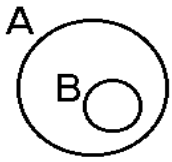
CONJUNTOS, RELACIONES Y GRUPOS

1. CONJUNTOS

1.1 Conjunto

Un conjunto está bien definido cuando se posee un criterio que permita afirmar si un elemento pertenece o no a dicho conjunto.

1.2 Inclusión



Un conjunto *B* está ***incluido*** en un conjunto *A* si no hay ningún elemento en *B* que no pertenezca también a *A*. Se dice entonces que *B* es un ***subconjunto*** de *A*. Se escribe $B \subseteq A$

Un posible procedimiento para demostrar que dos conjuntos son iguales es comprobar que todo elemento del primer conjunto pertenece al segundo y que todo elemento del segundo conjunto pertenece al primero. Es decir, aplicar que: $\left.\begin{array}{l} A \subseteq B \\ B \subseteq A \end{array}\right\} \Leftrightarrow A = B$

1.3 Conjunto Vacío

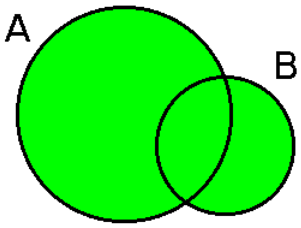
Es el que carece de elementos. Se escribe Ø. Se le considera incluido en cualquier conjunto: $\emptyset \subseteq A$.

1.4 Cardinal de un conjunto

Se denomina ***cardinal*** del conjunto al nº de sus elementos, y se dice que el conjunto es ***finito***. Es usual utilizar la notación *n*(*A*) para indicar el cardinal del conjunto *A*. Por ejemplo: $n(vocales) = 5$.

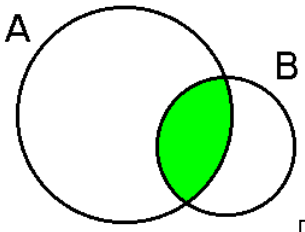
Si tiene infinitos elementos se dice que el conjunto es ***infinito.***

1.5 Unión de conjuntos



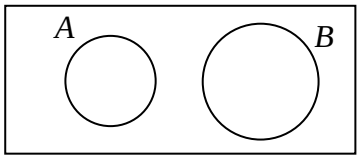
Se denomina ***unión*** de dos conjuntos al conjunto formado por los elementos pertenecientes al menos a uno de los conjuntos. Se escribe $A \cup B$

1.6 Intersección de conjuntos



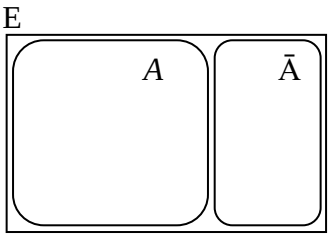
Se denomina ***intersección*** de dos conjuntos al conjunto formado por los elementos comunes pertenecientes a ambos conjuntos. Se escribe $A \cap B$

1.7 Conjuntos disjuntos



Son aquellos cuya intersección es el conjunto vacío. Es decir, que no tienen elementos comunes. *A* ∩ *B* = Ø

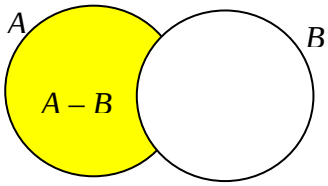
1.8 Complementario (o contrario) de un conjunto



Partiendo de un conjunto E (que se suele llamar ***universo***) y de uno de sus subconjuntos *A*, llamaremos ***complementario*** de *A* al conjunto formado por todos los elementos de E que no pertenecen a *A*. Se escribe Ā (También se utiliza el apóstrofe: A')

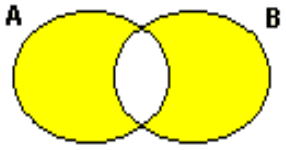
Obviamente cumplirán $A \cup \overline{A} = \mathrm{E}$ y $A \cap \overline{A} = \emptyset$

1.9 Diferencia de conjuntos



Se denomina ***diferencia*** de dos conjuntos al conjunto formado por los elementos del primer conjunto que no pertenezcan al segundo conjunto. Coincide con la intersección del primero con el complementario del segundo $A \cap \overline{B}$. Se escribe *A* – *B* (también $A \setminus B$)

1.10 Diferencia Simétrica

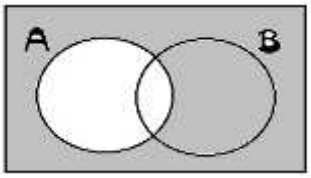


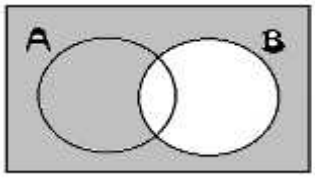
Se denomina ***diferencia Simétrica*** de dos conjuntos al conjunto formado por los elementos de la unión de ambos conjuntos y que no pertenezcan a su intersección. Coincide con la unión de sus dos diferencias y se puede expresar de varias formas: $(A-B)\cup(B-A)=(A\cap\overline{B})\cup(B\cap\overline{A})=(A\cup B)-(A\cap B)$. Se escribe $A\Delta B$

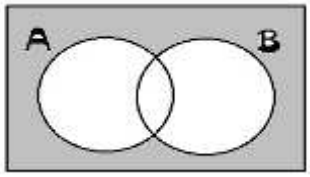
1.11 Propiedades de las operaciones de conjuntos:

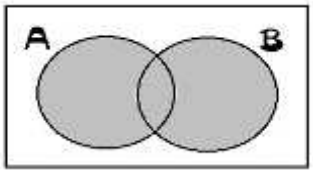
Conmutativas	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Asociativas	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Distributivas	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Idempotentes	$A \cup A = A$	$A \cap A = A$
Simplificativas	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
De Morgan	$\overline{A\cup B}=\overline{A}\cap\overline{B}$	$\overline{A\cap B}=\overline{A}\cup\overline{B}$

Estas y otras propiedades se pueden demostrar gráficamente mediante diagramas de Venn. Veamos por ejemplo, la 1ª de De Morgan : $\overline{A\cup B}=\overline{A}\cap\overline{B}$









$\overline{A}$	$\overline{B}$	$\overline{A}\cap\overline{B}$	$A\cup B$
Esta viñeta muestra el contrario de A	Esta viñeta muestra el contrario de B	Esta viñeta muestra la zona común del contrario de A con el contrario de B	La viñeta muestra la unión de A con B, que es contraria de la anterior

Estas propiedades pueden demostrarse también utilizando las tablas de verdad de la lógica de predicados. Para ello basta con interpretar el clásico **verdadero / falso** como un: **pertenece a / no pertenece a**

Por ejemplo, la tabla de verdad de la 1ª de De Morgan $\overline{A\cup B}=\overline{A}\cap\overline{B}$ es la que sigue:

A	B
v	v
v	f
f	v
f	f

$\overline{A}$	$\overline{B}$	$\overline{A}\cap\overline{B}$
f	f	f
f	v	f
v	f	f
v	v	v

$A\cup B$	$\overline{A\cup B}$
v	f
v	f
v	f
f	v

La propiedad queda demostrada al comprobar la igualdad entre las columnas de $\overline{A}\cap\overline{B}$ y $\overline{A\cup B}$

Veamos cómo se construye esta tabla razonando con el 2º de los cuatro casos.
Sea un elemento que **pertenece a** *A* pero **no pertenece a** *B*.
Pertenecerá entonces al contrario de *B* pero **no** al contrario de *A*, por lo que **no pertenece** a su intersección.
Por otro lado, al **pertenecer a** *A* (aunque **no pertenezca a** *B*), **pertenecerá** a $A\cup B$ y por lo tanto **no pertenecerá** a su contrario.

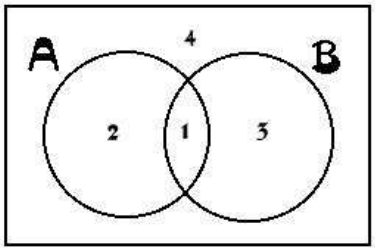
A	B
v	f

$\overline{A}$	$\overline{B}$	$\overline{A}\cap\overline{B}$
f	v	f

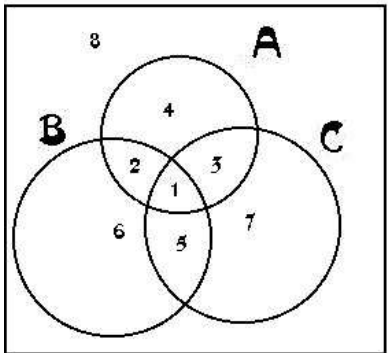
$A\cup B$	$\overline{A\cup B}$
v	f

Los restantes casos se razonarían de modo similar.

Por último, hacer ver que los cuatro casos de esta tabla de verdad se corresponden a las cuatro zonas en que quedad dividido el universo al representar dos conjuntos. Son las que se ven en el siguiente dibujo numeradas en el mismo orden de la tabla.



Para tres conjuntos, resultarían ocho casos, como muestra el dibujo siguiente:



1.12 Subconjuntos de un conjunto

Dado un conjunto, podemos construir otro formado por todos sus subconjuntos. Si el conjunto es finito y contiene ***n*** elementos, el número total de subconjuntos será 2^n contando desde el conjunto vacío hasta el propio conjunto dado pasando por subconjuntos con un único elemento, con dos elementos, etc.

Por ejemplo, partiendo del conjunto $A=\{1, 2, 3, 4\}$ sus $2^4 = 16$ subconjuntos serán:

Ø, {1}, {2}, {3}, {4}, {1,2}, {1,3}, {1,4}, {2,3}, {2,4}, {3,4}, {1,2,3}, {1,2,4}, {1,3,4}, {2,3,4}, {1,2,3,4}

2. RELACIONES ENTRE DOS CONJUNTOS

2.1 Producto cartesiano de 2 conjuntos

Es el conjunto formado por todos los pares ordenados posibles emparejando un elemento del primer conjunto con otro del segundo conjunto. Se escribe: *A x B*

Por ejemplo, dados estos conjuntos: $A=\{a,e,i,o,u\}$ $B=\{1,2\}$

Su producto cartesiano sería:

$$A\times B=\{(a,1),(a,2),(e,1),(e,2),(i,1),(i,2),(o,1),(o,2),(u,1),(u,2)\}$$

Salvo confusión, se pueden suprimir los paréntesis y comas de cada pareja, quedando así:

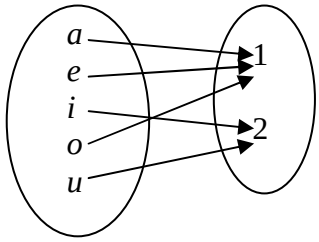
$$A\times B=\{a1,a2,e1,e2,i1,i2,o1,o2,u1,u2\}$$

En muchos casos haremos el producto cartesiano de un conjunto por sí mismo, es decir *A x A*

2.2 Relación entre dos conjuntos

Se llama ***relación*** entre dos conjuntos a un subconjunto de su producto cartesiano. Es decir, que elegimos con un cierto criterio algunas parejas de entre todas las posibles.

Ejemplo. El subconjunto $R=\{a1,e1,i2,o1,u2\}$ representaría la distinción entre vocales abiertas (1) y cerradas (2).



Una relación se puede visualizar con claridad mediante flechas y diagramas de Venn. La relación anterior se vería así:
En esta relación, *a*R1 expresaría que *a* y 1 están relacionados mientras que con la R tachada $a\not{R}2$ nos indicaría que no lo están *a* y 2.

Una relación entre dos conjuntos con un número finito de elementos puede también indicarse mediante una tabla de doble entrada en la que en cada celda se expresa mediante un 1 que dichos elementos están relacionados y mediante un 0 si no lo están. Por ejemplo, la relación anterior se vería así:

	1	***2***
a	1	0
e	1	0
i	0	1
o	1	0
u	0	1

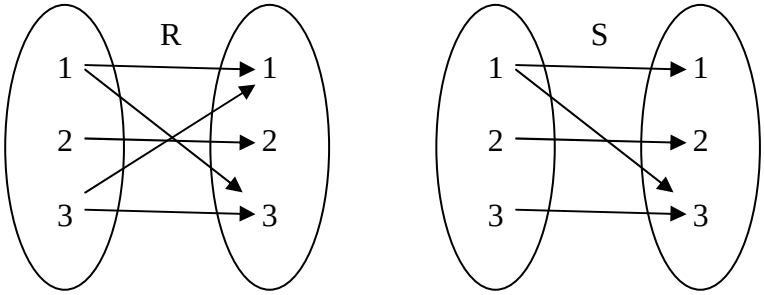
2.3 Relación de equivalencia

Dada una relación de un conjunto **consigo mismo**, se dice que es de ***equivalencia*** si cumple las tres propiedades siguientes:

Reflexiva	$\forall x \quad xRx$	Es decir, que todo elemento, debe estar relacionado consigo mismo
Simétrica	$\forall x,y \quad xRy \Rightarrow yRx$	Es decir, que, si existe una relación entre dos elementos, debe darse también en el orden contrario.
Transitiva	$\forall x,y,z \quad \left.\begin{matrix} xRy \\ yRz \end{matrix}\right\} \Rightarrow xRz$	Es decir, si un primer elemento está relacionado con un segundo, y éste lo está con un tercero, debe existir relación entre el primero y el tercero

En las relaciones de equivalencia se suele utilizar el símbolo ≡. Es decir, que en lugar de escribir xRy pondríamos x≡y indicando la relación (equivalencia) existente entre dichos elementos.

Por ejemplo la relación $R = \{11,13,22,31,33\}$ cumple las tres propiedades. Mientras que $S = \{11,13,22,33\}$ incumple la simétrica, ya que la pareja 13 obligaría a que existiera la pareja 31.



Si, en un conjunto finito, expresásemos la relación de equivalencia mediante una tabla, podríamos ver rápidamente el cumplimiento de dos de las tres propiedades. Observando si en todas las celdas de la diagonal principal está escrito un 1, comprobaríamos la propiedad reflexiva y observando la simetría de las restantes celdas respecto de esta diagonal comprobaríamos la propiedad simétrica.

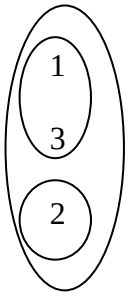
Las siguientes tablas son las correspondientes a las relaciones anteriores. Los unos de la diagonal principal nos aseguran que ambas relaciones cumplen la propiedad reflexiva mientras que la asimetría marcada en rojo en la tabla S nos indicaría el incumplimiento de la propiedad simétrica en dicha relación.

R	*1*	*2*	*3*
1	1	0	1
2	0	1	0
3	1	0	1

S	*1*	*2*	*3*
1	1	0	1
2	0	1	0
3	0	0	1

Para comprobar la propiedad transitiva se puede emplear el producto de matrices y observar la colocación de los ceros.

2.4 Clases de equivalencia



Toda relación de equivalencia establece una ***partición*** del conjunto en varios subconjuntos, formado cada uno de ellos por los elementos que están relacionados entre sí. Cada uno de estos subconjuntos se llama ***clase de equivalencia***.
Por ejemplo la anterior relación R se vería así:

2.5 Un ejemplo de clases de equivalencia: Clases de restos

Un ejemplo clásico de clasificación de los números enteros es el de las ***clases de restos***. Elegido un cierto número natural como **módulo**, se ordenan todos los números enteros en tantas filas como dicho módulo. Los infinitos números enteros que formen cada fila formarían una clase de equivalencia.

Por ejemplo, las clases de restos módulo 3:

Clase 0	.....	-6	-3	0	3	6	9	12	.....
Clase 1	.....	-5	-2	1	4	7	10	13	.....
Clase 2	.....	-4	-1	2	5	8	11	14	.....

Para saber rápidamente a qué clase pertenece un cierto elemento se busca el resto de su división entera (no decimal) entre el módulo elegido. Si el resto es cero, o sea que el número es múltiplo del módulo, pertenecería a la fila superior, la llamada clase cero. En otro caso, el resto (que estará entre uno y el módulo menos uno) indicaría la fila a la que pertenece. Si número fuese negativo se actúa igual pero dividiendo de manera que el cociente sea negativo pero el resto positivo.

El número 4571 pertenece a la clase 2 ya que al dividirlo entre 3 resulta dos de resto y -5 pertenece a la clase 1 ya que: $-5 = 3 \cdot (-2) + 1$.

Se puede comprobar que, dadas dos clases, independientemente de los números elegidos de ambas clases, su suma y su producto pertenecen a una clase determinada. Por ejemplo, si elegimos el 10 como representante de la clase 1 y el 8 de la clase 2, vemos que su suma pertenece a la clase 0 y su producto a la clase 2. Si repetimos el experimento cambiando por el 13 y el 20, vemos que las clases de su suma y de su producto son las mismas de antes.

$$\left.\begin{array}{l} 10 \in Clase\,1 \\ 8 \in Clase\,2 \end{array}\right\} \Rightarrow \begin{array}{l} 10+8=18 \in Clase\,0 \\ 10\cdot 8=80 \in Clase\,2 \end{array} \qquad \left.\begin{array}{l} 13 \in Clase\,1 \\ 20 \in Clase\,2 \end{array}\right\} \Rightarrow \begin{array}{l} 13+20=33 \in Clase\,0 \\ 13\cdot 20=260 \in Clase\,2 \end{array}$$

Estos hechos nos llevarían a escribir que, en módulo 3: $\begin{array}{l} \text{clase1}+\text{clase2}=\text{clase0} \\ \text{clase1}\cdot\text{clase2}=\text{clase2} \end{array}$ y nos permite definir dos operaciones nuevas: suma y producto de clases de restos módulo 3. Sus tablas de sumar y multiplicar serían:

+	C0	C1	C2
C0	C0	C1	C2
C1	C1	C2	C0
C2	C2	C0	C1

x	C0	C1	C2
C0	C0	C0	C0
C1	C0	C1	C2
C2	C0	C2	C1

Estudios similares se pueden realizar en otros módulos dando lugar a distintas sumas y multiplicaciones sin entrar en contradicción entre ellas. Por ejemplo:

$$\text{clase2}\cdot\text{clase3}=\text{clase1}\,(\text{en módulo }5)$$
$$\text{clase2}\cdot\text{clase3}=\text{clase2}\,(\text{en módulo }4)$$

2.6 Relación de orden

Dada una relación de un conjunto consigo mismo, se dice que es de ***orden*** si cumple las siguientes tres propiedades:

Reflexiva	$\forall x \quad xRx$	Es decir, que cualquier elemento, debe estar relacionado consigo mismo
Antisimétrica	$\forall x, y \quad \left.\begin{array}{l} xRy \\ yRx \end{array}\right\} \Rightarrow x = y$	Es decir, que no pueden existir dos elementos distintos que estén relacionados en los dos órdenes posibles
Transitiva	$\forall x, y, z \quad \left.\begin{array}{l} xRy \\ yRz \end{array}\right\} \Rightarrow xRz$	Es decir, si un primer elemento está relacionado con un segundo, y éste lo está con un tercero, debe existir relación entre el primero y el tercero

Cualquier ejemplo en el que ordenemos elementos se tratará casi seguro de una relación de orden. El orden de los números reales o el alfabético de las letras lo son.
En las relaciones de orden se suele utilizar el símbolo ≤. Es decir, que en lugar de escribir 1R2 pondremos 1≤2 indicando la relación (orden) existente entre dichos elementos.

Las tres propiedades anteriores quedarían entonces escritas así:

Reflexiva	$\forall x \quad x \le x$	Es decir, que cualquier elemento es menor o igual que sí mismo. De hecho es igual.
Antisimétrica	$\forall x, y \quad \left.\begin{array}{l} x \le y \\ y \le x \end{array}\right\} \Rightarrow x = y$	Es decir, que no pueden existir dos elementos **distintos** que siendo el primero menor o igual que el segundo, éste sea menor o igual que el primero
Transitiva	$\forall x, y, z \quad \left.\begin{array}{l} x \le y \\ y \le z \end{array}\right\} \Rightarrow x \le z$	Es decir, si un primer elemento es menor o igual a otro y éste es menor o igual que un tercero, el primero deberá ser menor o igual al tercero

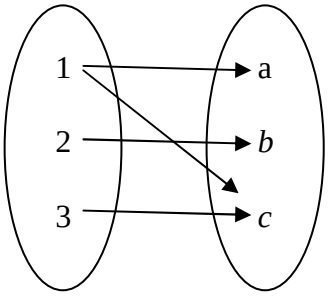
3. FUNCIÓN (o APLICACIÓN) ENTRE DOS CONJUNTOS

3.1 Definición de función (o aplicación) entre dos conjuntos

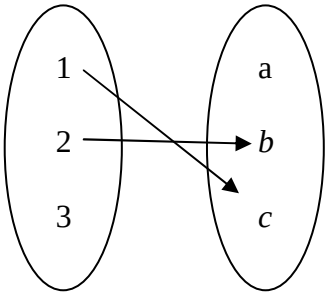
Se trata de una relación entre dos conjuntos que cumple la condición de que todo elemento del primer conjunto debe estar relacionado con uno y sólo uno del segundo conjunto. Al primer conjunto se le llama ***dominio*** de la función y al segundo conjunto ***codominio***. A los elementos que inician una relación funcional los llamaremos ***orígenes*** y los que la finalizan ***imágenes***. Todas las imágenes forman un subconjunto del conjunto final llamado ***recorrido***.

A la función *f* entre los conjuntos *A* y *B* se la puede representa simbólicamente así: $f : A \to B$

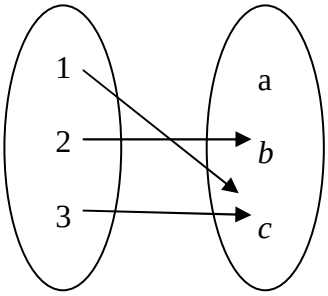
Ejemplos:



No es una función, ya que 1 está relacionado con más de un elemento del segundo conjunto.



No es una función, ya que 3 no está relacionado con ningún elemento del segundo conjunto.

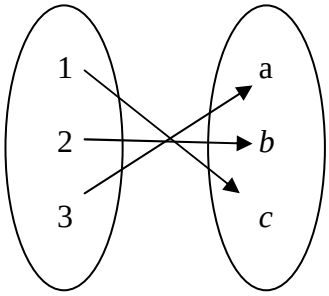


Sí es una función. Que el elemento *a* del 2º conjunto no esté relacionado con ningún elemento del 1º no incumple la definición de función.

Dominio = $\{1,2,3\}$

Codominio = $\{a,b,c\}$

Recorrido = $\{b,c\}$



Sí es una función.

Dominio = $\{1,2,3\}$

Codominio = $\{a,b,c\}$

Recorrido = $\{a,b,c\}$

3.2 Tipos de funciones

Según que cumplan o no una serie de propiedades definiremos tres tipos de funciones: ***Inyectivas***, ***Sobreyectivas*** y ***Biyectivas***.

3.2.1 Funciones Inyectivas

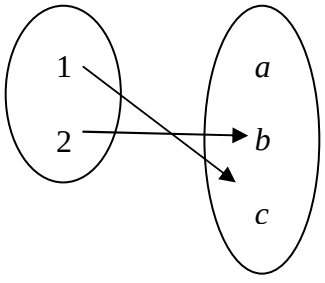
Una función se dice ***inyectiva*** si ningún elemento del codominio tiene más de un origen. En la práctica se suele emplear una demostración por reducción al absurdo partiendo de dos orígenes que compartan la misma imagen para concluir que la única opción es que deban ser iguales. Así: f inyectiva $\Leftrightarrow \left[f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \right]$

3.2.2 Funciones Sobreyectivas (También se les llama ***exhaustivas*** o también ***suprayectivas***)

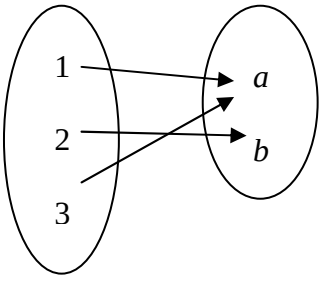
Una función se dice ***sobreyectiva*** si todo elemento del codominio tiene al menos un origen. Implicaría que el recorrido ocuparía todo el dominio. Su definición entonces es: f sobreyectiva $\Leftrightarrow \left[\forall y \in B \; \exists x \in A \mid f(x) = y \right]$

3.2.3 Funciones Biyectivas

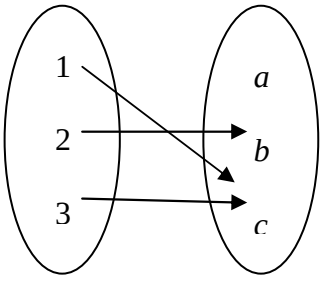
Una función se dice ***Biyectiva*** si es Inyectiva y sobreyectiva. También se les llama ***Biunívocas***.



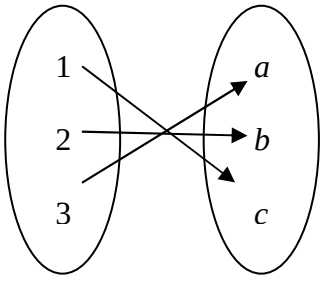
Es inyectiva, pero no sobreyectiva (*a* no tiene origen).



Es sobreyectiva, pero no es inyectiva (*a* tiene más de un origen).



No es sobreyectiva (*a* no tiene origen) ni inyectiva (*c* tiene más de un origen).



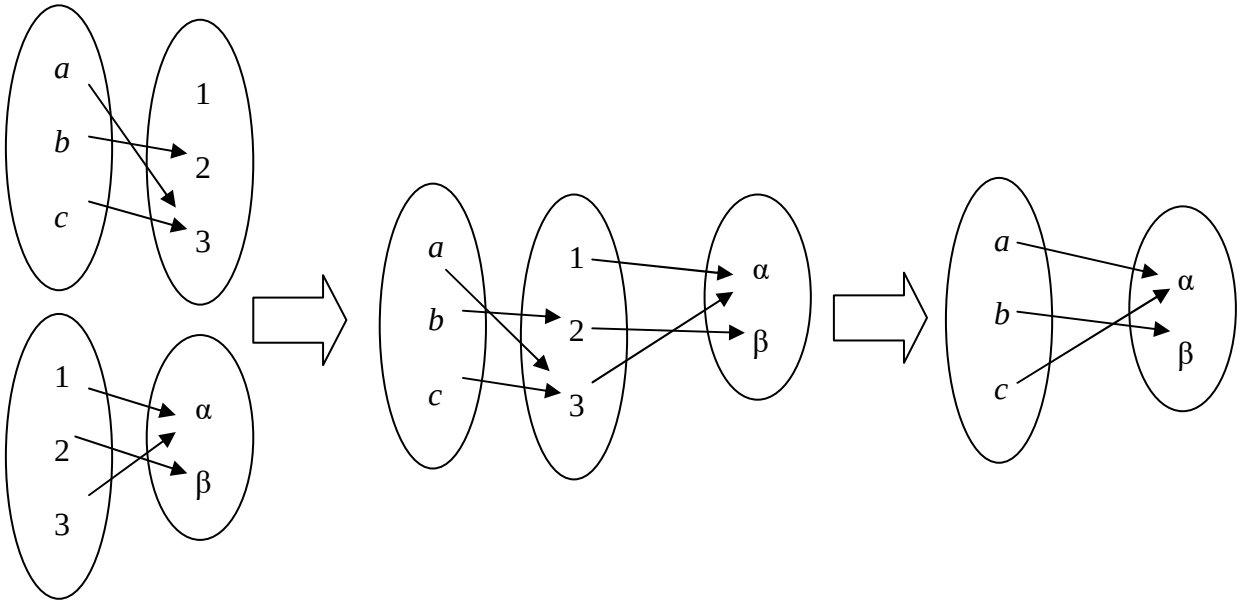
Es biyectiva.

3.3 Composición de funciones

Si tenemos dos funciones $f : A \to B$ $g : B \to C$ en las que el conjunto final de la primera función coincide con el inicial de la 2ª, se puede crear una nueva función que se denomina ***compuesta*** de ambas y que se construye enlazando los orígenes de la primera con las imágenes de la segunda.

Se escribe simbólicamente así: $g \circ f : A \to C$

Ejemplo:



La composición de funciones no es conmutativa, es decir que, con carácter general, no se cumple que: $f \circ g = g \circ f$. Veamos qué distintas circunstancias se podrían dar:

Si el conjunto *A* es distinto del conjunto *C*, sólo estará definida la composición en un cierto orden.

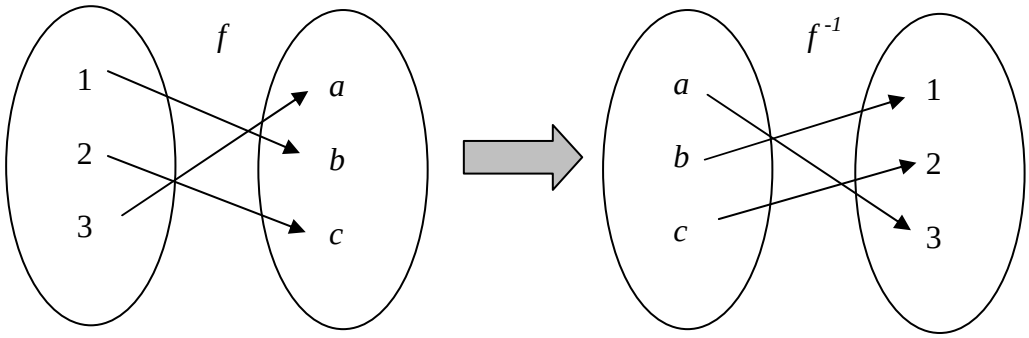
Si *A* = *C* podrán componerse en los dos sentidos, pero no podrían coincidir por estar definida la función compuesta en un caso sobre *A* y en el otro caso sobre *B*.

Si *A* = *B* = *C* ambos composiciones podrán hacerse y estarían definidas sobre el mismo conjunto. Pero ni siquiera en este caso está asegurado que coincidan las dos composiciones.

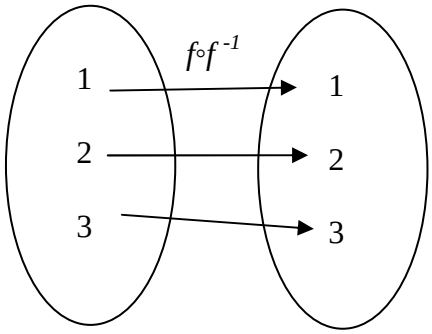
3.4 Función recíproca de una función biyectiva

Dada una función *f* biyectiva, se denomina ***recíproca*** (también ***inversa***) a aquella en la que hemos intercambiado el conjunto inicial (con los orígenes) por el conjunto final (con las imágenes) y viceversa. La nueva función, que obviamente es también biyectiva, se escribe así: f^{-1}.

Ejemplo:



Si se compone una función con su recíproca se obtiene la función identidad, es decir la que aplica cada elemento sobre sí mismo.



4. OPERACIONES BINARIAS

4.1 Definición de operación binaria

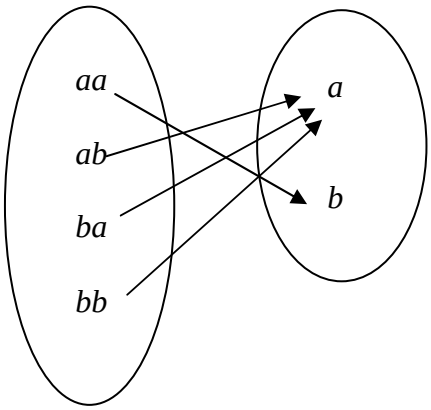
Siendo *A, B* dos conjuntos no vacíos, se denomina ***operación binaria*** a cualquier función $f : A\times A \to B$

Esta función relaciona una pareja ordenada de elementos de A con un cierto elemento de B. Este hecho lo podemos entender como que hemos hecho una operación entre los elementos de la pareja dando como resultado el elemento que indique su imagen. Si los dos conjuntos *A, B* son iguales, se dice que la operación está **cerrada**.

Por ejemplo la suma de números aplicada al conjunto de los números naturales pares es una operación cerrada (par + par = par), pero si la aplicásemos al conjunto de los números naturales impares, dichas sumas (impar + impar = par) no pertenecerían al conjunto de los impares, y no estaría la operación bien definida.

Por ejemplo $(2,3) \to 6$ significaría que la operación realizada entre el 2 y el 3, en este orden, resulta 6. Para ganar en claridad, el símbolo flecha se sustituye por un símbolo operacional: *, #, +, x etc. (si no causa confusión, sin ningún símbolo, como sucede con el producto de números reales). De ser el asterisco, una operación podría visualizarse así: 2*3 = 6. Y no hay que olvidar que, al tratarse de una función, debe estar definido el resultado de cualquier operación y ser único.

Si $A = \{a, b\}$ el siguiente diagrama de Venn muestra una posible operación binaria en *A* :



Si *A* es un conjunto finito, se visualiza mucho mejor la operación dándole forma de tabla entendiendo (por si la operación no fuese conmutativa) que el primer elemento de cada pareja es el de la 1ª columna y se opera con el de la 1ª fila que será entonces el segundo elemento de la pareja:

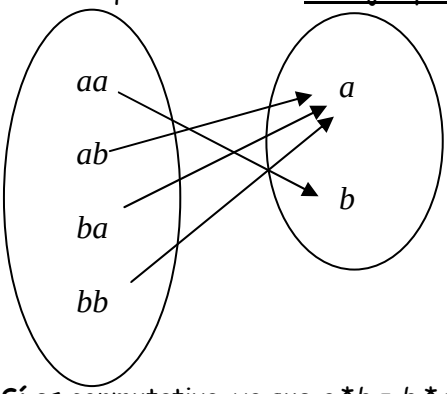
*	a	b
a	b	a
b	a	a

4.2 Propiedades de las operaciones binarias

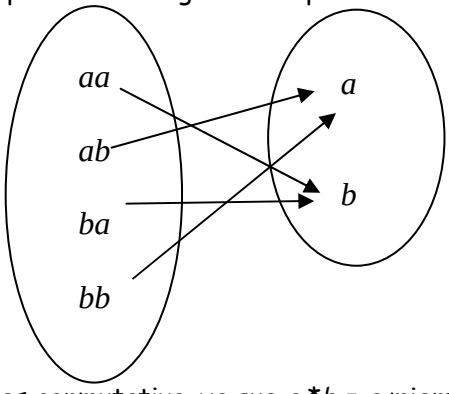
Una operación binaria *puede* cumplir alguna de estas propiedades: ***conmutativa***, ***asociativa***, ***elemento neutro***, ***elemento simétrico*** y, si estuviesen definidas dos operaciones distintas en el mismo conjunto, la ***distributiva***.

4.2.1 Propiedad Conmutativa

Cumplirá esta propiedad si para toda pareja el resultado de la operación no depende del orden de los elementos, es decir que *a *b = b *a*. Por ejemplo, si comparamos las siguientes operaciones:



Sí es conmutativa, ya que *a *b = b *a*



No es conmutativa, ya que *a *b = a* mientras que *b *a = b*

Si, en conjuntos finitos, vemos la operación en forma de tabla, su conmutatividad se observa por la simetría de la misma respecto de la diagonal principal. Con conjuntos infinitos, habría que demostrar la conmutatividad partiendo de cómo esté definida la operación.

Conocidos ejemplos de operaciones conmutativas son la suma de números, el producto de números, la unión de conjuntos y la intersección de conjuntos.

4.2.2 Propiedad Asociativa

Cumplirá esta propiedad si dados tres elementos cualesquiera cumple: $a*(b*c) = (a*b)*c$

Conocidos ejemplos de operaciones asociativas son la suma de números, el producto de números, la unión de conjuntos o la intersección de conjuntos.

No siempre es fácil comprobar la asociatividad de una operación, normalmente tendremos que probar con todos los tríos posibles y comprobar los resultados, o demostrarla a través de la definición de la operación. Por ejemplo, la primera operación representada en **4.2.1** y que era conmutativa, resulta ser no asociativa. Véase cómo se obtienen distintos resultados según se asocien los elementos *a*, *a* y *b* :

$a*(a*b) = a*a = b$ mientras que $(a*a)*b = b*b = a$

4.2.3 Propiedad Distributiva

Si dos operaciones distintas (* y #) están definidas sobre un mismo conjunto, se dice que cumple la propiedad distributiva de la primera (*) sobre la segunda (#) si dados tres elementos cualesquiera cumple:

$$a*(b\ \#\ c) = (a*b)\ \#\ (a*c)$$

Un ejemplo clásico es el de la distributividad del producto respecto de la suma de números reales:

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

pero recuerde que en los números reales **no** se cumple la distributividad de la suma respecto del producto.

$$a + (b\cdot c) \neq (a+b)\cdot(a+c)$$

Si embargo, en el álgebra de Boole de los conjuntos, se cumple tanto la distributividad de la unión respecto de la intersección como la distributividad de la intersección respecto de la unión.

No es fácil demostrar la distributividad entre dos operaciones, normalmente tendremos que probar todos los tríos posibles y comprobar los resultados, o demostrarla a través de la definición de las operaciones.

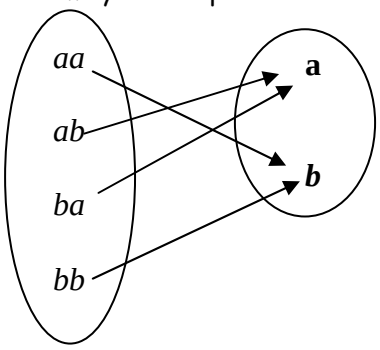
4.2.4 Propiedad del Elemento Neutro

Se dice que un conjunto tiene un ***elemento neutro*** (normalmente representado con la letra ***e,*** ó con el número **1** aunque no se trate de un número) para una cierta operación * si operado con todos los restantes elementos del conjunto tanto por la derecha como por la izquierda se obtiene como resultado el elemento con el que operamos.

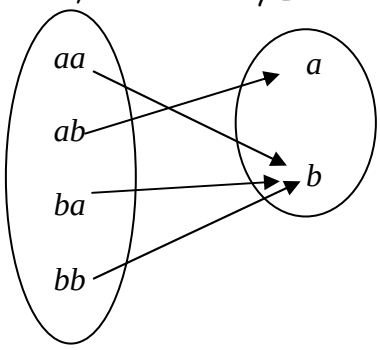
Es decir: $\forall a \in A \Rightarrow e*a = a*e = a$

Una operación binaria no tiene necesariamente elemento neutro aunque las operaciones tradicionales sí lo tienen (0 en la suma y 1 en el producto de números reales, Ø en la unión y *E* en la intersección de conjuntos).

Ejemplos:



b es elemento neutro, ya que:
$a*b = b*a = a$ y también $b*b = b$



a no es elemento neutro, ya que:
$a*a \neq a$ (y también $a*b \neq b$)
b tampoco es elemento neutro, ya que $b*a \neq a$
Para esta operación este conjunto no tiene elemento neutro.

Teorema de la Unicidad del Elemento Neutro: Si existe, el elemento neutro es *único*.

Demostración:

Si existiesen dos elementos neutros (e_1 y e_2) sucedería que:

$$e_1 * e_2 = \begin{cases} e_2\ (\text{por ser } e_1 \text{ elemento neutro}) \\ e_1\ (\text{por ser } e_2 \text{ elemento neutro}) \end{cases}$$

y como el resultado debe ser único, se cumplirá: $e_1 = e_2$

4.2.5 Propiedad del Elemento Simétrico

Partiendo de un conjunto que tenga elemento neutro para una cierta operación, se dice que cumple la propiedad de un ***elemento simétrico*** si para todo elemento *a* del conjunto podemos encontrar otro (en algún caso puede ser el mismo elemento), que llamaremos su simétrico, de manera que operados tanto por la derecha como por la izquierda resulten el elemento neutro. Se escribe así: a^{-1}

Es decir: $\forall a \in A \ \exists a^{-1} \in A \Rightarrow a^{-1} * a = a * a^{-1} = e$ siendo ***e*** el elemento neutro

De la simetría de la definición se deduce que el simétrico del simétrico de un elemento es el propio elemento. Es decir que: $\left(a^{-1}\right)^{-1} = a$.

Una operación binaria no tiene necesariamente simétricos aunque en las operaciones tradicionales sí existen. (*A* y $\overline{A}$ son simétricos en la unión de conjuntos; -5 es el simétrico (opuesto) del 5 en la suma y 1/5 simétrico (inverso) en el producto de números reales. Sin embargo, recuerde que no existe el inverso del número cero.

Ejemplos:

*	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

En esta tabla vemos que *a* es el elemento neutro.
El simétrico de *a* sería *a* (siempre sucede con el elemento neutro) y el de *d* sería *d*
El simétrico de *b* es *c* y el simétrico de *c* es *b* (se puede decir que *b* y *c* son simétricos)

*	a	b	c	d
a	a	b	c	d
b	b	d	b	d
c	c	c	d	c
d	d	c	b	a

En esta operación vemos que *a* es el elemento neutro.
El simétrico de *a* es *a*
El simétrico de *d* es *d*
Ni *b* ni *c* tienen simétrico

Teorema de la unicidad del Elemento simétrico: Si la operación cumple también la asociativa, el simétrico de cada elemento debe ser *único*.

Demostración:

Si, para un cierto elemento a, existiesen dos simétricos (s_1 y s_2) sucedería que:

$s_1 \overset{(1)}{=} s_1 * e \overset{(2)}{=} s_1 * (a * s_2) \overset{(3)}{=} (s_1 * a) * s_2 \overset{(4)}{=} e * s_2 \overset{(1)}{=} s_2 \Rightarrow$ Los dos simétricos son el mismo elemento.

(1): Por ser *e* el elemento neutro
(2): Por ser s_2 simétrico de *a*
(3): Por la propiedad asociativa
(4): Por ser s_1 simétrico de *a*

La simplificación que hacemos en el conjunto de los números reales es posible gracias a la existencia de elementos simétricos. Por ejemplo, si tenemos la igualdad $3 \cdot x = 3 \cdot y$, simplificamos rápidamente los treses $\not{3} \cdot x = \not{3} \cdot y$ y concluimos que *x* = *y*. Sin darnos cuenta, estamos utilizando las siguientes propiedades:

$$3 \cdot x = 3 \cdot y \overset{(1)}{\Longrightarrow} \frac{1}{3} \cdot (3 \cdot x) = \frac{1}{3} \cdot (3 \cdot y) \overset{(2)}{\Longrightarrow} (\frac{1}{3} \cdot 3) \cdot x = (\frac{1}{3} \cdot 3) \cdot y \overset{(3)}{\Longrightarrow} 1 \cdot x = 1 \cdot y \overset{(4)}{\Longrightarrow} x = y$$

(1): multiplicamos ambos miembros por el simétrico de 3
(2): aplicamos la propiedad asociativa
(3): aplicamos la propiedad del elemento simétrico
(4): aplicamos la propiedad del elemento neutro

Sin embargo, siendo *x* e *y* dos números reales, sabemos que de la igualdad $0 \cdot x = 0 \cdot y$, **no** se concluye que *x* = *y*. La razón algebraica es que 0 no tiene simétrico.

En un conjunto que cumpla, como le sucede a los números reales, estas mismas propiedades, se puede hacer esta simplificación. De manera que si *a* es un elemento con simétrico, podríamos hacer:

Simplificación:

$$a * x = a * y \overset{(1)}{\Longrightarrow} a^{-1} * (a * x) = a^{-1} * (a * y) \overset{(2)}{\Longrightarrow} (a^{-1} * a) * x = (a^{-1} * a) * y \overset{(3)}{\Longrightarrow} e * x = e * y \overset{(4)}{\Longrightarrow} x = y$$

Actuando de forma similar, también se podría eliminar un elemento que apareciera en la derecha de los dos miembros de una igualdad y tenga simétrico. Es decir, $x * a = y * a \Rightarrow x = y$.

Sin embargo, salvo que la operación sea conmutativa, de $a * x = y * a$, **no** se deduce que x e y sean iguales.

5. TEORÍA DE GRUPOS

5.1 Definición de grupo.

Un conjunto *G* no vacío en el que está definida una operación *, situación que resumiremos así: (*G*, *), se dice que tiene estructura de grupo si cumple las siguientes condiciones:

- La operación * está cerrada en el conjunto *G*
- Cumple la propiedad asociativa
- Tiene elemento neutro que pertenece a *G*
- Todos los elementos de *G* tienen un simétrico que pertenece a *G*

La operación * no necesita ser conmutativa, si lo fuese se dice que (*G*, *) es ***abeliano***.

La tabla de operar de un grupo finito se llama ***tabla de Cayley***.

Ejemplo:

$G = \{1, i, -1, -i\}$ respecto del producto de números complejos tiene estructura de grupo.

·	***1***	***i***	***-1***	***-i***
1	*1*	*i*	*-1*	*-i*
i	*i*	*-1*	*-i*	*1*
-1	*-1*	*-i*	*1*	*i*
-i	*-i*	*1*	*i*	*-1*

La operación está cerrada, ya que se obtienen resultados pertenecientes al mismo conjunto *G*.
1 es el elemento neutro
i, *-i* son simétricos el uno del otro
1, -1 son simétricos de sí mismos
La asociativa se cumple en el producto de cualquier trío de números complejos.

Obviamente se trata de un grupo abeliano porque el producto de números complejos es conmutativo

Ejemplo:

El grupo **no** abeliano con menor número de elementos es el que muestra la siguiente tabla de la operación * para seis elementos: $G = \{e, a, b, c, d, f\}$

*	***e***	***a***	***b***	***c***	***d***	***f***
e	*e*	*a*	*b*	*c*	*d*	*f*
a	*a*	*b*	*e*	*d*	*f*	*c*
b	*b*	*e*	*a*	*f*	*c*	*d*
c	*c*	*f*	*d*	*e*	*b*	*a*
d	*d*	*c*	*f*	*a*	*e*	*b*
f	*f*	*d*	*c*	*b*	*a*	*e*

El producto está bien definido, ya que se obtienen resultados pertenecientes al mismo conjunto *G*.
e es el elemento neutro
a, *b* son simétricos el uno del otro
e, *c*, *d*, *f* son simétricos de sí mismos
Eligiendo todos los tríos posibles, se demostraría que se cumple la propiedad asociativa.
No se cumple la propiedad conmutativa: véase cómo $a*c = d$ mientras que $c*a = f$

5.1.1 Orden de un grupo finito.

Si un grupo no tiene infinitos elementos, el número de los elementos que lo forman se denomina ***orden del grupo*** y se dice que el grupo es ***finito***. En otro caso se dice que el grupo es ***infinito***.

5.1.2 Orden de un elemento de un grupo.

Si operando un elemento consigo mismo m veces, se llega a obtener por primera vez el elemento neutro, este número m recibe el nombre de orden del elemento. Por ejemplo, el orden del grupo del epígrafe **5.1** es 6.

Es usual utilizar una notación exponencial para indicar una operación repetida utilizando el mismo elemento: Por ejemplo, $a*a*a$ se escribiría como a^3.

Si el grupo fuese infinito podría suceder que algún elemento tuviese orden finito pero también sería posible que operando indefinidamente un elemento consigo mismo nunca se obtuviera el elemento neutro ya que dispondríamos de infinitos resultados distintos posibles, ya que de haber repetido algún resultado, simplificando, significaría que ya hubiese aparecido antes el elemento neutro: Por ejemplo: $a^8 = a^5 \Rightarrow a^3 = e$

Teorema: En un grupo finito, todos sus elementos tendrán orden finito.

Demostración: $a \in G \overset{(1)}{\Rightarrow} \exists\, j,k \in N \mid a^j = a^k \overset{(2)}{\Rightarrow} a^{k-j} = e \Rightarrow$ El orden de a finito

(1): Como G tiene un número finito de elementos, operando *a* consigo mismo repetidas veces deberá repetirse necesariamente algún resultado, por ejemplo a^j y a^k (k > j)

(2): Simplificando en ambos miembros j veces el elemento *a*, vemos que necesariamente alguno de estos resultados es el elemento neutro.

Ejemplo: Halla el orden de los elementos del grupo del epígrafe **5.1**:
El orden de *e* es 1 (obvio)
$a^2 = a*a = b$ $a^3 = a^2*a = b*a = e$ Luego el orden de *a* es 3 (este mismo orden lo tiene *b*)
$c*c = e$ Luego el orden de *c* es 2 (este mismo orden lo tienen *d* y *f*)

5.1.3 Grupos cíclicos

Se llama grupo ***cíclico*** al que contiene a un elemento, llamado ***generador***, que operado consigo mismo repetidas veces, engendra todos los elementos del grupo.
Es decir, que si llamamos *g* al generador, el grupo será $G = \{ g, g^2, g^3, ... , g^n \}$ entendiendo por exponente al número de veces que operamos *g* consigo mismo: $g^3 = g*g*g$ etc. Si el número de elementos es *n* necesariamente el elemento neutro será la última potencia g^n. Obviamente la operación es cerrada y el simétrico de g^k es g^{n-k} . En forma de tabla se visualizan muy bien los grupos cíclicos.

Por ejemplo, la tabla del grupo cíclico de orden 5 llamando *g* a su generador y sabiendo que $g^5 = e$ sería:

*	g	g^2	g^3	g^4	e
g	g^2	g^3	g^4	e	g
g^2	g^3	g^4	e	g	g^2
g^3	g^4	e	g	g^2	g^3
g^4	e	g	g^2	g^3	g^4
e	g	g^2	g^3	g^4	e

Teorema: Los grupos cíclicos son siempre abelianos

Demostración: Curiosamente se basa en la propiedad asociativa.

$$\left.\begin{array}{l} a \in G \\ b \in G \end{array}\right\} \Rightarrow \left.\begin{array}{l} \exists j \in N \mid a = g^j \\ \exists k \in N \mid b = g^k \end{array}\right\} \Rightarrow a \cdot b = g^j \cdot g^k = g^{j+k} = g^{k+j} = g^k \cdot g^j = b \cdot a$$

5.2 Subgrupos

Partiendo de un grupo (*G*, *) y de un subconjunto *H*, decimos que (*H*, *) es un ***subgrupo*** de (*G*, *) si *H* tiene estructura de grupo respecto de la misma operación *
Puesto que en *G* se cumple la asociativa, tiene elemento neutro y todos los elementos tienen simétricos, sólo quedaría comprobar que:

- la operación * está cerrada en *H*
- el elemento neutro de *G* también pertenece a *H*
- todos los simétricos de los elementos de *H* también pertenecen a *H*

Todo grupo siempre contendrá al subgrupo formado exclusivamente por el elemento neutro. También se considerará como subgrupo al mismo grupo. Estos dos subgrupos se denominan ***impropios***, a los restantes subgrupos, de existir, se les denomina ***propios***.
En grupos grandes no siempre es fácil buscar subgrupos, pero operando un elemento consigo mismo repetidas veces y observando los resultados, sabremos con qué elementos formará un subgrupo.

Ejemplo de Subgrupos:
El grupo estudiado antes $G = \{1, i, -1, -i\}$ respecto del producto de números complejos tiene tres subgrupos:
En primer lugar, los subgrupos impropios $H_1 = \{1\}$ y $G = \{1, i, -1, -i\}$

El único subgrupo propio es $H_2 = \{1, -1\}$ ya que observando la tabla que resulta:

·	**1**	**-1**
1	1	-1
-1	-1	1

Vemos que: la operación está cerrada, contiene al elemento neutro y a los simétricos de sus elementos

Cualquier otro subconjunto **no** es subgrupo. Por ejemplo, observando la tabla que resulta escogiendo sólo los elementos $\{1, i\}$:

·	**1**	**i**
1	1	i
i	i	-1

Vemos que: la operación no está cerrada ya que aparece –1 que no pertenece al conjunto $\{1, i\}$
Además –*i*, que es simétrico de *i* no pertenece al conjunto $\{1, i\}$

5.2.1 Condición necesaria y suficiente para que un subconjunto de un grupo sea subgrupo

Dados un grupo $(G, \cdot)$ y H un subconjunto no vacío de G:

$$(H,*) \text{ es subgrupo de } (G,*) \Leftrightarrow \left(\forall a,b \in H \Rightarrow a * b^{-1} \in H\right)$$

Haremos la demostración en dos fases: primero veremos que el cumplimiento del enunciado de la izquierda implica necesariamente el cumplimiento del enunciado de la derecha y después que el de la derecha implica el de la izquierda, o como se suele decir, que para que se cumpla el de la izquierda es suficiente que se cumpla el de la derecha.

- Demostración necesaria ($\Rightarrow$) Utilizaremos como punto de partida que $(H,*) \text{ es subgrupo de } (G,*)$

$$\left.\begin{array}{l} b \in H \overset{(1)}{\Longrightarrow} b^{-1} \in H \\ a \in H \end{array}\right\} \overset{(2)}{\Longrightarrow} a * b^{-1} \in H$$

(1): Al ser $(H, \cdot)$ un subgrupo, H tendrá estructura de grupo, por lo que para cualquier elemento de H su simétrico también pertenecerá a H

(2): Al tener H estructura de grupo, la operación estará cerrada en H, por lo que, dados dos elementos de H, el resultado de su operación también pertenecerá a H

- Demostración suficiente ($\Leftarrow$) Utilizaremos como punto de partida $\forall a,b \in H \Rightarrow a * b^{-1} \in H$

Puesto que en G se cumple la propiedad asociativa y los elementos de H lo son de G, se cumplirá la ***asociativa*** *en H*.

Sabemos que G tiene elemento neutro (e) y que todos sus elementos tienen simétricos en G, falta demostrar que el elemento **neutro** también pertenece a H y que todos los **simétricos** de los elementos de H también pertenecen a H.

Elemento neutro de H: $b \in H \overset{(3)}{\Rightarrow} b * b^{-1} \in H \overset{(4)}{\Rightarrow} e \in H$

Simétricos en H: $\left.\begin{array}{l} e \in H \\ b \in H \end{array}\right\} \overset{(5)}{\Longrightarrow} e * b^{-1} \in H \overset{(6)}{\Longrightarrow} b^{-1} \in H$

Sólo falta demostrar que la operación $\cdot$ está **cerrada** en H.

Operación cerrada en H: $\left.\begin{array}{l} b \in H \overset{(7)}{\Longrightarrow} b^{-1} \in H \\ a \in H \end{array}\right\} \overset{(8)}{\Longrightarrow} a * \left(b^{-1}\right)^{-1} \in H \overset{(9)}{\Longrightarrow} a * b \in H$

(3): Es la condición de partida utilizando una pareja con dos elementos iguales (b y b)
(4): Propiedad de los elementos simétricos, que se cumple en G por tener estructura de grupo.
(5): Es la condición de partida utilizando como primer elemento de la pareja al elemento neutro e
(6): Propiedad del elemento neutro, que se cumple en G por tener estructura de grupo.
(7): Acabamos de demostrar que los simétricos de los elementos de H, pertenecen a H.
(8): Es la condición de partida utilizando como segundo elemento de la pareja al elemento simétrico de b
(9): El simétrico del simétrico de cualquier elemento, coincide con el propio elemento.

5.2.2 Condición necesaria y suficiente para que un subconjunto de un grupo finito sea subgrupo

Siendo G un conjunto finito. Dados un grupo $(G, *)$ y H un subconjunto no vacío de G:

$$(H,*) \text{ es subgrupo de } (G,*) \Leftrightarrow H \text{ es cerrado respecto de } *$$

- Demostración necesaria ($\Rightarrow$) Que $(H, *)$ sea un grupo necesita que la operación esté cerrada en H.
- Demostración suficiente ($\Leftarrow$) Utilizaremos como punto de partida que H es cerrado respecto de $*$

Al ser G un grupo finito, el orden de sus elementos es finito, sea b un elemento de H de orden m.

$$\left.\begin{array}{l} b \in H \overset{(1)}{\Longrightarrow} b^{m-1} \in H \overset{(2)}{\Longrightarrow} b^{-1} \in H \\ a \in H \end{array}\right\} \overset{(3)}{\Longrightarrow} a * b^{-1} \in H \overset{(4)}{\Longrightarrow} (H,*) \text{ es un grupo.}$$

(1): b^{m-1} es una operación de m-1 elementos de H, su resultado debe pertenecer a H al ser cerrado respecto de $*$.
(2): Como $b * b^{m-1} = b^m = e$ el simétrico de b será b^{m-1}
(3): H es cerrado respecto de $*$
(4): Teorema anterior

5.2.3 Subgrupo generado por un cierto elemento en un grupo finito:

Si escogemos cualquier elemento en un grupo finito y lo operamos consigo mismo repetidas veces hasta llegar por primera vez (orden m) al elemento neutro, el subconjunto $\{a, a^2, a^2 ..., a^{m-1}, e\}$ formado por el elemento de partida y todos estos resultados cumplirán los requisitos de grupo, por lo que será subgrupo del grupo inicial. Obviamente la operación está cerrada, tiene elemento neutro y los simétricos son: $\left(a^k\right)^{-1} = a^{m-k}$

5.2.4 Teorema de Lagrange

Si tenemos un grupo finito con *n* elementos, necesariamente sus subgrupos contendrán un número de elementos divisor de *n*.

Teorema de Lagrange : $\left.\begin{array}{l} G \text{ grupo finito orden } n \\ H \text{ subgrupo orden } m \end{array}\right\} \Rightarrow m \text{ es divisor de } n$

Ejemplos: un grupo de orden 6 podrá tener subgrupos de 1, 2, 3, 6 elementos pero nunca con 4 ó 5.
Un grupo de orden 12 podrá tener subgrupos de 1, 2, 3, 4, 6, 12 elementos.
En consecuencia, un grupo con un número primo de elementos sólo tendrá subgrupos impropios.

Corolario del Teorema de Lagrange: $\left.\begin{array}{l} G \text{ grupo finito de orden } n \\ a \in G \text{ elemento de orden } m \end{array}\right\} \Rightarrow m \text{ es divisor de } n$

Demostración:
Si a es un elemento de orden m, tendremos el subgrupo $\{a, a^2, a^3 ..., a^{m-1}, e\}$ que tiene orden m, por lo que m será divisor de n, por aplicación del teorema de Lagrange.

5.2.5 Clases Laterales

Sea (*G*, ∗) un grupo, sea *a* uno de sus elementos y sea H un subgrupo de *G*. Este subgrupo nos permitirá definir dos subconjuntos del grupo *G* que llamaremos: *clase lateral izquierda de H en G* y *clase lateral derecha de H en G* mediante los resultados que resulten de operar dicho elemento con todos los elementos del subgrupo H:

Clase lateral izquierda de H en G $= \{a * h \mid h \in H\}$ Se le nombra aH ó $a + H$ si la operación es la suma.

Clase lateral derecha de H en G $= \{h * a \mid h \in H\}$ Se le nombra Ha ó $H + a$ si la operación es la suma.

Lógicamente, si el elemento a pertenece a H, las dos clases laterales coinciden con el subgrupo *H*.

Ejemplo: Partiendo del grupo multiplicativo de los siguientes números complejos: *G* = ⟨ 1, i, -1, -i ⟩ y del subgrupo *H* = ⟨ 1, -1 ⟩, veamos las clases izquierdas que genera cada elemento de *G*:

$$a = 1 \rightarrow 1H = \{1 \cdot h \mid h \in H\} = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\} = H$$
$$a = i \rightarrow iH = \{i \cdot h \mid h \in H\} = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\}$$
$$a = -1 \rightarrow (-1)H = \{-1 \cdot h \mid h \in H\} = \{-1 \cdot 1, -1 \cdot (-1)\} = \{-1, 1\} = H$$
$$a = -i \rightarrow (-i)H = \{-i \cdot h \mid h \in H\} = \{-i \cdot 1, -i \cdot (-1)\} = \{-i, i\}$$

Al tratarse de una operación conmutativa, las clases derechas son idénticas a las izquierdas.

Ejemplo: Partiendo del grupo aditivo de los vectores del plano: $G = \{(x, y) \mid x, y \in \Re\}$ y del subgrupo formado por los vectores paralelos a un vector concreto (*a*, *b*): $H = \{(at, bt) \mid t \in \Re\}$, cada vector *v* de *G* genera la siguiente clase izquierda (que, por la conmutatividad, es idéntica a la clase derecha):

$$v = (x_0, y_0) \rightarrow v + H = \{(x_0, y_0) + (at, bt) \mid t \in \Re\} = \{(x_0 + at, y_0 + bt) \mid t \in \Re\}$$

Este ejemplo tiene una interpretación gráfica interesante. *G* es todo el plano, el subgrupo H sería una recta que pasase por el origen y las clases laterales de H en *G* serían rectas paralelas a H.

5.3 Ejemplos de grupos infinitos

Veremos a continuación ejemplos conocidos de grupos infinitos:

5.3.1 Grupos abelianos aditivos de los vectores del Plano

El conjunto formado por todos los vectores del plano con la suma tradicional de vectores tiene estructura de grupo abeliano en el que el elemento neutro es el vector nulo y el simétrico de un vector es su opuesto. El subconjunto formado por los vectores paralelos a uno dado es un subgrupo.

5.3.2 Grupos abelianos aditivos de números

(Z, +) el conjunto de los números enteros, con la suma, tiene estructura de grupo abeliano con 0 de elemento neutro y los opuestos como simétricos. Contiene, entre otros subgrupos, a los formados por los múltiplos de un determinado número entero.

(Q, +) el conjunto de los números racionales, con la suma, tiene estructura de grupo abeliano con 0 de elemento neutro y los opuestos como simétricos. Contiene, entre otros subgrupos, a (Z, +).

(R, +) el conjunto de los números reales, con la suma, tiene estructura de grupo abeliano con 0 de neutro y los opuestos como simétricos. Contiene como subgrupos, entre otros, a (Q, +) y a (Z, +).

(C, +) el conjunto de los números complejos, con la suma, tiene estructura de grupo abeliano con 0 de elemento neutro y los opuestos como simétricos. Contiene como subgrupos, entre otros, a todos los grupos anteriores: (Q, +) (Z, +) y a (R, +).

(N, +) no es grupo por carecer de simétricos (no contiene a los números negativos).

5.3.3 Grupos abelianos multiplicativos de números

(Q, ·) – {0} el conjunto de los números racionales, con el producto, tiene estructura de grupo abeliano con 1 de elemento neutro y los inversos como simétricos. Se excluye el 0 por carecer de inverso. Contiene, entre otros subgrupos, a los formados por las potencias de exponente entero de un determinado número racional.

(R, ·) – {0} el conjunto de los números reales, con el producto, tiene estructura de grupo abeliano con 1 de elemento neutro y los inversos como simétricos. Se excluye el 0 por carecer de inverso. Contiene como subgrupo, entre otros, a (Q, ·) - {0}

(C, ·) – {0} el conjunto de los números complejos, con el producto, tiene estructura de grupo abeliano con 1 de elemento neutro y los inversos como simétricos. Se excluye el 0 + 0·i por carecer de inverso. Contiene como subgrupos, entre otros, a (Q, ·) - {0} y a (R, ·) - {0}

(N, ·) (Z, ·) no son grupos por carecer de simétricos (no contienen a los números fraccionarios).

5.3.4 Grupo de las funciones invertibles

El conjunto formado por todas las funciones biyectivas $f : A \to A$ definidas en un mismo conjunto con la composición de funciones como operación, tiene estructura de grupo no abeliano en el que la función identidad $i(x) = x$ es el elemento neutro y el simétrico de cada función es su función recíproca (también llamada inversa).

5.3.5 Grupos abelianos aditivos de las matrices con un mismo orden

El conjunto formado por todas las matrices de un mismo orden (mxn) con la suma de matrices tiene estructura de grupo abeliano en el que la matriz nula de orden (mxn) es el elemento neutro y el simétrico de cada matriz será su opuesta.

5.3.6 Grupo multiplicativo de las matrices cuadradas regulares con un mismo orden

El conjunto formado por todas las matrices cuadradas de un mismo orden (nxn) que sean regulares, esto es, que por tener determinante distinto de cero tienen inversa, con el producto de matrices tiene estructura de grupo no abeliano en el que la matriz identidad I_n es el elemento neutro y el simétrico de cada matriz será su inversa.

5.4 Ejemplos de grupos finitos

5.4.1 Grupos de las raíces de la unidad

Al realizar las raíces cuadradas, cúbicas, ... enésimas del número 1, se obtienen *n* números complejos que forman un grupo respecto del producto. Resultan grupos cíclicos generados por $1_{2\pi/n.}$ Reciben el nombre de C_n

Las raíces cuadradas: $C_2 = \{1, -1\}$ con –1 como generador. $(-1)^1 = 1$ $(-1)^2 = 1$

Las raíces cúbicas: $C_3 = \{1, 1_{2\pi/3}, 1_{4\pi/3}\}$ con $1_{2\pi/3}$ como generador.

Las raíces cuartas: $C_4 = \{1, i, -1, -i\}$ que es un grupo ya visto antes y tiene como generador a $i = 1_{\pi/2}$:

$i^1 = i$ $i^2 = -1$ $i^3 = -i$ $i^4 = 1$

La tabla que aparece en el epígrafe de grupos cíclicos es el grupo de las raíces quintas, generado por $g = 1_{2\pi/5}$.

Las raíces enésimas $C_n = \{1, 1_{2\pi/n}, 1_{4\pi/n}, \ldots, 1_{2\pi(n-1)/n}\}$ con $1_{2\pi/n}$ como generador.

Los subgrupos de estos grupos dependen de los divisores de *n*. Por ejemplo, C_6 contiene como subgrupos propios a C_2 y a C_3.

5.4.2 Grupos abelianos aditivos de las clases de restos módulo *m*

Para cualquier valor de *m* el conjunto de las clases de restos módulo *m* forma siempre un grupo aditivo.

Por ejemplo las clases de restos módulo 5:

El grupo es $G = \{0, 1, 2, 3, 4\}$ en que cada cifra representa la clase a la que pertenece dicho número

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

La tabla está construida operando en módulo 5. Por ejemplo:
3 + 4 = 7 en la suma tradicional
3 ≡ clase3
4 ≡ clase4
7 ≡ clase2 (dividiendo 7 entre 5, el resto es 2)

Entonces: **clase3 + clase4 = clase2**
y lo resumimos con: **3 + 4 = 2**

Se trata de un grupo ya que 0 es elemento neutro, se cumple la asociativa (por cumplirse en *Z*) y todos los elementos tienen simétrico (1 y 4 simétricos, 2 y 3 simétricos 0 simétrico de sí mismo). Es abeliano por ser conmutativa la suma en *Z*.

5.4.3 Grupos abelianos multiplicativos de las clases de restos módulo *m*

En todos los casos excluiremos la clase 0 ya que carece de simétrico. Pero esto ya sucedía en los grupos multiplicativos de los conjuntos de números racionales, reales o complejos.

A diferencia de los aditivos, no todas las clases de restos en un cierto módulo *m* forman un grupo. Dependerá de que *m* sea o no un número primo.

Veamos las clases de restos módulo 5 y módulo 6 como ejemplos de *m* primo y compuesto:

En **módulo 5** tenemos $G = \{1, 2, 3, 4\}$
(nótese que hemos excluido la clase 0)

·	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

En esta operación vemos que 1 es el elemento neutro.
2 y 3 son simétricos
1 y 4 son simétricos de sí mismos
La asociativa se cumple por cumplirse en *Z*
Luego $(G, \cdot)$ es un grupo multiplicativo.
Al ser conmutativa la multiplicación en *Z* el grupo será abeliano.

En **módulo 6** tenemos $G = \{1, 2, 3, 4, 5\}$
(nótese que hemos excluido la clase 0)

·	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

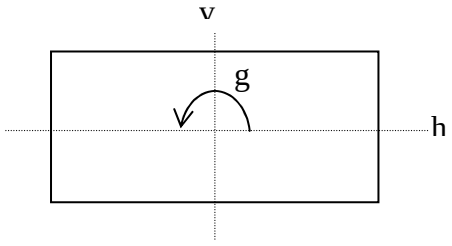
1 sería el elemento neutro.
Vemos que la operación no está cerrada ya que aparece el 0
2, 3 y 4 no tienen simétricos
Luego *G* no forma un grupo
Curiosamente $\{1, 5\}$ sí forma un grupo multiplicativo en módulo 6

5.4.4 Grupos de las simetrías de una figura plana

Convendremos en llamar en general simetrías de una figura plana a los movimientos *propios* (giros en torno a un punto) e *impropios* (reflexiones en torno a una recta) que convierten la figura en otra superponible a la original, es decir, que la dejan invariante.

Se puede estudiar para multitud de figuras planas en las que exista algún centro o eje de simetría. Las más habituales son las siguientes:

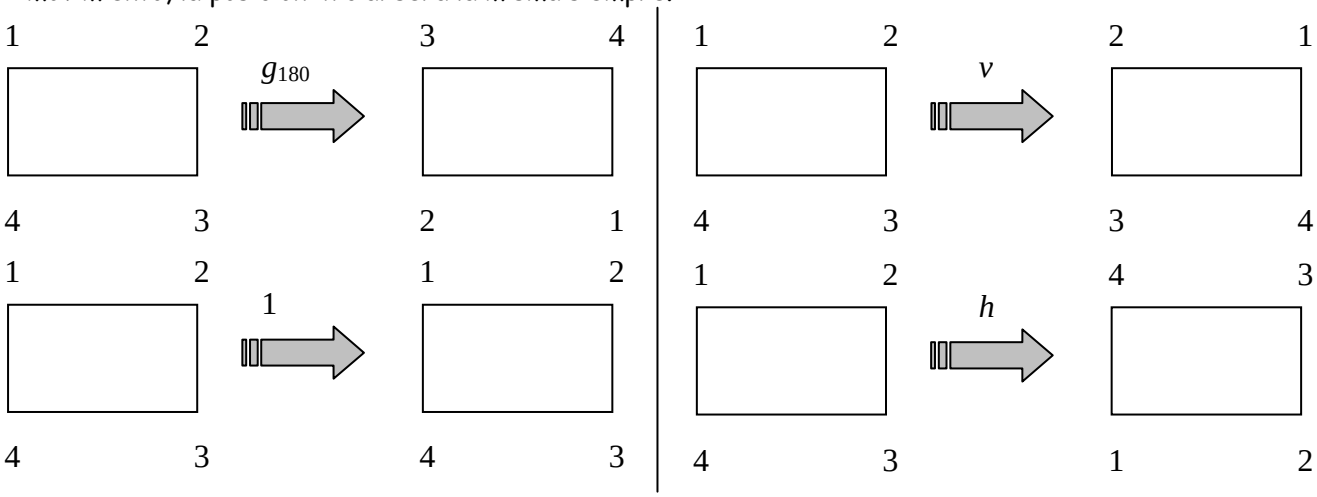
5.4.4.1 Grupo de las simetrías del rectángulo: D_2



Los elementos del grupo son los movimientos que podemos hacer al rectángulo manteniéndole superponible a su posición original.
Son cuatro:

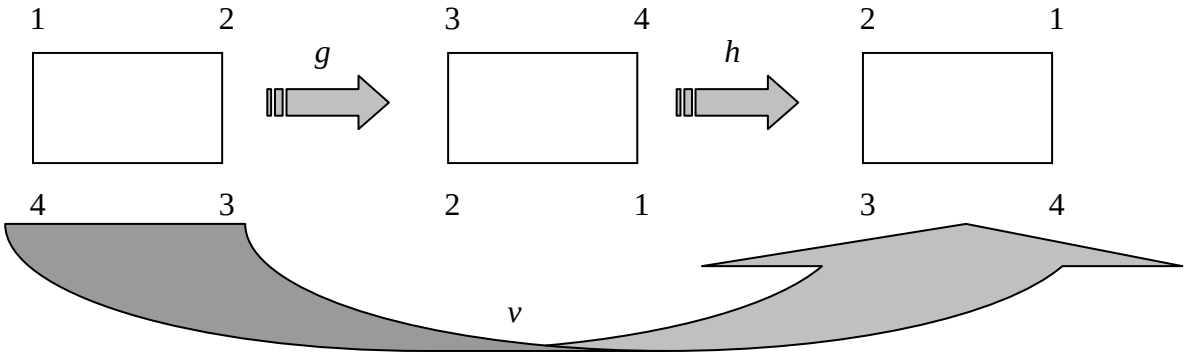
- Giro de 180° (lo llamaremos *g*)
- Giro de 360° (ó también 0°) (lo llamaremos 1)
- Reflexión en torno al eje de simetría vertical (lo llamaremos *v*)
- Reflexión en torno al eje de simetría horizontal (lo llamaremos *h*)

Para estudiar cada movimiento debemos identificar los vértices y señalar cómo quedan después del movimiento, la posición inicial será la misma siempre.



La operación del grupo será la composición de movimientos. Componer dos movimientos significará realizar el primero para, a continuación, concatenar el segundo. Si se hace un seguimiento de cómo quedan los vértices al final, deduciremos que dicha composición equivale a un movimiento simple.

Por ejemplo, $g*h$ significará hacer primero el giro de 180° y después la reflexión horizontal. Visto que el resultado final es el mismo que el de la reflexión v, se deduce que $g*h = v$



Realizadas todas las composiciones se obtiene la siguiente tabla:

*	1	g	v	h
1	1	g	v	h
g	g	1	h	v
v	v	h	1	g
h	h	v	g	1

El elemento neutro es el giro de 360° que por comodidad hemos llamado 1.

Vemos que resulta un grupo abeliano llamado ***grupo diédrico D_2***

Contiene a los siguientes subgrupos propios:

$\{1, g\}$ $\{1, v\}$ $\{1, h\}$

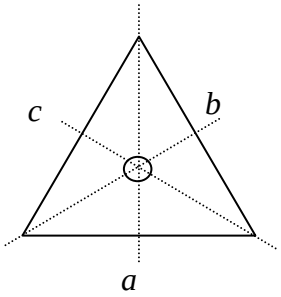
Salvo isomorfismos los únicos grupos con cuatro elementos son D_2 y C_4

5.4.4.2 Grupo de las simetrías del triángulo equilátero: D_3

Los elementos del grupo son los movimientos que podemos hacer al triángulo equilátero manteniéndole superponible a su posición original.

Son seis:

- Giro de 120° (lo llamaremos g)
- Giro de 240° (lo llamaremos g^2)
- Giro de 360° (ó también 0°) (lo llamaremos 1)
- Reflexiones en torno a las tres mediatrices: a, b, c



Realizadas todas las composiciones se obtiene la siguiente tabla:

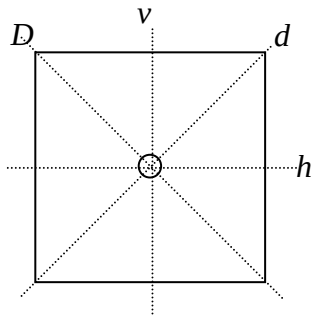
*	**1**	***g***	***g²***	***a***	***b***	***c***
1	1	*g*	g^2	*a*	*b*	*c*
g	*g*	g^2	1	*b*	*c*	*a*
g²	g^2	1	*g*	*c*	*a*	*b*
a	*a*	*c*	*b*	1	g^2	*g*
b	*b*	*a*	*c*	*g*	1	g^2
c	*c*	*b*	*a*	g^2	*g*	1

El elemento neutro es el giro de 360º que por comodidad hemos llamado 1.
Vemos que resulta un grupo llamado ***grupo diédrico*** D_3
Este es el grupo no abeliano con el menor número de elementos y es isomorfo al que aparece en el epígrafe **5.1**
Contiene a los siguientes subgrupos propios:
$\{1, a\}$ $\{1, b\}$ $\{1, c\}$ $\{1, g, g^2\}$
(éste último es cíclico isomorfo a C_3)

5.4.4.3 Grupo de las simetrías del cuadrado: D_4

Los elementos del grupo son los movimientos que podemos hacer al cuadrado manteniéndole superponible a su posición original.
Son ocho:

- Giro de 90º (lo llamaremos *g*)
- Giro de 180º (lo llamaremos g^2)
- Giro de 270º (lo llamaremos g^3)
- Giro de 360º (ó también 0º) (lo llamaremos 1)
- Reflexiones en torno a las dos mediatrices: *v*, *h*
- Reflexiones en torno a las dos diagonales: *D*, *d*



Realizadas todas las composiciones se obtiene la siguiente tabla:

*	1	*g*	g^2	g^3	*h*	*v*	*d*	*D*
1	*1*	*g*	g^2	g^3	*h*	*v*	*d*	*D*
g	*g*	g^2	g^3	*1*	*D*	*d*	*h*	*v*
g^2	g^2	g^3	*1*	*g*	*v*	*h*	*D*	*d*
g^3	g^3	*1*	*g*	g^2	*d*	*D*	*v*	*h*
h	*H*	*d*	*v*	*D*	*1*	g^2	*g*	g^3
v	*V*	*D*	*h*	*d*	g^2	*1*	g^3	*g*
d	*D*	*v*	*D*	*h*	g^3	*g*	*1*	g^2
D	*D*	*h*	*d*	*v*	*g*	g^3	g^2	*1*

El elemento neutro es el giro de 360º que por comodidad hemos llamado 1.
Vemos que resulta un grupo llamado ***grupo diédrico*** D_4
Es un grupo no abeliano.
Contiene a los siguientes subgrupos propios:
$\{1, h\}$ $\{1, v\}$ $\{1, d\}$ $\{1, D\}$ $\{1, g^2\}$
$\{1, g, g^2, g^3\}$ $\{1, g^2, d, D\}$ $\{1, g^2, v, h\}$

5.4.5 Grupos de las permutaciones de *n* objetos: S_n

Del estudio de estos grupos es de donde ha partido la teoría de grupos moderna.
Las permutaciones de *n* números nos ayudarán a indicar cómo son los movimientos, pero no son propiamente los elementos del grupo. Los elementos de estos grupos serán los movimientos que reordenen listas de objetos.
Las permutaciones las escribiremos siempre partiendo de un mismo orden (el numérico o el alfabético) indicando debajo la nueva ordenación. Por ejemplo la permutación $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ indica que, partiendo de tres elementos, se mantendría la posición del segundo objeto mientras que se intercambiarían las posiciones del primero y tercero.

La permutación que no modifica el orden inicial se denomina 'identidad' y jugará el papel de elemento neutro.

$$e = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & 2 & 3 & \dots & n-1 & n \end{pmatrix}$$

Para cada permutación, se podrá hallar su 'inversa', que sería aquella que devolviera al orden original los elementos ordenados. Lógicamente si encadenásemos ambas permutaciones se obtendría la permutación identidad. En la estructura de grupo diremos que son elementos simétricos.

Por ejemplo, como en la permutación $p=\begin{pmatrix}1&2&3&4&5\\5&3&1&4&2\end{pmatrix}$ el primer elemento pasa a la tercera posición, en la permutación inversa el tercer elemento deberá pasar a la primera posición; y como el segundo elemento de p pasa a la última posición, en la permutación inversa el último elemento deberá pasar a la segunda posición; estudiando de esta forma todas las ordenaciones se obtiene: $p^{-1}=\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}$

Como es sabido, el número total de las permutaciones de n elementos es $n!=n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot3\cdot2\cdot1$, por lo que estudiar el caso de cuatro elementos manejaría 24 permutaciones, grupo que resulta demasiado voluminoso para hacer un estudio completo, lo contrario que le ocurre el caso de dos elementos, al resultar un grupo de únicamente 2 permutaciones. El estudio adecuado es el de las 6 permutaciones de tres elementos:
El grupo $G=\{e, a, b, c, d, f\}$ estará formado con estas 6 permutaciones:

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\ a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\ b=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\ c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\ d=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\ f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

La operación será la composición (concatenación) de movimientos. Es decir que movimiento final reordenará los objetos tal como hayan quedado ordenados con el movimiento inicial. Por convenio se empieza con la permutación que se escribe en segundo lugar.
Veamos por ejemplo la operación $b*d$. Empezando con la permutación d, el elemento central mantendrá su posición intercambiándolas los extremos. Por lo que hasta ahora tendríamos: $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

Ahora se realizaría el movimiento de la permutación b. Con ésta, el primer objeto pasa al centro, el 2º al final y el último al inicio. Como los objetos que encuentra son $(3\ \ 2\ \ 1)$ los reordenará como $(1\ \ 3\ \ 2)$.

Como la permutación $c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ es la que realiza este movimiento deducimos que $b*d=c$

Todo este proceso se visualiza así: $b*d=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}*\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\\1&3&2\end{pmatrix}=c$

Realizadas todas las composiciones resulta la tabla:

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

La operación está cerrada, ya que se obtienen resultados pertenecientes al mismo conjunto G.
e es el elemento neutro
a, b son simétricos uno del otro
e, c, d, f son simétricos de sí mismos
Eligiendo todos los tríos posibles, se demostraría que se cumple la propiedad asociativa.
El grupo recibe el nombre de ***grupo simétrico S_3***
No se cumple la propiedad conmutativa, véase cómo $a*c=d$ mientras que $c*a=f$

Resulta una tabla similar a la del grupo diédrico de 6 elementos no abeliano ya visto. Se dice entonces que ***S_3 es isomorfo al grupo diédrico D_3***
Contiene a los subgrupos de orden dos: $\{e, c\}$ $\{e, d\}$ $\{e, f\}$ y al subgrupo de orden tres $\{e, a, b\}$.
Las permutaciones e, a, b reciben el nombre de permutaciones pares y las restantes c, d, f impares.

De forma similar, se pueden estudiar las permutaciones de n elementos resultando los ***grupos simétricos S_n***, que tienen obviamente $n!$ elementos. Cada uno de ellos contiene, entre otros, al subgrupo cíclico formado por los $\frac{n!}{2}$ elementos pares, al que se denomina grupo ***alternado***.

5.4.5.1 Notación de ciclos

Existe otra notación más compacta de las permutaciones, llamada notación de ciclos. Un ciclo de longitud L es una permutación que intercambia cíclicamente L elementos y fija los restantes.

Entre paréntesis aparecerán escritos varios elementos, se entenderá entonces que el segundo elemento es la imagen del primero, el tercero la imagen del segundo, y seguimos así hasta el último cuya imagen es el primero. Si hay otros elementos que no aparecen escritos en el ciclo, se entenderá que son imágenes de sí mismos. Esta notación revela mejor la estructura interna de la permutación.

Por ejemplo, el ciclo (1 3 5 6) equivale a la permutación: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix}$

Es posible que una permutación contenga más de un ciclo. De ser así, se escriben, unos a continuación de otros, varios ciclos entre paréntesis, y se actuaría de la misma manera.

Por ejemplo, la notación cíclica (1 3 5 6)(2 4) equivale a la permutación: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix}$ y viceversa.

Si queremos descomponer una permutación en ciclos disjuntos, empezaríamos con cualquier elemento. Lo escribimos, a su derecha escribimos su imagen, a la derecha de esta, la imagen de su imagen, y seguimos así hasta que se complete un ciclo. Luego cogemos cualquier elemento no contenido en el primer ciclo, volvemos a escribir su imagen a su derecha, y continuamos hasta completar el segundo ciclo. El proceso continúa hasta que la permutación entera ha quedado descrita como producto de ciclos disjuntos. Si algún elemento fuese imagen de sí mismo, no es necesario explicitarlo como ciclo de un elemento.

Por ejemplo, la permutación: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$ equivale a la notación cíclica: (1 3 5)(2 4)

La descomposición realizada por el procedimiento anterior no es única en principio, pues de haber empezado por otros elementos, podríamos haber obtenido otros resultados equivalentes:

Por ejemplo, la permutación: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$ también equivale a la notación cíclica: (4 2)(5 1 3)

La descomposición **canónica** de una permutación como producto de ciclos se obtiene colocando en primer lugar de cada ciclo el número más pequeño del mismo. Posteriormente se procede a la colocación de los ciclos, colocando primero el ciclo cuyo primer elemento sea menor. Frecuentemente, suelen omitirse los ciclos de longitud 1. Así la permutación (1 3)(2)(4 5) se escribe simplemente como (1 3)(4 5).

Si quisiésemos hallar el orden de determinada permutación, es decir, el mínimo número de veces que tuviésemos que componer una permutación consigo misma para obtener la permutación identidad, se puede aplicar el siguiente teorema:

$$orden(p) = m.c.m.(l_1, ..., l_m)$$

Si llamamos $l_1, ..., l_m$ a la longitud de los ciclos en que esté descompuesta la permutación, su orden coincidirá con su mínimo común múltiplo.

Ejemplo: Halla el orden de la permutación: $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}$

Primero obtenemos su notación cíclica: (1 4)(2 5 6 3). El primer ciclo tiene longitud 2 y el segundo 4.
Por lo tanto su orden es 4. Esto significa que p^4 resulta el elemento neutro.

La notación de ciclos es también útil para hallar fácilmente la inversa de una permutación:

Ejemplo: Halla la permutación inversa de $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}$

Primero convertiríamos dicha permutación en ciclos: $p = (1 \quad 4)(2 \quad 5 \quad 6 \quad 3)$

Su inversa, en ciclos, es obviamente: $p^{-1} = (4 \quad 1)(3 \quad 6 \quad 5 \quad 2)$, de donde: $p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 2 & 5 \end{pmatrix}$

5.5 Homomorfismo de Grupos

Hemos visto hasta ahora ejemplos de grupos en los que se podía observar gran parecido entre sus tablas de Cayley reconociendo la misma estructura aplicada a elementos y operaciones distintas. En primer lugar definiremos el homomorfismo de grupos, para terminar con lo que se denomina isomorfismo.
La definición de homomorfismo es la que sigue:

$$(G,*) \text{ es homomorfo a } (H,\circ) \Leftrightarrow \exists\, f: G \to H \mid \forall x_1, x_2 \in G \Rightarrow f(x_1 * x_2) = f(x_1) \circ f(x_2)$$

La función f recibe el nombre ***homomorfismo*** entre los grupos G y H

El homomorfismo se construirá de manera distinta según sean los grupos finitos o infinitos. De ser finitos el homomorfismo será simplemente una tabla mientras de ser infinitos definiríamos una función.

Ejemplo: Demuestra que la función definida entre el grupo aditivo de los números reales y el grupo multiplicativo de los números reales excluido el cero $f:(\Re,+)\to(\Re-\{0\},\cdot)$ con $f(x)=e^x$, es un homomorfismo.

$f(x_1+x_2)=e^{x_1+x_2}=e^{x_1}\cdot e^{x_2}=f(x_1)\cdot f(x_2)$

Ejemplo: Demuestra que el grupo multiplicativo de los números complejos excluido el cero es homomorfo al grupo multiplicativo de los números reales excluido el cero.

Es sabido que al multiplicar dos números complejos en forma polar se multiplican sus módulos (y se suman sus argumentos, pero esta parte no la necesitaremos) por lo que la función $f:(\square-\{0\},+)\to(\square-\{0\},\cdot)$ $f(z)=\sqrt{x^2+y^2}$ con $z=x+yi$ cumplirá la condición de homomorfismo: $f(z_1\cdot z_2)=f(z_1)\cdot f(z_2)$

5.5.1 Definición de Núcleo e imagen de un homomorfismo

Todos aquellos elementos de G cuya imagen mediante el homomorfismo f sea el elemento neutro de H (al que llamaremos e_H) forman un subconjunto de G llamado **núcleo** del homomorfismo y se escribe Ker(f).

$$Ker(f)=\{x\in G \mid f(x)=e_H\}$$

Todos aquellos elementos de H que sean imagen de algún elemento de G mediante el homomorfismo f forman un subconjunto de H llamado **imagen** del homomorfismo y se escribe Im(f).

$$\mathrm{Im}(f)=\{y\in H \mid \exists x\in G,\ f(x)=y\}$$

5.5.2 Propiedades de los homomorfismos para el elemento neutro y los elementos simétricos

Teorema: En todo homomorfismo, la imagen del elemento neutro e_G de $(G,*)$ es el elemento neutro e_H de $(H,\circ)$. Es decir, que $f(e_G)=e_H$.

Demostración:

$$x\in G,\ f(x*e_G)\overset{(1)}{=}f(x)\circ f(e_G)\overset{(2)}{\Rightarrow}f(x)=f(x)\circ f(e_G)\overset{(3)}{\Rightarrow}f(e_G)=e_H$$

(1): Definición de Homomorfismo
(2): Propiedad del elemento neutro en G
(3): Al ser H un grupo, podemos simplificar f(x)

Teorema: En todo homomorfismo, la imagen del simétrico de cualquier elemento de G es simétrica de la imagen de dicho elemento. Es decir, que $f(x^{-1})=(f(x))^{-1}$. O, dicho de otra forma, que $f(x)$ y $f(x^{-1})$ son simétricos.

Demostración:

$$x\in G,\ \left.\begin{array}{l} f(x)\circ f(x^{-1})\overset{(1)}{=}f(x*x^{-1})\overset{(2)}{=}f(e_G)\overset{(3)}{=}e_H \\ f(x^{-1})\circ f(x)\overset{(1)}{=}f(x^{-1}*x)\overset{(2)}{=}f(e_G)\overset{(3)}{=}e_H \end{array}\right\}\Rightarrow f(x) \text{ y } f(x^{-1}) \text{ son simétricos}$$

(1): Definición de Homomorfismo
(2): Propiedad de los elementos simétricos en G
(3): Anterior demostración

5.5.3 Teorema: El Núcleo de un homomorfismo es subgrupo del grupo inicial $(G,*)$

Demostración:

Demostraremos que el núcleo de un homomorfismo cumple la condición necesaria y suficiente de los subgrupos: $(Ker(f),*)\text{es subgrupo de}(G,*)\Leftrightarrow\left(\forall x_1,x_2\in Ker(f)\Rightarrow x_1*x_2^{-1}\in Ker(f)\right)$

$$\forall x_1,x_2\in Ker(f)\overset{(1)}{\Rightarrow}\left.\begin{array}{c}f(x_1)=e_H\\ f(x_2)=e_H\overset{(2)}{\Rightarrow}f(x_2^{-1})=e_H^{-1}\overset{(3)}{=}e_H\end{array}\right\}\overset{(4)}{\Rightarrow}$$

$$\overset{(4)}{\Rightarrow}f(x_1*x_2^{-1})=f(x_1)\circ f(x_2^{-1})=e_H\circ e_H\overset{(5)}{=}e_H\overset{(1)}{\Rightarrow}x_1*x_2^{-1}\in Ker(f)\overset{(6)}{\Rightarrow}(Ker(f),*)\text{es subgrupo de}(G,*)$$

(1): Definición de Núcleo de un homomorfismo
(2): Anterior demostración sobre simétricos
(3): Los elementos neutros son simétricos de sí mismos
(4): Definición de Homomorfismo
(5): Propiedad del elemento neutro
(6): Condición necesaria de los subgrupos

5.5.4 Teorema: La Imagen de un homomorfismo es subgrupo del grupo final $(H,\circ)$

Demostración:

Demostraremos que la imagen de un homomorfismo cumple la condición necesaria y suficiente de los subgrupos: $(\text{Im}(f),\circ)\text{es subgrupo de}(H,\circ)\Leftrightarrow\left(\forall y_1,y_2\in\text{Im}(f)\Rightarrow y_1\circ y_2^{-1}\in\text{Im}(f)\right)$

$$\forall y_1,y_2\in\text{Im}(f)\overset{(1)}{\Rightarrow}\left.\begin{array}{c}\exists x_1\in G\mid f(x_1)=y_1\\ \exists x_2\in G\mid f(x_2)=y_2\overset{(2)}{\Rightarrow}f(x_2^{-1})=y_2^{-1}\end{array}\right\}\overset{(3)}{\Rightarrow}$$

$$\overset{(3)}{\Rightarrow}f(x_1*x_2^{-1})=f(x_1)\circ f(x_2^{-1})=y_1\circ y_2^{-1}\overset{(1)}{\Rightarrow}y_1\circ y_2^{-1}\in\text{Im}(f)\overset{(4)}{\Rightarrow}(\text{Im}(f),\circ)\text{es subgrupo de}(H,\circ)$$

(1): Definición de Imagen de un homomorfismo
(2): Anterior demostración sobre simétricos
(3): Definición de Homomorfismo
(4): Condición necesaria de los subgrupos

Todos estos teoremas pueden ser útiles para construir un homomorfismo entre dos grupos o para demostrar que un grupo no es homomorfo a otro.

Ejemplo: Construye un homomorfismo entre Z_6, el grupo aditivo de las clases de restos módulo 6, y C_3, el grupo multiplicativo que las raíces cúbicas de la unidad.

Tenemos entonces: $Z_6=\{0,1,2,3,4,5\}$ y $C_3=\{1,a,b\}$ siendo $a=1_{\frac{2\pi}{3}}$ y $b=1_{\frac{4\pi}{3}}$

Sabemos que la imagen del elemento neutro de Z_6 debe ser el elemento neutro de C_3. Por lo tanto: $f(0)=1$

Como 3 es simétrico de sí mismo en Z_6, $\{0,3\}$ es subgrupo de Z_6, por lo que podría jugar el papel de núcleo del homorfismo f. Por lo tanto: $f(3)=1$

Como 1 y 5 son simétricos, sus respectivas imágenes deben ser también simétricas. Si optamos porque $f(1)=a$, nos obligaría a que $f(5)=b$.

Algo similar sucede con 2 y 4, que también son simétricos. Si decidimos que $f(2)=b$, nos obligaría a que $f(4)=a$.

Quedará entonces:

Z_6	C_3
x	$f(x)$
0	1
1	a
2	b
3	1
4	a
5	b

Únicamente queda comprobar que es un homomorfismo. Es decir que: $f(x_1+x_2)=f(x_1)\cdot f(x_2)$ para todas las parejas de elementos de Z_6. Al ser la suma una operación conmutativa, sólo haremos la mitad de los cálculos. Además, se pueden tratar de una sola vez todas las parejas en las que uno de los elementos es el neutro. Veamos todo ello:

$$\left.\begin{matrix} f(0+x)=f(x) \\ f(0)\cdot f(x)=1\cdot f(x)=f(x) \end{matrix}\right\} \quad \left.\begin{matrix} f(1+1)=f(2)=b \\ f(1)\cdot f(1)=a\cdot a=b \end{matrix}\right\} \quad \left.\begin{matrix} f(1+2)=f(3)=1 \\ f(1)\cdot f(2)=a\cdot b=1 \end{matrix}\right\} \quad \left.\begin{matrix} f(1+3)=f(4)=a \\ f(1)\cdot f(3)=a\cdot 1=a \end{matrix}\right\}$$

$$\left.\begin{matrix} f(1+4)=f(5)=b \\ f(1)\cdot f(4)=a\cdot a=b \end{matrix}\right\} \quad \left.\begin{matrix} f(1+5)=f(0)=1 \\ f(1)\cdot f(5)=a\cdot b=1 \end{matrix}\right\} \quad \left.\begin{matrix} f(2+2)=f(4)=a \\ f(2)\cdot f(2)=b\cdot b=a \end{matrix}\right\} \quad \left.\begin{matrix} f(2+3)=f(5)=b \\ f(2)\cdot f(3)=b\cdot 1=b \end{matrix}\right\}$$

$$\left.\begin{matrix} f(2+4)=f(0)=1 \\ f(2)\cdot f(4)=b\cdot a=1 \end{matrix}\right\} \quad \left.\begin{matrix} f(2+5)=f(1)=a \\ f(2)\cdot f(5)=b\cdot b=a \end{matrix}\right\} \quad \left.\begin{matrix} f(3+3)=f(0)=1 \\ f(3)\cdot f(3)=1\cdot 1=1 \end{matrix}\right\} \quad \left.\begin{matrix} f(3+4)=f(1)=a \\ f(3)\cdot f(4)=1\cdot a=a \end{matrix}\right\}$$

$$\left.\begin{matrix} f(3+5)=f(2)=b \\ f(3)\cdot f(5)=1\cdot b=b \end{matrix}\right\} \quad \left.\begin{matrix} f(4+4)=f(2)=b \\ f(4)\cdot f(4)=a\cdot a=b \end{matrix}\right\} \quad \left.\begin{matrix} f(4+5)=f(3)=1 \\ f(4)\cdot f(5)=a\cdot b=1 \end{matrix}\right\} \quad \left.\begin{matrix} f(5+5)=f(4)=a \\ f(5)\cdot f(5)=b\cdot b=a \end{matrix}\right\}$$

Por lo tanto, $(Z_6,+)$ es homomorfo a $(G,\cdot)$

5.6 Isomorfismo de Grupos

Ya habíamos encontrado ejemplos de grupos en los que se podía observar gran parecido entre sus tablas de Cayley. Este parecido se puede sistematizar de tal manera que podamos tener estudiados de manera abstracta todos los grupos posibles, de manera que, cuando encontremos cualquier ejemplo de grupo con elementos y operación concretas, tendrá la misma forma que uno de los grupos ya estudiados de manera abstracta. Para dos grupos finitos normalmente se visualizarán los emparejamientos mediante una tabla (o un diagrama de Venn), de cualquier manera los emparejamiento serán uno-uno (es decir, una biyección) de los elementos de ambos grupos de tal manera que si en la tabla de Cayley del primer grupo sustituyésemos cada elemento por su respectiva pareja, apareciese la misma tabla de Cayley del 2º grupo. En resumen, llamaremos isomorfismo a un homorfismo biyectivo y, de existir, diremos que los grupos son isomorfismo. Si los grupos fuesen infinitos, el isomorfismo será una función biyectiva con expresión algebraica que relacione ambos conjuntos.

Para dos grupos isomorfos no existe un único isomorfismo posible, normalmente se podrá construir de diversas formas. Las distintas variantes tendrán en común lo ya visto para los homorfismos: que aparecerán emparejados los elementos neutros y que, teniendo emparejados dos elementos, estarán emparejados sus simétricos respectivos. También, como demostraremos después, aparecerán emparejados elementos con el mismo orden.

La definición es la que sigue:

$$(G,*)\text{ es isomorfo a }(H,\circ)\Leftrightarrow \exists\ f\ (\text{biyectiva}): G\to H \mid \forall x_1,x_2\in G \Rightarrow f(x_1 * x_2)=f(x_1)\circ f(x_2)$$

La función *f* recibe el nombre de ***isomorfismo*** entre los grupos *G* y *H*

Ejemplo de Isomorfismo de grupos infinitos:

Se puede demostrar fácilmente que el conjunto $G=\{3n \mid n\in Z\}$ formado por todos los números enteros divisibles entre 3 con la suma tradicional de números reales tiene estructura de grupo aditivo: $\{G,+\}$

También se puede demostrar sin dificultad que el conjunto $H=\{2^n \mid n\in Z\}$ formado por todas las potencias de base 2 y exponente entero con el producto tradicional de números reales tiene estructura de grupo multiplicativo: $\{H,\cdot\}$

Ambos grupos son isomorfos, lo demostraremos construyendo la siguiente función:

$f:(G,+)\to(H,\cdot)$ con $f(3n)=2^n$ con $n\in Z$

Veamos que cumple la condición de Homomorfismo:

$f(3n_1+3n_2)=f(3(n_1+n_2))=2^{n_1+n_2}=2^{n_1}\cdot 2^{n_2}$ con $n_1,n_2\in Z$

Veamos que es Inyectiva:

$f(3n_1)=f(3n_2)\Rightarrow 2^{n_1}=2^{n_2}\Rightarrow 2^{n_1-n_2}=1\Rightarrow n_1-n_2=0\Rightarrow n_1=n_2$ con $n_1,n_2\in Z$

Veamos que es Sobreyectiva:

Para cada elemento 2^n de H, se puede encontrar un elemento de G que sea su origen, es obviamente: $3n$

Por lo tanto $(G,+)$ y $(H,\cdot)$ son isomorfos.

Ejemplo de Isomorfismo de grupos finitos:

El grupo multiplicativo de las clases de restos **módulo 5**: $G = \{1, 2, 3, 4\}$

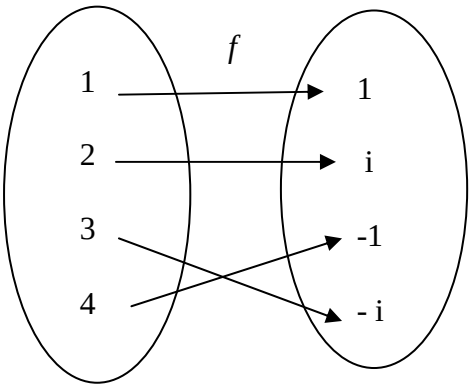
x_5	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

El grupo multiplicativo de raíces cuartas de la unidad: $H = \{1, i, -1, -i\}$

·	**1**	**i**	**-1**	**-i**
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

El isomorfismo se establece emparejando los cuatro elementos del primer grupo con los cuatro del segundo grupo. Al tener que ser una aplicación biyectiva, debe hacerse uno-uno. Es obligado emparejar a los elementos neutros (1 con 1) así como los de orden dos (simétricos de sí mismos) (4 con - 1)

Un posible isomorfismo (hay más opciones) es la del diagrama de la derecha.



A modo de ejemplo, la definición de isomorfismo, aplicada a uno de los 16 casos, indica que deben coincidir $f(2 \times 4) = f(2) \cdot f(4)$

$f(2 \times 4) = f(3) = -i$

$f(2) \cdot f(4) = i \cdot (-1) = -i$

De cumplirse en todos los casos, aseguraremos que, intercambiando en la tabla de multiplicar en módulo 5 los cuatro elementos del primer grupo por sus parejas respectivas, aparecerá la tabla de las raíces cuartas de la unidad.

5.6.1 Teorema: El orden de un elemento permanece invariable por un isomorfismo

Este teorema nos ayudará en casos concretos a construir isomorfismos, ya que sabremos que tenemos que emparejar elementos que tengan el mismo orden.

Dado un isomorfismo entre dos grupos finitos, el orden de cada elemento del primer grupo coincide con el orden de su imagen. Es decir, que: $\forall x \in G, \text{orden}(x) = \text{orden}(f(x))$

Demostración:

Veamos primero que el orden de f(x) es menor o igual que el orden de x:

$$\text{orden}(x) = n \overset{(1)}{\Rightarrow} x^n = e_G \Rightarrow f(x^n) = f(e_G) \overset{(2)}{=} e_H \Rightarrow f(x * x * \overset{[n]}{\ldots} * x) = e_H \overset{(3)}{\Rightarrow}$$

$$\Rightarrow f(x) \circ f(x) \circ \overset{[n]}{\ldots} \circ f(x) = e_H \Rightarrow (f(x))^n = e_H \overset{(1)}{\Rightarrow} \text{orden}(f(x)) \le n \Rightarrow \text{orden}(f(x)) \le \text{orden}(x)$$

(1): Definición de orden de un elemento en un grupo (3): Definición de isomorfismo

(2): Anterior demostración sobre elementos neutros

Veamos ahora que el orden de x es menor o igual que el orden de f(x):

$$\text{orden}(f(x)) = n \overset{(1)}{\Rightarrow} f(x) \circ f(x) \circ \overset{[n]}{\ldots} \circ f(x) = e_H \overset{(2)}{\Rightarrow} f(x * x * \overset{[n]}{\ldots} * x) = e_H \Rightarrow$$

$$\Rightarrow f(x^n) = e_H \overset{(3)}{\Rightarrow} x^n = e_G \overset{(1)}{\Rightarrow} \text{orden}(x) \le n \Rightarrow \text{orden}(x) \le \text{orden}(f(x))$$

(1): Definición de orden de un elemento en un grupo (2): Definición de isomorfismo

(3): Ya vimos que la imagen mediante un homomorfismo del elemento neutro de un grupo es el elemento neutro del otro grupo.

Es decir: $f(e_G) = e_H$. Además, como f es biyectiva, hay un único elemento cuya imagen sea e_H, por lo tanto, $x^n = e_G$.

Por lo tanto x y $f(x)$ tienen el mismo orden.