sqrt{3} - i$

(4) Si $z = \dfrac{\sqrt{6}}{2} - \dfrac{\sqrt{2}}{2}\, i$, entonces z^8 es ...
(a) $16 \operatorname{cis}(\frac{4}{3}\pi)$ (b) $16 \operatorname{cis}(\frac{2}{3}\pi)$ (c) $\sqrt{2} \operatorname{cis}(\frac{11}{6}\pi)$ (d) $16 \operatorname{cis}(\frac{11}{6}\pi)$.

(5) La igualdad de números combinatorios $\binom{n}{4} = \binom{n}{2}$ se verifica ...
(a) para dos valores de n (b) sólo para $n = 6$ (c) nunca.

(6) ¿Cuántos números de 6 cifras no repetidas pueden formarse con los dígitos 1, 2, 3, 4, 5, 6, 7, 8 y 9 de modo que aparezcan en ellos 3 cifras pares y 3 impares?
(a) $V_9^6 = 60.480$ (b) $V_4^3 \cdot V_5^3 \cdot P_6 = 1.036.800$ (c) $C_4^3 \cdot C_5^3 \cdot P_6 = 28.800$
(d) $V_4^3 \cdot V_5^3 = 1.440$.

(7) El resto de dividir a $X^{11} - X^6 + 1$ por $X - 3$ es ...
(a) 30 (b) 176.419 (c) 184.123 (d) 7.

(8) Sea f un polinomio de grado 5 con coeficientes reales. Se sabe que $-2i$ es raíz doble de f, -1 es raíz simple y $f(0) = 4$. ¿Cuánto vale el coeficiente principal de f?
(a) $-\dfrac{1}{4}$ (b) -4 (c) $\dfrac{1}{4}$ (d) 0.

(9) Si A es una matriz de orden 3×2, B es 3×2 y C es 2×2. Entonces $A \cdot B + C$ ...
(a) es una matriz cuadrada (b) es de orden 3×2 (c) es de orden 2×2
(d) no está definido.

(10) La matriz $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 0 & 4 & 0 \\ 3 & 0 & 5 & 2 \\ 4 & 0 & -2 & 0 \end{pmatrix}$ verifica ...
(a) A es inversible (b) $A = A^t$ (c) $det(A) = 0$ (d) $det(A) = 80$.

(11) El sistema $\left\{\begin{array}{rcrcrcl} x & + & y & + & z & = & 1 \\ 2x & + & 2y & + & 3z & = & 2 \\ 2x & + & 2y & + & 4z & = & 2 \end{array}\right.$ ...

(a) tiene a $(1, 1, -1)$ como solución (b) es compatible determinado

(c) es compatible indeterminado (d) es incompatible.

187. Elegir en cada inciso la **única** opción correcta.

(1) La igualdad $\frac{5}{7} + \frac{5^2}{7^2} + \cdots + \frac{5^n}{7^n} = \frac{5}{2} - \frac{5^{n+1}}{2 \cdot 7^n}$ vale ...

(a) sólo para $n = 1$ (b) nunca (c) para todo $n \in \mathbb{N}$ (d) ninguna de las opciones anteriores.

(2) El conjunto solución de la inecuación $\frac{1}{1+x} \geq \frac{1}{1-x}$ es ...

(a) $(-\infty, 0]$ (b) $(-1, 0] \cup (1, +\infty)$ (c) $[0, 1)$ (d) $\mathbb{R} - \{-1, 1\}$.

(3) $2^{-(2n-1)} - 2^{-(2n+1)} - 2^{-2n}$ es igual a ...

(a) 2^{-2n} (b) $2^{-(2n-1)}$ (c) $2^{-(2n+1)}$ (d) ninguna de las opciones anteriores.

(4) La ecuación $|x - 1| - 2x = -4$ tiene ...

(a) una solución (b) dos soluciones (c) cuatro soluciones (d) ninguna solución.

(5) Si $z = \sqrt{2}\,(\cos\,(\frac{2\pi}{3}) + i \cos\,(\frac{5\pi}{6}))$, entonces z^{-22} es ...

(a) $\frac{1}{2^{11}}$ cis $(\frac{4\pi}{3})$ (b) $\frac{1}{2^{11}}$ cis $(\frac{\pi}{3})$ (c) $\frac{1}{2^{11}}$ cis $(\frac{2\pi}{3})$ (d) $\frac{1}{2^{11}}$ cis $(\frac{5\pi}{3})$.

(6) $z = 5\,\text{cis}\,(\frac{5\pi}{6})$ es solución de una de las siguientes ecuaciones. ¿De cuál?

(a) $z^4 = \dfrac{2 - 2\sqrt{3}i}{-1 + \sqrt{3}i}$ (b) $z^6 = 5^6$ (c) $z^{12} = 5^{12}$ (d) de ninguna de las anteriores.

(7) Si $z = \sqrt{2} - \sqrt{3} - i$, el módulo de z vale ...

(a) $\sqrt{4 - 2\sqrt{6}}$ (b) $2 - 2\sqrt{6}$ (c) $\sqrt{6 - 2\sqrt{6}}$ (d) $\sqrt{6}$.

(8) La ecuación de números combinatorios $\left(\begin{array}{c} m \\ m-2 \end{array}\right) + \left(\begin{array}{c} m \\ m-1 \end{array}\right) = 28$ tiene ...

(a) una solución (b) dos soluciones (c) cuatro soluciones (d) ninguna solución.

(9) ¿Cuántas palabras pueden formarse con las letras de la palabra MAZAMORRA?

(a) $P_9 = 362.880$ (b) $P_9^{3,2,2} = 30240$ (c) $P_9^{3,2,2} = 15120$ (d) ninguna de las opciones anteriores.

(10) ¿Cuántos números capicúas pares de 6 cifras pueden formarse con los dígitos 1, 2, 3, 4, 5, 6, 7 y 8?

(a) $V_8'^6 = 8^6$ (b) $4 \cdot V_8'^5 = 4 \cdot 8^5$ (c) $4 \cdot V_8'^3 = 4 \cdot 8^3$ (d) $4 \cdot V_8'^2 = 4 \cdot 8^2$

(11) ¿Cuántas raíces DISTINTAS tiene el polinomio $f(X) = (3X^7 + 6X^6 + 18X^5 + 36X^4 - 27X^3 - 54X^2 - 42X - 84)(X^2 - 4)^2$? (Ayuda: se sabe que i es raíz.)

(a) siete (b) ocho (c) trece (d) ninguna de las opciones anteriores.

(12) Las raíces de $f(X) = X^8 + 3X^6 - X^2 - 3$ son ...

(a) $\sqrt{3}i$, $-\sqrt{3}i$ simples y 1 de multiplicidad 6

(b) $\sqrt{3}i$, $-\sqrt{3}i$ simples y 1 y -1 de multiplicidad 3

(c) $\sqrt{3}i$, $-\sqrt{3}i$ y las raíces de la unidad de orden 6, todas raíces simples

(d) ninguna de las opciones anteriores.

(13) f es un polinomio con coeficientes reales. Se sabe que 5 es raíz doble, $-2i$ es raíz doble y $\sqrt{3}i$ es raíz triple. f es de grado ...

(a) 10 (b) 7 (c) 12 (d) ninguno de los anteriores.

(14) ¿Cuántos polinomios hay de grado 5 con coeficientes en $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ y tales que $f(0) = 4$?

(a) $V'^6_{10} = 10^6$ (b) $9 \cdot V'^5_{10} = 9 \cdot 10^5$ (c) $9 \cdot V'^4_{10} = 9 \cdot 10^4$ (d) ninguna de las opciones anteriores.

(15) El sistema $\left\{ \begin{array}{rcrcrcl} x & + & 2y & - & 3z & = & 1 \\ x & + & y & - & 3z & = & 0 \\ 2x & + & 3y & - & 6z & = & 2 \end{array} \right.$ ...

(a) tiene a $(2, 1, 1)$ como solución (b) es compatible determinado

(c) es compatible indeterminado (d) es incompatible.

(16) ¿Cuál de las siguientes es una propiedad de determinantes? Si A y B son matrices cuadradas de orden n, entonces ...

(a) $det(A + B) = det(A) + det(B)$ (b) $det(A^{-1}) = det(A^t)$ (c) $det(2A) = 2det(A)$ (d) $det(A \cdot B) = det(A) \cdot det(B)$.

(17) La matriz $A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ -1 & 3 & 2 & -1 \\ 0 & 0 & 3 & 1 \end{pmatrix}$ verifica ...

(a) A no es inversible (b) $det(A) = 18$ (c) $det(A) = -12$ (d) ninguna de las opciones anteriores.