NOTAS DEL CURSO

MATEMÁTICA DISCRETA

Pascual Jara Martínez

Departamento de Álgebra. Universidad de Granada

Granada, 2005

Primera redacción: Agosto 2005–Enero 2006

Revisión: Octubre 2006

Introducción

Índice general

Capítulo I

Nociones básicas

1. Introducción

Vamos a comenzar por una introducción intuitiva al concepto que es la base del curso: el de *conjunto* . Hemos preferido hacer esto así ya que una introducción rigurosa del concepto conjunto exigiría demasiado esfuerzo a un posible lector, y lo apartaría de los objetivos centrales de este curso que son la introducción a las técnicas del trabajo matemático, y por que deseamos fijar las notaciones y el lenguaje que vamos a emplear a lo largo del curso.

Para poder comprender en su totalidad el concepto de conjunto y el álgebra de subconjuntos es necesario hacer pequeña introducción al álgebra de proposiciones, de esta forma ya tendremos dos ejemplos de álgebras de Boole.

El concepto de conjunto se complementa con el de función o aplicación entre conjuntos, veremos la definición y algunas de sus propiedades.

Otro concepto de interés es el de relación. Aquí vamos a estudiar relaciones de equivalencia y de orden, aunque las segundas las estudiaremos en profundidad en un capítulo posterior.

Acabamos el capitulo con una introducción a los cuantificadores y el álgebra de predicados y con algunos ejemplos como hacer una demostración.

Me gustaría volver a insistir que la aproximación los conceptos aquí tratados no es una aproximación axiomática sino intuitiva. Para una introducción a la teoría de conjuntos amena, y a la vez rigurosa, recomendamos el siguiente texto: [4].

2. Introducción intuitiva a la teoría de conjuntos

2.1. Conjuntos

Vamos a considerar un **conjunto** X como una *colección* de **elementos**. Los elementos de un conjunto son distintos dos a dos, esto es, cualesquiera dos elementos de un conjunto o son el mismo elemento o son elementos distintos, y no hay ningún orden o relación entre ellos.

Los conjuntos pueden ser definidos de dos formas distintas:

(-) por **extensión**, esto es, haciendo una lista de todos sus elementos, o
(-) por **comprensión**, esto es, mediante una propiedad que caracteriza a sus elementos.

Ejemplo. 2.1. (Definición por extensión)
Un ejemplo de un conjunto definido por extensión es:

$$A = \{1, 2, a, b, c\}.$$

Según lo dicho antes, observar que $\{1, 2, a, a\}$ no es un conjunto ya que en él aparecen dos elementos repetidos, esto es, un mismo elemento aparece dos veces.

Ejemplo. 2.2. (Definición por comprensión)
Un ejemplo de un conjunto definido por comprensión es:

$$P = \{x \mid \ x \text{ es un número natural par}\}.$$

Si un elemento x **pertenece** a un conjunto X, escribimos

$$\mathbf{x \in X},$$

y si **no pertenece**, escribimos

$$\mathbf{x \notin X}.$$

Ejemplo. 2.3.
En los ejemplos anteriores tenemos que

$$1 \in A = \{1, 2, a, b, c\}$$

y

$$1 \notin P = \{x \mid \ x \text{ es un número natural par}\}.$$

2.2. Subconjuntos

Dado un conjunto X, un **subconjunto** de X es un conjunto Y verificando que para cada elemento $y \in Y$ se tiene $y \in X$. Escribimos entonces $\mathbf{Y \subseteq X}$.

Dos subconjuntos X_1 y X_2 de un conjunto X son **iguales** si $X_1 \subseteq X_2$ y $X_2 \subseteq X_1$, y escribimos $\mathbf{X_1 = X_2}$.

Si dos subconjuntos X_1 y X_2 de un conjunto X no son iguales, entonces decimos que son **distintos**, y escribimos $\mathbf{X_1 \neq X_2}$.

Si X_1 es un subconjunto de X y $X_1 \neq X$, podemos escribir $\mathbf{X_1 \subset X}$ ó $\mathbf{X_1 \subsetneq X}$, y decimos que X_1 es un **subconjunto propio** de X.

Ejemplo. 2.4.

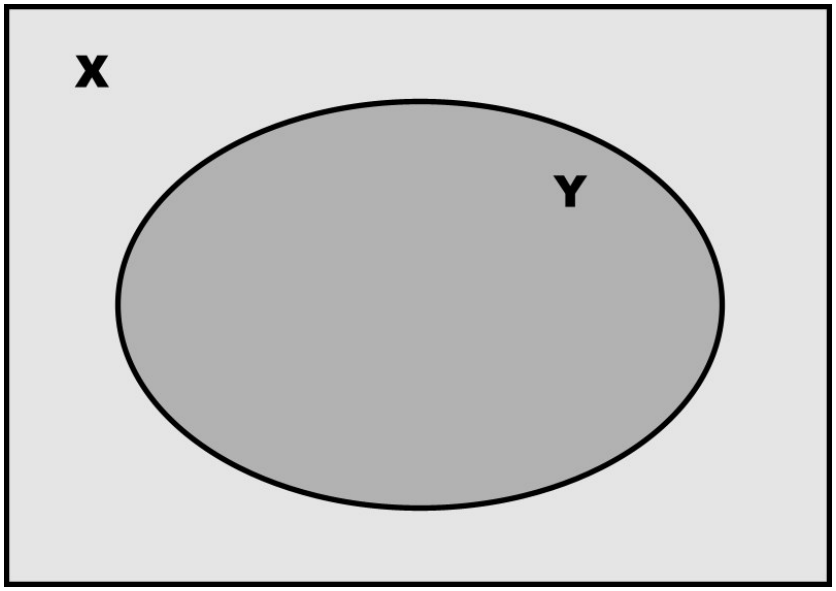
(1) Cada conjunto es un subconjunto de sí mismo.

Esto es, para cada conjunto X se tiene $X \subseteq X$; llamamos a X el **subconjunto impropio** de X.

(2) El conjunto $B = \{1,2\}$ es un subconjunto de $A = \{1,2,a,b,c\}$. Esto se representa por $B \subseteq A$. En cambio el conjunto $C = \{1,2,3\}$ no es un subconjunto de A. Esto se representa por $\mathbf{C \nsubseteq A}$.

(3) El conjunto $B_0 = \{2,1\}$ es igual al conjunto B; esto es, $\{1,2\} = \{2,1\}$.

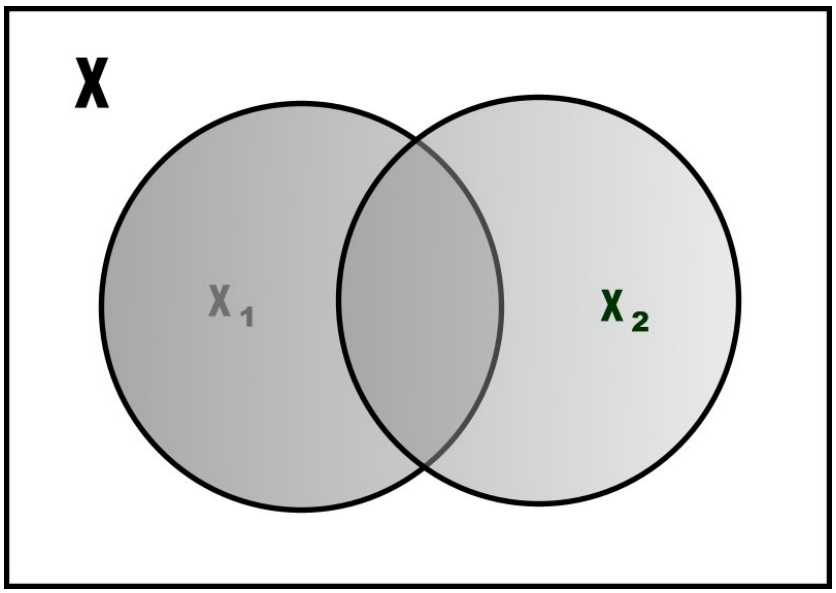
Si Y es un subconjunto de un conjunto X, a veces los representamos mediante un **diagrama de Venn**, esto es, el conjunto X se representa por el interior del cuadrado y el conjunto Y por el interior de la línea curva.



2.3. Operaciones con subconjuntos

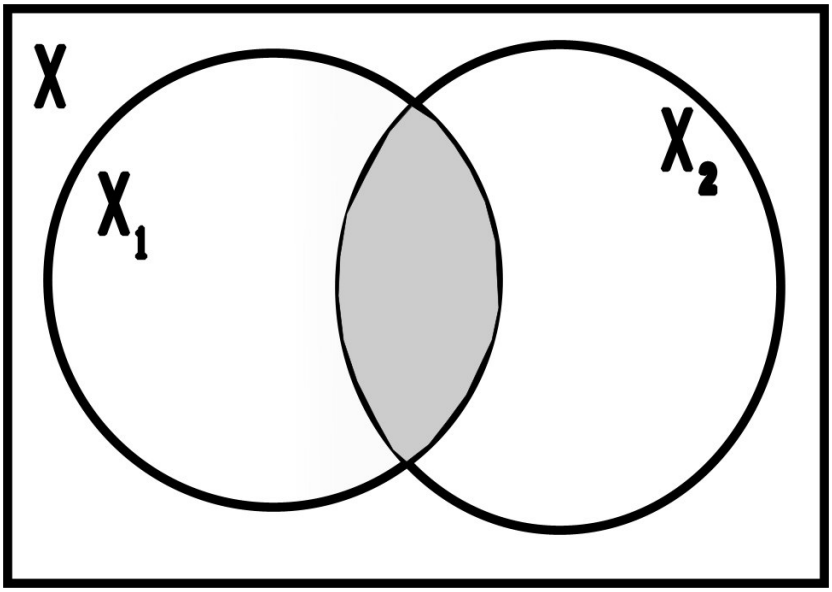
Si X_1 y X_2 son dos subconjuntos de un conjunto X, podemos definir su **unión** como el subconjunto de X definido por:

$$X_1 \cup X_2 = \{x \in X \mid \ x \in X_1 \text{ ó } x \in X_2\},$$



y su **intersección** como el subconjunto de X definido por:

$$X_1 \cap X_2 = \{x \in X \mid \ x \in X_1 \text{ y } x \in X_2\},$$



Ejemplo. 2.5.

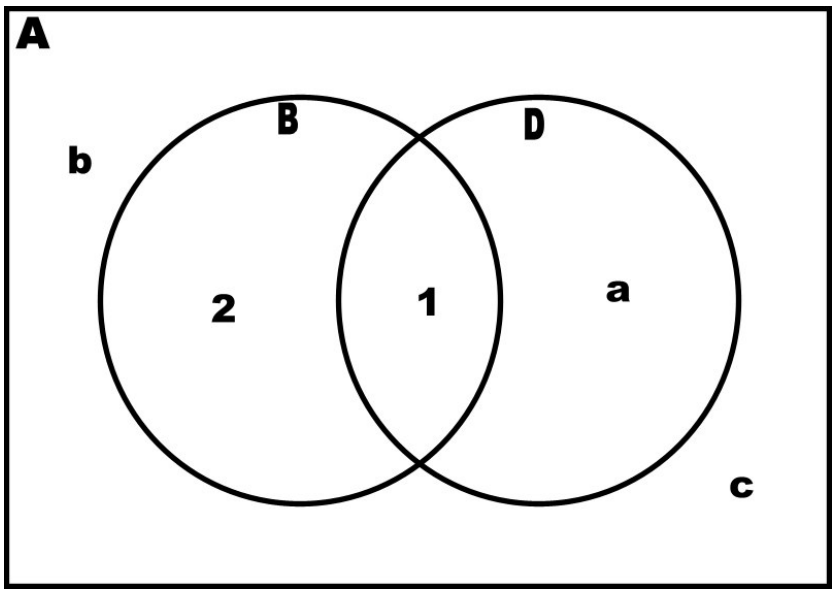
(1) Sea $D = \{1, a\}$. Como $B = \{1, 2\}$ y D son subconjuntos del conjunto $A = \{1, 2, a, b, c\}$, entonces podemos calcular su unión y su intersección. Se verifica:

$$B \cup D = \{1, 2, a\} \quad \text{y} \quad B \cap D = \{1\}.$$

(2) También $B = \{1, 2\}$ y $B_0 = \{2, 1\}$ son subconjuntos del conjunto A; en este caso tenemos

$$B \cup B_0 = B = B_0 \quad \text{y} \quad B \cap B_0 = B = B_0.$$

Existe un conjunto especial que está definido por la propiedad de no tener ningún elemento. Este conjunto se llama **vacío** y se representa por el símbolo $\varnothing$.

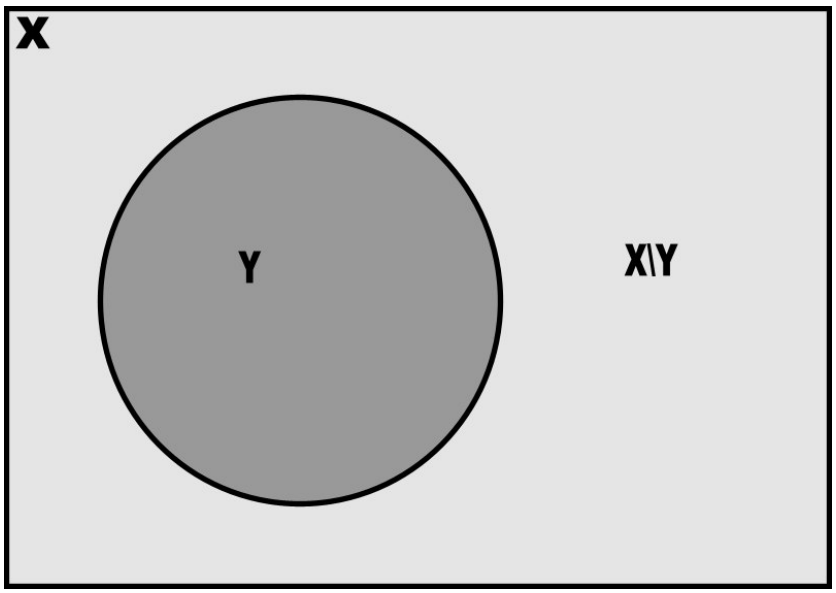


Cada conjunto X tiene un único subconjunto que no tiene ningún elemento, si representamos por $\varnothing$ a este subconjunto, entonces $\varnothing$ es un subconjunto de X. El subconjunto $\varnothing$ se llama **subconjunto vacío o trivial** de X.

Si la intersección de dos subconjuntos X_1 y X_2 de un conjunto X es igual a $\varnothing$, decimos que son **subconjuntos disjuntos**.

Sea Y un subconjunto de un conjunto X, llamamos **subconjunto complemento** de Y en X al siguiente subconjunto de X:

$$\overline{Y} = X \setminus Y = \{x \in X \mid \ x \notin Y\}.$$



Ejemplo. 2.6.
El complemento de $B = \{1,2\}$ en $A = \{1,2,a,b,c\}$ es:

$$\overline{B} = \{a,b,c\}$$

Observación. 2.7.
Observar que para cada subconjunto Y de un conjunto X, los subconjuntos Y y $\overline{Y}$ son siempre disjuntos.

Ejercicio. 2.8.
Sea X un conjunto e Y un subconjunto de X. Probar que $\overline{\overline{Y}} = Y$.

SOLUCIÓN. Tenemos que probar que $\overline{\overline{Y}} \subseteq Y$ y que $Y \subseteq \overline{\overline{Y}}$. Para esto último cojamos un elemento $y \in Y$, entonces $y \in X$ y además $y \notin \overline{Y}$, luego $y \in \overline{\overline{Y}}$.

Recíprocamente, si $y \in \overline{\overline{Y}}$, entonces por definición $y \in X$ y además $y \notin \overline{Y}$, luego $y \in Y$. □

Dado un conjunto X existe un conjunto cuyos elementos son todos los subconjuntos de X. Este conjunto lo llamamos **conjunto de las partes** ó **conjunto potencia** de X y lo representamos por $\mathcal{P}(X)$.

Ejemplo. 2.9.

(1) El conjunto de las partes del conjunto $A = \{1, 2, a, b, c\}$ es:

$$\begin{aligned}\mathcal{P}(A) = \{ &\varnothing, \{1\}, \{2\}, \{a\}, \{b\}, \{c\},\\ &\{1,2\}, \{1,a\}, \{1,b\}, \{1,c\}, \{2,a\}, \{2,b\}, \{2,c\}, \{a,b\},\\ &\{a,c\}, \{b,c\},\\ &\{1,2,a\}, \{1,2,b\}, \{1,2,c\}, \{1,a,b\}, \{1,a,c\}, \{1,b,c\},\\ &\{2,a,b\}, \{2,a,c\}, \{2,b,c\}, \{a,b,c\},\\ &\{1,2,a,b\}, \{1,2,a,c\}, \{1,2,b,c\}, \{1,a,b,c\}, \{2,a,b,c\},\\ &\{1,2,a,b,c\}\}.\end{aligned}$$

(2) El conjunto de las partes del conjunto $D = \{u, v, w\}$ es:

$$\mathcal{P}(D) = \{\varnothing, \{u\}, \{v\}, \{w\}, \{u,v\}, \{u,w\}, \{v,w\}, \{v,w\}, \{u,v,w\}\}.$$

(3) El conjunto de las partes del conjunto $\varnothing$ es:

$$\mathcal{P}(\varnothing) = \{\varnothing\}.$$

Observar que $\mathcal{P}(\varnothing)$ es un conjunto con un elemento.

(4) El conjunto de las partes del conjunto $\{\varnothing\}$ es:

$$\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}.$$

En lo que sigue vamos a usar, casi exclusivamente, conjuntos que tienen un número finito de elementos, a estos conjuntos los llamaremos **conjuntos finitos**, y a los que no tienen un número finito de elementos los llamaremos **conjuntos infinitos**.

Ejemplo. 2.10.

(1) El conjunto $A = \{1, 2, a, b, c\}$ es un conjunto finito.

(2) El conjunto $\mathbb{R}$ de los números reales es un conjunto infinito.

Cuando X es un conjunto finito el número de sus elementos lo llamamos su **cardinal**. También se define el **cardinal** de conjuntos infinitos, pero no vamos a tratar este problema aquí.

Ejercicio. 2.11.
Si X es un conjunto con n elementos, probar que el conjunto $\mathcal{P}(X)$ tiene 2^n elementos.

SOLUCIÓN. Subconjunto de X con 0 elementos hay exactamente uno. Subconjunto de X con un elemento hay exactamente n, el número de elementos de X. Subconjuntos de X con dos elementos hay $n(n-1)/2 = \binom{n}{2}$. En general si $t \leq n$, el número de subconjuntos de X con t elementos es $\binom{t}{n}$. Luego en total tenemos

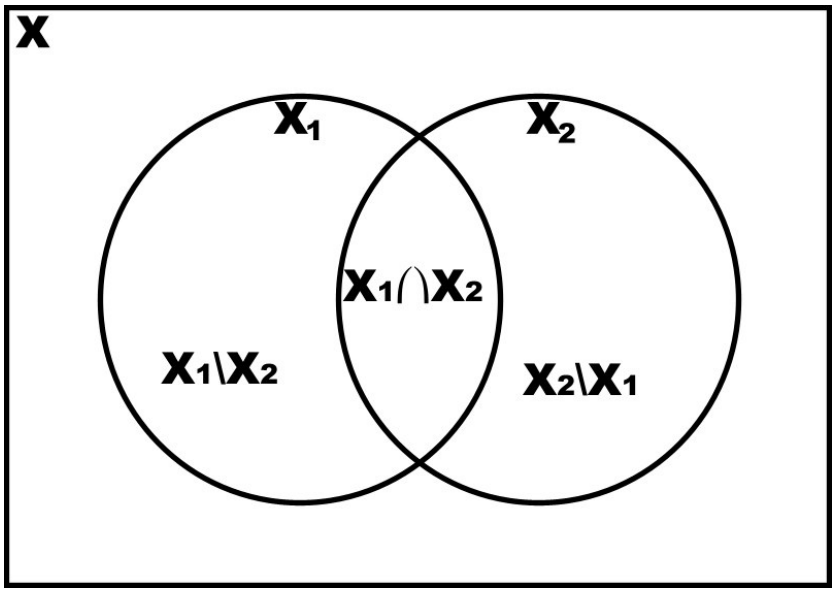
$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = (1+1)^n = 2^n.$$

□

Dados dos subconjuntos X_1 y X_2 de un conjunto X llamamos **diferencia** de X_1 y X_2 al subconjunto $X_1 \setminus X_2$ definido por:

$$X_1 \setminus X_2 = X_1 \cap \overline{X_2}.$$

Observar que en general se tiene $X_1 \setminus X_2 \neq X_2 \setminus X_1$.



Antes de abordar el problema de estudiar las propiedades que verifican la unión, intersección y complemento, vamos a estudiar cómo trabajar con afirmaciones o proposiciones.

La razón es la siguiente: si X_1, X_2 y X_3 son tres subconjuntos de un conjunto X,

¿Qué relación existe entre $(X_1 \cap X_2) \cup X_3$ y $(X_1 \cup X_3) \cap (X_2 \cup X_3)$?

Para establecer la relación existente entre ambos tenemos que analizar las expresiones que nos definen estos subconjuntos

$$\{x \in X_1 \text{ y } x \in X_2\} \text{ ó } x \in X_3$$

y

$$\{x \in X_1 \text{ ó } x \in X_3\} \text{ y } \{x \in X_2 \text{ ó } x \in X_3\}.$$

3. Álgebra de proposiciones

Una **proposición** es una afirmación. Por lo tanto las proposiciones pueden tomar dos valores:

V, verdadero o,

F, falso.

Vamos a representar las proposiciones por letras mayúsculas en negrita **A**.

Ejemplo. 3.1.

(1) "Hoy es lunes", es un ejemplo de una proposición.

(2) "El hambre en el mundo se puede erradicar", es un ejemplo de una proposición.

(3) "*Para sacar dinero del cajero primero tienes que introducir la tarjeta*", no es una proposición.

Si **A** y **B** son dos proposiciones, definimos nuevas proposiciones, a las que llamaremos **proposiciones compuestas**, mediante las siguientes construcciones:

A $\wedge$ **B**, que se lee "**A** y **B**", y su definición está dada por la tabla siguiente.

A $\wedge$ **B**

A	**A** $\wedge$ **B**	**B**
V	V	V
F	F	V
V	F	F
F	F	F

A $\vee$ **B**, que se lee "**A** ó **B**", y su definición está dada por la tabla siguiente.

A $\vee$ **B**

A	**A** $\vee$ **B**	**B**
V	V	V
F	V	V
V	V	F
F	F	F

$\neg$**A**, que se lee "no **A**", y su definición está dada por la tabla siguiente

$\neg$**A**

A	$\neg$**A**
V	F
F	V

Ejemplo. 3.2.

(1) "Hoy **no** es lunes"sería la negación de "Hoy es jueves".

(2) "El coche es rojo" o "La libreta es amarilla" sería la proposición "El coche es rojo **o** la libreta es amarilla".

(3) "El coche es mío" y "yo no tengo una bicicleta" sería la proposición "El coche es mío **y** yo no tengo una bicicleta".

(4) Podemos negar una proposición compuesta, por ejemplo la negación de "El coche es mío **y** yo no tengo una bicicleta" sería: "El coche **no** es mío **o** yo **tengo** una bicicleta".

Dos proposiciones **A** y **B** son **equivalentes** si **A** es verdadera cuando **B** lo es y **B** es verdadera cuando **A** lo es. Dadas dos proposiciones definimos una nueva proposición mediante

$\mathbf{A} \iff \mathbf{B}$

A	$\mathbf{A} \iff \mathbf{B}$	**B**
V	V	V
F	F	V
V	F	F
F	V	F

Entonces **A** y **B** son proposiciones equivalentes si la proposición $\mathbf{A} \iff \mathbf{B}$ toma solo el valor V.

Ejemplo. 3.3.
Las proposiciones $\mathbf{A} \vee \mathbf{B}$ y $\mathbf{B} \vee \mathbf{A}$ son proposiciones equivalentes para cualesquiera proposiciones **A** y **B**.

A	$\mathbf{A} \vee \mathbf{B}$	**B**	$(\mathbf{A} \vee \mathbf{B}) \iff (\mathbf{B} \vee \mathbf{A})$	**B**	$\mathbf{B} \vee \mathbf{A}$	**A**
A	$\vee$	**B**	$\iff$	**B**	$\vee$	**A**
V	V	V	V	V	V	V
F	V	V	V	V	V	F
V	V	F	V	F	V	V
F	F	F	V	F	F	F

Lo mismo ocurre con las proposiciones $\mathbf{A} \wedge \mathbf{B}$ y $\mathbf{B} \wedge \mathbf{A}$

Ejercicio. 3.4.
Probar que $\mathbf{A} \wedge \mathbf{B}$ *y* $\mathbf{B} \wedge \mathbf{A}$ *son proposiciones equivalentes para cualesquiera proposiciones* ***A*** *y* ***B****.*

Una proposición que toma siempre el valor V se llama una **tautología**.

Ejercicio. 3.5.
Probar que para cada proposición **A** *la proposición* $\mathbf{A} \vee \overline{\mathbf{A}}$ *es una tautología.*

3.1. Aplicaciones a la teoría de conjuntos

Podemos considerar ahora las propiedades elementales de las operaciones que hemos introducido entre los subconjuntos de un conjunto dado.

Proposición. 3.6.
Sea X un conjunto y sean X_1, X_2, X_3 subconjuntos de X, se verifica:

$$\begin{array}{rcll} X_1 \cup (X_2 \cup X_3) & = & (X_1 \cup X_2) \cup X_3 & \textbf{\textit{P. asociativa}} \\ X_1 \cap (X_2 \cap X_3) & = & (X_1 \cap X_2) \cap X_3 & \\ X_1 \cup X_2 & = & X_2 \cup X_1 & \textbf{\textit{P. conmutativa}} \\ X_1 \cap X_2 & = & X_2 \cap X_1 & \\ X_1 \cup X_1 & = & X_1 & \textbf{\textit{P. de idempotencia}} \\ X_1 \cap X_1 & = & X_1 & \\ X_1 \cup \varnothing & = & X_1 & \textbf{\textit{E. neutros}} \\ X_1 \cap X & = & X_1 & \\ X_1 \cap \varnothing & = & \varnothing & \textbf{\textit{P. absorción}} \\ X_1 \cup X & = & X & \end{array}$$

Otro tipo de propiedades son las siguientes:

Proposición. 3.7.
Sea X un conjunto y sean X_1, X_2, X_3 subconjuntos de X, se verifica:

$$\begin{array}{rcll} X_1 \cup (X_2 \cap X_3) & = & (X_1 \cup X_2) \cap (X_1 \cup X_3) & \textbf{\textit{P. distributiva}} \\ X_1 \cap (X_2 \cup X_3) & = & (X_1 \cap X_2) \cup (X_1 \cap X_3) & \\ \overline{X_1 \cup X_2} & = & \overline{X_1} \cap \overline{X_2} & \textbf{\textit{Ley de De Morgan}} \\ \overline{X_1 \cap X_2} & = & \overline{X_1} \cup \overline{X_2} & \\ X_1 \cup \overline{X_1} & = & X & \textbf{\textit{E. complementos}} \\ X_1 \cap \overline{X_1} & = & \varnothing & \end{array}$$

Observar que en estos casos todos los conjuntos que aparecen son siempre subconjuntos de un mismo conjunto X.

Para ver que estas igualdades son ciertas, esto es, que los conjuntos que en ellas aparecen son iguales, vamos a comprobar que tienen los mismos elementos. Haremos esto partiendo de la definición del subconjunto correspondiente y obteniendo las consecuencias oportunas.

Para este fin vamos a introducir la siguientes notación: *Cuando de una afirmación se deduce otra, escribimos las dos afirmaciones y entre ambas escribimos el símbolo* $\Rightarrow$.

En el párrafo anterior en realidad estamos introduciendo una nueva forma de obtener nuevas proposiciones a partir de otras dadas. Vamos a hacer una justificación de esto:

Si **A** y **B** son proposiciones, definimos una nueva proposición mediante

$$\mathbf{A} \Longrightarrow \mathbf{B} = (\neg \mathbf{A}) \vee \mathbf{B}$$

A	**A** $\Longrightarrow$ **B**	**B**
V	V	V
F	V	V
V	F	F
F	V	F

La nueva proposición **A** $\Longrightarrow$ **B** se lee:

"**A** implica **B**",

"de **A** se deduce **B**" o

"si **A** entonces **B**".

Tal y como hemos indicado antes indica que si la afirmación **A** es verdadera, entonces *necesariamente* **B** también lo es.

Puede parecer extraño el hecho de que **A** $\Longrightarrow$ **B** es verdadera cuando **A** es falsa y **B** es verdadera o falsa; esto refleja el bien conocido hecho de que de premisas falsas se podría obtener cualquier resultado verdadero o falso.

Observar que el único caso en que **A** $\Longrightarrow$ **B** es falsa es cuando **A** es verdadera y **B** es falsa, esto significa que no se va a poder deducir un resultado falso de un resultado verdadero.

Para probar las Proposiciones 3.6. y 3.7., antes tenemos que probar los resultados sobre proposiciones.

En nuestro caso, como ya conocemos que **A**$\vee$**B** y **B**$\vee$**A** son proposiciones equivalentes, resulta que podemos hacer la siguiente demostración:

Demostración de la propiedad conmutativa para la unión

$$\mathbf{X_1} \cup \mathbf{X_2} = \mathbf{X_2} \cup \mathbf{X_1}.$$

Comprobamos que se tiene $X_1 \cup X_2 \subseteq X_2 \cup X_1$ y también $X_2 \cup X_1 \subseteq X_1 \cup X_2$. Esto es, vemos que cada elemento $x \in X_1 \cup X_2$ verifica $x \in X_2 \cup X_1$.

$$\begin{aligned} x \in X_1 \cup X_2 &\Rightarrow x \in X_1 \ \vee \ x \in X_2 \\ &\Rightarrow x \in X_2 \ \vee \ x \in X_1 \\ &\Rightarrow x \in X_2 \cup X_1 \end{aligned}$$

En forma semejante se tiene que cada elemento $x \in X_2 \cup X_1$ verifica $x \in X_1 \cup X_2$.

$$\begin{aligned} x \in X_2 \cup X_1 &\Rightarrow x \in X_2 \ \vee \ x \in X_1 \\ &\Rightarrow x \in X_1 \ \vee \ x \in X_2 \\ &\Rightarrow x \in X_1 \cup X_2 \end{aligned}$$

Aquí hemos utilizado que se tiene una equivalencia entre las proposiciones $\mathbf{A} \vee \mathbf{B}$ y $\mathbf{B} \vee \mathbf{A}$ para cualesquiera proposiciones **A** y **B**.

Veamos otro ejemplo. Si probamos que son equivalentes las proposiciones $\neg(\mathbf{A} \vee \mathbf{B})$ y $(\neg\mathbf{A}) \wedge (\neg\mathbf{B})$, para cualesquiera proposiciones **A** y **B** (ley de de Morgan), esto es, si en la tabla siguiente debajo del símbolo $\Leftrightarrow$ sólo parecen V,

$(\neg$	$\mathbf{A})$	$\wedge$	$(\neg$	$\mathbf{B})$	$\Longleftrightarrow$	$\neg$	$(\mathbf{A}$	$\vee$	$\mathbf{B})$
F	V	F	F	V	V	F	V	V	V
V	F	F	F	V	V	F	F	V	V
F	V	F	V	F	V	F	V	V	F
V	F	V	V	F	V	V	F	F	F
2	1	3	2	1	4	3	1	2	1

entonces podemos hacer la demostración de la Ley de De Morgan para conjuntos.

Demostración de la ley de De Morgan

$$\overline{\mathbf{X_1} \cup \mathbf{X_2}} = \overline{\mathbf{X_1}} \cap \overline{\mathbf{X_2}}.$$

Comprobamos que se verifican las inclusiones $\overline{X_1 \cup X_2} \subseteq \overline{X_1} \cap \overline{X_2}$ y $\overline{X_1} \cap \overline{X_2} \subseteq \overline{X_1 \cup X_2}$.

Para la primera tenemos que ver que cada elemento $x \in \overline{X_1 \cup X_2}$ verifica también $x \in \overline{X_1} \cap \overline{X_2}$.

$$\begin{aligned} x \in \overline{X_1 \cup X_2} &\Rightarrow x \notin X_1 \cup X_2 \\ &\Rightarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Rightarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Rightarrow x \in \overline{X_1} \cap \overline{X_2} \end{aligned} \tag{I.1}$$

La inclusión $\overline{X_1} \cap \overline{X_2} \ \subseteq \ \overline{X_1 \cup X_2}$ se prueba simplemente invirtiendo las implicaciones que aparecen en la lista (I.1).

$$\begin{aligned} x \in \overline{X_1 \cup X_2} &\Leftarrow x \notin X_1 \cup X_2 \\ &\Leftarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Leftarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Leftarrow x \in \overline{X_1} \cap \overline{X_2} \end{aligned} \tag{I.2}$$

Esta lista (I.2) podríamos también haberla escrito como

$$\begin{aligned} x \in \overline{X_1} \cap \overline{X_2} &\Rightarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Rightarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Rightarrow x \notin X_1 \cup X_2 \\ &\Rightarrow x \in \overline{X_1 \cup X_2} \end{aligned} \tag{I.3}$$

Las listas (I.1) y (I.2) se pueden escribir abreviadamente como

$$\begin{aligned} x \in \overline{X_1 \cup X_2} &\Leftrightarrow x \notin X_1 \cup X_2 \\ &\Leftrightarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Leftrightarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Leftrightarrow x \in \overline{X_1} \cap \overline{X_2} \end{aligned} \tag{I.4}$$

Ejercicio. 3.8.
Probar todos los resultados que aparecen en la Proposición 3.6. y la Proposición 3.7. sobre propiedades de la unión, intersección y complementario de subconjuntos de un conjunto dado.

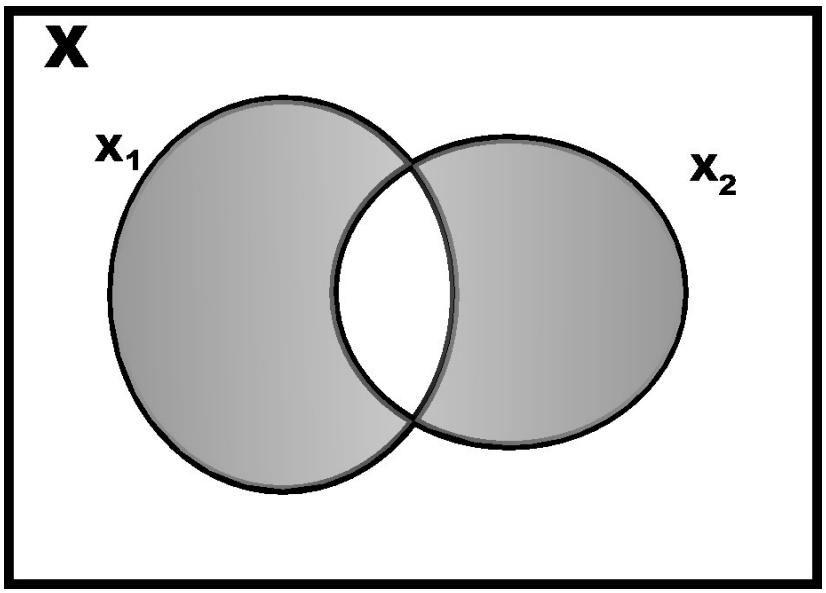
Existen muchos otros resultados sobre la unión, intersección y complementario que nos irán apareciendo a lo largo de este curso, y de otros cursos. Para su demostración podremos hacer uso de la misma técnica de demostración que hemos empleado aquí, pero también podemos hacer uso de los resultado que ya hayamos probado. Veamos un ejemplo.

Ejercicio. 3.9.
Sean X_1, X_2 subconjuntos de un conjunto X. Probar que se verifica

$$(X_1 \cap \overline{X_2}) \cup (\overline{X_1} \cap X_2) = (X_1 \cup X_2) \cap \overline{(X_1 \cap X_2)}$$

SOLUCIÓN. En este caso podemos también probar que cada elemento del primer subconjunto es un elemento del segundo y viceversa. Podéis comprobar que este proceso es largo. Es mejor entonces utilizar las relaciones que se han establecido en la Proposición 3.6. y la Proposición 3.7.. Tenemos entonces:

$$\begin{aligned} (X_1 \cap \overline{X_2}) \cup (\overline{X_1} \cap X_2) &= [X_1 \cup (\overline{X_1} \cap X_2)] \cap [\overline{X_2} \cup (\overline{X_1} \cap X_2)] \\ &= [(X_1 \cup \overline{X_1}) \cap (X_1 \cup X_2)] \cap [(\overline{X_2} \cup \overline{X_1}) \cap (\overline{X_2} \cup X_2)] \\ &= [X \cap (X_1 \cup X_2)] \cap [(\overline{X_2} \cup \overline{X_1}) \cap X] \\ &= (X_1 \cup X_2) \cap (\overline{X_2} \cup \overline{X_1}) \\ &= (X_1 \cup X_2) \cap \overline{(X_2 \cap X_1)} \\ &= (X_1 \cup X_2) \cap \overline{(X_1 \cap X_2)} \end{aligned}$$



□

El subconjunto $(X_1 \cap \overline{X_2}) \cup (\overline{X_1} \cap X_2)$ se llama la **diferencia simétrica** de X_1 y X_2. La vamos a representar por el símbolo Δ;

$$X_1 \Delta X_2 = (X_1 \cup X_2) \cap \overline{(X_1 \cap X_2)} = X_2 \Delta X_1.$$

3.2. Producto cartesiano de dos conjuntos

Dados dos conjuntos X e Y, existe un nuevo conjunto, al que llamamos el **producto cartesiano** de X e Y, cuyos elementos son:

$$X \times Y = \{(x, y) \mid \ x \in X \text{ y } y \in Y\}.$$

Si X' e Y' son subconjuntos de X e Y respectivamente, entonces $X' \times Y'$ se considera un subconjunto de $X \times Y$.

Ejercicio. 3.10.
Sean X e Y conjuntos y X_1, X_2 subconjuntos del conjunto X. Demostrar que se verifica

$$X_1 \times Y \cup X_2 \times Y = (X_1 \cup X_2) \times Y$$
$$X_1 \times Y \cap X_2 \times Y = (X_1 \cap X_2) \times Y$$

Ejercicio. 3.11.
Sean X e Y dos conjuntos y X', Y' subconjuntos de X e Y respectivamente. Demostrar que se verifica $\overline{X' \times Y'} = (\overline{X'} \times Y) \cup (X \times \overline{Y'})$

Observación. 3.12.
Hasta ahora las operaciones que hemos realizados entre conjuntos en realidad lo han sido entre subconjuntos de un conjunto dado. Podemos definir la unión o la intersección de dos conjuntos arbitrarios, pero preferimos establecer la siguiente convención o axioma.

Dados dos conjuntos X e Y, existe un conjunto Z tal que $X \subseteq Z$ e $Y \subseteq Z$.

Entonces podemos definir la unión o intersección de dos conjuntos arbitrarios apelando a la definición de unión e intersección de subconjuntos de un conjunto.

4. Aplicaciones

Sean X e Y dos conjuntos, una **aplicación** de X a Y es una regla que permite asignar a cada elemento del conjunto X un *único* elemento del conjunto Y.

Si f es una aplicación de X en Y, vamos a representar f mediante:

$$f\colon X \longrightarrow Y \quad \text{ó} \quad X \xrightarrow{f} Y$$

Si $x \in X$ y $f\colon X \longrightarrow Y$ es una aplicación, llamamos $f(x)$ al único elemento de Y que asigna f a x, y lo llamamos **imagen** de x por f.

El conjunto

$$\mathrm{Im}(f) = \{f(x) \in Y \mid \ x \in X\}$$

se llama la **imagen de la aplicación** f, y es un subconjunto de Y.

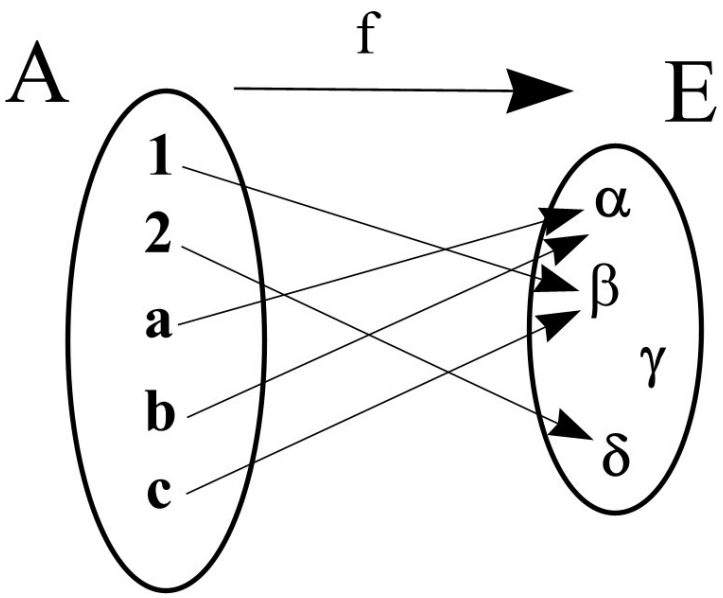
En general, si X_1 es un subconjunto de X, llamamos **imagen** de X_1 por f al subconjunto $f(X_1)$ de Y definido como:

$$f(X_1) = \{f(x) \in Y \mid \ x \in X_1\}.$$

Si Y_1 es un subconjunto de Y, llamamos **imagen inversa** de Y_1 por f al subconjunto $f^{-1}(Y_1)$ de X definido como:

$$f^{-1}(Y_1) = \{x \in X \mid \ f(x) \in Y_1\}.$$

Ejemplo. 4.1.
Sean $A = \{1, 2, a, b, c\}$ y $E = \{\alpha, \beta, \gamma, \delta\}$ dos conjuntos y f: $A \longrightarrow E$ la aplicación definida por $f(1) = \beta, f(2) = \delta, f(a) = \alpha, f(b) = \alpha, f(c) = \beta$.



Entonces la imagen de f es:

$$\mathrm{Im}(f) = \{\alpha, \beta, \delta\}.$$

La imagen de $B = \{1, 2\} \subseteq A$ es:

$$f(B) = \{\beta, \delta\}.$$

La imagen inversa de $F = \{\gamma, \delta\} \subseteq E$ es:

$$f^{-1}(F) = \{2\}.$$

Ejercicio. 4.2.
Sea $f : X \longrightarrow Y$ una aplicación y sean $A, B \subseteq X$ subconjuntos de X.

(1) Probar que $f(A \cup B) = f(A) \cup f(B)$.

(2) ¿Qué relación existe entre $f(A \cap B)$ y $f(A) \cap f(B)$?

Ejercicio. 4.3.
Sea $f : X \longrightarrow Y$ una aplicación y sean $C, D \subseteq Y$ subconjuntos de Y.

(1) Probar que $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(2) ¿Qué relación existe entre $f^{-1}(A \cap B)$ y $f^{-1}(A) \cap f^{-1}(B)$?

Vamos a establecer el concepto de aplicación de forma más rigurosa. Sean X e Y dos conjuntos, un **grafo de aplicación** de X en Y es un subconjunto G del conjunto producto cartesiano $X \times Y$ verificando la siguiente propiedad:

$$\textit{para cada } x \in X \textit{ existe un único } y \in Y \textit{ tal que } (x,y) \in G.$$

De la definición se deduce que si un par (x,y) pertenece a G, el elemento y está unívocamente determinado por el elemento x, por lo que vamos a representar y por $G(x)$. Así pues un grafo de aplicación G determina una aplicación

$$x \mapsto G(x),$$

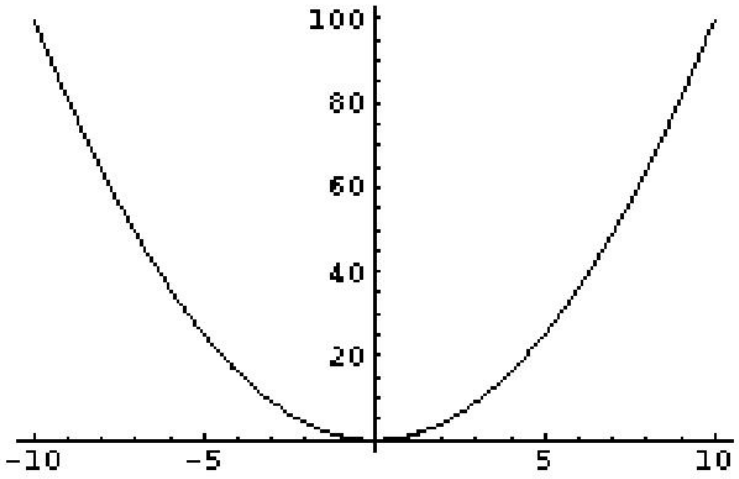
en el sentido en que las hemos definido anteriormente. Y recíprocamente, si $f\colon X \longrightarrow Y$ es una aplicación, definimos el **grafo** de f mediante

$$Gr(f) = \{(x, f(x)) \in X \times Y \mid \ x \in X\}.$$

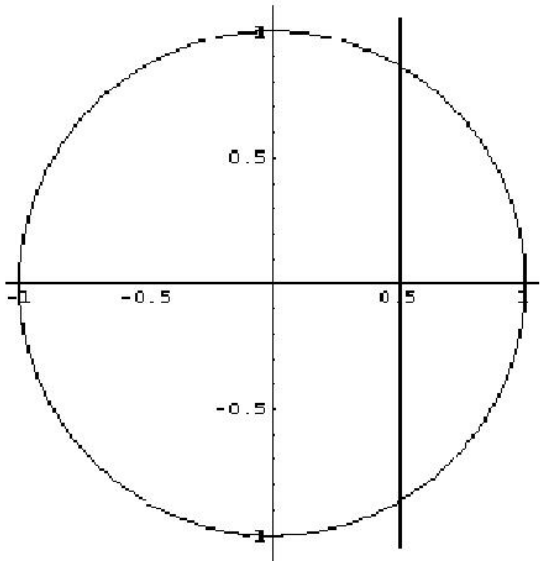
Entonces $Gr(f)$ es un grafo de aplicación.

La formalización del concepto de aplicación pasa pues por identificar los dos conceptos, el de aplicación y el de grafo de aplicación.

Ejemplo. 4.4.
Observar que si consideramos la aplicación $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$, resulta que la gráfica de la función es la parábola siguiente. Por lo tanto f es una aplicación de $\mathbb{R}$ en $\mathbb{R}$ y su grafo son los puntos de la parábola.



Observar que si consideramos la gráfica de una circunferencia $x^2 + y^2 = 1$, esta gráfica *no es un grafo de aplicación*, $x \mapsto y$, de $\mathbb{R}$ a $\mathbb{R}$, pues hay puntos, por ejemplo $x = \frac{1}{2}$ que tienen dos posibles imágenes: $\frac{\sqrt{3}}{4}$ y $-\frac{\sqrt{3}}{4}$.



En resumen. *Dados dos conjuntos X e Y, dar una aplicación f de X a Y es lo mismo que dar un subconjunto $G \subseteq X \times y$ que es un grafo de aplicación. En este caso la aplicación $f : X \longrightarrow y$ lleva cada elemento $x \in X$ en el único elemento $y \in Y$ tal que el par $(x, y) \in G$, entonces el elemento y está determinado unívocamente por x y f, por lo que lo representaremos por $f(x)$.*

4.1. Tipos de aplicaciones

Sea $f\colon X \longrightarrow Y$ una aplicación, decimos que f es **sobreyectiva** si $\mathrm{Im}(f) = Y$, esto es, si para cada elemento $y \in Y$ existe un elemento $x \in X$ tal que $f(x) = y$.

Llamamos **inyectiva** a una aplicación $f\colon X \longrightarrow Y$ tal que para cualesquiera dos elementos x_1, $x_2 \in X$, si $f(x_1) = f(x_2)$, entonces $x_1 = x_2$.

Ejercicio. 4.5.
Sea $g\colon \mathbb{Q}^+ \longrightarrow \mathbb{Q}^+$ definida por $f(x) = x^2$ para cada $x \in \mathbb{Q}^+$. Probar que la aplicación g es inyectiva y no es sobreyectiva.

SOLUCIÓN. Para comprobarlo procedemos como sigue: si $g(x_1) = g(x_2)$, entonces tenemos $x_1^2 = x_2^2$, de donde deducimos que $x_1 = x_2$, ya que ambos son positivos.

Sin embargo g no es una aplicación sobreyectiva, ya que por ejemplo $2 \notin \mathrm{Im}(g)$.

Para comprobarlo basta suponer que esto no fuese cierto, entonces existiría un elemento $x \in \mathbb{Q}^+$ tal que $x^2 = 2$, lo cual es imposible, ya que $\sqrt{2}$ no es un número racional. □

Ejemplo. 4.6.
La aplicación f del ejemplo de la página 21 no es sobreyectiva ya que $\gamma \notin \mathrm{Im}(f)$, y no es inyectiva, ya que, por ejemplo, $f(1) = \beta = f(c)$.

Una aplicación $f\colon X \longrightarrow Y$ que es a la vez inyectiva y sobreyectiva se llama una **aplicación biyectiva** o una **biyección**.

Ejemplo. 4.7.
La aplicación $h : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ definida $h(x) = x^2$ para cada $x \in \mathbb{R}$ es una biyección.

4.2. Composición de aplicaciones

Supongamos que $f\colon X \longrightarrow Y$ y $g\colon Y \longrightarrow Z$ son aplicaciones, definimos una nueva aplicación $g \circ f\colon X \longrightarrow Z$ como sigue:

$$(g \circ f)(x) = g(f(x)) \text{ para cada } x \in X.$$

$g \circ f$ se llama la **composición** de f y g. La composición de f y g se suele representar también simplemente por gf.

Para cada conjunto X existe una aplicación especial, llamada **identidad** en X, a la que representamos por 1_X y que está definida por $1_X(x) = x$ para cada $x \in X$.

Lema. 4.8.
Sea $f\colon X \longrightarrow Y$ una aplicación. Se verifica $f \circ 1_X = f$ y $1_Y \circ f = f$.

Si $f\colon X \longrightarrow Y$ es una aplicación, llamamos una **aplicación inversa** de f a una aplicación $g\colon Y \longrightarrow X$ que verifica $f \circ g = 1_Y$ y $g \circ f = 1_X$.

Observación. 4.9.
En general si una aplicación f tiene una inversa, esta inversa se representa por f^{-1}.

¡OJO!. No confundir con la notación f^{-1} utilizada para la imagen inversa de un subconjunto.

Lema. 4.10.
Si una aplicación $f\colon X \longrightarrow Y$ tiene una inversa, entonces es una biyección.

Ejercicio. 4.11.
Demostrar que si $f\colon X \longrightarrow Y$ es una biyección, entonces existe una inversa de f.

Tenemos entonces que una aplicación $f\colon X \longrightarrow Y$ es biyectiva si y solo si tiene una inversa.

Observación. 4.12.
Observar que al decir que una aplicación $f : X \longrightarrow Y$ tiene una inversa hemos dicho que existe una aplicación $g : Y \longrightarrow X$ verificando $fg = 1_Y$ y $gf = 1_X$, no basta con solo una de las igualdades, ya que dada la aplicación $f : \{1,2\} \longrightarrow \{a\}$ existe una aplicación $g : \{a\} \longrightarrow \{1,2\}$ verificando $fg = 1_{\{a\}}$, pero no es biyectiva. En efecto, es fácil ver que no es una aplicación inyectiva.

5. Relaciones de equivalencia y de orden

Una **relación** R en un conjunto X es una regla que permite distinguir si dos elementos están o no relacionados. Si dos elementos $x, y \in X$ están relacionados mediante la relación R escribimos xRy.

Veamos algunas de las propiedades que *puede* verificar una relación.

Propiedad reflexiva. Decimos que la relación R verifica la propiedad reflexiva si para cada elemento $x \in X$ se verifica xRx.

$$\forall x \in X,\ xRx.$$

Propiedad simétrica. Decimos que R verifica la propiedad simétrica si cuando para dos elementos $x, y \in X$ se verifica xRy, entonces también se tiene yRx.

$$\forall x, y \in X,\ \text{si } xRy,\ \text{entonces } yRx.$$

Propiedad transitiva. Decimos que R verifica la propiedad transitiva si cuando para tres elementos $x, y, z \in X$ se verifica xRy e yRz, entonces también se verifica xRz.

$$\forall x, y, z \in X,\ \text{si } xRy \text{ e } yRz,\ \text{entonces } xRz.$$

Propiedad antisimétrica. Decimos que R verifica la propiedad antisimétrica si cuando para dos elementos $x, y \in X$ se verifica xRy e yRx, entonces se verifica $x = y$.

$$\forall x, y \in X,\ \text{si } xRy \text{ e } yRx,\ \text{entonces } x = y.$$

Vamos a poner ejemplos de relaciones que verifican algunas de estas propiedades.

Ejemplo. 5.1.
Consideramos el conjunto $\mathbb{N}$ de los números naturales y definimos aRb si existe $c \in \mathbb{N}$ tal que $a = b + 2c$ ó $b = a + 2c$. Entonces R verifica las propiedades reflexiva, simétrica y transitiva.

Ejemplo. 5.2.
Consideramos el conjunto $\mathbb{Z}$ de los números naturales y definimos aRb si $a - b$ es un múltiplo de 2, (existe $c \in \mathbb{Z}$ tal que $a - b = 2c$). Entonces R verifica las propiedades reflexiva, simétrica y transitiva.

Ejemplo. 5.3.
Consideramos el conjunto $\mathbb{N}$ de los números naturales y definimos la relación $a \mid b$ si existe $c \in \mathbb{N}$ tal que $b = ac$. Entonces $\mid$ verifica las propiedades reflexiva, antisimétrica y transitiva.

Ejemplo. 5.4.
Consideramos el conjunto $\mathbb{Z}$ de los números enteros y definimos la relación $a \mid b$ si existe $c \in \mathbb{Z}$ tal que $b = ac$. Entonces $\mid$ verifica las propiedades reflexiva y transitiva, y *no verifica la propiedad antisimétrica.*

Si R es una relación en un conjunto X, podemos considerar el **grafo** de R como el subconjunto

$$Gr(R) = \{(x, y) \in X \times X \mid \ xRy\}.$$

Está claro que definir una relación en un conjunto X es lo mismo que dar su grafo, esto es, un subconjunto de $X \times X$.

El uso de grafos permite hacer algunas construcciones sobre relaciones de forma fácil.

Observar los siguientes hechos:
(1). Una relación R es *reflexiva* si y solo si la diagonal de $X \times X$ está incluida en el grafo de R.
(2). Una relación R es *simétrica* si y solo si el grafo de R es simétrico respecto a la diagonal. (Esto es, si $(x, y) \in Gr(R)$, entonces $(y, x) \in Gr(R)$.

5.1. Relación de equivalencia

Decimos que una relación R que verifica las propiedades reflexiva, simétrica y transitiva es una **relación de equivalencia**.

Si R es una relación de equivalencia en un conjunto X, para cada elemento $a \in X$ definimos la **clase de equivalencia** de a como el subconjunto

$$\overline{a} = [a] = \{x \in X \mid \ aRx\}.$$

Lema. 5.5.
Si $a, b \in X$, entonces se verifica $\overline{a} = \overline{b}$ ó $\overline{a} \cap \overline{b} = \varnothing$, esto es, cada dos clases de equivalencia ó son iguales ó son disjuntas.

Si R es una relación de equivalencia en un conjunto X, el conjunto de todas las clases de equivalencia se llama el **conjunto cociente** de X por R, y se representa por X/R.

Ejercicio. 5.6.
En el conjunto $\mathbb{R} \times \mathbb{R}$ se considera la relación

$$(a_1, a_2)R(b_1, b_2) \text{ si } a_1^2 + a_2^2 = b_1^2 + b_2^2.$$

Probar que R es una relación de equivalencia en $\mathbb{R} \times \mathbb{R}$ y describir el conjunto cociente.

Si R es una relación de equivalencia en un conjunto X y X/R es el conjunto cociente, existe una aplicación sobreyectiva p: $X \longrightarrow X/R$ que a cada elemento $x \in X$ le asocia $p(x) = \overline{x}$.

5.2. Relación de orden

Decimos que una relación R que verifica las propiedades reflexiva, antisimétrica y transitiva es una **relación de orden**.

Un conjunto X junto con una relación de orden se llama un conjunto **parcialmente ordenado**.

Si Y es un subconjunto de un conjunto parcialmente ordenado X con relación orden R, llamamos:

elemento maximal de Y a un elemento $m \in Y$ tal que no existe ningún elemento $y \in Y$ tal que mRy.

cota superior de Y en X a un elemento $c \in X$ tal que yRc para cada elemento $y \in Y$.

elemento máximo de Y a un elemento $m \in Y$ tal que yRm para cada elemento $y \in Y$. Esto es, un máximo de Y es una cota superior de Y en X que pertenece a Y.

Ejercicio. 5.7.
Demostrar que en un conjunto parcialmente ordenado el elemento máximo de un subconjunto, si existe, es único.

SOLUCIÓN. Sea Y un subconjunto de un conjunto X con una relación de orden R, y supongamos que Y tiene dos elementos máximos m_1 y m_2. Por ser m_1 un máximo de Y y ser $m_2 \in Y$ se verifica $m_2 R m_1$.

Por análogos motivos se verifica $m_1 R m_2$.

Entonces como R verifica la propiedad antisimétrica, se verifica $m_1 = m_2$ y el máximo de Y es único. □

También existen las nociones duales, esto es, las nociones de **elemento minimal**, de **cota inferior** y de **elemento mínimo** ó **primer elemento**.

Finalmente, un elemento $s \in X$ se dice que es un **supremo** de Y si es un mínimo del conjunto de las cotas superiores de Y. El concepto dual es el de **ínfimo**.

Ejercicio. 5.8.
Escribir las nociones aquí mencionadas para una relación de orden en X representada por el símbolo $\leq$ en vez del símbolo R.

Ejercicio. 5.9.
Orden lexicográfico Se considera $\mathbb{N} \times \mathbb{N}$, y en él la relación:

$$(a,b) \leq (c,d), \text{ si } a < c \text{ ó } a = c \text{ y } b \leq d.$$

Demuestra que esta relación es una relación de orden en $\mathbb{N} \times \mathbb{N}$.

Nota. Es preciso destacar que las definiciones que hemos hecho de conjunto, aplicación entre conjuntos y relación en un conjunto carecen totalmente de rigurosidad. El objetivo hasta aquí ha sido señalar que, en este momento, nos interesa más el manejo de los conceptos que los conceptos en sí mismos.

De cualquier forma remitimos al alumno o alumnos interesados en profundizar en estos conceptos a los libros de la bibliografía para definiciones más rigurosas de las nociones aquí introducidas.

6. Cuantificadores

Sea $\mathbb{R}$ el conjunto de los números reales. Para cada número natural n definimos un subconjunto C_n de $\mathbb{R}$ mediante

$$C_n = [0, n) = \{r \in \mathbb{R} \mid \ 0 \leq r < n\} = [0, n).$$

El menor subconjunto de $\mathbb{R}$ que contiene a todos los C_n es exactamente $[0, \infty)$.

Podemos hablar entonces de la unión de todos los subconjuntos C_n, para n un número natural, y representamos esta unión como

$$\cup\{C_n \mid \ n \in \mathbb{N}\} \quad \text{ó} \quad \cup_{n\in\mathbb{N}} C_n.$$

Si consideramos ahora un conjunto X y subconjuntos X_n de X, entonces también podemos definir la unión de los subconjuntos X_n; esta será:

$$\cup\{X_n \mid \ n \in \mathbb{N}\} \quad \text{ó} \quad \cup_{n\in\mathbb{N}} X_n,$$

y sus elementos son

$$\{x \in X \mid \ \text{existe un } n \in \mathbb{N} \text{ tal que } x \in X_n\}.$$

Aquí hemos utilizado como conjunto de índices el conjunto $\mathbb{N}$, pero esto no es imprescindible y podríamos haber utilizado otro conjunto, supongamos que Λ, con elementos λ. Tendremos entonces

$$\cup\{X_\lambda \mid \ \lambda \in \Lambda\} = \cup_{\lambda\in\Lambda} X_\lambda = \{x \in X \mid \ \text{existe un } \lambda \in \Lambda \text{ tal que } x \in X_\lambda\}.$$

La intersección de los subconjuntos X_λ se define entonces como

$$\cap\{X_\lambda \mid \ \lambda \in \Lambda\} = \cap_{\lambda\in\Lambda} X_\lambda = \{x \in X \mid \ \text{para cada } \lambda \in \Lambda \text{ se tiene } x \in X_\lambda\}.$$

En todo este proceso nos aparecen dos cuantificadores, el **cuantificador existencial**, usado en la definición de unión, y el **cuantificador universal**, usado en la intersección. Vamos a representar por $\exists$ el cuantificador existencial y por $\forall$ el cuantificador universal.

Escribimos entonces

$$\cup\{X_\lambda \mid \ \lambda \in \Lambda\} = \{x \in X \mid \ \exists\lambda \in \Lambda, \ x \in X_\lambda\}.$$

y

$$\cap\{X_\lambda \mid \ \lambda \in \Lambda\} = \{x \in X \mid \ \forall\lambda \in \Lambda, \ x \in X_\lambda\}.$$

Las afirmaciones que tienen una variable en vez de proposiciones las vamos a llamar **funciones proposicionales**, de forma que si $\mathbf{A}(x)$ es una función proposicional, para cada valor a del argumento x tenemos que $\mathbf{A}(a)$ es una proposición.

En el ejemplo anterior $x \in X_\lambda$ es una *función proposicional* con variable λ. *Los cuantificadores actúan pues sobre las variables de las funciones proposicionales.*

Ejemplo. 6.1.

(I) Se considera la función proposicional $P(X)$ definida por: "X es mayor que 2".

(II) Se consideran el cuantificador $\exists$ y la proposición:

$$\exists x \in C,\ P(x).$$

Esta proposición se lee: *existe x en C tal que $P(x)$ es cierta*, esto es, "existe un elemento x en C tal que x es mayor que 2". Es cierta si C es por ejemplo el conjunto $\{0,1,2,3\}$ y falsa si C es el conjunto $\{-1,0,1,2\}$.

(III) Si se considera el cuantificador $\forall$ y la proposición:

$$\forall x \in C,\ P(x).$$

Esta proposición se lee: *para todo x en C se tiene que $P(x)$ es cierta*, esto es, "para todo elemento x en C se tiene que x es mayor que 2". Es cierta si C es por ejemplo el conjunto $\{3,4,5\}$ y es falsa si C es el conjunto $\{0,1,2,3\}$.

6.1. Relación de equivalencia y partición de un conjunto

Una **partición de un conjunto** X es un conjunto de subconjuntos de X, disjuntos dos a dos, cuya unión es X.

Si R es una relación de equivalencia en un conjunto X, entonces el conjunto de las clases de equivalencia, para la relación de equivalencia R, forma una partición de X; *la llamamos la partición definida por la relación R.*

El resultado recíproco también es cierto, esto es, para cualquier partición $\{X_\lambda \mid \lambda \in \Lambda\}$ de un conjunto X, existe una relación de equivalencia R en X de forma que la partición definida por R coincide con la partición $\{X_\lambda \mid \lambda \in \Lambda\}$.

En efecto, basta definir R como sigue: *"si x e y son elementos de X entonces xRy si x e y pertenecen a un mismo subconjunto X_λ"*.

Lema. 6.2.
La relación R, así definida, es una relación de equivalencia.

DEMOSTRACIÓN. (1). Propiedad reflexiva. Para cada $x \in X$, ya que la unión de los subconjuntos X_λ es X, existe un índice $\lambda \in \Lambda$ tal que $x \in X_\lambda$, luego xRx.

$$\forall x \in X,\ xRx$$

(2). Propiedad simétrica. Para cualesquiera $x, y \in X$, si xRy, entonces existe un índice $\lambda \in \Lambda$ tal que $x, y \in X$, pero es claro que también se verifica $y, x \in X_\lambda$, ya que el orden de los elementos x e y es irrelevante, entonces yRx.

$$\forall x \in X, \forall y \in X,\ xRy \implies yRx$$

(3). Propiedad transitiva. Para cualesquiera $x, y, z \in X$, si xRy e yRz, entonces existen índices $\lambda, \mu \in \Lambda$ tales que $x, y \in X_\lambda$ e $y, z \in X_\mu$. Como $X_\lambda = X_\mu$ ó $X_\lambda \cap X_\mu = \varnothing$ y se verifica $y \in X_\lambda \cap X_\mu$, resulta $X_\lambda = X_\mu$, luego $x, z \in X_\lambda$ y tenemos xRz.

$$\forall x \in X, \forall y \in X, \forall z \in X,\ xRy \text{ e } yRz \implies xRz$$

□

Ejercicio. 6.3.
Se considera el conjunto $N = \{1, 2\}$. Determinar la relación de equivalencia que define la partición $\{\{1\}, \{2\}\}$.

Ejercicio. 6.4.
Obtener la partición dada por la relación de equivalencia del Ejemplo 5.1..

Ejercicio. 6.5.
Dar la relación de equivalencia en $\mathbb{N} \setminus \{0\}$ que da la siguiente partición:

$$\{1, \ldots, 9\}, \{10, 11, \ldots, 99\}, \{100, 101, \ldots, 999\}, \ldots$$

Queremos hacer un comentario sobre las notaciones anteriores. Como ya hemos señalado, el símbolo $\implies$ indica que la afirmación tras el símbolo es cierta cuando lo es la afirmación que aparece antes de él. En la página 33 aparece $xRy \Rightarrow yRx$, esto es, *si se verifica xRy, entonces se verifica yRx*. Una forma alternativa de leerlo es la siguiente: *xRy implica yRx*.

Aquí vamos a usarlo, en combinación con los cuantificadores en múltiples contextos.

Veamos un ejemplo. Consideramos el conjunto $A = \{1, 2, a, b, c\}$ y los subconjuntos $B = \{1, 2\}$ y $B_1 = \{1, 2, a\}$. Como B es un subconjunto de B_1 se tiene:

$$\forall x \in A,\ x \in B \implies x \in B_1$$

Si quisiéramos expresar que B_1 no es un subconjunto de B tendríamos que escribir:

$$\exists x \in A,\ x \in B_1 \text{ y } x \notin B$$

En efecto esta segunda expresión es la negación de la primera, ya que $\mathbf{A} \Longrightarrow \mathbf{B}$ está definido como $(\neg\mathbf{A}) \vee \mathbf{B}$. En forma simbólica se escriben

$$\forall x \in A,\ \mathbf{A}(x) \Longrightarrow \mathbf{B}(x)$$

o equivalentemente

$$\forall x \in A,\ (\neg\mathbf{A}(x)) \vee \mathbf{B}(x)$$

y su negación, que sería:

$$\exists x \in A,\ \mathbf{A}(x) \wedge (\neg\mathbf{B}(x))\ [= \neg((\neg\mathbf{A}(x)) \vee \mathbf{B}(x))]\,.$$

7. Métodos de demostración

A continuación vamos a ver cómo hacer demostraciones de algunos resultados en Matemáticas. Aunque ya hemos hecho alguna en lo que llevamos expuesto, se trata aquí de hacer un pequeño resumen de estos métodos.

7.1. Método directo

Consiste en probar $\mathbf{A} \Longrightarrow \mathbf{B}$ directamente, haciendo uso de las definiciones y resultados previos.

Hasta ahora las demostraciones que hemos hecho son todas directas. Pero existen otros métodos de hacer demostraciones que vamos a detallar.

7.2. Método contra-recíproco

Consiste en probar $\mathbf{A} \Longrightarrow \mathbf{B}$ mediante una demostración directa de la proposición equivalente $(\neg\mathbf{B}) \Longrightarrow (\neg\mathbf{A})$

7.3. Método de reducción al absurdo

Consiste en probar $\mathbf{A} \Longrightarrow \mathbf{B}$ mediante una demostración directa de una de las siguientes proposiciones:

$$\mathbf{A} \wedge (\neg\mathbf{B}) \Longrightarrow \neg\mathbf{A} \quad \text{ó}$$

$$\mathbf{A} \wedge (\neg\mathbf{B}) \Longrightarrow \mathbf{B}.$$

La siguiente es una demostración por reducción al absurdo utilizando el siguiente argumento: "*Si de una afirmación (A) se deduce una afirmación (B), que es falsa, entonces la afirmación (A) es falsa*".

(Nota. Observar la tabla de verdad de $\Rightarrow$.)

Teorema. 7.1. (Teorema de Euclides)
Existen infinitos números naturales primos.

DEMOSTRACIÓN. Supongamos que no es cierto el enunciado del Teorema, entonces hay únicamente un número finito de números naturales primos, sean estos $p_1, \ldots, p_t$. El número $q = p_1 \cdots p_t + 1$ da de resto 1 al dividirlo por todos los primos conocidos. Tenemos pues un número distinto de 0 y 1 que no es un producto de números primos, lo que es una contradicción.

Afirmación (**A**): *no es cierto el enunciado del Teorema.*

Afirmación (**B**): *existe un número natural distinto de 0 y 1 que no es un producto de números primos.*

Hemos probado que $\mathbf{A} \Rightarrow \mathbf{B}$, pero como sabemos que siempre se verifica $\neg\mathbf{B}$, llegamos a probar la implicación $\neg\mathbf{B} \Rightarrow \neg\mathbf{A}$ que era lo que queríamos. □

Otro ejemplo de demostración por reducción al absurdo se obtiene al probar el siguiente resultado:

Ejercicio. 7.2.
Demostrar que $\sqrt{2}$ no es un número racional.

7.4. Enunciados de teoremas

Teorema directo:	$\mathbf{A}$	$\Longrightarrow$	$\mathbf{B}$
Teorema contrario:	$(\neg\mathbf{A})$	$\Longrightarrow$	$(\neg\mathbf{B})$
Teorema recíproco:	$\mathbf{B}$	$\Longrightarrow$	$\mathbf{A}$
Teorema contra-recíproco:	$(\neg\mathbf{B})$	$\Longrightarrow$	$(\neg\mathbf{A})$

Son equivalentes
el teorema directo y el contra-recíproco
y también son equivalentes, entre sí
el teorema contrario y el recíproco.

Veamos un ejemplo.

Vamos a suponer que X e Y son conjuntos finitos y que $f\colon X \longrightarrow Y$ es una aplicación.

Enunciado directo:

Lema. 7.3.
Si f es inyectiva, entonces $\mathrm{Card}(X) \leq \mathrm{Card}(Y)$.

El enunciado contra-recíproco, y equivalente, de este Lema es el siguiente:

Lema. 7.4. (Principio del palomar)
Si $\mathrm{Card}(Y) < \mathrm{Card}(X)$, *entonces f no es inyectiva.*

Es claro que los enunciados son equivalentes:
Vamos a llamar **A** a la afirmación *"f es inyectiva"* y **B** a la afirmación *"*$\mathrm{Card}(X) \leq \mathrm{Card}(Y)$*"*.
Entonces el Lema 7.3. se escribe

$$\mathbf{A} \Longrightarrow \mathbf{B}$$

y el Lema 7.4. se escribe

$$(\neg\mathbf{B}) \Longrightarrow (\neg\mathbf{A}).$$

Capítulo II

Números naturales y números enteros

8. Números naturales

Vamos a representar por $\mathbb{N}$ al conjunto de los *números naturales,* por lo tanto $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$.

La primera propiedad que vamos a utilizar de los números naturales es la siguiente:

Propiedad I.
En $\mathbb{N}$ hay un elemento distinguido*, el* cero*, al que vamos a representar por 0, y cualquier elemento de $\mathbb{N}$, distinto de cero, se puede obtener a partir de 0 repitiendo, el número de veces que sea necesario, una operación que vamos a llamar* siguiente *(y que se puede interpretar como sumar 1).*

Observar que cada número natural, salvo el cero, es el **siguiente** de otro al que llamaremos su **anterior**.

Como consecuencia los números naturales son, según la representación que usemos:

0			
1	$0+1$	$0+1$	I
2	$(0+1)+1$	$1+1$	II
3	$((0+1)+1)+1$	$2+1$	III
4	$\vdots$	$3+1$	IV
5	$\vdots$	$4+1$	V
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Observar que en la columna de la izquierda aparece una forma, como otra, de representar a los números naturales.

Propiedad II.
El conjunto $\mathbb{N}$ *de los números naturales verifica el* ***Principio de Inducción****:* Si $Y \subseteq \mathbb{N}$ es un subconjunto que contiene a cero, $0 \in Y$, y si para cada elemento $y \in Y$ se verifica $y+1 \in Y$, entonces $Y = \mathbb{N}$.

En el conjunto $\mathbb{N}$ tenemos dos operaciones, la **suma** $(+)$ y el **producto** $(\times)$, las cuales verifican las propiedades:

$a+b=b+a$	P. Conmutativa	$a\times b=b\times a$
$a+(b+c)=(a+b)+c$	P. Asociativa	$a\times(b\times c)=(a\times b)\times c$
$a+0=a$	Elemento cero	$a\times 0=0$
	Elemento uno	$a\times 1=a$
	P. Distributiva	$a\times(b+c)=a\times b+a\times c$

para cualesquiera números $a, b, c \in \mathbb{N}$.

Se verifican también las siguientes propiedades de simplificación:

$$\begin{array}{lcl} a+c=b+c & \Rightarrow & a=b \\ a\times c=b\times c \text{ y } c\neq 0 & \Rightarrow & a=b \\ a\times c=0 \text{ y } c\neq 0 & \Rightarrow & a=0 \end{array}$$

Veamos una sencilla aplicación del *Principio de Inducción.*

Ejemplo. 8.1.
Es bien conocido que se verifican las siguientes relaciones:

$$\begin{aligned} 1+2 &= 3=\tfrac{6}{2}\\ 1+2+3 &= 6=\tfrac{12}{2}\\ 1+2+3+4 &= 10=\tfrac{20}{2}\\ &\vdots \end{aligned}$$

En donde los numeradores de las fracciones se consiguen fácilmente como:

$$\begin{aligned} &(1+2)\times 2,\\ &(1+3)\times 3,\\ &(1+4)\times 4,\\ &\vdots \end{aligned}$$

Podemos entonces conjeturar que se verifica el siguiente resultado:

Lema. 8.2.
$1+2+3+\cdots+t$ *es igual a* $\frac{(1+t)\times t}{2}$.

Para probar que esto es así procedemos como sigue:

(1). Llamamos $Y=\{n\in\mathbb{N}\mid\ 1+2+3+\cdots+n=\frac{(1+n)\times n}{2}\}\cup\{0\}$, el incluir 0 en Y es debido al hecho de que no tenemos definida la suma anterior para el valor $n=0$ si, como es natural, las sumas las comenzamos siempre en 1.

(2). Es claro que $0,1,2,3,4\in Y$.

(3). Si $t\in Y$, vamos a ver que también $t+1\in Y$. En efecto, se tiene:

$$\begin{aligned} 1+2+3+\cdots+t+(t+1) &= (1+2+3+\cdots+t)+(t+1)\\ &= \tfrac{(1+t)\times t}{2}+(t+1) \qquad = \left(\tfrac{t}{2}+1\right)\times(t+1)\\ &= \left(\tfrac{t+2}{2}\right)\times(t+1) \qquad = \tfrac{(t+2)\times(t+1)}{2}\\ &= \tfrac{(1+(t+1))\times(t+1)}{2} \end{aligned}$$

y por tanto $t+1\in Y$. Por el principio de inducción se tiene $Y=\mathbb{N}$.

8.1. El orden natural

En el conjunto $\mathbb{N}$ tenemos una relación ($\leq$), definida por

$$a \leq b \text{ si existe } c \in \mathbb{N} \text{ tal que } b = a + c.$$

Observar que para cada número entero n se verifica $0 \leq n$ ya que siempre se tiene: $n = 0 + n$.

Escribimos $a < b$ si $a \leq b$ y $a \neq b$. Si $a, b, c \in \mathbb{N}$ se verifica

$$a + c < b + c \text{ si y solo si } a < b.$$

Para el producto tenemos un resultado similar, si $a, b, c \in \mathbb{N}$ y $c \neq 0$, se verifica

$$a \times c < b \times c \text{ si y solo si } a < b.$$

Se tiene también que si $a < b$, entonces $a + 1 \leq b$.

La primera propiedad sobre la relación $\leq$ es:

Lema. 8.3.
La relación $\leq$ es una relación de orden en $\mathbb{N}$, esto es, tenemos que $\mathbb{N}$ es un conjunto parcialmente ordenado.

Un conjunto parcialmente ordenado X con relación de orden R se llama **totalmente ordenado**, si para cada par de elementos

$$x, y \in X \text{ se tiene } xRy \text{ ó } yRx.$$

Corolario. 8.4.
El conjunto $\mathbb{N}$, junto con la relación de orden $\leq$, es un conjunto totalmente ordenado.

Un conjunto parcialmente ordenado X con relación de orden R se llama **bien ordenado** si para cada subconjunto no vacío $Y \subseteq X$ existe el mínimo de Y (también nos podemos referir a este mínimo como **primer elemento**).

En este caso también se suele decir que la relación de orden R es un **buen orden**.

Corolario. 8.5.
El conjunto $\mathbb{N}$ junto con la relación de orden $\leq$ es un conjunto bien ordenado.

DEMOSTRACIÓN. La demostración se hace utilizando el principio de inducción. Sea Y un subconjunto no vacío de $\mathbb{N}$, y supongamos que Y no tiene un primer elemento. Llamamos Z al conjunto de números naturales definido por:

$$Z = \{n \in \mathbb{N} \mid \ n \leq y \text{ para cada } y \in Y\}.$$

Es claro que $0 \in Z$, ya que 0 es menor que cualquier elemento de $\mathbb{N}$, y por tanto de Y. Supongamos que tenemos un $n \in Z$. Si $n \in Y$, entonces n es un primer elemento de Y, lo que es una contradicción. Si $n \notin Y$, entonces $n < y$ para cada $y \in Y$, luego $n+1 \leq y$ para cada $y \in Y$ y tenemos $n+1 \in Z$. Ahora el principio de inducción nos dice que $Z = \mathbb{N}$. Pero como Y es no vacío, tenemos un elemento $y \in Y$, y como $y+1 \in \mathbb{N} = Z$, resulta que $y+1 \leq y$, lo que es una contradicción. □

Observar que como consecuencia del Corolario 8.5. se tiene:

Lema. 8.6.
No existen cadenas infinitas estrictamente decrecientes de números naturales.

Una **cadena** en un conjunto parcialmente ordenado es un subconjunto no vacío tal que para cada par de elementos a y b se tiene $a \leq b$ ó $b \leq a$. Es claro que $\mathbb{N}$, junto con el orden que hemos definido, es una cadena.

8.2. Definición por recurrencia

Los números naturales aparecen en todos los campos de la Matemática y de las ciencias en general. Vamos a analizar en detalle un tipo usual de definición en la que los números naturales juegan un papel fundamental, es la definición por recurrencia.

Una **sucesión** de números reales es simplemente asignar a cada número natural un número real (se puede imaginar como una aplicación a de $\mathbb{N}$ en $\mathbb{R}$). Como los números naturales son 0,1,2,3, etc., los elementos que conforman la sucesión se escriben en la misma forma:

$$a_0, a_1, a_2, a_3, \ldots$$

y de forma abreviada como $\{a_n\}_n$. Cada uno de los a_i lo llamamos un **término** de la sucesión. Observar que ahora $\{a_0, a_1, a_2, a_3, \ldots\}$ no es un conjunto, pues en la sucesión puede haber términos repetidos.

Hay numerosos ejemplos de sucesiones. En algunos casos sus términos siguen reglas prefijadas que hacen fácil su descripción; en otros casos los términos son fáciles de calcular a partir de los términos anteriores. Pero en general los términos de una sucesión no van a verificar reglas que permitan una fácil descripción de los mismos.

Ejemplo. 8.7.

(1) La sucesión $\{a_n\}_n$, siendo $a_n = 1$ para cada índice n.

(2) La sucesión $\{a_n\}_n$, siendo a_n la cifra n–ésima en el desarrollo decimal de $\frac{1}{7}$ y $a_0 = 0$.

(3) La sucesión $\{a_n\}_n$, siendo a_n la cifra n–ésima en el desarrollo decimal de π y $a_0 = 3$.

(4) La sucesión $\{a_n\}_n$, siendo a_n la suma de los dos términos anteriores, con valores iniciales $a_0 = 0$ y $a_1 = 1$.

(5) La sucesión $\{a_n\}_n$, siendo $a_n = \frac{1}{n}$.

Es claro que salvo en el caso (3), en todos los demás es sencillo, o al menos lo parece, el calcular cualquier término de la sucesión.

Vamos a centrarnos en esta parte en estudiar un caso similar a las sucesiones del tipo de las definidas en el caso (4).

Decimos que una sucesión verifica una **regla de recurrencia** si el término n–ésimo (n es variable) puede calcularse en función de t términos anteriores (t es fijo). El caso más sencillo lo proporcionan las sucesiones o progresiones aritméticas y geométricas.

8.3. Sucesiones aritméticas

Una sucesión $\{a_n\}_n$ se dice que es una **sucesión aritmética** o una **progresión aritmética** si existe un número real d tal que para cada n el término a_{n+1} se calcula como $a_{n+1} = a_n + d$. Observar que como consecuencia de la definición una sucesión aritmética está determinada por el primer término a_0 y el número d.

Llamamos a a_0 el **término inicial** de la sucesión y a d la **diferencia** que define la progresión.

Ejemplo. 8.8.

(1) Escribir los diez primeros términos de la progresión aritmética definida por $a_0 = 2$ y $d = 4$.

(2) Escribir los diez primeros términos de la progresión aritmética definida por $a_0 = 1$, $d = 0$.

(3) Escribir los diez primeros términos de la progresión aritmética definida por $a_0 = 0$, $d = 1$.

(4) Escribir los diez primeros términos de la progresión aritmética definida por $a_0 = \pi$, $d = 0,5$.

Dada una progresión aritmética hay dos problemas que son fácilmente resolubles, el primero consiste en calcular la forma que tendrá el término general, esto es, el término a_n para cualquier valor de n, es evidente que esta forma en general dependerá de a_0, d y n, y el segundo problema es el cálculo de la suma de s términos consecutivos.

8.4. El término general de una progresión aritmética

Los términos de la progresión aritmética son:

$$a_0, a_1 = a_0 + d, a_2 = a_1 + d, a_3 = a_2 + d, a_4 = a_3 + d, \ldots$$

Es claro que si en la expresión de a_2 en vez de a_1 escribimos su valor, tenemos:

$$a_2 = a_1 + d = a_0 + d + d = a_0 + 2d.$$

Para ver que este resultado es cierto para cada valor de n, esto es, que $a_n = a_0 + nd$, vamos a hacer inducción sobre n.

Si $n = 0$, es claro que $a_0 = a_0 + 0d$; suponemos que el resultado es cierto para $t \geq 0$ y vamos a ver que también lo es para $t + 1$:

$$a_{t+1} = a_t + d = a_0 + td + d = a_0 + (t + 1)d.$$

8.5. La suma de s términos consecutivos

Queremos calcular el valor de $a_n + a_{n+1} + a_{n+2} + \cdots + a_{n+s-1}$.

Utilizando el resultado previo escribimos $a_t = a_0 + td$, la suma resulta igual a

$$\begin{aligned}
&a_n + a_{n+1} + a_{n+2} + \cdots + a_{n+s-1} \\
&= (a_0 + nd) + (a_0 + (n+1)d) + (a_0 + (n+2)d) + \cdots + (a_0 + (n+s-1)d) \\
&= s(a_0 + nd) + (0 + 1 + \ldots + (s-1))\, d \\
&= s(a_0 + nd) + \tfrac{(s-1)sd}{2} \\
&= s\left(\tfrac{2a_0+2nd+(s-1)d}{2}\right) = s\left(\tfrac{a_0+nd+a_0+(n+s-1)d}{2}\right) = \tfrac{(a_n+a_{n+s-1})s}{2}
\end{aligned}$$

Cuando $n = 0$, esto es, cuando la suma comienza con el primer término de la progresión, entonces resulta

$$a_0 + a_1 + a_2 + \cdots + a_{s-1} = \frac{(a_0 + a_{s-1})s}{2}.$$

Ejercicio. 8.9.
Se considera la sucesión cuyos primeros términos son: 1, 5, 9, 13, 17, ...

(1) Calcular el término general de esta sucesión.

(2) Calcular la suma de los 100 primeros términos de esta sucesión.

SOLUCIÓN.

(1) Es claro que la diferencia es 4, entonces el término n–ésimo es $a_n = a_{n-1}+4$, y por tanto una expresión para el término general es: $a_n = 1+4n$.

(2) La suma $a_0+a_1+a_2+\cdots+a_{99} = \frac{(a_0+a_{99})100}{2}$, luego se tiene que la suma es: $\frac{(1+(1+4\times 99))100}{2} = \frac{398\times 100}{2} = 19900$.

□

8.6. Sucesiones geométricas

Una sucesión $\{a_n\}_n$ se dice que es una **sucesión geométrica** o una **progresión geométrica** si existe un número real r tal que para cada n el término a_{n+1} se calcula como $a_{n+1} = (a_n)r$.

Observar que como consecuencia de la definición una sucesión geométrica está determinada por el primer término a_0 y el número r. Llamamos a r la **razón**que define la progresión.

Los dos problemas a los que hacíamos referencia en el estudio de las progresiones aritméticas se pueden también plantear también en este caso.

8.7. El término general de una progresión geométrica

Los términos de la progresión aritmética son:

$$a_0, a_1 = a_0 r, a_2 = a_1 r, a_3 = a_2 r, a_4 = a_3 r, \ldots$$

Es claro que si en la expresión de a_2 en vez de a_1 escribimos su valor, tenemos:

$$a_2 = a_1 r = a_0 rr = a_0 r^2.$$

Para ver que este resultado es cierto para cada valor de n, esto es, que $a_n = a_0 r^n$, vamos a hacer inducción sobre n. Si $n = 0$, es claro que $a_0 = a_0 r^0$; suponemos que el resultado es cierto para t y vamos a ver que también lo es para $t+1$:

$$a_{t+1} = a_t r = a_0 r^t r = a_0 r^{t+1}.$$

8.8. La suma de s términos consecutivos

La suma de s términos consecutivos de una progresión geométrica. Cuando $r = 1$ la suma es muy fácil de calcular, vamos a suponer que $r \neq 1$.

Queremos calcular el valor de $a_n + a_{n+1} + a_{n+2} + \cdots + a_{n+s-1}$. Utilizando el resultado previo, escribimos $a_t = a_0 r^t$, la suma resulta igual a

$$\begin{aligned}
&a_n + a_{n+1} + a_{n+2} + \cdots + a_{n+s-1} \\
&= (a_0 r^n) + \left(a_0 r^{n+1}\right) + \cdots + \left(a_0 r^{n+s-1}\right) \\
&= a_0 \left(r^n + r^{n+1} + \cdots + r^{n+s-1}\right) \\
&= a_0 \left(r^0 + r^1 + \cdots + r^{n+s-1}\right) - \left(r^0 + r^1 + \cdots + r^{n-1}\right) \\
&= a_0 \left(r^0 + r^1 + \cdots + r^{n+s-1}\right) \tfrac{r-1}{r-1} - \left(r^0 + r^1 + \cdots + r^{n-1}\right) \tfrac{r-1}{r-1} \\
&= a_0 \tfrac{r^{n+s}-1}{r-1} - \tfrac{r^n-1}{r-1} = a_0 \tfrac{r^{n+s}-r^n}{r-1}
\end{aligned}$$

Cuando $n = 0$, esto es, si la suma comienza con el primer término de la progresión, entonces resulta

$$a_0 + a_1 + a_2 + \cdots + a_{s-1} = a_0 \frac{r^s - 1}{r - 1}.$$

ya que siempre se tiene la igualdad: $(1 + r + \cdots + r^{s-1})(r-1) = r^s - 1$.

Ejercicio. 8.10.
Hallar la suma $1 + 2 + 2^2 + 2^3 + \cdots + 2^n$.

SOLUCIÓN. Podemos utilizar la fórmula dada en la página 47 para el caso $r = 2$, $a_0 = 1$ y $s = n+1$ y obtenemos:

$$a_0 \frac{r^s - 1}{r - 1} = 1 \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

□

SOLUCIÓN. Podemos hacer la demostración de este resultado por inducción sobre n. Para $n = 0$ el resultado es cierto: $1 = 2^{0+1} - 1 = 1$. Suponemos que el resultado es cierto para $n \geq 0$ y vamos a ver que también es cierto para $n+1$. En efecto,

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2^{n+2} - 1.$$

□

Ejercicio. 8.11.
Se define la sucesión $\{a_n\}_n$ como sigue: $a_0 = 1$, $a_{n+1} = \sum_{i=0}^{n} a_i$. Calcular una fórmula para el término general de esta sucesión.

SOLUCIÓN. Es claro que $a_0 = 1$, $a_1 = 1$, $a_2 = a_0 + a_1 = 1 + 1 = 2$, $a_3 = a_0 + a_1 + a_2 = 1 + 1 + 2 = 4 = 2^2$, $a_4 = a_0 + a_1 + a_2 + a_3 = 1 + 1 + 2 + 4 = 8 = 2^3$. Vamos a suponer que se verifica la fórmula $a_n = 2^{n-1}$ si $n \geq 1$. Si llamamos $Y = \{n \in \mathbb{N}^* \mid a_n = 2^{n-1}\} \cup \{0\}$, entonces $0 \in Y$, y si suponemos que $n \in Y$, $n \geq 1$, vamos a probar que $n+1 \in Y$. Para esto procedemos como sigue:

$$a_{n+1} = \sum_{i=0}^{n} a_i = \sum_{i=0}^{n-1} a_i + a_n = a_n + a_n = 2a_n = 2 \cdot 2^{n-1} = 2^n.$$

Y por tanto $Y = \mathbb{N}$. □

Ejercicio. 8.12.
Don Ramón tiene una pequeña cantidad de dinero en un banco por la que mensualmente le dan un interés de un 6 % anual. Si la cantidad que ahora tiene Don Ramón es de 100.000 euros, ¿qué cantidad tendrá al cabo de un año?

SOLUCIÓN. El interés mensual que recibe Don Ramón es del 0,5 %, entonces el primer mes el dinero que tendrá Don Ramón es $100.000 \times 1,005 = 100.500$, al segundo mes será $100.500 \times 1,005$, etc. En consecuencia al cabo de doce meses tendrá:

$$100.000 \times (1,005)^{12} = 106.168.$$

□

Ejercicio. 8.13.
A Don David le gusta echar una copa cada noche. Para esto el día primero del mes compró una botella de un litro de una bebida con un contenido en alcohol del 40 %. Pero Don David quiere dejar de beber y para ello ha ideado el siguiente truco, tras beberse la correspondiente copa rellena la botella con la misma cantidad de agua que el líquido que bebe. Si la copa que habitualmente utiliza Don David es de 50 cm^3, averiguar cual será el contenido en alcohol de la botella tras beber veinte copas.

SOLUCIÓN. Tras la primera copa el contenido en alcohol será igual a $\frac{19}{20}$ del original, ya que sacamos $\frac{1}{20}$ del contenido inicial y lo rellenamos con agua. Tras la segunda copa será otra vez $\frac{19}{20}$ del contenido existente. Por esto tras veinte copas el contenido será $\left(\frac{19}{20}\right)^{20} = 0,358486$ del contenido inicial, esto es: $14,3394$ %. □

9. Sistemas de numeración

9.1. División euclídea

En esta sección vamos a utilizar fundamentalmente un concepto la **división euclídea** de números naturales. Comenzamos por una nueva formulación del Principio de Inducción, el **Segundo Principio de inducción**, cuya demostración dejamos al aplicado lector.

Proposición. 9.1. (Segundo Principio de inducción)
Sea $X \subseteq \mathbb{N}$ un subconjunto del conjunto de los números naturales, entonces $X = \mathbb{N}$ si verifica las dos siguientes propiedades:

(1) $0 \in X$.

(2) Si x es un número natural tal que $y \in X$ para todos los números naturales y anteriores a x ($y < x$), entonces $x \in X$.

Proposición. 9.2. (División euclídea de números naturales)
Sean a y b dos números naturales, $b \neq 0$, entonces existen otros dos números naturales q y r, únicos, verificando $a = bq + r$ y $0 \leq r < b$.

DEMOSTRACIÓN. Llamamos $Y = \{x \in \mathbb{N} \mid \ x = bq + r \text{ con } 0 \leq r < b, \text{ con } q, r \in \mathbb{N}\}$. Basta ver que $Y = \mathbb{N}$. Se tiene $0 \in Y$, y si $x \in Y$ verifica que todo número natural menor que x pertenece a Y, vamos a probar que también $x + 1$ pertenece a Y, y como consecuencia del Segundo Principio de Inducción se tendrá el resultado. Si $x \in Y$ está en las condiciones anteriores, consideramos $x + 1$. Si $x + 1 < b$, tenemos la expresión buscada: $x + 1 = b \cdot 0 + (x + 1)$. Si $x + 1 \geq b$, entonces existe un número natural y tal que $x + 1 = b + y$ (nosotros hemos representado otras veces este número y por $x + 1 - b$).

Ahora el número y es menor que $x + 1$, y por tanto $y \leq x$, por la hipótesis se tiene $y \in Y$ y existen q', r' tal que $y = bq' + r'$. Ahora procedemos como sigue:

$$\begin{aligned} y &= bq' + r' \\ x + 1 &= b + y = b + bq' + r' \\ x + 1 &= b(q' + 1) + r' \end{aligned}$$

y resulta que $x + 1 \in Y$. Falta probar que para cada pareja de números naturales a y b los números q y r son únicos. Supongamos que tenemos dos expresiones $a = bq_1 + r_1$ y $a = bq_2 + r_2$, con $q_1 \leq q_2$ entonces

$$bq_1 + r_1 = a = bq_2 + r_2$$

y

$$q_2 = q_1 + y \text{ para algún número natural.}$$

Entonces

$$r_1 = by + r_2.$$

Pero $r_1 < b$, luego necesariamente $y = 0$, y por tanto $q_2 = q_1$, y $r_2 = r_1$. □

El método utilizado en la demostración es en cierto modo constructivo, sin embargo el que aquí se detalla no es el mejor algoritmo para hacer la división euclídea de dos números naturales.

Cada número natural no nulo es el siguiente de otro, de forma que cada número natural está determinado por el lugar que ocupa en la cadena de todos los números naturales.

No hemos hecho hincapié hasta el momento sobre la forma de escribir los números naturales. Si recordamos la tabla de la página 40,

0		
1	$0+1$	$0+1$
2	$(0+1)+1$	$1+1$
3	$((0+1)+1)+1$	$2+1$
4	$\vdots$	$3+1$
5	$\vdots$	$4+1$
$\vdots$	$\vdots$	$\vdots$

en las columnas primera y segunda, tenemos dos formas de representar los números naturales. En la columna primera la representación es la siguiente: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ..., mientras que en la columna segunda es: 0, 0+1, 0+1+1, 0+1+1+1, 0+1+1+1+1, ... Es claro que la primera forma de representar los números naturales es más útil que la segunda a la hora de hacer cálculos y otras operaciones.

La representación de los números naturales como 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ... se llama **escritura posicional de base decimal** y, aunque parezca lo contrario es de muy reciente introducción.

Cada número se expresa en función unos símbolos; las **cifras**: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, las cuales, dependiendo de la posición que ocupen, tienen un valor u otro. Así en el número 1231 la primera y la cuarta cifra, (comenzando siempre por la derecha) son iguales a 1, pero tienen valores diferentes. La primera representa que se repite una vez la base elevada a 0, mientras que la segunda indica que se repite una vez la base 10 elevada a 3. En efecto, el número anterior 1231 es:

$$1231 = 1 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 1 \times 10^0.$$

El uso de la base 10 se podría justificar por el número de dedos que tiene en las manos una persona normal, y no ha sido siempre la base utilizada para escribir los números y contar.

9.2. Sistemas de numeración: formulación abstracta

Un **sistema de numeración** *es un conjunto de reglas que permiten escribir los números naturales y hacer operaciones entre ellos.* El sistema que hemos utilizado en el párrafo anterior se llama **sistema de numeración posicional de base diez**.

Si queremos escribir el número $x = 1231$ en otra base, por ejemplo la base 8. Lo primero que tenemos que hacer es determinar las cifras que vamos a necesitar en este nuevo sistema de numeración. Por ejemplo éstas podrían a ser: 0,1,2,3,4,5,6,7. A continuación escribimos el numero en la forma $x = a_t 8^t + a_{t-1}8^{t-1} + \cdots + a_1 8^1 + a_0 8^0$.

Para hacer esto podemos proceder como sigue: si suponemos que ya hemos realizado el proceso, entonces a_0 es el resto de la división euclídea de x por 8, siendo el cociente igual a $a_t 8^{t-1} + a_{t-2}8^{t-1} + \cdots + a_1 8^0$, pues se tiene:

$$x = 8(a_t 8^{t-1} + a_{t-2}8^{t-1} + \cdots + a_1 8^0) + a_0$$

Si repetimos ahora el proceso con el cociente de la anterior división, $a_t 8^{t-1} + a_{t-1}8^{t-2} + \cdots + a_1 8^0$, encontramos el valor de a_1, y así hasta llegar a determinar todas las cifras del numero x escrito en base 8. En nuestro caso

$$\begin{aligned} 1231 &= 153 \times 8 + 7 \\ 153 &= 19 \times 8 + 1 \\ 19 &= 2 \times 8 + 3 \\ 2 &= 0 \times 8 + 2 \end{aligned}$$

$$\begin{aligned} x &= 2 \times 8^3 + 3 \times 8^2 + 1 \times 8^1 + 7 \times 8^0 \\ &= 2 \times 512 + 3 \times 64 + 1 \times 8 + 7 \\ &= 1024 + 192 + 8 + 7 = 1231. \end{aligned}$$

¿Cómo escribir el número x en la base 8? Para esto simplemente utilizamos las cifras que hemos encontrado, que en nuestro caso son 2317. Pero para distinguirlo del número 2317 escrito en otra base, por ejemplo la base 10, vamos a escribir por ejemplo

$$x = 2317_8.$$

Con el convenio de que cuando el número está escrito en base decimal, base 10, no es necesario agregar el correspondiente subíndice.

Para hacer ahora operaciones, suma y producto, con números escritos en el sistema de numeración posicional de base ocho necesitamos conocer las tablas de la suma y el producto de los números que se pueden expresar con una cifra, esto es, de los números 0, 1, 2, 3, 4, 5, 6 y 7.

El mismo número $x = 1231$ escrito en otras bases es:

Base 2: 10011001111_2
Base 3: 1200121_3
Base 4: 103033_4
Base 5: 14411_5
Base 6: 5411_6
Base 7: 3406_7
Base 8: 2317_8
Base 9: 1617_9

En cambio si queremos escribirlo en base 11, los restos sucesivos son:

$$\begin{aligned} 1231 &= 11 \times 111 + 10, \\ 111 &= 11 \times 10 + 1, \\ 10 &= 11 \times 0 + 10, \end{aligned}$$

luego el número debe tener las cifras 10, 01 y 10. Es conveniente buscar un único símbolo para representar la cifra 10 en la base 11. Una forma puede ser llamarla *a*, y entonces el número *x* en la base 11 se escribe: $a1a_{11}$.

Vamos a escribirlo en otras bases mayores que 11 siguiendo el mismo proceso de buscar representación para las cifras superiores a 9 mediante letras.

Base 11: $a1a_{11}$
Base 12: 867_{12}
Base 13: 739_{13}
Base 14: $63d_{14}$
Base 15: 571_{15}
Base 16: $4cf_{16}$

Si tenemos un número escrito en base 10, para sumar necesitamos saber las tablas de la suma del 0 al 9 y lo mismo para multiplicar. Si el número está en la base 8 sólo necesitamos saber las tablas del 0 al 7. En cambio si el número está en base 16 necesitaremos conocer las tablas del 0 al f.

Si x es un número real, el **logaritmo decimal** de x es el número al que hay que elevar 10 para obtener x, esto es,

$$10^{\log(x)} = x.$$

Se pueden definir logaritmos sobre otras bases. Así para un número B, el logaritmo de x en la base B es el número al que hay que elevar B para obtener x:

$$B^{\log_B(x)} = x$$

La relación entre los logaritmos $\log(x)$ y $\log_B(x)$ se obtiene de la siguiente forma, teniendo en cuenta que las dos expresiones representan al mismo número x:

$10^{\log(x)} = x = B^{\log_B(x)}$ tomando logaritmo se tiene:

$\log(x) \cdot \log(10) = \log_B(x) \cdot \log(B)$ se obtiene entonces:

$\log_B(x) = \frac{\log(x)}{\log(B)}$.

Como el logaritmo de 8 en la base 10 es: $\log(8) = 0,90309$, resulta que el logaritmo en base 8 de x es: $\log_8(x) = \frac{3,09026}{0,90309} = 3,42187$. Obtenemos que el número de cifras de x en la base 8 es 4.

Como el logaritmo de 2 en la base 10 es: $\log(2) = 0,30103$, resulta que el logaritmo en base 2 de x es: $\log_2(x) = \frac{3,09026}{0,30103} = 10,2656$. El número de cifras de x en la base 2 es 11.

Necesitamos un resultado que nos asegure que dada una base B, cada número natural puede escribirse, de forma única, en el sistema de numeración posicional de base B.

Teorema. 9.3. (Teorema fundamental de los sistemas de numeración)
Sean a y b números naturales, existen números naturales c_t, c_{t-1}, ..., c_1, c_0, determinados de forma única, verificando $a = c_t b^t + c_{t-1} b^{t-1} + \cdots + c_1 b + c_0$.

DEMOSTRACIÓN. La división euclídea $a = bq + r$ nos determina c_0 de forma única, en efecto $c_0 = r$, el resto de la división. Además el cociente q es $c_t b^{t-1} + c_{t-1} b^{t-2} + \cdots + c_1$, vamos a llamar q_0 a este cociente.

Si repetimos el proceso llegamos a que c_1 está también determinado de forma única como el resto de la división euclídea de q_0 por b. Sea esta división $q_0 = bq_1 + c_1$. Vamos entonces determinando el coeficiente c_{i+1} al hacer la división de q_i por b.

Un posible método de demostración consiste en hacer inducción en la misma forma que en la Proposición 9.2.. □

Ejercicio. 9.4.
Dado el número $x = 324567$, expresarlo en las bases: 2, 5, 16.

SOLUCIÓN. 1001111001111010111_2

40341232_5

$4f3d7_{16}$ □

Ejercicio. 9.5.
Dado el número $x = 234a5109_{11}$*, expresarlo en base 10.*

SOLUCIÓN. 45086424 □

Ejercicio. 9.6.
Dado el número $x = 777733322_8$*, expresarlo en las bases 2 y 16.*

SOLUCIÓN. $11111111111011011011010010_2$

$7ffb6d2_{16}$ □

Ejercicio. 9.7.
Dado el número $x = 1111333022_4$*, expresarlo en las bases 2 y 16.*

SOLUCIÓN. 1010101111111001010_2

$55fca_{16}$ □

Ejercicio. 9.8.
Determinar una base β *con respecto a la cual se verifica la igualdad:* $21 \times 31 = 1033$.

SOLUCIÓN. Los números involucrados son: $2\beta+1$, $2\beta+3$ y $\beta^3+3\beta+3$, y verifican la relación:

$$\begin{aligned}(2\beta+1)(2\beta+3) &= \beta^3+3\beta+3\\ 4\beta^2+8\beta+3 &= \beta^3+3\beta+3\\ \beta^3-4\beta^2-5\beta &= 0\end{aligned}$$

Las raíces son: $\beta = 0, -1$ y 5. Por tanto la base pedida es: $\beta = 5$. □

10. Números enteros

Al igual que en el caso de $\mathbb{N}$, suponemos que el alumno conoce el conjunto $\mathbb{Z}$ de los **números enteros**, y conoce también que en él hay definidas dos operaciones: suma y producto, que verifican las siguientes propiedades.

La suma:

(I) **Propiedad asociativa**. $a+(b+c)=(a+b)+c$, para todos $a, b, c \in \mathbb{Z}$.

(II) **Propiedad conmutativa**. $a+b=b+a$, para todos $a, b \in \mathbb{Z}$.

(III) **Existencia de elemento neutro**. Existe un elemento $0 \in \mathbb{Z}$ tal que para todos $a \in \mathbb{Z}$ tenemos $0+a=a$.

(IV) **Existencia de elemento opuesto**. Dado $n \in \mathbb{Z}$ existe $m \in \mathbb{Z}$ tal que $n+m=0$.

El producto:

(I) **Propiedad asociativa**. $a(bc)=(ab)c$, para todos $a, b, c \in \mathbb{Z}$.

(II) **Propiedad conmutativa**. $ab=ba$, para todos $a, b \in \mathbb{Z}$.

(III) **Existencia de elemento neutro**. Existe un elemento $1 \in \mathbb{Z}$ tal que para todos $a \in \mathbb{Z}$ tenemos $1a=a$.

(IV) **Propiedad distributiva del producto respecto a la suma**. $a(b+c)=ab+ac$ para todos $a, b, c \in \mathbb{Z}$.

Estas operaciones nos permiten estudiar la aritmética de $\mathbb{Z}$ de forma fácil.

(V) **Propiedad cancelativa del producto**. Si $ac=bc$ y $c \neq 0$, entonces $a=b$.

El primer hecho a tener en cuenta es que $\mathbb{Z}$ verifica la siguiente propiedad: si $n, m \in \mathbb{Z}$ verifican $nm=0$, entonces $n=0$ ó $m=0$, esto es; $\mathbb{Z}$ es un **dominio de integridad**.

10.1. La relación de orden en $\mathbb{Z}$

Podemos suponer que $\mathbb{Z}$ contiene a $\mathbb{N}$, el conjunto de los números naturales. La relación de orden en $\mathbb{N}$ se puede extender a una relación de orden en $\mathbb{Z}$ definiendo:

$$n \leq m, \text{ si existe } a \in \mathbb{N} \text{ tal que } m = n + a.$$

Como es usual escribimos $n < m$ cuando $n \leq m$ y $n \neq m$, y $n \geq m$ (resp. $n > m$) cuando $m \leq n$ (resp. $m < n$).

Lema. 10.1.
La relación $\leq$ es una relación de orden en el conjunto $\mathbb{Z}$ de los números enteros.

Esta relación verifica las siguientes propiedades:

(1) $\{n \in \mathbb{Z} \mid 0 \leq n\} = \mathbb{N}$.

(2) **Propiedad de Tricotomía.** Para cada número entero $n \in \mathbb{Z}$ se verifica:

$$n < 0, \quad n = 0 \quad \text{o} \quad n > 0.$$

(3) Si $n, m \in \mathbb{Z}$, $n \leq m$ y $a \in \mathbb{Z}$, entonces $n + a \leq m + a$.

(4) Si $n, m \in \mathbb{Z}$, $n \leq m$ y $a \geq 0$, entonces $na \leq ma$.

(5) Si $n, m \in \mathbb{Z}$, $n \leq m$ y $a \leq 0$, entonces $na \geq ma$.

Ejercicio. 10.2.
Probar que para todo número entero $n \in \mathbb{Z}$ se verifica: $n^2 \geq n$.
En particular $n^2 \geq 0$ para todo $n \in \mathbb{Z}$.

SOLUCIÓN. Hacemos una disyunción de casos:

(1) Si $n = 0$, entonces $n^2 = 0 = n$.

(2) Si $n > 0$, entonces $n > 1$, y por tanto $n^2 = n \cdot n > 1 \cdot n = n$.

(3) Si $n < 0$, entonces $n^2 = n \cdot n > 0 \cdot n = 0 > n$.

□

Ejercicio. 10.3.
Probar que para cualesquiera $n, m \in \mathbb{Z}$ se verifica $n^2 + m^2 \geq 2nm$.

SOLUCIÓN. Como tenemos $(n-m)^2 \geq 0$, basta desarrollar para obtener $n^2 - 2nm + m^2 \geq 0$, entonces resulta $n^2 + m^2 \geq 2nm$. □

10.2. Divisores. Números primos

Sean d, $n \in \mathbb{Z}$ números enteros, decimos que d es un **divisor** de n, ó que n es un **múltiplo** de d, si existe otro número entero m tal que $n = dm$.

Si d es un divisor de n escribiremos $d \mid n$, y si no lo es, entonces escribimos $d \nmid n$.

La relación $\mid$ en $\mathbb{Z}$ verifica las propiedades reflexiva y transitiva, y no verifica las propiedades simétrica ni antisimétrica.

Cada número entero no nulo n tiene siempre cuatro (¡o dos!) divisores, estos son: $1, -1, n$ y $-n$. Tenemos que 1 y -1 son **unidades** y dividen a cada número entero. A n y $-n$ los llamaremos **divisores impropios** de n, y a los restantes, si existen, los llamaremos **divisores propios** de n.

Dos números enteros n, m se llaman **asociados** si $n \mid m$ y $m \mid n$, es fácil demostrar que dos números enteros no nulos n y m son elementos asociados si $n = \pm m$.

El uso de los divisores nos permite definir números enteros especiales, *los números primos*. Un número entero, distinto de 0, 1 y -1, es **primo** si no tiene divisores propios. Es claro que si p es un número entero primo, entonces $-p$ también lo es, y por tanto dado un número primo siempre existe un número entero primo positivo, que se diferencia de él posiblemente en el signo. Los números primos nos permiten dar una expresión sencilla y manejable (¡en algunos casos!) de los números enteros.

Teorema. 10.4. (Teorema fundamental de la Aritmética.)
Todo número entero n distinto de 0, 1 y -1 *se expresa de forma, esencialmente, única del siguiente modo:*

$$n = \pm {p_1}^{e_1} \cdots {p_r}^{e_r},$$

donde $p_1, \ldots, p_r$ *son números enteros primos positivos y donde* $e_1, \ldots, e_r$ *y r son números enteros positivos.*

DEMOSTRACIÓN. Podemos reducirnos a hacer la demostración para números enteros positivos. Definimos un conjunto $Y \subseteq \mathbb{N}$ mediante:

$$Y = \{0, 1\} \cup \{x \in \mathbb{N} \mid ; x = {p_1}^{e_1} \cdots {p_r}^{e_r} \text{ como en el enunciado}\}.$$

Para ver que $Y = \mathbb{N}$, basta ver por el Segundo Principio de Inducción que si un número natural y verifica que todo número natural $x < y$ pertenece a Y, entonces $y \in Y$. Supongamos que $x \neq 0, 1$ verifica esta propiedad; si x primo, entonces x pertenece a Y; si x no es primo, entonces tiene una factorización en divisores propios, sea $x = x_1 x_2$, entonces x_1 y x_2 son menores que x y por la hipótesis ambos pertenecen a Y. Existen pues expresiones

$$x_1 = {p_1}^{e_1} \cdots {p_r}^{e_r}$$
$$x_2 = {q_1}^{f_1} \cdots {q_s}^{f_s}$$

y en consecuencia $x = x_1 x_2 = {p_1}^{e_1} \cdots {p_r}^{e_r} {q_1}^{f_1} \cdots {q_s}^{f_s}$ y $x \in Y$.

Falta probar la unicidad de esta expresión. Supongamos que $x = {p_1}^{e_1} \cdots {p_r}^{e_r} = {q_1}^{f_1} \cdots {q_s}^{f_s}$ son dos de estas expresiones. Si $p_1 = q_1$, entonces simplificando se tiene ${p_1}^{e_1-1} \cdots {p_r}^{e_r} = {q_1}^{f_1-1} \cdots {q_s}^{f_s}$; este número es menor que x, y otra vez el Segundo Principio de Inducción nos permite asegurar que las dos expresiones son la misma salvo el orden. Si $p_1 \neq q_1$, supongamos que $p_1 > q_1$, entonces $p_1 - q_1 = r \in \mathbb{N}$, y resulta:

$$\begin{aligned} p_1(p_1^{e_1-1} \cdots {p_r}^{e_r} - q_1^{f_1-1} \cdots {q_s}^{f_s}) &= {p_1}^{e_1} \cdots {p_r}^{e_r} - p_1 q_1^{f_1-1} \cdots {q_s}^{f_s} \\ &= {q_1}^{f_1} \cdots {q_s}^{f_s} - p_1 q_1^{f_1-1} \cdots {q_s}^{f_s} \\ &= (q_1 - p_1) {q_1}^{f_1-1} \cdots {q_s}^{f_s}, \end{aligned}$$

que es menor que n, y otra vez el Segundo Principio de Inducción nos permite asegurar que esta expresión es única; en particular como p_1 es uno de los factores de esta expresión, deber aparecer en los factores de $(q_1 - p_1){q_1}^{f_1-1} \cdots {q_s}^{f_s}$, pero estos son, por la hipótesis de inducción, los q_i y los factores de $q_1 - p_1$, si fuese uno de los q_i podemos hacer uso de la parte anterior, y si es uno de los factores de $q_1 - p_1$, entonces divide a q_1, lo que implica que $p_1 = q_1$, lo que es una contradicción. □

Lema. 10.5.
Sea p un enteros primo, si $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.

SOLUCIÓN. Si $a, b = 0, 1$, el resultado es cierto. Sean $a, b \neq 0, 1$. Si se consideran las factorizaciones de a y de b, entonces p ha de ser uno de los primos que aparecen en ellas. □

Esta descomposición es interesante como más adelante veremos al estudiar el máximo común divisor y el mínimo común múltiplo. Antes de pasar a esto vamos a enunciar y demostrar un resultado clásico de la teoría de números en el que aplicaremos el Teorema fundamental de la Aritmética.

Teorema. 10.6. (Teorema de Euclides.)
Existe un número infinito de enteros primos.

DEMOSTRACIÓN. Supongamos que existan únicamente s enteros primos, $p_1, \ldots, p_s$, definimos $n = p_1 \cdots p_s + 1$, entonces n es distinto de $0, 1$ y -1, y además no es divisible por ningún entero primo, lo que es una contradicción con el Teorema fundamental de la Aritmética.

□

Ejemplo. 10.7. (Aplicación. Divisores de un número.)
Sea n un número entero positivo distinto de 0 y 1, el cual se escribe

$$n = p_1^{e_1} \cdots p_t^{e_t}.$$

Si consideramos el número N definido por:

$$N = (1 + p_1 + \cdots + p_1^{e_1})(1 + p_2 + \cdots + p_2^{e_2}) \cdots (1 + p_t + \cdots + p_t^{e_t}),$$

entonces cualquier divisor de n aparece como uno de los sumandos en el desarrollo del producto que define N y recíprocamente, cada uno de estos sumandos es un divisor de n. Como consecuencia el número de divisores de n es igual a:

$$(e_1+1)(e_2+1)\cdots(e_t+1).$$

Llamamos a este número $d(n)$.

Es claro que N es la suma de todos los divisores de n. Sin embargo es conveniente hacer alguna modificación en la descripción de N para poder calcular más fácilmente su valor. Para esto procedemos como sigue. Teniendo en cuenta que se tiene al igualdad:

$$(p-1)(1+p+\cdots+p^e)=p^{e+1}-1,$$

resulta que

$$(1+p+\cdots+p^e)=\frac{p^{e+1}-1}{p-1},$$

y por lo tanto se tiene:

$$N=\frac{p_1^{e_1+1}-1}{p_1-1}\cdot\frac{p_2^{e_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_t^{e_t+1}-1}{p_t-1}.$$

Para calcular el producto de todos los divisores de n, basta considerar que si escribimos todos estos divisores en orden creciente: $d_0, d_1, \ldots, d_r$, entonces $d_0 = 1$ y $d_r = n$. Al considerar el resto $d_1, d_2, \ldots, d_{r-1}$, se observa que si $d_1 = \sqrt{n}$, entonces la lista se reduce a un sólo elemento, y si $d < \sqrt{n}$, entonces $d_1 d_{r-1} = n$. En efecto, como d_1 es un divisor y no es 1 ni n, se tiene $n = d_1 h$, siendo h uno de los $d_2, \ldots, d_{r-1}$; si $h \neq d_r - 1$, entonces existe un k tal que $d_{r-1}k = n$; este k es uno de los $d_2, \ldots, d_{r-2}$. En particular $d_1 < k$, y como $h < d_{r-1}$, resulta $n = d_1 h < k d_{r-1} = n$, lo que es una contradicción. En consecuencia se debe tener $h = d_{r-1}$ y tenemos el resultado. Este proceso se puede ir repitiendo eliminado ahora, si la lista tiene más de un elemento, d_1 y d_{r-1}; y a la nueva lista le aplicamos el mismo proceso. Finalmente llegaremos a una lista con un solo elemento o a una lista vacía, y se obtendrá el siguiente resultado: en la lista original se tiene $d_i d_{r-i} = n$ para cada índice $i = 0, \ldots, r$.

Si llamamos P al producto de todos los divisores de n, tenemos:

$$\begin{aligned}
P &= d_0\, d_1\, \cdots\, d_{r-1}\, d_r \\
P &= d_r\, d_{r-1}\, \cdots\, d_1\, d_0 \\
P^2 &= (d_0 d_r)(d_1 d_{r-1})\cdots(d_{r-1} d_1)(d_r d_0) = n^{t+1} = n^{d(n)}.
\end{aligned}$$

En consecuencia se tiene $P = \sqrt{n^{d(n)}}$.

Ejercicio. 10.8.
Se considera el número entero positivo $n = 1800$. Calcular el número de divisores y la suma y el producto de todos ellos.

SOLUCIÓN. Se calcula la factorización de n en factores primos; en este caso es: $n = 2^3 \cdot 3^2 \cdot 5^2$. Entonces el número de divisores es: $(3+1)(2+1)(2+1) = 36$. La suma de todos ellos es:

$$\begin{aligned} N &= \tfrac{2^4-1}{2-1} \cdot \tfrac{3^3-1}{3-1} \cdot \tfrac{5^3-1}{5-1} \\ &= \tfrac{15}{1} \cdot \tfrac{26}{2} \cdot \tfrac{124}{4} \\ &= 15 \cdot 13 \cdot 31 = 6045 \end{aligned}$$

El producto de los divisores de 1800 es:

$$P = \sqrt{1800^{36}} =$$

$$39346408075296537575424000000000000000000000000000000000000.$$

En *Mathematica* la orden **Divisors[n]** da una lista con todos los divisores de n, en este caso es:

$$\begin{aligned} L = \{&1,2,3,4,5,6,8,9,10,12,15,18,20,24,25,30,36,40,45,50,60, \\ &72,75,90,100,120,150,180,200,225,300,360,450,600,900,1800\} \end{aligned}$$

La suma se calcula con:

$$\mathbf{Sum}[\mathbf{L}[[\mathbf{i}]], \{\mathbf{i}, \mathbf{Lenght}[\mathbf{L}]\}]$$

y el producto con:

$$\mathbf{Product}[\mathbf{L}[[\mathbf{i}]], \{\mathbf{i}, \mathbf{Length}[\mathbf{L}]\}].$$

□

Ejemplo. 10.9.
Los números primos no están distribuidos de forma uniforme a lo largo de la cadena de números enteros positivos. Por ejemplo, menores que 10 hay solo cuatro números primos: 2, 3, 5 y 7, y menores que 100 hay veinticinco: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 91, 97.

En *Mathematica* la orden **PrimePi[n]** nos da el número de enteros primos positivos menores que n.

$$\mathbf{PrimePi}[\mathbf{100}] = 25.$$
$$\mathbf{PrimePi}[\mathbf{1000}] = 168.$$
$$\mathbf{PrimePi}[\mathbf{1000000}] = 78498.$$

Si n es un número entero positivo el número de números primos positivos menores que n se representa por $\pi(n)$. Una aproximación a este número la propuso Legendre, quien afirmaba que $\pi(n)$ se aproxima por $\frac{n}{\lg(n)-0{,}83}$. Posteriormente Gauss da otra aproximación a $\pi(n)$

mediante la fracción $\frac{n}{\lg(n)}$. A continuación incluimos una tabla en la que aparecen estas aproximaciones y los valores correctos de $\pi(n)$ para algunas potencias de 10.

n	$\pi(n)$	Legendre	Razón	Gauss	Razón
100	25	26	0,96154	22	1,13636
100^2	1229	1193	1,03018	1086	1,13168
100^3	78498	77009	1,01934	72382	1,08450
100^4	5761455	5684828	1,01348	5428681	1,06130
100^5	455052511	450534653	1,01003	434294482	1,04780
100^6	37607912018	37312011198	1,00793	36191206825	1,03915
100^7	3204941750802	3184085553026	1,00655	3102103442166	1,03315

10.3. Máximo común divisor

Sean n y m números enteros positivos, definimos el **máximo común divisor**, **mcd**, de n y m como el mayor número entero positivo d que divide a n y m; es claro que d siempre existe, y que si n y m tienen las siguientes expresiones en función de números enteros primos positivos

$$n = p_1^{e_1} \cdots p_r^{e_r}, \quad e_i > 0,$$
$$m = q_1^{f_1} \cdots q_s^{f_s}, \quad f_j > 0,$$

entonces podemos obtener una expresión sencilla para d de la siguiente forma: primero extendemos las expresiones anteriores para que consten de los mismos factores primos, posiblemente con exponentes nulos, así obtenemos expresiones del tipo siguiente:

$$n = p_1^{e_1} \cdots p_t^{e_t},$$
$$m = p_1^{g_1} \cdots p_t^{g_t},$$

con $t \geq r$, $t \geq s$ y donde $e_i, g_i \geq 0$, entonces

$$d = p_1^{h_1} \cdots p_t^{h_t},$$

con $h_i = \min\{e_i, g_i\}$. De la misma forma se define el **mínimo común múltiplo**, **mcm**, M de n y m, como el menor número entero positivo múltiplo de n y m; siguiendo con las anteriores notaciones tenemos

$$M = p_1^{l_1} \cdots p_t^{l_t},$$

con $l_i = max\{e_i, g_i\}$.

Ejercicio. 10.10.
Comprobar que se verifica la siguiente igualdad:

$$dM = nm,$$

como consecuencia calculado uno de los dos, d ó M, conocemos el otro.

Ejercicio. 10.11.
En el conjunto $\mathbb{N}$ *de los números naturales la relación de divisibilidad es una relación de orden. Comprobar que en él el ínfimo de dos números n y m es el máximo común divisor y el supremo es el mínimo común múltiplo.*

Vamos a determinar el mcd y el mcm de dos números enteros positivos según sus propiedades de divisibilidad; resulta que si n y m son enteros positivos, el mcd d de n y m verifica la siguiente propiedad:

$$\begin{array}{l} d \mid n,\ d \mid m, \quad \text{y} \\ \text{si } x \text{ es otro número entero tal que } x \mid n \text{ y } x \mid m, \text{ entonces } x \mid d. \end{array}$$

Es fácil ver que un número entero d que verifica la propiedad anterior es el mcd de n y m ó su opuesto, por lo tanto esta propiedad caracteriza al mcd. De forma análoga es sencillo comprobar que la siguiente propiedad caracteriza al mcm.

$$\begin{array}{l} n \mid M,\ m \mid M, \text{ y} \\ \text{si } x \text{ es otro número entero tal que } n \mid x \text{ y } m \mid x, \text{ entonces } M \mid x. \end{array}$$

La definición de máximo común divisor y de mínimo común múltiplo se puede extender a números enteros en la siguiente forma:
Si a y b son números enteros un **máximo común divisor** de a y b es un entero d, tal que:

$$\begin{array}{l} d \mid a, d \mid b \quad \text{y} \\ \text{si existe un entero } c \text{ tal que } c \mid a, c \mid b, \text{ entonces } c \mid d. \end{array}$$

Para cada par de números enteros pueden existir dos máximos comunes divisores, concretamente d y $-d$. Para nuestros propósitos vamos a considerar siempre el valor positivo o nulo.

De forma análoga se define el **mínimo común múltiplo**.

Ejercicio. 10.12.
Probar que se verifican las siguientes propiedades para el máximo común divisor de números enteros:

(I) $\text{m. c. d.}\{a,b\} = \text{m. c. d.}\{a,-b\} = \text{m. c. d.}\{-a,b\} = \text{m. c. d.}\{-a,-b\}$.

(II) $\text{m. c. d.}\{a,0\} = a$.

(III) $\text{m. c. d.}\{a\cdot c, b\cdot c\} = \text{m. c. d.}\{a,b\}\cdot$.

(IV) *Si* $d \mid a$ *y* $d \mid b$, *entonces* $\text{m. c. d.}\{\frac{a}{d},\frac{b}{d}\} = \frac{\text{m.c.d.}\{a,b\}}{d}$

(V) $\text{m. c. d.}\{\text{m. c. d.}\{a,b\},c\} = \text{m. c. d.}\{a,\text{m. c. d.}\{b,c\}\}$.

Ejercicio. 10.13.
Enunciar las propiedades correspondientes para al mínimo común múltiplo.

Ejercicio. 10.14.
Sean a, b, q y r números enteros tales que $a = bq + r$*, probar que* $\mathrm{m.\,c.\,d.}\{a, b\} = \mathrm{m.\,c.\,d.}\{b, r\}$.

Existen otras formas de representar el mcd y el mcm (positivo ó nulo) de dos números enteros n y m, estas son (n, m) y $[n, m]$ respectivamente.

Dos números enteros n y m se llaman **primos relativos** *si* $\mathrm{m.\,c.\,d.}\{n, m\} = 1$.

Ejercicio. 10.15.
Probar que $\mathrm{m.\,c.\,d.}\{a, bc\} = 1$ *si y solo si* $\mathrm{m.\,c.\,d.}\{a, b\} = 1 = \mathrm{m.\,c.\,d.}\{a, c\}$.

Ejercicio. 10.16.
Probar que si $a \mid bc$ *y* $\mathrm{m.\,c.\,d.}\{a, b\} = 1$*, entonces* $a \mid c$.

10.4. Algoritmo de la división

Recordemos rápidamente el Algoritmo de la división en $\mathbb{Z}$.

Teorema. 10.17. (Algoritmo de la división.)
Dados dos números enteros a y b, con $b > 0$*, existen dos únicos números enteros q y r verificando:*

(1) $a = bq + r$,

(2) $0 \leq r < b$.

DEMOSTRACIÓN. Llamemos $S = \{a - bs \mid \ s \in \mathbb{Z}, a - bs \geq 0\}$, tenemos que S es no vacío ya que $a - b(-a^2) \geq 0$; entonces S tiene un primer elemento $r = a - bq$. Por hipótesis $r \geq 0$; si $r \geq b$, entonces $r = b + r'$, y despejando el valor de r' tenemos

$$r' = r - b = a - bq - b = a - b(q + 1) \in S,$$

y ya que $r' < r$, llegamos a una contradicción, luego $r < b$ y se tiene que el enunciado es cierto a falta de la unicidad. Supongamos que tenemos dos expresiones distintas

$$a = bq + r = bq' + r'$$

con $0 \leq r, r' < b$, entonces restando una de la otra tenemos la igualdad

$$0 = b(q - q') + (r - r'),$$

de donde deducimos que $r - r' = 0$, esto es que $r = r'$, y por tanto también $q = q'$. □

r se llama **resto** y q **cociente** de la división de a por b. Observar que el resto r es siempre positivo, mientras que el cociente q puede ser positivo o negativo.

Como consecuencia del anterior Teorema tenemos:

Corolario. 10.18. (Algoritmo de la división.)
Dados dos números enteros a y b, con $b \neq 0$, existen dos únicos números enteros q y r verificando:

(1) $a = bq + r$,

(2) $0 \leq r < |b|$.

DEMOSTRACIÓN. Si $b > 0$ podemos aplicar el Teorema 10.17.. Si $b < 0$, entonces $-b$ es positivo y por el Teorema tenemos $a = (-b)q + r$ con $0 \leq r < -b$. En consecuencia se obtiene $a = b(-q) + r$ con $0 \leq r < |b|$. La unicidad es también consecuencia del Teorema. □

10.5. Máximo común divisor. Identidad de Bezout

Vamos a calcular el mcd de dos números enteros utilizando el Algoritmo de la división, pero antes veamos una propiedad interesante del mcd. Sean n y m números enteros (positivos), consideramos el conjunto

$$T = \{an + bm \mid \ a, b \in \mathbb{Z}\},$$

y hacemos $(T \cap \mathbb{N}) \setminus \{0\}$, este conjunto es no vacío ya que $n \in (T \cap \mathbb{N}) \setminus \{0\}$; existe por tanto un primer elemento d de $(T \cap \mathbb{N}) \setminus \{0\}$, supongamos $d = a_0 n + b_0 m$ con $a_0, b_0 \in \mathbb{Z}$. Vamos a demostrar que d es el mcd de n y m. Para ver que $d \mid n$ hacemos la división de n por d obteniendo $n = dq + r$ con $0 \leq r < d$, entonces

$$r = n - dq = n - (a_0 n + b_0 m)q = n(1 - a_0 q) - m b_0 q \in T \cap \mathbb{N},$$

lo que es una contradicción salvo que $r = 0$, y en este caso $d \mid n$. De igual forma se tiene $d \mid m$. Es sencillo comprobar que si x es otro número entero tal que $x \mid n$ y $x \mid m$, entonces también $x \mid d$, luego d es el mcd de n y m. Observar que en este caso se tiene $T = \{xd \mid \ x \in \mathbb{Z}\}$.

El resultado anterior se conoce como **Identidad de Bezout**, y se enuncia como sigue.

Lema. 10.19. (Identidad de Bezout.)
Sean n y m números enteros (positivos) y sea d su mcd, entonces existen números enteros a y b tales que $d = an + bm$; en particular se tiene la igualdad:

$$\{an + bm \mid \ a, b \in \mathbb{Z}\} = \{xd \mid \ x \in \mathbb{Z}\}.$$

Algoritmo de Euclides para el cálculo del mcd. Una justificación de este algoritmo la veremos más adelante. Baste por ahora hacer uso del mismo para habituarnos a la aritmética de $\mathbb{Z}$. Este algoritmo consiste en tomar los dos números enteros, no nulos, n y m, ordenarlos de mayor a menor y hacer divisiones sucesivas de la siguiente forma:

1. Dividimos n por m obteniendo un resto r_1.

   $$n = mq_1 + r_1,\ 0 \leq r_1 < m.$$

   Resulta que el mcd de n y m es el mismo que el de m y r_1. (Hacer como ejercicio).

2. Dividimos m por r_1 obteniendo un resto r_2.

   $$m = r_1 q_2 + r_2,\ 0 \leq r_2 < r_1.$$

   Al igual que antes tenemos que el mcd de m y r_1 es igual al mcd de r_1 y r_2.

3. Dividimos r_1 por r_2 obteniendo un resto r_3.

   $$r_1 = r_2 q_3 + r_3,\ 0 \leq r_3 < r_2.$$

   Al igual que antes tenemos que el mcd de r_1 y r_2 es igual al mcd de r_2 y r_3.

4. Este proceso se repite hasta llegar a un resto igual a cero, pues la sucesión r_1, r_2, ... es una sucesión de números enteros positivos estrictamente decreciente.

5. Resulta que el último resto no nulo es el mcd de n y m. En efecto, supongamos que $r_{t+1} = 0$ y $r_t \neq 0$, entonces:

   $$\mathrm{m.\,c.\,d.}\{n, m\} = \mathrm{m.\,c.\,d.}\{m, r_1\} = \mathrm{m.\,c.\,d.}\{r_1, r_2\} = \cdots = \mathrm{m.\,c.\,d.}\{r_{t-1}, r_t\} = r_t,$$

   ya que r_t divide a r_{t-1}, pues el resto de la división de r_{t-1} por r_t es $r_{t+1} = 0$.

6. Este proceso nos permite también obtener números enteros a y b que verifican la Identidad de Bezout: $d = an + bm$. Basta desandar el camino para expresar r_t como una combinación lineal, con coeficientes enteros de n y m.

Cálculo de los coeficientes de la identidad de Bezout. Es claro que cada resto r_i, $i = 1, \ldots, t$ se puede expresar en la forma $r_i = a_i n + b_i m$; basta desandar el camino seguido al hacer las divisiones sucesivas. Por ejemplo $r_1 = n - q_1 m$, luego $a_1 = 1$ y $b_1 = -q_1$. Y $r_2 = m - r_1 q_2 = m - (n - q_1 m)q_2 = -q_2 n + (1 + q_1 q_2)$. Si suponemos que conocemos las expresiones de r_{i-1} y r_i, vamos a calcular la expresión para r_{i+1}. En efecto, se tiene:

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_{i+1} \\ &= a_{i-1} n + b_{i-1} m - (a_i n + b_i m) q_{i+1} \\ &= (a_{i-1} - a_i q_{i+1}) n + (b_{i-1} - b_i q_{i+1}) m. \end{aligned}$$

Esto es,

$$a_{i+1} = a_{i-1} - a_i q_{i+1} \text{ y } b_{i+1} = b_{i-1} - b_i q_{i+1}.$$

Podemos entonces completar la siguiente tabla, con los valores iniciales que se indican, tomando $r_{-1} = n$ y $r_0 = m$:

	r	q	a	b
-1			1	0
0			0	1
1			1	$-q_1$
2			$-q_2$	$1+q_1q_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Ejemplo. 10.20.
Calcular la identidad de Bezout para 27 y 8: $(27a + 8b = 1)$.

En nuestro caso hacemos las divisiones sucesivas:

	3	2	1
27	8	3	2
3	2	1	

$$\begin{aligned} 1 &= 3 - 1 \times 2 \\ &= 3 - 1 \times (8 - 2 \times 3) = 3 \times 3 - 1 \times 8 \\ &= 3 \times (27 - 3 \times 8) - 1 \times 8 = 3 \times 27 - 10 \times 8. \end{aligned}$$

	r	q	a	b
-1			1	0
0			0	1
1	3	3	1	-3
2	2	2	$0-2=-2$	$1-(-3)2=7$
3	1	1	$1-(-2)1=3$	$-3-(7)1=-10$

10.6. Resolución de ecuaciones diofánticas

Una ecuación diofántica en números enteros es una ecuación del tipo

$$nX + mY = c, \tag{II.1}$$

en donde n, m y c son números enteros.

Una **solución de la ecuación diofántica** (II.1) es una pareja de números enteros (a, b) verificando $na + mb = c$.

Observar que si la ecuación diofántica tiene una solución, entonces c pertenece al conjunto $T = \{nx + my \mid \ x, y \in \mathbb{Z}\} = \{xd \mid \ x \in \mathbb{Z}\}$, siendo $d = \text{m. c. d.}\{n, m\}$, luego c es un múltiplo de d.

Proposición. 10.21.
Si la ecuación diofántica $nX + mY = c$ tiene solución entera, entonces c es un múltiplo del máximo común divisor de n y m.

Ejemplo. 10.22.
Comprobar que la ecuación diofántica $4X - 6Y = 5$ no tiene solución.

SOLUCIÓN. Basta aplicar el razonamiento anterior. Alternativamente comprobar que para cualquier solución (a, b) se tendría que 2 divide a $4a - 6b$, mientras que 2 no divide a 5, luego esta ecuación diofántica no tiene solución. □

Se trata ahora de comprobar si el recíproco de la Proposición 10.21. es cierto, esto es, comprobar que si $d = \text{m. c. d.}\{n, m\}$ y $d \mid c$, entonces la ecuación $nX + mY = c$ tiene solución y calcular esta o estas soluciones.

Supongamos que $nX + mY = c$ es una ecuación diofántica, que $d = \text{m. c. d.}\{n, m\}$ y que $d|c$. Entonces dividiendo por d en ambos miembros se obtiene

$$\frac{n}{d}X + \frac{m}{d}Y = \frac{c}{d}.$$

Como ahora se tiene $\text{m. c. d.}\{\frac{n}{d}, \frac{m}{d}\} = 1$, podemos suponer que ésta es la situación inicial. Esto es, podemos suponer que $d = 1$ en la hipótesis de partida.

Debido a la identidad de Bezout existen números enteros α y β tales que $n\alpha + m\beta = 1$, en consecuencia, si multiplicamos por c se tiene

$$n(\alpha c) + m(\beta c) = c,$$

y la pareja $(\alpha c, \beta c)$ es una solución de la ecuación diofántica.

¿Existen más soluciones?

Basta ver que, dada una solución (a, b) de la ecuación diofántica siempre se verifica

$$c = na + mb = na + nm - nm + mb = n(a + m) + m(b - n),$$

y por tanto $(a + m, b - n)$ es también una solución. Esto lo podemos hacer, en vez de con nm, con cualquier múltiplo común de n y m.

Por otro lado si (a', b') es otra solución, entonces se verifica $na' + mb' = c$, esto es, $n(a - a') + m(b - b') = 0$ Tenemos entonces $n(a - a') = m(b' - b)$, un múltiplo común de n y m, y por

tanto de su mínimo común múltiplo, que en este caso es nm. Luego $nm \mid n(a-a')$, de donde $m \mid a-a'$, y existe $t \in \mathbb{Z}$ tal que $tm = a-a'$, luego $a' = a - tm$. Y por el mismo motivo $n \mid b'-b$ y existe $s \in \mathbb{Z}$ tal que $b' = b+sn$. Tenemos

$$c = na' + mb' = n(a-tm) + m(b+sn) = na + mb - tnm + snm,$$

y resulta $tnm = snm$, de donde $t = s$. En consecuencia, si (a', b') es otra solución de la ecuación diofántica, tenemos $a' = a - tm$ y $b' = b + tn$ para un cierto $t \in \mathbb{Z}$. Esto nos permite, conocida una de ellas, calcular todas las soluciones de una ecuación diofántica. Tenemos entonces:

Proposición. 10.23.
La ecuación diofántica $nX + mY = c$ tiene solución entera, si y solo si c es un múltiplo del máximo común divisor de n y m. En este caso si el par a, b es una solución, entonces el resto de las soluciones se obtienen como los pares $a - tm$ y $b + tn$, cuando t varía en $\mathbb{Z}$.

Ejemplo. 10.24.
Calcular las soluciones de la ecuación diofántica $4X - 6Y = 10$.

SOLUCIÓN. Reducimos la ecuación anterior dividiendo ambos miembros por $2 = \mathrm{m.c.d.}\{4,6\}$, y obtenemos la ecuación $2X-3Y = 5$. Una solución es: $(1,-1)$. Las soluciones de la ecuación son de la forma $(1+t3, -1+t2)$ para $t \in \mathbb{Z}$, esto es, las soluciones son:

$$(1,-1),(4,1),(7,3),\ldots,(-2,-3),(-5,-5),\ldots$$

□

Ejemplo. 10.25.
Calcular las soluciones de la ecuación diofántica $7X - 11Y = 2$.

SOLUCIÓN. Primero como 7 y 11 son primos relativos, calculamos la identidad de Bezout haciendo divisiones sucesivas:

	1	1	1
11	7	4	3
4	3	1	

$$1 = 4-3 = 4-(7-4) = -7+2\cdot 4 = -7+2(11-7) = -3\cdot 7 + 2\cdot 11$$

Luego se tiene $1 = -3\cdot 7 - (-2)\cdot 11$, multiplicando por 2 tenemos $2 = -6\cdot 7 - (-4)\cdot 11$. Entonces una solución es $(-6,-4)$. Comprobación:

$$7\cdot(-6) - 11\cdot(-4) = -42 + 44 = 2.$$

El resto de las soluciones son: $(-6 - t(-11), -4 + t7) = (11t-6, 7t-4)$. Observar que todas ellas también se pueden escribir como $(11t-6, 7t-4) = (11(t-1)+5, 7(t-1)+3)$, luego otra forma de expresar todas las soluciones es: $(11t+5, 7t+3)$. □

10.7. Congruencias

Dado un número entero positivo n, distinto de 1, existe en $\mathbb{Z}$ una relación de equivalencia R_n definida por:

$$xR_ny \text{ si } x-y \text{ es un múltiplo de } n$$

Observar que también podemos considerar n un entero negativo, en este caso se tiene $R_n = R_{-n}$, por esta razón reducimos el estudio a considerar enteros positivos.

La clase de equivalencia $[y]$ de un número entero y está formada por todos los números enteros x que están relacionados con y, esto es, todos los números enteros x tales que $x-y = tn$ para algún $t \in \mathbb{Z}$, luego x es un número de la forma: $x = y + tn$.

Podemos hacer un listado de los elementos de $[y]$:

$$[y] = \{y, y+n, y+2n, y+3n, \ldots, y-n, y-2n, y-3n, \ldots\}.$$

Recordar que las clases de equivalencia formaban una partición del conjunto, en este caso de $\mathbb{Z}$, resulta pues que las siguientes clases son la partición de $\mathbb{Z}$ asociada a la relación R_n:

$$\begin{aligned}
[0] &= \{0, n, 2n, 3n, \ldots, -n, -2n, -3n, \ldots\},\\
[1] &= \{1, 1+n, 1+2n, 1+3n, \ldots, 1-n, 1-2n, 1-3n, \ldots\}\\
[2] &= \{2, 2+n, 2+2n, 2+3n, \ldots, 2-n, 2-2n, 2-3n, \ldots\}\\
&\vdots\\
[n-1] &= \{n-1, 2n-1, 3n-1, 4n-1, \ldots, -1, -n-1, -2n-1, \ldots\}
\end{aligned}$$

Observar que $[n] = [0]$, $[n+1] = [1]$, etc. y que $[-1] = [n-1]$, $[-2] = [n-2]$, etc. Como consecuencia tenemos exactamente n clases distintas. El conjunto de todas estas clases lo representamos por $\mathbb{Z}_n$.

Como cada clase de $\mathbb{Z}_n$ contiene un único elemento x que verifica $0 \leq x < n$, a este elemento x lo llamamos el **representante canónico** de la clase, y por abuso de notación a veces escribimos x en lugar de $[x]$. Recordar que otra forma de representar a la clases $[x]$ era escribir $\overline{x}$.

$$[y] = \{y, y+n, y+2n, y+3n, \ldots, y-n, y-2n, y-3n, \ldots\} = \overline{y}.$$

En $\mathbb{Z}_n$ es posible definir operaciones a partir de las operaciones en $\mathbb{Z}$, así se tiene:

$$\overline{y_1} + \overline{y_2} := \overline{y_1 + y_2}.$$

$$\overline{y_1} \times \overline{y_2} := \overline{y_1 \times y_2}.$$

Para definir estas operaciones podemos tomar el representante de las clases de y_1 y de y_2 que queramos, en la seguridad de que el resultado obtenido es el mismo, esto es, es independiente de los representantes elegidos.

En efecto si $\overline{y_1} = \overline{y_1'}$ e $\overline{y_2} = \overline{y_2'}$, entonces $y_i - y_i' = t_i n$ para ciertos $t_i \in \mathbb{Z}$ y para $i = 1, 2$. Se tiene:

$$(y_1 + y_2) - (y_1' + y_2') = (y_1 - y_1') + (y_2 - y_2') = t_1 n + t_2 n = (t_1 + t_2)n,$$

luego $\overline{y_1 + y_2} = \overline{y_1' + y_2'}$ tal y como queríamos. Por otro lado para el producto se tiene:

$$\begin{aligned}(y_1 \times y_2) - (y_1' \times y_2') &= y_1 \times y_2 - y_1 \times y_2' + y_1 \times y_2' - y_1' \times y_2' \\ &= y_1 \times (y_2 - y_2') + (y_1 - y_1') \times y_2' \\ &= y_1 t_2 n + t_1 n y_2' \\ &= (y_1 t_2 + t_1 y_2')n,\end{aligned}$$

luego $\overline{y_1 \times y_2} = \overline{y_1' \times y_2'}$.

Teorema. 10.26.
El conjunto $\mathbb{Z}_n$, con las operaciones suma y producto, antes definidas, es un anillo conmutativo.

Observar que en $\mathbb{Z}_n$ puede ocurrir que el producto de dos elementos no nulos sea nulo. Por ejemplo en $\mathbb{Z}_6$ se tiene

$$\overline{2} \times \overline{3} = \overline{0}.$$

Comprobar que esto pasa siempre que n admite una factorización propia $n = n_1 n_2$ con $n_i \neq \pm 1$, esto es, siempre que n no es un número entero primo.

Un elemento de $a \in \mathbb{Z}_n$ se llama **invertible** si existe un elemento $b \in \mathbb{Z}_n$ tal que $ab = 1$. También se dice que a es una **unidad**.

Lema. 10.27.
Cuando p es un número primo vamos a comprobar que cada elemento no nulo de $\mathbb{Z}_p$ es invertible.

DEMOSTRACIÓN. En efecto, si $\overline{x} \neq \overline{0}$, entonces x no es múltiplo de p, y por tanto es primo relativo con p; esto significa, por la identidad de Bezout, que existen números enteros a y b verificando $ax + bp = 1$. Pero entonces tenemos la siguiente igualdad:

$$\overline{1} = \overline{ax + bp} = \overline{ax} + \overline{bp} = \overline{ax} + \overline{0} = \overline{ax}$$

y resulta que $\overline{a}$ es el inverso de $\overline{x}$. □

Observar que como consecuencia de este resultado en un anillo $\mathbb{Z}_n$ la clase $\overline{x}$ es invertible si y solo si x y n son primos relativos.

Ejercicio. 10.28.
Calcular el inverso de la clase de 10 en el anillo $\mathbb{Z}_{27}$.

SOLUCIÓN. Basta calcular la identidad de Bezout para 27 y 10: $(27a + 10b = 1)$; en nuestro caso hacemos las divisiones sucesivas:

	2	1	2
27	10	7	3
7	3	1	

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2 \times (10 - 7) = 3 \times 7 - 2 \times 10 \\ &= 3 \times (27 - 2 \times 10) - 2 \times 10 = 3 \times 27 - 8 \times 10. \end{aligned}$$

	r	q	a	b
-1			1	0
0			0	1
1	7	2	1	-2
2	3	1	$0 - 1 = -1$	$1 - (-2)1 = 3$
3	1	2	$1 - (-1)2 = 3$	$-2 - 3 \times 2 = -8$

El inverso de la clase de 10 en $\mathbb{Z}_{27}$ es $\overline{-8} = \overline{19}$. □

Ejemplo. 10.29. (Números pseudo–aleatorios.)
Los números aleatorios se suelen emplear en aplicaciones de simulación, y son de gran valor. En general, sin embargo, es difícil obtener listas eficientes de números aleatorios. Se recurre entonces a generar listas de números en el ordenador que hagan las veces de los números aleatorios, sin necesidad de que lo sean; se conocen como números pseudo–aleatorios.

Un método de generar números pseudo–aleatorios se basa en el uso de las congruencias. si queremos generar una sucesión de números pseudo–aleatorios, damos tres parámetros:

m**,** el módulo,

c**,** el coeficiente,

d**,** el incremento,

x**,** la semilla.

verificando:

$$c, d, x_0 < m, \qquad c \geq 2, \qquad d, x \geq 0.$$

La forma de generar una sucesión $\{x_n\}_n$ de números pseudo–aleatorios es tomar $x_0 = x$, y definir, de forma recursiva, $x_{n+1} = cx_n + d \pmod{m}$, para $n \geq 0$. Los elementos que componen la sucesión dependen de los valores que asignemos a los parámetros m, c, d y x. Si los números pseudo–aleatorios queremos que estén comprendidos entre o y 1, basta considerar la sucesión $\{x_n/m\}_n$.

Ejemplo. 10.30.
Construir la sucesión de números aleatorios para los parámetros siguientes: $m = 1001$, $c = 2$, $d = 3$, $x = 5$.

Tenemos $x_0 = x = 5$, $x_1 = 2 \cdot 5 + 3 = 13 \pmod{1001}$, y el resto se obtienen utilizando la fórmula $x_{n+1} = 2x_n + 3 \pmod{1001}$. El cálculo es sencillo usando algunas funciones de *Mathematica*.

Primero definimos una función, sea L, mediante:

$$\mathbf{L[0]} = \mathbf{5},$$
$$\mathbf{L[n\_Integer]} := \mathbf{Mod[2\ L[n-1] + 3, 1001]}$$

Ahora podemos escribir los primeros números pseudo–aleatorios:

$$\mathbf{Table[L[i], \{i, 0, 10\}]},$$

el resultado es:

$$5, 13, 29, 61, 125, 253, 509, 20, 43, 89, 181$$

en este caso a partir del término x_{60}, que es igual a 5, se repiten todos los términos de la sucesión.

$$\mathbf{Table[L[i], \{i, 0, 60\}]}$$
$$\{5, 13, 29, 61, 125, 253, 509, 20, 43, 89, 181, 365, 733, 468, 939,$$
$$880, 762, 526, 54, 111, 225, 453, 909, 820, 642, 286, 575, 152, 307,$$
$$617, 236, 475, 953, 908, 818, 638, 278, 559, 120, 243, 489, 981, 964,$$
$$930, 862, 726, 454, 911, 824, 650, 302, 607, 216, 435, 873, 748, 498,$$
$$999, 1000, 1, 5\}$$

10.8. Resolución de ecuaciones en congruencias

En el anillo $\mathbb{Z}_n$ podemos plantearnos las mismas cuestiones que en $\mathbb{Z}$. Por ejemplo resolver ecuaciones.

La ecuación $aX + b = 0$ en $\mathbb{Z}_n$, siendo $a, b \in \mathbb{Z}_n$ tiene solución si existe $x \in \mathbb{Z}_n$ tal que $ax + b = 0$.

¿Cómo resolver una ecuación de este tipo?

Observar que si llamamos a a un representante de la clase $a \in \mathbb{Z}_n$ y lo mismo para b y x, entonces la ecuación tiene solución si existe un número entero x tal que $ax+b$ es un múltiplo de n, y por lo tanto si existe $t \in \mathbb{Z}$ tal que $ax + b + tn = 0$. Tenemos pues una ecuación diofántica con incógnitas x y t, la cual tendrá solución si y solo si $\mathrm{m.c.d.}\{a, n\}$ divide a b. En particular cuando $\mathrm{m.c.d.}\{a, n\} = 1$, ya que en este caso existe el inverso de a en $\mathbb{Z}_n$, la solución sería $x = -ba^{-1}$.

Ejemplo. 10.31.
Resolver en $\mathbb{Z}_6$ la ecuación $4X = 2$.

SOLUCIÓN. Observar que en este caso podemos hacer una comprobación con todos los elementos de $\mathbb{Z}_6$, obteniendo:

x	$4x$
0	0
1	4
2	2
3	0
4	4
5	2

como consecuencia tenemos dos soluciones: 2 y 5.
El método indicado anteriormente supone resolver la ecuación diofántica $4X + 6T = 2$. una solución es: $(-1, 1)$, y todas las soluciones son de la forma $(-1 - t3, 1 + t2) = (-(t + 1)3 + 2, (t + 1)2 - 1) = (3s + 2, -2s - 1)$, llamando $s = -(t + 1)$. Entonces todas las soluciones de la ecuación $4X = 2$ en $\mathbb{Z}_6$ son de la forma $\overline{3s + 2}$, esto es, como basta considerar dos valores consecutivos $s = 0$ y $s = 1$, las soluciones serán: $x = 2$ y $x = 5$ □

Cuando se trata de un anillo $\mathbb{Z}_p$, siendo p un número entero primo, la resolución de ecuaciones o de sistemas de ecuaciones se realiza con los métodos algebraicos al uso.

Ejemplo. 10.32.
Resolver en $\mathbb{Z}_{11}$ la ecuación $7X = 2$.

SOLUCIÓN. Otra vez el método exhaustivo es eficaz debido al tamaño de $\mathbb{Z}_{11}$.

x	$7x$	x	$7x$
0	0	6	9
1	7	7	5
2	3	8	1
3	10	9	8
4	6	10	4
5	2		

La solución es 5.
Otra forma es multiplicar por el inverso de 7 en $\mathbb{Z}_{11}$, que observando la tabla es igual a 8,

entonces la solución es: $x = 7^{-1} \times 2 = 8 \times 2 = 5$. Para el cálculo del inverso podemos también utilizar la identidad de Bezout, la cual es: $1 = -3 \times 7 + 2 \times 11$, ver página 68, entonces el inverso de 7 es -3=8, ya que $\overline{-3} = \overline{8}$ en $\mathbb{Z}_{11}$. □

10.9. Teorema chino del resto

Sean n_1 y n_2 dos enteros positivos distintos de 1. Los anillos $\mathbb{Z}_{n_1}$, $\mathbb{Z}_{n_2}$ y $\mathbb{Z}_{n_1 n_2}$ son ya bien conocidos para nosotros. Deseamos averiguar que relación existe entre ellos.

Dados dos anillos conmutativos A y B definimos en el producto cartesiano $A \times B$ dos operaciones:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \times (a_2, b_2) = (a_1 \times a_2, b_1 \times b_2)$$

Lema. 10.33.
$A \times B$ es un anillo conmutativo.

Así pues $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ y $\mathbb{Z}_{n_1 n_2}$ son dos anillos, con el mismo número de elementos: $n_1 n_2$.

¿Son iguales?

Ejemplo. 10.34.
$\mathbb{Z}_2 \times \mathbb{Z}_3$ y $\mathbb{Z}_6$ son iguales (¡isomorfos!).

SOLUCIÓN. Definimos una aplicación $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ mediante:

x	$\longrightarrow$	$f(x)$
0		$(0,0)$
1		$(1,1)$
2		$(0,2)$
3		$(1,0)$
4		$(0,1)$
5		$(1,2)$

es una biyección y es un homomorfismo de anillos, luego los dos anillos son isomorfos (=iguales). □

Ejemplo. 10.35.
¿$\mathbb{Z}_2 \times \mathbb{Z}_2$ y $\mathbb{Z}_4$ son iguales?

SOLUCIÓN. En este caso no son iguales, ya que en $\mathbb{Z}_2 \times \mathbb{Z}_2$ cuando sumamos un elemento consigo mismo el resultado es siempre $(0,0)$, el elemento cero. Mientras que en $\mathbb{Z}_4$ se tiene $\overline{1}+\overline{1}=\overline{2}\neq\overline{0}$. □

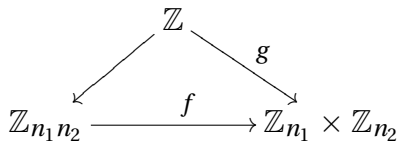
La pregunta es ¿bajo qué condiciones se tiene un isomorfismo $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_1 n_2}$?

El caso de $\mathbb{Z}_2 \times \mathbb{Z}_3$ nos pone sobre la pista de que los subíndices son primos, pero también son primos los subíndices en el caso $\mathbb{Z}_2 \times \mathbb{Z}_2$. ¡Sin embargo en este caso no son primos relativos!

Lema. 10.36.
Sean n_1 y n_2 enteros positivos primos relativos distintos 1, entonces la aplicación $f : \mathbb{Z}_{n_1 n_2} \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ definida por $f(1) = (1,1)$ es un isomorfismo de anillos.

DEMOSTRACIÓN. Primero observamos que para cada entero r se verifica $f(\overline{r}) = (\overline{r}, \overline{r})$. Vamos a ver que f es inyectiva, si $f(\overline{a}) = (0,0)$, entonces $\overline{a} = \overline{0}$ en $\mathbb{Z}_{n_i}$, esto es, a es un múltiplo de n_i, luego es un múltiplo de $n_1 n_2$, su mínimo común múltiplo. Por tanto $\overline{a} = 0$ en $\mathbb{Z}_{n_1 n_2}$. Ahora, como ambos tienen en mismo número de elementos, la aplicación f es biyectiva y ambos anillos son isomorfos. □

En particular $f : \mathbb{Z}_{n_1 n_2} \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ es sobreyectiva y por tanto también lo es la aplicación $g : \mathbb{Z} \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$.



Esto significa que cada par $(\overline{a_1}, \overline{a_2}) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ es la imagen de un elemento de $\mathbb{Z}$, esto es, el sistema

$$\left.\begin{array}{ll} X \equiv a_1 & (\text{mód } n_1) \\ X \equiv a_2 & (\text{mód } n_2) \end{array}\right\}$$

tiene solución cuando n_1 y n_2 son primos relativos.

¿Cómo calcular una solución?

Como n_1 y n_2 son primos relativos, existen a, $b \in \mathbb{Z}$ tales que $an_1 + bn_2 = 1$, entonces se tiene

$$a_1 = an_1a_1 + bn_2a_1 \equiv bn_2a_1 \quad (\text{mód } n_1)$$

y

$$a_2 = an_1a_2 + bn_2a_2 \equiv an_1a_2 \quad (\text{mód } n_2).$$

De aquí deducimos que los $bn_2a_1 + an_1a_2$ son una solución al sistema.

Observar que la solución al sistema es única salvo el módulo $n_1 n_2$.

Este resultado puede extenderse en el siguiente sentido: si $n_1, \ldots, n_t$ son números enteros positivos, primos relativos dos a dos, entonces para cualquier elección de números enteros $a_1, \ldots, a_t$ el sistema

$$\left.\begin{array}{ll} X \equiv a_1 & (\text{mód } n_1) \\ \vdots & \\ X \equiv a_t & (\text{mód } n_t) \end{array}\right\}$$

tiene solución, única salvo módulo $n_1 \cdots n_t$. La forma de resolver este problema es considerar primero el sistema

$$\left.\begin{array}{ll} X \equiv a_1 & (\text{mód } n_1) \\ X \equiv a_2 & (\text{mód } n_2) \end{array}\right\}$$

y calcular una solución, sea ésta, por ejemplo, b, entonces pasamos a considerar ahora el sistema con $t-1$ ecuaciones

$$\left.\begin{array}{ll} X \equiv b & (\text{mód } n_1 n_2) \\ X \equiv a_3 & (\text{mód } n_3) \\ \vdots & \\ X \equiv a_t & (\text{mód } n_t) \end{array}\right\}$$

en donde hamos sustituido las dos primera por $X \equiv b \pmod{n_1 n_2}$. Y se continúa en esta forma hasta obtener una solución del sistema.

Un sistema en congruencias

$$\left.\begin{array}{ll} X \equiv a_1 & (\text{mód } n_1) \\ X \equiv a_2 & (\text{mód } n_2) \end{array}\right\}$$

puede tener solución aunque n_1 y n_2 no sean primos relativos, vamos a ver una solución necesaria y suficiente para que exista solución del sistema.

Supongamos que x es una solución, entonces ser verifica

$$\begin{array}{ll} x - a_1 = \lambda_1 n_1 & \lambda_1 \in \mathbb{Z} \\ x - a_2 = \lambda_2 n_2 & \lambda_2 \in \mathbb{Z} \end{array}$$

entonces se verifica:

$$a_1 - a_2 = -\lambda_1 n_1 + \lambda_2 n_2,$$

esto es, $a_1 - a_2$ es un múltiplo de $\text{m. c. d.}\{n_1, n_2\}$. Veamos que el recíproco también es cierto. Si $d = \text{m. c. d.}\{n_1, n_2\} = \alpha_1 n_1 + \alpha_2 n_2$ y $a_1 - a2 = \lambda d = \lambda\alpha_1 n_1 + \lambda\alpha_2 n_2$. Entonces

$$x = a_1 - \lambda\alpha_1 n_1 = a_2 + \lambda\alpha_2 n_2$$

es una solución del sistema en congruencias. En efecto, se verifica:

$$\begin{array}{l} x - a_1 = -\lambda\alpha_1 n_1 \\ x - a_2 = \lambda\alpha_2 n_2. \end{array}$$

El resto de las soluciones se obtiene sumando un múltiplo del mínimo común múltiplo de n_1 y ${}_n2$. En efecto, si tenemos dos soluciones x_1 y x_2, entonces su diferencia es un múltiplo de n_1 y de n_2, luego es un múltiplo de $\mathrm{m.\,c.\,m.}\{n_1, n_2\}$. Por otro lado es fácil ver que si $M = \mathrm{m.\,c.\,m.}\{n_1, n_2\}$ y x es una solución, entonces $x + \lambda M$, $\lambda \in \mathbb{Z}$, es también una solución.

Ejemplo. 10.37.
Calcular las soluciones del sistema en congruencias:

$$\left.\begin{array}{l} X \equiv 2 \pmod{12} \\ X \equiv 5 \pmod{21} \end{array}\right\}$$

SOLUCIÓN. Ya que $2 - 5$ es un múltiplo de $\mathrm{m.\,c.\,d.}\{12, 21\} = 3$, el sistema tiene solución. Escribimos la identidad de Bezout para $\mathrm{m.\,c.\,d.}\{12, 21\}$, esto es,

$$3 = 2 \times 12 - 21.$$

Se tiene entonces las identidades:

$$\begin{array}{l} 2 - 5 = -(2 \times 12 - 21) = -2 \times 12 + 21, \\ 2 + 2 \times 12 = 5 + 21 = 26. \end{array}$$

Una solución es: 26. La solución general es de la forma $26 + \lambda\,\mathrm{m.\,c.\,m.}\{12, 21\} = 26 + \lambda 84$.

□

Ejemplo. 10.38.
Calcular las soluciones del sistema en congruencias:

$$\left.\begin{array}{l} X \equiv 2 \pmod{12} \\ X \equiv 5 \pmod{21} \\ Z \equiv 18 \pmod{32} \end{array}\right\}$$

SOLUCIÓN. Resolvemos el sistema

$$\left.\begin{array}{l} X \equiv 2 \pmod{12} \\ X \equiv 5 \pmod{21} \end{array}\right\}$$

cuya solución es: $X \equiv 26 \pmod{84}$. Tenemos entonces el sistema:

$$\left.\begin{array}{l} X \equiv 26 \pmod{84} \\ X \equiv 18 \pmod{32} \end{array}\right\}$$

La resolución de este sistema sigue los mismos pasos que en el ejemplo anterior.

(1) Calculo del $\mathrm{m.\,c.\,d.}$ y la identidad de Bezour: $\mathrm{m.\,c.\,d.}\{84, 32\} = 4 = -3 \times 84 + 8 \times 32$.

(2) Expresión de la diferencia 26-18 como múltiplo del $\mathrm{m.\,c.\,d.}$: $26 - 18 = 8 = 2(-3 \times 84 + 8 \times 32) = -6 \times 84 + 16 \times 32$.

(3) Cálculo de la solución particular: $26 + 6 \times 84 = 18 + 16 \times 32 = 530$.

(4) Cálculo de la solución general: $530 + \lambda\,\mathrm{m.\,c.\,m.}\{84, 32\} = 530 + 672\lambda$.

□

Capítulo III

El anillo de polinomios

11. Introducción

Los sistemas de números que se introducen de forma natural son los siguientes: $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$, que corresponden a los números naturales, enteros y racionales respectivamente. En estos sistemas, que tienen propiedades algebraicas cada vez más complejas, existen dos operaciones, la suma y el producto, verificando las siguientes propiedades:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$
SUMA	asociativa conmutativa ex. el. neutro —	asociativa conmutativa ex. el. neutro ex. el. opuesto	asociativa conmutativa ex. el. neutro ex. el. opuesto
	—	GRUPO ABELIANO	GRUPO ABELIANO
PRODUCTO	 conmutativa ex. el. neutro —	asociativa conmutativa ex. el. neutro —	asociativa conmutativa ex. el. neutro ex. el. inverso
	—	—	GRUPO ABELIANO
SUMA Y PRODUCTO	 distributiva	 distributiva	 distributiva
		ANILLO	CUERPO

La construcción realizada de estos sistemas de números permite expresar todas sus elementos a partir de números naturales, que son los enteros no negativos.

Por cuestiones de "*continuidad*" los números racionales se completan a los números reales. Teniendo entonces un conjunto de números, $\mathbb{R}$, con una estructura de cuerpo. La existencia de números reales que no son racionales es fácil de establecer; por ejemplo $\sqrt{2}$ no es un número racional. Si queremos tratar los números reales, de forma exacta, a partir de los números racionales nos damos cuenta de que solamente unos cuantos de aquellos permiten este tratamiento, ejemplos son el citado $\sqrt{2}$ o el número de oro, $\phi = \frac{1+\sqrt{5}}{2}$, ya que ambos son raíces de polinomios con coeficientes enteros; X^2-2 y X^2-X-1 respectivamente. Existen otros números reales que no admiten esta aproximación, ejemplos son π, la razón entre el diámetro y la longitud de la circunferencia, ó e, la base de los logaritmos naturales.

¿Cómo podemos estudiar $\sqrt{2}$? Consideramos el anillo $\mathbb{Q}[X]$ y el conjunto de los múltiplos del polinomio X^2-2, al que representamos por (X^2-2). Entonces el cociente $\mathbb{Q}[X]/(X^2-2)$ es un anillo, que además es un cuerpo. Los elementos de $\mathbb{Q}[X]/(X^2-2)$ son clases, y cada una tiene un representante del tipo $aX+b$, siendo $a, b \in \mathbb{Q}$. Es pues un espacio vectorial de dimensión dos con base $\{\overline{1}, \overline{X}\}$. Observar que $\overline{X}$ verifica $\overline{X}^2 = \overline{2}$, ya que $\overline{X^2-2} = 0$, y por tanto $\overline{X}$ puede ser considerado como $\sqrt{2}$; esto es, hemos ampliado el conjunto de los números racionales con un nuevo elemento que es una raíz cuadrada de 2.

Para el número de oro ϕ podemos hacer un tratamiento similar, esta vez con el polinomio X^2-X-1.

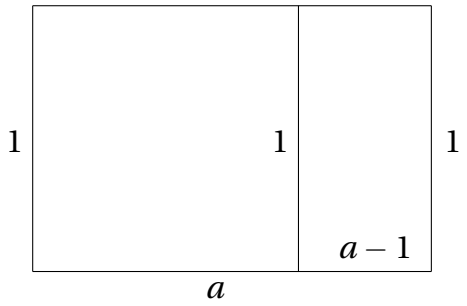
Observamos que el uso de los polinomios es necesario si queremos estudiar algunos números reales. Este uso de polinomios nos va a permitir introducir otros números que no son reales, como por ejemplo i, que será una raíz del polinomio X^2+1. De esta forma tenemos

el cuerpo $\mathbb{Q}[X]/(X^2+1)$, pero también el cuerpo $\mathbb{R}[X]/(X^2+1)$, que se va a identificar con el cuerpo de los números complejos, al que representamos por $\mathbb{C}$.

Hemos ido introduciendo nuevos sistemas de números y en cada caso hemos visto que se obtenían cuerpos, más adelante veremos que para tener un cuerpo $K[X]/(p(X))$ es necesario y suficiente que $p(X)$ sea un polinomio irreducible. Y también veremos que los polinomios irreducibles hacen el papel de los números enteros primos, esto es, cada polinomio en $K[X]$ es, de forma única, un producto de polinomios irreducibles. Por esta razón nos interesará dar criterios para ver cuando un polinomio es o no irreducible. En nuestro estudio nos vamos a restringir a trabajar sobre los anillos de polinomios con coeficientes en $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, y a veces en $\mathbb{Z}_p$, y utilizaremos $\mathbb{Z}[X]$ como una herramienta para estudiar el caso más difícil: los polinomios en $\mathbb{Q}[X]$.

El número de oro.

Si se considera un rectángulo de dimensiones 1 y $a > 1$, y si a este rectángulo le quitamos un cuadrado de lado 1, ¿cuándo las proporciones entre los lados del rectángulo original y el nuevo están en la misma proporción? El número de oro es el valor de a para el que esto se verifica.



Como $\frac{a}{1} = \frac{1}{a-1}$, resulta $a(a-1) = 1$, esto es, a es raíz del polinomio $X^2 - X - 1$.

11.1. Definición de anillo

Un **anillo** es una cuaterna $(A, +, \times, 1)$ formada por un conjunto no vacío A, dos operaciones binarias: $+$ y $\times$ y un elemento $1 \in A$ verificando las siguientes propiedades:

(1) $(A, +)$ es un **grupo abeliano**, esto es, la operación $+$, suma, verifica las propiedades asociativa, conmutativa, existe un elemento neutro, lo llamamos **cero** del anillo, y cada elemento de A tiene un elemento **opuesto**.

(2) La operación $\times$, producto, verifica las propiedades asociativa y conmutativa.

(3) 1 es un elemento neutro para la operación $\times$, lo llamamos **uno** del anillo.

(4) Se verifica la propiedad distributiva del producto respecto a la suma: $a \times (b + c) = (a \times b) + (a \times c)$ para cada $a, b, c \in A$.

De estas propiedades se obtienen algunas consecuencias inmediatas como las siguientes:

Lema. 11.1.
Sea A un anillo, entonces se verifica:

(1) El elemento cero está unívocamente determinado, lo representamos por 0.

(2) Para cada elemento $a \in A$ el elemento opuesto de a está unívocamente determinado, lo representamos por $-a$.

(3) Para cada elemento $a \in A$ se verifica $-a = (-1) \times a$.

(4) Para cada elemento $a \in A$ se verifica $0 \times a = 0$.

(5) Para cada par de elementos $a, b \in A$ se verifica $(-a) \times b = -(ab) = a \times (-b)$.

El producto $a \times b$ también se suele representar por ab.

Ejemplo. 11.2.
El conjunto $\mathbb{Z}$ de los números enteros, con la suma, y producto y el 1 es un anillo. También lo son anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Anillos con un número finito de elementos son los $\mathbb{Z}_n$.

El concepto de divisor de cero es fundamental en la teoría de anillos. Dado un anillo A un elemento $a \in A$ es un **divisor de cero** si existe un elemento $0 \neq b \in A$ tal que $ab = 0$. Es claro que 0 es un divisor de cero y que hay anillos que no tienen divisores de cero no nulos, como por ejemplo $\mathbb{Z}$. Un anillo que no tiene divisores de cero no nulos se llama un **dominio de integridad**.

Ejemplo. 11.3.
El anillo $\mathbb{Z}_4$ no es un dominio de integridad. El anillo $\mathbb{Z}_3$ es un dominio de integridad.

En algunos anillos cada elemento no nulo tiene un inverso con respecto al producto; a estos anillos los llamaremos **cuerpos**.

Ejemplo. 11.4.
El anillo $\mathbb{Z}$ no es un cuerpo, y tampoco lo es $\mathbb{Z}_4$. Los anillos $\mathbb{Q}$ ó $\mathbb{Z}_3$ son cuerpos.

11.2. Homomorfismos

Dados dos anillos A y B, una aplicación $f : A \longrightarrow B$ que verifica las propiedades:

(1) $f(a+b) = f(a) + f(b)$, para cada $a, b \in A$,

(2) $f(a \times b) = f(a) \times f(b)$, para cada $a, b \in A$,

(3) $f(1) = 1$.

se llama un **homomorfismo de anillos**.

Hemos representado las operaciones en A y en B con los mismos símbolos.

Algunas consecuencias inmediatas de la definición de homomorfismo de anillos son:

Lema. 11.5.
Dado un homomorfismo de anillos $f : A \longrightarrow B$ se verifica:

(1) $f(0) = 0$,

(2) Para cada $a \in A$ se tiene $f(-a) = -f(a)$.

(3) Si $a \in A$ tiene inverso, a^{-1}, entonces $f(a^{-1}) = f(a)^{-1}$.

Hacer la demostración como ejercicio.

Asociados a un homomorfismo de anillos existen dos conjuntos: el núcleo y la imagen.

11.3. Ideales

Dado un homomorfismo de anillos $f : A \longrightarrow B$ se define el **núcleo** de f como:

$$\mathrm{Ker}(f) = \{x \in A \mid \ f(x) = 0\}.$$

Lema. 11.6.
Para cada homomorfismo de anillos $f : A \longrightarrow B$ se verifica:

(1) $\mathrm{Ker}(f)$ *es un subgrupo abeliano, esto es, para cualesquiera $x, y \in \mathrm{Ker}(f)$ se tiene $x + y \in \mathrm{Ker}(f)$, $-x \in \mathrm{Ker}(f)$ y $0 \in \mathrm{Ker}(f)$;*

(2) Para cualesquiera $x \in \mathrm{Ker}(f)$ y $a \in A$ se tiene $ax \in \mathrm{Ker}(f)$.

Se introduce un tipo de subconjuntos de un anillo a través de estas propiedades del núcleo de un homomorfismo. Un subconjunto no vacío $I \subseteq A$ se llama un **ideal** de A si verifica:

(1) I es un subgrupo abeliano, esto es, para cualesquiera $x, y \in I$ se tiene $x+y \in I$, $-x \in I$ y $0 \in I$;

(2) Para cualesquiera $x \in I$ y $a \in A$ se tiene $ax \in I$.

Cada ideal I de un anillo A define una relación de equivalencia en A mediante:

$$a \equiv_I b \quad \text{si} \quad a - b \in I.$$

El conjunto cociente $A/\equiv_I$ se representa por A/I, y en él existe una única estructura de anillo de forma que la proyección $p : A \longrightarrow A/I$ sea un homomorfismo de anillos; esta es:

$$\begin{array}{l} [a] + [b] = [a+b], \\ [a]\,[b] = [a\,b], \\ 1 = [1], \end{array}$$

para cualesquiera $a, b \in A$.

Resulta entonces que I coincide con el núcleo de p; así pues cada ideal I de un anillo A es el núcleo de un homomorfismo de anillos con dominio A. El anillo A/I se llama el **anillo cociente** de A por el ideal I.

11.4. Subanillos

Dado un homomorfismo de anillos $f : A \longrightarrow B$ la **imagen** de f se define como

$$\mathrm{Im}(f) = \{y \in B \mid \text{ existe } a \in A \text{ tal que } f(a) = y\}.$$

Lema. 11.7.
Para cada homomorfismo de anillos $f : A \longrightarrow B$ se verifica:

(1) $\mathrm{Im}(f)$ es un subgrupo abeliano, esto es, para cualesquiera $x, y \in \mathrm{Im}(f)$ se tiene $x+y \in \mathrm{Im}(f)$, $-x \in \mathrm{Im}(f)$ y $0 \in \mathrm{Im}(f)$;

(2) Para cualesquiera $x, y \in \mathrm{Im}(f)$ se tiene $xy \in \mathrm{Im}(f)$;

(3) $1 \in \mathrm{Im}(f)$.

Se introduce un tipo de subconjunto de un anillo a través de estas propiedades de la imagen de un homomorfismo. Un subconjunto no vacío $S \subseteq A$ se llama un **subanillo** de A si verifica:

(1) S es un subgrupo abeliano, esto es, para cualesquiera $x, y \in S$ se tiene $x+y \in S$, $-x \in S$ y $0 \in S$;

(2) Para cualesquiera $x, y \in S$ se tiene $xy \in S$;

(3) $1 \in S$.

11.5. Elementos primos e irreducibles

Vamos a suponer que A es un dominio de integridad.

Lema. 11.8.
El conjunto de los elementos invertibles es cerrado para la multiplicación, tomar inverso y el elemento 1.

Dados $a, b \in A$, decimos que $a \mid b$, y se lee, a **divide** a b, si existe $c \in A$ tal que $b = ac$. Dos elementos $a, b \in A$ se llaman **asociados** si $a \mid b$ y $b \mid a$; se escribe $a \sim b$.

Lema. 11.9.
(1) La relación $\sim$ es una relación de equivalencia en A.

(2) Dos elementos $a, b \in A$ son asociados si existe un elemento invertible $u \in A$ tal que $b = au$.

Un elemento $p \in A$ se llama **primo** si verifica:

(1) p es no nulo y no es invertible;

(2) Si $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.

Un elemento $q \in A$ se llama **irreducible** si verifica:

(1) q es no nulo y no es invertible;

(2) Si $q = ab$, entonces a es una unidad o b es una unidad.

Esto es, si q no tiene una factorización propia.

Lema. 11.10.
Todo elemento primo es irreducibles.

DEMOSTRACIÓN. Supongamos que p es un elemento primo, para ver que es irreducible supongamos que p se escribe como $p = ab$, entonces $p \mid ab$, y por tanto $p \mid a$ ó $p \mid b$. Supongamos que $p \mid a$, entonces existe $c \in A$ tal que $a = pc$. Tenemos la igualdad $p = ab = pcb$. Como A es un dominio de integridad, entonces $1 = cb$ y se tiene que b es un elemento invertible.
□

12. Anillos de polinomios

Sea A un anillo conmutativo y X una *indeterminada*, esto es; un símbolo que no pertenece a A. Llamamos **polinomio en X con coeficientes en A** a una expresión formal del tipo

$$a_nX^n + \cdots + a_1X + a_0,$$

con $a_n, \ldots, a_1, a_0 \in A$, $n \in \mathbb{N}$ y donde $X^2, \ldots, X^n$ son nuevos símbolos que están relacionados con X. Los elementos $a_n, \ldots, a_1, a_0$ se llaman los **coeficientes** del polinomio.

Representamos el conjunto de todos los polinomios en X con coeficientes en A por $A[X]$.

Sean, en lo que sigue, $p(X) = a_nX^n + \cdots + a_1X + a_0$ y $q(X) = b_mX^m + \cdots + b_1X + b_0$ dos polinomios elementos de $A[X]$.

Decimos que $p(X)$ y $q(X)$ son **polinomios iguales** si

$$a_i = b_i, \text{ para } 0 \leq i \leq \min\{n, m\} \text{ y } a_j = 0, b_j = 0 \text{ si } j > \min\{n, m\}.$$

Como consecuencia o un polinomio tiene todos sus coeficientes iguales a cero, en cuyo caso es igual al polinomio 0 o tiene algún coeficiente no nulo, en cuyo caso es igual a un único polinomio $a_nX^n + \cdots + a_1X + a_0$ que verifica la condición $a_n \neq 0$. Salvo que se indique lo contrario los polinomios que introduciremos estarán representados en esta forma única.

Dado un polinomio no nulo $p(X) = a_nX^n + \cdots + a_1X + a_0$, $a_n \neq 0$, llamamos **coeficiente líder** de $p(X)$ a a_n y **coeficiente ó término independiente** de $p(X)$ a a_0. Llamamos a n el **grado** de $p(X)$, y lo notamos $\operatorname{grad}(p(X))$. El polinomio $p(X)$ es **constante** si $n = 0$. Cuando el coeficiente líder es igual a uno el polinomio se llama **mónico**.

Diremos que el polinomio nulo $p(X) = 0$ es un polinomio constante que tiene grado $-\infty$.

Definimos a continuación dos operaciones binarias en el conjunto $A[X]$. Sean $p(X)$ y $q(X)$ como antes, entonces definimos una **operación suma** mediante:

$$p(X) + q(X) = (a_h + b_h)X^h + \cdots + (a_1 + b_1)X + (a_0 + b_0),$$

y una **operación producto**:

$$p(X)q(X) = a_nb_mX^{n+m} + \cdots + t_iX^i + (a_0b_1 + a_1b_0)X + a_0b_0,$$

donde $a_k = 0$ si $k > n$, $b_l = 0$ si $l > m$, $h = max\{n, m\}$ y $t_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$, $0 \leq i \leq n + m$.

Lema. 12.1.
En la situación anterior $A[X]$ es un anillo con elemento uno igual al polinomio constante 1.

Si $X_1, \ldots, X_r$ son indeterminadas sobre A, definimos, por recurrencia, el anillo de polinomios en las indeterminadas $X_1, \ldots, X_r$ con coeficientes en A como $A[X_1, \ldots, X_r] = A[X_1, \ldots, X_{r-1}][X_r]$. Podemos definir el grado en cada una de las indeterminadas, ya que para cada $1 \leq i \leq r$ existe un isomorfismo

$$A[X_1, \ldots, X_r] \cong A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_r][X_i].$$

Como consecuencia cada elemento $p(X_1, \ldots, X_r) \in A[X_1, \ldots, X_r]$ se expresa de forma única como una suma finita de la siguiente forma:

$$p(X_1, \ldots, X_r) = \sum_{(e_1, \ldots, e_r) \in \mathbb{N}^r} a_{e_1 \ldots e_r} X_1^{e_1} \cdots X_r^{e_r},$$

donde $a_{e_1 \ldots e_r} \in A$ son casi todos nulos. A cada uno de los sumandos de esta suma, con $a_{e_1 \ldots e_r} \neq 0$, lo llamamos un **monomio** de $p(X_1, \ldots, X_r)$. Definimos el grado de un monomio simplemente como la suma de los grados en cada una de las indeterminadas, y decimos que un polinomio es **homogéneo** si todos sus monomios tienen el mismo grado.

12.1. Aritmética del anillo de polinomios

Volvamos ahora a la situación de polinomios en una indeterminada. Vamos a estudiar la aritmética del anillo $A[X]$.

Lema. 12.2.
Sea A un anillo y $p(X)$, $q(X) \in A[X]$, entonces se tiene que $\operatorname{grad}(p(X)q(X)) \leq \operatorname{grad}(p(X)) + \operatorname{grad}(q(X))$. *Y si A es un DI, entonces se verifica la igualdad.*

DEMOSTRACIÓN. Tenemos que $p(X)q(X) = a_n b_m X^{n+m} + \cdots + a_0 b_0$, si $a_n b_m = 0$, entonces $\operatorname{grad}(p(X)q(X)) < \operatorname{grad}(p(X)) + \operatorname{grad}(q(X))$. Si A es un DI, entonces $a_n b_m \neq 0$ y $\operatorname{grad}(p(X)q(X)) = \operatorname{grad}(p(X)) + \operatorname{grad}(q(X))$. □

Es fácil ver que en general no se tiene la igualdad.

Ejemplo. 12.3.
Se consideran los polinomios $p(X) = 2X + 1$ y $q(X) = 3X + 2$ con coeficientes en $\mathbb{Z}_6$, entonces $\operatorname{grad}(p(X)q(X)) = 1 \neq 2 = \operatorname{grad}(p(X)) + \operatorname{grad}(q(X))$.

Corolario. 12.4.
Sea A un anillo, son equivalentes:

(a) A *es un DI.*

(b) $A[X]$ *es un DI.*

(c) $\mathrm{grad}(p(X)q(X)) = \mathrm{grad}(p(X)) + \mathrm{grad}(q(X))$ *para cada* $p(X), q(X) \in A[X]$.

Sea A un anillo, definimos una aplicación $t_A : A \to A[X]$ mediante $t_A(a) = a$, el polinomio constante, para cada $a \in A$.

Lema. 12.5.
En la situación anterior t_A *es un homomorfismo de anillos inyectivo. Vamos a identificar* A *con su imagen por* t_A *en* $A[X]$.

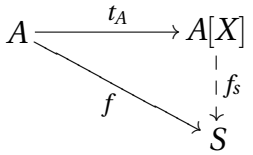
Corolario. 12.6.
Si A *un DI, entonces los elementos invertibles de* $A[X]$ *coinciden con los elementos invertibles de* A.

DEMOSTRACIÓN. Es claro que todo elemento invertible de A es también invertible en $A[X]$. Supongamos que $p(X) \in A[X]$ es un elemento invertible, entonces existe $q(X) \in A[X]$ tal que $p(X)q(X) = 1$. Aplicando el Lema 12.2., tenemos que $0 = \mathrm{grad}(1) = \mathrm{grad}(p(X)q(X)) = \mathrm{grad}(p(X)) + \mathrm{grad}(q(X))$, por tanto $\mathrm{grad}(p(X)) = 0$, y $p(X)$ es un polinomio constante, esto es; pertenece a A. □

Este resultado no es cierto en general, como el siguiente Ejemplo prueba.

Ejemplo. 12.7.
El el anillo $\mathbb{Z}_4[X]$ el polinomio $p(X) = 2X + 1$ es un polinomio invertible, ya que $p(X)p(X) = (2X + 1)(2X + 1) = 1$, y es claro que $p(X)$ no es un polinomio constante.

Teorema. 12.8. (Propiedad universal del anillo de polinomios)
Sea A *un anillo y* $f : A \longrightarrow S$ *un homomorfismo de anillos. Para cada* $s \in S$ *existe un único homomorfismo de anillos* $f_s : A[X] \longrightarrow S$ *tal que* $f_s(X) = s$ *y* $f = f_s t_A$.



DEMOSTRACIÓN. Sea $p(X) = a_n X^n + \cdots + a_1 X + a_0$ un polinomio en $A[X]$. Definimos $f_s(p(X)) = f(a_n)s^n + \cdots + f(a_1)s + f(a_0)$. Así definido f_s es un homomorfismo de anillos y verifica $f_s(X) = s$ y $f = f_s t_A$. Para probar la unicidad, podemos aplicar que X y A generan el anillo $A[X]$. □

Como consecuencia, esta propiedad universal determina, salvo isomorfismo, el anillo de polinomios en una indeterminada X. Esto es; si Y es otra indeterminada, entonces los anillos $A[X]$ y $A[Y]$ son isomorfos.

Otra consecuencia del Teorema 12.8. es la siguiente:

Corolario. 12.9.
Para cada elemento $a \in A$ existe un único homomorfismo de anillos $e_a : A[X] \to A$ inducido por la identidad en A y el elemento $a \in A$.

El homomorfismo e_a se llama **homomorfismo de evaluación** en a. La imagen del polinomio $p(X)$ por e_a la notaremos simplemente por $p(a)$. Observar que consiste en sustituir, en la expresión de polinomio $p(X)$, X por a, X^2 por a^2, etc.

Proposición. 12.10.
Sea $g : A \longrightarrow B$ un homomorfismo de anillos, y X una indeterminada, entonces g induce un único homomorfismo de anillos, $g' : A[X] \longrightarrow B[X]$, entre los anillos de polinomios haciendo conmutativo el diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\quad g \quad} & B \\ {\scriptstyle t_A}\downarrow & & \downarrow{\scriptstyle t_B} \\ A[X] & \xrightarrow[g']{\quad - - - \quad} & B[X] \end{array}$$

Donde t_A y t_B son los homomorfismos canónicos del Lema 12.5. de A en $A[X]$ y de B en $B[X]$ respectivamente.

DEMOSTRACIÓN. Es consecuencia directa de la propiedad universal del anillo de polinomios cuando tomamos $f = t_B g$ y $b = X \in B[X]$ □

12.2. Divisibilidad en anillos de polinomios

Teorema. 12.11. (Algoritmo de Euclides)
Sea A un anillo y $p(X)$, $q(X) \in A[X]$, con $q(X) \neq 0$ y coeficiente líder un elemento invertible en A. Entonces existen polinomios, únicos, $c(X)$, $r(X) \in A[X]$ que verifican:

(1) $p(X) = q(X)c(X) + r(X)$ *y*

(2) $\operatorname{grad}(r(X)) < \operatorname{grad}(q(X))$.

DEMOSTRACIÓN. Vamos a hacer la demostración por inducción sobre el grado de $p(X)$. Si $\text{grad}(p(X)) < \text{grad}(q(X))$, basta tomar $c(X) = 0$ y $r(X) = p(X)$. Supongamos que $\text{grad}(p(X)) \geq \text{grad}(q(X))$. Si $\text{grad}(q(X)) = 0$, entonces tomamos $c(X) = p(X)q(X)^{-1}$ y $r(X) = 0$. Supongamos ahora que el resultado es cierto para todos los polinomios de grado menor que el de $p(X)$, y fijando notación sean $n = \text{grad}(p(X)) \geq \text{grad}(q(X)) = m \geq 0$; definimos

$$p_1(X) = p(X) - (a_n b_m^{-1})X^{n-m}q(X),$$

es claro que $\text{grad}(p_1(X)) < n$, y entonces, por la hipótesis de inducción tenemos

$$\left.\begin{array}{l} p_1(X) = q(X)c_1(X) + r_1(X) \\ \text{grad}(r_1(X)) < \text{grad}(q(X)) \end{array}\right\} \text{ con } c_1(X) \text{ y } r_1(X) \text{ únicos.}$$

Se tiene entonces la siguiente igualdad:

$$p(X) = q(X)\left[c_1(X) + (a_n b_m^{-1})X^{n-m}\right] + r_1(X).$$

Por tanto únicamente queda probar la unicidad de esta descomposición. Supongamos que tenemos dos descomposiciones

$$p(X) = q(X)c_1(X) + r_1(X) = q(X)c_2(X) + r_2(X),$$

con $\text{grad}(r_i(X)) < \text{grad}(q(X))$, $i = 1, 2$.

Entonces tenemos:

$$r_1(X) - r_2(X) = q(X)[c_1(X) - c_2(X)],$$

y si $c_1(X) - c_2(X) \neq 0$, entonces se verifica:

$$\text{grad}(r_1(X) - r_2(X)) = \text{grad}(q(X)[c_1(X) - c_2(X)] =$$

$$\text{grad}(q(X)) + \text{grad}(c_1(X) - c_2(X)) \geq \text{grad}(q(X)) > \text{grad}(r_1(X) - r_2(X)),$$

lo cual es una contradicción. Entonces ha de ser necesariamente $c_1(X) = c_2(X)$, y como consecuencia $r_1(X) = r_2(X)$. □

Vamos a dar nombre a los polinomios que nos aparecen en el Teorema 12.11.. El polinomio $c(X)$ se llama **cociente** de $p(X)$ por $q(X)$, y $r(X)$ se llama **resto** de la división.

Corolario. 12.12.
Cuando K es un cuerpo, y $p(x)$, $q(x) \in K[X]$ tales que $q(X) \neq 0$, entonces podemos hacer la división de $p(X)$ por $q(x)$ ya que el coeficiente líder de $q(X)$ es una unidad en K.

12.3. Definición de dominio euclídeo

El anillo $K[X]$, cuando K es un cuerpo, y el anillo $\mathbb{Z}$ de los números enteros son ejemplos de un tipo especial de anillos en los que es posible hacer una división con resto. Estos anillos son dominios de integridad y en ellos existe una función euclídea, el grado y el valor absoluto, respectivamente, $d : A \setminus \{0\} \longrightarrow \mathbb{N}$. verificando la siguiente propiedad para cualesquiera $0 \neq a, b \in A$:

(1) $d(ab) \geq d(b)$.

(2) *existen* $c, r \in A$ *tales que* $a = bc + r$ *y* $r = 0$ *ó* $d(r) < d(b)$.

Un dominio de integridad A en el que existe una aplicación $d : A \longrightarrow \mathbb{N}$ verificando estas condiciones se llama un **dominio euclídeo**.

Ejemplo. 12.13.

(1) Si K es un cuerpo entonces $K[X]$ es un dominio euclídeo con función euclídea δ definida por $\delta(p(X)) = \mathrm{grad}(p(X))$, y como hemos comprobado antes en él tenemos una división con resto.

(2) En el anillo $\mathbb{Z}$ de los números enteros tenemos que el valor absoluto es una función euclídea y la división con resto usual.

En un dominio euclídeo se tienen las siguientes propiedades:

(1) cada ideal I está generado por un elemento, esto es, existe un elemento $a \in A$ tal que $I = \{ax \mid \ x \in A\}$;

(2) cada elemento irreducible es primo.

(3) cada elemento no nulo y no invertible se escribe, de forma única, como un producto de elementos irreducibles.

12.4. Máximo común divisor y mínimo común múltiplo

La aritmética de los números enteros podemos imitarla en el anillo $K[X]$ de polinomios con coeficientes en un cuerpo K. Dados dos polinomios $p(X)$, $q(X) \in K[X]$, decimos que $p(x)$ **divide a** $q(X)$ si existe un polinomio $h(X) \in K[X]$ tal que $q(X) = p(X)\ h(X)$, y se representa por $p(X) \mid q(X)$; también se dice que $p(X)$ es un **divisor** de $q(X)$.

La relación *divide* en $K[X]$ verifica, tal y como ocurría en el caso de la división con números enteros, las propiedades reflexiva y transitiva, pero no las propiedades simétrica o antisimétrica.

Dos polinomios $p(X), q(X) \in K[X]$ se llaman **asociados** si $p(X) \mid q(X)$ y $q(X) \mid p(X)$, y lo representamos por $p(X) \sim q(X)$.

Ejercicio. 12.14.
Demuestre que un polinomio $p(X) \in K[X]$ es una unidad (esto es, es invertible) si y solo si es un polinomio contante no nulo.

SOLUCIÓN. Ver Corolario 12.6. □

Ejercicio. 12.15.

(1) *Demuestre que $p(X), q(X) \in K[X]$ son asociados si y solo si existe una unidad $u \in K[X]$ tal que $q(X) = u\,p(X)$.*

(2) *Demuestre que la relación asociado es una relación de equivalencia en $K[X]$.*

(3) *¿Cuál es la clase de equivalencia de un polinomio $p(X) \in K[X]$?*

Dados dos polinomios $p(X), q(X) \in K[X]$ un **divisor común** es un polinomio $d(X) \in K[X]$ tal que $d(X) \mid p(X)$ y $d(X) \mid q(X)$, y un **máximo común divisor** es un divisor común $h(X)$ al que divide cualquier otro divisor común, esto es, $d(X)$ es un máximo común divisor de $p(X)$ y $q(X)$ si

$$\begin{aligned} &d(X) \mid p(X) \text{ y } d(X) \mid q(X), \text{ y} \\ \text{si } &t(X) \mid p(X) \text{ y } t(X) \mid q(X), \text{ entonces } t(X) \mid d(X). \end{aligned}$$

El máximo común divisor de $p(X)$ y $q(X)$ se representa por $\mathrm{m.\,c.\,d.}\{p(X), q(X)\}$.

Ejercicio. 12.16.

(1) *Demuestre que si $d_1(X)$ y $d_2(X)$ son dos máximos comunes divisores de $p(X)$ y $q(X) \in K[X]$, entonces $d_1(X)$ y $d_2(X)$ son asociados.*

(2) *El máximo común divisor de dos polinomios en $K[X]$ determina unívocamente una clase de equivalencia en $K[X]$ para la relación de equivalencia* asociado.

Dados dos polinomios $p(X), q(X) \in K[X]$ un **múltiplo común** es un polinomio $m(X) \in K[X]$ tal que $p(X) \mid m(X)$ y $q(X) \mid m(X)$, y un **mínimo común múltiplo** es un múltiplo común $m(X)$ que divide a cualquier otro múltiplo común, esto es, $m(X)$ es un mínimo común múltiplo de $p(X)$ y $q(X)$ si

$$\begin{aligned} &p(X) \mid m(X) \text{ y } q(X) \mid m(X), \text{ y} \\ \text{si } &p(X) \mid t(X) \text{ y } q(X) \mid t(X), \text{ entonces } m(X) \mid t(X). \end{aligned}$$

El mínimo común múltiplo de $p(X)$ y $q(X)$ se representa por $\mathrm{m.\,c.\,m.}\{p(X), q(X)\}$.

De forma análoga a como ocurría con el máximo común divisor tenemos los siguientes resultados:

Ejercicio. 12.17.

(1) Demuestre que si $m_1(X)$ y $m_2(X)$ son dos mínimos comunes múltiplos de $p(X)$ y $q(X) \in K[X]$, entonces $m_1(X)$ y $m_2(X)$ son asociados.

(2) El mínimo común múltiplo de dos polinomios en $K[X]$ determina unívocamente una clase de equivalencia en $K[X]$ para la relación de equivalencia asociado.

Identidad de Bezout

Teorema. 12.18. (Identidad de Bezout)
Si $p(X)$, $q(X) \in K[X]$ son polinomios con máximo común divisor $d(X)$, existen polinomios $a(X)$, $b(X) \in K[X]$ tales que

$$d(X) = a(X)\ p(X) + b(X)\ q(X).$$

*Esta relación se conoce como una **identidad de Bezout** para $p(X)$ y $q(X)$.*

DEMOSTRACIÓN. Para simplificar vamos a representar el polinomio $p(X)$ simplemente por p, y este criterio lo vamos a seguir también para los demás elementos de $K[X]$.

Consideramos $p, q \in K[X]$ y $d = \text{m. c. d.}\{p, q\}$. Como $d \mid p$ y $d \mid q$, entonces $d \mid pa + qb$, para cualesquiera $a, b \in K[X]$. Llamamos $I = \{px+qy \mid \ x, y \in K[X]\}$, y sea $h = px+qx \in I$ de grado mínimo. Dividiendo p por h se tiene $p = hc + r = (px + qy)c + r$, luego $r = p(1 - x) + qy \in I$, por tanto $r = 0$ y resulta $h \mid p$. De la misma forma $h \mid q$, y en consecuencia $d \mid h$, esto es, d y h son asociados, luego existen $a, b \in K[X]$ tales que $d = pa + qb$. □

Ejercicio. 12.19.
Demuestre que si $p(X)$, $q(X) \in K[X]$ tienen máximo común divisor $d(X)$ y mínimo común múltiplo $m(X)$, entonces $p(X)\ q(X) \sim d(X)\ m(X)$.

SOLUCIÓN. Llamamos p, q, d y m a $p(X)$, $q(X)$, $d(X)$ y $m(X)$ respectivamente. La identidad de Bezout permite expresar d como $d = pa+qb$, para ciertos $a, b \in K[X]$. Para ciertos $x, y \in K[X]$ se tiene $m = px = qy$. Tenemos entonces $dm = (pa + qb)m = pam + qbm = paqy + qbpx = pq(ay+bx)$, de donde se obtiene $m = \frac{pq}{d}(ay+bx)$. Como $\frac{pq}{d} = p\frac{q}{d} = q\frac{p}{d}$ es un múltiplo común de p y q, entonces existe $z \in K[X]$ tal que $\frac{pq}{d} = mz$. De aquí se obtiene $m = mz(ay + bx)$, y simplificando $1 = z(ay + bx)$, esto es, $p(X)\ q(X) \sim d(X)\ m(X)$. □

Algoritmo de Euclides

En ocasiones es conveniente tener un método de cálculo de los polinomios que aparecen en la Identidad de Bezout, lo que proporciona un método para el cálculo del máximo común divisor; uno de los más sencillos es el **Algoritmo de Euclides**. Sean $p(X)$, $q(X) \in K[X]$ polinomios, no nulos, a los cuales representaremos por p y q respectivamente. Hacemos la división de p por q:

$$p = q\, c_1 + r_1, \text{ con } r_1 = 0 \text{ ó } \operatorname{grad}(r_1) < \operatorname{grad}(q).$$

Si $r_1 = 0$, entonces $q \mid p$ y resulta que el máximo común divisor de p y q es q; si $r_1 \neq 0$, entonces $\mathrm{m.c.d.}\{p, q\} = \mathrm{m.c.d.}\{q, r_1\}$. Se tiene $\operatorname{grad}(r_1) < \operatorname{grad}(p)$, por lo que hacer ahora la división de q por r_1, resulta:

$$q = r_1\, c_2 + r_2, \text{ con } r_2 = 0 \text{ ó } \operatorname{grad}(r_2) < \operatorname{grad}(r_1).$$

Si $r_2 = 0$, entonces $r_1 \mid q$ y resulta que el máximo común divisor de q y r_1 es r_1; si $r_2 \neq 0$, entonces $\mathrm{m.c.d.}\{q, r_1\} = \mathrm{m.c.d.}\{r_1, r_2\}$. Se tiene $\operatorname{grad}(r_2) < \operatorname{grad}(r_1)$, por lo que hacer ahora la división de r_1 por r_2 ...

De esta forma uno de los $r_i = 0$, en cuyo caso, si $r_{i-1} \neq 0$, tenemos $\mathrm{m.c.d.}\{p, q\} = r_{i-1}$, o todos los r_i son no nulos, en este caso tenemos una sucesión decreciente de números enteros positivos:

$$\operatorname{grad}(q) > \operatorname{grad}(r_1) > \operatorname{grad}(r_2) > \cdots > \operatorname{grad}(r_i) > \cdots,$$

como no existen sucesiones infinitas estrictamente decrecientes, esta posibilidad no se puede dar, y en consecuencia algún $r_i = 0$, y estamos en el caso anterior.

Para tener un método que permita calcular una expresión del máximo común divisor de p y q en función de p y q, vamos a ver como escribir cada uno de los restos en términos de p y q.

$$\begin{aligned} r_1 &= p - qc_1; \\ r_2 &= q - r_1 c_2 = q - (p - qc_1)c_2 = p(-c_2) + q(1 + c_1 c_2); \end{aligned}$$

Para averiguar los coeficientes a_{i+1}, b_{i+1} tales que $r_{i+1} = pa_{i+1} + qb_{i+1}$, si conocemos el valor de a_i, b_i y a_{i-1}, b_{i-1}, entonces

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i c_{i+1} \\ &= (pa_{i-1} + qb_{i-1}) - (pa_i + qb_i)c_{i+1} \\ &= p(a_{i-1} - a_i c_{i+1}) + q(b_{i-1} - b_i c_{i+1}) \end{aligned}$$

Como consecuencia se tiene:

$$\begin{aligned} a_{i+1} &= a_{i-1} - a_i c_{i+1} \\ b_{i+1} &= b_{i-1} - b_i c_{i+1} \end{aligned}$$

Este proceso podemos resumirlo en la siguiente tabla:

i	r_i	c_i	a_i	b_i
-1			1	0
0			0	1
1	r_1	c_1	1	$-c_1$
2	r_2	c_2	$-c_2$	$1+c_1c_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i+1$	r_{i+1}	c_{i+1}	$a_{i-1}-a_ic_{i+1}$	$b_{i-1}-b_ic_{i+1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Ejemplo. 12.20.
Calcule el m.c.d. de los polinomios $p(X)=X^3+X^2+X+1$ y $q(X)=X^3+X^2-X-1\in\mathbb{Q}[X]$.

SOLUCIÓN. Las divisiones son:

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

El máximo común divisor es $2X+2$, que es asociado a $X+1$. Luego $\mathrm{m.c.d.}\{X^3+X^2+X+1, X^3+X^2-X-1\}=X+1$.

i	r_i	c_i	a_i	b_i
-1			1	0
0			0	1
1	$2X+2$	1	1	-1
2	0	$\frac{1}{2}X^2-\frac{1}{2}$		

La expresión del m.c.d. es:

$$2X+2=(X^3+X^2+X+1)-(X^3+X^2-X-1);$$

$$X+1=\frac{1}{2}(X^3+X^2+X+1)-\frac{1}{2}(X^3+X^2-X-1).$$

□

Ejemplo. 12.21.
Calcule el m.c.d. de los polinomios $p(X)=X^4+2X^3+1$ y $q(X)=X^4-2X^2+1\in\mathbb{Q}[X]$.

SOLUCIÓN. Las divisiones son:

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

El máximo común divisor es $2X+2$, que es asociado a $X+1$. Luego $\mathrm{m.c.d.}\{X^4+2X^3+1, X^4-2X^2+1\} = X+1$.

i	r_i	c_i	a_i	b_i
-1			1	0
0			0	1
1	$2X^3+2X^2$	1	1	-1
2	$-X^2+1$	$\frac{1}{2}X-\frac{1}{2}$	$-\frac{1}{2}X+\frac{1}{2}$	$\frac{1}{2}X+\frac{1}{2}$
3	$2X+2$	$-2X-2$	$-X^2+2$	X^2+2X
0	0	$-\frac{1}{2}X+\frac{1}{2}$		

La expresión del m.c.d. es:

$$2X+2 = (X^4+2X^3+1)(-X^2+2)+(X^4-2X^2+1)(X^2+2X);$$

$$X+1 = (X^4+2X^3+1)(-\frac{1}{2}X^2+1)+(X^4-2X^2+1)(\frac{1}{2}X^2+X).$$

□

Dos polinomios $p(X)$, $q(X) \in K[X]$ se llaman **primos entre sí** si su máximo común divisor es igual a 1.

Ejemplo. 12.22.
Los polinomios $p(X) = X^3+X^2-X+1$, $q(X) = X^3-X^2-X+1 \in \mathbb{Q}[X]$ son primos relativos.

De esta forma la aritmética de los anillos de polinomios $K[X]$ con coeficientes en un cuerpo K está perfectamente determinada, es similar a la aritmética del anillo $\mathbb{Z}$ de los números enteros. Más complicado es el estudio de la aritmética de otros anillos de polinomios, como por ejemplo el anillo $\mathbb{Z}[X]$. La técnica a emplear será reducir, en parte, el estudio del anillo $\mathbb{Z}[X]$ al estudio del anillo $\mathbb{Q}[X]$ del que conocemos perfectamente su aritmética por el Corolario 12.12.

13. Raíces de polinomios

Sea A un anillo, y $p(X) \in A[X]$ un polinomio, un elemento $\alpha \in A$ se llama **raíz** ó un **cero** de $p(X)$ si $p(\alpha) = 0$. Vamos a traducir en términos de la aritmética del anillo $A[X]$ el hecho de que α sea una raíz de un polinomio $p(X)$, para ello usaremos la división de polinomios.

Lema. 13.1.
Sea A un anillo y $p(X) \in A[X]$, para cada $\alpha \in A$ existe un único polinomio $c(X) \in A[X]$ verificando: $p(X) = (X-\alpha)c(X) + p(\alpha)$.

DEMOSTRACIÓN. Aplicando el Algoritmo de Euclides a los polinomios $p(X)$ y $X-\alpha$, resulta que existen polinomios $c(X)$ y $r(X)$ tales que $p(X) = (X-\alpha)c(X)+r(X)$ y $\operatorname{grad}(r(X)) < \operatorname{grad}(X-\alpha) = 1$, luego $r(X)$ es un polinomio constante. Aplicando el homomorfismo de evaluación e_α tenemos:

$$p(\alpha) = e_\alpha(p(X)) = e_\alpha((X-\alpha)c(X) + r(X)) = (\alpha-\alpha)c(\alpha) + r(\alpha) = r(\alpha),$$

entonces tenemos el resultado $p(X) = (X-\alpha)c(X) + p(\alpha)$. □

Corolario. 13.2.
Sea A un anillo, $p(X) \in A[X]$ y $\alpha \in A$. Son equivalentes:

(a) $p(X)$ es divisible por $X-\alpha$ en $A[X]$, esto es, $X-\alpha \mid p(X)$.

(b) α es una raíz de $p(X)$.

Una generalización de este resultado es el siguiente:

Proposición. 13.3.
Sea A un DI, $p(X) \in A[X]$ y $\alpha_1, \ldots, \alpha_k \in A$ raíces de $p(X)$, distintas dos a dos, entonces $(X-\alpha_1)\ldots(X-\alpha_k) \mid p(X)$.

DEMOSTRACIÓN. Para $k = 1$ el resultado es exactamente el Corolario 13.2.. Supongamos que $k > 1$ y que el resultado sea cierto para todo conjunto de menos de k raíces. Entonces $(X-\alpha_2)\ldots(X-\alpha_k) \mid p(X)$, luego existe un polinomio $q(X)$ tal que $p(X) = (X-\alpha_2)\ldots(X-\alpha_k)q(X)$; aplicando e_{α_1} tenemos:

$$0 = p(\alpha_1) = (\alpha_1-\alpha_2)\ldots(\alpha_1-\alpha_k)q(\alpha_1),$$

y ya que $\alpha_1 \neq \alpha_i$ para $i = 2, \ldots, k$, resulta que ha de ser $q(\alpha_1) = 0$. Como consecuencia $(X-\alpha_1) \mid q(X)$ y tenemos $q(X) = (X-\alpha_1)q_0(X)$, entonces $p(X) = (X-\alpha_2)\ldots(X-\alpha_k)(X-\alpha_1)q_0(X)$, de donde deducimos que $(X-\alpha_1)\ldots(X-\alpha_k) \mid p(X)$. □

La hipótesis de ser A un DI es necesaria como prueba el siguiente Ejemplo.

Ejemplo. 13.4.
Tomamos $A = \mathbb{Z}_6$ y $p(X) = X^2 + 5X$, tenemos $p(X) = (X+3)(X+2) = X(X+5)$, entonces raíces de $p(X)$ son 0, 1, 2 y 3, sin embargo $X(X+5)(X+3)(X+2)$ no divide a $p(X)$.

Corolario. 13.5.
Sea A un DI, $p(X)$, $q(X) \in A[X]$ polinomios de grado n; si existen $n+1$ elementos distintos $\alpha_1, \ldots, \alpha_{n+1}$ tales que $p(\alpha_i) = q(\alpha_i)$, para $1 \leq i \leq n+1$, entonces $p(X) = q(X)$.

Corolario. 13.6.
Sea A un DI y $p(X) \in A[X]$; si $p(X)$ se anula en todos los elementos de un subconjunto infinito de A, entonces $p(X) = 0$.

La división de un polinomio $p(X) \in A[X]$ por un polinomio de grado uno $X - \alpha$ se puede realizar de forma sencilla a partir de la **Regla de Ruffini**. Ya que la división de $p(X)$ por $X - \alpha$ es una expresión del tipo

$$p(X) = (X - \alpha)c(X) + r(X),$$

y el resto $r(X)$ es nulo o de grado menor que uno, resulta que en este caso siempre $r(X)$ es un polinomio constante. Si $p(X) = a_n X^n + \cdots + a_1 X + a_0$, entonces podemos proceder como sigue:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
		$a_n\alpha$	$a_n\alpha^2 + a_{n-1}\alpha$	$\cdots$		
$\alpha)$						
	a_n	$a_n\alpha + a_{n-1}$	$a_n\alpha^2 + a_{n-1}\alpha + a_{n-2}$	$\cdots$	Z_1	$\vert Z_0$

Observar que el valor en Z_0 es exactamente $a_n\alpha^n + a_{n-1}\alpha^{n-1} \cdots + a_1\alpha + a_0 = p(\alpha)$, la evaluación de $p(X)$ en α, y que se tiene la división:

$$p(X) = \left[a_n X^{n-1} + (a_n\alpha + a_{n-1})X^{n-2} + (a_n\alpha^2 + a_{n-1}\alpha + a_{n-2})X^{n-3} + \cdots\right](X - \alpha) + p(\alpha).$$

El método que se obtiene para la evaluación del polinomio $p(X)$ en α a través de la Regla de Ruffini se conoce como **método de Horner** para la evaluación de polinomios, y consiste en hacer el siguiente cálculo:

$$p(\alpha) = ((\ldots(((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + a_{n-3})\ldots)\alpha + a_1)\alpha + a_0.$$

Ejemplo. 13.7.
Hacer la división de $p(X) = X^4 - 3X^3 + 5X^2 - X + 2$ por $X - 2$. En este caso se tiene:

$X^4 -3X^3 +5X^2 -X +2$	$X-2$
$-X^4 +2X^3$	X^3
$-X^3 +5X^2 -X +2$	
$X^3 -2X^2$	$-X^2$
$3X^2 -X +2$	
$-3X^2 +6X$	$3X$
$5X +2$	
$-5X +10$	5
12	

El cociente es $X^3 - X^2 + 3X + 5$, y el resto es 12.

Utilizando la Regla de Ruffini se tiene:

$$\begin{array}{cccccc} & 1 & -3 & 5 & -1 & 2 \\ & & 2 & -2 & 6 & 10 \\ \hline {\scriptstyle 2)} & 1 & -1 & 3 & 5 & \vert 12 \end{array}$$

Luego el cociente es $X^3 - X^2 + 3X + 5$, y el resto es 12.

13.1. Fórmula de interpolación de Lagrange

Sea A un DI. Vamos a determinar un polinomio $p(X) \in A[X]$ verificando que en elementos distintos $\alpha_1, \ldots, \alpha_n \in A$ tome los valores $b_1, \ldots, b_n \in A$, y cuyo grado sea como máximo $n-1$. Tal polinomio si existe es único, ya que si existen dos $p(X)$ y $q(X)$, como los grados son menores que n, y $p(X) - q(X)$ tiene n raíces, resulta que $p(X) - q(X) = 0$.

Para probar su existencia basta con definirlo. Definimos polinomios $p_i(X)$ como:

$$p_i(X) = \frac{(X-\alpha_1)\cdots(X-\alpha_{i-1})(X-\alpha_{i+1})\cdots(X-\alpha_n)}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)}$$

y finalmente $p(X)$ se define como:

$$p(X) = \sum_{i=1}^{n} b_i p_i(X) = b_1 p_1(X) + \cdots + b_n p_n(X).$$

El método de interpolación de Lagrange es un caso particular de la resolución de sistemas de congruencias, supongamos que queremos determinar un polinomio $p(X)$ tal que en el punto α_i tome el valor b_i, para $i = 1, \ldots, n$; entonces tenemos el sistema de congruencias

$$p(X) \equiv b_i \pmod{X - \alpha_i}\}_{i=1,\ldots,n}$$

El polinomio de interpolación de Lagrange $p(X)$ es entonces una solución a este sistema.

13.2. Derivada de un polinomio. Raíces múltiples

Nos encaminamos ahora a estudiar las raíces múltiples de un polinomio. Para ello vamos a introducir, de forma algebraica, la derivada de un polinomio. Sean A un DI y X, T dos indeterminadas. Para cada $p(X) \in A[X]$ consideramos el polinomio $p(X+T) \in A[X,T]$. Este

polinomio se puede escribir como un elemento de $A[X][T]$ en la forma

$$p(X+T) = p_m(X)T^m + \cdots + p_1(X)T + p_0(X),$$

con $p_i(X) \in A[X]$, $0 \leq i \leq m$.

Es inmediato comprobar que $p_0(X) = p(X)$, y que $T \mid p(X+T) - p(X)$. Definimos la **derivada formal** del polinomio $p(X)$ como el único polinomio $Dp(X) \in A[X]$ que verifica:

$$p(X+T) - p(X) \equiv Dp(X)T \pmod{T^2}.$$

Vamos a comprobar que $Dp(X)$ está determinado de forma única. Supongamos que $q(X) \in A[X]$ verifica:

$$p(X+T) - p(X) \equiv q(X)T \pmod{T^2},$$

entonces $q(X)T \equiv Dp(X)T \pmod{T^2}$, y por tanto existe un polinomio $h(X,T) \in A[X,T]$ tal que $q(X)T - Dp(X)T = T^2h(X,T)$, simplificando por T tenemos $q(X) - Dp(X) = Th(X,T)$, luego $q(X) = pD(X)$ al evaluar en $T = 0$.

Es claro de lo anterior que $Dp(X) = p_1(X) = a_1 + a_2X + \cdots + a_nX^{n-1}$.

Lema. 13.8.
Sea A un DI, la derivada define una aplicación $D : A[X] \longrightarrow A[X]$ verificando:

1. $D(p_1(X) + p_2(X)) = Dp_1(X) + Dp_2(X)$, *para* $p_1(X), p_2(X) \in A[X]$.
2. $D(ap(X)) = aDp(X)$, *para* $p(X) \in A[X]$ *y* $a \in A$.
3. $D(p_1(X)p_2(X)) = Dp_1(X)p_2(X) + p_1(X)Dp_2(X)$, *para* $p_1(X), p_2(X) \in A[X]$.

DEMOSTRACIÓN. (1) Tenemos $p_1(X+T) - p_1(X) \equiv Dp_1(X)T \pmod{T^2}$ y $p_2(X+T) - p_2(X) \equiv Dp_2(X)T \pmod{T^2}$, y sumando ambas expresiones

$$(p_1(X+T) + p_2(X+T)) - (p_1(X) + p_2(X)) \equiv (Dp_1(X) + Dp_2(X))T \pmod{T^2}.$$

Luego $D(p_1(X) + p_2(X)) = Dp_1(X) + Dp_2(X)$.
(2) Tenemos $p(X+T) - p(X) \equiv Dp(X)T \pmod{T^2}$ y multiplicando por a tenemos

$$ap(X+T) - ap(X) \equiv aDp(X)T \pmod{T^2}.$$

Luego $D(ap(X)) = aDp(X)$.
(3) Tenemos las expresiones $p_1(X+T) - p_1(X) \equiv Dp_1(X)T \pmod{T^2}$ y $p_2(X+T) - p_2(X) \equiv Dp_2(X)T \pmod{T^2}$. Multiplicando la primera por $p_2(X+T)$ y la segunda por $p_1(X)$ y sumando tenemos:

$$p_1(X+T)p_2(X+T) - p_1(X)p_2(X) \equiv$$

$$(p_2(X+T)Dp_1(X) + p_1(X)Dp_2(X))T \pmod{T^2},$$

y ya que $p_2(X+T) \equiv p_2(X) + Dp_2(X)T \pmod{T^2}$, tenemos:

$$p_1(X+T)p_2(X+T) - p_1(X)p_2(X) \equiv$$

$$(p_2(X)Dp_1(X) + p_1(X)Dp_2(X))T \pmod{T^2}.$$

Luego $D(p_1(X)p_2(X)) = p_1(X)Dp_2(X) + p_2(X)Dp_1(X)$. □

Si $p(X) \in A[X]$ y $\alpha \in A$ es una raíz de $p(X)$, llamamos **multiplicidad** de α al mayor número entero positivo k tal que $(X-\alpha)^k \mid p(X)$. Las raíces de multiplicidad uno se llaman **raíces simples**, las de multiplicidad mayor que uno se llaman **raíces múltiples**. Por extensión las raíces de multiplicidad cero no son auténticas raíces del polinomio.

Tenemos de forma inmediata que si $\alpha_1, \ldots, \alpha_r$ son raíces de $p(X)$ con multiplicidades $k_1, \ldots, k_r$, respectivamente, entonces $(X-\alpha_1)^{k_1} \cdots (X-\alpha_r)^{k_r} \mid p(X)$.

Proposición. 13.9.
Sea A un DI y $p(X) \in A[X]$ un polinomio, si $\alpha \in A$ son equivalentes:

(a) α es una raíz múltiple de $p(X)$.

(b) $p(\alpha) = Dp(\alpha) = 0$.

DEMOSTRACIÓN. (a) ⇒ (b). Sea α una raíz múltiple de $p(X)$, entonces existe $k > 1$ tal que $p(X) = (X-\alpha)^k q(X)$, para algún polinomio $q(X) \in A[X]$. Aplicando D tenemos:

$$Dp(X) = k(X-\alpha)^{k-1}q(X) + (X-\alpha)^k Dq(X),$$

y valorando en α tenemos que $Dp(\alpha) = 0$.
(b) ⇒ (a). Ya que $p(\alpha) = 0$, resulta que α es una raíz de $p(X)$, y se tiene una factorización $p(X) = (X-\alpha)q(X)$. Aplicando D tenemos:

$$Dp(X) = q(X) + (X-\alpha)Dq(X),$$

y valorando en α tenemos

$$0 = Dp(\alpha) = q(\alpha),$$

por tanto $X-\alpha \mid q(X)$, y α es una raíz múltiple de $p(X)$. □

Corolario. 13.10.
Sea A un DI, $p(X) \in A[X]$ un polinomio y $\alpha \in A$, si α es una raíz de $p(X)$ de multiplicidad $k \geq 1$, entonces $(X-\alpha)^{k-1}$ divide a $Dp(X)$.

Vamos a tratar de afinar el resultado anterior, para ello necesitamos restringir el tipo de anillos al que se va a aplicar.

Si A es un anillo, existe un único morfismo de anillos $f : \mathbb{Z} \longrightarrow A$, definido por $f(n) = n1$, para cada $n \in \mathbb{Z}$. El núcleo de f es un ideal de $\mathbb{Z}$ generado por un entero positivo ó nulo m. El entero m se llama la **característica** del anillo A. Es claro que si A es un DI, entonces la característica de A es cero ó un número primo; en este caso, el subanillo $\mathrm{Im}(f)$ se llama el **subanillo primo** de A.

Teorema. 13.11.
Sea A un DI de característica cero. Si $\alpha \in A$ es una raíz de multiplicidad $k \geq 1$ de un polinomio $p(X) \in A[X]$, entonces α es una raíz de multiplicidad exactamente $k-1$ de $Dp(X)$.

DEMOSTRACIÓN. Supongamos que $p(X) = (X-\alpha)^k q(X)$, con $q(X) \in A[X]$, $q(\alpha) \neq 0$, entonces tenemos:

$$Dp(X) = k(X-\alpha)^{k-1} q(X) + (X-\alpha)^k Dq(X) =$$

$$= (X-\alpha)^{k-1}(kq(X) + (X-\alpha)Dp(X)).$$

El segundo factor no se anula para α, luego la multiplicidad de α en $Dp(X)$ es exactamente $k-1$. □

El siguiente Ejemplo muestra que la condición de característica cero no podemos suprimirla.

Ejemplo. 13.12.
Consideramos $p(X) = X^5 + 1 \in \mathbb{Z}_5[X]$, es claro que $p(X) = (X+1)^5$, luego -1 es una raíz de multiplicidad cinco de $p(X)$. Sin embargo $Dp(X) = 0$, y el Teorema 13.11. no es aplicable.

Sin embargo, para característica distinta de cero tenemos el siguiente teorema.

Teorema. 13.13.
Sea A un DI y $p(X) \in A[X]$ un polinomio con $Dp(X) = 0$, se verifica:

1. *Si la característica de A es cero, entonces $p(X)$ es constante.*
2. *Si la característica de A es $p \neq 0$, entonces $p(X) = q(X^p)$ para algún polinomio $q(X) \in A[X]$.*

DEMOSTRACIÓN. Tenemos $Dp(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$, entonces la primera parte es inmediata. Para la segunda tenemos que $ia_i = 0$ para todo $i = 1, \ldots, n$, luego $a_i = 0$ si i no es un múltiplo de p, y por tanto el polinomio $p(X)$ tiene una expresión del tipo siguiente:

$$p(X) = a_0 + a_pX^p + a_{2p}X^{2p} + \cdots + a_{rp}X^{rp},$$

que es un polinomio del tipo indicado. □

Denotamos por D^r aplicar r veces D.

Teorema. 13.14. (Fórmula de Taylor)
Sea A un DI de característica cero, si $p(X) \in A[X]$ es un polinomio de grado n, entonces $p(X)$ tiene una expresión del tipo

$$p(X) = p(a) + \frac{Dp(a)}{1!}(X-a) + \cdots + \frac{D^np(a)}{n!}(X-a)^n,$$

para todo $a \in A$.

DEMOSTRACIÓN. Tenemos la siguiente expresión para $p(X)$:

$$p(X) = p((X-a)+a) = b_0 + b_1(X-a) + \cdots + b_n(X-a)^n.$$

Se trata entonces de determinar los coeficientes b_i. Tenemos:

$$D^r(b_i(X-a)^i) = \begin{cases} 0 & \text{si } r > i \\ i(i-1)\cdots(i-r+1)b_i(X-a)^{i-r} & \text{si } r \leq i \end{cases}$$

Por tanto, valorando en a tenemos:

$$D^r(b_i(X-a)^i)(a) = \begin{cases} 0 & \text{si } r > i \\ r!b_r & \text{si } r = i \\ 0 & \text{si } r < i \end{cases}$$

Entonces $D^rp(a) = r!b_r$ y como consecuencia podemos calcular el valor de cada b_r, esto es, $b_r = \frac{D^rp(a)}{r!}$. □

Veamos una aplicación de este último resultado.

Corolario. 13.15.
Sea A un DI de característica cero, $p(X) \in A[X]$ y $\alpha \in A$, entonces son equivalentes:

(a) α es raíz de $p(X)$ de multiplicidad $k \geq 1$.

(b) $p(\alpha) = Dp(\alpha) = \ldots = D^{k-1}p(\alpha) = 0$ y $D^kp(\alpha) \neq 0$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Tenemos $(X-\alpha)^k \mid p(X)$, luego $p(X) = (X-\alpha)^k q(X)$, siendo $q(\alpha) \neq 0$. Se tienen entonces la igualdad:

$$Dp(X) = (X-\alpha)^{k-1}(kq(X) + (X-\alpha)Dq(X)) = (X-\alpha)^{k-1}q_1(X),$$

donde $q_1(X) = kq(X) + (X-\alpha)Dq(X)$, y α no es raíz de $q_1(X)$. Si continuamos de esta forma tenemos:

$$\begin{gathered} D^2p(X) = (X-\alpha)^{k-2}((k-1)q_1(X) + (X-\alpha)Dq_1(X)) = (X-\alpha)^{k-2}q_2(X), \\ \cdots\cdots\cdots\cdots, \\ D^{k-1}p(X) = (X-\alpha)q_{k-1}(X), \\ D^kp(X) = q_k(X), \end{gathered}$$

donde los polinomios $q_2(X), \ldots, q_k(X)$ se han ido construyendo de la misma forma que $q_1(X)$, y para los cuales α no es raíz. Se tiene entonces el resultado.
(b) $\Rightarrow$ (a). Aplicando la fórmula de Taylor para $p(X)$ en $\alpha \in A$ tenemos:

$$p(X) = \frac{D^kp(\alpha)}{k!}(X-\alpha)^k + \cdots + \frac{D^np(\alpha)}{n!}(X-\alpha)^n == (X-\alpha)^kq(X),$$

donde $q(X) = \frac{D^kp(\alpha)}{k!} + \cdots + \frac{D^np(\alpha)}{n!}(X-\alpha)^{n-k} \in A[X]$ verifica $q(\alpha) \neq 0$, luego α es una raíz de exactamente multiplicidad k de $p(X)$. □

13.3. Teorema Fundamental del Álgebra

En nuestro estudio se han considerado polinomios con coeficientes sobre los conjunto de números más usuales, esto es, sobre los enteros, $\mathbb{Z}$, sobre los racionales, $\mathbb{Q}$, sobre los reales, $\mathbb{R}$ y sobre los complejos, $\mathbb{C}$. Observar que se tienen embebimientos $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, y que mientras que $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos $\mathbb{Z}$ no lo es. El caso de polinomios con coeficientes en $\mathbb{Z}$ lo estudiaremos en la Sección 14 reduciendo su estudio al caso de $\mathbb{Q}$. Queda pues por estudiar el caso de $\mathbb{C}$ y $\mathbb{R}$.

Teorema. 13.16. (Teorema Fundamental del Álgebra)
Cada polinomio no constante $p(X) \in \mathbb{C}[X]$ de grado n tiene n raíces en $\mathbb{C}$, esto es, es un producto $(X-\alpha_1)\cdots(X-\alpha_n)$ con posiblemente algún α_i repetido.

Como consecuencia de este resultado podemos dar un resultado aceptable para polinomios con coeficientes en $\mathbb{R}$.

Lema. 13.17.
Sea $p(X) \in \mathbb{R}$ un polinomio no nulo con coeficientes reales, si $\alpha \in \mathbb{C}$ es un número complejo que es raíz de $p(X)$, entonces $\overline{\alpha}$, el conjugado de α, es también raíz de $p(X)$.

DEMOSTRACIÓN. Sea $c : \mathbb{C} \longrightarrow \mathbb{C}$ la conjugación compleja, esto es, $c(a+bi) = \overline{a-bi} = a-bi$. Tenemos entonces un homomorfismo de anillos, también llamado $c : \mathbb{C}[X] \longrightarrow \mathbb{C}[X]$, definido

$$c(X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) = X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_1}X + \overline{a_0}.$$

Como $p(X)$ tiene coeficientes reales, entonces $c(p(X)) = p(X)$, y por tanto para cualquier $\beta \in \mathbb{C}$ se verifica $c(p(\beta)) = p(c(\beta))$. Si α es una raíz de $p(X)$, se verifica:

$$p(c(\alpha)) = c(p(\alpha)) = c(0) = 0,$$

luego $c(\alpha)$ es una raíz de $p(X)$. □

Lema. 13.18.
Sea $p(X) \in \mathbb{R}$ un polinomio no nulo con coeficientes reales, si $\alpha \in \mathbb{C} \setminus \mathbb{R}$ es una raíz de $p(X)$, entonces $X^2 - (\alpha + \overline{\alpha})X + \alpha\,\overline{\alpha} \in \mathbb{R}[X]$ es un factor de $p(X)$.

DEMOSTRACIÓN. Como α es una raíz de $p(X)$, también $\overline{\alpha}$ es raíz, y por lo tanto $(X-\alpha)(X-\overline{\alpha})$ es un factor de $p(X)$. Basta finalmente comprobar que se tiene un polinomio con coeficientes reales:

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\,\overline{\alpha}$$

en donde si $\alpha = a+bi$, con $a, b \in \mathbb{R}$, entonces

$$\begin{aligned} \alpha + \overline{\alpha} &= (a+bi) + (a-bi) = 2a \in \mathbb{R}, \\ \alpha\,\overline{\alpha} &= (a+bi)\,(a-bi) = a^2 + b^2 \in \mathbb{R}. \end{aligned}$$

□

Teorema. 13.19.
Sea $p(X) \in \mathbb{R}$ un polinomio no nulo con coeficientes reales, entonces $p(X)$ es un producto de polinomios de grado uno y polinomios de grado dos.

DEMOSTRACIÓN. Consideramos el polinomio $p(X)$ con coeficientes en $\mathbb{C}$, entonces $p(X)$ tiene una factorización

$$p(X) = (X-\alpha_1)\cdots(X-\alpha_n),$$

con $\alpha_i \in \mathbb{C}$. Reordenamos los α_i de forma que α_j y α_{j+1} son conjugados para $j = 1, 3, \ldots, 2h-1$ y $\alpha_{2h+1}, \alpha_{2h+2}, \ldots, \alpha_n$ son reales. La factorización anterior se puede escribir:

$$\begin{aligned} p(X) &= (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_{2h-1})(X-\alpha_{2h})(X-\alpha_{2h+1})\cdots(X-\alpha_n), \\ &= (X-\alpha_1)(X-\overline{\alpha_1})\cdots(X-\alpha_{2h-1})(X-\overline{\alpha_{2h-1}})(X-\alpha_{2h+1})\cdots(X-\alpha_n), \\ &= \textstyle\prod_{j=1}^{h}[(X-\alpha_{2j-1})(X-\overline{\alpha_{2j-1}})]\prod_{j=2h+1}^{n}(X-\alpha_j), \\ &= \textstyle\prod_{j=1}^{h}[X^2 - (\alpha_{2j-1}+\overline{\alpha_{2j-1}})X + \alpha_{2j-1}\,\overline{\alpha_{2j-1}}]\prod_{j=2h+1}^{n}(X-\alpha_j). \end{aligned}$$

□

14. Polinomios con coeficientes en $\mathbb{Z}$

El estudio de polinomios con coeficientes en $\mathbb{Q}$ no es fácil. Aunque sabemos que $\mathbb{Q}[X]$ es un dominio euclídeo, el cálculo de las factorizaciones posibles de polinomios es un problema de difícil solución si nos limitamos a trabajar solamente en $\mathbb{Q}[X]$. Por esta razón, vamos a hacer uso de la inclusión $\mathbb{Z} \subseteq \mathbb{Q}$, y de la inclusión que ésta induce entre los anillos de polinomios. Veremos que el estudio de los polinomios en $\mathbb{Z}[X]$ cuenta con herramientas adicionales y veremos cómo aplicar este estudio al estudio de las factorizaciones de polinomios en $\mathbb{Q}[X]$.

Sea $p(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, definimos el **contenido** de $p(X)$ como

$$c(p(X)) = \text{m. c. d.}\{a_n, \ldots, a_1, a_0\}.$$

Un polinomio $p(X)$ se llama **primitivo** si $c(p(X)) = 1$.

Lema. 14.1.
Sea $p(X) \in \mathbb{Z}[X]$ un polinomio no constante, entonces existe un polinomio primitivo $q(X) \in \mathbb{Z}[X]$ tal que $p(X) = cq(X)$, donde $c = c(p(X))$.
Esta descomposición es única en el siguiente sentido: Si además $p(X) = c'q'(X)$, con $q'(X) \in \mathbb{Z}[X]$ primitivo y $c' \in \mathbb{Z}$, entonces c y c' son asociados en $\mathbb{Z}$ y $q(X)$ y $q'(X)$ son asociados en $\mathbb{Z}[X]$.

Teorema. 14.2. (Lema de Gauss)
El producto en $\mathbb{Z}[X]$ de dos polinomios primitivos es un polinomio primitivo.

DEMOSTRACIÓN. Supongamos que $p(X)$ y $q(X)$ son polinomios primitivos; si $p(X)q(X)$ no es un polinomio primitivo, entonces existe un elemento primo, $d \in \mathbb{Z}$ tal que d divide a todos los coeficientes de $p(X)q(X)$. Sabemos que existen coeficientes de $p(X)q(X)$ que no son múltiplos de d, sean a_s y b_r los coeficientes con subíndice menor que no son múltiplos de d. El coeficiente de X^{s+r} en $p(X)q(X)$ es:

$$a_0 b_{s+r} + \cdots + a_{s-1} b_{r+1} + a_s b_r + a_{s+1} b_{r-1} + \cdots + a_{s+r} b_0$$

que es un múltiplo de d, así como todos los sumandos salvo posiblemente $a_s b_r$. Por tanto d también divide a $a_s b_r$, de donde se deduce que $d \mid a_s$ ó $d \mid b_r$, lo que es una contradicción. □

Corolario. 14.3.
Para cada par de polinomios $p(X)$, $p'(X) \in \mathbb{Z}[X]$ se verifica:

$$c(p(X)p'(X)) \sim c(p(X))c(p'(X)).$$

DEMOSTRACIÓN. Tenemos que $p(X) = cq(X)$ y $p'(X) = c'q'(X)$ con $c = c(p(X))$, $c' = c(p'(X))$ y $q(X)$, $q'(X)$ primitivos. Entonces tenemos $p(X)p'(X) = cc'q(X)q'(X)$ con $q(X)q'(X)$ un polinomio primitivo, por tanto

$$c(p(X)p'(X)) \sim cc' = c(p(X))c(p'(X)).$$

□

Asociamos a cada polinomio no constante con coeficientes en $\mathbb{Q}$ un único polinomio primitivo en $\mathbb{Z}[X]$.

Proposición. 14.4.
Si $q(X) \in \mathbb{Q}[X]$ es un polinomio no constante, entonces existen $a, b \in \mathbb{Z}$ verificando que $q(X) = ab^{-1}p(X)$ con $p(X) \in \mathbb{Z}[X]$ un polinomio primitivo. Además $p(X)$ está unívocamente determinado salvo asociados (unidades de $\mathbb{Z}$).

DEMOSTRACIÓN. Ya que $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$, tenemos

$$p(X) = (a_0 b_0^{-1}) + (a_1 b_1^{-1})X + \cdots + (a_n b_n^{-1})X^n$$

para a_i, $b_i \in \mathbb{Z}$. Podemos tomar $b = \text{m.c.m.}\{b_0, \ldots, b_n\}$, entonces $b \neq 0$, y todos los coeficientes del polinomio $bp(X)$ pertenecen a $\mathbb{Z}$, luego $bp(X) \in \mathbb{Z}[X]$. Además, ya que $p(X)$ no es constante, tampoco $bp(X)$ lo es. Calculamos el contenido de $bp(X)$ y lo llamamos a, entonces $bp(X) = aq(X)$ con $q(X)$ un polinomio primitivo en $\mathbb{Z}[X]$. Por tanto $p(X) = ab^{-1}q(X)$. Para estudiar la unicidad, supongamos que $p(X) = ab^{-1}q(X) = cd^{-1}q'(X)$ con $a, b, c, d \in \mathbb{Z}$ y $q(X)$, $q'(X)$ polinomios primitivos en $\mathbb{Z}[X]$. Entonces $adq(X) = cbq'(X)$, y por ser $q(X)$ y $q'(X)$ primitivos resulta que ad y cb son asociados, luego $q(X)$ y $q'(X)$ son también asociados. □

Lema. 14.5.
Si $p(X) \in \mathbb{Z}[X]$ es un polinomio primitivo y para $a, b \in \mathbb{Z}$ el polinomio $ab^{-1}p(X)$ tiene todos sus coeficientes en $\mathbb{Z}$, entonces $b \mid a$.

DEMOSTRACIÓN. Ya que $ab^{-1}p(X) \in \mathbb{Z}[X]$, podemos escribirlo en la forma $cq(X)$, con $c = c(ab^{-1}p(X))$ y $q(X)$ un polinomio primitivo en $\mathbb{Z}[X]$. Entonces $ap(X) = bcq(X)$, de donde se deduce que a y bc son asociados, luego $b \mid a$. □

14.1. Polinomios irreducibles

Un polinomio $p(X)$ con coeficientes en $\mathbb{Z}$, es **irreducible** (en $\mathbb{Z}[X]$) si no existen polinomios (que no son unidades) $p_1(X)$, $p_2(X) \in \mathbb{Z}[X]$ tales que $p(X) = p_1(X)p_2(X)$.

Es claro que los únicos elementos irreducibles en $\mathbb{Z}[X]$ son los elementos primos de $\mathbb{Z}$ y los polinomios primitivos irreducibles no constantes. Por otro lado todo polinomio no constante e irreducible $p(X) \in \mathbb{Z}[X]$ es un polinomio primitivo, ya que en caso contrario tendríamos una factorización propia $p(X) = c(p(X))q(X)$ con $q(X)$ un polinomio primitivo en $\mathbb{Z}[X]$.

La misma definición es posible hacerla sobre cualquier otro anillo de polinomios.

Vamos a relacionar las polinomios irreducibles en $\mathbb{Z}[X]$ con polinomios irreducibles en $\mathbb{Q}[Z]$.

Teorema. 14.6.
Si $p(X) \in \mathbb{Z}[X]$ es un polinomio no constante e irreducible, entonces $p(X) \in \mathbb{Q}[X]$ es irreducible.

DEMOSTRACIÓN. Sea $p(X) \in \mathbb{Z}[X]$ un polinomio no constante e irreducible. Si $p(X) = p_1(X)p_2(X)$ es un factorización propia en $\mathbb{Q}[X]$ con los $p_i(X)$ no unidades. Entonces existen polinomios primitivos $q_i(X) \in \mathbb{Z}[X]$ y elementos $a, b, c, d \in \mathbb{Z}$ tales que $p_1(X) = ab^{-1}q_1(X)$ y $p_2(X) = cd^{-1}q_2(X)$. Por tanto tenemos

$$p(X) = ac(bd)^{-1}q_1(X)q_2(X)$$

y

$$bdp(X) = acq_1(X)q_2(X) \in \mathbb{Z}[X].$$

Como $p(X)$, $q_1(X)$ y $q_2(X)$ son polinomios primitivos, tenemos que $p(X)$ y $q_1(X)q_2(X)$ son asociados en $\mathbb{Z}[X]$, y por ser $p(X)$ irreducible, resulta que $q_1(X)$ ó $q_2(X)$ es una unidad, luego un polinomio constante, lo que es una contradicción. □

El resultado recíproco es el siguiente:

Proposición. 14.7.
Si $q(X) \in \mathbb{Q}[X]$ es un polinomio no constante e irreducible, tal que $q(X) = ab^{-1}p(X)$ con $a, b \in \mathbb{Z}$ y $p(X) \in \mathbb{Z}[X]$ primitivo, entonces $p(X)$ es irreducible.

Como consecuencia el estudio de los polinomios irreducibles en $\mathbb{Q}[X]$ lo reducimos al estudio de los polinomios irreducibles en $\mathbb{Z}[X]$.

15. Criterios de irreducibilidad de polinomios

Veamos algunos criterios de irreducibilidad de polinomios en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$.

Observar que si un polinomio $p(X)$ tiene una raíz α en $\mathbb{Z}$, entonces tiene un factor de grado uno $(X-\alpha)$, y por tanto si su grado es mayor que uno es un polinomio reducible en $\mathbb{Z}[X]$. El recíproco es cierto para polinomios de grado dos o tres, y no es cierto para polinomios de grado cuatro o superior.

Como consecuencia para estudiar la reducibilidad de un polinomio lo primero que hay que hacer es estudiar si tiene ó no raíces.

Vamos a ver algoritmos que nos permitan calcular las raíces racionales de polinomios con coeficientes enteros.

Lema. 15.1.
Si $a, b \in \mathbb{Z}$ son primos relativos, $b \neq 0$ y ab^{-1} es una raíz del polinomio $p(X) = a_0 + \cdots + a_n X^n \in A[X]$, entonces $a \mid a_0$ y $b \mid a_n$.

DEMOSTRACIÓN. Si ab^{-1} es una raíz de $p(X)$, entonces se verifica:

$$0 = p(ab^{-1}) = a_0 + a_1(ab^{-1}) + \cdots + a_n(ab^{-1})^n.$$

Multiplicando por b^n resulta

$$a_0 b^n + a_1 ab^{n-1} + \cdots + a_n a^n = 0,$$

entonces b divide a a_n y a divide a a_0. □

Otro criterio de irreducibilidad es el siguiente:

Teorema. 15.2. (Criterio de irreducibilidad por reducción)
Sea $f : \mathbb{Z} \to \mathbb{Z}_p$ el homomorfismo canónico anillos. Si $p(X) \in \mathbb{Z}[X]$ verifica que $\operatorname{grad}(f(p(X))) = \operatorname{grad}(p(X))$ y $f(p(X))$ es irreducible en $\mathbb{Z}_p[X]$, entonces $p(X)$ no se escribe como un producto de dos polinomios no constantes de $\mathbb{Z}[X]$, por lo tanto si es primitivo es irreducible.

DEMOSTRACIÓN. Supongamos que $p(X)$ admite una descomposición en $\mathbb{Z}[X]$ como producto de polinomios no constantes

$$p(X) = p_1(X)p_2(X).$$

Aplicando f tenemos:

$$f(p(X)) = f(p_1(X)p_2(X)) = f(p_1(X))f(p_2(X)).$$

Ya que $\mathrm{grad}(p(X)) = \mathrm{grad}(f(p(X))$, resulta que $\mathrm{grad}(p_1(X)) = \mathrm{grad}(f(p_i(X)))$, para $i = 1, 2$. Luego $f(p(X))$ no es irreducible en $\mathbb{Z}_p[X]$. □

Veamos a continuación algunas aplicaciones de este último criterio.

Ejemplo. 15.3.
El polinomio $p(X) = X^3 + X^2 + 15$ es irreducible en $\mathbb{Z}[X]$.

Consideramos la proyección canónica $\mathbb{Z} \to \mathbb{Z}_2$ y el homomorfismo inducido entre los anillos de polinomios $f : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$. Entonces $f(p(X)) = X^3 + X^2 + 1$, ya que $f(p(X))$ es irreducible en $\mathbb{Z}_2[X]$, resulta que $p(X)$ no puede descomponerse en $\mathbb{Z}[X]$.

Este método de reducción puede aplicarse en un sentido diferente para determinar la reducibilidad o irreducibilidad de polinomios.

Ejemplo. 15.4.
El polinomio $p(X) = X^4 + 2X^3 + 7X^2 - 4X + 5$ es irreducible en $\mathbb{Z}[X]$.

Consideramos la proyección canónica $\mathbb{Z} \to \mathbb{Z}_2$ y el homomorfismo inducido entre los anillos de polinomios $f : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$. Entonces $f(p(X)) = X^4 + X^2 + 1$, que admite la descomposición $(X^2 + X + 1)^2$, luego no es irreducible en $\mathbb{Z}_2[X]$. Consideramos la proyección canónica $\mathbb{Z} \to \mathbb{Z}_3$ y el homomorfismo inducido entre los anillos de polinomios $g : \mathbb{Z}[X] \to \mathbb{Z}_3[X]$. Entonces $g(p(X)) = X^4 + 2X^3 + X^2 + 2X + 2)$, que admite la descomposición $(X+1)(X^3 + X^2 + 2)$, luego no es irreducible en $\mathbb{Z}_3[X]$. Uniendo los dos resultados obtenidos tenemos que $p(X)$ es irreducible en $\mathbb{Z}[X]$. Ya que una posible descomposición en irreducibles en $\mathbb{Z}[X]$ induce una descomposición en $\mathbb{Z}_2[X]$, con lo cual la descomposición en $\mathbb{Z}[X]$ sería en producto de dos polinomios de grado dos. Y esa misma descomposición induce en $\mathbb{Z}_3[X]$ una descomposición en producto de polinomios de grado como máximo dos, lo que es una contradicción con la descomposición que hemos hallado en $\mathbb{Z}_3[X]$ como un producto de un polinomio de grado uno y un polinomio de grado tres.

Teorema. 15.5. (Criterio de irreducibilidad de Eisenstein)
Si $p(X) \in \mathbb{Z}[X]$ es no constante y existe un elemento primo $d \in \mathbb{Z}$ verificando:
$d \nmid a_n$,
$d^2 \nmid a_0$ *y*
$d \mid a_i$, $0 \leq i \leq n-1$,
entonces $p(X)$ es irreducible en $\mathbb{Q}[X]$. Además si $p(X)$ es primitivo en $\mathbb{Z}[X]$, entonces también es irreducible en $\mathbb{Z}[X]$.

DEMOSTRACIÓN. Supongamos que $p(X) \in \mathbb{Q}[X]$ es reducible, entonces

$$p(X) = p_1(X)p_2(X)$$

con $p_1(X)$, $p_2(X) \in \mathbb{Q}[X]$ no unidades (no constantes). Existen elementos $a, b, c, e \in \mathbb{Z}$ y $q_1(X)$, $q_2(X)$ polinomios primitivos en $\mathbb{Z}[X]$ tales que

$$p_1(X) = ab^{-1}q_1(X) \qquad p_2(X) = ce^{-1}q_2(X),$$

Tenemos por tanto

$$bep(X) = acq_1(X)q_2(X).$$

Simplificando por los factores comunes de be y ac podemos suponer que son primos relativos. Ya que $d \nmid a_n$, si $d \mid be$ entonces $d \mid c((ac)q_1(X)q_2(X)) = ac$, lo que es una contradicción, entonces $d \nmid be$. Por otro lado, si $d \mid ac$, entonces $d \mid c(p(X))$, y por tanto $d \mid a_n$, lo que es una contradicción. Supongamos que

$$q_1(X) = c_rX^r + \cdots + c_0, \quad c_r \neq 0, 1 \leq r < n,$$

$$q_2(X) = d_sX^s + \cdots + d_0, \quad d_s \neq 0, l \leq s < n,$$

entonces de $d \mid a_0$ y $d^2 \nmid a_0$ deducimos que d ó divide a c_0 ó a d_0 (solamente a uno de los dos). Supongamos que $d \mid d_0$ y $d \nmid c_0$. Ya que d no divide a todos los coeficientes de $q_2(X)$, por ser éste un polinomio primitivo, resulta que podemos encontrar un índice t tal que $d \nmid d_t$ y $d \mid d_j$ para todo $j \leq t$. Si consideramos ahora el coeficiente de índice t de $bep(X)$, resulta

$$bea_t = (ac)(c_0d_t + c_1d_{t-1} + \cdots + c_td_0).$$

Como $d \mid a_t$ entonces divide a la suma (por ser $t \leq s < n$), también divide a todos los sumandos menos al primero c_0d_t, lo que es una contradicción. Como consecuencia $p(X)$ es un polinomio irreducible en $\mathbb{Q}[X]$. El resto se sigue de forma sencilla. □

Ejemplo. 15.6.
El polinomio $X^4+16X^3+8X^2+4X+2$ es irreducible en $\mathbb{Z}[X]$, y por tanto en $\mathbb{Q}[X]$, y el polinomio $3^4 + 48X^3 + 24X^2 + 12X + 6$ es irreducible en $\mathbb{Q}[X]$, y como no es primitivo no es irreducible en $\mathbb{Z}[X]$.

Ejercicio. 15.7.
Demuestre que el polinomio $p(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ *es irreducible en* $\mathbb{Z}[X]$.

SOLUCIÓN. A priori no podemos aplicar ningún criterio de irreducibilidad de los estudiados. Vamos a hacer un pequeño cambio en el polinomio que nos permita aplicar el criterio de irreducibilidad de Eisenstein.

Hacemos el desarrollo de Taylor para $a = 1$. Los cálculos necesarios son:

$$\begin{array}{ll}
p(X) = \sum_{i=0}^{6} X^i; & p(1) = 7 \\
Dp(X) = \sum_{i=0}^{6} iX^{i-1} = 6X^5 + 5X^4 + 4X^3 + 3X^2 + 2X + 1 & Dp(1) = 21 \\
D^2p(X) = \sum_{i=0}^{6} i(i-1)X^{i-2} = 30X^4 + 20X^3 + 12X^2 + 6X + 2 & D^2p(1) = 70 \\
D^3p(X) = \sum_{i=0}^{6} i(i-1)(i-2)X^{i-3} = 120X^3 + 60X^2 + 24X + 6 & D^3p(1) = 210 \\
D^4p(X) = \sum_{i=0}^{6} i(i-1)(i-2)(i-3)X^{i-4} = 360X^2 + 120X + 24 & D^4p(1) = 504 \\
D^5p(X) = \sum_{i=0}^{6} i(i-1)(i-2)(i-3)(i-4)X^{i-5} = 720X + 120 & D^5p(1) = 840 \\
D^6p(X) = \sum_{i=0}^{6} i(i-1)(i-2)(i-3)(i-4)(i-5)X^{i-6} = 720 & D^6p(1) = 720
\end{array}$$

$$\begin{aligned}
p(X) &= \sum_{i=0}^{6} \frac{D^i p(1)}{i!}(X-1)^i \\
&= 7 + 21(X-1) + \frac{70}{2}(X-1)^2 + \frac{210}{6}(X-1)^3 + \frac{504}{24}(X-1)^4 + \frac{840}{120}(X-1)^5 + \frac{720}{720}(X-1)^6 \\
&= 7 + 21(X-1) + 35(X-1)^2 + 35(X-1)^3 + 21(X-1)^4 + 7(X-1)^5 + (X-1)^6
\end{aligned}$$

Definimos un homomorfismo de anillos $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[Y]$ mediante $\varphi : X \mapsto Y + 1$. Como existe inverso φ^{-1}, definido por $\varphi^{-1} : Y \mapsto X - 1$, entonces φ es un isomorfismo de anillos. En consecuencia un polinomio $q(X) \in \mathbb{Z}[X]$ es irreducible si y solo si $\varphi(p(X))$ es irreducible en $\mathbb{Z}[X]$. La imagen de

$$\begin{aligned}
p(X) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
&= 7 + 21(X-1) + 35(X-1)^2 + 35(X-1)^3 + 21(X-1)^4 + 7(X-1)^5 + (X-1)^6
\end{aligned}$$

es

$$\varphi(p(X)) = 7 + 21Y + 35Y^2 + 35Y^3 + 21Y^4 + 7Y^5 + Y^6,$$

que por el criterio de Eisenstein, para el entero primo positivo 7, es un polinomio irreducible en $\mathbb{Q}[X]$ y, por ser primitivo, también en $\mathbb{Z}[X]$. Luego el polinomio $p(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ es irreducible en $\mathbb{Z}[X]$. □

El resultado anterior se puede generalizar en el siguiente sentido:

Ejercicio. 15.8.
Demuestre que si q es u entero primo positivo el polinomio $p(X) = X^{q-1} + X^{q-2} + \cdots + X^3 + X^2 + X + 1$ es irreducible en $\mathbb{Z}[X]$.

SOLUCIÓN. Observar que $(X-1)p(X) = X^q - 1$. Si llamamos $h(X) = X^q - 1$, vamos a aplicar el mismo resultado del desarrollo de Taylor a $h(X)$. Primero observar que para $i \geq 1$ se tiene:

$D^i h(X) = q(q-1)\cdots(q-i+1)X^{q-i}$. El desarrollo buscado es:

$$\begin{aligned}
&(X-1)p(X) = h(X)\\
&= \textstyle\sum_{i=0}^{q} \frac{D^i p(1)}{i!}(X-1)^i\\
&= \textstyle\sum_{i=1}^{q} \frac{q(q-1)\cdots(q-i+1)}{i!}(X-1)^i\\
&= (X-1)\textstyle\sum_{i=1}^{q} \frac{q(q-1)\cdots(q-i+1)}{i!}(X-1)^{i-1}\\
&= (X-1)\textstyle\sum_{j=0}^{q-1} \frac{q(q-1)\cdots(q-j)}{(j+1)!}(X-1)^j\\
&= (X-1)\textstyle\sum_{j=0}^{q-1} \binom{q}{j+1}(X-1)^j.
\end{aligned}$$

Entonces

$$p(X) = \textstyle\sum_{j=0}^{q-1} \binom{q}{j+1}(X-1)^j$$

Para el cambio $X \mapsto Y+1$ tenemos el polinomio

$$\sum_{j=0}^{q-1} \binom{q}{j+1} Y^j = \binom{q}{1} + \binom{q}{2} Y + \binom{q}{3} Y^2 + \cdots + \binom{q}{q-1} Y^{q-2} + \binom{q}{q} Y^{q-1}$$

Para cada $j+1 = 0, 1, \ldots, q-2$ se tiene que q divide a $\binom{q}{j+1}$, luego q divide a cada coeficiente menos al líder. Además el término independiente de este polinomio es $\binom{q}{1} = q$ y no es múltiplo de q^2. Entonces por el criterio de Eisenstein resulta que el polinomio $\sum_{j=0}^{q-1} \binom{q}{j+1} Y^j$ es irreducible, y en consecuencia también lo es el polinomio $p(X)$. □

15.1. Criterio de descomposición

Hasta ahora hemos tratado de determinar si un polinomio $p(X) \in \mathbb{Z}[X]$ es o no irreducible. Vamos ahora a tratar de encontrar, cuando es no constante, mónico y reducible, una descomposición en producto de polinomios no constantes.

En general los métodos de descomposición son más complicados que los criterios de irreducibilidad. Sin embargo, vamos a estudiar el **método de descomposición de Kronecker** que es particularmente sencillo cuando se aplica a polinomios, con coeficientes no excesivamente grandes, en el anillo $\mathbb{Z}[X]$.

Consideramos $p(X) \in \mathbb{Z}[X]$, un polinomio mónico no constante de grado n. Si $p(X)$ admite una factorización $p(X) = p_1(X)p_2(X)$ en $\mathbb{Z}[X]$, entonces, por ejemplo, $grad(p_1(X)) \leq n/2$. Llamemos s a la parte entera de $n/2$. Si tomamos $s+1$ elementos distintos $a_0, \ldots, a_s$ de $\mathbb{Z}$, al valorar $p(X)$ en a_i tenemos:

$$p(a_i) = p_1(a_i)p_2(a_i), \quad 0 \leq i \leq s.$$

Luego $p_1(a_i)$ es un divisor de $p(a_i)$, y como $p(a_i)$ tiene un número finito de divisores, resulta que cada $p_1(a_i)$ toma valores en un conjunto finito. Por la fórmula de interpolación de Lagrange, existe un único polinomio $q(X)$ de grado menor ó igual que s tal que $q(a_i) = p_1(a_i)$, $0 \leq i \leq s$, entonces $q(X) = p_1(X)$ y tendríamos de esta forma determinado un factor de $p(X)$.

Si no conocemos previamente la factorización de $p(X)$, consideramos todas las posibles elecciones de colecciones $d_0, \ldots, d_s$ con $d_i \mid p(a_i)$, $0 \leq i \leq s$. Al calcular en cada caso el polinomio de interpolación de Lagrange, $q(X)$, tal que $q(a_i) = d_i$, $0 \leq i \leq s$, si $p(X)$ es reducible, alguno de estos polinomios debe ser un factor de $p(X)$; y por el contrario si es irreducible evidentemente ninguno de ellos lo es.

Ejemplo. 15.9.
Estudiar si es reducible en $\mathbb{Z}[X]$ el polinomio $p(X) = X^7 - 2X^6 + 3X^5 - 2X^3 + 6X^2 - 4X + 4$ y, si lo es, encontrar una descomposición en irreducibles.

Ya que el grado es siete, resulta que $s = 3$. Consideramos esta vez, de forma excepcional, tres elementos de $\mathbb{Z}$: $a_0 = -1$, $a_1 = 0$, $a_2 = 1$.

Valoramos $p(X)$ en a_i obteniendo: $p(a_0) = 10$, $p(a_1) = 4$, $p(a_2) = 6$.

Consideremos los divisores $d_0 = 2$, $d_1 = 1$, $d_2 = 2$.

Construimos el polinomio de interpolación de Lagrange

$$q(X) = 2\frac{X(X-1)}{(-1-0)(-1-1)} + 1\frac{(X+1)(X-1)}{(0+1)(0-1)} + 2\frac{(X+1)X}{(1+1)(1-0)} = X^2 + 1.$$

Y resulta que $X^2 + 1$ es irreducible y es un divisor de $p(X)$:

$$p(X) = (X^2 + 1)(X^5 - 2X^4 + 2X^3 + 2X^2 - 4X + 4)$$

Estudiamos ahora el polinomio $p_2(X) = X^5 - 2X^4 + 2X^3 + 2X^2 - 4X + 4$. Ya que su grado es cinco, resulta que $s = 2$. Consideramos tres elementos de $\mathbb{Z}$: $a_0 = -1$, $a_1 = 0$, $a_2 = 1$.

Valoramos $p_2(X)$ en a_i obteniendo: $p_2(a_0) = 5$, $p_2(a_1) = 4$, $p_2(a_2) = 3$.

Consideremos los divisores $d_0 = 5$, $d_1 = 2$, $d_2 = 1$.

Construimos el polinomio de interpolación de Lagrange

$$q(X) = 5\frac{X(X-1)}{(-1-0)(-1-1)} + 2\frac{(X+1)(X-1)}{(0+1)(0-1)} + 1\frac{(X+1)X}{(1+1)(1-0)} =$$

$$= \frac{5}{2}X(X-1) - 2(x^2-1) + \frac{1}{2}(X^2+X) =$$

$$= \frac{1}{2}(2X^2 - 4X + 4) = X^2 - 2X + 2.$$

Y resulta que $X^2 - 2X + 2$ es irreducible y es un divisor de $p_2(X)$:

$$p_2(X) = (X^2 - 2X + 2)(X^3 + 2).$$

Ya que el otro factor es irreducible, resulta que hemos obtenido una descomposición en irreducibles de $p(X)$ en la siguiente forma:

$$p(X) = (X^2 + 1)(X^2 - 2X + 2)(X^3 + 2).$$

Es conveniente destacar que en el anterior ejemplo en el primer paso hemos tomado menos elementos a_i de lo que indicaba el número s, esto puede ser arriesgado en casos generales, ya que estamos descartando a priori posibles factores de $p(X)$ de grado tres.

Capítulo IV

Conjuntos ordenados. Retículos

16. Relaciones de orden

Sea X un conjunto, una relación de orden en X es una relación R verificando las propiedades:

Propiedad reflexiva. $\forall x \in X,\ xRx$.

Propiedad antisimétrica. Si xRy e yRx, entonces $x = y$.

Propiedad transitiva. Si xRy e yRz, entonces xRz.

La forma usual de representar una relación de orden es mediante el símbolo $\leq$, o también por $\preccurlyeq$ y otros.

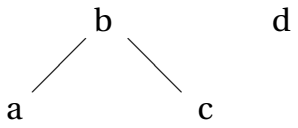
El par $(X, \leq)$, formado por un conjunto X y una relación de orden $\leq$ en X, se llama un **orden parcial** o también un **conjunto parcialmente ordenado**. Si se sobreentiende la relación de orden $\leq$, decimos simplemente que X es un conjunto parcialmente ordenado.

Ejemplo. 16.1.
Sea $X = \{a, b, c\}$ y se considera la relación de orden en X, definida por:

$$a \leq a, \quad a \leq b, \quad b \leq b, \quad c \leq b, \quad c \leq c.$$

Con esta relación tenemos que X es un conjunto parcialmente ordenado.

Una forma gráfica de representar este conjunto parcialmente ordenado es mediante un diagrama (**diagrama de Hasse**) como el de la siguiente figura:



en donde un nivel inferior y una línea entre ellos indican prelación entre los elementos.

16.1. Órdenes totales

Un conjunto parcialmente ordenado $(X, \leq)$ se llama un **orden total** o también un **conjunto totalmente ordenado**, si para cada par de elementos x_1, x_2 de X se tiene:

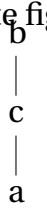
$$x_1 \leq x_2 \quad \text{ó} \quad x_2 \leq x_1.$$

Ejemplo. 16.2.
Sea $X = \{a, b, c\}$ y se considera la relación de orden en X, definida por:

$$a \leq a, \quad a \leq b, \quad a \leq c, \quad b \leq b, \quad c \leq b, \quad c \leq c.$$

Con esta relación tenemos que X es un conjunto totalmente ordenado.

Una forma gráfica de representar este conjunto totalmente ordenado es mediante el diagrama de Hasse que aparece en la siguiente figura:



16.2. Elementos notables de un conjunto ordenado

Sea X un conjunto parcialmente ordenado con relación de orden $\leq$.

Dado un subconjunto $A \subseteq X$, un elemento $x \in X$ se llama una **cota superior** de A si para cada elemento $a \in A$ se tiene $a \leq x$. Un elemento $a \in A$ que es una cota superior se llama un **máximo** de A. Si $A = \varnothing$, decimos que el conjunto de las cotas superiores de A es vacío.

Las nociones duales son **cota inferior** y **mínimo**.

Lema. 16.3.
Si A es un subconjunto no vacío de un conjunto parcialmente ordenado X, entonces existe a lo más un máximo de A (¡puede no existir máximo!).

El máximo de A se representa por $\max(A)$ y el mínimo de A se representa por $\min(A)$.

Una cota superior que es un mínimo del conjunto de las cotas superiores de A se llama un **supremo** de A. La noción dual es la de **ínfimo**.

Lema. 16.4.
Si A es un subconjunto no vacío de un conjunto parcialmente ordenado X, entonces existe a lo más un supremo de A (¡puede no existir supremo!).

El supremo de A se representa por $\sup(A)$ y el ínfimo de A se representa por $\inf(A)$.

Ejemplo. 16.5.
Consideramos el conjunto $\mathbb{R}$ de los números reales con la relación de orden usual y los subconjuntos

$A = [0,1]$,
$B = [0,1)$,
$C = \{\text{números reales positivos}\}$.

Entonces $\sup(A) = 1 = \sup(A)$ y todos los números reales positivos mayores o iguales que 1 se cotas superiores. Se verifica que $\max(A) = 1$ y no existe el máximo de B.

El conjunto C no tiene cotas superiores, luego no tiene máximo ni supremo.

Sea X un conjunto parcialmente ordenado y $A \subseteq X$ un subconjunto no vacío. Un elemento $m \in A$ se llama **maximal** si no existe ningún elemento $a \in A$ tal que $m \leq a$ y $m \neq a$. (En lo que sigue escribimos estas dos condiciones simplemente como $<$.)

La noción dual es la de **elemento minimal**.

Lema. 16.6.
Cada conjunto finito, no vacío, parcialmente ordenado tiene un elemento maximal.

DEMOSTRACIÓN. Sea X un conjunto finito no vacío parcialmente ordenado. Tomamos $x_0 \in X$. Si x_0 es un elemento maximal, entonces ya tenemos un elemento maximal en X. En caso contrario existe un elemento $x_1 \in X$ tal que $x_0 < x_1$. Si x_1 es un elemento maximal, entonces ya tenemos un elemento maximal en X. En caso contrario existe $x_2 \in X$ tal que $x_1 < x_2$. De esta forma, si no encontrásemos un elemento maximal, construiríamos una sucesión $x_0, x_1, \ldots$, de elementos distintos dos a dos; como X es finito, esta sucesión debe tener como máximo tantos elementos como tiene X, en cualquier caso es una sucesión finita y el último elemento será un elemento maximal de X. □

16.3. Conjuntos bien ordenados

Un subconjunto parcialmente ordenado X con relación de orden $\leq$, se llama **bien ordenado** si cada subconjunto no vacío tiene un **primer elemento** (=mínimo). También se dice que $\leq$ es un **buen orden**.

En consecuencia todo conjunto bien ordenado es un orden total.

Ejemplo. 16.7.
El conjunto $\mathbb{N}$ de los números naturales es un conjunto bien ordenado, en cambio $\mathbb{Z}$ no lo es y tampoco lo es $\mathbb{R}$.

De particular importancia son los conjuntos finitos parcialmente ordenados. Primero observamos el siguiente resultado:

Proposición. 16.8.
Todo conjunto finito, no vacío, totalmente ordenado es bien ordenado.

DEMOSTRACIÓN. Si X es un conjunto finito no vacío totalmente ordenado e $Y \subseteq X$ es un subconjunto no vacío, sea $Y = \{y_1, \ldots, y_t\}$. Procedemos como sigue:

(1) se ordenan en una lista los elementos de Y, por ejemplo $y_1, y_2, \ldots, y_t$,

(2) se compara y_1 con y_2. Si $y_1 \leq y_2$, entonces se mantiene el orden de la lista, si $y_2 \leq y_1$, se permutan y_1 e y_2, obteniendo así una nueva lista.

(3) se compara el primer elemento y de la lista obtenida en el paso (2) con el elemento y_3, si $y \leq y_3$ se mantiene el orden de la lista, si $y_3 \leq y$, se permutan y e y_3, obteniendo así una nueva lista.

(i) ($3 < i \leq t$). se compara el primer elemento y de la lista obtenida en el paso $(i-1)$ con el elemento y_i, si $y \leq y_i$ se mantiene el orden de la lista, si $y_i \leq y$, se permutan y e y_i, obteniendo así una nueva lista.

($t+1$) el primer elemento de la lista obtenida en el paso $(t-1)$ es el mínimo de Y.

□

16.4. Inducción de órdenes

Si X es un conjunto parcialmente ordenado, con relación de orden $\leq_X$, e Y es un subconjunto de X, entonces podemos definir en Y una relación de orden mediante

$$y_1 \leq_Y y_2 \quad \text{si} \quad y_1 \leq_X y_2 \quad \text{en } X.$$

Decimos que el orden $\leq_Y$ es el **orden inducido** en Y por el orden $\leq_X$.

Aplicación.
Suponemos que tenemos un conjunto parcialmente ordenado $(X, \leq)$, que representa el orden en que se deben realizar determinadas tareas. Deseamos hacer una lista de estas tareas para realizarlas de forma consecutiva, esto es, deseamos determinar un buen orden $\preceq$ en el conjunto X que respete el orden $\leq$, esto es, que si $a \leq b$, entonces $a \preceq b$. Decimos entonces que el orden $\preceq$ es **compatible** con el orden $\leq$. En términos de los grafos que definen las relaciones de orden esto significa que el grafo de $\leq$ está contenido en el grafo de $\preceq$. La determinación del menor de tales órdenes $\preceq$ se realiza mediante la **ordenación topológica** que describimos a continuación.

Sea X un conjunto finito no vacío parcialmente ordenado con relación de orden $\leq$. Si el cardinal de X es $t+1$, se realizan los siguientes pasos:

(1) Se toma un elemento minimal x_0 de X, el cual existe por el Lema 16.6..

(2) Se considera el conjunto $X_1 = X \setminus \{x_0\}$ y en él el orden inducido por el orden de X. Si X_1 es no vacío, por el Lema 16.6. existe un elemento minimal, sea x_1.

(i) ($2 < i < t$). Se considera el conjunto $X_{i-1} = X \setminus \{x_0, \ldots, x_{i-2}\}$ y en él el orden inducido por el orden de X. Si X_{i-1} es no vacío, por el Lema 16.6. existe un elemento minimal, sea x_i.

($t+1$) Tenemos todos los elementos de X en una lista $x_0, x_1, \ldots, x_{t-1}, x_t$, definimos entonces en X un nuevo orden mediante: $x_i \preceq x_j$ si i es menor que j.

Falta comprobar que este nuevo orden es compatible con el orden $\leq$. Sean $x, y \in X$ tales que $x \leq y$, si suponemos que $y = x_j$, entonces y es un elemento minimal de $X_j = X \setminus \{x_0, \ldots, x_{j-1}\}$, y por tanto $x \notin X_j = X \setminus \{x_0, \ldots, x_{j-1}\}$, esto es, $x \in \{x_0, \ldots, x_{j-1}\}$, luego $x = x_i$ con i menor que j, y tenemos $x = x_i \preceq x_j = y$.

16.5. Producto cartesiano

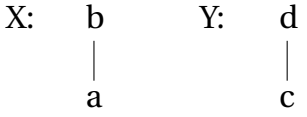
De particular interés es el orden inducido en el producto cartesiano de dos conjuntos parcialmente ordenados.

Sean X e Y dos conjuntos parcialmente ordenados con relaciones de orden $\leq_X$ y $\leq_Y$, respectivamente, entonces en $X \times Y$ podemos definir varias relaciones de orden; veamos alguna de ellas.

Orden producto cartesiano

$$(x_1, y_1) \leq_{car} (x_2, y_2) \quad \text{si} \quad x_1 \leq_X x_2 \quad \text{e} \quad y_1 \leq_Y y_2. \tag{IV.1}$$

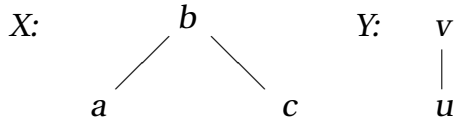
Ejemplo. 16.9.
Se consideran los conjuntos $X = \{a, b\}$ e $Y = \{c, d\}$ con relaciones de orden dadas por los diagramas de Hasse siguientes:



Determinar el diagrama de Hasse de la relación de orden producto cartesiano en $X \times Y$.

Tenemos que X e Y con conjuntos totalmente ordenados; ¿es $X \times Y$ un conjunto totalmente ordenado?

Ejercicio. 16.10.
Hacer el mismo estudio para los conjuntos parcialmente ordenados dados por los diagramas de Hasse siguientes:

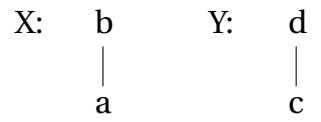


Orden lexicográfico

$$(x_1, y_1) \leq_{lex} (x_2, y_2) \quad \text{si} \quad \begin{cases} x_1 <_X x_2 \text{ ó} \\ x_1 = x_2 \text{ e } y_1 \leq_Y y_2 \end{cases} \tag{IV.2}$$

Llamamos a esta relación de orden $\leq_{lex}$ el **orden lexicográfico** definido por los órdenes $\leq_X$ y $\leq_Y$.

Ejemplo. 16.11.
Se consideran los conjuntos $X = \{a, b\}$ e $Y = \{c, d\}$ con relaciones de orden dadas por los diagramas de Hasse siguientes:



Determinar el diagrama de Hasse de la relación de orden lexicográfico en $X \times Y$.

Tenemos, en este caso, que X e Y con conjuntos bien ordenados. ¿Es $X \times Y$ un conjunto bien ordenado?

Proposición. 16.12.
Sean X e Y conjuntos bien ordenados con relaciones de orden $\leq_X$ y $\leq_Y$, respectivamente, entonces $\leq_{lex}$ es un buen orden en $X \times Y$.

DEMOSTRACIÓN. Recordemos que un conjunto parcialmente ordenado es un conjunto bien ordenado si cada subconjunto no vacío tiene un primer elemento. Sean $(X, \leq_X)$ y $(Y, \leq_Y)$ conjuntos bien ordenados no vacíos. Entonces $X \times Y$ es un conjunto no vacío. Consideramos en $X \times Y$ el orden lexicográfico. Si Z es un subconjunto no vacío de $X \times Y$. Llamamos (x_λ, y_λ) a los elementos de Z, en donde λ varía en un conjunto Λ. Consideramos el conjunto $Z_X = \{x_\lambda \colon \ \lambda \in \Lambda\}$; por ser X bien ordenado, existe un primer elemento en Z_X, sea x_{λ_0}. Consideramos $Z_Y = \{y_\lambda \colon \ x_\lambda = x_{\lambda_0}\}$; este conjunto es no vacío, ya que al menos contiene a y_{λ_0}, y por lo tanto Z_Y tiene un primer elemento, sea y_{λ_1}, entonces $(x_{\lambda_0}, y_{\lambda_1}) = (x_{\lambda_1}, y_{\lambda_1})$ es un primer elemento de Z y tenemos el resultado. □

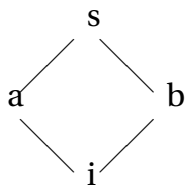
17. Retículos

Llamamos **retículo** a un conjunto parcialmente ordenado en el que para cada par de elementos x e y existe el supremo y el ínfimo, de $\{x, y\}$.

Si X es un retículo, el supremo de $\{x, y\}$ se representa también por $x \vee y$, y el ínfimo se representa también por $x \wedge y$.

Observación. 17.1.
Observar que un orden total es siempre un retículo, sin embargo el recíproco no es cierto, pues dados dos elementos a y b puede existir el supremo y el ínfimo y pueden no estar relacionados a y b.

Ejemplo. 17.2.
Veamos el siguiente ejemplo de un retículo que no es un conjunto totalmente ordenado.



Es claro que $a \wedge b = i$ y $a \vee b = s$. Sin embargo $a \not\leq b$ y $b \not\leq a$.

17.1. Caracterización algebraica de retículo

Podemos pensar en un retículo como en un conjunto X con dos operaciones binarias $\vee$ y $\wedge$, verificando las siguientes propiedades:

(I) **Propiedades conmutativas**.
$a \vee b = b \vee a \quad$ y $\quad a \wedge b = b \wedge a, \quad \forall a, b \in X$.

(II) **Propiedades asociativas**.
$a \vee (b \vee c) = (a \vee b) \vee c \quad$ y $\quad a \wedge (b \wedge c) = (a \wedge b) \wedge c \quad \forall a, b, c \in X$.

(III) **Propiedades de Idempotencia**.
$a \vee a = a \quad$ y $\quad a \wedge a = a \quad \forall a \in X$.

(IV) **Propiedades de absorción**.
$a \vee (a \wedge b) = a \quad$ y $\quad a \wedge (a \vee b) = a \quad \forall a, b \in X$.

Si X es un retículo y existe $\min(X)$, representamos a este elemento por 0, y si existe $\max(X)$, lo representamos por 1. Si existen los elementos 0 y 1, decimos que X es un **retículo acotado**.

Se verifican las siguientes propiedades:

(V) $a \wedge 0 = 0, \quad a \vee 0 = a, \quad a \wedge 1 = a \quad$ y $\quad a \vee 1 = 1 \quad \forall a \in X.$

Ejercicio. 17.3.
Probar que todo retículo finito es un retículo acotado.

17.2. Retículos distributivos. Retículos complementados

Un retículo X se llama **distributivo** si verifica:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \text{ y}$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

para cualesquiera $a, b, c \in X$.

Si X es un retículo acotado, y $a \in X$, llamamos **complemento** de a en X a cualquier elemento $b \in X$ que verifique:

$$a \vee b = 1 \text{ y } a \wedge b = 0.$$

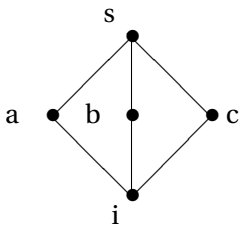
Lema. 17.4.
Si X es un retículo acotado y distributivo y $a \in X$, entonces existe a lo sumo un único complemento de a.

DEMOSTRACIÓN. Supongamos que a tiene dos complementos, y sean estos b_1 y b_2, entonces se verifica:

$$b_1 = b_1 \wedge 1 = b_1 \wedge (a \vee b_2) = (b_1 \wedge a) \vee (b_1 \wedge b_2) = 0 \vee (b_1 \wedge b_2) = b_1 \wedge b_2$$

De la misma forma se obtiene $b_2 = b_1 \wedge b_2$, y por tanto $b_1 = b_2$ □

Ejemplo. 17.5.
Existen retículo en los que el complemento no es único.



El complemento de a es tanto b como c. Como consecuencia no es un retículo distributivo

En el siguiente capítulo vamos a estudiar retículos distributivos con mayor detalle.

Capítulo V

Álgebras de Boole

18. Álgebras de Boole

Vamos a introducir las álgebras de Boole para trabajar, de forma unificada, con estructuras tan diversas como el álgebra de conjuntos o el álgebra de proposiciones. El ejemplo más sencillo es el conjunto $\{0,1\}$ y, por extensión el conjunto de aplicaciones de un producto de copias de $\{0,1\}$ a $\{0,1\}$.

Comenzamos definiendo en el conjunto $\{0,1\}$ dos nuevas operaciones, la **suma** y el **producto**, cuyas tablas son respectivamente:

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

Amen de estas dos operaciones vamos a considerar una tercera operación, a la que llamaremos **complemento**, que una operación unaria y que está definida mediante:

$$0 \mapsto \overline{0} = 1 \qquad 1 \mapsto \overline{1} = 0.$$

Para simplificar representamos por B el conjunto $\{0,1\}$ y el producto $\times$ en B lo representamos

como la yuxtaposición de los factores.

Llamamos B^n al producto cartesiano de n copias de B, siendo $0 \neq n \in \mathbb{N}$.

Una **función booleana de grado** n es una aplicación de B^n en B. Los valores de una función booleana $f : B^n \longrightarrow B$ son 0 ó 1, y se representan en la forma $f(x_1, \ldots, x_n)$, en donde $(x_1, \ldots, x_n)$ es una n–upla de elementos de B. Llamamos a cada x_i una **variable booleana** de f. Observar que cada x_i puede tomar solo los valores 0 y 1.

Ejemplo. 18.1.
Considerar la función booleana $f : B^3 \longrightarrow B$ definida por $f(x, y, z) = xy + x\overline{z}$, y calcular todos los valores que toma esta función.

SOLUCIÓN. Construimos la siguiente tabla, en la que para cada posible valor de las variables booleanas x, y y z se da el valor de la función f.

x	y	z	xy	$\overline{z}$	$x\overline{z}$	$f(x,y,z) = xy + x\overline{z}$
1	1	1	1	0	0	1
1	1	0	1	1	1	1
1	0	1	0	0	0	0
1	0	0	0	1	1	1
0	1	1	0	0	0	0
0	1	0	0	1	0	0
0	0	1	0	0	0	0
0	0	0	0	1	0	0

□

Dos funciones booleanas $f, g : B^n \longrightarrow B$ son **iguales** si toman los mismos valores, esto es, si para cualquier n–upla $(b_1, \ldots, b_n) \in B^n$ se tiene $f(b_1, \ldots, b_n) = g(b_1, \ldots, b_n)$.

Una **expresión booleana** en las variables $x_1, \ldots, x_n$ es cualquier expresión construida según la regla de recursión siguiente:

(1) $0, 1, x_1, \ldots, x_n$ son expresiones booleanas;

(2) si E y F son expresiones booleanas, también lo son las expresiones siguientes: $\overline{E}$, $E + F$ y EF.

En el ejemplo 18.1. tenemos que $xy + x\overline{z}$ es una expresión booleana. Se dice que la expresión $xy + x\overline{z}$ **representa** a la función f. Otra expresión que representa a la función f es por ejemplo: $xyz + x\overline{y}\overline{z}$. ¡Comprobar!

Dos expresiones booleanas son **equivalentes** si representan la misma función.

Existe el problema de contar cuantas funciones booleanas hay de un grado dado. Por ejemplo, existen cuatro funciones booleanas de grado uno; éstas están dadas en el siguiente cuadro:

x	f_1	f_2	f_3	f_4
1	1	1	0	0
0	1	0	1	0

la razón es que hay cuatro aplicaciones de B en B. En general de B^n en B hay 2^{2^n} aplicaciones distintas, ya que en B^n el número de n–uplas es 2^n.

Ejercicio. 18.2.
Determinar explícitamente cuantas funciones booleanas hay de grado dos y de grado tres.

18.1. Funciones booleanas

Consideramos el conjunto $\mathcal{B}_n$ de las funciones booleanas de grado n. En este conjunto definimos tres operaciones como sigue:

La suma. $(f+g)(x_1,\dots,x_n) = f(x_1,\dots,x_n) + g(x_1,\dots,x_n)$.
El producto. $(fg)(x_1,\dots,x_n) = f(x_1,\dots,x_n)g(x_1,\dots,x_n)$.
El complemento. $\overline{f}(x_1,\dots,x_n) = \overline{f(x_1,\dots,x_n)}$.

Ahora las propiedades de las operaciones de $B=\{0,1\}$ pasan a propiedades de $\mathcal{B}_n$. Se tienen entonces que la suma y el producto en $\mathcal{B}_n$ verifican, entre otras, las siguientes propiedades:

(I) **Propiedad asociativa**. $f+(g+h) = (f+g)+h$, para cualesquiera $f,g,h \in \mathcal{B}_n$.

(II) **Propiedad conmutativa**. $f+g = g+f$ para cualesquiera $f,g \in \mathcal{B}_n$.

(III) **Existencia de elemento neutro**. La función $0(b_1,\dots,b_n) = 0$ para cada $(b_1,\dots,b_n) \in B^n$ verifica que cualquier $f \in \mathcal{B}_n$ tenemos $0+f=f$.

(IV) **Propiedad de idempotencia**. $f+f=f$ para cualquier $f \in \mathcal{B}_n$

(V) **Propiedad distributiva de la suma respecto al producto**. $f+(gh) = (f+g)(f+h)$ para cualesquiera $f,g,h \in \mathcal{B}_n$.

(VI) **Propiedad asociativa**. $f(gh) = (fg)h$, para cualesquiera $f,g,h \in \mathcal{B}_n$.

(VII) **Propiedad conmutativa**. $fg = gf$ para cualesquiera $f,g \in \mathcal{B}_n$.

(VIII) **Existencia de elemento neutro**. La función $1(b_1,\dots,b_n)=1$ para cada $(b_1,\dots,b_n)\in B^n$ verifica que para cualquier $f\in\mathcal{B}_n$ tenemos $1f=f$.

(IX) **Propiedad de idempotencia**. $ff=f$, para cualquier $f\in\mathcal{B}_n$

(X) **Propiedad distributiva del producto respecto a la suma**. $f(g+h)=fg+fh$ para cualesquiera $f,g,h\in\mathcal{B}_n$.

(XI) **Propiedad de acotación**. $f+1=1$ y $f0=0$, para cualquier $f\in\mathcal{B}_n$

Todas estas propiedades se pueden probar de la misma forma, viendo que las funciones booleanas que intervienen en cada una de ellas toman los mismos valores.

A modo de ejemplo veamos que se verifica la *Propiedad distributiva de la suma respecto al producto*:

DEMOSTRACIÓN. Sean $f,g,h\in\mathcal{B}_n$, y sea $(b_1,\dots,b_n)\in B^n$ un elemento arbitrario, se verifica:

$$\begin{aligned}(f+(gh))(b_1,\dots,b_n) &= f(b_1,\dots,b_n)+(g\,h)(b_1,\dots,b_n)\\ &= f(b_1,\dots,b_n)+(g(b_1,\dots,b_n)\;h(b_1,\dots,b_n))\\ &= [f(b_1,\dots,b_n)+g(b_1,\dots,b_n)]\,[f(b_1,\dots,b_n)+h(b_1,\dots,b_n)]\\ &\quad \text{ya que en } B \text{ se verifica esta propiedad}\\ &= (f+g)(b_1,\dots,b_n)\,(f+h)(b_1,\dots,b_n)\\ &= [(f+g)\,(f+h)](b_1,\dots,b_n)\end{aligned}$$

□

Estas propiedades se pueden complementar con las propias del complemento:

(XII) **Propiedad de doble complemento**. $\overline{\overline{f}}=f$, para cualquier $f\in\mathcal{B}_n$

(XIII) **Propiedad de de Morgan**. $\overline{fg}=\overline{f}+\overline{g}$ y $\overline{f+g}=\overline{f}\;\overline{g}$, para cualesquiera $f,g\in\mathcal{B}_n$.

(XIV) **Existencia de inverso con respecto al 1**. $f+\overline{f}=1$, para cualquier $f\in\mathcal{B}_n$

(XV) **Existencia de inverso con respecto al 0**. $f\overline{f}=0$, para cualquier $f\in\mathcal{B}_n$

Todas estas propiedades se pueden probar de la misma forma, viendo que las funciones booleanas que intervienen en cada una de ellas toman siempre los mismos valores. A modo de ejemplo veamos que se verifica una de las propiedades de de Morgan.

$$\begin{aligned}\overline{fg}(b_1,\dots,b_n) &= \overline{(fg)(b_1,\dots,b_n)}\\ &= \overline{f(b_1,\dots,b_n)g(b_1,\dots,b_n)}\\ &= \overline{f(b_1,\dots,b_n)}+\overline{g(b_1,\dots,b_n)}\\ &= \overline{f}(b_1,\dots,b_n)+\overline{g}(b_1,\dots,b_n)\\ &= (\overline{f}+\overline{g})(b_1,\dots,b_n)\end{aligned}$$

Se puede hacer un listado mínimo eliminando algunas de estas propiedades, ya que algunas se pueden deducir del resto. Por ejemplo la existencia de inverso con respecto al 0 se obtiene de la existencia de inverso con respecto al 1 y el resto de las propiedades. Una forma de probar esto es:

$$f\overline{f} = \overline{\overline{f}\,\overline{f}} = \overline{\overline{f} + \overline{f}} = \overline{\overline{f} + f} = \overline{1} = 0$$

Hay otras propiedades que se pueden probar a partir de éstas, como por ejemplo la Propiedad de absorción.

Lema. 18.3. (Propiedad de absorción.)
Para cualesquiera $f, g \in \mathcal{B}_n$ se verifica: $f(f+g) = f = f + fg$.

DEMOSTRACIÓN. Es claro que

$$f(f+g) = ff + fg = f + fg.$$

Vamos a probar que son iguales a f utilizando la propiedad distributiva de la suma respecto al producto:

$$f + fg = f(1+g) = f1 = f.$$

□

18.2. Definición abstracta de álgebra de Boole

Hemos estudiado ejemplos de las estructuras abstractas que queremos formalizar: **las álgebras de Boole**. Vamos a dar una definición (¡abstracta!) de las mismas.

Un **álgebra de Boole** es un conjunto $\mathcal{B}$ junto con dos operaciones binarias, $\vee$ y $\wedge$, y una operación unaria, $\bar{}$, que verifican las siguientes propiedades para cualesquiera elementos a, b, $c \in \mathcal{B}$:

(I) **Propiedad conmutativa**. $a \vee b = b \vee a$ y $a \wedge b = b \wedge a$.

(II) **Propiedad asociativa**. $a \vee (b \vee c) = (a \vee b) \vee c$ y $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

(III) **Elemento neutro**. $a \vee 0 = a$ y $a \wedge 1 = a$.

(IV) **Propiedad de complemento**. $a \vee \overline{a} = 1$ y $a \wedge \overline{a} = 0$.

(V) **Propiedad distributiva**. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ y $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Todas las propiedades de las funciones booleanas que se han citado en las páginas 129 y 130 se pueden ahora enunciar y probar para álgebra de Boole abstractas.

Los conjuntos $\mathcal{B}_n$, junto con las operaciones $+$, $\times$ y $(\bar{})$ son ejemplos de álgebras de Boole.

Ahora es fácil comprobar que en realidad ya hemos visto y estudiado, a lo largo del curso, otros ejemplos de álgebras de Boole.

Ejemplo. 18.4.
Sea X un conjunto, entonces el conjunto potencia o conjunto de las partes de X, $P(X)$, es un álgebra de Boole con las operaciones:

$\vee$	unión
$\wedge$	intersección
$\bar{}$	complemento

Existen más ejemplos que veremos a continuación.

Principio de dualidad. Si observamos las propiedades que definen un álgebra de Boole, observamos que todas ellas siguen siendo ciertas si intercambiamos $\vee$ y $\wedge$ y a la vez 0 y 1. Al realizar este proceso a una expresión en un álgebra de Boole, obtenemos otra expresión, que se llama su **expresión dual**. En un álgebra de Boole dos expresiones son iguales si y solo si sus duales son iguales.

Ejemplo. 18.5.
(1) Si se considera la expresión $x \vee x = x, \forall x$, su dual es: $x \wedge x = x, \forall x$.

(2) El dual de $x \vee 0 = x, \forall x$, es: $x \wedge 1 = x, \forall x$.

(3) El dual de $x \vee (x \wedge y) = x, \forall x, y$, es: $x \wedge (x \vee y) = x, \forall x, y$.

18.3. Teorema de estructura de las álgebras de Boole finitas

Dadas dos álgebras de Boole B y B', un **homomorfismo** de B a B' es una aplicación $\varphi : B \longrightarrow B'$ que verifica:

(1) $\varphi(b_1 \vee b_2) = \varphi(b_1) \vee \varphi(b_2,$

(2) $\varphi(b_1 \wedge b_2) = \varphi(b_1) \wedge \varphi(b_2,$

(3) $\varphi(\overline{b}) = \overline{\varphi(b)}$.

Dos álgebras de Boole B y B' se llaman **isomorfas** si existe un homomorfismo de álgebras de Boole, $\varphi B \longrightarrow B'$ que es una biyección, La aplicación φ se dice que es un **isomorfismo de álgebras de Boole**.

Un elemento a de un álgebra de Boole B se llama un **átomo** si $a \neq 0$ y cuando $a = b_1 \vee b_2$, entonces $b_1 = a$ ó $b_2 = a$.

Lema. 18.6.
Si B es un álgebra de Boole finita, entonces existen átomos en B.

DEMOSTRACIÓN. Tomamos un elemento $0 \neq b \in B$, si b no es un átomo, existen $b_1, b_1' \in B$ tales que $b = b_1 \vee b_1'$ y $b_1 \neq b \neq b_1'$. Si b_1 no es un átomo, existen $b_2, b_2' \in B$ tales que $b_1 = b_2 \vee b_2'$ y $b_2 \neq b_1 \neq b_2'$. De esta forma, se construye una sucesión $b, b_1, b_2, \ldots$ de elementos distintos. Como B es finito, esta sucesión es finita y por tanto necesariamente algún b_i es un átomo. □

Ejercicio. 18.7.
Sea B un álgebra de Boole y $a, b \in B$. Son equivalentes:

(a) $a = a \wedge b$.

(b) $b = a \vee b$.

SOLUCIÓN. Si $a = a \wedge b$, entonces $b = (a \vee \overline{a}) \wedge b = (a \wedge b) \vee (\overline{a} \wedge b) = a \vee (\overline{a} \wedge b) = (a \vee \overline{a}) \wedge (a \vee b) = a \vee b$. La otra implicación se obtiene por dualidad. □

Ejercicio. 18.8.
Sea B un álgebra de Boole, si $a \in B$ es un átomo y $b \in B$, entonces $a \wedge b = 0$ ó $a \wedge b = a$.

SOLUCIÓN. Si $a \wedge b \neq 0$, entonces de $a = a \wedge 1 = a \wedge (b \vee \overline{b}) = (a \wedge b) \vee (a \wedge \overline{b})$ se deduce, por ser a un átomo, que $a = a \wedge b$ ó $a = a \wedge \overline{b}$. Si $a = a \wedge \overline{b}$, entonces $\overline{b} = a \vee \overline{b}$, lo que es una contradicción, ya que en este caso se tendría $a \wedge b = a \wedge \overline{b} \wedge b = a \wedge 0 = 0$. □

Ejercicio. 18.9.
Sea B un álgebra de Boole, si a y b son átomos entonces $a \wedge b = 0$ ó $a = a \wedge b = b$.

Proposición. 18.10.
Si B es un álgebra de Boole finita, entonces para cada elemento $0 \neq b \in B$ existen átomos b_1, $\ldots$, b_t en B distintos dos a dos, y determinados de forma única, tales que $b = b_1 \vee \cdots \vee b_t$.

DEMOSTRACIÓN. Dado $b \neq 0$, por la demostración del Lema, existe un átomo b_1, y un elemento b_1' tales que $b = b_1 \vee b_1'$. Si $b_1' \neq 0$, entonces existe un átomo b_2 y un elemento b_2' tales que $b_1' = b_2 \vee b_2'$, luego $b = b_1 \vee b_2 \vee b_2'$. Siguiendo con este proceso encontramos una expresión del tipo $b = b_1 \vee b_2 \vee \cdots \vee b_t \vee b_t'$. Si $b_t' = 0$, entonces b admite la descripción pedida.

Si $b_i \neq 0$, entonces obtenemos una expresión $b = b_1 \vee b_2 \vee \cdots \vee b_{t+1} \vee b'_{t+1}$. Como B es finito, entonces la sucesión de elementos distintos b'_1, b'_2, ... tiene que ser finita, y en consecuencia se llega a un $b'_s = 0$. Para obtener átomos distintos dos a dos basta eliminar los que aparezcan repetidos.

Supongamos que tenemos dos expresiones $b = b_1 \vee \cdots \vee b_t = c_1 \vee \cdots \vee c_s$ en donde los b_i son átomos distintos dos a dos, y los c_j son átomos distintos dos a dos. Entonces para cada índice i se tiene:

$$b_i = b_i \wedge (b_1 \vee \cdots \vee b_t) = b_i \wedge (c_1 \vee \cdots \vee c_s) = (b_i \wedge c_1) \vee \cdots \vee (b_i \wedge c_s).$$

Como b_i es un átomo, se tiene $b_i = b_i \wedge c_j$ para algún índice j, pero como c_j es también un átomo, entonces $b_i = b_i \wedge c_j = c_j$. Sin pérdida de generalidad podemos suponer que $i = 1 = j$. Si consideramos b_2, existe un índice j tal que $b_2 = c_j$. También sin pérdida de generalidad podemos suponer que $j = 2$, luego $b_2 = c_2$. De esta forma llegamos a las igualdades $b_i = c_i$, para $i = 1, 2, \ldots, t$, y en consecuencia $t \leq s$. Si trabajamos ahora con los c_j en vez de con los b_i, llegamos a que $s \leq t$, y por tanto $t = s$ y los átomos que aparecen son los mismos; puede variar el orden en que estos aparecen. □

Teorema. 18.11.
Si B es un álgebra de Boole finita, entonces existe un conjunto X tal que B y $P(X)$ son álgebras de Boole isomorfas.

DEMOSTRACIÓN. Si B es un álgebra de Boole finita, supongamos que en B tenemos n átomos distintos dos a dos; sean estos b_1, ..., b_n. Por la Proposición cada elemento de B se escribe de forma única como $b_{i_1} \vee \cdots \vee b_{i_s}$ para $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, n\}$. Para conocer el número de elementos de B basta contar el número de expresiones distintas de la forma $b_{i_1} \vee \cdots \vee b_{i_s}$ que podemos construir; este número es exactamente el número de subconjuntos de $\{1, \ldots, n\}$. Por lo tanto B tiene 2^n elementos.

Vamos a establecer un isomorfismo entre B y $P(\{1, \ldots, n\})$. A cada elemento $b \in B$, que se escribe de forma única como $b = b_{i_1} \vee \cdots \vee b_{i_s}$, le asociamos mediante φ el subconjunto $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, n\}$. Vamos a ver que φ es un isomorfismo. Sean $b = b_{i_1} \vee \cdots \vee b_{i_s}$ y $c = c_{j_1} \vee \cdots \vee c_{j_r}$, entonces:

$$\begin{aligned}
\varphi(b \vee c) &= \varphi(b_{i_1} \vee \cdots \vee b_{i_s} \vee c_{j_1} \vee \cdots \vee c_{j_r}) \\
&= \{i_1, \ldots, i_s, j_1, \ldots, j_r\} \text{ en donde eliminamos los elementos repetidos} \\
&= \{i_1, \ldots, i_s\} \cup \{, j_1, \ldots, j_r\} \\
&= \varphi(b_{i_1} \vee \cdots \vee b_{i_s}) \cup \varphi(\vee c_{j_1} \vee \cdots \vee c_{j_r}) \\
&= \varphi(b) \cup \varphi(c).
\end{aligned}$$

$$\begin{aligned}
\varphi(b \wedge c) &= \varphi((b_{i_1} \vee \cdots \vee b_{i_s}) \wedge (c_{j_1} \vee \cdots \vee c_{j_r})) \\
&= \varphi(\textstyle\bigvee_{i_h, j_k} (b_{i_h} \wedge c_{j_1})
\end{aligned}$$

La expresión $b_{i_h} \wedge c_{j_1}$ es b_{i_h} si $i_h = j_k$ y 0 en caso contrario, luego tenemos:

$$\begin{aligned}\varphi(b \wedge c) &= \varphi(\textstyle\bigvee_{i\in\{i_1,\ldots,i_s\}\cap\{,j_1,\ldots,j_r\}} b_i \\ &= \{i_1,\ldots,i_s\} \cap \{,j_1,\ldots,j_r\} \\ &= \varphi(b_{i_1} \vee \cdots \vee b_{i_s}) \cap \varphi(c_{j_1} \vee \cdots \vee c_{j_r}) \\ &= \varphi(b) \cap \varphi(c).\end{aligned}$$

Es claro que $\overline{b} = \bigvee_{i\notin\{i_1,\ldots,i_s\}} b_i$, luego se tiene:

$$\begin{aligned}\varphi(\overline{b}) &= \varphi(\textstyle\bigvee_{i\notin\{i_1,\ldots,i_s\}} b_i) \\ &= \overline{\{i_1,\ldots,i_s\}} \\ &= \overline{\varphi(b)}.\end{aligned}$$

□

Como consecuencia tenemos los siguientes resultados:

Corolario. 18.12.
Si B es un álgebra de Boole finita, entonces el cardinal de B es de la forma 2^n para algún entero natural n.

Teorema. 18.13.
Si X es un conjunto finito de cardinal 2^n, entonces $P(X)$ y $\mathcal{B}_n$ son álgebras de Boole isomorfas.

19. Formas canónicas de funciones booleanas

Se trata ahora de ver que toda función booleana se puede escribir como una expresión booleana, y que por lo tanto el problema de estudiar funciones booleanas se reduce a estudiar, salvo equivalencia, expresiones booleanas.

Recordemos que una función booleana de grado n, $f : B^n \longrightarrow B$, está determinada al conocer su valor en cada n–upla $(b_1, \ldots, b_n) \in B^n$, y que el valor en cada una de las n–uplas es siempre 0 ó 1.

En el estudio de funciones booleanas de grado n tenemos n variables booleanas: $x_1, \ldots, x_n$. Vamos a introducir notaciones que nos permitan tratar con estas variables booleanas y con sus complementos.

Llamamos **literal** a una variable booleana o a un complemento de una variable booleana.

Llamamos **minitérmino**(=**minterm**) a un producto $y_1 \cdots y_n$, en donde cada y_i es el literal x_i ó $\overline{x_i}$. Observar que al considerar un minitérmino como una función booleana, su valor es siempre 0 salvo en un sólo caso, el cual corresponde a una combinación prefijada de valores de las variables x_i o sus complementos, en que vale 1.

Ejemplo. 19.1.
Si tenemos las variables x_1, x_2, x_3 y x_4, los siguientes son minitérminos: $x_1\overline{x_2}\,\overline{x_3}x_4$, $x_1x_2x_3\overline{x_4}$, $\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}$, $x_1x_2x_3x_4$. En cambio no lo son: x_1, x_2, x_3, x_4, $x_1x_2\overline{x_4}$, $x_1x_2x_3x_4x_5$.

Ejercicio. 19.2.
Dar el minitérmino que toma el valor 1 para los valores de las variables siguientes:

$$x_1 = x_3 = x_5 = 1, \qquad x_2 = x_4 = x_6 = 0.$$

SOLUCIÓN. El minitérmino es $x_1\,\overline{x_2}\,x_3\,\overline{x_4}\,x_5\,\overline{x_6}$. □

Dada una función booleana $f : B^n \longrightarrow B$, si f toma el valor 1 para la n–upla $(b_1, \ldots, b_n)$, entonces existe un minitérmino que toma el valor 1 precisamente en $(b_1, \ldots, b_n)$. Vamos a desarrollar una estrategia para escribir este minitérmino. Un método podría ser el siguiente. Escribimos

$$x_i^{(b)} = \begin{cases} x_i & \text{si } b = 1 \\ \overline{x_i} & \text{si } b = 0 \end{cases}$$

Entonces el minitérmino que andamos buscado se escribe $x_1^{(b_1)} \cdots x_n^{(b_n)}$. Al considerar ahora todas las n–uplas $(b_1, \ldots, b_n)$ tales que $f(b_1, \ldots, b_n) = 1$, se verifica:

$$f = \sum_{(b_1,\ldots,b_n),\, f(b_1,\ldots,b_n)=1} x_1^{(b_1)} \cdots x_n^{(b_n)}.$$

Llamamos a esta expresión la **forma normal disyuntiva de la función booleana** f o el **desarrollo en suma de productos de la función booleana**. Observar que esta forma normal disyuntiva, para cada función booleana, es única.

De forma dual se puede expresar cada función booleana en como un producto de sumas de expresiones booleanas de literales, se obtienen así la **forma normal conjuntiva de la función booleana** f o el **desarrollo en producto de sumas de la función booleana** y el concepto de **maxitérmino**.

Se define un **maxitérmino** (=**maxterm**) para las variables $x_1, \ldots, x_n$, como una suma de n literales $y_1 + \cdots + y_n$, en donde y_i es igual a x_i ó a $\overline{x_i}$. Como consecuencia un maxitérmino toma siempre el valor 1, salvo para un caso especial, aquel en el que todos los literales que aparecen toman el valor 0. En este sentido es el complemento de un minitérmino.

Observar que cada maxitérmino es el complemento de un minitérmino:

minitérmino	maxitérmino
$x_1x_2x_3x_4$	$\overline{x_1} + \overline{x_2} + \overline{x_3} + \overline{x_4}$
$x_1\overline{x_2}x_3\overline{x_4}$	$\overline{x_1} + x_2 + \overline{x_3} + x_4$

Ejercicio. 19.3.
Se considera la función f de grado tres con valores:

x	y	z	f
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Los valores para los que la función f toma el valor 1 son: $(1,1,0)$, $(1,0,0)$ y $(0,1,1)$. Entonces los minitérminos que necesitamos son: $xy\overline{z}$, $x\overline{yz}$ y $\overline{x}yz$. En consecuencia la expresión de f en función de los minitérminos es:

$$f = xy\overline{z} + x\overline{yz} + \overline{x}yz,$$

que es la forma normal disyuntiva de f. Para obtener la forma normal conjuntiva basta considerar la forma normal disyuntiva de $\overline{f}$, que en nuestro caso también se puede expresar como:

$$\overline{f} = xyz + x\overline{y}z + \overline{x}y\overline{z} + \overline{x}\overline{y}z + \overline{xyz}.$$

Al tomar complementos se tiene:

$$f = (\overline{x} + \overline{y} + \overline{z})(\overline{x} + y + \overline{z})(x + \overline{y} + z)(x + y + \overline{z})(x + y + z),$$

la forma normal conjuntiva de la función booleana f.

En la siguiente tabla marcamos con $*$ los minitérminos que aparecen en la forma normal disyuntiva y con $\star$ los maxitérminos que aparecen en la forma normal conjuntiva.

minitérmino		*binario*	*maxitérmino*	
xyz		111	$\overline{x}+\overline{y}+\overline{z}$	$\star$
$xy\overline{z}$	$*$	110	$\overline{x}+\overline{y}+z$	
$x\overline{y}z$		101	$\overline{x}+y+\overline{z}$	$\star$
$x\overline{y}\overline{z}$	$*$	100	$\overline{x}+y+z$	
$\overline{x}yz$	$*$	011	$x+\overline{y}+\overline{z}$	
$\overline{x}y\overline{z}$		010	$x+\overline{y}+z$	$\star$
$\overline{x}\overline{y}z$		001	$x+y+\overline{z}$	$\star$
$\overline{x}\overline{y}\overline{z}$		000	$x+y+z$	$\star$

19.1. Conjuntos funcionalmente completos

Como consecuencia de que cada función booleana tiene una forma normal disyuntiva, resulta que toda función booleana se puede expresar con literales y los operadores del conjunto $\{+,\times,^-\}$. Decimos entonces que este conjunto de operadores es un **conjunto funcionalmente completo**.

Sin embargo, como es posible expresar el operador suma $(+)$ en términos de los otros dos teniendo en cuenta la propiedad de de Morgan:

$$x+y=\overline{\overline{x}\,\overline{y}},$$

resulta que el conjunto $\{\times,^-\}$ es también funcionalmente completo.

Por dualidad se tiene que la expresión siguiente es siempre cierta:

$$xy=\overline{\overline{x}+\overline{y}},$$

entonces tenemos que el conjunto $\{+,^-\}$ es también funcionalmente completo.

A la pregunta de si existe un conjunto funcionalmente completo formado por un sólo operador la respuesta es sí. Para comprobarlo definimos un operador nuevo mediante la tabla:

$x\uparrow y$	0	1
0	1	1
1	1	0

x	y	$x\uparrow y$
1	1	0
1	0	1
0	1	1
0	0	1

Para ver que $\{\uparrow\}$ es un conjunto funcionalmente completo, basta ver que se pueden expresar los operadores de $\{\times, \bar{}\}$ en términos de $\uparrow$. En efecto, tenemos:

$$\overline{x} = x \uparrow x$$
$$xy = (x \uparrow y) \uparrow (x \uparrow y).$$

Llamamos a $\uparrow$ el operador "**no y**", ya que es claro que se tiene: $x \uparrow y = \neg(x \wedge y)$.

Consideramos otro operador, representado por $\downarrow$, y definido por la tabla:

$x \downarrow y$	0	1
0	1	0
1	0	0

x	y	$x \downarrow y$
1	1	0
1	0	0
0	1	0
0	0	1

Llamamos a $\downarrow$ "**no o**", ya que es claro que se tiene $x \downarrow y = \neg(x \vee y)$.

20. El álgebra Boole de las proposiciones lógicas

Ejemplo. 20.1.
Si consideramos el conjunto de todas las proposiciones, entonces tenemos otro ejemplo de álgebra de Boole con las operaciones:

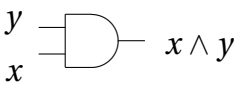
$\vee$	ó
$\wedge$	y
-	no

21. Circuitos lógicos

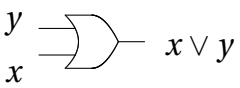
En un ordenador se utiliza el bit como unidad de medida, de almacenamiento y de comunicación; el bit se transmite a través de las diferencias de voltage, y el medio que se emplea es el circuito. Hay esencialmente dos tipos de circuitos, por un lado aquellos en los que la salida depende de la entrada y del estado mismo del circuito (memoria); esto se llaman **circuitos secuenciales**, y por otro lado están los **circuitos lógicos** o **combinatorios**, en los que la salida depende exclusivamente de la entrada y no del estado del circuito.

Los circuitos lógicos están formados por dispositivos a los que llamaremos **puertas lógicas**. Vamos a considerar tres tipo de ellas:

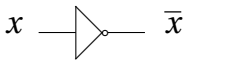
puerta Y. tiene dos entradas y una salida; si las entradas son los bits x e y, entonces la salida se representa por $x \wedge y$. En el circuito este dispositivo se representa mediante:



puerta O. tiene dos entradas y una salida; si las entradas son los bits x e y, entonces la salida se representa por $x \vee y$. En el circuito este dispositivo se representa mediante:



puerta NO. tiene una entrada y una salida; si la entrada es el bit x, entonces la salida se representa por $\overline{x}$. En el circuito este dispositivo se representa mediante:



Los bits toman únicamente los valores 0 y 1, entonces, según los valores de x e y, el valor de $x \wedge y$ está dado en la tabla siguiente, que es la tabla del operador $\wedge$ en un álgebra de Boole.

x	y	$x \wedge y$
1	1	1
0	1	0
1	0	0
0	0	0

el valor de $x \vee y$ está dado en la tabla siguiente, que es la tabla del operador $\vee$ en un álgebra

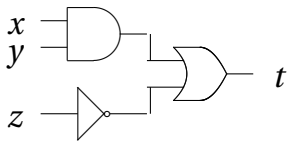
de Boole.

x	y	$x \vee y$
1	1	1
0	1	1
1	0	1
0	0	0

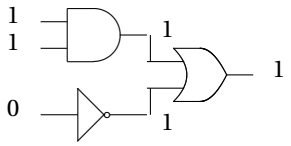
el valor de $\overline{x}$ está dado en la tabla siguiente, que es la tabla del operador $\bar{}$ en un álgebra de Boole.

x	$\overline{x}$
1	0
0	1
1	0
0	1

Ejemplo. 21.1.
Vamos a estudiar el siguiente circuito lógico y obtener la expresión booleana que éste determina:



Observar que para valores concretos de x, y y z, por ejemplo: $x = 1$, $y = 1$, $z = 0$, se tiene:



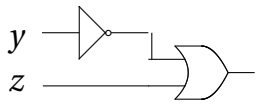
Observar que para otros valores de x, y y z se podría hacer lo mismo. Lo que estamos haciendo es pues la tabla de la expresión booleana: $(x \wedge y) \vee \overline{z}$.

x	y	z	$x \wedge y$	$\overline{z}$	$(x \wedge y) \vee \overline{z}$
1	1	1	1	0	1
1	1	0	1	1	1
1	0	1	0	0	0
1	0	0	0	1	1
0	1	1	0	0	0
0	1	0	0	1	1
0	0	1	0	0	0
0	0	0	0	1	1

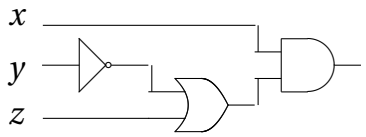
También es posible hacer el proceso a la inversa, esto es, pasar de una expresión booleana a un circuito lógico.

Ejemplo. 21.2.
Dada la expresión booleana $(x \wedge (\overline{y} \vee z)) \vee y$, determinar un circuito lógico que la represente.

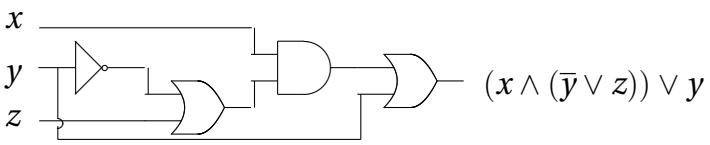
$\overline{\mathbf{y}} \vee \mathbf{z}$.



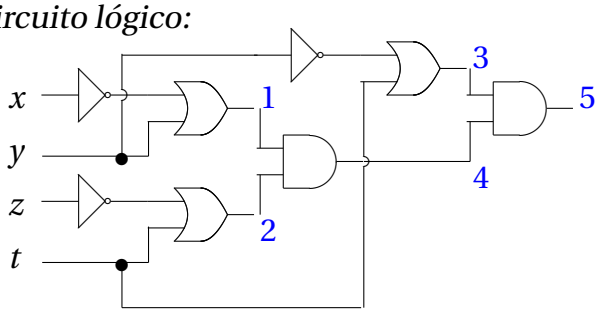
$\mathbf{x} \wedge (\overline{\mathbf{y}} \vee \mathbf{z})$.



$(\mathbf{x} \wedge (\overline{\mathbf{y}} \vee \mathbf{z})) \vee \mathbf{y}$.



Ejercicio. 21.3.
Considerar el siguiente circuito lógico:



y determinar cual es el valor que se tiene en cada uno de los puntos marcados con un número.

SOLUCIÓN. Los valores son:

(1) $\overline{x} \vee y$.

(2) $\overline{z} \vee t$.

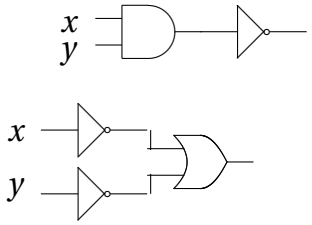
(3) $\overline{y} \vee t$.

(4) $(\overline{x} \vee y) \wedge (\overline{z} \vee t)$.

(5) $(\overline{y} \vee t) \wedge ((\overline{x} \vee y) \wedge (\overline{z} \vee t))$.

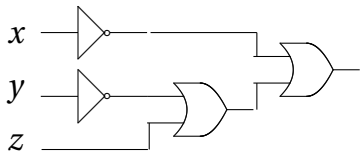
□

Existen circuitos lógicos que para idénticas entradas tienen idénticas salidas, esto es, las expresiones booleanas que representan estos circuitos son equivalentes. cuando esto ocurre diremos que los dos circuitos son **equivalentes**. Veamos un ejemplo de dos circuitos equivalentes, y que representan la ley de de Morgan.

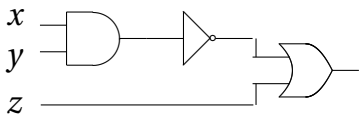


Ejercicio. 21.4.
Probar que los siguientes circuitos con equivalentes.

(a)

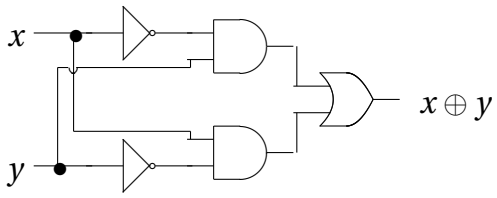


(b)



Ejercicio. 21.5.
Consideramos la expresión booleana $(x \wedge \overline{y}) \vee (\overline{x} \wedge y)$. *Observar que es la expresión booleana equivalentes a la* ***diferencia simétrica*** *de subconjuntos de un conjunto. Dar un circuito lógico que represente esta expresión.*

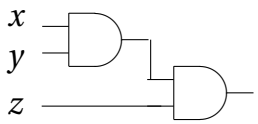
SOLUCIÓN. El diagrama es:



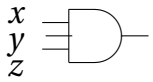
□

Existen otras puertas lógicas, que se pueden construir a partir de las ya introducidas. Las primeras que vamos a estudiar tratan de simplificar el diseño de los circuitos, son la puertas múltiples.

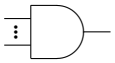
puerta Y múltiple. Si se tiene el siguiente circuito



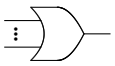
una forma de representarlo es la siguiente,



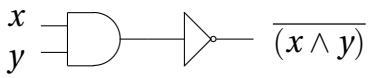
Si tenemos más de tres variables podemos utilizar:



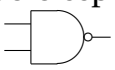
puerta O múltiple. El resultado análogo para la puerta O es la puerta O múltiple:



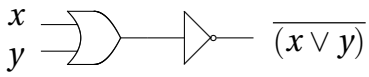
puerta NO Y. En la página 139 se introdujo el operador $\uparrow$, al cual llamábamos **no y**. El circuito lógico que representa a este operador es:



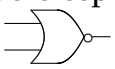
Recordemos que el conjunto $\{\uparrow\}$ es funcionalmente completo, por esta razón este operador es usado con frecuencia y se diseña un símbolo especial para él. Este símbolo es:



puerta NO O. En la página 139 se introdujo el operador $\downarrow$, al cual llamábamos **no o**. El circuito lógico que representa a este operador es:

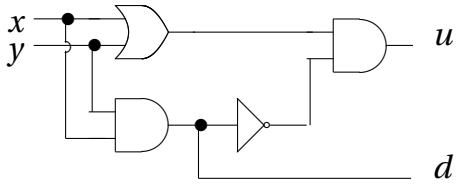


Recordemos que el conjunto $\{\downarrow\}$ es funcionalmente completo, por esta razón este operador es usado con frecuencia y se diseña un símbolo especial para él. Este símbolo es:



Ejemplo. 21.6. (Circuito semisumador.)
Se trata de dar un circuito que admita dos entradas: x e y y dos salidas d y u, de forma que la suma de los bits x e y, considerados como unidades de un sistema binario, sea du, en donde d es la decena y u es la unidad de la suma de x e y.

SOLUCIÓN. El circuito es:

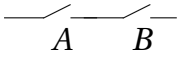


□

22. Circuitos de conmutadores

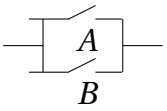
Llamamos **circuito de conmutadores** o circuito de **interruptores** a un circuito en que los dispositivos son interruptores; cada uno de los dispositivos puede estar abierto o cerrado. Cuando un interruptor está abierto se le asigna el valor 1 y si está cerrado se le asigna el valor 0. Las diferentes posiciones de los conmutadores se pueden combinar en la tabla de conmutación del circuito.

Veamos el siguiente ejemplo de circuito de interruptores:



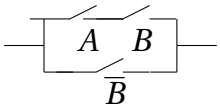
Este circuito permite pasar la corriente sólo cuando A y B están cerrados, por esta razón representa al operador booleano $\wedge$.

El circuito



permite pasar la corriente cuando A ó B está cerrado, por esta razón representa al operador booleano $\vee$.

De esta forma tenemos que cada circuito de conmutadores que representa una expresión booleana, por ejemplo, la expresión booleana $(A \wedge B) \vee \overline{B}$ se representa por el circuito:



La relación entre circuitos de conmutadores y expresiones booleanas es clara.

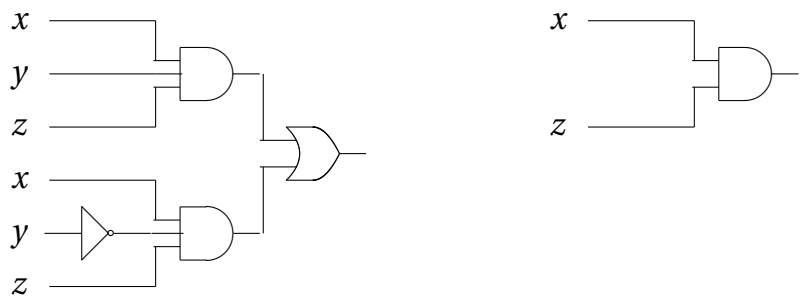
23. Minimización de circuitos

Dos expresiones booleanas equivalentes son fáciles de detectar; ya que basta considerar las expresiones booleanas que ellas definen y comparar sus valores. Es más difícil elegir un representante minimal de entre todas las expresiones equivalentes a una expresión booleana dada.

Ejemplo. 23.1.
Considerar la expresión $xyz + x\bar{y}z$; ésta es la forma disyuntiva de la función booleana que toma el valor 1 sólo cuando $x = y = z = 1$ ó $x = z = 1$ e $y = 0$. Sin embargo existe una expresión booleana equivalente, que es aparentemente más sencilla. Un forma de obtener esta expresión es simplemente aplicar la propiedad distributiva:

$$xyz + x\bar{y}z = x(y + \bar{y})z = xz.$$

¿Cuál de estas dos expresiones anteriores es más sencilla? Observar los circuitos lógicos asociados a cada una de ellas:



Para trabajar en la minimización lo primero es dar un criterio para ver cuando una expresión booleana es *más sencilla* que otra. El criterio es el siguiente: "*una expresión booleana es más sencilla que otra si tiene menos operadores **NO**, **Y**, **O***".

Traducido al caso de circuitos lógicos, tenemos que "*un circuito lógico es más sencillo que otro si tiene menos puertos lógicos y menos entradas en los puertos **Y**, **O***".

23.0.1. Importancia del cálculo de expresiones mínimas

La razón, amén de la economía que produce en las expresiones, la importancia del cálculo de expresiones mínimas estriba, por ejemplo, en la construcción de circuitos integrados, en los que cada puerta lógica tiene un coste en dinero y en tiempo. Por esto reducir su número es importante. El otro tema importante que sería el poder comparar expresiones booleanas para ver si son iguales, lo tenemos resuelto, ya que la forma normal disyuntiva o la forma normal

conjuntiva con únicas, y por lo tanto, calculando estas formas, siempre podemos saber si dos expresiones booleanas son o no iguales.

23.1. Primer procedimiento de minimización: Diagramas de Karnaugh

Todos los procesos de minimización se basan en encontrar términos que puedan combinarse entre sí para producir una expresión más sencilla, si ello es posible. Considerar el Ejemplo 23.1.. Por esta razón cada uno de los términos debería tener el mayor número de literales, y es por eso que vamos a partir de la forma normal disyuntiva de la función booleana.

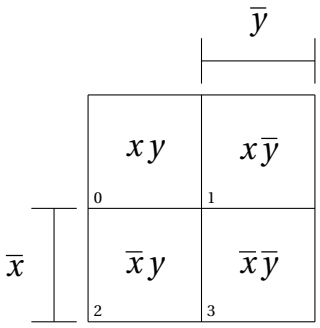
Ejemplo. 23.2.
La expresión $xy + \overline{x}\,\overline{z}$ y la expresión $yx + y\overline{z} + \overline{x}\,\overline{z}$ representan a la misma función booleana. Sin embargo $yx + y\overline{z} + \overline{x}\ \overline{z}$ no tiene términos que se puedan combinar para producir una expresión más sencilla. La forma normal disyuntiva de esta función es: $xyz + xy\overline{z} + \overline{x}y\overline{z} + \overline{x}\,\overline{y}\,\overline{z}$.

Ejercicio. 23.3.
Comprobar, mediante las tablas de verdad, que las tres expresiones anteriores representan a la misma función booleana.

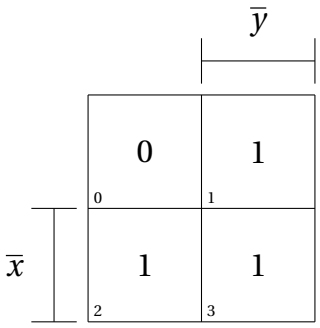
Como ya hemos mencionado nuestro punto de inicio va a ser la forma normal disyuntiva de la función booleana. El método a seguir se basa en estudiar, de forma independiente, cada uno de las casos que se presentan.

23.1.1. Caso de dos variables: x e y

En este caso tenemos cuatro posibles minitérminos: xy, $\overline{x}y$, $x\overline{y}$ y $\overline{x}\,\overline{y}$, que podemos representar en el siguiente diagrama:



Si un minitérmino aparece en la expresión entonces en la casilla correspondiente ponemos un "1", y si no aparece ponemos un "0". Por ejemplo, si consideramos la expresión $f = x\overline{y} + \overline{x}y + \overline{x}\,\overline{y}$, entonces el **diagrama de Karnaugh** es:



Dos casillas se llaman **adyacentes** si los minitérminos que representan difieren en un literal; en este caso si están en la misma fila o en la misma columna del diagrama de Karnaugh.

Se observa que si tenemos casillas adyacentes en las que hay "1", entonces podemos hacer una **reducción**. En el ejemplo anterior los siguientes pares son casillas adyacentes:

2 y [3] y

1 y [3].

La pareja $([2],[3])$ produce la reducción:

$$x\overline{y}+\overline{x}y+\overline{x}\,\overline{y}=x\overline{y}+\overline{x}(y+\overline{y})=x\overline{y}+\overline{x}.$$

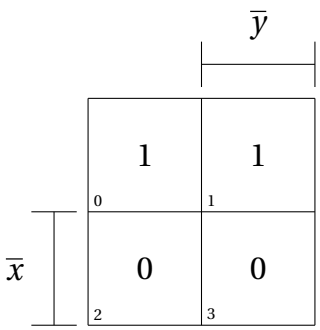
Podemos continuar como sigue:

$$x\overline{y}+\overline{x}=xy+\overline{x}+x\overline{x}+\overline{x}\,\overline{y}=(x+\overline{x})(\overline{y}+\overline{x})=\overline{y}+\overline{x}=\overline{x}+\overline{y}.$$

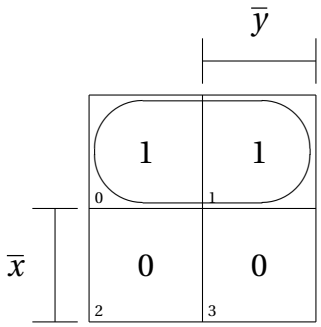
Por lo tanto $\overline{x}+\overline{y}$ es una expresión equivalente a $f=x\overline{y}+\overline{x}y+\overline{x}\,\overline{y}$ y resulta ser más sencilla.

Ejercicio. 23.4.
Dada la expresión booleana $f=xy+x\overline{y}$, determinar una expresión equivalente más sencilla.

SOLUCIÓN. Se escribe el diagrama de Karnaugh de $f=xy+x\overline{y}$, que resulta ser:



A continuación se buscan casillas adyacentes, en este caso:



Tenemos entonces la siguiente reducción:

$$f = xy + x\overline{y} = x(y + \overline{y}) = x.$$

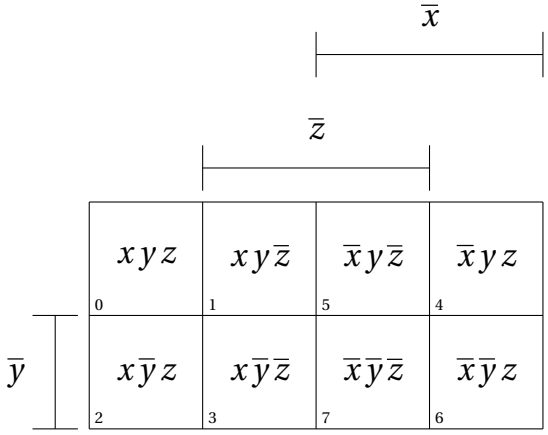
□

Observar que se trata de buscar casillas adyacentes y utilizarlas para reducir la expresión dada.

Ejercicio. 23.5.
Dada la expresión booleana $f = xy + x\overline{y} + \overline{x}y + \overline{x}\,\overline{y}$, determinar una expresión equivalente más sencilla.

23.1.2. Caso de tres variables: x, y y z

Para poder representar todos los minitérminos, en este caso, recordar que son exactamente ocho, vamos a utilizar el siguiente diagrama:



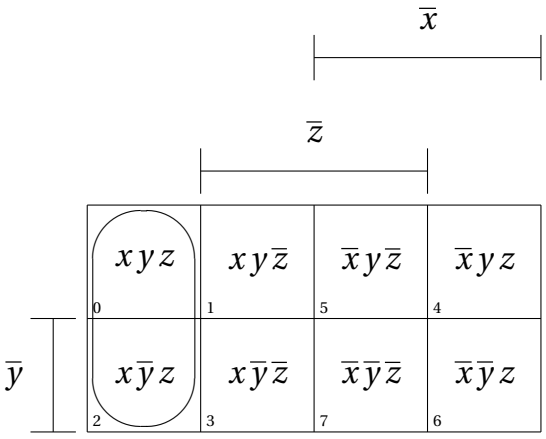
En donde la columna cuarta se continua a la derecha con la columna primera y la primera

se continua a la izquierda con la columna cuarta. (La forma geométrica espacial sería un cilindro.)

Al igual que antes, dada una expresión booleana, en cada casilla colocamos un "1"ó un "0"según que el minitérmino aparezca o no en dicha expresión. Una vez completo el diagrama, hacemos uso de la siguiente observación: si existen casillas adyacentes con "1", entonces podemos combinar los minitérminos para reducir la expresión.

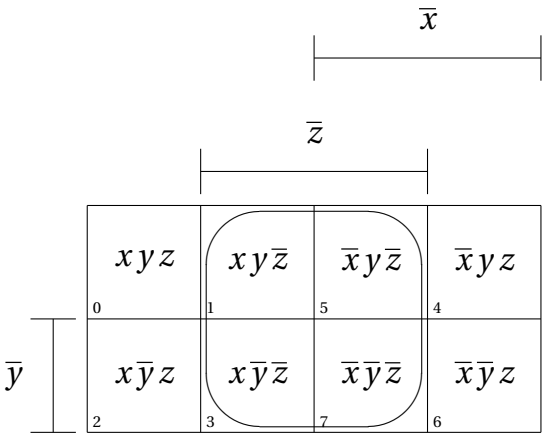
En este caso tenemos varios tipos de casillas adyacentes:

(1) Tipo vertical.

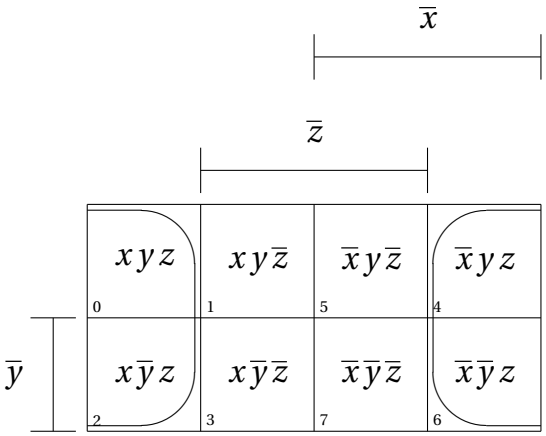


o cualquiera otra columna. En el caso de la figura tenemos la reducción: $xyz + x\overline{y}z = xz$.

(2) Tipo vertical doble.

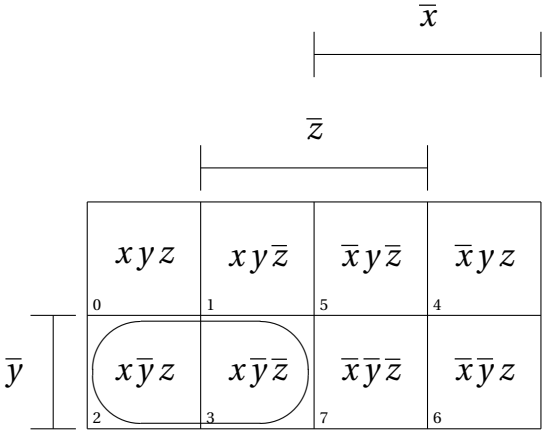


o cualquiera que agrupe dos columnas contiguas. En el caso de la figura tenemos la reducción: $xy\overline{z} + \overline{x}yz + x\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} = \overline{z}$. También vale

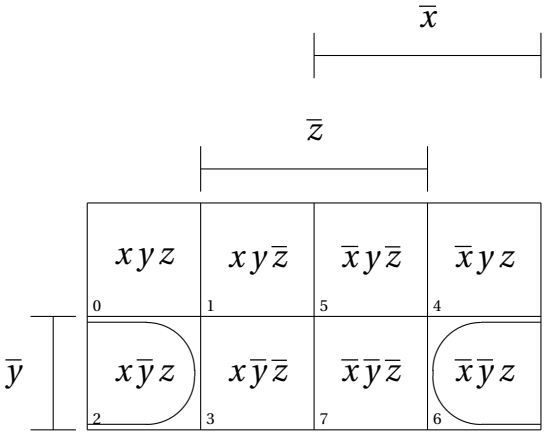


para la que tenemos la reducción: $xyz + \overline{x}yz + x\overline{y}z + \overline{x}\,\overline{y}z = z$.

(3) Tipo horizontal.

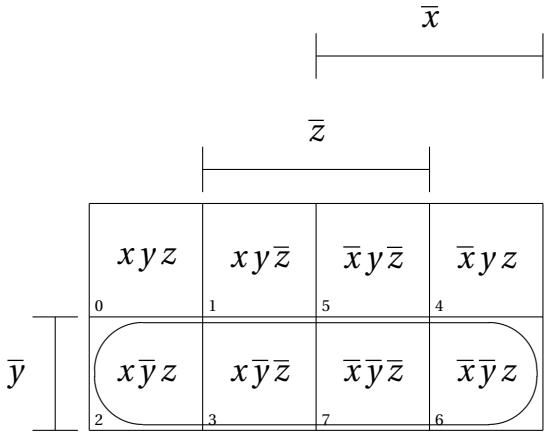


o cualesquiera otras dos casillas contiguas en la misma fila. En el caso de la figura tenemos la reducción: $x\overline{y}z + x\overline{y}\,\overline{z} = x\overline{z}$. También tenemos



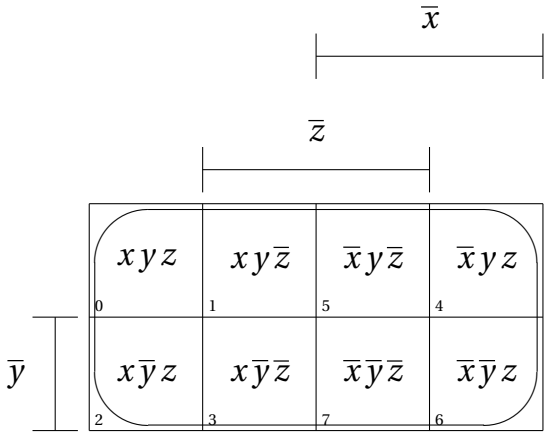
que proporciona la reducción: $x\overline{y}z + \overline{x}\,\overline{y}z = \overline{y}z$.

(4) Tipo horizontal doble.



En el caso de la figura tenemos la reducción: $x\overline{y}z + x\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} + x\overline{y}\,\overline{z} = \overline{y}$.

(5) El total.



En el caso de la figura tenemos la reducción: $xyz+xy\overline{z}+x\overline{y}z+x\overline{y}\,\overline{z}+\overline{x}yz+\overline{x}y\,\overline{z}+\overline{x}\,\overline{y}\,z+\overline{x}\overline{y}\,\overline{z} = 1$.

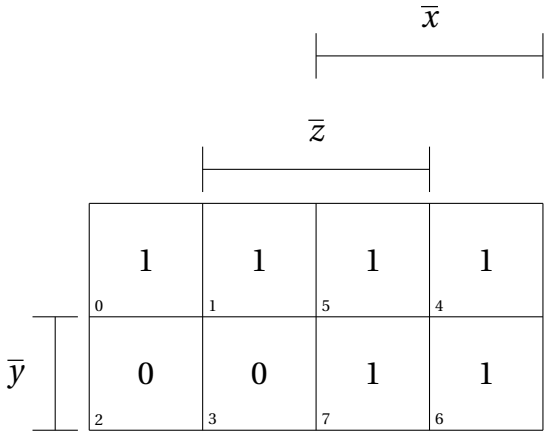
23.1.3. ¿Cómo actuar el en caso de tres variables?

Llamamos a cada una de las posibles agrupaciones de "1"en el diagrama de Karnaugh, que aparecen en la lista anterior, un **bloque**. Cada bloque produce una reducción; llamamos **implicante** a cada una de estas reducciones. Por ejemplo, en la lista anterior, en el punto (1) el bloque vertical nos daba como resultado de la reducción xz; éste es el implicante en este caso.

Un **implicante primo** es aquel para el que el bloque de "1"que lo define no está contenido, propiamente, en otro bloque de "1", esto es, es maximal.

Un **implicante esencial** es aquel que es primo y que contiene un "1"que no contiene ningún otro bloque maximal.

Ejemplo. 23.6.
Consideremos la expresión $f = xyz + xy\overline{z} + \overline{x}yz + \overline{x}y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{x}\overline{y}\,\overline{z}$, cuyo diagrama de Karnaugh es:

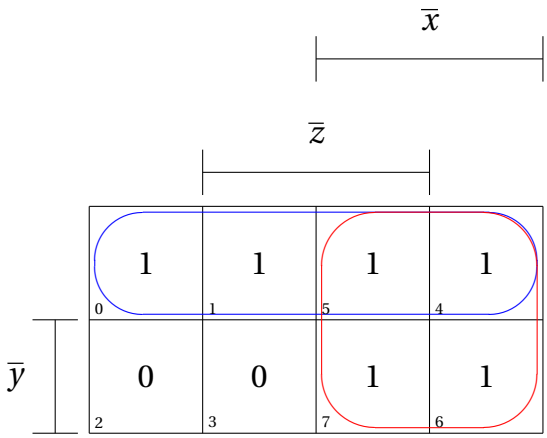


Tenemos los siguientes implicantes:

(1) Con dos casillas: xy, $y\overline{z}$, $\overline{x}y$, yz, $\overline{x}\,\overline{y}$ (horizontales), $\overline{x}\,\overline{z}$, $\overline{x}z$ (verticales).

(2) Con cuatro casillas: y (horizontal), $\overline{x}$ (vertical).

Como consecuencia ningún implicante con bloque de dos casillas es primo, y los de cuatro casillas, y y $\overline{x}$, son primos y además esenciales.



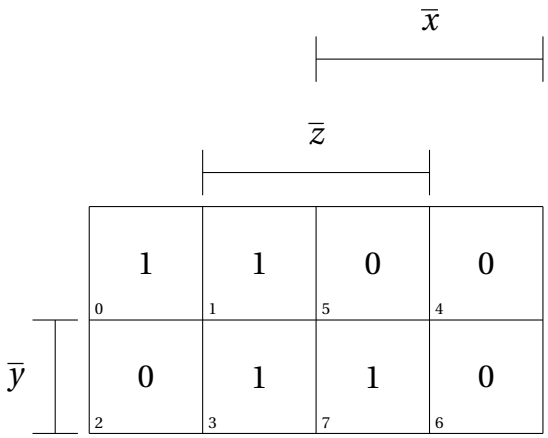
La forma de reducir la expresión es utilizar los implicantes esenciales. Veamos este ejemplo:

$$\begin{aligned}
&xyz + xy\overline{z} + \overline{x}yz + \overline{x}y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{xy}\,\overline{z} \\
&= xyz + xy\overline{z} + \overline{x}yz + \overline{x}y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{xy}\,\overline{z} \\
&= y + \overline{x}\,\overline{y}\,z + \overline{xy}\,\overline{z} \\
&= y + \overline{x}\,\overline{y} \\
&= (y + \overline{x})(y + \overline{y}) \\
&= y + \overline{x}.
\end{aligned}$$

Utilizando el otro implicante esencial se tiene:

$$\begin{aligned}
&\overline{x}yz + \overline{x}y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{xy}\,\overline{z} \\
&= xyz + xy\overline{z} + \overline{x}yz + \overline{x}y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{xy}\,\overline{z} \\
&= xyz + xy\overline{z} + \overline{x} \\
&= xy(z + \overline{z}) + \overline{x} \\
&= xy + \overline{x} \\
&= (x + \overline{x})(y + \overline{x}) = y + \overline{x}.
\end{aligned}$$

Ejemplo. 23.7.
Se considera la expresión booleana $x\,y\,z + x\,y\,\overline{z} + x\,\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z}$, cuyo diagrama de Karnaugh es:



Tenemos los siguientes implicantes:

(1) Con dos casillas: $x\,y$, $\overline{y}\,\overline{z}$ (horizontales), $x\,\overline{z}$ (verticales).

Todos ellos son primos, ya que sus bloques son maximales, pero $x\,\overline{z}$ no es esencial, mientras que los otros dos sí lo son.

Si hacemos la reducción utilizando el implicante no esencial, el resultado es:

$$\begin{aligned}
&x\,y\,z + x\,y\,\overline{z} + x\,\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x\,y\,z + x\,y\,\overline{z} + x\,\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x\,y\,z + x\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x(y\,z + \overline{z}) + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x(y + \overline{z}) + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x\,y + x\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x\,y + (x + \overline{x}\,\overline{y})\overline{z} \\
=\,&x\,y + (x + \overline{y})\overline{z} \\
=\,&x\,y + x\,\overline{z} + \overline{y}\,\overline{z}.
\end{aligned}$$

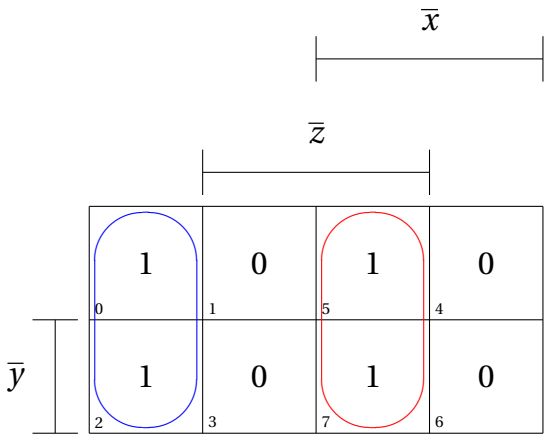
Si hacemos la reducción utilizando los implicantes esenciales, el resultado es:

$$\begin{aligned}
&x\,y\,z + x\,y\,\overline{z} + x\,\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x\,y\,z + x\,y\,\overline{z} + x\,\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\
=\,&x\,y + \overline{y}\,\overline{z} \\
=\,&x\,y + \overline{y}\,\overline{z}.
\end{aligned}$$

Este ejemplo nos advierte de que para comenzar la reducción es conveniente utilizar los implicantes esenciales en primer lugar, y una vez realizada la primera reducción se procede con las siguientes dibujando el nuevo diagrama de Karnaugh.

Ejercicio. 23.8.
Dada la expresión booleana $f = x\,y\,z + x\,\overline{y}\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z}$, determinar una expresión equivalente más sencilla.

SOLUCIÓN. Primero se dibuja el diagrama de Karnaugh y se determinan los bloques.



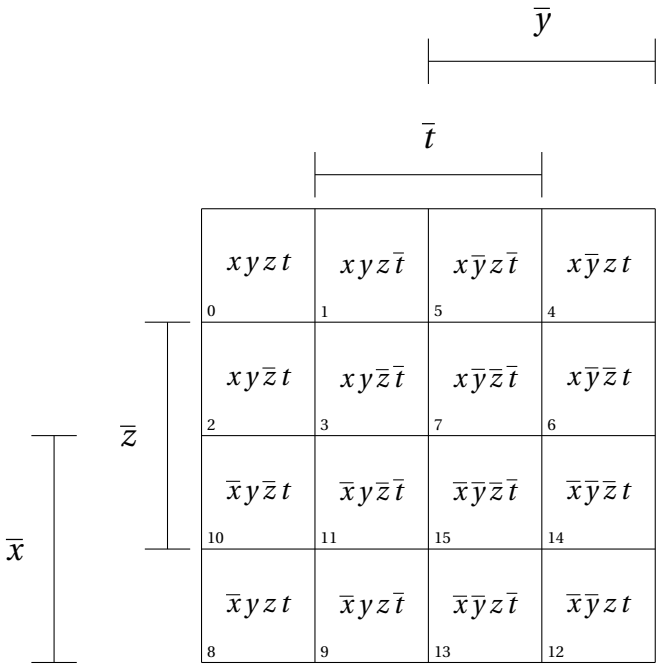
A continuación se hacen las reducciones:

$$\begin{aligned} & x\,y\,z + x\,\overline{y}\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\ = & x\,y\,z + x\,\overline{y}\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\ = & x\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z} \\ = & x\,z + \overline{x}\,\overline{z} \\ = & x\,z + \overline{x}\,\overline{z} \end{aligned}$$

□

23.1.4. Caso de cuatro variables: x, y, z y t

Para poder representar todos los minitérminos, en este caso, recordar que son exactamente dieciseis, vamos a utilizar el siguiente diagrama:

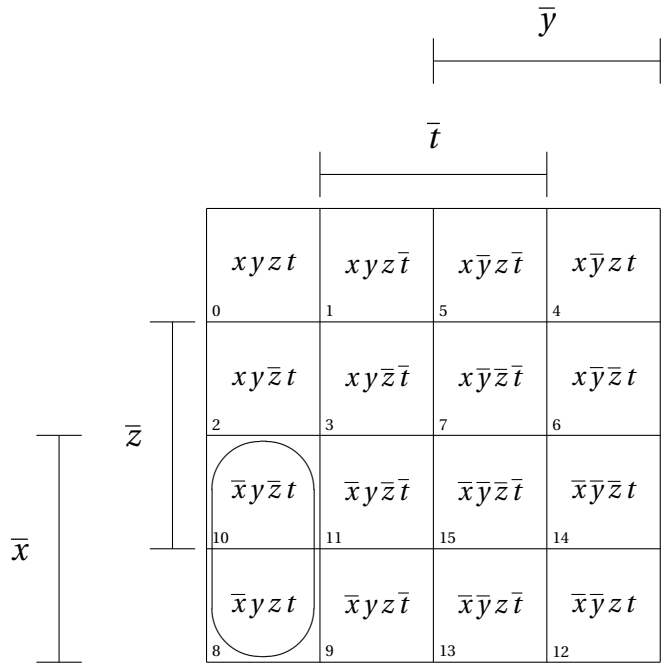


En donde la columna cuarta se continua a la derecha con la columna primera, la primera se continua a la izquierda con la columna cuarta y lo mismo para las filas. (La forma geométrica espacial sería una esfera.)

Al igual que antes, dada una expresión booleana, en cada casilla colocamos un "1"ó un "0"según que el minitérmino aparezca o no en dicha expresión. Una vez completo el diagrama, hacemos uso de la siguiente observación: si existen casillas adyacentes con "1", entonces podemos combinar los minitérminos para reducir la expresión.

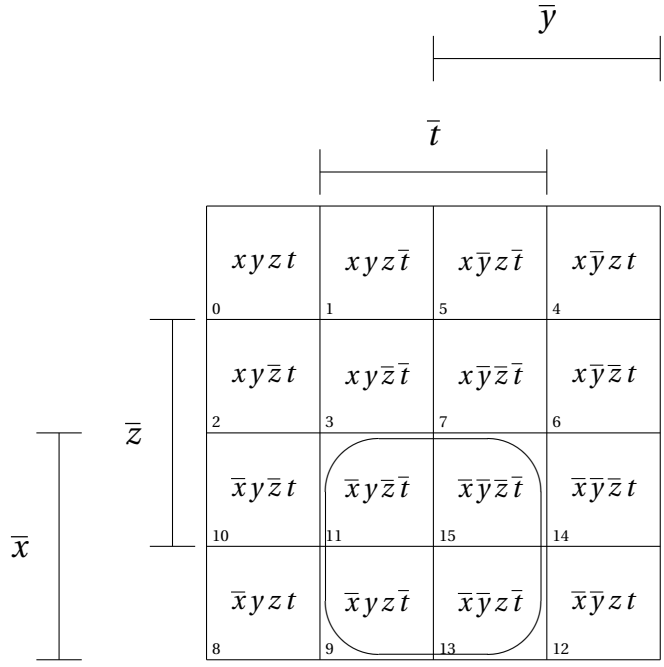
En este caso tenemos varios tipos de casillas adyacentes:

(1) Tipo vertical.

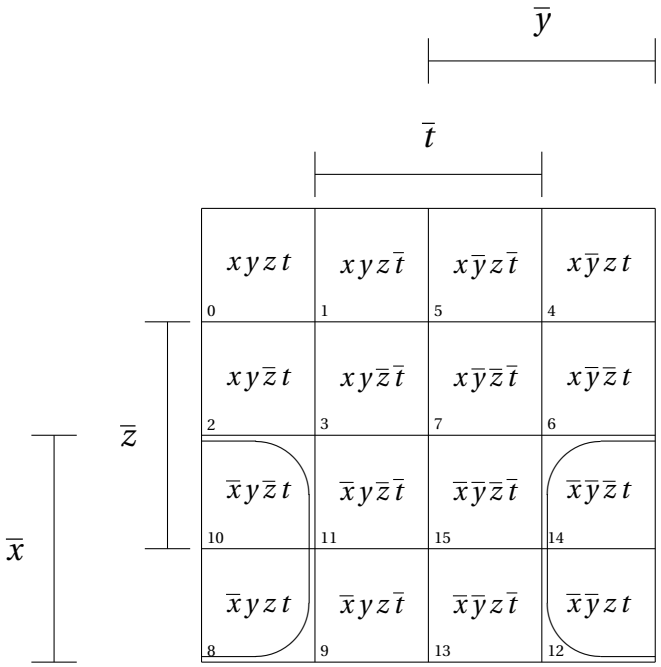


o cualquier par de casillas contiguas en otra columna. En el caso de la figura tenemos la reducción: $\overline{x}y\overline{z}t + \overline{x}yzt = xyt$.

(2) Tipo vertical doble.

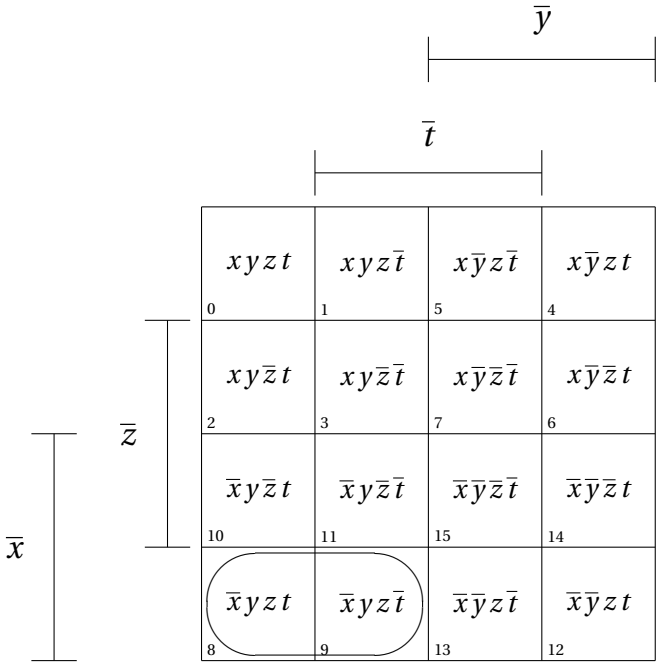


o cualquiera que agrupe dos columnas contiguas. En el caso de la figura tenemos la reducción: $\overline{x}y\overline{z}\overline{t} + \overline{x}\overline{y}\overline{z}\overline{t} + \overline{x}yz\overline{t} + \overline{x}\overline{y}z\overline{t} = \overline{x}y\overline{t} + \overline{x}\overline{y}\overline{t} = \overline{x}\overline{t}$. También vale

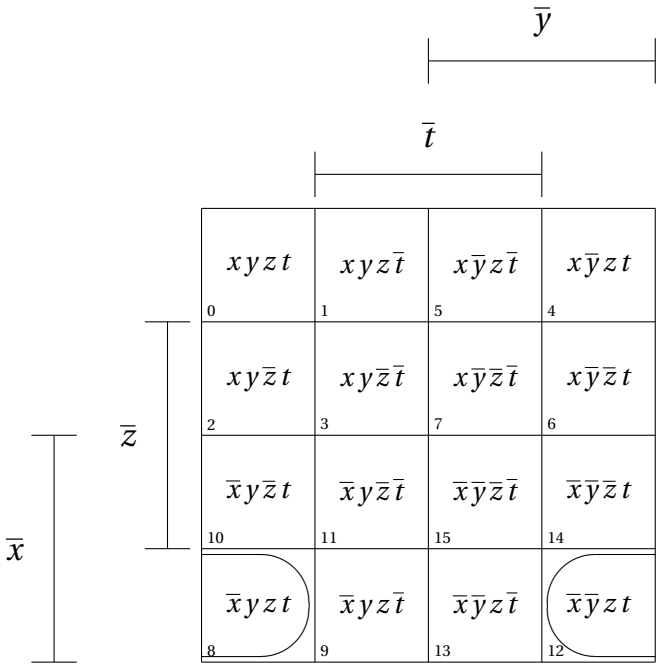


para la que tenemos la reducción: $\overline{x}\,y\,\overline{z}\,t+\overline{x}\,\overline{y}\,\overline{z}\,t+\overline{x}\,y\,z\,t+\overline{x}\,\overline{y}\,z\,t=\overline{x}\,y\,t+\overline{x}\,\overline{y}\,t=\overline{x}\,t$.

(3) Tipo horizontal.

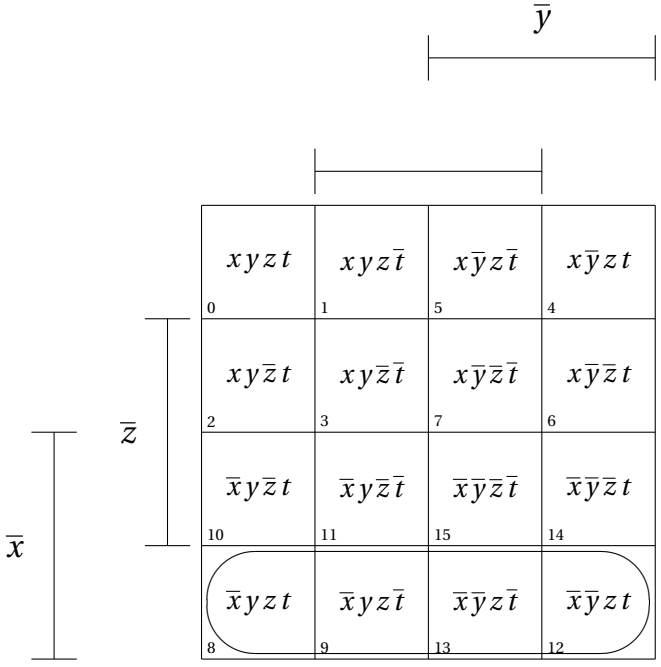


o cualesquiera otras dos casillas contiguas en la misma fila. En el caso de la figura tenemos la reducción: $\overline{x}\,y\,z\,t+\overline{x}\,y\,z\,\overline{t}=\overline{x}\,y\,z$. También tenemos



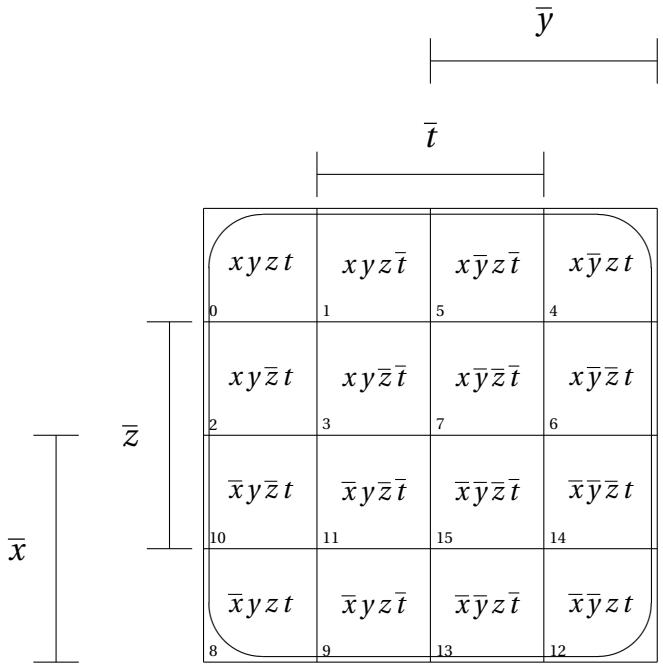
que proporciona la reducción: $\overline{x}yzt + \overline{x}\overline{y}zt = \overline{x}zt$.

(4) Tipo horizontal/vertical doble.



En el caso de la figura tenemos la reducción: $\overline{x}yzt + \overline{x}yz\overline{t} + \overline{x}\overline{y}z\overline{t} + \overline{x}\overline{y}zt = \overline{x}z$.

(5) El total.



En el caso de la figura tenemos la reducción: $xyzt + xyz\overline{t} + x\overline{y}z\overline{t} + x\overline{y}zt + xy\overline{z}t + xy\overline{z}\overline{t} + x\overline{y}\overline{z}\overline{t} + x\overline{y}\overline{z}t + \overline{x}y\overline{z}t + \overline{x}y\overline{z}\overline{t} + \overline{x}\overline{y}\overline{z}\overline{t} + \overline{x}\overline{y}\overline{z}t + \overline{x}yzt + \overline{x}yz\overline{t} + \overline{x}\overline{y}z\overline{t} + \overline{x}\overline{y}zt = 1$.

23.1.5. ¿Cómo actuar el en caso de cuatro variables?

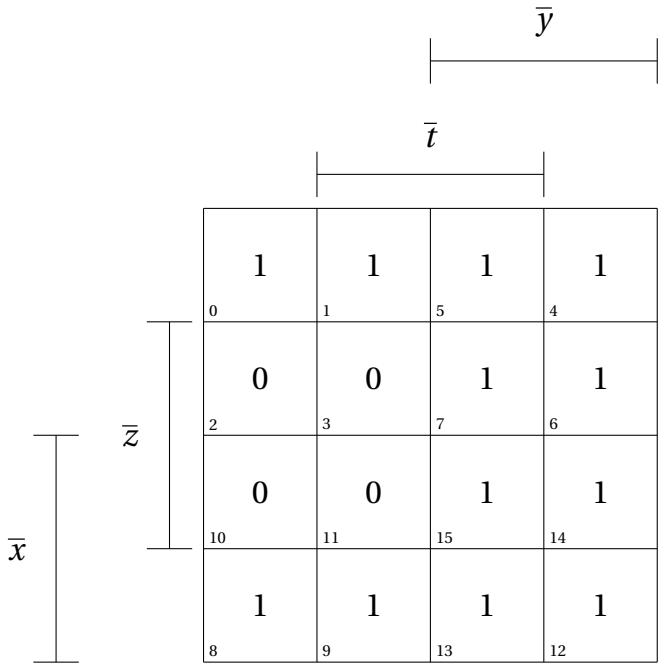
Seguimos el mismo proceso que en el caso de tres variables.

Llamamos a cada una de las posibles agrupaciones de "1.en el diagrama de Karnaugh, que aparecen en el lista anterior, un **bloque**. Cada bloque produce una **reducción**. Llamamos **implicante** a cada una de estas reducciones. Por ejemplo, en la lista anterior, en el punto (1) el bloque vertical nos daba como resultado de la reducción xzt; éste es el implicante en este caso.

Un **implicante primo** es aquel para el que el bloque de "1"que lo define no está contenido, propiamente, en otro bloque de "1", esto es, es maximal.

Un **implicante esencial** es aquel que es primo y que contiene un "1"que no contiene ningún otro bloque maximal.

Ejemplo. 23.9.
Consideremos la expresión $f = xyzt + xyz\overline{t} + x\overline{y}z\overline{t} + x\overline{y}zt + x\overline{y}\overline{z}\overline{t} + x\overline{y}\overline{z}t + \overline{x}\overline{y}\overline{z}\overline{t} + \overline{x}\overline{y}\overline{z}t + \overline{x}yzt + \overline{x}yz\overline{t} + \overline{x}\overline{y}z\overline{t} + \overline{x}\overline{y}zt$, cuyo diagrama de Karnaugh es:

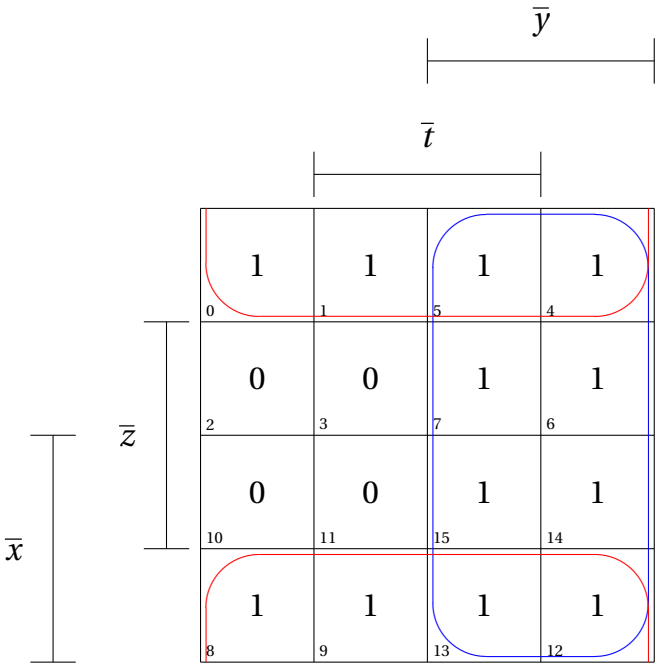


Tenemos los siguientes implicantes:

(1) Con cuatro casillas: xz, $\overline{x}z$ (horizontales), $\overline{y}\,\overline{t}$, $\overline{y}t$ (verticales).

(2) Con ocho casillas: $\overline{y}$, z

Como consecuencia los implicantes esenciales son los que corresponden a $\overline{y}$ y z.



Vamos a reducir la expresión utilizando los implicantes esenciales. Veamos las dos posibilidades:

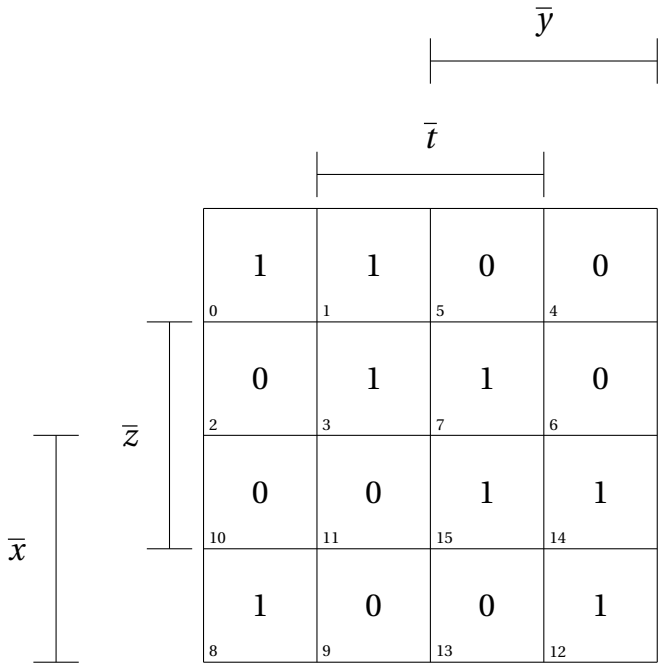
$$\begin{aligned}
&xyzt + xyz\overline{t} + x\overline{y}z\overline{t} + x\overline{y}zt + x\overline{y}\,\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}t + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\overline{y}\,\overline{z}t + \\
&\overline{x}yzt + \overline{x}yz\,\overline{t} + \overline{x}\,\overline{y}\,z\overline{t} + \overline{x}\,\overline{y}zt \\
&= xyzt + xyz\overline{t} + x\overline{y}z\overline{t} + x\overline{y}zt + x\overline{y}\,\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}t + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\overline{y}\,\overline{z}t + \\
&\overline{x}yzt + \overline{x}yz\,\overline{t} + \overline{x}\,\overline{y}\,z\overline{t} + \overline{x}\,\overline{y}zt \\
&= xyzt + xyz\overline{t} + \overline{x}yzt + \overline{x}yz\,\overline{t} + \overline{y} \\
&= (xt + x\overline{t} + \overline{x}t + \overline{x}\,\overline{t})yz + \overline{y} \\
&= yz + \overline{y} \\
&= (y + \overline{y})(z + \overline{y}) \\
&= z + \overline{y}.
\end{aligned}$$

Utilizando el otro implicante esencial se tiene:

$$\begin{aligned}
&xyzt + xyz\overline{t} + x\overline{y}z\overline{t} + x\overline{y}zt + x\overline{y}\,\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}t + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\overline{y}\,\overline{z}t + \\
&\overline{x}yzt + \overline{x}yz\,\overline{t} + \overline{x}\,\overline{y}\,z\overline{t} + \overline{x}\,\overline{y}zt \\
&= xyzt + xyz\overline{t} + x\overline{y}z\overline{t} + x\overline{y}zt + x\overline{y}\,\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}t + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\overline{y}\,\overline{z}t + \overline{x}yzt + \\
&\overline{x}yz\,\overline{t} + \overline{x}\,\overline{y}\,z\overline{t} + \overline{x}\,\overline{y}zt \\
&= x\overline{y}\,\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}t + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\overline{y}\,\overline{z}t + z \\
&= (x\overline{t} + xt + \overline{x}\,\overline{t} + \overline{x}t)\overline{y}\,\overline{z} + z \\
&= \overline{y}\,\overline{z} + z \\
&= (\overline{y} + z)(\overline{z} + z) \\
&= \overline{y} + z.
\end{aligned}$$

Ejemplo. 23.10.
Se considera la expresión booleana $x\,y\,z\,t + x\,y\,z\,\overline{t} + x\,y\,\overline{z}\,\overline{t} + x\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}\,t + \overline{x}\,y\,z\,t + \overline{x}\,\overline{y}\,z\,t$,

cuyo diagrama de Karnaugh es:

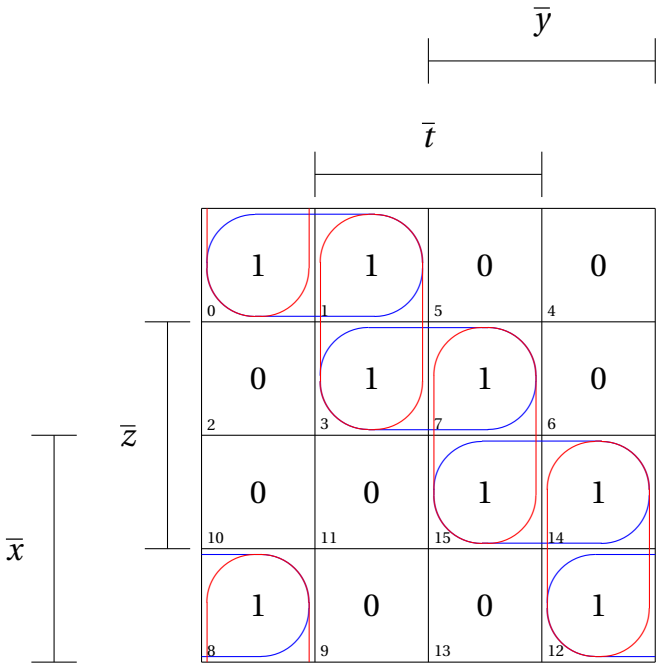


Tenemos los siguientes implicantes, todos de dos casillas:

(1) xyz, $x\overline{z}\,\overline{t}$, $\overline{x}\,\overline{y}\,\overline{z}$, $\overline{x}zt$ (horizontales).

(2) yzt, $xy\overline{t}$, $\overline{y}\,\overline{z}\,\overline{t}$, $\overline{x}\,\overline{y}t$ (verticales).

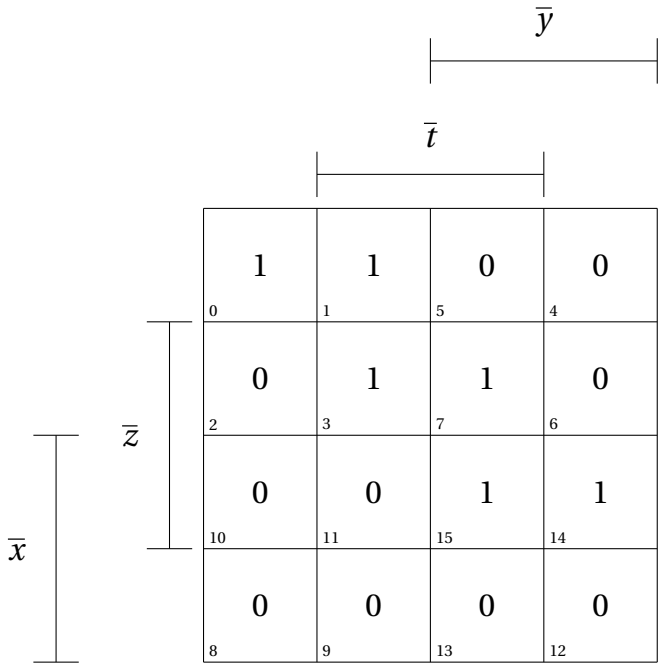
Todos ellos son primos, ya que sus bloques son maximales, pero ninguno es esencial.



Hacemos la reducción utilizando los implicantes horizontales: xyz, $x\overline{z}\,\overline{t}$, $\overline{x}\,\overline{y}\,\overline{z}$, $\overline{x}zt$.

$$\begin{aligned} & xyzt + xyz\overline{t} + xy\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}t + \overline{x}yzt + \overline{x}\,\overline{y}zt \\ = {} & xyz + x\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z} + \overline{x}zt \\ = {} & (xyz + \overline{x}\,\overline{y}\,\overline{z}) + (x\overline{z}\,\overline{t} + \overline{x}zt). \end{aligned}$$

Ejemplo. 23.11.
Se considera la expresión booleana $xyzt + xyzt + xy\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}t$, cuyo diagrama de Karnaugh es:

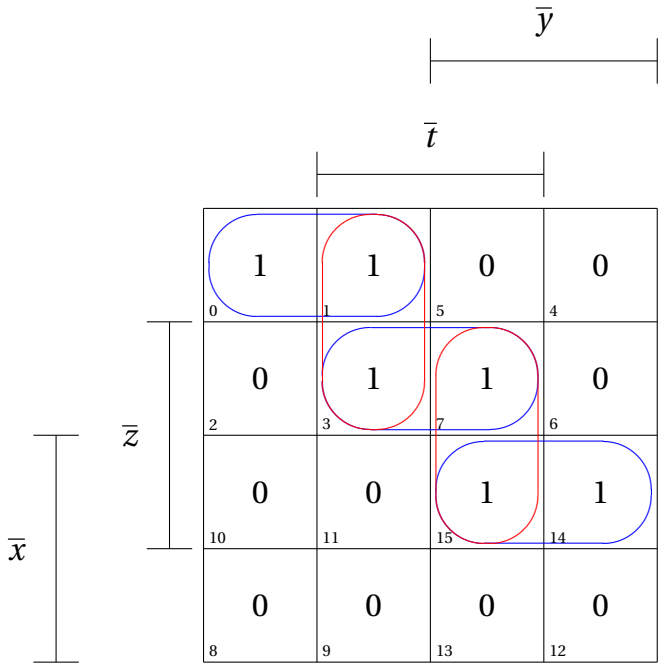


Tenemos los siguientes implicantes, todos de dos casillas:

(1) (horizontales: xyz, $x\overline{z}\,\overline{t}$, $\overline{x}\,\overline{y}\,\overline{z}$)

(2) (verticales: $xy\overline{t}$, $\overline{y}\,\overline{z}\,\overline{t}$).

Todos ellos son primos, ya que sus bloques son maximales. De ellos xyz y $\overline{x}\,\overline{y}\,\overline{z}$ son esenciales.

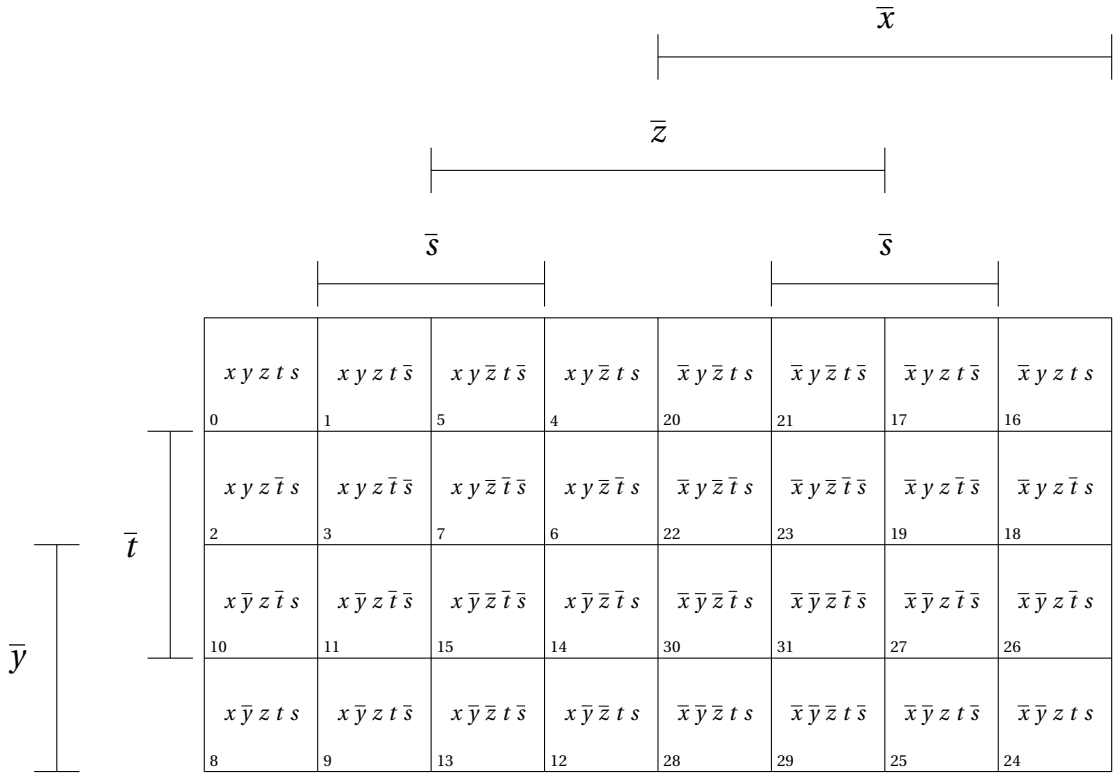


Hacemos la reducción utilizando los implicantes horizontales: xyz, $x\overline{z}\,\overline{t}$, $\overline{x}\,\overline{y}\,\overline{z}$.

$$\begin{aligned} & xyzt + xyzt + xy\overline{z}\,\overline{t} + x\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z}t \\ = {} & xyz + x\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z} \\ = {} & xyz + \overline{x}\,\overline{y}\,\overline{z} + x\overline{z}\,\overline{t} \end{aligned}$$

23.1.6. Caso de cinco variables: x, y, z, t y s

Para poder representar todos los minitérminos, en este caso, recordar que son exactamente treinta y dos, vamos a utilizar el siguiente diagrama:



En donde la columna octava se continua a la derecha con la columna primera y la primera se continua a la izquierda con la columna octava y lo mismo para las filas primera y cuarta. (La forma geométrica espacial sería una esfera.)

Determinar en este caso los bloques y los implicantes.

Observar que las filas y columnas se construyen de forma que de una a la contigua se produce un cambio de un literal; esta forma de ordenación es debida a Gray. Ejemplos de ordenación son los siguientes:

(1) 1,0.

(2) 11,10,00,01.

(3) 111,110,100,101,001,000,010,011.

(4) 1111,1110,1100,1101,1001,1000,1010,1011,
0011,0010,0000,0001,0101,0100,0110,0111.

(5) ...

El problema de este método es que no se puede automatizar. Una mejora la proporciona el método de minimalización de Quine–McCluskey.

23.2. Segundo procedimiento de minimización: Método de Quine-McCluskey

Este método es más fácil de automatizar. Se consideran los términos, a cada término se le asocia una sucesión de 0, 1 y el símbolo especial "–"; si aparece el literal x se escribe "1", si aparece el literal $\overline{x}$ se escribe "0", y si no aparecen los literales x y $\overline{x}$, se escribe "–". Es claro que para poder escribir la sucesión necesitamos previamente establecer un orden entre las variables. Así si las variables son x, y, z y t, entonces al término $x\,y\,\overline{z}\,t$ le asociamos la sucesión "1101"; y al término $x\overline{yz}$ le asociamos "100–". Observar que si tenemos sólo tres variables x, y y z, entonces al término $x\overline{yz}$ le asociamos la sucesión "100", al término y le asociamos "– 1 –", y al término $\overline{x}$ le asociamos "0– –".

Se combinan todas las parejas de literales que permiten una reducción, esto es, aquellas que se diferencien en un solo literal ó en un único símbolo "0", "1"ó "–". Los resultados obtenidos se vuelven a combinar entre sí, aquellos que tengan los mismos literales. Este proceso se repite hasta que no es posible hacer más reducciones.

Los resultados obtenidos se pueden escribir en una tabla para hacerlos más accesibles.

Una vez realizadas todas las reducciones posibles, aquellos términos que se han utilizado para reducciones pueden no considerarse, pues utilizaremos las reducciones, y bastará considerar sólo aquellos que no se hayan utilizado para reducciones.

El problema es cuáles de ellos son necesarios. Para esto completamos otra tabla. En la cabecera de cada columna se escriben los minitérminos, y en la cabecera de las filas las reducciones no utilizadas. En cada fila con cabecera un término no utilizado se marcan las casillas correspondientes a los minitérminos que se han utilizado para obtenerlos. Finalmente para obtener la expresión mínima basta considerar los términos no utilizados de forma que se cubran todos los minitérminos.

Veamos un ejemplo.

Ejemplo. 23.12.
Se considera la función booleana f con forma normal disyuntiva $xy\overline{z}+x\overline{y}\,\overline{z}+\overline{x}y\overline{z}+\overline{x}\,\overline{y}z+\overline{x}\,\overline{y}\,\overline{z}$.

SOLUCIÓN. Construimos la tabla de Quine–McCluskey:

1	$xy\overline{z}$	1 1 0	$(1,2)$	1 − 0	$x\overline{z}$	$((1,2),(3,5))$	− − 0	$\overline{z}$
2	$x\overline{y}\,\overline{z}$	1 0 0	$(1,3)$	− 1 0	$y\overline{z}$	$((1,3),(2,5))$	− − 0	
3	$\overline{x}y\overline{z}$	0 1 0	$(2,5)$	− 0 0	$\overline{y}\,\overline{z}$			
4	$\overline{x}\,\overline{y}z$	0 0 1	$(3,5)$	0 − 0	$\overline{x}\,\overline{z}$			
5	$\overline{x}\,\overline{y}\,\overline{z}$	0 0 0	$(4,5)$	0 0 −	$\overline{x}\,\overline{y}$			

Ahora construimos la tabla que relaciona los minitérminos con los términos no usados:

	$xy\overline{z}$	$x\overline{y}\,\overline{z}$	$\overline{x}y\overline{z}$	$\overline{x}\,\overline{y}z$	$\overline{x}\,\overline{y}\,\overline{z}$
$(1,2,3,5)=\overline{z}$	X	X	X		X
$(4,5)=\overline{x}\,\overline{y}$				X	X

Como consecuencia la forma mínima es: $\overline{x}\,\overline{y}+\overline{z}$. □

Ejercicio. 23.13.
Dada la función booleana f con forma normal disyuntiva $xyzt+xyz\overline{t}+xy\overline{z}\,\overline{t}+x\overline{y}\,\overline{z}\,\overline{t}+\overline{x}\,\overline{y}\,\overline{z}\,\overline{t}+\overline{x}\,\overline{y}\,\overline{z}t$.

SOLUCIÓN. Construimos la tabla de Quine–McCluskey:

1	$xyzt$	1 1 1 1	$(1,2)$	1 1 1 −	xyz
2	$xyz\overline{t}$	1 1 1 0	$(2,3)$	1 1 − 0	$xy\overline{t}$
3	$xy\overline{z}\,\overline{t}$	1 1 0 0	$(3,4)$	1 − 0 0	$x\overline{z}\,\overline{t}$
4	$x\overline{y}\,\overline{z}\,\overline{t}$	1 0 0 0	$(4,5)$	− 0 0 0	$\overline{y}\,\overline{z}\,\overline{t}$
5	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{t}$	0 0 0 0	$(5,6)$	0 0 0 −	$\overline{x}\,\overline{y}\,\overline{z}$
6	$\overline{x}\,\overline{y}\,\overline{z}t$	0 0 0 1			

Ahora construimos la tabla que relaciona los minitérminos con los términos no usados:

	$xyzt$	$xyz\overline{t}$	$xy\overline{z}\,\overline{t}$	$x\overline{y}\,\overline{z}\,\overline{t}$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{t}$	$\overline{x}\,\overline{y}\,\overline{z}t$
$(1,2)=xyz$	X	X				
$(2,3)=xy\overline{t}$		X	X			
$(3,4)=x\overline{z}\,\overline{t}$			X	X		
$(4,5)=\overline{y}\,\overline{z}\,\overline{t}$				X	X	
$(5,6)=\overline{x}\,\overline{y}\,\overline{z}$					X	X

Como consecuencia la forma mínima es: $xyz+x\overline{z}\,\overline{t}+\overline{x}\,\overline{y}\,\overline{z}$. □

Ejercicio. 23.14.
Dada la función booleana f con forma normal disyuntiva $xyzt+xyz\overline{t}+xy\overline{z}\,\overline{t}+x\overline{y}\,\overline{z}\,\overline{t}+\overline{x}\,\overline{y}\,\overline{z}\,\overline{t}+\overline{x}\,\overline{y}\,\overline{z}t+\overline{x}yzt+\overline{x}\,\overline{y}zt$.

SOLUCIÓN. Construimos la tabla de Quine–McCluskey:

1	$xyzt$	1 1 1 1	$(1,2)$	1 1 1 $-$	xyz
2	$xyz\overline{t}$	1 1 1 0	$(2,3)$	1 1 $-$ 0	$xy\overline{t}$
3	$xy\overline{z}\,\overline{t}$	1 1 0 0	$(3,4)$	1 $-$ 0 0	$x\overline{z}\,\overline{t}$
4	$x\overline{y}\,\overline{z}\,\overline{t}$	1 0 0 0	$(4,5)$	$-$ 0 0 0	$\overline{y}\,\overline{z}\,\overline{t}$
5	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{t}$	0 0 0 0	$(5,6)$	0 0 0 $-$	$\overline{x}\,\overline{y}\,\overline{z}$
6	$\overline{x}\,\overline{y}\,\overline{z}t$	0 0 0 1	$(1,7)$	$-$ 1 1 1	yzt
7	$\overline{x}yzt$	0 1 1 1	$(6,8)$	0 0 $-$ 1	$\overline{x}\,\overline{y}t$
8	$\overline{x}\,\overline{y}zt$	0 0 1 1	$(7,8)$	0 $-$ 1 1	$\overline{x}zt$

Ahora construimos la tabla que relaciona los minitérminos con los términos no usados:

	$xyzt$	$xyz\overline{t}$	$xy\overline{z}\,\overline{t}$	$x\overline{y}\,\overline{z}\,\overline{t}$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{t}$	$\overline{x}\,\overline{y}\,\overline{z}t$	$\overline{x}yzt$	$\overline{x}\,\overline{y}zt$
$(1,2) = xyz$	X	X						
$(2,3) = xy\overline{t}$		X	X					
$(3,4) = x\overline{z}\,\overline{t}$			X	X				
$(4,5) = \overline{y}\,\overline{z}\,\overline{t}$				X	X			
$(5,6) = \overline{x}\,\overline{y}\,\overline{z}$					X	X		
$(1,7) = yzt$	X						X	
$(6,8) = \overline{x}\,\overline{y}t$						X		X
$(7,8) = \overline{x}zt$							X	X

Como consecuencia la forma mínima es: $xyz + x\overline{z}\,\overline{t} + \overline{x}\,\overline{y}\,\overline{z} + \overline{x}\,z\,t$. □

23.3. Diagramas de Karnaugh. Aplicación

Capítulo VI

Introducción a la teoría de grafos

24. Definición de grafo

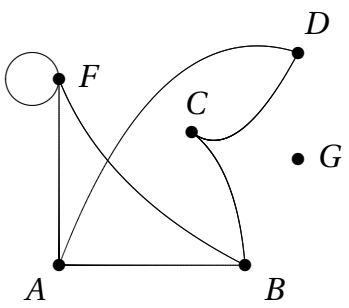
Un **grafo** es un par de conjuntos $G = (V, E)$ verificando que $E \subseteq V \times V$ y si $A, B \in V$, entonces, a lo más, hay un elemento a de E tal que $a = (A, B)$ ó $a = (B, A)$, (por esta razón el elemento a lo representaremos por $\{AB\}$ para obviar el orden que lleva implícita la notación de pares). Lo que aquí vamos a entender como grafo en otros textos se suele llamar **grafo simple**.

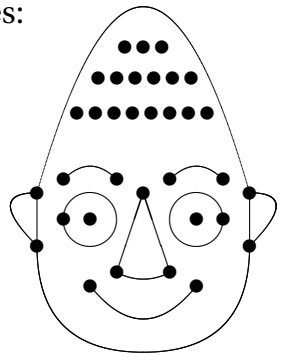
Los elementos de V se llaman los **vértices** del grafo G y los elementos de E se llaman los **lados**, **aristas** o **arcos** de G.

Para esta primera aproximación vamos a suponer que $V \cap E = \varnothing$ (y que V y E son finitos).

Todo grafo se puede representar mediante un gráfico formado por puntos, que representan a los vértices, y líneas, que representan a los lados.

Veamos un ejemplo de este tipo de representaciones:





En el caso primero los vértices son $V = \{A, B, C, D, F\}$ y los lados son:

$$E = \{\{AB\}, \{AF\}, \{FB\}, \{AD\}, \{CB\}, \{CD\}, \{FF\}\}.$$

En el segundo caso tenemos 34 vértices y 14 lados. Es claro que estas representaciones de grafos en el plano son posibles solo en algunos casos especiales y que un grafo puede tener varias representaciones distintas.

De cara al estudio de grafos, vamos a introducir alguna notación extra.

Si G es un grafo, el conjunto de sus vértices se representa por $V(G)$, y el conjunto de sus lados por $E(G)$.

Existe un grafo especial, el **grafo vacío**, que está definido por $\varnothing = (\varnothing, \varnothing)$.

Dado un vértice A y un lado b, decimos que A es **incidente** con b si $b = \{AX\}$ ó $b = \{XA\}$ para algún vértice X. Para simplificar vamos a representar que A es incidente con b mediante $A \in b$. Es claro que cada lado b tiene a lo más dos vértices que son incidente con él, los llamamos los **extremos** de b. Cuando los dos extremos de un lado coinciden, el lado se llama un **lazo**.

Un lado cuyos extremos son los vértices A y B se dice que **une** a dichos vértices, la forma de representar este lado es $\{AB\}$. Los vértices A y B se llaman **adyacentes** o **vecinos**. Un vértice que no tiene otros adyacentes se llama un **vértice aislado**. Dos lados a y b son **adyacentes** si tienen un extremo común.

Si dos vértices o dos lados no son adyacentes, se llaman **independientes**.

24.1. Matrices asociadas a grafos

Dado un grafo G con vértices $V(G) = \{A_1, \ldots, A_n\}$, se define la **matriz de adyacencia** de G como la matriz $M(G) = (m_{ij})_{ij}$, que es una matriz $n \times n$ y en la que la entrada m_{ij} es el número de lados que unen A_i con A_j.

Si el grafo G además tiene t lados, $E(G) = \{a_1, \ldots, a_t\}$, se define la **matriz de incidencia** de G como la matriz $I(G) = (b_{ij})_{ij}$, que es una matriz $n \times t$ y en la que la entrada b_{ij} es igual a 1 si A_i es incidente con a_j y 0 en caso contrario.

Ejemplo. 24.1.
Consideramos el grafo definido por $\{A_1, A_2, A_3, A_4, A_5, A_6\}$, los vértices de un hexágono y la diagonal $\{A_1A_4\}$. La matrix de adyacencia es:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

para los lados $\{\{A_1A_2\},\{A_2A_3\},\{A_3A_4\},\{A_4A_5\},\{A_5A_6\},\{A_6A_1\},\{A_1A_4\}$, la matrix de incidencia es:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Observar que la primera es simétrica y la segunda **no** lo es.

25. Lados en grafos

25.1. Grafos completos

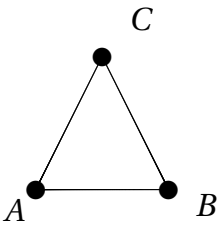
Un grafo G se llama **completo** si cada dos vértices distintos de G son adyacentes. Para cada entero positivo n existe un único grafo completo, sin lazos, al cual vamos a representar por K_n. Si V es un conjunto de vértices, el **grafo completo con vértices** V se representa por $K(V)$.

Ejemplo. 25.1.
Si $n = 0$, entonces K_0 es el grafo vacío.

Si $n = 1$, tenemos K_1 es el grafo con un sólo vértice y ningún lado.

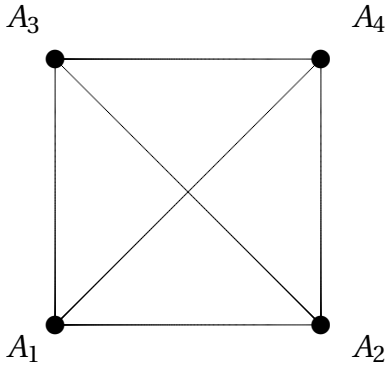
Si $n = 2$, entonces K_2 es el grafo con dos vértices y un solo lado, el que une estos vértices.

Si $n = 3$, entonces K_3 tiene tres vértices y tres lados; una representación es la siguiente:



Problema. 25.2.
¿Cuántos lados tiene un grafo completo de 4, 6 y 8 vértices?

SOLUCIÓN. Si $n = 4$, para averiguar el número de lados de K_4, numeramos los vértices, por ejemplo: A_1, A_2, A_3 y A_4, ahora necesitamos un lado de A_1 a cada uno de los restantes vértices, en total 3; un lado de A_2 a cada uno de los vértices A_3 y A_4, en total 2, y uno más de A_3 a A_4. Luego el número de vértices es: $3 + 2 + 1 = 6$



Para K_6 tenemos $5 + 4 + 3 + 2 + 1 = 15$, y para K_8 tenemos $\frac{(1+7)7}{2} = 28$. □

Problema. 25.3.
Probar que el grafo completo de n vértices tiene exactamente $(n-1)+(n-2)+\cdots+2+1=\frac{n(n-1)}{2}$ *lados.*

SOLUCIÓN. Etiquetamos los vértices como A_1, ..., A_n. Contamos los lados del grafo de la siguiente forma: (1) consideramos los lados con extremo A_1, hay exactamente $n-1$; (2) de los restantes contamos aquellos que tienen extremo A_2, hay exactamente $n-2$. Siguiendo de esta forma al llegar al paso (i) y contar los lados que restan con extremos el vértice A_i resultan $n-i$. Luego el número de lados es:

$$(n-1)+(n-2)+\cdots+2+1+0=\frac{(n-1+0)n}{2}=\frac{n(n-1)}{2}.$$

□

Ejemplo. 25.4.
Observar que si G es un grafo completo con n vértices, la matriz de adyacencia de G es del siguiente tipo:

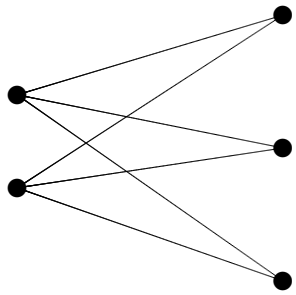
$$\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 0 \end{pmatrix}$$

25.2. Grafos bipartidos

Un grafo G se llama **bipartido** si existe una partición de $V(G)$, sea $V(G)=V_1\cup V_2$, tal que cada lado de G une un vértice de V_1 con un vértice de V_2.

El grafo bipartido en el que V_1 tiene r vértices, V_2 tiene s vértices y en el que hay un lado que une cada vértice de V_1 con cada vértice de V_2 lo llamamos el **grafo bipartido completo**, y se representa por $K_{r,s}$

Ejercicio. 25.5.
El grafo bipartido $K_{2,3}$ *tiene 6 lados; una representación del mismo es:*



Problema. 25.6.
Averiguar cuantos lados tiene el grafo bipartido completo $K_{r,s}$.

SOLUCIÓN. Consideramos los vértices como $\{A_1,\dots,A_r\}$ y $\{B_1,\dots,B_s\}$ que representan la partición del conjunto de vértices. Al existir un lado por cada par de vértices A_i, B_j, resulta que el grafo tiene $r\times s$ lados. □

Ejemplo. 25.7.
Observar que si G es un grafo bipartido con conjunto partición del conjunto de vértices $\{A_1,\dots,A_r\}\cup\{B_1\dots,B_s\}$, entonces la matriz de adyacencia de G es del siguiente tipo:

$$\left(\begin{array}{ccc|ccc} 0 & \overset{r}{\cdots} & 0 & 1 & \overset{s}{\cdots} & 1 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline 1 & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 1 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right)$$

26. Invariantes de grafos

Dados dos grafos $G = (V, E)$ y $G' = (V', E')$, una **aplicación de grafos** de G a G' es una par de aplicaciones $f = (f_V, f_E)$, verificando: $f_V : V \longrightarrow V'$ y $f_E : E \longrightarrow E'$, que está definida por $f_E(\{AB\}) = \{f_V(A)f_V(B)\}$ para cada lado $\{AB\} \in E$.

Dos grafos G y G' se llaman **isomorfos** si existe una aplicación de grafos $f = (f_V, f_E)$ tal que f_V y f_E son biyecciones. Si f es un isomorfismo se representa por $f : G \cong G'$, y a veces por $G = G'$, ya que vamos a identificar grafos que son isomorfos.

Una propiedad (P) de grafos, tal que si un grafo G verifica la propiedad (P) y G' es un grafo isomorfo a G entonces G' también verifica (P), se llama un **invariante de grafos**.

Los primeros invariantes que podemos considerar en un grafo son:
- el número de vértices y
- el número de lados.

Recordemos que vamos a trabajar en este curso con grafos que tienen sólo un número finito de vértices y un número finito de lados.

Entre grafos podemos definir las operaciones conjuntistas usuales:

Si G es un grafo, un **subgrafo** G' de G es otro grafo que verifica:

$$V(G') \subseteq V(G) \quad \text{y} \quad E(G') \subseteq E(G).$$

En este caso también se dice que G es un **supergrafo** de G'.

Si G_1 y G_2 son subgrafos de un grafo G, podemos definir la **unión** y la **intersección** de G_1 y G_2 en la forma usual. Podremos entonces hablar de **subgrafos disjuntos**.

Si $G' \subseteq G$ es un subgrafo de G, definimos el **complemento** de G' en G como el subgrafo $G'' \subseteq G$ que verifica:

$$V(G'') = V(G) \quad \text{y} \quad E(G'') = E(G) \setminus E(G').$$

Si G' es un subgrafo de un grafo G que verifica $V(G') = V(G)$ se dice que G' es un **subgrafo generador** de G.

Si G' es un subgrafo de un grafo G, decimos que G' es un **subgrafo completo** (también se llama **subgrafo inducido**) de G si

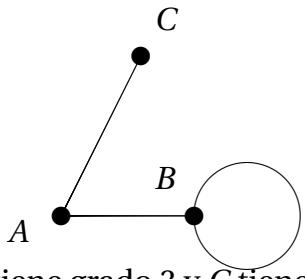
$$E(G') = E(G) \cap K(V(G')),$$

esto es, si para cada par de vértices A y B de G' se tiene $\{AB\} \in E(G')$ si y solo si $\{AB\} \in E(G)$.

Si G es un grafo, para cada conjunto de vértices $X \in V(G)$ existe un único subgrafo completo G' de G tal que $V(G') = X$; vamos a representar a este grafo por $G[X]$.

Dado un grafo G, y un vértice A de G, se llama **grado** de A al número de lados que lo tienen como extremo, (cuando tenemos un lazo, éste se cuenta dos veces). Vamos a representar este número por $d(A)$.

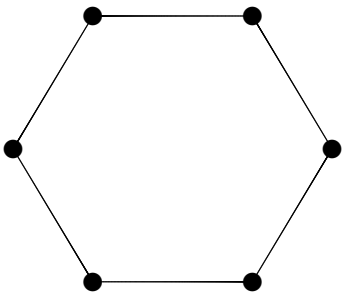
Ejemplo. 26.1.
Se considera el grafo representado por la figura



Observar que A tiene grado 2, B tiene grado 3 y C tiene grado 1.

Llamamos **regular** a un grafo en el que todos los vértices tienen el mismo grado.

Observar que todo grafo completo es regular, pero que el recíproco no es cierto com prueba el siguiente ejemplo.



La sucesión de los grados de los vértices de un grafo G la llamamos la **sucesión de grados** de G. Observar que la sucesión de grados es un invariante de grafos, esto es, si dos grafos son isomorfos, entonces tienen la misma sucesión de grafos.

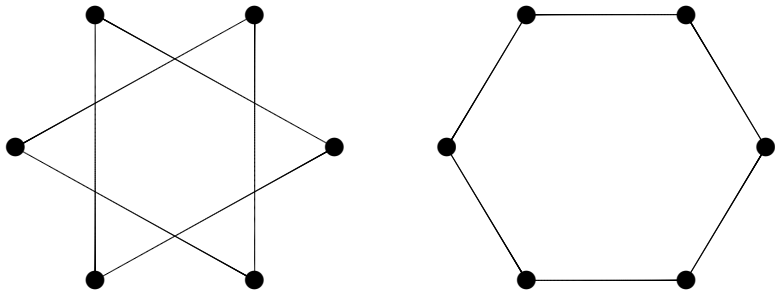
Una sucesión de números enteros no negativos se llama una **sucesión gráfica** si es la sucesión de grados de un grafo.

Lema. 26.2.
La relación entre los grados y el número de lados en G es: $\sum_{A \in V(G)} d(A) = 2\,|E|$.

DEMOSTRACIÓN. Para cada lado $e \in E(G)$, consideramos los vértices adyacentes, por ejemplo E_1E_2, puede ser $E_1 = E_2$. Si $e_1, \ldots, e_s$ es la lista de todos los lados, podemos construir una lista de vértices: E_{11}, E_{12}, E_{21}, E_{22}, $\ldots$, E_{s1}, E_{s2}. En esta lista aparecen $2s$ vértices. Este número es igual a la suma de los grados de todos los vértices, ya que el grado de un vértice A es igual al número de veces que A aparece en la lista E_{11}, E_{12}, E_{21}, E_{22}, $\ldots$, E_{s1}, E_{s2}. De aquí se sigue el resultado. □

Ejercicio. 26.3.
Probar que hay grafos no isomorfos con la misma sucesión de grados

SOLUCIÓN. Consideramos el grafo consistente en dos triángulos sin vértices en común. Todos los vértices tienen grado 2, luego la sucesión de grados es: 2,2,2,2,2,2. Por otro lado el grafo consistente en un hexágono tiene tiene la misma sucesión de grados, y estos grafos no son isomorfos.



□

Ejercicio. 26.4.
Probar que los grafos mencionados en el Ejercicio anterior no son isomorfos.

SOLUCIÓN. Llamamos A_1, A_2 y A_3 a los vértices de un triángulo, B_1, B_2 y B_3 a los vértices del otro triángulo y C_1, $\ldots$, C_6 a los vértices del hexágono. Si la imagen de A_1 es C_1, entonces la imagen de A_2 tiene que ser C_2 ó C_6, un vértice unido a C_1; supongamos que sea C_2, entonces la imagen de A_2 debe ser C_3, un vértice unido a C_2 distinto de C_1. Por otro lado, como A_3 está unido a A_1, también deben estar unidos C_1 y C_3, lo que evidentemente no es cierto. En consecuencia no existe un isomorfismo de grafos entre estos dos grafos. □

Ejercicio. 26.5.
Dar un ejemplo de dos grafos con tres vértices que no son isomorfos pero que tiene la misma sucesión de grados.

¡OJO!

El siguiente Lemma es válido para multigrafos, pero no para grafos simples. Basta considerar la sucesión que solo tiene un elemento, por ejemplo el 4; en este caso necesitaríamos dos

lazos en el único vértice que tenemos y esto no está permitido en un grafo (=grafo simple). Tampoco lo es la sucesión $(4,0,0,0,0,0)$.

Lema. 26.6.
La sucesión $(d_1, d_2, \ldots, d_n)$ es una sucesión gráfica si y sólo si $\sum_{i=1}^{n} d_i$ es un número par.

Sin embargo podemos modificar el enunciado para tener un resultado aplicable a los grafos que estamos estudiando (grafos simples). Resulta sin embargo un enunciado algo más complejo.

Proposición. 26.7.
Sea $(d_1, d_2, \ldots, d_n)$ una sucesión decreciente (¡no estrictamente decreciente!) con suma par y todos los d_i no nulos. Los siguientes enunciados son equivalentes:

(a) $(d_1, \ldots, d_n)$ es una sucesión gráfica de un grafo sin lazos.

(b) $d_k \leq n-1$ y $\sum_{i\leq k} d_i \leq \sum_{i>k} d_i + 2(k-1)$ para cada índice k.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Es claro que cada sucesión gráfica tiene suma par, y si A_i es un vértice, entonces su grado d_i es menor o igual que $n-1$. Por otro lado, si consideramos el vértice A_1, y lo eliminamos junto con los lados incidentes con él, resulta un nuevo grafo con sucesión de grados $(d'_2, \ldots, d'_n)$ y se verifica $d'_2 \leq \sum_{i>2} d'_i$, y de aquí se obtiene $d_2 \leq \sum_{i>2} d_i - d_1 + 2$; el 2 de la suma aparece cuando $d'_2 = d_2 - 1$. Entonces $\sum_{i\leq 2} d_i \leq \sum_{i>3} d_i + 2$. Por inducción se tiene entonces el resultado: $\sum_{i\leq k} d_i \leq \sum_{i>k} d_i + 2(k-1)$

(b) $\Rightarrow$ (a). Hacemos inducción sobre el número de vértices. Si $n = 2$, entonces cada grado es menor o igual que 1, y para que la suma sea par, la sucesión es $(1,1)$. Supongamos que el resultado es cierto para grafos con menos de n vértices, y sea $(d_1, \ldots, d_n)$ una sucesión decreciente cuya suma sea par y que verifique las condiciones indicada en (b).

Si $d_1 = t$, la sucesión $(e_2, \ldots, e_n) := (d_2 - 1, d_3 - 1, \ldots, d_{t+1} - 1, d_{t+2}, \ldots, d_n)$ tiene suma par, cada componente e_i es menor o igual que $n-2$, ya que si $e_{t+2} > n-2$, entonces $t = d_1 > n-2$, y se tendría $e_{t+1} = e_n$, luego no existiría el elemento e_{t+2}.

Además se verifica $e_2 \leq \sum_{i>2} e_i$, ya que $d_2 \leq \sum_{i>2} d_i - d_1 + 2$. Para cualquier índice k se tiene $e_k \leq \sum_{i>k} e_k - \sum_{i<k} e_i + 2(k-1)$ como aplicación de la hipótesis (b).

Podemos aplicar la hipótesis de inducción y tenemos un grafo sin lazos con vértices A_2, …, A_n, cuya sucesión de grados es $(e_2, \ldots, e_n)$. Finalmente basta agregar un nuevo vértice, que hará el papel de vértice A_1 y los lados $\{A_1A_i\}$, para $i = 2, 3, \ldots t+1$. La sucesión de grados de este nuevo grafo es la sucesión $(d_1, \ldots, d_n)$. □

Para caracterizar cuando una sucesión $(d_1, \ldots, d_n)$ decreciente es la sucesión gráfica de un

grafo que admite lazos podemos trabajar de la misma forma, en este caso tendremos que imponer, por ejemplo, la condición $d_i \leq n+1$.

27. Caminos en grafos

Dado un grafo G, un **camino** en G del vértice A_0 al vértice A_t es una sucesión de vértices y lados: $A_0a_0A_1a_1\dots a_{t-1}A_t$, con $t \geq 0$, en donde el lado a_i tiene extremos A_i y A_{i+1}. Cuando $A_0 = A_t$ el camino se llama un **camino cerrado**. El entero t se llama la **longitud del camino** (t es el número de lados). Dado un vértice A podemos considerar el camino A; en este caso decimos que este camino tiene longitud cero.

Un camino $A_0a_0A_1a_1\dots a_{t-1}A_t$ se llama un **recorrido** si los vértices $A_0,\dots,A_{t-1}$ y los vértices $A_1,\dots,A_{t-1},A_t$ son todos distintos. Un recorrido se llama un **ciclo** si $A_0 = A_t$.

Proposición. 27.1.
Sea G un grafo y A, B dos vértices de G; si existe un camino $A\dots B$, entonces existe un recorrido $A\dots B$.

DEMOSTRACIÓN. Dado un camino $Aa_0A_1\dots A_{t-1}a_{t-1}B$, si no es un recorrido existen dos vértices iguales en la lista $A,A_1,\dots,A_{t-1}$, sean A_i y $A_j := A_{i+s}$, $s \geq 0$, entonces $Aa_0A_1\dots a_{i-1}A_ia_jA_{j+1}\dots A$ es un camino de longitud menor al que hemos quitado un camino cerrado. Si no es un recorrido, entonces podemos quitar otro camino cerrado y así hasta obtener un recorrido $Aa_0\dots a_tB$. Igual se hace trabajando con B en vez de A. □

Corolario. 27.2.
Sea G un grafo y A, B dos vértices de G; si existen dos caminos distintos de A a B, entonces existe un ciclo en G.

DEMOSTRACIÓN. Podemos considerar que tenemos dos recorridos distintos de A a B. Sean $Aa_0A_1a_1\dots A_{t-1}a_{t-1}B$ y $Ab_0B_1b_1\dots B_{s-1}b_{s-1}B$. Se considera el camino: $Aa_0A_1a_1\dots A_{t-1}a_{t-1}Bb_{s-1}B_{s-1}\dots$ Se tiene que A es distinto de los A_i y de los B_j. Si A es igual a B, entonces uno de los recorridos es un ciclo y tenemos el resultado. Si A es distinto de B, puede ser que algún A_i sea igual a algún B_j, Tomando el menor de éstos A_i y el B_j correspondiente, tenemos que $Aa_0A_1a_1\dots a_{i-1}A_ib_{j-1}B_{j-i}\dots b_1B_1b_0A$ es un camino en el que todos los vértices $\{A,A_1,\dots,A_i.B_{j-1}\dots,B$ son distintos, luego tenemos un recorrido, y por tanto un ciclo. □

Un camino $A_0a_0A_1a_1\dots a_{t-1}A_t$ se llama un **camino simple** o un **circuito** si los lados $a_0,\dots,a_{t-1}$ son todos distintos. Un camino simple o circuito se llama un **circuito cerrado** si $A_0 = A_t$.

Ejercicio. 27.3.
Probar que todo recorrido es un camino simple.

Nombre	vértices repetidos	lados repetidos	coinciden inicio y fin
camino	—	—	—
camino cerrado	—	—	SI
recorrido	NO	no	—
ciclo	NO	no	SI
camino simple= circuito	—	NO	—
circuito cerrado	—	NO	SI

Teorema. 27.4. (Teorema del número de caminos)
El número de caminos de longitud k del vértice A_i al vértice A_j es el elemento (i,j) de la matriz $M(G)^k$.

DEMOSTRACIÓN. Es claro que existe un lado de A_i a A_j si y solo si el elemento m_{ij} de $M(G)$ es igual a 1, y no existe ningún lado si y solo si el mencionado elemento es igual a 0. Supongamos que el resultado es cierto para k y vamos a ver que también lo es para $k+1$.

Vamos a llamar $M(G) = (m_{ij})_{ij}$ y $M(G)^{k+1} =: (c_{ij})_{ij}$.

Todo camino de longitud $k+1$ de A_i a A_j, éste se puede escribir como

$$A_i b_0 B_1 b_1 \dots B_k b_k A_j.$$

Observar que tenemos un camino $A_i b_0 B_1 b_1 \dots B_k$ de A_i a B_k; si suponemos que $B_k = A_h$, este camino aporta una unidad al coeficiente (i,h), y al coeficiente (h,i), de la matriz $M(G)^k =: (d_{ij})_{ij}$. Tenemos un lado de A_h a A_j, que hace que los coeficientes (h,j) y (j,h) de la matriz $M(G)$ sean iguales a 1. El coeficiente c_{ij} se obtiene sumando, en h, los productos de los coeficientes d_{ih} y m_{hj}, luego tiene un sumando igual al coeficiente d_{ih}. Como consecuencia, ya que $c_{ij} = \sum_h d_{ih} m_{hj}$ tenemos el resultado de que c_{ij} es igual al número de caminos de A_i a A_j, pues hemos ido contando los caminos de longitud k que van de A_i a todos los vértices A_h y todos los lados de cada A_h a A_j. □

Dado un camino $A_0 a_0 A_1 a_1 \dots A_{t-1} a_{t-1} A_t$, escribiremos también, por simplicidad, $a_0 a_1 \dots a_{t-1}$.

Lema. 27.5.
Un grafo G es bipartido si y solo si G no tiene ciclos de longitud impar.

DEMOSTRACIÓN. Si G es un grafo bipartido es claro que no puede tener ciclos de longitud impar. Recíprocamente, si G no tiene ciclos de longitud impar, y prescindiendo de los vértices

aislados, podemos proceder como sigue: Dado un lado e, con extremos E_1 y E_2, construimos conjuntos $V_2^0 = \{E_1\}$ y $V_1^0 = \{E_2\}$.

Vamos a ir ampliando estos conjuntos de vértices como sigue:

$$V_1^1 = \{E \mid \exists\{EE_1\}\};$$
$$V_2^1 = \{E \mid \exists\{EE'\}, \{E'E_1\}\}.$$

Observar que en este caso se tiene que $E' \in V_1^1$ y además $V_1^1 \cap V_2^1 = \varnothing$; ya que si existe $F \in V_1^1 \cap V_2^1$, entonces existen $\{FE_1\}$, $\{FE'\}, \{E'E_1\}$, para un cierto E', y por tanto un ciclo de longitud 3 (impar). También se tiene $V_1^1 \cap V_2^0 = \varnothing$.

En general se define:

$$V_1^t = \{E \mid \text{ existe un camino de longitud 2t-1 (impar) de } E \text{ a } E_1\};$$
$$V_2^t = \{E \mid \text{ existe un camino de longitud 2t (par) de } E \text{ a } E_1\}.$$

Se tiene $V_1^t \cap V_2^{t-1} = \varnothing$, ya que si $F \in V_1^t \cap V_2^{t-1}$, entonces existe un camino de longitud $2t-1$ de E_1 a F, y un camino de longitud $2(t-1)$ de E_1 a F; entonces podemos construir un camino de longitud $4t-3$ de E_1 a E_1, lo que es una contradicción. También se tiene $V_1^t \cap V_2^t = \varnothing$; la demostración es análoga a la anterior.

Este proceso de construir los pares de conjuntos V_1^t y V_2^t es estacionario, esto es, existe un t tal que $V_1^t = V_1^{t+1} = \cdots$ y $V_2^t = V_2^{t+1} = \cdots$, llamamos a estos conjuntos V_1 y V_2 respectivamente. Estos conjuntos V_1 y V_2 verifican la propiedad de que si un lado tiene un extremo en uno de ellos, el otro extremo pertenece al otro. Si existe un lado de G que no tiene sus extremos en los V_i, entonces construimos nuevos conjuntos V_1' y V_2' siguiendo el proceso antes descrito. Basta definir entonces $V_1 = V_1 \cup V_1'$ y $V_2 = V_2 \cup V_2'$. De esta forma, y tras sucesivas ampliaciones, llegamos a conjuntos V_1 y V_2 tales que todo lado de G tiene un extremo en cada uno de los conjuntos V_i y por lo tanto el grafo es bipartido. □

Lema. 27.6.
Si G es un grafo en el que únicamente dos vértices son impares (= vértices de grado impar), entonces existe un recorrido entre ellos.

DEMOSTRACIÓN. Basta comprobar que tenemos un camino. Hacemos inducción sobre el número de lados del grafo. Llamamos A y B a estos vértices de grado impar, y sean $\{A_i \mid i = 1, \ldots, s\}$ el resto. Por ser A de grado impar existe un lado con extremo A que no es un lazo. Pueden ocurrir dos casos: (1) el otro extremo es B, entonces tenemos el resultado, ó (2) el otro extremo es uno de los A_i. Seguimos analizando este caso.

Al suprimir del grafo este lado volvemos a tener sólo dos vértices de grado impar: uno es B y el otro es A_i, pero este nuevo grafo tiene un lado menos. Aplicando la hipótesis de inducción tenemos un recorrido de A_i a B, y agregando el lado eliminado tenemos un camino de A a B.

Si el camino no es un recorrido entonces aparece un vértice al menos dos veces y por tanto un ciclo; podemos eliminar este ciclo y seguimos teniendo un camino de A a B. Si hacemos esto para todos los vértices que aparezcan varias veces obtenemos finalmente un camino de A a B que es un recorrido. □

28. Grafos conexos

Un **grafo conexo** es un grafo en el que para cada dos vértices A y B existe un camino $\{AB\}$. Un **grafo disconexo** es un grafo que no es conexo.

Una **componente conexa** de un grafo es un subgrafo conexo maximal. Si G es un grafo, vamos a utilizar la notación $k(G)$ para indicar el número de componentes conexas de G.

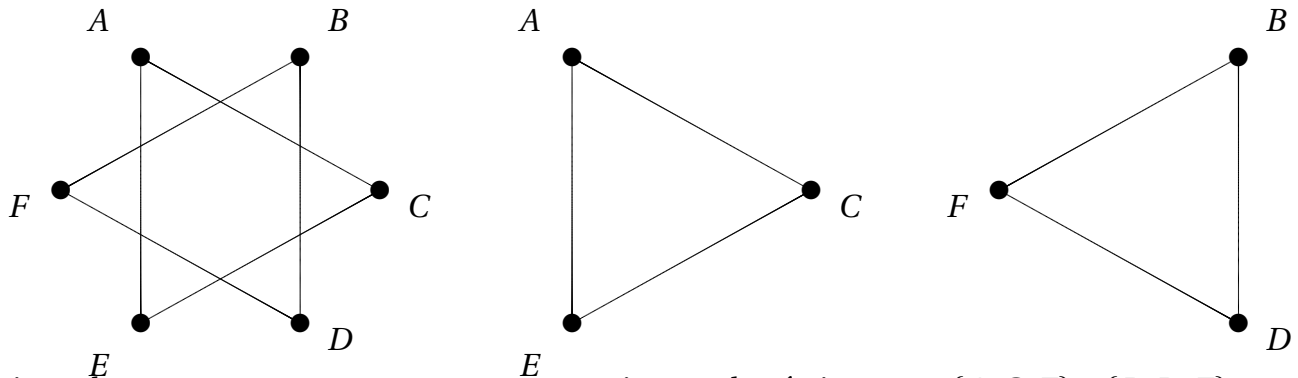
Teorema. 28.1.
Todo grafo es la unión de sus componentes conexas.

DEMOSTRACIÓN. Dado un grafo G, definimos en el conjunto de vértices $V(G)$ una relación, que es de equivalencia, mediante:

$$A \sim B \qquad \text{si existe un camino de } A \text{ a } B.$$

Al considerar caminos de longitud cero tenemos que la relación anterior verifica la propiedad reflexiva. Sea $V(G) = V_1 \cup \ldots \cup V_t$ la partición dada por las clases de equivalencia, y sea $G_i := K(V_i)$, el subgrafo completo de G definido por V_i para $i = 1, \ldots, t$. Entonces cada G_i es una componente conexa y se tiene $G = G_1 \cup \ldots \cup G_t$. □

Ejemplo. 28.2.
Sea G el grafo definido por la figura:



tiene dos componentes conexas, cuyos conjuntos de vértices son: $\{A, C, E\}$ y $\{B, D, F\}$

Si A es un vértice de un grafo G, representamos por $G \setminus \{A\}$ al grafo que se obtiene de G al suprimir el vértice A y todos los lados que tienen a A como extremo. Un vértice A de un grafo G se llama un **vértice de corte** o un **punto de articulación** si el grafo $G \setminus \{A\}$ tiene más componentes conexas que G.

conexo

Dado un grafo G un **bloque** de G es un subgrafo que no tiene vértices de corte y que es maximal respecto a esta propiedad.

Observar que un subgrafo en el que no exista ningún lado es un bloque, pues un vértice aislado no es nunca un vértice de corte ó punto de articulación.

Lema. 28.3.
Cuando dos bloques G_1 y G_1 comparten un único vértice, éste debe ser un vértice de corte de $G_1 \cup G_2$.

DEMOSTRACIÓN. Primero simplificamos al poder considerar $G = G_1 \cup G_2$ sin pérdida de generalidad. Podemos también suponer que los bloques son conexos, ya que en caso contrario basta considerar los subgrafos conexos que contengan al vértice común.

Sean los bloques G_1 y G_2 y el vértice común A. Vamos a ver que en el grafo $G_1 \cup G_2$ el vértice A es un vértice de corte. Es claro que $G_1 \cup G_2$ es conexo. Si también $G_1 \cup G_2 \setminus \{A\}$ conexo, entonces para cada vértice B de G_1 y para cada vértice C de G_2 existe un recorrido de B a C, que no puede contener a A; sea este recorrido $Be_0A_1 \dots A_te_tC$. Cada uno de los vértices B, A_1, $\dots$, A_t, C pertenece a G_1 ó a G_2, como $B \in G_1$ y $C \in G_2$, y ninguno pertenece a ambos, si llamamos $A_0 = B$ y $A_{t+1} = C$, debe de existir un índice i tal que $A_i \in G_1$ y $A_{i+1} \in G_2$, pero entonces el lado $\{A_iA_{i+1}\}$ no puede pertenecer a $G_1 \cup G_2$, lo que es una contradicción. Así pues necesariamente $G_1 \cup G_2 \setminus \{A\}$ no es conexo y A es un vértice de corte. □

Si f es un lado de un grafo G, representamos por $G\setminus\{f\}$ al grafo que se obtiene de G al suprimir el lado f. Un lado f de un grafo G se llama un **lado puente** si $G \setminus \{f\}$ tiene más componentes conexas que G.

Lema. 28.4.
Un lado f de un grafo conexo G es un puente de G si y solo si no pertenece a ningún ciclo de G.

DEMOSTRACIÓN. Condición necesaria. Si f pertenece a un ciclo, sea este ciclo $AfBe_1 \dots e_tA$. Entonces en $G \setminus \{f\}$ tenemos que A pertenece a una componente conexa y B a otra, pero como tenemos un recorrido: $Be_1 \dots e_tA$ de B a A, llegamos a una contradicción.
Condición suficiente. Si suponemos que $G \setminus \{f\}$ es conexo, y si $f = \{AB\}$, entonces existe un recorrido de A a B, sea $Ae_1 \dots e_tB$, como consecuencia tenemos un ciclo al que pertenece f: $Ae_1 \dots e_tBfA$, lo que es una contradicción. □

Corolario. 28.5.
Si f es un lado puente de un grafo conexo, entonces $G \setminus \{f\}$ tiene exactamente dos componentes conexas.

29. Árboles

Un **árbol** es un grafo conexo que no tiene ciclos (**acíclico**). En un árbol los vértices de grado uno se llaman **hojas**.

Lema. 29.1.
Si G es un árbol con n vértices, entonces se verifica:

(1) Para cada par de vértices A y B de G existe, como máximo, un único recorrido de A a B.

(2) Todos los lados de G son puentes.

(3) $\mid E(G) \mid = n-1$.

DEMOSTRACIÓN. (1). Si existen dos caminos distintos de A a B, entonces existen un ciclo por el Corolario 27.2..
(2). Como es un grafo conexo, el resultado se sigue del Lema 28.4..
(3). Al quitar un lado el árbol se convierte en un grafo con dos componentes conexas, cada una de las cuales es a su vez un árbol. Procediendo de esta forma, y haciendo inducción sobre el número de vértices, tenemos el resultado. □

Lema. 29.2.
Todo árbol, que contiene al menos un lado, tiene al menos dos hojas.

DEMOSTRACIÓN. Sea G un árbol con al menos un lado, por lo tanto el número n de vértices es mayor o igual que dos. Por el Lema 26.2. tenemos que la suma de los grados de todos los vértices es exactamente $2 \mid E \mid$, y por el Lema 29.1. se tiene $\mid E \mid = n-1$, luego la suma de los grados es igual a $2n-2$. Si todos los vértices tienen grado mayor o igual que 2 la suma de los grados será mayor o igual que $2n$, lo que es una contradicción. □

Los árboles pueden ser caracterizados como grafos con determinadas características.

Teorema. 29.3.
Los siguientes enunciados son equivalentes para un grafo G con n vértices:

(a) Para cada par de vértices A y B de G existe un único recorrido de A a B.

(b) G es conexo y todos los lados son puentes.

(c) G es acíclico y maximal (maximal significa que la adición de un lado crea un ciclo).

(d) G es conexo y $\mid E \mid = n-1$.

(e) G es acíclico y $|E| = n-1$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Es claro que G es conexo. Por otro lado, dado un lado $f = \{AB\}$, se tiene que en $G \setminus \{f\}$ las componentes conexas de A y B no están conectadas, por lo tanto f es un lado puente.
(b) $\Rightarrow$ (c). Como G es conexo y todos los lados son puente, no pueden existir ciclos, luego G es acíclico. Para comprobar la maximalidad, si agregamos a G un lado, sea $g = \{CD\}$, como G es conexo, existe un camino de C a D en G, y por lo tanto en $G \cup g$ existe un ciclo, por lo tanto G es acíclico maximal.
(c) $\Rightarrow$ (d). En el caso en que haya dos vértices A y B tales que no exista un camino de A a B, resulta que A y B pertenecen a componentes conexas distintas; si agregamos a G un lado, el lado $\{AB\}$, entonces el grafo sigue siendo acíclico, pero esto está en contradicción con el hecho de que G es un grafo acíclico maximal. Luego G es conexo. Vamos a contar los lados de G. Dado un vértice A_0 de G definimos $V_0 = \{A_0\}$ y definimos $V_1 = \{A \mid \exists \{A_0A\}\}$, Es claro que tenemos de esta forma $|V_1|$ lados de G y que no existe ningún otro lado entre los vértices de $V_1 \cup \{A_0\}$. Definimos $V_2 = \{A \mid \exists \{AB\},\ B \in V_1\} \setminus (V_1 \cup \{A_0\})$; es claro que tenemos exactamente $|V_2|$ nuevos lados y que no hay ningún otro lado, distinto a los ya considerados, entre los vértices de $V_2 \cup V_1 \cup \{A_0\}$. De esta forma construimos V_3, V_4, etc. Se tiene que $G = \cup_i V_i$, que esta unión es disjunta y finita y que el número de lados de G es $\sum_{i=1} |V_i| = |G| - 1 = n-1$.
(d) $\Rightarrow$ (e). Si G no es acíclico existe ciclo, sea $\{AB\}$. Si $A = B$, entonces es claro que un vértice que no puede estar conectado con el resto. Si $A \neq B$, y eliminamos el lado $\{AB\}$, entonces el grafo sigue siendo conexo, pero otra vez, al tener $n-2$ lados un vértice no puede estar conectado con el resto. En consecuencia G es acíclico.
(e) $\Rightarrow$ (a). Por el Corolario 27.2. tenemos que al no existir ciclos existe a lo mas un camino entre cada dos vértices. Si hay dos vértices A y B que no están conectados, podemos considerar las componentes conexas de A y de B, una de las dos debe tener al menos tantos lados como vértices. Hacemos inducción sobre el número de vértices para esta propiedad y obtenemos que existe un ciclo, lo que es una contradicción. En consecuencia entre cada dos vértices existe un único recorrido. □

Un **bosque** es un grafo acíclico. (Esto es, se quita a árbol la condición de ser conexo.)

Ejercicio. 29.4.
Probar que si un bosque con n vértices tiene k componentes conexas entonces el número de lados es $n-k$.

Un **árbol generador de un grafo** G, es un subgrafo que es árbol y contiene a todos los vértices del grafo.

Lema. 29.5.
Todo grafo conexo posee un árbol generador.

DEMOSTRACIÓN. Se considera un vértice A_0 y se define un grafo $G_0 = (\{A_0\}, \varnothing)$. Se define:

$$\begin{aligned} V_1 &= \{A \mid \exists\{AA_0\}\} \setminus V_0, \\ E_1' &= \{\{AA_0\} \mid A \in V_1\}, \\ G_1 &= (V_1 \cup \{A_0\}, E_1'). \end{aligned}$$

Tenemos que G_1 es un subgrafo de G que es un árbol. Se define:

$$\begin{aligned} V_2 &= \{A \mid \exists\{AB\},\ B \in V(G_1)\} \setminus V(G_1), \\ E_2' &= \{\{AB\} \mid A \in V_2\},\ \text{uno para cada } A \in V_2, \\ G_2 &= (V_2 \cup V(G_1), E_2' \cup E(G_1)). \end{aligned}$$

Tenemos que G_2 es un subgrafo de G que es un árbol. Se sigue de esta forma hasta que se alcance un G_i tal que $V(G_i) = V(G)$. En este caso se tiene que G_i es un árbol generador de G. □

Un **árbol binario** es un grafo conexo acíclico tal que el grado de cada vértice es menor o igual que 2.

Un **árbol binario con raíz** es un grafo que tiene uno de sus vértices, llamado raíz, de grado no mayor a 2. Elegida la raíz cada vértice tendrá un único padre, y nunca más de dos hijos. Así pues un árbol binario es un árbol con raíz en el que cada nodo tiene como máximo dos hijos.

Un **árbol binario completo**s un árbol en el que cada nodo tiene cero o dos hijos.

Un **árbol binario perfecto** es un árbol binario completo en el que todas las hojas (vértices con cero hijos) tienen la misma **profundidad** (distancia desde la raíz, también llamada **altura**).

Ejemplo. 29.6.
Si G es un árbol completo, entonces tiene un número impar de vértices.

SOLUCIÓN. Destacamos un vértice R de G como raíz, entonces el grado de R es igual a 0 ó 2. Si es cero, entonces el grafo se reduce a un vértice. Supongamos pues que es igual a 2. Tenemos además otros dos tipos de vértices: las hojas, que tienen grado 1, sea h el número de hojas de G; y los restantes vértices que necesariamente tienen grado 3, al tener un padre y dos hijos, representamos por n el número de estos vértices de grado 3. Por la fórmula de los grados, si llamamos l al número de lados de G, se tiene

$$2 + h + 3n = 2l.$$

Por otro lado el número de lados de G es igual a $2 + 2n$, ya que éste es el número de hijos de todos los vértices de G. Al introducir este valor en la igualdad anterior resulta:

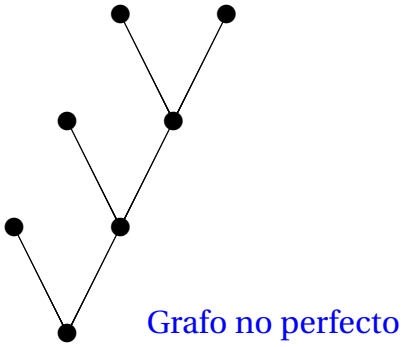
$$2 + h + 3n = 2(2 + 2n),$$

esto es, $h = n+2$, y por tanto el número v de vértices de G es: $v = 1+h+n = 1+n+2+n = 2n+3$.

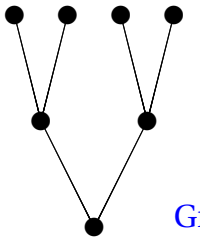
Si llamamos k al número de vértices que no son hojas, resulta $v = 2k+1$. En este caso el número de lados es: $l = 2k$, y el número de hojas es: $h = v-(2k+1)$. □

Ejemplo. 29.7.
Existen dos árboles binarios completos con 7 vértices que no son isomorfos.

SOLUCIÓN. Consideramos los árboles binarios de las figuras siguientes, que son árboles completos con el mismo número de vértices y no son isomorfos:



Grafo no perfecto



Grafo perfecto

□

30. Caminos de Euler

Si G es un grafo conexo, un **camino de Euler** en G es un camino en el que aparecen todos los lados una sola vez (esto es, es un camino simple).

Si G es un grafo conexo, un **circuito de Euler** es un camino de Euler que es cerrado. Un grafo que tiene un circuito de Euler se llama un **grafo de Euler**.

Proposición. 30.1.
Sea G un grafo conexo.

(1) Si G es un grafo de Euler, entonces todos los vértices tiene grado par.

(2) Si G tiene un camino de Euler que no es un circuito de Euler, entonces G tiene todos los vértices menos dos (el inicio y el fin del camino) de grado par.

DEMOSTRACIÓN. (1). Para calcular el grado de un vértice A en un grafo de Euler, tenemos que tener en cuenta que como los lados podemos disponerlos en una sucesión: $a_0, a_1, \ldots, a_t$, por cada lado a_i incidente con el vértice A, si a_i es un ciclo, entonces a_i aporta al grado de A dos unidades; si a_i no es un ciclo tenemos que necesariamente a_{i-1} ó a_{i+1} también son incidentes con A, y por tanto a_i, junto con el otro a_{i-1} ó a_{i+1} aportan dos unidades al grado de A. En consecuencia el grada de A es par.

(2). Si G tiene un camino de Euler que no es un circuito, sean A y B los extremos del camino; si añadimos un lado $\{AB\}$, entonces el grafo G' obtenido tiene un circuito de Euler, y por tanto es un grafo de Euler, y todos los vértices de G' tienen grado par. Al pasar a G eliminando el lado $\{AB\}$, resulta que todos los vértices tiene grado par salvo A y B que tienen grado impar. □

Para probar el inverso veamos primero el siguiente lema técnico.

Lema. 30.2.
Si un grafo G tienen todos los vértices de grado mayor estrictamente que uno, entonces G contiene un ciclo.

DEMOSTRACIÓN. Dado un vértice A_0, ya que el grado de A_0 es mayor que uno, existe un vértice A_1 incidente con A_0, esto es, existe un lado $\{A_0A_1\}$. Si $A_1 = A_0$, entonces tenemos un ciclo. Si $A_0 \neq A_1$, como el grado de A_1 es mayor que uno, existe un lado $\{A_1A_2\}$. Si $A_2 = A_i$, $i = 0, 1$, entonces tenemos un ciclo. Si $A_2 \neq A_i$, $i = 0, 1$, entonces existe un lado $\{A_2A_3\}$. Si $A_3 = A_i$, $i = 0, 1, 2$, tenemos un ciclo. Si $A_3 \neq A_i$, $i = 0, 1, 2$, entonces podemos construir un A_4. Utilizando que el número de vértices es finito necesariamente existe un índice j tal que $A_j = A_i$, para algún $i < j$, y de esta forma tenemos un ciclo. □

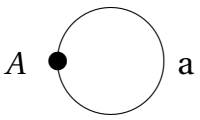
Teorema. 30.3.
Sea G un grafo conexo.

(1) Si cada vértice es de grado par, entonces G es un grafo de Euler.

(2) Si todos los vértices son pares salvo dos, entonces G tiene un camino de Euler.

DEMOSTRACIÓN. La parte (2) es consecuencia directa de (1).

(1). Hacemos inducción sobre el número de lados. Si hay un solo lado, entonces el grado es un ciclo de longitud uno, y por tanto es un circuito de Euler.



Supongamos que todo grafo conexo con los vértices pares de n lados es un grafo de Euler, y consideremos un grafo con los vértices pares y con $n+1$ lados. Como todos los vértices son de grado mayor que uno, existe un ciclo en G. Al eliminar todos los lados que aparecen en el ciclo tenemos un nuevo grafo en el que todos los vértice tienen grado par, y puede que no sea conexo. Cada una de sus componentes conexas es por la hipótesis de inducción un grafo de Euler. Para construir un circuito de Euler en G procedemos como sigue: elegimos un vértice A_0 perteneciente al ciclo, como A_0 está en una de las componentes conexas, añadimos el ciclo correspondiente a esa componente conexa. A continuación agregamos lados del ciclo hasta pasar al primer vértice que que no pertenezca a la componente conexa de A_0, sea este nuevo vértice A_1. Añadimos el ciclo correspondiente a la componente conexa de A_1 y seguimos el proceso hasta llegar de nuevo, siguiendo el ciclo, a A_0. De esta forma obtenemos un circuito de Euler. □

Algoritmo de Fleury para el cálculo de caminos de Euler, si existen, en grafos conexos.

(1) Si hay un vértice de grado impar, lo tomamos como A; si todos los vértices son de grado par, se elige uno como vértice A;

(2) Se definen dos sucesiones, una de vértices: $S_V = \{A\}$, y otra de lados: $S_E = \varnothing$.

(3) Si no hay ningún lado $\{AX\}$, para algún $X \in V(G)$, entonces el algoritmo termina, dando como salida el par (S_V, S_E);

(4) Si hay un solo lado $\{AX\}$, sea éste $\{AB\}$; redefinimos el grafo G eliminando el vértice A y el lado $\{AB\}$ y se va al paso (6);

(5) Si hay más de un lado $\{AX\}$, se elige uno de estos, sea $\{AB\}$, de forma que el grafo obtenido al partir de G al eliminar $\{AB\}$ sea conexo y redefinimos el grafo G eliminando el lado $\{AB\}$;

(6) Se redefinen $S_V = S_V \cup \{B\}$, agregando B al final, y $S_E = S_E \cup \{\{AB\}\}$, agregando $\{AB\}$ al final;

(7) Se cambia A por B y se va al paso (3).

31. Caminos de Hamilton

Se trata ahora de determinar recorridos en un grafo conexo que pasen por todos los vértices (una sola vez).

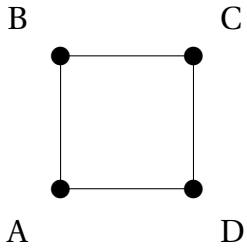
Dado un grafo G conexo, un **camino de Hamilton** en G es un recorrido que pasa por todos los vértices una sola vez.

Dado un grafo G conexo, un **circuito de Hamilton** es un camino de Hamilton que es cerrado.

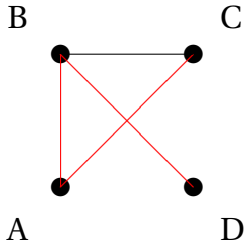
Un grafo conexo con un circuito de Hamilton se llama un **grafo de Hamilton** o **grafo hamiltoniano**.

Un camino de Hamilton no puede contener lazos, ya que no puede pasar dos veces por el mismo vértice. Si un grafo con n vértices tiene un camino de Hamilton, entonces el número mínimo de lados es $n-1$, y si tiene un circuito de Hamilton, entonces debe tener al menos n lados.

Ejemplo. 31.1.
El siguiente grafo es un grafo de Hamilton.

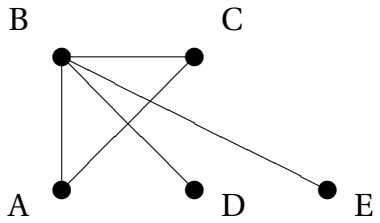


Ejemplo. 31.2.
En el siguiente ejemplo el recorrido señalado en rojo, $\{CA\}\{AB\}\{BD\}$, es un camino de Hamilton. Observar que el grafo no es un grafo de Hamilton.



De aquí podemos deducir fácilmente que si un grafo tiene un vértice de grado uno, entonces el grafo no es de Hamilton.

Ejemplo. 31.3.
En el siguiente ejemplo no existen caminos de Hamilton.



Observar que si pasamos de D a E lo tenemos que hacer necesariamente a través de B, lo que impide que podamos llegar a A ó C.

De cara a tener grafos de Hamilton es de interés que tengamos una gran cantidad de lados, aunque esto no es imprescindible como más adelante veremos.

Proposición. 31.4.
Sea G un grafo con n vértices. Se verifica:

(1) Si el número de lados de G es mayor o igual que $\frac{(n-1)(n-2)}{2}+2$*, entonces G es un grafo de Hamilton.*

(2) Si $n \geq 3$ *y para cada par de vértices no adyacentes, A y B, se verifica* $d(A)+d(B) \geq n$*, entonces G es grafo de Hamilton.*

DEMOSTRACIÓN. (2). Si G no es un grafo de Hamilton, vamos probar que existen al menos dos vértices no adyacentes tales que la suma de sus grados es menor que n. Si G no es un grafo de Hamilton es porque no existe un recorrido que contenga todos los vértices o porque si existe un recorrido que contiene todos los vértices, éste no es cerrado. En el segundo caso basta añadir un lado para tener un circuito de Hamilton, y por tanto un grafo de Hamilton. En el primer caso podemos añadir un lado para incluir un nuevo vértice; si el recorrido así obtenido no contiene todos los vértices, podemos repetir el proceso hasta llegar a uno que los contenga; si el recorrido no es cerrado, basta aplicar la construcción anterior para obtener un grafo con un circuito de Hamilton. Sea G' el grafo de Hamilton obtenido. Sea $\{A_0A_1\}$ el último lado añadido. Llamamos G'' al grafo que verifica: $V(G'')=V(G')$ y $V(G'')=V(G')\setminus\{\{A_0A_1\}\}$, observar que G'' no es un grafo de Hamilton. El lado $\{A_0A_1\}$ formará parte de un circuito de Hamilton en G'. Supongamos que éste es: $\{A_0A_1\}\{A_1A_2\}\{A_2A_3\}\cdots\{A_{n-2}A_{n-1}\}\{A_{n-1}A_0\}$. Veamos que para cada índice i, $1 \leq i \leq n-1$ los lados $\{A_0A_{i-1}\}$ y $\{A_1A_i\}$ no pertenecen simultáneamente a $V(G'')$: Si $i=2$, entonces $\{A_0A_{i-1}\}=\{A_0A_1\}\notin V(G'')$. Si $i>2$, y $\{A_0A_{i-1}\},\{A_1A_i\}\in V(G'')$, entonces podemos construir el circuito de Hamilton

$$\{A_1A_i\}\{A_iA_{i+1}\}\cdots\{A_{n-1}A_0\}\{A_0A_{i-1}\}\{A_{i-1}A_{i-2}\}\cdots\{A_2A_1\},$$

en G'', lo que contradice que G'' no es un grafo de Hamilton.

Como consecuencia, contando ahora el número de lados se debe verificar $d(A_0)+d(A_1) < n$. Esto prueba el resultado.

(1). Supongamos que $\frac{(n-1)(n-2)}{2}+2 \leq E(G)$. Si G no es de Hamilton, existen dos vértices no adyacentes A y B tales que $d(A)+d(B) < n$. Consideramos el subgrafo completo G' de G cuyos vértices son $V(G') = V(G) \setminus \{A,B\}$. Como G' es también un subgrafo de K_{n-2}, el número de lados $\mid E(G') \mid$ es menor o igual que $\frac{(n-2)(n-3)}{2}$. Por otro lado $\mid E(G') \mid = \mid E(G) \mid -d(A)-d(B)$, ya que el lado A, $B \notin V(G')$. Resulta entonces

$$\frac{(n-1)(n-2)}{2}+2 \leq \mid E(G) \mid = \mid E(G') \mid +d(A)+d(B) \leq \frac{(n-2)(n-3)}{2}+d(A)+d(B).$$

De aquí se obtiene:

$$d(A)+d(B) \geq \frac{(n-1)(n-2)}{2}+2-\frac{(n-2)(n-3)}{2}$$

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

$$= \frac{(n-2)2+4}{2} = n.$$

Lo que es una contradicción, y por tanto G ha de ser un grafo de Hamilton. □

Corolario. 31.5. (Teorema de Dirac)
Sea G un grafo con n vértices, si para cada vértice A se tiene $d(A) \geq \frac{n}{2}$, entonces G es de Hamilton.

Veamos ejemplos de grafos que no son hamiltonianos y que el número de sus lados está comprendido entre n y $\frac{(n-1)(n-2)}{2}+2$.

Ejemplo. 31.6.
El grafo completo K_{n-1} tiene $n-1$ vértices y $\frac{(n-1)(n-2)}{2}$ lados. Construimos un nuevo grafo agregando un vértice y un lado que una este vértice con uno de los vértices del grafo completo. Este grafo no es hamiltoniano ya que tenemos un vértice de grado uno. El número de lados es: $\frac{(n-1)(n-2)}{2}+1$. Este ejemplo prueba que el resultado obtenido en el apartado (1) de la proposición anterior no se puede mejorar.

Veamos ejemplos de grafos hamiltonianos con n lados.

Ejemplo. 31.7.
Se define el **grafo poligonal** de $n \geq 3$ vértices como el grafo con vértices $V = \{A_0, A_1, \ldots, A_{n-1}\}$ y lados $E = \{\{A_iA_{i+1}\} \mid \ i = 0,1,\ldots,n-2\} \cup \{\{A_{n-1}A_0\}\}$. En este caso se tiene que el número de lados n que es menor que $\frac{(n-1)(n-2)}{2}+2$ si $n > 3$ e igual si $n = 3$.

Veamos como aplicación cuando un grafo bipartido es un grafo de Hamilton.

Ejercicio. 31.8.
Si G es un grafo bipartido con conjuntos de vértices V_1 y V_2, de forma que $\mid V_i \mid = n_i$, $i = 1,2$, entonces se verifica:

(1) Si existe un camino de Hamilton en G, entonces $\mid n_1 - n_2 \mid \leq 1$.

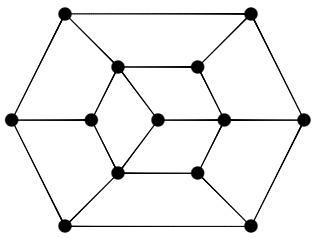
(2) Si G es un grafo de Hamilton, entonces $\mid n_1 - n_2 \mid = 0$.

(3) Si G en un grafo bipartido completo y $\mid n_1 - n_2 \mid \leq 1$, entonces G tiene un camino de Hamilton.

(4) Si G en un grafo bipartido completo y $\mid n_1 - n_2 = \leq 0$, entonces G tiene un circuito de Hamilton.

SOLUCIÓN. (1). Cada camino de Hamilton parte de un conjunto V_i, por ejemplo V_1, y acaba en un vértice de V_j. Como se han de recorrer todos los vértices, el camino será del tipo $\{A_0B_0\}\{B_0A_1\}\{A_1B_2\}\cdots\{XY\}$. Si $Y \in V_1$, entonces podemos suponer que $Y = A_{n_1-1}$ ó $Y = A_0$ (si es un circuito, este caso lo veremos en el siguiente apartado). Observar que los vértices utilizados de V_2, los B_h, son exactamente: B_0, B_1, ..., B_{n_1-2}, pero éste debe ser B_{n_2-1}, luego tenemos $n_2 - 1 = n_1 - 2$ y por tanto $n_1 - n_2 = 2 - 1 = 1$. Si $Y \in V_2$, entonces podemos suponer que $Y = B_{n_2-1}$. Observar que como se han utilizado todos los vértices de cada conjunto V_i se tiene $X = A_{n_1-1}$. La relación entre los índices es $n_1 - 1 = n_2 - 1$, y se tiene $n_1 - n_2 = 0$. El resultado se completa con el siguiente apartado.
(2). Si tenemos un circuito de Hamilton, entonces tenemos que considerar el caso que nos quedó en el apartado anterior; resulta que entonces el índice del último elemento utilizado de V_2 es $n_2 - 1$, y este valor debe coincidir con $n_1 - 1$, luego $n_1 - n_2 = 0$.
(3). Si G es un grafo bipartido completo y $\mid n_1 - n_2 \mid \leq 1$ basta dar un camino de Hamilton; es inmediato, basta enumerar los vértices alternativamente de V_1 y de V_2.
(4). En este caso se tiene un circuito de Hamilton ya que podemos acabar en el vértice inicial. □

Ejemplo. 31.9.
El siguiente grafo no es de Hamilton, ya que es un grafo bipatido con 13 vértices.



32. Grafos planos

Dado un grafo G, una **representación** de G es fijar un conjunto de puntos en el plano, uno por cada vértice, y unir mediante líneas o curvas aquellos puntos que para los que existe un lado entre los vértices correspondientes del grafo.

Una representación de un grafo G se dice **plana** si las líneas que unen los puntos que representan los vértices no se cortan.

Un grafo G se llama un **grafo plano** si tiene una representación plana.

Si un grafo tiene una representación gráfica, llamamos **caras de la representación** a cada una de las regiones del plano en que éste queda divido por la representación. Cada cara está determinada por un circuito de longitud al menos 3 al que llamamos la **frontera** de la cara.

Lema. 32.1. (Característica de Euler)
Sea G un grafo plano y conexo, sean v el número de vértices de G y e el número de lados de G y c el número de caras de una representación plana, se verifica:

$$v - e + c = 2.$$

En general si G es un grafo plano con t componentes conexas, entonces se verifica:

$$v - e + c = 1 + t.$$

DEMOSTRACIÓN. Supongamos que G es un grado plano conexo. Haremos inducción sobre el número de lados de G. Si hay un único lado tenemos las siguientes posibilidades:

El primer caso $v = 1$, $e = 1$ y $c = 2$, luego tenemos el resultado. En el segundo caso se tiene $v = 2$, $e = 1$ y $c = 1$, luego tenemos el resultado. Observar que este resultado es independiente de la representación que usemos.

Supongamos que el resultado es cierto para cada grafo plano conexo que tenga menos que n lados (suponemos que no depende de la representación plana utilizada). Sea G un grafo plano conexo de n lados con v vértices y con una representación plana de c caras.

Caso 1. G tiene un ciclo. Definimos un nuevo grafo G' a partir de G quitando una de los lados de un ciclo. (Se tiene que el grafo sigue siendo plano y conexo). Este grafo tiene v' vértices, e' lados y c' caras en la representación que tenemos. La relación con los números anteriores es:

$$v = v' \qquad e = e' + 1, \qquad c = c' + 1$$

ya que al quitar un lado de un ciclo estamos uniendo dos de las caras de la representación plana de G. En consecuencia tenemos el resultado a partir de a hipótesis de inducción.

Caso 2. G no tiene un ciclo. Conocemos que en este caso algún vértice tiene grado uno, ver Lema 30.2.. Definimos un nuevo grafo G' eliminando este vértice y el lado con él incidente. El grafo obtenido es plano y conexo. Este grafo tiene v' vértices, e' lados y c' caras en la representación que tenemos. La relación con los números anteriores es:

$$v = v' + 1 \qquad e = e' + 1, \qquad c = c'$$

ya que al quitar el lado no modificamos el número de caras de la representación plana de G. En consecuencia tenemos el resultado a partir de la hipótesis de inducción.

Queda el caso en que G no es conexo, en este caso para cada componente conexa de G tenemos una representación plana y la representación plana de G es la unión disjunta de las representaciones de todas las componente. Si las componentes son $C_1, \ldots, C_t$, cada una de ellos con v_t vértices, e_t lados y c_t caras, la unión disjunta tiene $\sum_i v_i$ vértices, $\sum_i e_i$ lados y el número de caras es la suma del número de caras de cada una de las representaciones de las componentes conexas, menos uno, y al este número hay que añadir uno. Tenemos entonces:

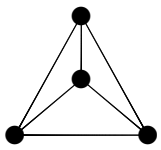
$$\begin{aligned} v - e + c &= \sum_i v_i - \sum_i e_i + \sum_i (c_i - 1) + 1 \\ &= \sum_i (v_i - e_i + c_i) - \sum_i 1 + 1 = \sum_i 2 - \sum_i 1 + 1 = t + 1. \end{aligned}$$

□

Todo poliedro se puede proyectar en el plano dando lugar a una representación plano de un grafo conexo con el mismo número de vértices y caras que el poliedro y con tantos lados cono aristas tiene el poliedro.

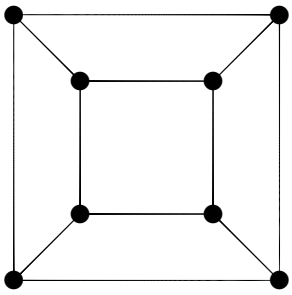
Corolario. 32.2.
En todo poliedro con v vértices, e aristas y c caras se verifica $v - e + c = 2$.

Ejemplo. 32.3.
El grafo completo K_4 es un grafo plano. Una representación plana es:



Observer que tiene cuatro caras.

Ejemplo. 32.4.
El cubo cuando se despliega en el plano tiene la representación:



Observar que el número de caras es seis y que el grafo es regular.

Aplicación al estudio de sólidos regulares

Dado un sólido regular S, consideramos el grafo plano asociado, sea G. Se verifica

$$v - e + c = 2.$$

El grafo G es un grafo regular de grado d. El número d es el número de aristas que concurren en un vértice, por lo tanto se tiene $d \geq 3$. Tenemos la relación dada por la suma de todos los grados de los vértices de un grafo:

$$v \cdot d = 2 \cdot e.$$

Como las caras del sólido son polígonos regulares de t lados, en el producto $c \cdot t$ contamos cada arista dos veces, luego se tiene:

$$c \cdot t = 2e.$$

Volviendo a la relación original (Euler), tenemos, al calcular en función de d:

$$v - e + c = 2$$

$$\tfrac{2e}{d} - e + \tfrac{2e}{t} = 2$$

$$\tfrac{1}{d} + \tfrac{1}{t} = \tfrac{1}{2} + \tfrac{1}{e}.$$

Con las restricciones $d \geq 3$ y $t \geq 3$, si suponemos que simultáneamente se tiene d, $t \geq 4$, entonces $\frac{1}{4} \geq \frac{1}{d}$ y $\frac{1}{4} \geq \frac{1}{t}$ y podemos hacer;

$$\frac{1}{2} + \frac{1}{e} = \frac{1}{d} + \frac{1}{t} \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$

de donde se obtiene $\frac{1}{e} \leq 0$, lo que es una contradicción.

Supongamos que $t = 3$, esto es el sólido tiene por caras triángulos. Resulta:

$$\frac{1}{d} + \frac{1}{3} = \frac{1}{2} + \frac{1}{e},$$

$$\frac{1}{e} = \frac{1}{d} + \frac{1}{3} - \frac{1}{2} = \frac{1}{d} - \frac{1}{6}$$

$$e = \frac{6d}{6-d}.$$

Tenemos entonces la restricción $d < 6$, y por tanto tenemos las posibilidades, teniendo en cuenta que $6 - d$ debe dividir a $6d$:

d	$6-d$	$6d$	$e =$ lados	$c = \frac{2e}{3} =$ caras, nombre
5	1	30	30	20 icosaedro
4	2	24	12	8 octaedro
3	3	18	6	4 tetraedro
2	4	12	3	no existe
1	5	6		

Supongamos que $d = 3$. Resulta:

$$\frac{1}{3} + \frac{1}{t} = \frac{1}{2} + \frac{1}{e},$$

$$\frac{1}{e} = \frac{1}{t} + \frac{1}{3} - \frac{1}{2} = \frac{1}{t} - \frac{1}{6}$$

$$e = \frac{6t}{6-t}.$$

Tenemos que la restricción $t < 6$, y tenemos las posibilidades:

t	$6-t$	$6t$	$e =$ lados	$c = \frac{2e}{t} =$ caras, nombre
5 (pentágonos)	1	30	30	12 dodecaedro
4 (cuadrados)	2	24	12	6 cubo
3 (triángulos)	3	18	6	4 tetraedro
2	4	12	3	no existe
1	5	6		

Lema. 32.5.
Sea G un grafo plano conexo, que no tiene lazos, entonces se tienen las relaciones $3c \leq 2e$ y $e \leq 3v - 6$.

DEMOSTRACIÓN. Definimos un nuevo concepto, el **grado de una cara**, como el número de lados que forman la dicha cara. En nuestro caso cada cara tiene grado mayor o igual que tres, y por tanto la suma de los grados de todas las caras es mayor o igual que tres veces el número de caras. Como cada lado es común a dos caras, la suma de los grados de las caras es el doble

del número de lados, pero este número es $2e$, luego tenemos $2e \geq 3c$.
Por otro lado, por la relación de Euler, se tiene $v - e + c = 2$, introduciendo la acotación anterior resulta $e = v + c - 2 \leq v + \frac{2e}{3} - 2 = \frac{3v+2e-6}{3}$, y de aquí $3e \leq 3v + 2e - 6$ y tenemos: $3 \leq 3v - 6$. □

Corolario. 32.6.
Si cada cara está formada por al menos t lados, entonces las acotaciones del Lemma quedarían:

$$tc \leq 2e \qquad (t-2)e \leq t(v-2).$$

DEMOSTRACIÓN. Hacer como ejercicio. □

Veamos ejemplos de grafos que no son planos.

Ejemplo. 32.7.
El grafo K_5 no es plano.
Tenemos $v = 5$, $e = \frac{5\times 4}{2} = 10$, pero por el Lema anterior se tiene la acotación: $e \leq 3v - 6 = 3 \times 5 - 6 = 9$, lo que es una contradicción.

Ejemplo. 32.8.
El grafo $K_{3,3}$ no es plano.
Al ser un grafo bipartido, cada si es plano cada cara debe estar formada por al menos cuatro lados. Tenemos $v = 6$ y $e = 3 \times 3 = 9$, y por el Corolario anterior se tiene la acotación: $2e \leq 4(v-2) = 4 \times (6-2) = 16$, lo que es una contradicción.

Lema. 32.9.
Todo árbol es un grafo plano.

DEMOSTRACIÓN. Hacemos inducción sobre el número de vértices n. Si $n = 0$ ó 1, entonces el resultado es cierto de forma trivial, además en una representación plana aparecen exactamente una cara. Supongamos que sea cierto este resultado para todo árbol de menos de n vértices. Dado un árbol con n vértices, si eliminamos un lado obtenemos un árbol o bien dos árboles, en ambos casos con menos de n vértices, que por hipótesis son grafos planos. Como consecuencia cada árbol con n vértices se obtiene añadiendo un lado a un árbol de $n-1$ vértices de forma que no tengamos ciclos, o bien mediante un lado que conecta dos árboles "disjuntos"; en ambos casos el grafo tendrá una representación plana. □

Observar que si tenemos un árbol, como éste tiene una sola cara se verifica: $v - e = 1 = 2$, esto es: $v = e + 1$.

Veamos si podemos averiguar cuales son los grafos que no son planos.

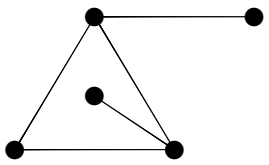
Si G es un grafo una **contracción simple** de G es el grafo que se obtiene al identificar en G dos vértices adyacentes. Una **contracción** de G es una sucesión de contracciones simples.

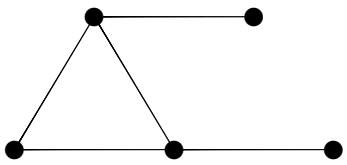
Lema. 32.10.
Cada contracción de un grafo plano es un grafo plano.

Proposición. 32.11. (Teorema de Kuratowski)
Un grafo es plano si y solo si ningún subgrafo puede contraerse a K_5 ó $K_{3,3}$.

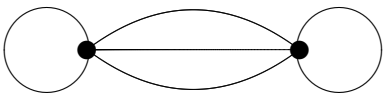
Otro concepto relativo a grafos planos es el de grafo dual. Si G es un grafo plano con una representación plana en la que tenemos t caras, definimos el **grafo dual** de G como el grafo con t vértices $C_0, \ldots, C_{t-1}$, uno para cada una de las caras, y dados dos vértices C_i y C_j, para cada lado que sea frontera común de las caras c_i y c_j consideramos un lado entre C_i y C_j. Observar que este grafo puede ser un multigrafo, esto es, entre dos vértices puede haber más de un lado. Observar también que el grafo dual depende de la representación del grafo elegida.

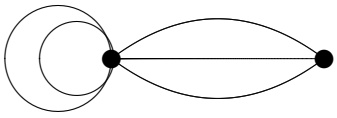
Ejemplo. 32.12.
Consideramos las representaciones siguientes para el grafo G:





Los grafos duales son respectivamente:





33. Coloración de grafos

Dado un grafo G, una **coloración** de G con valores en un conjunto C es una aplicación $f : V(G) \longrightarrow C$ verificando que si existe un lado $\{AB\}$, entonces $f(A) \neq f(B)$. Podemos suponer que los grafos que vamos a estudiar en esta sección son grafos sin lazos.

De forma intuitiva f asigna colores a cada uno de los vértices de G, y si dos vértices son adyacentes, entonces están coloreados de diferente forma.

El **número cromático** de un grafo G es el menor cardinal de los conjuntos C tales existe una coloración de G con valores en C. El número cromático del grafo G se representa por $\aleph(G)$.

(1) El grafo con dos vértices y un lado, K_2, tiene índice cromático 2.

(2) El grafo completo K_n tiene índice cromático n.

(3) Los grafos bipartidos tienen índice cromático 2 y viceversa.

(4) El índice cromático de un subgrafo $G' \subseteq G$ de un grafo G es menor que el índice cromático del grafo G.

(5) Si un grafo es plano, entonces su índice cromático es menor o igual que 4. El recíproco no es cierto ya que el índice cromático de $K_{3,3}$ es dos y $K_{3,3}$ no es un grafo plano.

Dado un grafo G, representamos por $p(G,n)$ el número de coloraciones distintas de G con n colores. Llamamos a $p(G,x)$ el **polinomio cromático** de G.

(1) Si un grafo G tiene al menos un lado, entonces $p(G,1) = 0$.

(2) Si consideramos K_2, entonces un vértice se puede colorear de n formas distintas, y el segundo de $n-1$ formas, entonces el número total de coloraciones es $p(K_2,n) = n(n-1)$. Y $p(K_t,n) = n(n-1)(n-2)\cdots(n-t+1)$.

(3) Si el grafo G tiene t componentes conexas, $G_1, \ldots, G_t$, entonces $p(G,n) = \prod_i p(G_i,n)$. Lo que reduce el problema a trabajar con grafos conexos.

(4) Si consideramos un recorrido no cerrado con t vértices, entonces $p(G,n) = n(n-1)^{t-1}$, ya que podemos elegir cualquier color para uno de ellos, y para un adyacente tenemos $n-1$ posibilidad, este proceso se repite.

Dado un grafo G y un lado $\{AB\}$ que no es un lazo, definimos $G_{\{AB\}}$ como el grafo que tiene los mismos vértices que G y todos los lados de G salvo el lado $\{AB\}$. Definimos $G'_{\{AB\}}$ el grafo que se obtiene a partir de $G_{\{AB\}}$ identificando los vértices A y B.

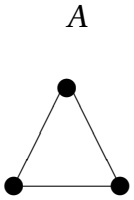
Teorema. 33.1.
Dado un grafo G y dos vértices adyacentes A y B se verifica:

$$p(G_{\{AB\}}, n) = p(G, n) + p(G'_{\{AB\}}, n).$$

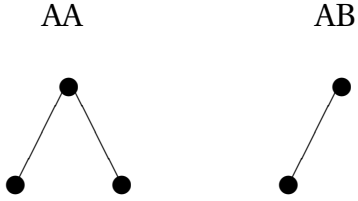
DEMOSTRACIÓN. Se trata de descomponer las posibles coloraciones de $G_{\{AB\}}$ en dos conjuntos, uno el aquellas coloraciones en las que A y B tienen color distintos, que son las coloraciones de G, y otro el de las coloraciones en las que A y B tienen el mismo color, que son las coloraciones de $G'_{\{AB\}}$. □

Como consecuencia se tiene $p(G, n) = p(G_{\{AB\}}, n) - p(G'_{\{AB\}}, n)$, y por tanto se reduce el problema de calcular el polinomio cromático al cálculo de polinomios cromáticos de grafos con menos elementos.

Ejercicio. 33.2.
Calcular el polinomio cromático del grafo



SOLUCIÓN.

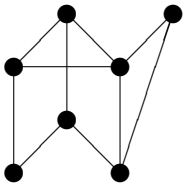


$n \to$	2	3	n
AA	2	3×2^2	$n(n-1)^2$
AB	2	3×2	$n(n-1)$
A	0	3×2	$n(n-1)(n-2)$

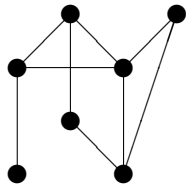
$$p(A, n) = n(n-1)^2 - n(n-1) = n(n-1)(n-1-1) = n(n-1)(n-2)$$

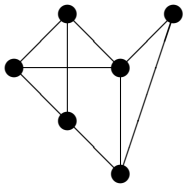
□

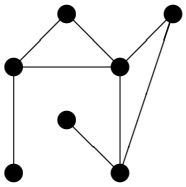
Ejercicio. 33.3.
Calcular el polinomio cromático del grafo

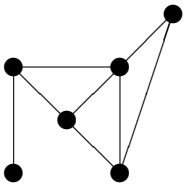


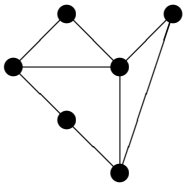
SOLUCIÓN. Tenemos que descomponer el grado y utilizando el Teorema calcular el polinomio cromático. Hacemos el listado de descomposiciones, etiquetando cada una de ellas.

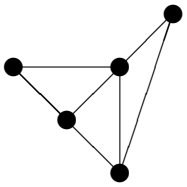

A

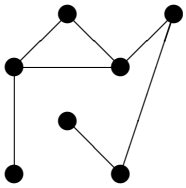

B

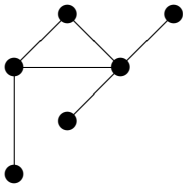

AA

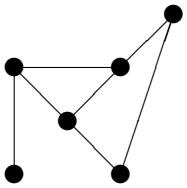

AB

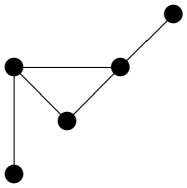

BA


BB

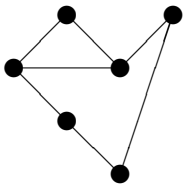

AAA

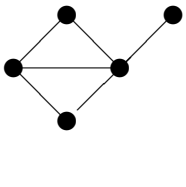

AAB

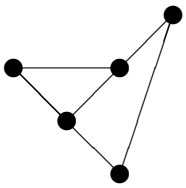

ABA

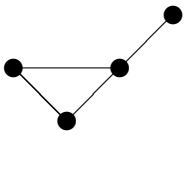


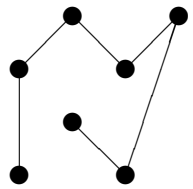
ABB

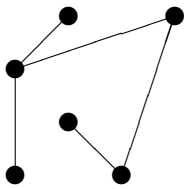

BAA

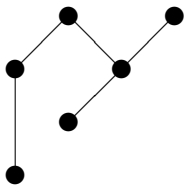

BAB

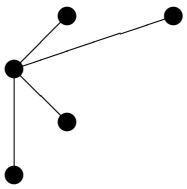

BBA

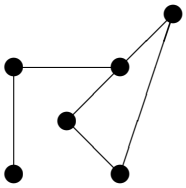

BBB

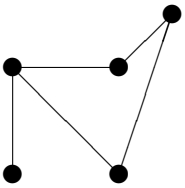

AAAA

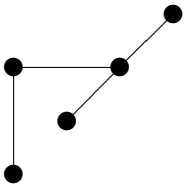

AAAB

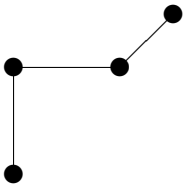

AABA

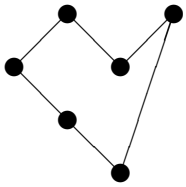

AABB

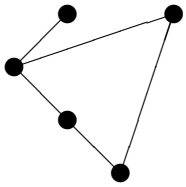

ABAA

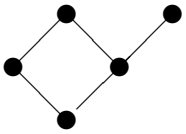

ABAB

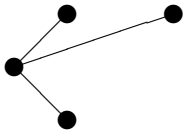

ABBA

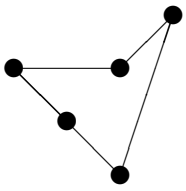

ABBB

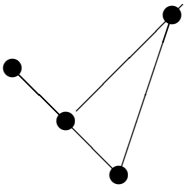

BAAA

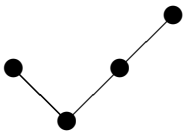

BAAB

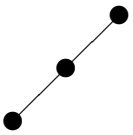

BABA


BABB


BBAA

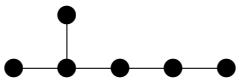

BBAB


BBBA


BBBB

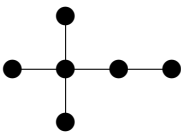
El polinomio cromático de *AAAA* es $p(AAAA, n) = n(n-1)^6$.

El polinomio cromático de *AAAB* es $p(AAAB, n) = n(n-1)^5$.

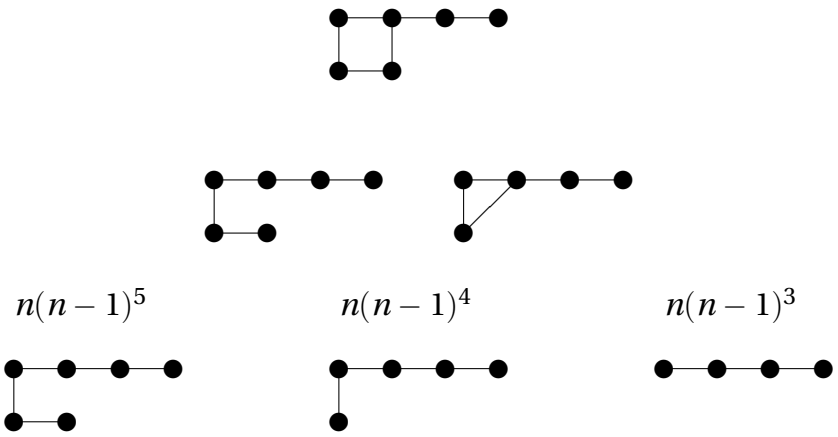


El polinomio cromático de *AABA* es igual al de *AAAB*, luego $p(AABA, n) = n(n-1)^5$.

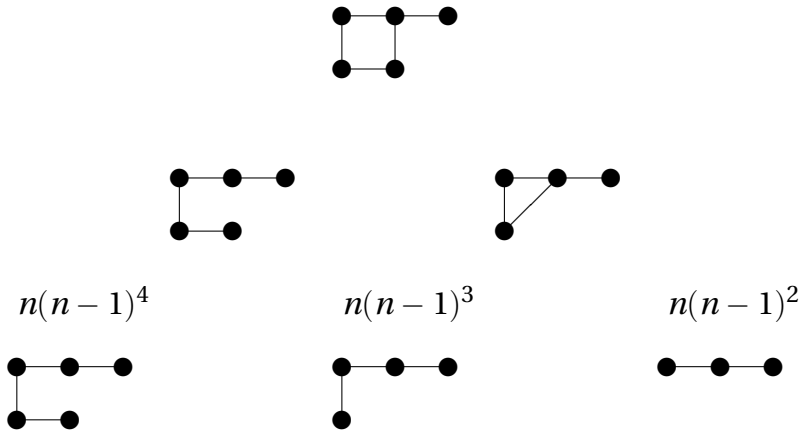
El polinomio cromático de *AABB* es $p(AABB, n) = n(n-1)^4$.



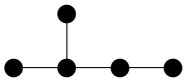
El polinomio cromático de *ABAA* es el del grafo siguiente, que se calcula según la sucesión que aquí aparece; el resultado es: $p(ABAA, n) = n(n-1)^5 - n(n-1)^4 + n(n-1)^3 = n(n-1)^3(n^2-3n+3)$.



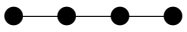
El polinomio cromático de *ABAB* es el del grafo siguiente, que se calcula según la sucesión que aquí aparece; el resultado es: $p(ABAB, n) = n(n-1)^4 - n(n-1)^3 + n(n-1)^2 = n(n-1)^2(n^2-3n+3)$.



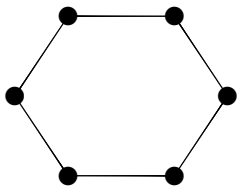
El polinomio cromático de *ABBA* es $p(ABBA, n) = n(n-1)^4$.

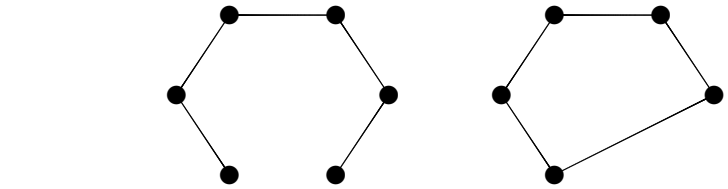


El polinomio crimático de *ABBB* es $p(ABBB, n) = n(n-1)^3$.

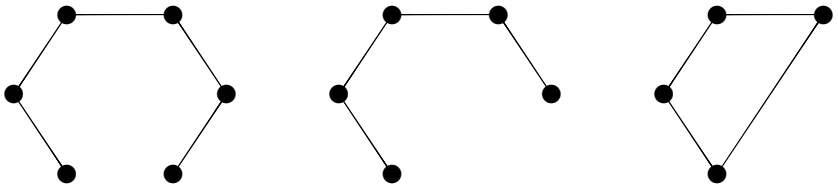


El polinomio cromático de *BAAA* es $p(BAAA, n) = n(n-1)^5 - n(n-1)^4 + n(n-1)[(n-1)^2 - (n-1)+1] = n(n-1)[(n-1)^4 - (n-1)^3 + (n-1)^2 - (n-1)+1] = n(n-1)\frac{(n-1)^5-1}{n} = (n-1)[(n-1)^5 - 1]$.





$n(n-1)^5$ $n(n-1)^4$ $n(n-1)[(n-1)^2-(n-1)+1]$

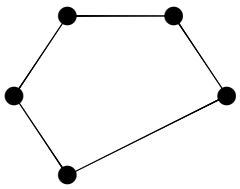


El polinomio cromático de *BAAB* es igual al de *ABAB*, luego $p(BAAB,n) = n(n-1)^2(n^2-3n+3)$.

El polinomio cromático de *BABA* es igual al de *ABAB*, luego $p(BABA,n) = n(n-1)^2(n^2-3n+3)$.

El polinomio cromático de *BABB* es $p(BABB,n) = n(n-1)^3$.

El polinomio cromático de *BBAA* es $p(BBAA,n) = n(n-1)^4 - n(n-1)[(n-1)^2-(n-1)+1] = n(n-1)[(n-1)^3-(n-1)^2+(n-1)-1] = n(n-1)\frac{(n-1)^4-1}{n} = (n-1)[(n-1)^4-1]$.



El polinomio cromático de *BBAB* es $p(BBAB,n) = n(n-1)^2(n-2)$.

El polinomio cromático de *BBBA* es $p(BBBA,n) = n(n-1)^3$.

El polinomio cromático de *BBBB* es $p(BBBB,n) = n(n-1)^2$.

En consecuencia el polinomio cromático del grafo es:

$$
\begin{aligned}
&p(A) = p(AAAA, n) - p(AAAB, n) - p(AABA, n) + p(AABB, n) + \cdots \\
&= n(n-1)^6 - n(n-1)^5 - n(n-1)^5 + n(n-1)^4 \\
&-n(n-1)^3[(n-1)^2 - (n-1) + 1] + n(n-1)^2[(n-1)^2 - (n-1) + 1] \\
&+n(n-1)^4 - n(n-1)^3 - (n-1)[(n-1)^5 - 1] \\
&+n(n-1)^2[(n-1)^2 - (n-1) + 1] + n(n-1)^2[(n-1)^2 - (n-1) + 1] \\
&-n(n-1)^3 + (n-1)[(n-1)^4 - 1] - n(n-1)^2(n-2) \\
&-n(n-1)^3 + n(n-1)^2 \\
&= n(n-1)^6 - 2n(n-1)^5 + 2n(n-1)^4 - 3n(n-1)^3 + n(n-1)^2 \\
&-n(n-1)^3[(n-1)^2 - (n-1) + 1] + 3n(n-1)^2[(n-1)^2 - (n-1) + 1] \\
&-(n-1)[(n-1)^5 - 1] + (n-1)[(n-1)^4 - 1] - n(n-1)^2(n-2) \\
&= n(n-1)^6 - 2n(n-1)^5 + 2n(n-1)^4 - 3n(n-1)^3 + n(n-1)^2 \\
&-(n-1)^3[(n-1)^3 - 1] + 3(n-1)^2[(n-1)^3 - 1] - (n-1)[(n-1)^5 - 1] \\
&+(n-1)[(n-1)^4 - 1] - (n-1)^2[(n-1)^2 - 1] \\
&= n^7 - 10n^6 + 43n^5 - 102n^4 + 142n^3 - 116n^2 + 52n - 10.
\end{aligned}
$$

Observar que tenemos varios tipos de grafos que estudiar, unos son recorridos, otros son recorridos que salen del mismo vértice y otros son polígonos que que tienen recorridos saliendo de alguno de sus vértices, luego es conveniente hacer un estudio de cada uno de estos casos e incluirlos en una tabla para llegar a realizar el cálculo de los polinomios cromáticos de forma rápida. □

33.1. Grafos planos 5-coloreables

Si consideramos un grafo plano G, entonces se verifica $v - e + c = 2$, y como consecuencia, ver Lema 32.5., se tiene $e \leq 3v - 6$. De este resultado podemos deducir el siguiente:

Lema. 33.4.
Si G es un grafo plano, entonces existe un vértice de grado menor o igual que 5.

DEMOSTRACIÓN. Si todos los vértices tienen grado mayor que 5, se tendrá $6v \leq \sum_A d(A) = 2l$, luego tenemos la acotación $3v \leq e$, que uniendo a la que antes mencionamos resulta:

$$3v \leq e \leq 3v - 6,$$

lo que es una contradicción. □

Teorema. 33.5.
Todo grafo plano es 5-coloreable.

DEMOSTRACIÓN. Tenemos que si $v \leq 5$, entonces el grafo es 5-coloreable. Vamos a demostrar el resultado por inducción sobre el número de vértices. Supongamos que $e > 5$. Por el Lema anterior el grafo G tiene un vértice A de grado menor o igual que 5. Considerasmo una representación plano del grafo G. Definimos un nuevo grado $G' = G \setminus \{A\}$. Como $|G'| < |G|$, resulta que G' es 5-coloreable. Vamos a extender la coloración de g' a G. Si los vértices adyacentes a A se pueden pintar con cuatro colores entonces G es coloreable, pues utilizamos el quinto para pintar A. Si los vértices adyacentes A son pintados con los cinco colores, entonces numeramos estos vértices B_1, B_2, B_3, B_4 y B_5 de forma que tengamos un pentágon ocon A en su interior y suponemos que el color de B_i es i. Llamamos G'_{ij} al subgrafo completo de G' cuyos vértices son los que están coloreados con i y j. Si B_i y B_j están en componentes conexas distintas de G'_{ij}, entonces podemos cambiar i por j en esta componente conexa, esta nueva coloración la extendemos a G' y entonces tenemos que los cinco vértices adyacentes a A se pueden pintar con cinco colores, y por tanto el grafo es 5–coloreable. Si B_i y B_j están siempre en la misma componente conexa de G'_{ij} par todas las parejas i, j, entonces existe un camino de B_i a B_j en G'_{ij}, esto es coloreable con los colores i y j. Consideramos un camino cerrado agregando el lado $\{B_iB_j\}$. Si tomamos $i = 1$ y $j = 3$, entonces en el camino cerrado que contiene B_1 y B_3 el vértice B_2 queda en el interior y B_4 en el exterior (Teorema de la curva de Jordan), y por tanto como en G'_{24} tenemos un camino de B_2 a B_4, este camino debe cortar al camino que contiene a B_1 y B_3 en un vértice. Este vértice será de los colores 1 ó 3 y 2 ó 4, lo que es una contradicción. Por tanto este caso no se puede dar y el grafo es siempre 5-coloreable. □

Capítulo VII

Combinatoria

34. Principio de la suma

Teorema. 34.1.
Sean X e Y dos conjuntos finitos, si llamamos $|X|$ al número de elementos de X, se verifica:

(1) ***Principio de inclusión–exclusión.*** $|X \cup Y| = |X| + |Y| - |X \cap Y|$.

(2) ***Principio de la suma.*** *Si X e Y con conjuntos disjuntos, entonces* $|X \cup Y| = |X| + |Y|$.

DEMOSTRACIÓN. (1). Si contamos los elementos de X una vez y otra vez cada uno de los elementos de Y, resulta que hemos contados dos veces los que aparecen en la intersección, luego necesitamos restar estos para calcular el número de elementos de la unión.
(2). Es una consecuencia del apartado (1). □

DEMOSTRACIÓN. [Alternativa] Si primero probamos la propiedad (2), la cual es inmediata, podemos reducir el caso (1) al caso (2) considerando las relaciones $X = (X \setminus Y) \cup (X \cap Y)$ e $Y = (Y \setminus X) \cup (X \cap Y)$, luego $X \cup Y$ es la unión de tres conjuntos disjuntos dos a dos: $X \cup Y = (X \setminus Y) \cup (Y \setminus X) \cup (X \cap Y)$, y tenemos el resultado. □

Ejemplo. 34.2.
¿Cuántos números enteros positivos, menores o iguales que 50, hay que sean múltiplos de 2 ó múltiplos de 3?

SOLUCIÓN. Llamamos X al conjunto de los enteros positivos menores que 50 y múltiplos de 2, entonces $|X| = 25$, ya que $X = \{2t \mid \ t = 1 \ldots, 25\}$. Por otro lado, sea Y el conjunto de los

enteros positivos menores que 30 y múltiplos de 3, entonces $|Y|= 16$, ya que $Y = \{3t \mid \ t = 1,\dots,16\}$.

Falta calcular ahora el conjunto $X\cap Y$, que es el conjunto de los múltiplos de 6, esto es: $X\cap Y = \{6t \mid \ t = 1,\dots,8\}$, luego $|X\cap Y|= 8$. El resultado es:

$$|X\cup Y|=|X| + |Y| - |X\cap Y|= 25 + 16 - 8 = 33.$$

□

Ejercicio. 34.3.
¿Cuántos números enteros positivos, menores o iguales que 10.000.000, hay que sean múltiplos de 3 ó de 7?

La extensión natural del Teorema 34.1. es el siguiente:

Corolario. 34.4. (Principio de inclusión–exclusión)
Dados conjuntos $X_1,\dots,X_t$, se verifica:

$$|\cup_{i=1}^t X_i|= \sum_{i=1}^t |X_i| - \sum_{1\le i_1<i_2\le t} |X_{i_1}\cap |X_{i_2}|| + \cdots + (-1)^{s+1} \sum_{1\le i_1<\cdots<i_s\le t} |X_{i_1}\cap\cdots\cap X_{i_s}| + \cdots + (-1)^{t+1} |X_1\cap\cdots\cap X_{i_t}|$$

DEMOSTRACIÓN. Basta hacer inducción sobre el número de conjuntos. El resultado es cierto para $t = 2$, y si suponemos que es cierto para t, al considerar $t+1$ conjuntos tenemos:

$$\begin{aligned}
& |\cup i = 1^{t+1} X_i| \\
= \;& |(\cup_{i=1}^t X_i)\cup X_{t+1}| \\
= \;& |\cup_{i=1}^t X_i| + |X_{t+1}| - |(\cup_{i=1}^t X_i)\cap X_{t+1}| \\
= \;& \textstyle\sum_{i=1}^t |X_i| - \sum_{1\le i_1<i_2\le t} |X_{i_1}\cap |X_{i_2}|| + \cdots \\
& + (-1)^{s+1} \textstyle\sum_{1\le i_1<\cdots<i_s\le t} |X_{i_1}\cap\cdots\cap X_{i_s}| + \cdots \\
& + (-1)^{t+1} |X_1\cap\cdots\cap X_{i_t}| + |X_{t+1}| - |\cup_{i=1}^t (X_i\cap X_{t+1})| \\
= \;& \textstyle\sum_{i=1}^t |X_i| - \sum_{1\le i_1<i_2\le t} |X_{i_1}\cap |X_{i_2}|| + \cdots \\
& + (-1)^{s+1} \textstyle\sum_{1\le i_1<\cdots<i_s\le t} |X_{i_1}\cap\cdots\cap X_{i_s}| + \cdots \\
& + (-1)^{t+1} |X_1\cap\cdots\cap X_{i_t}| + |X_{t+1}| \\
& - \Big[\textstyle\sum_{i=1}^t |X_i\cap X_{t+1}| - \sum_{1\le i_1<i_2\le t} |X_{i_1}\cap |X_{i_2}|\cap X_{t+1}| + \cdots \\
& + (-1)^{s+1} \textstyle\sum_{1\le i_1<\cdots<i_s\le t} |X_{i_1}\cap\cdots\cap X_{i_s}\cap X_{t+1}| + \cdots \\
& + (-1)^{t+1} |X_1\cap\cdots\cap X_{i_t}\cap X_{t+1}|\Big]
\end{aligned}$$

$$
\begin{aligned}
= \quad & \textstyle\sum_{i=1}^{t} |X_i| - \sum_{1\le i_1<i_2\le t} |X_{i_1}\cap |X_{i_2}|| + \cdots \\
& + (-1)^{s+1} \textstyle\sum_{1\le i_1<\cdots<i_s\le t} |X_{i_1}\cap\cdots\cap X_{i_s}| + \cdots + (-1)^{t+1} |X_1\cap\cdots\cap X_{i_t}| \\
& + |X_{t+1}| \\
& + \Big[- \textstyle\sum_{i=1}^{t} |X_i\cap X_{t+1}| + \sum_{1\le i_1<i_2\le t} |X_{i_1}\cap |X_{i_2}|\cap X_{t+1}| + \cdots \\
& + (-1)^{s+2} \textstyle\sum_{1\le i_1<\cdots<i_s\le t} |X_{i_1}\cap\cdots\cap X_{i_s}\cap X_{t+1}| + \cdots \\
& + (-1)^{t+2} |X_1\cap\cdots\cap X_{i_t}\cap X_{t+1}|\Big] \\
= \quad & \textstyle\sum_{i=1}^{t} |X_i| - \sum_{1\le i_1<i_2\le t+1} |X_{i_1}\cap |X_{i_2}|| + \cdots \\
& + (-1)^{s+1} \textstyle\sum_{1\le i_1<\cdots<i_s\le t+1} |X_{i_1}\cap\cdots\cap X_{i_s}| + \cdots \\
& + (-1)^{t+2} |X_1\cap\cdots\cap X_{t+1}|
\end{aligned}
$$

□

Ejemplo. 34.5.
Averiguar cuantos números enteros positivos primos hay menores o iguales que 120.

SOLUCIÓN. Podemos hacer el cálculo de este número mediante algún algoritmo de criba, como la criba de Eratóstenes. Pero supongamos que solo tenemos capacidad de cálculo para unos pocos números primos, como los primeros números primos son: 2, 3, 5, 7, 11, ..., y como $11^2 = 121$, solo tenemos que ver qué números enteros positivos menores que 120 son múltiplos de 2, 3, 5, ó 7 y restarlos del total de números.

Llamamos X_p al conjunto de enteros positivos menores o iguales que 120 que son múltiplos de p. En nuestro caso tenemos:

$$X_p = \{pt \mid \ t = 1, \ldots, [\frac{120}{p}]\},$$

luego tenemos un total de $[\frac{120}{p}]$ elementos en X_p:

$$|X_2| = 60; |X_3| = [\frac{120}{3}] = 40; |X_5| = 24; |X_7| = [\frac{120}{7}] = [17,1] = 17;$$

Llamamos $X_{p,q}$ al conjunto de enteros positivos menores o iguales que 120 y que son múltiplos de p y q, $p \neq q$, esto es la intersección de X_p y X_q; en nuestro caso tenemos $X_{p,q} = X_{pq}$ y resulta $|X_{p,q}| = [\frac{120}{pq}]$.

Ahora consideramos las ternas de elementos distintos dos a dos de $\{2,3,5,7\}$, obteniendo que la intersección $X_{p_1}\cap X_{p_2}\cap X_{p_3}$ tiene $[\frac{120}{p_1p_2p_3}]$ elementos, lo mismo para cuaternas.

El número de enteros positivos compuestos menores o iguales que 120 es:

$$
\begin{aligned}
&([\tfrac{120}{2}]-1)+([\tfrac{120}{3}]-1)+([\tfrac{120}{5}]-1)+([\tfrac{120}{7}]-1)\\
&-\left([\tfrac{120}{2\times 3}]+[\tfrac{120}{2\times 5}]+[\tfrac{120}{2\times 7}]+[\tfrac{120}{3\times 5}]+[\tfrac{120}{3\times 7}]+[\tfrac{120}{5\times 7}]\right)\\
&+\left([\tfrac{120}{2\times 3\times 5}]+[\tfrac{120}{2\times 3\times 7}]+[\tfrac{120}{2\times 5\times 7}]++[\tfrac{120}{3\times 5\times 7}]\right)\\
&-[\tfrac{120}{2\times 3\times 5\times 7}]\\
&=60+40+24+17-4-(20+12+8+8+5+3)+(4+2+1+1)-0\\
&=89
\end{aligned}
$$

Si tenemos 89 números compuestos, como 1 no es compuesto, pero tampoco no es primo, resulta que el número de primos es $120-(89+1)=30$. Los primos 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, 101, 103, 107, 109, 113. □

35. Principio del producto

Teorema. 35.1.
Sean X e Y dos conjuntos finitos, se verifica: $|X \times Y| = |X| \times |Y|$.

DEMOSTRACIÓN. Basta considerar $|X| = n$ y $|Y| = m$, por ejemplo sean $X = \{0, \ldots, n-1\}$ e $Y = \{0, \ldots, m-1\}$, entonces definimos una aplicación

$$f : X \times Y \longrightarrow \{0, 1, \ldots, nm-1\}$$

mediante: $f(x, y) = x \times m + y$. Es claro que f es una biyección. □

Como generalización se tiene que si $X_1, \ldots, X_t$ es una familia finita de conjuntos finitos, entonces:

$$|X_1 \times \cdots \times X_t| = |X_1| \times \cdots \times |X_t| \ .$$

Ejemplo. 35.2.
Se tiene una fila horizontal de t casillas. Cada una de ellas hay que rellenarla con un color tomado de un conjunto con s colores. ¿De cuántas formas se puede hacer este proceso?

SOLUCIÓN. Es claro que el proceso lo podemos dividir en t procesos independientes, cada uno de los cuales consiste en rellenar una casilla de uno de los colores. Como cada uno de estos procesos independientes tiene s posibilidades, resulta que el número total buscado es:

$$s \times \overset{t}{\cdots} \times s = s^t.$$

□

Ejemplo. 35.3.
Averiguar cuantas formas distintas existen rellenar una quiniela de fútbol si ésta consta de 15 casillas y cada una hay que rellenarla con uno de los signos: $1, \times, 2$.

SOLUCIÓN. $3^{14} = 4\,782\,969$. □

Ejemplo. 35.4.
Averiguar cuántas matrículas distintas se pueden construir en España si cada una de ellas constase de un número de 4 dígitos, del 0 al 9, y tres letras de entre las siguientes:

$$\{B, C, D, F, G, H, J, K, L, M, N, P, R, S, T, V, W, X, Y, Z\}.$$

SOLUCIÓN. $10^4 \times 20^3 = 80\,000\,000$. □

Ejemplo. 35.5.
Averiguar cuántos números de seis dígitos, representativos, se pueden escribir en un sistema binario. ¿Cuántos hay que contengan la secuencia 01.

SOLUCIÓN. El número es: 2^5, ya que tenemos que determinar cinco dígitos, pues el primer dígito siempre ha de ser 1.
Si queremos que tengan la secuencia 01, tenemos los siguientes casos:

$$101\_\_\_, \qquad 1\_01\_\_, \qquad 1\_\_01\_, \qquad 1\_\_\_01.$$

Cada uno de estos casos tiene huecos señalados que se puede rellenar con 0 ó 1, entonces para cada uno de los cuatro casos anteriores tenemos 2^3 números.

Observar que existen números comunes para dos casos distintos. Por ejemplo 101 01 0 es un ejemplo tanto del primer como del tercer caso. Tenemos entonces que analizar los ejemplos comunes a cada dos casos:
Casos 1 y 2, Casos 2 y 3, Casos 3 y 4: la intersección es vacía.
Casos 1 y 3: la intersección es: $\{101010, 101010\}$.
Casos 1 y 4: la intersección es: $\{101101, 101101\}$.
Casos 2 y 4: la intersección es: $\{100101, 110101\}$.

No hay intersección para tres casos.

El número total pedido es:

$$2^3 + 2^3 + 2^3 + 2^3 - (2 + 2 + 2) = 4 \times 8 - 6 = 2(16 - 3) = 26.$$

□

Observar que si se tienen dos conjuntos finitos X e Y, cada aplicación de X a Y está definida al asignar a cada elemento de X un único elemento de Y. Por tanto consiste en dar una lista de elementos de Y indizada en los elementos de X. De lo anterior obtenemos que el número total de aplicaciones distintas que existen de X a Y es: $|Y|^{|X|}$.

A consecuencia de este resultado, utilizamos al notación Y^X para referirnos al conjunto de todas las aplicaciones de X a Y.

Teorema. 35.6.
Dados dos conjuntos finitos X e Y, se verifica: $|Y^X| = |Y|^{|X|}$.

36. Variaciones

Vamos ahora a estudiar algunos tipos de aplicaciones, por ejemplo las aplicaciones inyectivas entre dos conjuntos:

Proposición. 36.1.
Dados dos conjuntos finitos X e Y, con $|X|= m$ y $|Y|= n$, el número de aplicaciones inyectivas de X a Y es: $n(n-1)\cdots(n-m+1)$.

DEMOSTRACIÓN. Si suponemos que $X = \{x_1, x_2 \ldots, x_m\}$, cada aplicación inyectiva $f : X \longrightarrow Y$ está determinada por el valor de los elementos $f(x_1)$, $f(x_2)$, $\ldots$, $f(x_m)$. Resulta que $f(x_1)$ puede ser elegido como cualquiera de los n elementos de Y. Una vez elegido $f(x_1)$, para elegir $f(x_2)$ debemos retirar de Y el valor $f(x_1)$, entonces tenemos $n-1$ posibles elecciones. Para elegir $f(x_2)$ tenemos $n-2$ posibles elecciones, y en general para elegir $f(x_t)$ tenemos $n-t+1$ posibles elecciones, ya que antes hemos tenido que retirar $f(x_1)$, $\ldots$, $f(x_{t-1})$. Como consecuencia tenemos $n(n-1)\ldots(n-m+1)$. Observar que si $n < m$, entonces no existe ninguna aplicación inyectiva de X a Y, y esto está reflejado en que el factor $(n-m+1)$ es igual a cero. □

Cada una de las aplicaciones inyectivas de X a Y selecciona m elementos de Y, esto es, selecciones m elementos de un conjunto que tiene n; llamamos **variación** a cada una de estas selecciones. , por esto el número de variaciones de un conjunto de n elementos tomados m a m es $n(n-1)\cdots(n-m+1)$, y se representa por V_m^n, $V_{n,m}$, ó $V(n,m)$.

Observar que en una variación intervienen dos elementos fundamentales, uno es el orden, y otro es que los elementos no se repiten. Por este último hecho se suele utilizar también para las variaciones el nombre de **variaciones sin repetición**.

Ejemplo. 36.2.
En una sociedad que consta de 40 miembros hay que elegir la junta directiva que está formada por tres cargos: presidente, tesorero y secretario, que deben ser ocupados por personas distintas. ¿De cuántas formas se puede formar la junta directiva?

SOLUCIÓN. Está claro que se trata de variaciones sin repetición, pues dos cargos no pueden ser ocupados por la misma persona y los cargos son distinguibles, así pues el número pedido es: $40 \times 39 \times 38$. □

El caso de variaciones con repetición ha sido indirectamente estudiado en la sección 34.

Problema. 36.3.
Una variación del ejemplo anterior es el siguiente: En la sociedad anterior hay que elegir un conjunto de tres representantes, indistinguibles entre sí. ¿De cuántas formas se pueden elegir

éstos?

Veamos una forma alternativa de introducir las variaciones sin y son repetición.

Hacemos la distinción entre **conjunto**: colección finita o infinita de elementos entre los que no hay dos repetidos ni orden entre ellos, **familia**: colección de elementos entre los que puede hacer elementos repetidos y **lista**: familia en la que se tiene en cuenta el orden relativo de sus elementos.

Un ejemplo de conjunto es $\{A, B, C\}$, un ejemplo de familia es: $\{A, B, A, C, D\}$, la cual considerada como lista es distinta, por ejemplo, de $\{A, A, B, C, D\}$.

Dado un conjunto, una familia o una lista X, llamamos **longitud** de X al número de elementos de X.

Ejemplo. 36.4.
Dado el conjunto $\mathcal{A} = \{A, B, C, \ldots, Z\}$ consideramos la familia $\mathcal{F}_1$ de todas las palabras de tres letras de $\mathcal{A}$. La longitud de esta familia es: $27 \times 27 \times 27$.

Llamamos a cada uno de los componentes de la familia $\mathcal{F}_1$ una *variación con repetición* del conjunto $\mathcal{A} = \{A, B, C, \ldots, Z\}$. En general si tenemos un conjunto con n elementos, $\mathcal{C} = \{a_1, \ldots, a_n\}$, la longitud de la familia de las palabras de t elementos que se pueden formar con elementos de $\mathcal{C}$ es igual a n^t.

Ejemplo. 36.5.
Dado el conjunto $\mathcal{A} = \{A, B, C, \ldots, Z\}$, consideramos la familia $\mathcal{F}_2$ de todas las palabras de tres letras en las que no hay letras repetidas. La longitud de la lista $\mathcal{F}_2$ es: $27 \times 26 \times 25$.

Llamamos a cada uno de los componentes de la familia $\mathcal{F}_2$ una *variación* del conjunto $\mathcal{A} = \{A, B, C, \ldots, Z\}$. En general si tenemos un conjunto con n elementos, $\mathcal{C} = \{a_1, \ldots, a_n\}$, la longitud de la familia de las palabras de t elementos, en las que no hay elementos repetidos, que se pueden formar con elementos de $\mathcal{C}$ (es claro que $t \leq n$) es igual a $n(n-1)\cdots(n-t+1)$.

Ejercicio. 36.6.
¿Cuántos números de tres cifras hay en los que todas sus cifras sean impares?

SOLUCIÓN. Tenemos el conjunto $\{1, 3, 5, 7, 9\}$, tenemos que formar las variaciones con repetición de este conjunto formadas por tres elementos; su número es: $5^3 = 125$. □

Ejercicio. 36.7.
¿Cuántos números de tres cifras hay en los que todas sus cifras sean pares?

SOLUCIÓN. Las cifras pares son: $\{0, 2, 4, 6, 8\}$. Un número de tres cifrar tiene la primera cifra distinta de cero, luego puede ser cualquiera de los elementos del conjunto $\{2, 4, 6, 8\}$, esto es,

hay cuatro posibilidades. En cambio las restantes cifras pueden ser cualquiera de los elementos del conjunto $\{0,2,4,6,8\}$. Tenemos entonces que el número solicitado es: $4\times5\times5=100$. □

Ejercicio. 36.8.
¿Cuántos números de tres cifras hay en los que todas sus cifras sean múltiplos de tres?

Ejercicio. 36.9.
¿Cuántos números, escritos en binario, tienen a lo más diez cifras?

SOLUCIÓN. Si un número tiene diez o menos cifras, este número se puede escribir en la forma $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$, en donde a_i puede tomar el valor 0 ó 1. Entonces el número solicitado es: 2^{10}. □

Ejercicio. 36.10.
¿Cuántas palabras se pueden formar con las tres consonantes, B, C y D, y las cinco vocales, sin repetir ninguna?

Ejercicio. 36.11.
Cuántas palabras se pueden formar con las letras de la palabra JESÚS sin repetir ninguna letra?

Ejercicio. 36.12.
¿Cuántos números de tres cifras tienen todas sus cifras todas distintas?

Ejercicio. 36.13.
Una biblioteca tiene exactamente ciento cincuenta libros. Si los colocamos todos en un mismo estante, ¿de cuántas formas podemos hacerlo?

Ejercicio. 36.14.
Manuel toma notas en clase en folios en los que escribe por una sola cara. Al final de la clase se le han caído los folios al suelo, y al recogerlos comprueba que están desordenados. Si tiene cinco folios escritos, ¿de cuántas formas puede ordenarlos?

Ejercicio. 36.15.
*Ana ha comprado un coche cuya matrícula es: 1234XYZ. ¿Cuántos coches habrá que tengan una matrícula del tipo ****XYZ formada con los números de la matrícula de Ana?*

37. Permutaciones

Las variaciones sin repetición de n elementos tomados de n en n se llaman **permutaciones**. Así el número de permutaciones de n elementos es igual a $V_n^n = n(n-1)\cdots 1 = n!$. Representaremos este número por P_n.

En efecto el número de permutaciones de un conjunto de n elementos es el número de ordenaciones que del mismo podemos hacer.

38. Principio del palomar

Un enunciado de este principio puede hacerse en términos de aplicaciones.

Proposición. 38.1. (Principio del palomar)
Si X e Y son conjuntos finitos con $|X| = m > n = |Y|$, entonces ninguna aplicación de X en Y es inyectiva.

En otros términos, si se dispone de m objetos que hay que distribuir en n cajas, siendo $m > n$, entonces al menos una caja tiene que contener dos objetos.

Ejemplo. 38.2.
Si en clase hay 110 alumnos y las calificaciones van de 0 a 10, se permite una única cifra decimal, entonces al menos dos alumnos tienen la misma calificación.

Ejemplo. 38.3.
Con el actual sistema de matriculación hay coches que tienen en su matrícula los mismos números (en este caso no consideramos las letras que los acompañan).

Ejercicio. 38.4.
Cualquier número entero tiene un múltiplo que, en su expresión decimal, está formado únicamente por los dígitos 0 y 1.

DEMOSTRACIÓN. Dado $n \in \mathbb{Z}$, si $n = 0, 1$, entonces es claro. Supongamos que $n \geq 2$, consideramos los números:

$$x_0 = 1, x_1 = 11 = 10 + 1, x_2 = 111 = 10^2 + 10 + 1, \ldots,$$
$$x_n = 11 \overset{n}{\cdots} 11 = 10^n + 10^{n-1} + \cdots + 10 + 1.$$

Al considerar las clases de estos números en $\mathbb{Z}_n$, al menos dos de estas clases deben coincidir, y por tanto tenemos el resultado. □

Ejercicio. 38.5.
Demostrar que en cada conjunto de n números enteros positivos siempre podemos encontrar un subconjunto tal que la suma de sus elementos sea múltiplo de n.

DEMOSTRACIÓN. Supongamos que el conjunto es $\{x_1, \ldots, x_n\}$ y definimos n elementos $\{y_1, \ldots, y_n\}$, mediante:

$$y_i = x_1 + \cdots + x_i, \qquad l \leq i \leq n.$$

Al reducir los y_i módulo n tenemos n elementos en $\mathbb{Z}_n$, y por tanto uno de ellos es cero o hay dos que son iguales. Si $\overline{y_i} = \overline{y_{i+s}}$, entonces resulta que $y_{i+s} - y_i = x_{i+1} + \cdots + x_{i+s}$ es un múltiplo de n. □

El Principio del Palomar admite una generalización que nos da una aproximación más fina. al mismo resultado.

Proposición. 38.6. (Principio del palomar generalizado)
Si se distribuyen n objetos en m recipientes, al menos uno de los recipientes contiene $[\frac{n}{m}]$ *objetos.*
Además, si $n > n[\frac{n}{m}]$*, entonces uno de los recipientes contiene* $[\frac{n}{m}]+1$ *objetos.*

DEMOSTRACIÓN. Supongamos que en una distribución todos los recipientes tienen menos de $[\frac{n}{m}]$ objetos, entonces el número total de objetos en los recipientes es estrictamente menor que $m[\frac{n}{m}] \leq n$, lo que es una contradicción.
La segunda parte es inmediata. □

Ejemplo. 38.7.
Si en un aparcamiento hay 54 515 automóviles, todos con matrícula nueva, entonces al menos seis coches tienen en su matrícula el mismo número.

39. Combinaciones

Continuemos con el Problema 36.3..

Si tenemos un conjunto de n elementos y consideramos variaciones de m elementos, como en las variaciones se tiene en cuenta el orden, para cada una de ellas tenemos un total de $m!$ que tienen los mismos elementos, posiblemente en orden distinto. Por tanto el número de subconjuntos de m elementos que tiene un conjunto de n elementos es:

$$\frac{V_m^n}{m!}$$

Cada uno de los conjuntos elegidos se llama una **combinación**, y por tanto el número anterior es el número de combinaciones de un conjunto de n elementos tomados de n en n.

Es claro que se tiene:

$$\frac{V_m^n}{m!} = \frac{n(n-1)\cdots(n-m+1)}{n!} = \frac{n!}{m!n!}.$$

Si representamos este número por $\binom{n}{m}$, se tiene la igualdad $\binom{n}{m} = \binom{n}{n-m}$. Llamamos a $\binom{n}{m}$ un **número binomial**.

Este número binomial se representa también por $C_{n,m}$, C_m^n ó $C(n,m)$, aunque preferimos la notación inicial.

Una combinación es una familia de elementos, esto es, el orden de los mismos no es tenido en cuenta.

Ejemplo. 39.1.
Las listas *ABC* y *BCA* son la misma familia, y por lo tanto son la misma combinación.

Ya hemos utilizamos los números binomiales para la expresión de las potencias de un binomio en términos de productos de potencias de los sumandos, **Teorema del binomio de Newton**.

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

El cálculo de los coeficientes del binomio de Newton se puede también obtener a partir del

conocido **Triángulo de Tartaglia**.

						1								
					1		1							
				1		2		1						
			1		3		3		1					
		1		4		6		4		1				
	1		5		10		10		5		1			

El algoritmo para construir la tabla es bien conocido. Cada término es la suma de los dos justo encima en la fila superior. Esta propiedad es justo la que aparece en el siguiente Lema, para el que supondremos que $\binom{n}{m}$ es cero si $m < 0$ ó $m > n$:

Lema. 39.2.
Para cada par de números naturales n y m se verifica:

$$\binom{n}{m-1} + \binom{n}{m} = \binom{n+1}{m}.$$

DEMOSTRACIÓN. Es inmediato del siguiente desarrollo:

$$\begin{aligned}
&\tbinom{n}{m-1} + \tbinom{n}{m} \\
&= \frac{n!}{(m-1)!(n-m+1)!} + \frac{n!}{m!(n-m)!} \\
&= \frac{n!m}{(m-1)!m(n-m+1)!} + \frac{n!(n-m+1)}{m!(n-m)!(n-m+1)} \\
&= \frac{n!m+n!(n-m+1)}{m!(n-m+1)!} \\
&= \frac{n!(m+n-m+1)}{m!(n-m+1)!} \\
&= \frac{(n+1)!}{m!(n-m+1)!} = \tbinom{n+1}{m}.
\end{aligned}$$

□

DEMOSTRACIÓN. [Alternativa.] Una forma alternativa de obtener este resultado es la siguiente: si queremos elegir m elementos de un conjunto de $n+1$ elementos $\{x_0, \ldots, x_n\}$, podemos seleccionar uno de ellos, por ejemplo x_0 y considerar las elecciones en las que aparezca x_0, esto es las selecciones de $m-1$ elementos que podemos hacer del conjunto $\{x_1, \ldots, x_n\}$, cuyo número es $\binom{n}{m-1}$, y las selecciones que podemos hacer en las que no interviene x_0, esto es, las selecciones de m elementos que podemos hacer del conjunto $\{x_1, \ldots, x_n\}$, cuyo número es $\binom{n}{m}$. Ahora el Principio de la suma nos dice que el resultado es: $\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$. □

Ejemplo. 39.3.
Determinar el número de subconjuntos de 2 elementos que tiene el conjunto $X = \{a, b, c, d, e, f, g, h\}$.

SOLUCIÓN. Como $|X| = 8$, el número buscado es $\binom{8}{2} = \frac{8\times 7}{2!} = 28$. □

Ejemplo. 39.4.
Si queremos calcular las palabras de n bits que contienen un número determinado, s, de unos y ceros, podemos trabajar como sigue:

SOLUCIÓN. Como las palabras serán de n bits, llamamos b_i al i–ésimo bit. Si la palabra tiene s bits iguales a 1, basta elegir s elementos del conjunto $\{b_1, \ldots, b_n\}$. Los no elegidos serán los que son iguales a 0. Observar que no importa el orden de los b_i elegidos, por tanto tenemos un ejemplo de combinaciones. En este caso el resultado es:

$$\binom{n}{s} = \frac{n!}{s!(n-s)!}.$$

□

Ejemplo. 39.5.
El conjunto de los alumnos de una clase está formado por 10 mujeres y 9 hombres, se quiere elegir un equipo de seis personas entre las que haya al menos un hombre y una mujer. ¿De cuántas formas se podrá formar el equipo?

SOLUCIÓN. Hacemos un recuento de todas las posibilidades, esto es, averiguamos cuantos equipos se pueden formar en los que hay únicamente mujeres, el número es: $\binom{10}{6}$, y el número de equipos en los que haya únicamente hombres, el número es: $\binom{9}{6}$. Como el número total de posibles equipos es: $\binom{19}{6}$, resulta, por el principio de la suma, que el número que queremos averiguar es:

$$\binom{19}{6} - \binom{10}{6} - \binom{9}{6} = 27\,132 - 210 - 84 = 26\,838.$$

□

TABLA RESUMEN. Elección de m objetos de un conjunto de n objetos distinguibles.

	Con orden	Sin orden
Con repetición	V_m^n	$\binom{n}{m}$
Sin repetición	n^m	$CR(n,m) = \binom{n+m+-1}{m}$

40. Combinaciones con repetición

Vamos a estudiar ahora el caso en que se produce la repetición de elementos al hacer una elección. Si tenemos un conjunto con n elementos y queremos elegir m de ellos, si importa el orden el que lo hagamos tenemos el caso de variaciones con repetición que ya hemos estudiado en la sección 34. Si no importa el orden tenemos combinaciones con repetición.

El ejemplo arquetípico es aquel en el que tenemos que hacer cuatro extracciones de bolas de una bolsa en la que hay tres bolas diferentes: A, B y C. Observamos que, como no influye el orden, todos los casos que se presentan son:

$AAAA$	$AAAB$	$AABB$	$ABBB$	$BBBB$
$AAAC$	$AACC$	$ACCC$	$CCCC$	$BCCC$
$BBCC$	$BCCC$	$ABBC$	$ABCC$	$AABC$

Para buscar un método algorítmico que nos permita calcular este número podemos introducir dos nuevos símbolos que van a ser separadores de las letras A, B y C, estos son $\|$ y $\|$, y la forma en que actuan es la siguiente:

$AAAA\|\|\|$	$AAA\|B\|\|$	$AA\|BB\|\|$	$A\|\|BBB\|\|$	$\|\|BBBB\|\|$
$AAA\|\|\|C$	$AA\|\|\|CC$	$A\|\|\|CCC$	$\|\|\|CCCC$	$\|\|B\|\|CCC$
$\|\|BB\|\|CC$	$\|\|B\|\|CCC$	$A\|\|BB\|\|C$	$A\|\|B\|\|CC$	$AA\|\|B\|\|C$

Observar que cada uno de los casos queda perfectamente determinado por la posición de los separadores $\|$ y $\|$, y que estos deben ocupar dos posiciones de un conjunto de 6, esto es, el número de posibilidades es: $\binom{6}{2}$.

Este ejemplo puede extenderse al caso general de **combinaciones con repetición**, en el que se eligen m elementos, posiblemente con repetición, de un conjunto de n elementos. En este caso debemos tener $n-1$ separadores, y estos pueden colocarse en un total de $n+m-1$ posiciones, luego el resultado es:

$$\binom{n+m-1}{m-1} = \binom{n+m-1}{n}.$$

Emplearemos la notación CR_m^n para referimos al número de combinaciones con repetición de n objetos tomados de m en m.

Ejemplo. 40.1.
Dada la ecuación $X+Y+Z+T=13$, determinar cuantas soluciones tiene en el conjunto $\mathbb{N}$ de los números naturales.

SOLUCIÓN. Podemos traducir el problema a un contexto gráfico del siguiente modo: se tratar de sacar 13 bolas de un cajón que tiene bolas con 4 etiquetas distintas: X, Y, Z y T. El número

de extracciones iguales a X será el valor de X, el de Y el valor de Y, el de Z el valor de Z y el de T el valor de T. Por tanto el número de soluciones distintas es:

$$\binom{13+4-1}{4-1} = \binom{16}{3} = 560.$$

□

Una variación de este ejemplo es la siguiente.

Ejemplo. 40.2.
Dada la ecuación $X+Y+Z+T=13$, determinar cuantas soluciones tiene en el conjunto $\mathbb{N}$ de los números naturales en las que ningún valor sea 0.

SOLUCIÓN. En este caso hacemos un cambio de variable, llamando $X' = X-1$, $Y' = Y-1$, $Z' = Z-1$ y $T' = T-1$, entonces la ecuación es: $X'+Y'+Z'+T' = 9$, y el número de soluciones, según el ejemplo anterior, es: $\binom{9+4-1}{4-1} = \binom{12}{3} = 220$. □

Podemos entonces calcular el número de soluciones entre las que al menos hay una nula.

Ejemplo. 40.3.
Dada la ecuación $X+Y+Z+T=13$, determinar cuantas soluciones tiene en el conjunto $\mathbb{N}$ de los números naturales en las al menos un valor es 0.

SOLUCIÓN. Basta calcular la diferencia $\binom{16}{3} - \binom{12}{3} = 560 - 220 = 340$. □

Otro problema del mismo tipo es el siguiente:

Ejemplo. 40.4.
Consideramos n bolas indistinguibles y m cajas distinguibles, ordenadas en una fila horizontal. ¿De cuántas formas se pueden distribuir las n bolas en las m cajas?

SOLUCIÓN. Consideramos las n bolas en una fila e insertamos $m-1$ separadores entre ellas. Tenemos en total $n+m-1$ posiciones. Si se elige una de las posiciones se tienen dos grupos, y por tanto si se cogen $m-1$ posiciones se tienen m grupos, y por tanto m cajas. La solución es: $\binom{n+m-1}{m-1} = CR(n,m) = \binom{n+m-1}{n}$. □

Podemos modificar el ejemplo en la siguiente forma:

Ejemplo. 40.5.
Consideramos n bolas indistinguibles y m cajas distinguibles, ordenadas en una fila horizontal. ¿De cuántas formas se pueden distribuir las n bolas en las m cajas de forma que ninguna caja quede vacía?

SOLUCIÓN. Consideramos las n bolas en una fila e insertamos separadores entre cada dos de ellas, y al inicio y al final:

$$\_ \circledast \_ \circledast \_ \cdots \_ \circledast \_ \circledast \_$$

Observar que tenemos $n+1$ separadores, de los cuales los de los extremos son de diferente tipo. Para determinar las m cajas, basta selecciones $m-1$ separadores (de los que no son extremos). Esto se puede hacer de $\binom{n-1}{m-1}$ formas distintas. □

SOLUCIÓN. [Alternativa] Podemos también razonar como sigue: Del total de bolas reservamos m, una para cada caja, de esta forma nos quedan $n-m$. Se trata entonces de distribuir $n-m$ bolas en m cajas distinguibles, y este valor, por el ejemplo 40.4., es $CR(n-m,m)$, por tanto el valor es: $CR(n-m,m)=\binom{n-1}{m-1}$. □

TABLA RESUMEN. Distribuir n bolas en m cajas.

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles	m^n	
Indistinguibles	$CR(m,n)=\binom{m+n-1}{n}$	

TABLA RESUMEN. Distribuir n bolas en m cajas (con al menos una bola en cada caja).

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles		
Indistinguibles	$\binom{n-1}{m-1}$	

Vamos a completar estas tablas.

Distribuir n bolas indistinguibles en m cajas indistinguibles, con al menos una bola en cada caja. Esto es lo mismo que hallar el tipo de particiones de un conjunto de n elementos en m subconjuntos, esto es, solo nos interesa el número de elementos de estos subconjuntos. Por ejemplo si tenemos 4 bolas, podemos distribuirlas en dos subconjuntos en dos formas: 1+3 ó 2+2, ya que no importan cuales son las bolas ni el orden de las cajas. En el caso general se trata pues de hallar el número de tipos de particiones de un conjunto de n elementos.

Llamamos $\Pi(n)$ el número de tipos de particiones de un conjunto de n elementos. Si $n=4$, entonces los tipos de particiones son: 4, 1+3, 2+2, 1+1+2, 1+1+1+1, luego $\Pi(4)=5$.

Este número $\Pi(n)$ se puede descomponer como la siguiente suma, si llamamos $\Pi(n,i)$ el número de tipos de particiones de un conjunto de n elementos en i subconjuntos: $\Pi(n)=\sum_{i=1}^{n}\Pi(n,i)$.

Una propiedad sencilla es la siguiente: $\Pi(n) = \Pi(2n, n)$, la razón es que al considerar un tipo de partición de un conjunto de $2n$ elementos, una partición asociada a este tipo tiene en n subconjuntos (no vacíos), como cada uno de ellos tiene al menos un elemento, si quitamos de cada uno un elemento, eliminando los conjuntos vacíos tenemos una partición de un conjunto de n elementos, y por tanto un tipo. Esta correspondencia es una biyección.

De cara a determinar los valores de $\Pi(n)$, necesitamos destacar algunas propiedades inmediatas:

$$\Pi(n, m) = 0 \text{ si } m > n;$$
$$\Pi(n, n) = \Pi(n, 1) = 1;$$
$$\Pi(n, i) = \sum_{j=1}^{i} \Pi(n-i, j);$$
$$\Pi(n, i) = \Pi(n-1, i-1) + \Pi(n-i, i).$$

Tenemos que la igualdad $\Pi(n, i) = \Pi(n-1, i-1) + \Pi(n-i, i)$ es consecuencia de considerar los tipos de particiones en los que uno de los subconjuntos es unitario, $(\Pi(n-1, i-1))$, y los tipos de particiones en los que todo subconjunto tiene más de un elemento $(\Pi(n-i, i))$.

Estas reglas permiten el cálculo de $\Pi(n, m)$ para todos los valores n y m.

Por lo tanto el número de formas distintas en que se puede distribuir n bolas indistinguibles en m cajas indistinguibles es: $\Pi(n, m)$.

Distribuir n bolas indistinguibles en m cajas indistinguibles.

Si seguimos con el razonamiento anterior, basta añadir m bolas a las n anteriores, de esta forma podemos reducir al caso anterior en el que en cada caja había al menos una bola. Por tanto el resultado es: $\Pi(n+m, m)$.

TABLA RESUMEN. Distribuir n bolas en m cajas.

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles	m^n	
Indistinguibles	$CR(m, n) = \binom{m+n-1}{n}$	$\Pi(n+m, m)$

TABLA RESUMEN. Distribuir n bolas en m cajas (con al menos una bola en cada caja).

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles		
Indistinguibles	$\binom{n-1}{m-1}$	$\Pi(n, m)$

Distribuir n bolas distinguibles distribuidas entre m cajas distinguibles, con al menos una bola en cada caja. Observamos que el número de distribuirlas sin la restricción de que todas las cajas sean no vacías es m^n, la razón es que cada distribución se puede identificar con una aplicación del conjunto $\{1,2,\ldots,n\}$ en $\{1,2,\ldots,m\}$, que asigna a cada bola su caja. Llamamos N al total de estas distribuciones.

Llamamos N_i a las distribuciones de N en las que la caja i–ésima es vacía, entonces queremos calcular el cardinal de $N \setminus (\cup_{i=1}^m N_i)$. El cardinal de N_i es $(m-1)^n$, y es claro que el cardinal de $N_i \cap N_j$ es $(m-2)^n$, si $i \neq j$, y en general el cardinal de $N_{i_1} \cap \cdots \cap N_{i_t}$ es $(m-t)^n$. Usando el principio de inclusión–exclusión el cardinal pedido es:

$$\begin{aligned}
&|N| - |\cup_{i=1}^m N_i| \\
&= m^n - (\textstyle\sum_{j=1}^m (-1)^{j+1} \sum_{1\le i_1<\cdots<i_j\le m} |N_{i_1} \cap \cdots \cap N_{i_j}|) \\
&= m^n - (\textstyle\sum_{j=1}^m (-1)^{j+1} \sum_{1\le i_1<\cdots<i_j\le m} (m-j)^n) \\
&= m^n + \textstyle\sum_{j=1}^m (-1)^j \binom{m}{j} (m-j)^n \\
&= \textstyle\sum_{j=0}^m (-1)^j \binom{m}{j} (m-j)^n.
\end{aligned}$$

TABLA RESUMEN. Distribuir n bolas en m cajas.

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles	m^n	
Indistinguibles	$CR(m,n) = \binom{m+n-1}{n}$	$\Pi(n+m,m)$

TABLA RESUMEN. Distribuir n bolas en m cajas (con al menos una bola en cada caja).

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles	$\sum_{j=0}^m (-1)^j \binom{m}{j} (m-j)^n$	
Indistinguibles	$\binom{n-1}{m-1}$	$\Pi(n,m)$

Distribuir n bolas distinguibles distribuidas entre m cajas indistinguibles, con al menos una bola en cada caja.

Retomamos el caso anterior en el que las cajas eran distinguibles, el número es: $\sum_{j=0}^m (-1)^j \binom{m}{j} (m-j)^n$. Si ahora consideramos las cajas indistinguibles, resulta que como tenemos m cajas, tendremos que dividir poe $m!$. El valor es:

$$\sum_{j=0}^{m} (-1)^j \binom{m}{j} (m-j)^n.$$

Llamamos a est número el **número de Stirling de segunda clase**, y se representa por $\{{n \atop m}\}$.

Para calcular los números de Stirling se segunda clase se deben tener en cuenta las siguientes propiedades:

$$\{{n \atop 1}\} = 1 = \{{n \atop n}\};$$
$$\{{n \atop m}\} = \{{n-1 \atop m-1}\} + m\{{n-1 \atop m}\}.$$

Para probar esta igualdad consideramos una de las bolas, por ejemplo la n–ésima, si es la única que pertenece a una caja, el número de casos es: $\{{n-1 \atop m-1}\}$, y si está en una caja, junto con otras, primero consideramos las distribuciones de éstas, el número es: pertenece $\{{n-1 \atop m}\}$, y ahora como la n–ésima puede estar en m cajas, el número que tenemos que sumar es: $m\{{n-1 \atop m}\}$. pertenezca a

Distribuir n bolas distinguibles distribuidas entre m cajas indistinguibles.

Basta ver el caso de distribuir las n bolas en $1, 2, \ldots, m$ cajas y sumar. El resultado es:

$$\{{n \atop 1}\} + \{{n \atop 2}\} + \cdots + \{{n \atop m}\} = \sum_{i=1}^{m} \{{n \atop i}\}.$$

TABLA RESUMEN. Distribuir n bolas en m cajas.

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles	m^n	$\sum_{i=1}^{m} \{{n \atop i}\}$
Indistinguibles	$CR(m,n) = \binom{m+n-1}{n}$	$\Pi(n+m, m)$

TABLA RESUMEN. Distribuir n bolas en m cajas (con al menos una bola en cada caja).

Bolas↓—Cajas→	Distinguibles	Indistinguibles
Distinguibles	$\sum_{j=0}^{m} (-1)^j \binom{m}{j} (m-j)^n$	$\{{n \atop m}\}$
Indistinguibles	$\binom{n-1}{m-1}$	$\Pi(n, m)$

41. Permutaciones con repetición

Ya hemos estudiado el ejemplo de las permutaciones, se trata ahora de incluir la posibilidad de que exista repetición entre los elementos a considerar. Por ejemplo, si se considera la palabra ALCANTARILLA, ¿de cuántas formas se puede reordenar sus letras para obtener palabras distintas?.

Observar que tenemos 4 Aes, por lo que la permutación de las mismas entre sí siempre produce la misma palabra; como hay 4! de estas combinaciones, el número total de permutaciones de 12 letras tenemos que dividirlo por 4!. Lo mismo tenemos que hacer con aquellas otras letras que se repiten, en este caso la L, que se repite 3 veces.

Así pues el número de palabras distintas que podemos formar con las letras de la palabra ALCANTARILLA es:

$$\frac{12!}{4!3!}.$$

Podemos enunciar entonces el siguiente resultado.

Proposición. 41.1.
Si se tienen n objetos de t tipos distintos, de los que del tipo i tenemos n_i iguales entre sí, entonces las formas distintas en que podemos ordenar los n elementos son:

$$\frac{n!}{n_1!\cdots n_2!}.$$

DEMOSTRACIÓN. Se considera el número total de ordenaciones, permutaciones, de n objetos, este número es $n!$. De estos, al considerar los objetos del tipo i, como hay exactamente n_i, tenemos $n_1!$ que son iguales y tienen los elementos de tipo distinto a i en la misma posición, luego el número hay que dividirlo por $n_i!$ Como este razonamiento hay que hacerlo para cada índice, tenemos el resultado. □

DEMOSTRACIÓN. [Alternativa.] Supongamos que disponemos de n huecos que hay que rellenar con los n elementos. Consideramos los elementos de tipo 1, para estos sólo tenemos que elegir las posiciones en los que los colocaremos, pero es no es necesario elegir orden entre ellas, por lo tanto el número total de elecciones es: $\binom{n}{n_1}$.

Ahora vamos a colocar los elementos de tipo 2, que siguiendo el mismo procedimiento se podrán colocar en $\binom{n-n_1}{n_2}$. Entonces, tras tratar los elementos de todos los tipos tenemos:

$$\begin{aligned}
&\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-\cdots-n_{t-1}}{n_t}\\
&=\frac{n!}{n!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdots\frac{(n-n_1-\cdots-n_{t-1})!}{n_t!0!}\\
&=\frac{n!}{n_1!n_2!\cdots n_t!}.
\end{aligned}$$

□

Las permutaciones con repetición pueden ser interpretadas en varios contextos. Veamos uno de ellos.

Ejemplo. 41.2.
Se consideran t cajas ordenadas y se consideran n objetos indistinguibles. ¿De cuántas formas se pueden distribuir los n objetos entre las t cajas de forma que en la caja i–ésima haya n_i objetos y que $n_1 + \cdots + n_t = n$?

SOLUCIÓN. La traducción del problema al caso estudiado se basa en ordenar n objetos de t tipos distintos tales que del tipo i hay n_i cajas. □

Ejemplo. 41.3.
¿De cuantas formas se pueden distribuir 6 cartas de una baraja de 40 cartas entre 4 jugadores?

SOLUCIÓN. La traducción que hacemos del problema es la siguiente: consideramos 5 tipos, uno para cada jugador y un quinto para el resto. Se trata de hacer una permutación de 40 objetos, de 5 tipos distintos: 1, 2, 3, 4 y 5, de forma que $n_1 = n_2 = n_3 = n_4 = 5$ y $n_5 = 16$. Por tanto el número es:

$$\frac{40!}{6!6!6!6!16!} = 145\,109\,380\,709\,331\,781\,142\,400.$$

□

Generalizamos los números binomiales $\binom{n}{m}$ a los **números multinomiales**, definidos en la forma:

$$\binom{n}{n_1 \ \cdots \ n_t} = \frac{n!}{n_1! \cdots n_t!},$$

con $n_1 + \cdots + n_t = n$.

Ejercicio. 41.4.
Dados enteros positivos o nulos tales que $n_1 + \cdots + n_t = n + 1$, entonces se verifica:

$$\sum_{i=1}^{t} \binom{n}{n_1 \ \cdots \ n_i - 1 \ \cdots \ n_t} = \binom{n+1}{n_1 \ \cdots \ n_t},$$

siendo $\binom{n}{n_1 \cdots n_i - 1 \cdots n_t} = 0$ si $n_i = 0$.

Ejercicio. 41.5. (Teorema multinomial)
Dadas indeterminadas $X_1, \ldots, X_t$ sobre un cuerpo K, en el anillo de polinomios $K[X_1, \ldots, X_t]$ se verifica la igualdad:

$$(X_1 + \ldots + X_t)^n = \sum_{n_1 + \cdots + n_t = n} \binom{n}{n_1 \ \cdots \ n_t} X_1^{n_1} \cdots X_t^{n_t}.$$

Si observamos los exponentes de los sumandos de la suma

$$\sum_{n_1+\cdots+n_t=n} \binom{n}{n_1 \ \cdots \ n_t} X_1^{n_1} \cdots X_t^{n_t},$$

observamos que todos suman n. Para averiguar cuantos sumandos hay en la suma anterior basta ver de cuantas formas distintas, importando el orden de los sumandos, se puede escribir un número natural como suma de t números naturales, esto es, el número de soluciones en $\mathbb{N}$ de la ecuación $Y_1 + \cdots + Y_t = n$. Ver Ejemplo 40.1.

Ejercicio. 41.6.
*Bernardo ha comprado un coche antes que Ana, por eso la matrícula de este coche es: 1233XYZ. ¿Cuántos coches habrá que tengan una matrícula del tipo ****XYZ formada con los números de la matrícula de Bernardo?*

SOLUCIÓN. Supongamos que tenemos tres elementos A,B y C. Se trata de calcular las diferentes formas en que podemos ordenar A,B,C,C. Una forma de hacer esto es etiquetar C de dos formas, por ejemplo mediante subíndices, tenemos entonces la familia $\{A, B, C_1, C_2\}$, la cual la podemos ordenar de $4 \times 3 \times 2 \times 1 = 24$ formas distintas. Las configuraciones C_1ABC_2 y C_2ABC_1 producen la configuración $CABC$, y esto es general, esto es, para cada configuración de $\{A, B, C\}$ tenemos dos configuraciones de $\{A, B, C_1, C_2\}$, luego el número que andamos buscando es: $\frac{4\times3\times2\times1}{2} = 12$.

Aplicando al caso en que $A = 1$, $B = 2$ y $C = 3$, resulta que habrá doce matrículas distintas.
□

Tenemos entonces el problema de determinar cuantas configuraciones se pueden formar con t elementos, por ejemplo $a_1, \ldots, a_t$, de los cuales cada a_i se repite n_i, para $i = 1, \ldots, r$. La solución es:

$$\frac{(n_1 + \cdots + n_t)!}{n_1! \cdots n_t!}.$$

Ejemplo. 41.7.
El número del carnet de identidad de Cándido es 12421241. ¿Cuántos carnet de identidad se pueden formar con estos números?

SOLUCIÓN. El número 1 se repite tres veces, el número 2 se repite tres veces y el número 4 se repite dos veces. El número pedido es:

$$\frac{(3+3+2)!}{3!3!2!} = \frac{8!}{3!3!2!} = \frac{8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2}{3 \times 2 \times 3 \times 2 \times 2} = 7 \times 2 \times 5 \times 4 \times 2 = 5{,}600.$$

□

Ejercicio. 41.8.
Hacer el mismo problema para los números:

1. *12121212*
2. *11112233*
3. *11111222*
4. *11111122*
5. *11111112*

Ejercicio. 41.9.
¿Cuál es la letra del carnet de identidad de Cándido?

SOLUCIÓN. Este es un pequeño cálculo en que utilizaremos la división euclídea de números enteros y una biyección. Dado el número del DNI se divide éste por 23 para calcular el resto de la división, que como sabéis es un número comprendido entre 0 y 22. Se establece la biyección que si indica a continuación entre el conjunto $\{0, 1, \ldots, 22\}$ y el conjunto de letras $\{A, B, C, \ldots, Z\}$.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E

En el caso de Cándido el DNI es: 12421241, que al dividirlo por 23 se escribe: $12421241 = 5540053 \times +22$, luego le corresponde la letra E, de forma que el NIF de Cándido es: 12421241E. □

Ejercicio. 41.10.
¿Cuántos números de cinco cifras hay que tengan sus dos últimas cifras impares?

SOLUCIÓN. Uno de estos números será de la forma *abc de*, en donde *d*, *e* con cifras impares, esto es, tomadas en el conjunto $\{1, 3, 5, 7, 9\}$, *bc* son cifras cualesquiera, esto es, tomadas en el conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ y *a* es una cifra distinta de 0, esto es, tomada en el conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. El número pedido es:

$$9 \times 10 \times 10 \times 5 \times 5 = 22{,}500.$$

□

Ejercicio. 41.11.
¿Cuántos números de dos cifras hay que tengan una cifra igual a 7?

SOLUCIÓN. Si la primera cifra es igual a 7, las restantes pueden ser cualesquiera, entonces tenemos 10 números distintos.

Si la primera cifra no es igual a 7, como no puede ser igual a 0, entonces debe ser tomada del conjunto $\{1,2,3,4,5,6,8,9\}$. La otra cifra debe ser igual a 7, luego tenemos 8 números distintos.

El número pedido es: 10+8=18. □

Ejercicio. 41.12.
¿Cuántos números de tres cifras hay que tengan una cifra igual a 7?

SOLUCIÓN. Si la primera cifra es igual a 7, las restantes pueden ser cualesquiera, entonces tenemos 10^2 números distintos.

Si la primera cifra no es igual a 7, como no puede ser igual a 0, entonces debe ser tomada del conjunto $\{1,2,3,4,5,6,8,9\}$. Las otras dos cifras deben tener una cifra iguala 7, pero ya sabemos que este número es 18.

El número pedido es: $10^2 + 8 \times 18 = 100 + 144 = 244$. □

Ejercicio. 41.13.
¿Cuántos números de cuatro cifras hay que tengan dos cifras iguales a 7?

SOLUCIÓN. El número pedido es: $10^3 + 8 \times 244 = 1000 + 1952 = 2{,}952$. □

Ejercicio. 41.14.
¿Cuántos números de tres cifras hay que tengan dos cifras iguales a 7?

SOLUCIÓN. Si la primera cifra es igual a 7, las dos restantes deben tener al menos un 7, entonces tenemos 18 números distintos.

Si la primera cifra no es igual a 7, como no puede ser igual a 0, entonces debe ser tomada del conjunto $\{1,2,3,4,5,6,8,9\}$. Las otras dos cifras deben ser iguales a 7, luego tenemos 8 números distintos.

El número pedido es: 18+8=26. □

Ejercicio. 41.15.
¿Cuántos números de cuatro cifras hay que tengan dos cifras iguales a 7?

SOLUCIÓN. Si la primera cifra es igual a 7, las tres restantes deben tener al menos un 7, entonces tenemos 244 números distintos.

Si la primera cifra no es igual a 7, como no puede ser igual a 0, entonces debe ser tomada del conjunto $\{1,2,3,4,5,6,8,9\}$. De las otras tres cifras al menos dos han de ser iguales a 7, luego tenemos 8×26 números distintos.

El número pedido es: $244 + 8 \times 26$. □

Ejercicio. 41.16.
¿Cuántos números de tres cifras hay que tengan entre sus cifras un 5 y un 7?

SOLUCIÓN. Si la primera cifra es igual a 7, las dos restantes deben tener al menos un 5, entonces tenemos 18 números distintos. Si la primera cifra es igual a 5, las dos restantes deben tener al menos un 7, entonces tenemos 18 números distintos.

Si la primera cifra no es 5 ni 7, como no puede ser igual a 0, entonces debe ser tomada del conjunto $\{1,2,3,4,6,8,9\}$. De las otras dos cifras una debe ser 5 y otro 7, luego tenemos 8 números distintos.

El número pedido es: 18+18+7=43. □

Ejercicio. 41.17.
¿Cuántos números de cuatro cifras hay que tengan entre sus cifras un 5 y un 7?

SOLUCIÓN. Si la primera cifra es igual a 7, las tres restantes deben tener al menos un 5, entonces tenemos 244 números distintos. Si la primera cifra es igual a 5, las tres restantes deben tener al menos un 7, entonces tenemos 244 números distintos.

Si la primera cifra no es 5 ni 7, como no puede ser igual a 0, entonces debe ser tomada del conjunto $\{1,2,3,4,6,8,9\}$. De las otras tres cifras una debe ser 5 y otro 7, luego tenemos $7 \times 43 = 301$ números distintos.

El número pedido es: $244 + 244 + 7 \times 43 = 488 + 301 = 789$. □

Ejercicio. 41.18.
Hacer lo mismo agregando el adjetivo "exactamente".

Ejercicio. 41.19.
Un número se llama rumboso *si todas sus cifras están ordenadas de menor a mayor de izquierda a derecha. Por ejemplo el número 247 es rumboso, y el número 231 no lo es. ¿Cuántos números rumbosos de cuatro cifras podemos construir?*

Ejercicio. 41.20.
Un número se llama aburrido *si todas sus cifras, salvo a lo más una de ellas, son iguales. Por ejemplo todo número de una y dos cifras es aburrido; los números 877 ó 7877 so aburridos, y el número 8778 no lo es. ¿Cuántos números aburridos de cuatro cifras podemos construir?*

Ejercicio. 41.21.
Un número se llama inquieto *si dos cifras contiguas son siempre distintas. Por ejemplo los números 7, 18, 181, ó 1234 son números inquietos, en cambio el 188 no lo es. ¿Cuántos números inquietos de cuatro cifras podemos construir?*

Llamamos una *reordenación* de una lista a otra lista que tiene exactamente los mismos elementos, y llamamos *desordenación* de una lista a una lista que contiene los mismos elementos pero ninguno ocupa la posición que ocupaba en la lista original.

Ejemplo. 41.22.
Dada la lista $\{A, B, C\}$ reordenaciones son: ABC, BCA ó BAC, y desordenaciones son BCA o CAB, pero no BAC o ABC.

Ejercicio. 41.23.
Calcular las reordenaciones y las desordenaciones de las listas

1. $\{A, B\}$
2. $\{A, B, C\}$
3. $\{A, B, C, D\}$
4. $\{A, B, C, D, E\}$

Ejercicio. 41.24.
¿Cuántas reordenaciones de la lista $\{A, B, C, D\}$ existen en las que:

1. *B ocupe siempre la posición segunda,*
2. *B no ocupe la posición segunda,*
3. *A no ocupe las posiciones primera o segunda,*
4. *A no ocupe las posiciones primera o segunda ni B ocupe las posiciones primera o tercera,*
5. *A no ocupe la posición primera, B no ocupe la posición segunda, C no ocupe la posición tercera y D no ocupe la posición cuarta.*

Bibliografía

[1] N. L. Biggs, *Matemática discreta*, Vicens-Vives, 1994.

[2] F. García Merayo, G. Hernández Peñalver, A. Nevot Luna, *Problemas resueltos de matemática discreta*, Thonson, 2003.

[3] Ralph P. Grimaldi, *Matemática discreta y combinatoria: una introducción con aplicaciones*, Addison-Wesley Iberoamericana, 1998.

[4] Paul R. Halmos, *Teoría intuitiva de conjuntos*, Compañía Editorial Continental, 1982. 1

[5] R. Johnsonbaugh, *Matemáticas discretas*, Iberoamericana, 1988.

[6] J. D. Lipson, *Elements of Algebra and Algebraic Computing*, Benjamin/Cummings, 1981

[7] N. Peermingeat, *Algebra de Boole. Teoría, métodos de cálculo. Aplicaciones*, Alianza editorial, 1988.

[8] Robin J. Wilson. *Introduction to Graph Theory*, Longman Scientific and Technical, 1999.

[9] K. Rosen, *Matemática Discreta y sus Aplicaciones*, 5ª Edición, McGraw-Hill, 2004.

[10] K. A. Ross, C. R. B. Wright, *Discreta Mathematics*, Prentice-Hall, 1992.

Índice alfabético