Universidad
Europea de Madrid
LAUREATE INTERNATIONAL UNIVERSITIES

LEYES, ESTRUCTURAS BÁSICAS Y COCIENTES

CONJUNTOS Y GRUPOS

Índice

Presentación

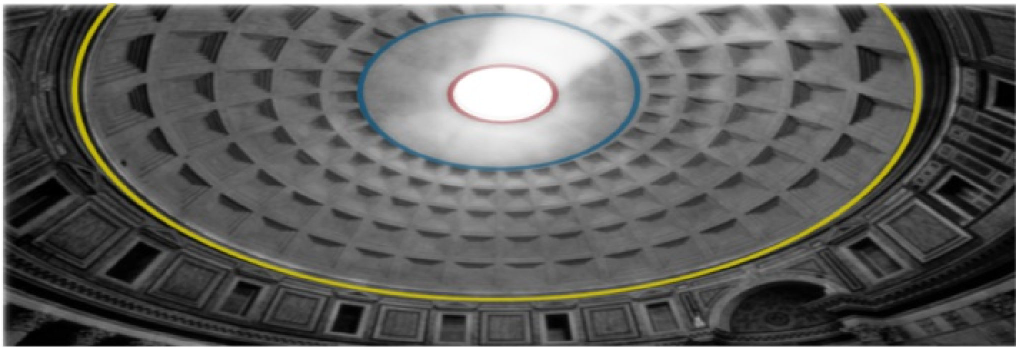
Cuando se estudia un sistema, por complejo que este sea, siempre se puede encontrar un ladrillo constituyente, una estructura tan elemental que si se descompone pierde su sentido. En álgebra eso es el **conjunto.**

Los conjuntos son la estructura algebraica más elemental. La agrupación de elementos matemáticos menos restrictiva que se puede dar. Es la base de todas las demás y, por tanto, la más sólida de entre ellas. Su definición es tan abierta que admite toda clase de posibilidades, con lo que su estudio es paradójicamente complejo.

¿Pero qué pasa cuando se le añade una ley que permite establecer relaciones entre esos elementos? Un gesto tan sencillo como ese hará que toda una nueva familia surja y las posibilidades se expandan exponencialmente. Esto es en lo que se basa el concepto de grupo, que estudiaremos al final del tema.

En este tema aprenderemos:

- Qué es un conjunto, cómo se estudia, qué lo compone.
- Nos acercaremos a qué es y cómo funciona la inyectividad, sobreyectividad y biyectividad.
- Qué es un grupo, como se estudia, qué lo hace tan especial.
- Qué es una aplicación, como afecta a conjuntos y grupos.



Conjuntos

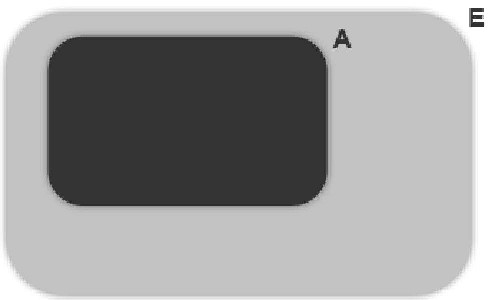
Un **conjunto** es una colección de objetos o elementos, que puede ser finita o infinita. Si un conjunto no tiene ningún elemento se le conoce como conjunto vacío.

Ejemplo de conjunto finito e infinito

Subconjunto

Un conjunto A es una parte o un subconjunto de E, si sólo si, todo elemento de A pertenece a E.

$\{A \subset E \Leftrightarrow \forall x \in A \Rightarrow x \in E\}$



Propiedades de los conjuntos

$A \subset A \rightarrow$Todo conjunto está contenido en sí mismo.

Ejemplo

Ejemplo de conjunto finito e infinito

- **Conjunto finito**: las letras del abecedario.
- **Conjunto infinito**: los puntos de la recta real.

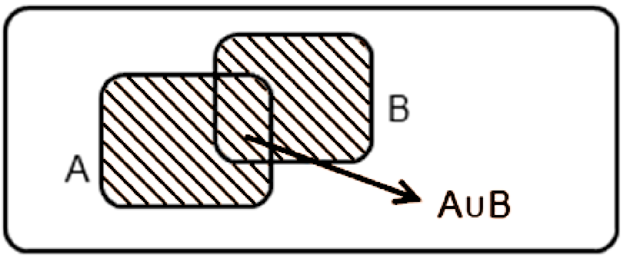
- $Si\, A \subset B \wedge B \subset A \rightarrow A = B$, ya que tienen los mismos elementos:
  - $\{A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B\}$
  - $\{B \subset A \Leftrightarrow \forall x \in B \Rightarrow x \in A\}$
- Si $A \subset B \wedge B \subset C \rightarrow A \subset C$

Igualdad y unión de subconjuntos

A continuación procederemos a estudiar una serie **de relaciones formulables entre subconjuntos**. Estas nos resultarán de enorme utilidad en el estudio de dominio en futuros temas. Veámoslas ahora de forma sencilla:

Igualdad de subconjuntos (A=B)

Como vemos en la imagen, dos conjuntos son iguales sí y sólo, si uno está contenido en el otro y el otro está contenido en el uno.



$A = B \Leftrightarrow A \subset B \wedge B \subset A$

Unión de subconjuntos ($A \cup B$)

Puede observarse que la unión de dos conjuntos está formada por aquellos elementos que pertenecen a un conjunto o bien al otro.

$A \cup B = \{x \in U / x \in A \vee x \in B\}$

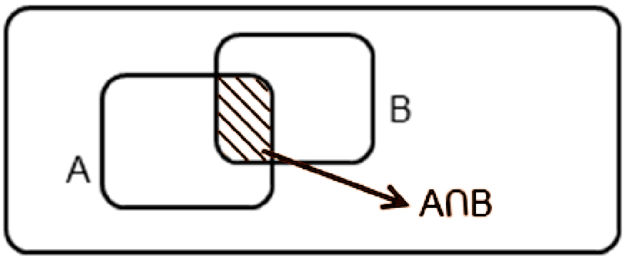
Las **propiedades** de la unión son las siguientes:

Idempotencia	A ⋃ A = A
Propiedad conmutativa	A ⋃ B = B ⋃ A
Propiedad asociativa	(A ⋃ B) ⋃ C = A ⋃ (B ⋃ C)
Propiedad distributiva respecto a la intersección	A ⋃ (B ∩ C) = (A ⋃ B) ∩ (A ⋃ C) (B ∩ C) ⋃ A = (B ⋃ A) ∩ (C ⋃ A)
Ley de absorción	A ⋃ (A ∩ B) = A = A ∩ (A ⋃ B)

Intersección

Intersección de subconjuntos ($A \cap B$)

Puede observarse que la intersección de dos conjuntos está formada por aquellos elementos que pertenecen simultáneamente a un conjunto y al otro.



$A \cap B = \{x \in U / x \in A \wedge x \in B\}$

Las **propiedades de la intersección** son las siguientes:

Idempotencia	A ∩ A = A
Propiedad conmutativa	A ∩ B = B ∩ A
Propiedad asociativa	(A ∩ B) ∩ C = A ∩ (B ∩ C)
Propiedad distributiva respecto a la intersección	A ∩ (B ⋃ C) = (A ∩ B) ⋃ (A ∩ C) (B ⋃ C) ∩ A = (B ∩ A) ⋃ (C ∩ A)
Ley de absorción	A ⋃ (A ∩ B) = A = A ∩ (A ⋃ B)

Correspondencia y aplicaciones

Correspondencia

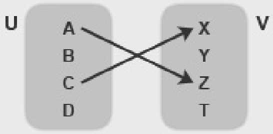
Una correspondencia entre dos conjuntos es una **relación** establecida entre los elementos del primer conjunto y los del segundo. Dicha relación sólo ha de **definirse** y no tiene por qué responder a ninguna propiedad específica.

La correspondencia es la relación más sencilla de entre las existentes entre dos conjuntos, pero es la base de una muchísimo más importante que nos acompañará durante todo el curso, la aplicación.

Veamos unos ejemplos de aplicación y no aplicación:

Correspondencia entre dos conjuntos

Por ejemplo, en el gráfico de conjuntos siguiente se ha hecho una correspondencia que relaciona los elementos A y C de U con los elementos X y Z de V respectivamente.



¿Qué es una aplicación?

Una aplicación es una correspondencia que cumple lo siguiente:

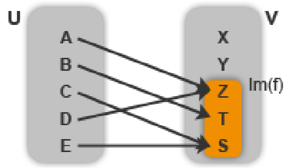
$$f : A \to B$$
$$\{\forall x \in A\ \exists! y \in B / f(x) = y\}$$

Que se leería del siguiente modo:

- (1ª expresión) f es una aplicación que lleva a los elementos del conjunto A hasta los del conjunto B. Habitualmente se llama a A el CONJUNTO INICIAL y a B el CONJUNTO FINAL. O bien conjunto de partida y de llegada.
- (2ª expresión) Para todo elemento "x" perteneciente al conjunto A existe un solo ($\exists!$) elemento "y" perteneciente al conjunto B, tal que (/) el transformado de "x" mediante f es igual a "y".

Conjunto Imagen e Inyectividad

E l **conjunto imagen** está integrado por todos aquellos elementos del conjunto de llegada que son transformados (les llega una correspondencia) de un elemento del conjunto inicial.



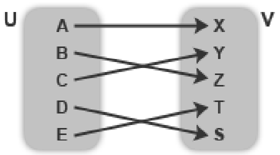
Conjunto imagen: Im(f)

La imagen es por tanto un subconjunto del conjunto final.

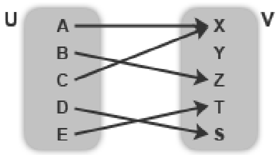
$\mathrm{Im}(f) = \{y \in B / \exists x \in A \quad y = f(x)\}$

Se llamarán **inyectivas** aquellas **aplicaciones** en las que elementos distintos del conjunto inicial tienen imágenes distintas en el conjunto final. Es decir, que ningún elemento del conjunto final recibirá más de una correspondencia del inicial. Esto no implica que todos los elementos del conjunto final tengan que ser imagen de un elemento.

Se formula de dos maneras distintas:
$$f \quad inyectivo \Leftrightarrow \begin{cases} x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \\ \vee \\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \end{cases}$$



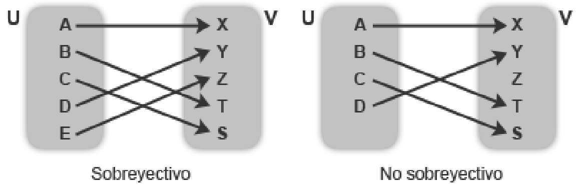
Inyectivo



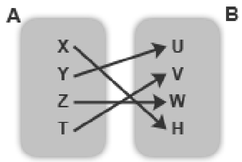
No inyectivo

Sobreyectividad y biyectividad

Aplicación sobreyectiva
Se llamarán sobreyectivas aquellas aplicaciones en las que todos los elementos de la imagen tienen un original. Esto no implica que no puedan recibir más de una correspondencia. Se formula del siguiente modo: $f\ sobreyectiva \Leftrightarrow \forall y \in B\ \exists x \in A / f(x) = y$



Aplicación biyectiva
Una aplicación es llamada biyectiva cuando esta es inyectiva y sobreyectiva simultáneamente. La biyectividad equivale a que haya el mismo número de elementos en el inicial que en el final para poder darse.



BIYECTIVO

Grupos infinitos

Una ley es una relación entre dos elementos de un conjunto que da como resultado otro elemento. Una ley, a la que durante este tema denotaremos *, se denomina ley de composición interna (LCI) cuando operando dos elementos del conjunto mediante esa ley, obtenemos otro elemento de ese mismo conjunto, de la forma:

$$\forall a,b \in G \quad a*b=c \in G$$

Por ejemplo, la suma de números naturales es una ley de composición interna, puesto que dos números naturales cualesquiera, sumados, dan otro número natural. Como por ejemplo, el 2 y el 3:

$$2,3 \in N \quad 2+3=5 \in N$$

Un conjunto denotado G dotado de una ley de composición interna *, con infinitos elementos, tiene estructura algebraica de grupo y se denota (G,*) si cumple los siguientes axiomas:

Axioma 1: La ley * es asociativa: $\forall a,b,c \in G \quad a*(b*c)=(a*b)*c$

Axioma 2: G tiene un elemento neutro (e) con *: $\forall a \in G \quad \exists! e \in G \quad / \quad a*e=e*a=a$

Axioma 3: La ley * dota a cada elemento (a) de G de un simétrico (a'): $\forall a \in G \quad \exists a' \in G \quad / \quad a*a'=a'*a=e$

Un grupo se llama abeliano si su ley es conmutativa, es decir, si al operar dos elementos, el orden en el que se introducen estos es indiferente: $\forall a,b \in G \quad b*a=a*b$.

En un grupo no abeliano, hay que tener en cuenta una serie de normas, llamadas las **reglas de exponentes**:

- $\forall a \in G \quad a^n = a*a*a*\overbrace{\cdots}^{n\ veces}*a$
- $\forall a \in G \quad a^n * a^m = a^{n+m} \quad \forall n,m \in N$
- $\forall a \in G \quad (a^n)^m = a^{n \cdot m} \quad \forall n,m \in N$
- $\forall a,b,c \in G \quad (a*b*c)' = c'*b'*a'$

Siendo esta última la más importante, de las reglas. El simétrico de la operación de varios elementos es la operación de los simétricos, en orden contrario.

Propiedad asociativa

En un grupo, el orden en el que se realicen las operaciones de más de dos elementos es indiferente siempre y cuando los elementos ocupen puestos fijos dentro de la operación.

Elemento neutro

El elemento neutro es único y no depende del elemento (a) del grupo escogido.

Por ejemplo, en el grupo de los números enteros (Z), con la ley suma (+) el elemento neutro es el 0, ya que cualquier número sumado al 0 da ese mismo número: a+0=a.

Mientras que en el grupo de los números reales (R), con la ley producto (·) el elemento neutro es el 1, ya que cualquier número multiplicado por 1 da ese mismo número: a·1=a.

Elemento simétrico

Se dice que dos elementos son simétricos cuando su operación da como resultado el elemento neutro. Así, dado un elemento a de G, a' será su simétrico si a*a'=e.

Al elemento simétrico de un grupo, cuando la ley interna es aditiva (suma) se llama opuesto y si la ley es multiplicativa (producto), inverso.

Por ejemplo, en el grupo de los números enteros (Z) con la ley suma (+), el simétrico del 2 es el -2, que se llama su opuesto. En el grupo de los números reales (R) con la ley producto (·), el simétrico del 2 es el 1/2, que se llama su inverso.

Hay que observar que efectivamente, cada elemento operado con su simétrico, da el neutro del grupo:

En N con la ley +: $\forall a \in N \quad a+(-a)=0$

En R con la ley ·: $\forall a \in R \quad a \cdot \frac{1}{a}=1$

Concepto de subgrupo

Una parte, no vacía, H de un grupo (G,*) es subgrupo si, y sólo si, H tiene estructura de grupo con la ley definida en G.

Sin embargo, es poco práctico demostrar la axiomática completa de un grupo cada vez que queramos definir un subconjunto del mismo como subgrupo. Por esta razón se suele utilizar la siguiente demostración:

$$H\ es\ subgrupo\ de\ G \Leftrightarrow \forall x, y \in H \quad x * y' \in H$$

Es decir, que H es subgrupo si dados dos elementos cualesquiera de H, uno operado por el simétrico del otro da como resultado otro elemento de H.

Veamos un ejemplo:

Los números enteros Z con la suma (Z,+) forman un grupo. Un subgrupo de este grupo podrían ser los números pares. Si tomamos dos números pares cualesquiera, el 6 y el 8 por ejemplo, el uno operado por el simétrico del otro, sale: 6+(-8)=-2, que es otro número par. Es decir, otro elemento del subgrupo. Esto se cumplirá para cualquier pareja de pares que tomemos, luego H, el conjunto de los números pares, es subgrupo de (Z,+).

Propiedades:

- El neutro de H y el de G es siempre el mismo elemento.
- El neutro de G siempre pertenece a todos los subgrupos.
- La intersección de subgrupos es siempre subgrupo.
- La unión de subgrupos, en general, no es subgrupo.
- En cualquier grupo (G,*) existen siempre dos subgrupos que llamaremos triviales o impropios. Son los formados, por un lado, por tan solo el elemento neutro y, por otro lado, por todos los elementos del grupo: $\{e\}$ y G.

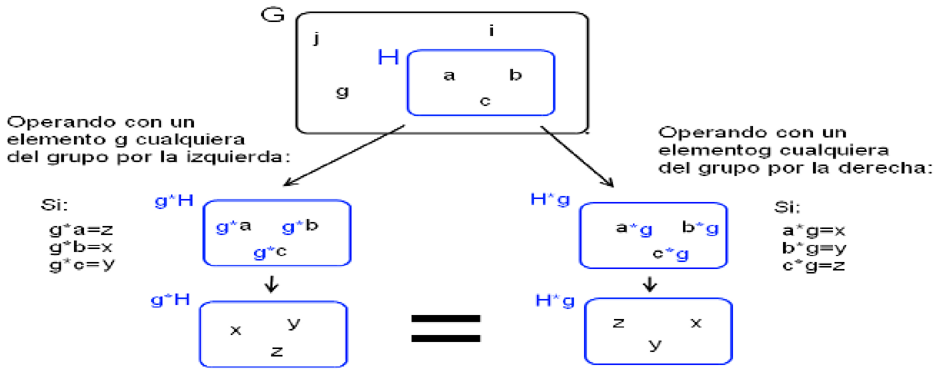
Concepto de subgrupo normal

H, subgrupo de (G,*), se llama subgrupo normal o invariante si y solo si:

1. $\forall g \in G \quad \wedge \quad \forall h \in H \quad g * h * g' \in H$
2. $\forall g \in G \quad \wedge \quad \forall h \in H \quad g * H * g' = H$
3. $\forall g \in G \quad \wedge \quad \forall h \in H \quad g * H = H * g$

Con que se demuestre cualquiera de estas tres afirmaciones, puede decirse que H es un subgrupo normal.

Hay que destacar que esto no es un tipo de conmutatividad, ya que lo importante no es que den los mismos resultados elemento a elemento, sino globalmente, como se intenta explicar en el siguiente croquis.



> **Demostrar cualquiera de las afirmaciones**
>
> A fin de cuentas, en lo que realmente consisten es en afirmar que si los elementos del subgrupo H los opero por la izquierda por cualquier elemento de G y luego los opero por la derecha por ese mismo elemento, el resultado global es el mismo.

Homomorfismos entre grupos

Se denomina homomorfismo a una aplicación f entre dos grupos (G_1,*), que llamaremos inicial o de salida, y (G_2, Δ), que llamaremos final o de llegada, que cumple lo siguiente:

$$f : G_1 \to G_2$$
$$\forall a, b \in G_1 \quad f(a * b) = f(a) \Delta f(b)$$

Es decir: el transformado de la operación de dos elementos es la operación de los transformados de dichos elementos.

Además de lo descrito, un homomorfismo también habrá de transformar, siempre, el neutro del primer grupo en el neutro del segundo:

$$f(e_1) = e_2 \quad con\ e_1 \in G_1 \ \ y \ \ e_2 \in G_2$$

Los homomorfismos se clasifican según la aplicación sea inyectiva, sobreyectiva o biyectiva y según coincidan o no los grupos inicial y final.

Definamos ahora dos partes fundamentales de un homomorfismo: su núcleo y su imagen.

Núcleo	El **núcleo** de un homomorfismo es el subgrupo del grupo inicial que forman todos aquellos elementos que se **transforman en el neutro** del grupo final: $N(f) = \{x \in G_1 / f(x) = e_2\}$ Si f es inyectivo, el núcleo está formado únicamente por el elemento neutro del grupo inicial: G_1.
Imagen	La **imagen** de un homomorfismo es el subgrupo del grupo final que forman todos aquellos elementos que **son transformados de otro**: $\mathrm{Im}(f) = \{y \in G_2 / \exists x \in G_1 \quad f(x) = y\}$ Si f es sobreyectivo, la imagen está formada por todos los elementos del grupo final: G_2.

Clasificación de los homomorfismos

	$f: G_1 \to G_2 \quad (G_1 \neq G_2)$	$f: G \to G \quad (G_1 = G_2 = G)$
f aplicación	**Homomorfismo**	**Endomorfismo**
f aplicación inyectiva	**Monomorfismo**	**Endomorfismo inyectivo**
f aplicación sobreyectiva	**Epimorfismo**	**Endomorfismo sobreyectivo**
f aplicación biyectiva	**Isomorfismo**	**Automorfismo**

Grupos finitos

Llamaremos orden de un grupo, o de un subgrupo, al número de elementos que este contiene.

Un grupo (G,*) se llamará grupo finito cuando posea un orden finito, es decir, cuando este formado por un número finito (natural) de elementos.

En un grupo finito, en lugar de analizarse la axiomática completa de grupo, se podrá afirmar que cumple las condiciones de grupo si con él se puede definir una tabla de Cayley.

Por ejemplo, tomemos el grupo G={1, -1, i, -i}, con la ley interna multiplicación habitual (·) dónde i es la unidad imaginaria y formemos su tabla de Cayley.

		2º operador			
	Ley: ·	1	-1	i	-i
1er operador	1	1	-1	i	-i
	-1	-1	1	-i	i
	i	i	-i	-1	1
	-i	-i	i	1	-1

1

En primer lugar tenemos el 1.

Vemos que 1 en la tabla corresponde con el elemento neutro, porque cada elemento operado con él es igual a sí mismo.

-1

En segundo lugar tenemos el -1.

El -1 operado consigo mismo da el 1, con lo que es su propio simétrico. Esta clase de elementos se denominan autosimétricos.

i y –i

En tercer lugar, tenemos al i y al –i.

i•(-i)=1, mientras que (-i)•i=1, con lo que se trata de una pareja de simétricos.

operador	i	i	-i	-1	1
	-i	-i	i	1	-1

En la columna de la izquierda tenemos los primeros operadores y en la fila superior los segundos. Cada elemento de la tabla se completa como en el juego *hundir la flota*, es decir, que el elemento que sale de operar -1 con i lo colocaremos en la intersección de la fila del operador -1 y en la columna del operador i. Efectivamente, vemos que (-1)·i=-i. Si el grupo es abeliano, la tabla será simétrica.

Tabla de Cayley

Una tabla de Cayley tiene todos los elementos del grupo dispuestos según una fila y una columna y ordenados de forma idéntica en ambas. El interior de la tabla lo forman todas las operaciones posibles entre los elementos. Si no se repite ningún elemento en ninguna fila o columna de la tabla, y todos los elementos que resultan pertenecen al grupo, se puede afirmar que el conjunto dispuesto en la tabla es un grupo finito.

El Teorema de Lagrange

En grupos hay que distinguir entre orden de un grupo, o de un subgrupo, y orden de un elemento.

El orden de un elemento es el menor número de veces que hemos de operar un elemento consigo mismo para obtener el neutro.

Orden de a: $$o(a)=n \quad \Leftrightarrow \quad \underbrace{a*a*a*\ldots*a}_{n\ veces\ "a"}=e$$

Así, en el grupo (G,·) que usamos antes como ejemplo, con G={1, -1, i, -i}, vemos que el orden de G (grupo) es 4 porque tiene cuatro elementos. Veamos los órdenes de sus elementos.

	Ley: ·	2º operador			
		1	-1	i	-i
1er operador	1	1	-1	i	-i
	-1	-1	1	-i	i
	i	i	-i	-1	1
	-i	-i	i	1	-1

1

Orden del 1: o(1)=1

Los neutros de cada grupo son los únicos elementos que presentan orden 1. Esto es debido a que, según la definición de orden, solo será necesario escribirlos una vez para obtener el neutro:

$$\underbrace{1}_{una\ vez}=1$$

-1

Orden del -1: o(-1)=2

Los autosimétricos, por su propia definición, siempre tienen orden 2, porque al ser sus propios simétricos, al operarse consigo mismos dan el neutro:

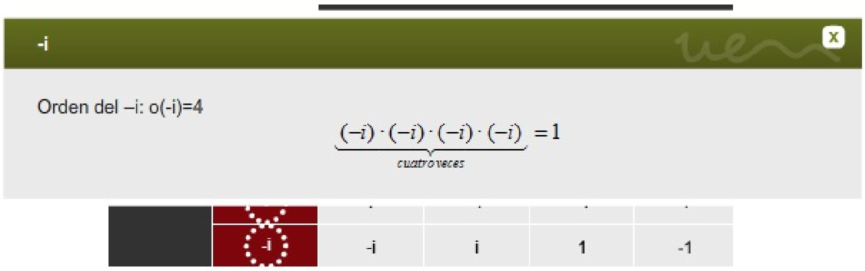
$$\underbrace{(-1)\cdot(-1)}_{dos\ veces}=1$$

i

Orden del i: o(i)=4

$$\underbrace{i\cdot i\cdot i\cdot i}_{cuatro\ veces}=1$$

	-i	-i	i	1	-1



Como puedes comprobar, los elementos simétricos siempre tienen el mismo orden. Ahora, fijémonos en el orden del grupo G (4) y en los órdenes de sus elementos (1, 2 y 4): los órdenes de los elementos de un grupo son siempre divisores del orden del grupo.

En detalle [Afirmaciones basadas en el Teorema de Lagrange] Documentos [Grupos cíclicos y subgrupo generado por A]

Orden de un grupo

Recuerda: el orden de un grupo, como ya hemos visto, es el número de elementos del mismo.

En detalle

Afirmaciones basadas en el Teorema de Lagrange

Según se afirma en el **Teorema de Lagrange**:

- El orden de los elementos de un grupo es siempre divisor del orden de dicho grupo.
- Los órdenes de los subgrupos de un grupo son siempre divisores del orden de dicho grupo.

Resumen

Subconjunto. Un conjunto A es una parte o un subconjunto de E, si sólo si, todo elemento de A pertenece a E: $\{A \subset E \Leftrightarrow \forall x \in A \Rightarrow x \in E\}$.

Conjunto imagen. El conjunto imagen está integrado por todos aquellos elementos del conjunto de llegada que son transformados (les llega una correspondencia) de un elemento del conjunto inicial. $\mathrm{Im}(f) = \{y \in B / \exists x \in A \quad y = f(x)\}$.

Aplicación inyectiva: $f \quad inyectivo \Leftrightarrow \begin{cases} x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \\ \vee \\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \end{cases}$

Aplicación sobreyectiva: $f\ sobreyectiva \Leftrightarrow \forall y \in B\ \exists x \in A / f(x) = y$.

Aplicación biyectiva: Una aplicación es llamada biyectiva cuando ésta es inyectiva y sobreyectiva simultáneamente.

(G,*) es grupo si cumple:

- **Ley interna**: $\forall a, b \in G \quad a * b = c \in G$
- **Axioma 1**: Asociativa: $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$
- **Axioma 2**: Neutro: $\forall a \in G \quad \exists! e \in G \quad / \quad a * e = e * a = a$
- **Axioma 3**: Simétrico: $\forall a \in G \quad \exists a' \in G \quad / \quad a * a' = a' * a = e$