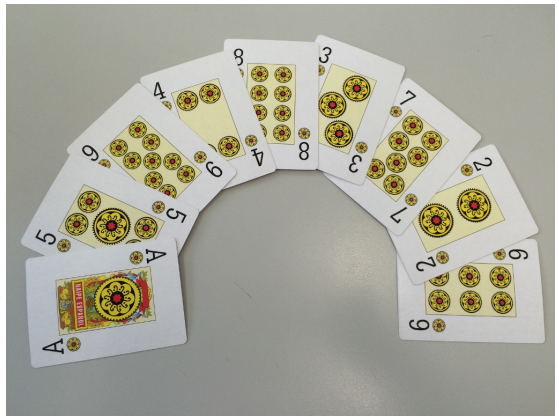
Tema 2: Introducción a la teoría de grupos

Miguel Ángel Olalla Acosta
miguelolalla@us.es

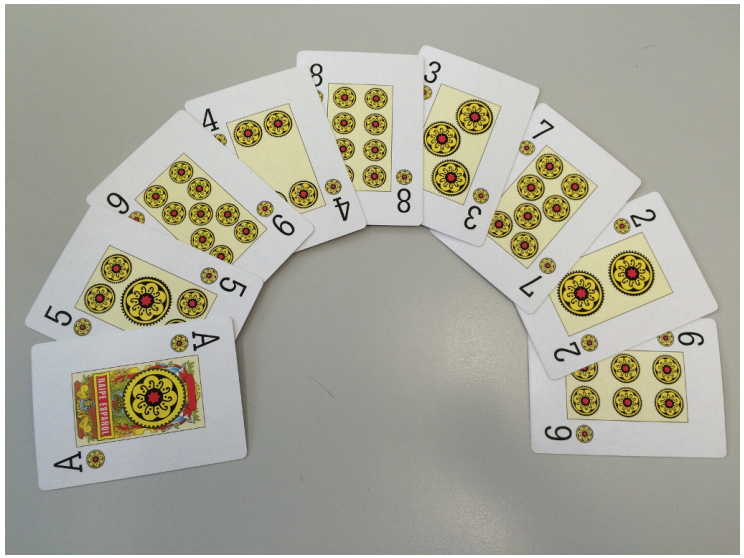
Departamento de Álgebra
Universidad de Sevilla

Octubre de 2017



Contenido

Permutaciones de un conjunto



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 6 & 4 & 2 & 9 & 7 & 5 & 3 \end{pmatrix}$$

Permutaciones de un conjunto

Definición (Permutación de un conjunto)

Sea X un conjunto, se llama permutación de X *a cualquier aplicación biyectiva $\sigma : X \to X$.*

Nota

El conjunto de todas las permutaciones de un conjunto X se denota por

$$\mathrm{Sim}(X).$$

Propiedades

Proposición (2.1.1)

Sea X un conjunto, se verifican las siguientes propiedades:

1. *La composición de dos permutaciones cualesquiera de X es también una permutación de X.*
2. *La aplicación identidad en X es una permutación de X.*
3. *La inversa de cualquier permutación de X es también una permutación de X.*
4. *La composición de permutaciones verifica la propiedad asociativa.*

Operación binaria

Definición (Operación binaria)

Una aplicación de $G \times G$ en G tal que a cada par ordenado $(a, b) \in G \times G$ le asocia un único elemento $a \star b$ de G se denomina **operación binaria.**

Grupo

Definición (Grupo)

Un grupo es un par $(G, \star)$, donde G es un conjunto y $\star$ es una operación binaria sobre G verificando las siguentes propiedades:

1. *La operación es asociativa.*
2. *La operación tiene elemento neutro. Es decir,*

$$\exists e \in G \text{ tal que } \forall x \in G,\ x \star e = e \star x = x.$$

3. *Cada elemento de G posee un simétrico. Es decir,*

$$\forall x \in G\ \exists x^{-1} \in G \text{ tal que } x \star x^{-1} = x^{-1} \star x = e.$$

El Grupo Simétrico

Teorema (El grupo simétrico)

El conjunto $\mathrm{Sim}(X)$ *de las permutaciones de un conjunto* X*, junto con la composición de permutaciones, es un grupo.*

Ejemplos

Ejemplo (2.1.2)

Algunos grupos bien conocidos

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *y* $\mathbb{C}$ *son grupos con la suma.*
2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ *y* $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ *son grupos con la multiplicación.*
3. *El conjunto* $\{-1, 1\}$ *con el producto es un grupo con dos elementos.*
4. *El conjunto de las matrices* $n \times n$*, con elementos en un cuerpo* k *y determinante no nulo,* $GL(n, k)$*, es un grupo con la multiplicación de matrices.*
5. *Las simetrías de un polígono regular junto con la operación composición es un grupo.*

Propiedades

Proposición (2.1.3)

El elemento neutro de un grupo $(G, \star)$ es único.

Proposición (2.1.4)

En un grupo $(G, \star)$, el simétrico de un elemento $x \in G$ es único.

Proposición (2.1.5)

Si x, y son elementos de un grupo $(G, \star)$ tales que $x \star y = e$, entonces $y = x^{-1}$ y $x = y^{-1}$.

Propiedades

La composición de permutaciones **no verifica la propiedad conmutativa**.

Ejemplo (2.1.6)

Sea $X = \{1, 2, 3\}$ *y sean las permutaciones de* X

$$\sigma: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ y } \tau: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Entonces las composiciones de σ *y* τ *son*

$$\tau \circ \sigma: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ y } \sigma \circ \tau: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

De este ejemplo concluimos que si X *tiene al menos tres elementos el grupo* $Sim(X)$ *no es conmutativo.*

Grupo abeliano

Definición

Grupo abeliano Dado un grupo G, si la operación de grupo es conmutativa entonces se dice que el grupo es **abeliano** *o* **conmutativo**.

Soporte

Definición

Sean X un conjunto y σ una permutación de $\mathrm{Sim}(X)$. *Llamamos* **soporte** *de σ al conjunto*

$$\mathrm{sop}(\sigma) = \{x \in X \mid \sigma(x) \neq x\}.$$

Ciclos y trasposiciones

Definición (Ciclos y trasposiciones)

Se dice que $\sigma \in \mathrm{Sim}(X)$ *es un* **ciclo de longitud** 0, *o un* 0-**ciclo**, *si es la identidad.*
Se dice que $\sigma \in \mathrm{Sim}(X)$ *es un* **ciclo de longitud** r, *o un* r-**ciclo** *(con* $r \geq 2$*), si su soporte es un conjunto finito de* r *elementos*

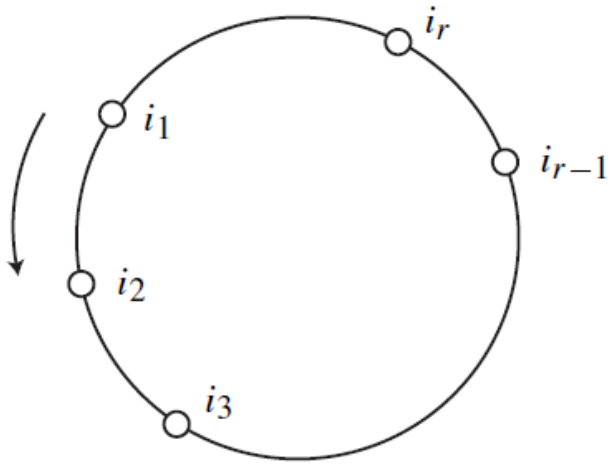
$$\mathrm{sop}(\sigma) = \{i_1, i_2, \ldots, i_r\}$$

donde $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots$, $\sigma(i_{r-1}) = i_r$ *y* $\sigma(i_r) = i_1$.
Decimos que $\sigma \in \mathrm{Sim}(X)$ *es una* **trasposición** *si es un ciclo de longitud 2.*

Notación

Nota (2.2.1)

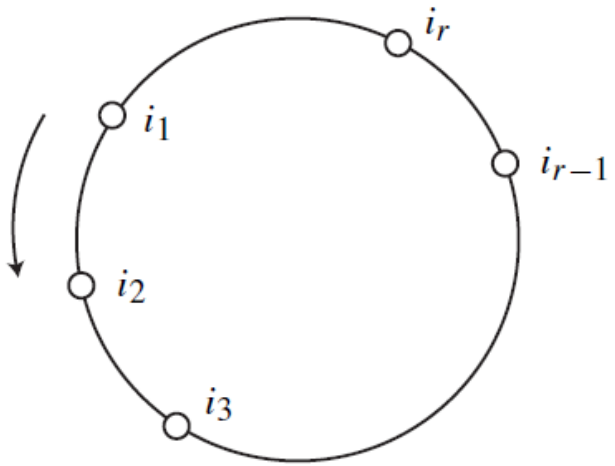
Sea $\sigma \in \mathrm{Sim}(X)$ *un ciclo tal que* $\mathrm{sop}(\sigma) = \{i_1, i_2, \ldots, i_r\}$ *donde* $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots$, $\sigma(i_r) = i_1$.



En este caso el ciclo de escribirá $\sigma = (i_1 i_2 \ldots i_r)$, *sabiendo que si* $x \in X$ *no aparece en la lista entonces* $\sigma(x) = x$.
Siguiendo esta notación podemos escribir el ciclo identidad como $1_X = ()$.

Notación

Nota (2.2.1)



Obsérvese que con esta notación tenemos diferentes representaciones de un mismo ciclo:

$$\sigma = (i_1 i_2 \dots i_r) = (i_2 i_3 \dots i_r i_1) = \cdots = (i_r i_1 \dots i_{r-1}).$$

Ejemplos

Ejemplo (2.2.2)

Veamos algunos ejemplos:

1. *La permutación del conjunto* $\{1,2,3,4,5\}$ *definida por*

$$\sigma: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

   es el 3*-ciclo* $(1\ 2\ 5)$*.*

2. *La permutación del conjunto* $\{1,2,3,4,5,6,7,8\}$ *definida por*

$$\sigma: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 5 & 8 & 7 & 2 & 3 & 4 \end{pmatrix}$$

   no es un ciclo. Sin embargo $\tau = (1\ 6\ 2) \circ (3\ 5\ 7) \circ (4\ 8)$ *es composición de ciclos.*

Notación por yuxtaposición

Nota (2.2.3)

En adelante, siempre que no haya posibilidad de equívoco, prescindiremos en un grupo $(G, \star)$ del símbolo "$\star$" para la operación de dos (o más) elementos. Escribiremos por yuxtaposición xy en lugar de $x \star y$.

En particular, en el caso de permutaciones, escribiremos $\tau\sigma$ en lugar de $\tau \circ \sigma$.

Permutaciones disjuntas

Definición (Permutaciones disjuntas)

Dos permutaciones $\sigma, \tau \in \mathrm{Sim}(X)$ se dicen disjuntas si sus soportes son disjuntos.

Teorema (Permutaciones disjuntas y conmutatividad)

Si $\sigma, \tau \in \mathrm{Sim}(X)$ son permutaciones disjuntas entonces

$$\tau\sigma = \sigma\tau.$$

Ejemplo

Hay permutaciones no disjuntas que sí conmutan.

Ejemplo (2.2.4)

Sea $X = \{1, 2, 3, 4, 5\}$ *y sean las permutaciones de* $\mathrm{Sim}(X)$

$$\sigma: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \text{ y } \tau: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Ambas permutaciones no son disjuntas, pues $\mathrm{sop}(\sigma) \cap \mathrm{sop}(\tau) = \{1, 3, 5\}$. *Sin embargo, no es difícil comprobar que*

$$\tau\sigma = \sigma\tau: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

Notación. Potencia de un elemento

Nota (2.2.5)

De igual manera que se usa la yuxtaposición, xy, para expresar la operación de dos elementos de un grupo $(G, \star)$, es natural definir potencias de elementos de G.
Sean $x \in G$ e i un entero no negativo. La i-ésima potencia de x, x^i, se define mediante la siguiente regla recursiva:

$$x^0 = e,\ x^i = x^{i-1}x.$$

Esta definición la podemos extender a potencias negativas poniendo

$$x^{-i} = (x^{-1})^i.$$

En adelante se usará esta notación también para permutaciones.

Orden de un elemento

Definición (Orden de un elemento)

Sea $(G, \star)$ un grupo.
Diremos que un elemento $x \in G$ tiene **orden finito** *si existe un número entero positivo m tal que $x^m = e$. En este caso, el* **orden de** *x, que denotaremos $o(x)$, es el menor entero positivo que cumple esta propiedad.*

Diremos que $x \in G$ tiene **orden infinito** *si $x^m \neq e$ para todo $m > 0$.*

Elementos de orden infinito

Proposición (2.2.6)

Un elemento $x \in G$ tiene orden infinito si y sólo si todas sus potencias x^k con $k \in \mathbb{Z}$ son distintas.

Orden de un elemento

Proposición (2.2.7)

Sean G un grupo y $x \in G$. Se tienen las siguientes propiedades:

1. $o(x) = 1 \iff x = e$.
2. *Si $x \in G$ tiene orden finito, entonces x^{-1} también y $o(x) = o(x^{-1})$.*
3. *Si $x \in G$ tiene orden infinito, x^{-1} tiene orden infinito.*
4. *Si G es finito, todo elemento de G tiene orden finito.*
5. *Si $o(x) = m$ y $x^n = e$, entonces m es un divisor de n.*
   Dicho de otra forma, las potencias de x iguales a e son exactamente las de la forma x^{km} con $k \in \mathbb{Z}$.

Orden de un ciclo

Proposición (Orden de un ciclo)

El orden de un ciclo de longitud $m \geq 1$ es m.

Expresión en ciclos disjuntos

Teorema (Expresión en ciclos disjuntos)

Toda permutación con soporte finito puede expresarse como producto de ciclos disjuntos, además esta descomposición es única salvo el orden de los ciclos.

Descomposición en ciclos disjuntos

Ejemplo (2.2.8)

En $X = \{1, 2, 3, 4, 5, 6, 7\}$ *consideremos la permutación*

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix}.$$

$$\overline{1} = \{1, 3, 5, 4\} = \overline{3} = \overline{5} = \overline{4} \rightsquigarrow (1354),$$

$$\overline{2} = \{2, 6\} = \overline{6} \rightsquigarrow (26),$$

$$\overline{7} = \{7\} \rightsquigarrow ().$$

Luego $\sigma = (1354)(26)$.

Consecuencias de la descomposición en ciclos disjuntos

Corolario (2.2.9)

Sea X un conjunto con al menos dos elementos. Toda permutación de $\mathrm{Sim}(X)$ *con soporte finito puede expresarse como producto de trasposiciones.*

Corolario (2.2.11)

Toda permutación con soporte finito tiene orden finito.

Orden de un grupo

Definición (Orden de un grupo)

Sea $(G, \star)$ un grupo. Definimos su **orden**, *que notaremos por $|G|$, como el cardinal del conjunto G.*

Nota

Sea el conjunto $X = \{1, 2, \ldots, n\}$, en este caso notaremos al conjunto de las permutaciones de n elementos por S_n.

Teorema (Orden de S_n)

El orden del grupo S_n es $|S_n| = n!$.

Descomposición en ciclos disjuntos y trasposiciones

Teorema (Descomposición en ciclos disjuntos y trasposiciones)

Toda permutación de S_n se descompone de manera única, salvo orden, como producto conmutativo de ciclos disjuntos. Además toda permutación de S_n se puede expresar como producto de trasposiciones, esta vez **no** *de manera única.*

Inversiones en una permutación

Definición (Inversiones en una permutación)

Se dice que un par (i, j) *es una* **inversión** *de* $\sigma \in S_n$, *si*

$$i < j \qquad y \qquad \sigma(i) > \sigma(j).$$

Signo de una permutación

Definición (Signo de una permutación)

Si $\sigma \in S_n$ tiene un número par de inversiones, diremos que σ es **par**, *y que* $\text{signo}(\sigma) = 1$.

Si $\sigma \in S_n$ tiene un número impar de inversiones, diremos que σ es **impar**, *y que* $\text{signo}(\sigma) = -1$.

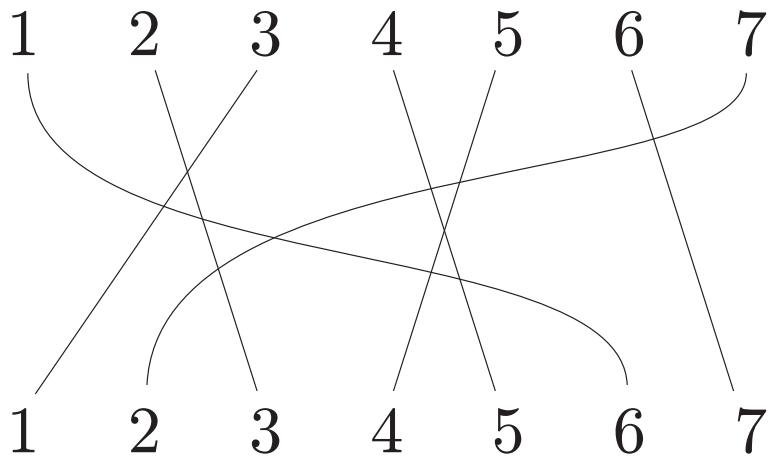
Contando inversiones

Ejemplo (2.2.15)

¿Es la permutación

$$\sigma: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 1 & 5 & 4 & 7 & 2 \end{pmatrix}$$

par o impar?

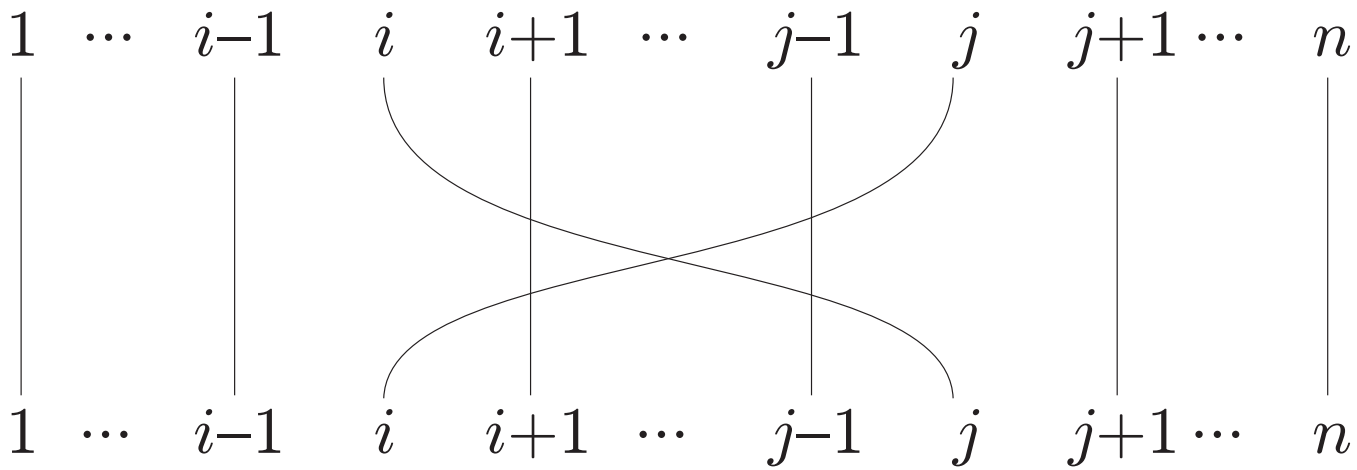


Hay 11 inversiones, luego signo$(\sigma) = -1$ y σ es una permutación impar.

Signo de una trasposición

Proposición (2.2.16)

Las trasposiciones son siempre impares.



Propiedades de signo

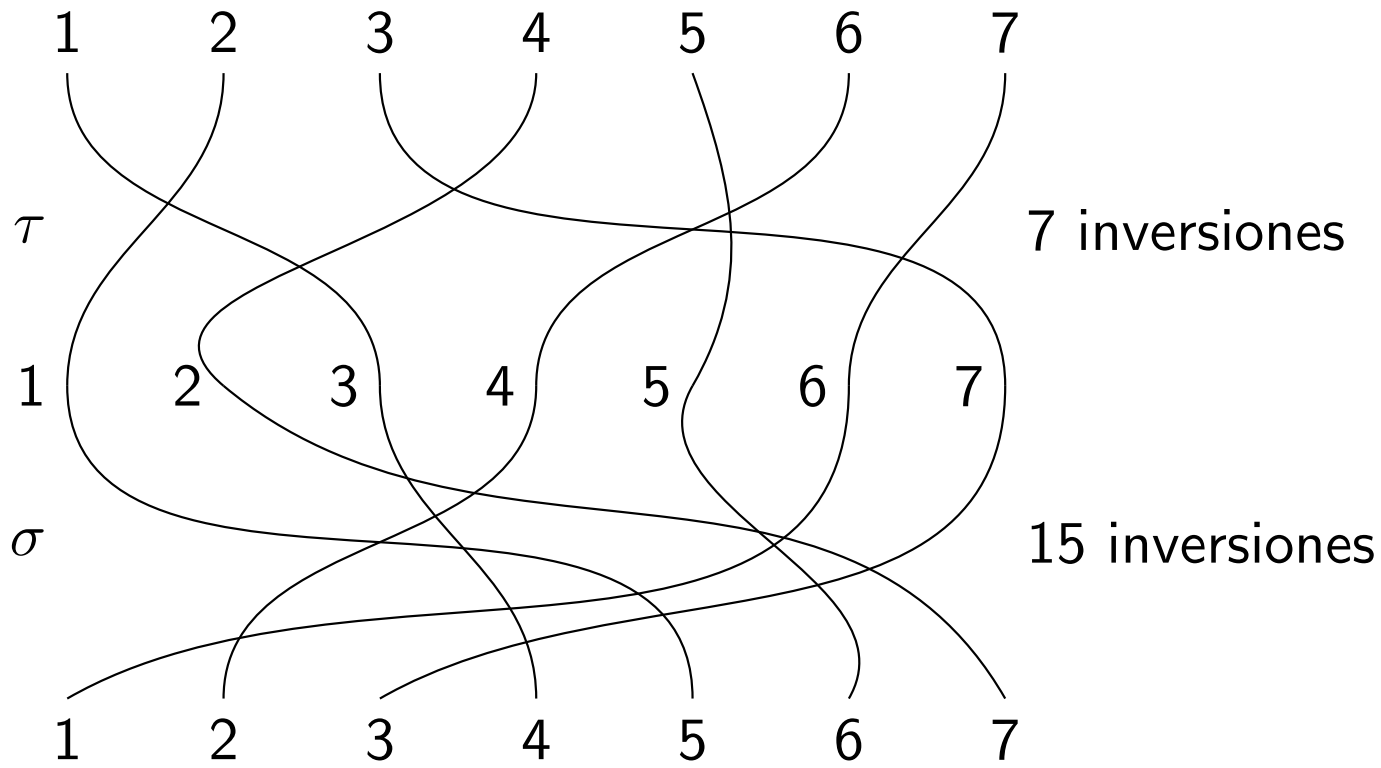
Proposición (2.2.17)

Sean $\sigma, \tau \in S_n$. Se satisfacen las siguientes propiedades:

1. $\text{signo}(\sigma\tau) = \text{signo}(\sigma)\,\text{signo}(\tau)$.
2. $\text{signo}(\sigma^{-1}) = \text{signo}(\sigma)$.

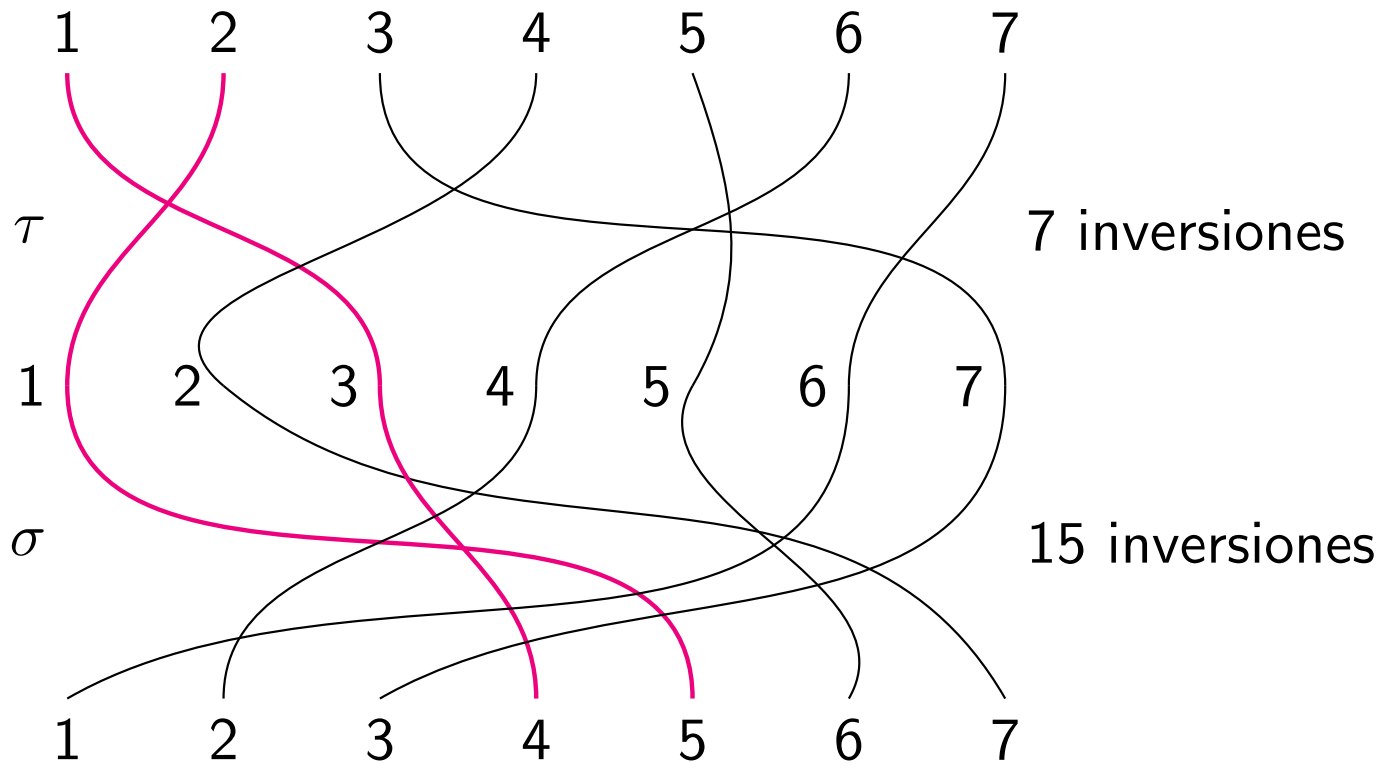
Signo del producto

Sean $\tau = (1\ 3\ 7\ 6\ 4\ 2)$ y $\sigma = (1\ 5\ 6)(2\ 7\ 3\ 4)$ permutaciones de S_7.
Entonces $\sigma\tau$ es:



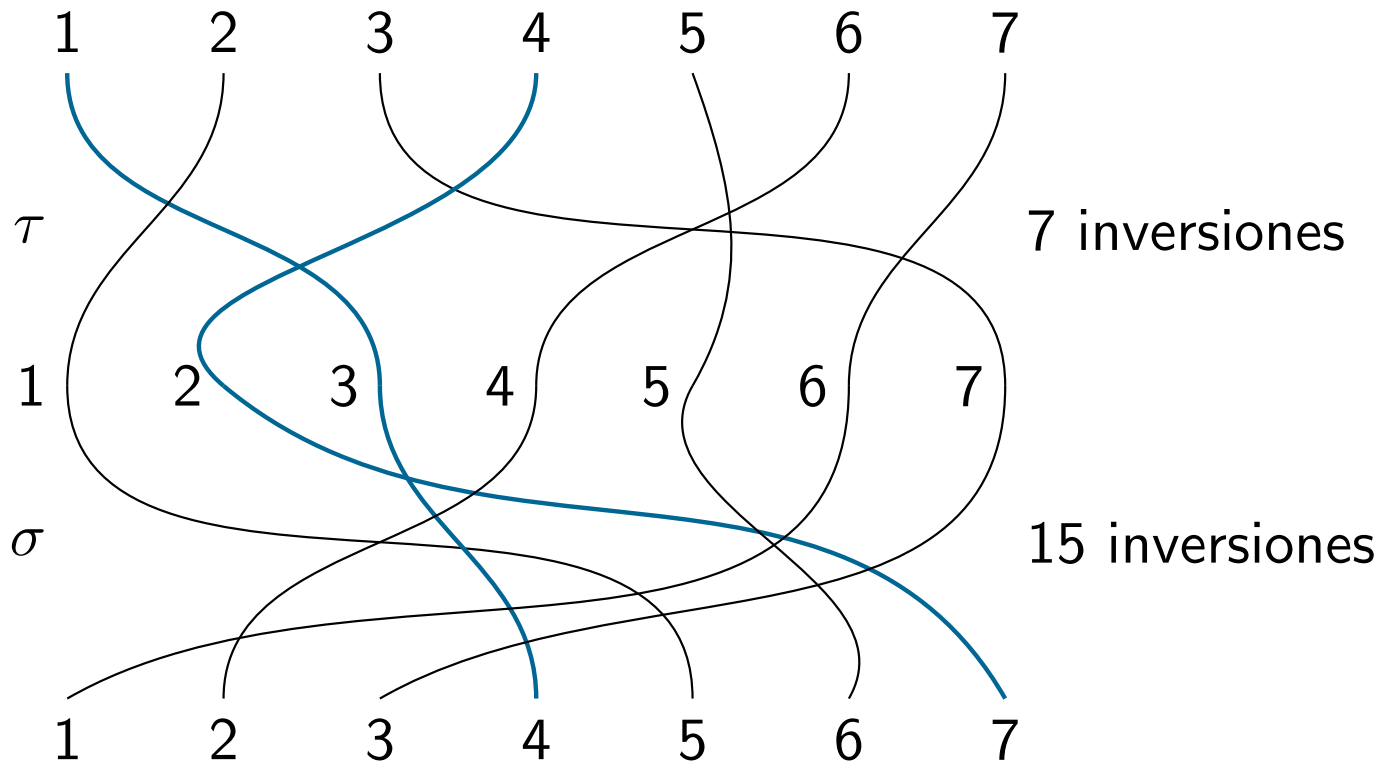
Signo del producto

Sean $\tau = (1\ 3\ 7\ 6\ 4\ 2)$ y $\sigma = (1\ 5\ 6)(2\ 7\ 3\ 4)$ permutaciones de S_7.
Entonces $\sigma\tau$ es:



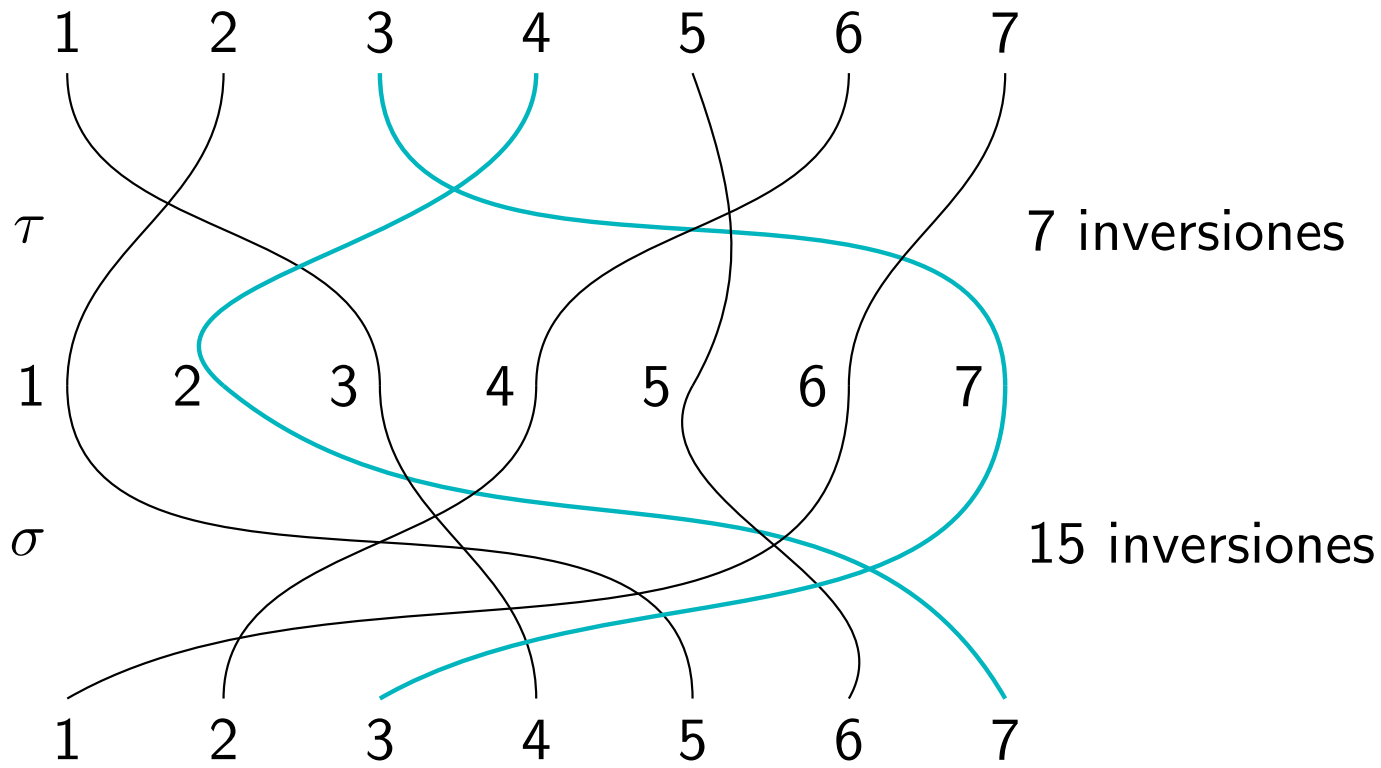
Signo del producto

Sean $\tau = (1\ 3\ 7\ 6\ 4\ 2)$ y $\sigma = (1\ 5\ 6)(2\ 7\ 3\ 4)$ permutaciones de S_7.
Entonces $\sigma\tau$ es:



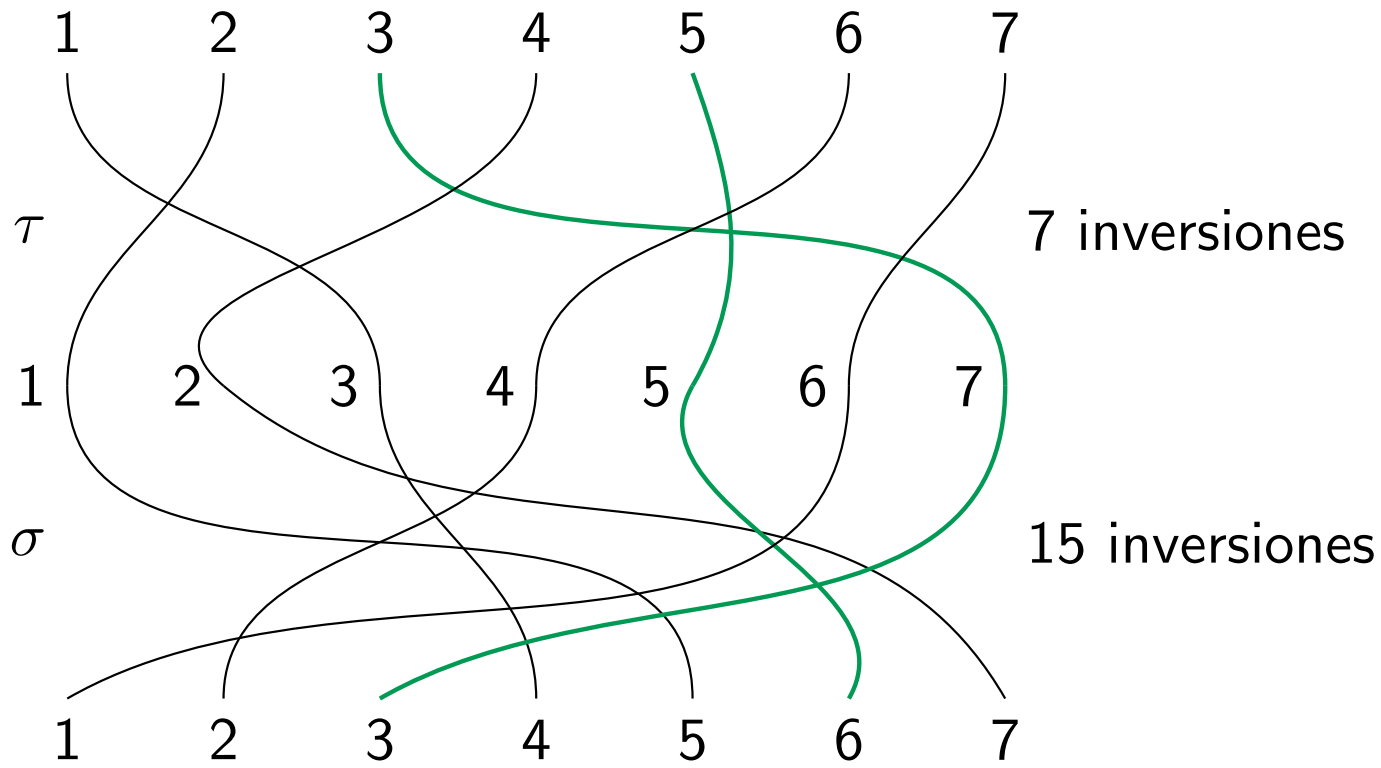
Signo del producto

Sean $\tau = (1\ 3\ 7\ 6\ 4\ 2)$ y $\sigma = (1\ 5\ 6)(2\ 7\ 3\ 4)$ permutaciones de S_7.
Entonces $\sigma\tau$ es:



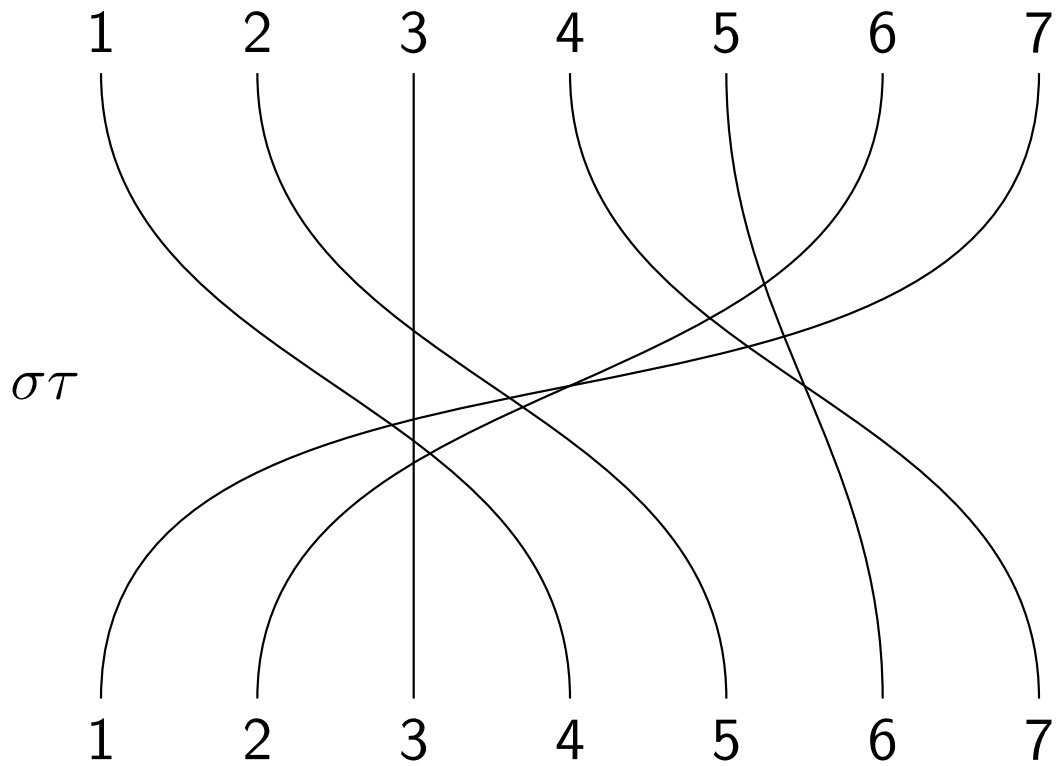
Signo del producto

Sean $\tau = (1\ 3\ 7\ 6\ 4\ 2)$ y $\sigma = (1\ 5\ 6)(2\ 7\ 3\ 4)$ permutaciones de S_7.
Entonces $\sigma\tau$ es:



Signo del producto

Sean $\tau = (1\ 3\ 7\ 6\ 4\ 2)$ y $\sigma = (1\ 5\ 6)(2\ 7\ 3\ 4)$ permutaciones de S_7.
Entonces $\sigma\tau$ es:



$22 - 2 \cdot 4 = 14$ inversiones

Trasposiciones y signo

Corolario (2.2.18)

Una permutación $\sigma \in S_n$ es par (impar) si y sólo si es producto de un número par (impar) de trasposiciones.

Fórmula de Cauchy

Teorema (Fórmula de Cauchy)

Sea $\sigma \in S_n$ el producto de c ciclos disjuntos entonces

$$\text{signo}(\sigma) = (-1)^{m-c},$$

siendo $m = \#(\text{sop}(\sigma))$ el número de elementos del soporte de σ.

Nota (2.2.19)

En particular, el signo de un ciclo de longitud m es $(-1)^{m-1}$. Luego la paridad del ciclo está cambiada respecto de su longitud: **un ciclo de longitud par es impar y un ciclo de longitud impar es par**.

Subgrupo

Definición (Subgrupo)

Sea $(G, \star)$ un grupo. Un subconjunto H de G se dice que es un **subgrupo** *de $(G, \star)$ si $(H, \star)$ es un grupo. Es decir, si el conjunto H, y la operación definida en G, cumplen las propiedades de la definición de grupo.*

Un subgrupo es, por tanto, un grupo dentro de otro grupo con la misma operación.

Ejemplos

Ejemplo (2.3.1)

Vimos que los conjuntos de números $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *y* $\mathbb{C}$ *son grupos abelianos con la suma. De hecho es una cadena de subgrupos* $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Lo mismo ocurre con los grupos $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ *y* $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ *con la multiplicación. Es también una cadena de subgrupos* $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.

Sabemos que $GL(n, k)$, *el conjunto de las matrices invertibles* $n \times n$ *con elementos en un cuerpo* k, *es un grupo con la multiplicación de matrices. Sea* $SL(n, k)$ *el subconjunto de* $GL(n, k)$ *formado por las matrices con determinante igual a* 1. *Comprobamos que* $SL(n, k)$ *es un subgrupo de* $GL(n, k)$.

Ejemplos

Ejemplo (2.3.1)

El subconjunto de S_4, $C = \{(), (1234), (13)(24), (1432)\}$, es un subgrupo con la composición de permutaciones. Veamos la tabla de multiplicar de los elementos de C:

$\circ$	$()$	(1234)	$(13)(24)$	(1432)
$()$	$()$	(1234)	$(13)(24)$	(1432)
(1234)	(1234)	$(13)(24)$	(1432)	$()$
$(13)(24)$	$(13)(24)$	(1432)	$()$	(1234)
(1432)	(1432)	$()$	(1234)	$(13)(24)$

Se da así la circunstancia de que un subgrupo de un grupo no conmutativo, como S_4, puede ser conmutativo.

Subgrupos

Nota (2.3.2)

Si G es un grupo y $H \subset G$ es finito, para comprobar que es subgrupo es suficiente hacer la tabla de multiplicar y razonar como en el ejemplo anterior.

Si H es infinito hay que demostrar que la operación es interna entre elementos de H, que el elemento neutro pertenece a H y que el simétrico de cada elemento de H está también en H.

En cualquier caso, la propiedad asociativa se "hereda" de G.

Subgrupos

El siguiente resultado nos permite "ahorrarnos" verificar alguna propiedad a la hora de demostrar que un subconjunto es subgrupo.

Proposición (2.3.3)

Sean $(G, \star)$ un grupo y $H \subset G$ un subconjunto **no vacío**. *Las condiciones siguientes son equivalentes:*

1. *H es un subgrupo de $(G, \star)$.*
2. *H es no vacío y se satisface la siguiente propiedad*

$$\forall x, y \in H, xy^{-1} \in H.$$

El grupo alternado

Teorema (El grupo alternado A_n)

El conjunto A_n de las permutaciones pares de S_n es un subgrupo llamado **grupo alternado**.

El grupo alternado

Lema

Sean $(G, \star)$ un grupo y $A \subset G$ un subconjunto. Entonces para todo $x \in G$ los conjuntos A y $xA = \{xa \mid a \in A\}$ son equipotentes.

Proposición (2.3.5)

Sea $H \in S_n$ un subgrupo que tiene alguna permutación impar, entonces H posee tantas permutaciones pares como impares.

Corolario (2.3.6)

Si $n \geq 2$, el número de elementos de A_n es $|A_n| = n!/2$, es decir, hay tantas permutaciones pares como impares.

Subgrupo generado

Teorema (Subgrupo generado)

Sean $(G, \star)$ un grupo y $A \subset G$ un subconjunto no vacío. Sea $A^{-1} = \{x^{-1} \in G \mid x \in A\}$ el conjunto de los elementos simétricos a los de A. Entonces el conjunto que se obtiene al operar sucesiones arbitrarias de elementos de A y A^{-1},

$$\langle A \rangle = \{x_1 \star \cdots \star x_n \mid x_i \in A \cup A^{-1}, n \geq 1\},$$

es un subgrupo de G llamado **subgrupo generado por** *A.*

Subgrupo generado

Ejemplo (2.3.7)

En el grupo S_4 calcular todos los elementos del subgrupo $H = \langle (124), (12) \rangle$. Hay que ir operando los elementos (124), (12) y sus inversos, adjuntando a la lista los nuevos elementos que se obtengan.

$\circ$	$()$	(124)	(12)	(142)	(14)	(24)
$()$	$()$	(124)	(12)	(142)	(14)	(24)
(124)	(124)	(142)	(14)	$()$	(24)	(12)
(12)	(12)	(24)	$()$	(14)	(142)	(124)
(142)	(142)	$()$	(24)	(124)	(12)	(14)
(14)	(14)	(12)	(124)	(24)	$()$	(142)
(24)	(24)	(14)	(142)	(12)	(124)	$()$

En este caso $H = \{(), (124), (142), (12), (14), (24)\}$.

Grupo cíclico

Definición (Grupo cíclico)

Se dice que un grupo G es **cíclico** *si existe $a \in G$ tal que*

$$G = \langle a \rangle = \langle \{a\} \rangle = \{a^m \mid m \in \mathbb{Z}\}.$$

Grupo cíclico

Ejemplo (2.3.8)

El grupo S_3 no es cíclico, pues no existe ninguna permutación que genere todo el grupo. El grupo alternado $A_3 = \{(), (123), (132)\}$ es cíclico, pues $A_3 = \langle (123) \rangle = \langle (132) \rangle$.

De hecho, para comprobar si un grupo finito de orden m es o no cíclico, hay que verificar si existe o no en el grupo algún elemento de orden m. En S_3 no hay elementos de orden 6 mientras que en A_3 hay un par de elementos de orden 3.

El grupo de los enteros con la suma, $(\mathbb{Z}, +)$, es cíclico infinito, pues $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Teorema de Lagrange

Proposición

Sean G un grupo y $H \subset G$ un subgrupo. Entonces los conjuntos $xH = \{xh \mid h \in H\}$ para cada $x \in G$ forman una partición de G.

Nota

Notaremos por G/H a la partición anterior. Es decir,

$$\frac{G}{H} = \{xH \mid x \in G\}.$$

Definición (Índice de un subgrupo)

Dado un grupo G y un subgrupo $H \subset G$, el **índice** *de H en G, denotado $|G : H|$, es el número de elementos de G/H. Es decir:*

$$|G : H| = \#(G/H)$$

Teorema de Lagrange

Teorema (Teorema de Lagrange)

Sea G un grupo finito, $H \subset G$ un subgrupo. Entonces $|H|$ divide a $|G|$.

Teorema (Índice de un subgrupo en un grupo finito)

Si G es un grupo finito y $H \subset G$ es un subgrupo, entonces

$$|G : H| = \frac{|G|}{|H|}$$

Teorema de Lagrange

Corolario (2.3.14)

Sea G un grupo finito y sea $x \in G$, entonces el orden de x divide al orden de G.

Corolario (2.3.15)

Si G es un grupo de orden un número primo, entonces G es cíclico.

Una relación de equivalencia

Observación

Dados un grupo G y un subgrupo $H \subset G$, hemos visto que los conjuntos xH, con $x \in G$, forman una partición de G. Esto nos permite definir una relación de equivalencia.

Definición (2.3.9)

Sean G un grupo y $H \subset G$ un subgrupo. Sobre G definimos la relación de equivalencia $\sim_H$ de la manera siguiente: Dados $x, y \in G$,

$$x \sim_H y \Leftrightarrow xH = yH.$$

Observación

Obsérvese que

$$xH = yH \Leftrightarrow x^{-1}y \in H.$$

Una relación de equivalencia

Nota (2.3.11)

Lo usual es notar al conjunto cociente de G por la relación de equivalencia $\sim_H$ como

$$\frac{G}{H} := \frac{G}{\sim_H}.$$

Clases a izquierda y a derecha

Nota (2.3.13)

Las clases de equivalencia para $\sim_H$*, de la forma* xH*, se llaman* clases a izquierda. *Observemos que podríamos haber definido otra relación de equivalencia* ${}_H\sim$ *de la siguiente forma:*

$$x\ {}_H\sim y \Leftrightarrow Hx = Hy \Leftrightarrow yx^{-1} \in H.$$

En este caso las clases de equivalencia son de la forma Hx*, con* $x \in G$*, y se llaman* clases a derecha. *En principio, las clases a izquierda no tienen por qué coincidir con las clases a la derecha (salvo en el caso evidente* $1H = H1 = H$*). Cuando coinciden, se dice que el grupo* H *es* **normal**: *esto se estudiará al final de este tema.*

Homomorfismos de grupos

Definición (Homomorfismo de grupos)

Dados dos grupos $(G, \star)$ *y* $(H, *)$, *un* **homomorfismo**

$$f : (G, \star) \longrightarrow (H, *)$$

es una aplicación $f : G \to H$ *que sastisface*

$$f(x_1 \star x_2) = f(x_1) * f(x_2), \qquad \forall x_1, x_2 \in G.$$

Notación

Nota (2.4.1)

Seguiremos usando la yuxtaposición para expresar la operación entre dos elementos. Aunque ahora intervienen dos grupos con operaciones que pueden ser distintas, normalmente por el contexto sabremos si los elementos que intervienen están en el primer grupo o en el segundo. Así, escribiremos por ejemplo

$$f(x_1x_2) = f(x_1)f(x_2), \qquad \forall x_1, x_2 \in G.$$

Igualmente se notará por e tanto al elemento neutro de G como al de H. Si hiciera falta distinguir, para evitar confusiones, se usará e_G y e_H respectivamente.

Ejemplos de homomorfismos

1.- La *identidad*, $1_G : (G, \star) \to (G, \star)$.

2.- La inclusión de un subgrupo $K \subset G$, $i : (K, \star) \to (G, \star)$.

3.- El signo de una permutación, signo: $S_n \to \{\pm 1\}$.

4.- La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ definida como $f(x) = n \cdot x$ es un homomorfismo $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ para todo entero n.

5.- Si $(G, *)$ es un grupo abeliano, la exponenciación $f : G \to G$, definida como $f(x) = x^n$ es un homomorfismo $f : (G, *) \to (G, *)$ para todo entero n.

Ejemplos de homomorfismos

6.- Si $\mathrm{GL}(n,\mathbb{R})$ es el grupo de matrices invertibles $n \times n$ de números reales, el determinante $\det\colon \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}\setminus\{0\}$ es un homomorfismo respecto de la multiplicación en ambos lados.

7.- La aplicación exponencial $f\colon \mathbb{R} \to (0,+\infty)$, $f(x) = e^x$, es un homomorfismo $f\colon (\mathbb{R},+) \to ((0,+\infty),\cdot)$.

8.- Dado un grupo $(G,\star)$ y un elemento $x \in G$, la aplicación $c_x\colon G \to G$ dada por $c_x(y) = x^{-1}yx$ es un homomorfismo, llamado *conjugación por* x.

Ejemplos de aplicaciones que no son homomorfismos

1.- Si $(G, *)$ no es abeliano, la exponenciación $f : G \to G$ definida en el anterior punto 5 no es un homomorfismo, al menos para $n = 2$.

2.- La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ definida como $f(x) = x^n$ no es un homomorfismo $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ para ningún $n \geq 2$.

Propiedades

Proposición (2.4.3)

Si $f : (G, \star) \to (H, *)$ *es un homomorfismo,*

$$f(e) = e, \qquad f(x^{-1}) = f(x)^{-1}, \quad \forall x \in G.$$

Es decir, los homomorfismos preservan el elemento neutro y los simétricos.

Proposición (2.4.4)

Dados tres grupos y dos homomorfismos como en el siguiente diagrama,

$$(G, \star) \xrightarrow{f} (H, *) \xrightarrow{g} (K, \bullet),$$

la composición

$$g \circ f : (G, \star) \longrightarrow (K, \bullet)$$

también es un homomorfismo.

Monomorfismos, epimorfismos e isomorfismos

Definición (Monomorfismos, epimorfismos e isomorfismos)

Decimos que un homomorfismo $f : (G, \star) \to (H, *)$ *es un* **monomorfismo**, **epimorfismo** *o* **isomorfismo** *si la aplicación* f *es inyectiva, sobreyectiva o biyectiva, respectivamente. Los isomorfismos se denotan del siguiente modo*

$$f : (G, \star) \xrightarrow{\cong} (H, *).$$

Ejemplo (2.4.5)

De los homomorfismos del Ejemplo anterior, 2 y 4 son monomorfismos, y 3 y 6 son epimorfismos y 1, 7 y 8 son isomorfismos. En general 5 no es un monomorfismo ni un epimorfismo.

Isomorfismos

Proposición (2.4.6)

La composición de dos isomorfismos es un isomorfismo.

Proposición (2.4.7)

Si $f : (G, \star) \to (H, *)$ *es un isomorfismo la aplicación inversa* $f^{-1} : H \to G$ *es un isomorfismo*

$$f^{-1} : (H, *) \longrightarrow (G, \star).$$

Ejemplo (2.4.8)

Los inversos de los isomorfismos 1, 7 y 8 del ejemplo anterior son, respectivamente, $1_G^{-1} = 1_G$, *el isomorfismo* $f^{-1} : ((0, +\infty), \cdot) \to (\mathbb{R}, +)$ *definido por* $f^{-1}(x) = \log(x)$, *y el isomorfismo* $(c_x)^{-1} = c_{x^{-1}}$ *definido por* $c_{x^{-1}}(y) = xyx^{-1}$.

Grupos isomorfos

Definición (Grupos isomorfos)

Dos grupos $(G, \star)$ *y* $(H, *)$ *son* **isomorfos** *si existe un isomorfismo*

$$f : (G, \star) \xrightarrow{\cong} (H, *).$$

Corolario (2.4.9)

La relación de ser isomorfos es de equivalencia.

Núcleo de un homomorfismo

Definición (Núcleo de un homomorfismo)

Dado un homomorfismo $f : (G, \star) \to (H, *)$, *el* **núcleo** *de* f *es*

$$\mathrm{Ker}(f) = \{x \in G \,;\, f(x) = e\} \subset G.$$

Ejemplo (2.4.10)

El núcleo de signo: $S_n \to \{\pm 1\}$ *es el grupo alternado.*

Núcleo e imagen de un homorfismo

Proposición (2.4.11)

Dado un homomorfismo $f : (G, \star) \to (H, *)$*, su núcleo* $(\mathrm{Ker}(f), \star)$ *es un subgrupo de* $(G, \star)$*, y su imagen* $(\mathrm{Im}(f), *)$ *es un subgrupo de* $(H, *)$*.*

Proposición (2.4.12)

Dado un homomorfismo $f : (G, \star) \to (H, *)$*, se tiene:*

1. f *es inyectivo si y sólo si* $\mathrm{Ker}(f) = \{e\}$.
2. f *es sobreyectivo si y sólo si* $\mathrm{Im}(f) = H$.

Subgrupos normales

Dado un grupo $(G, \star)$ y un elemento $x \in G$, recordemos el isomorfismo $c_x : G \to G$ que *conjuga por* x a los elementos de G, es decir, $c_x(y) = x^{-1}yx$ para todo $y \in G$.
Dado un subgrupo $K \subset G$, podemos aplicarle el isomorfismo c_x a todos sus elementos y obtendremos un subgrupo de G (el conjugado de K por x):

$$c_x(K) = x^{-1}Kx = \{x^{-1}yx;\ y \in K\}.$$

El grupo $x^{-1}Kx$ podría ser el propio K, o podría ser distinto. Diremos que K es *normal en* G cuando obtenemos siempre el propio K, sea cual sea el elemento $x \in G$ escogido.

Subgrupos normales

Definición (Subgrupos normales)

Dado un grupo $(G, \star)$ y un subgrupo $K \subset G$, decimos que K es **normal** *en G si*

$$x^{-1}Kx \subset K, \qquad \forall x \in G.$$

Lema (2.5.1)

Si $K \subset G$ es un subgrupo normal, la inclusión de la definición anterior es de hecho una igualdad.

Nota (2.5.2)

Del lema anterior se deduce que un subgrupo K es normal en G si y sólo si $aK = Ka$ para todo $a \in G$. En otras palabras, un subgrupo K es normal en G si y sólo si las clases a izquierda (definidas para K) coinciden con las clases a derecha.

Subgrupos normales

Es importante observar que la igualdad $x^{-1}Kx = K$ no implica que los elementos de K quedan fijos al conjugarlos por x. Lo que queda fijo es el conjunto K, pero sus elementos pueden permutarse. Por tanto, K es normal si y sólo si conjugar K por x corresponde a una *permutación* de K, para todo $x \in G$.
Esta permutación puede ser trivial o no. En el siguiente caso, la permutación sí es trivial para todo x.

Proposición (2.5.3)

Si $(G, \star)$ es abeliano, todo subgrupo $K \subset G$ es normal.

Subgrupos normales

Ejemplo (2.5.4)

Los subgrupos trivial y total $\{e\}, G \subset G$ *son normales en cualquier grupo* G*. El subgrupo* $K = \{1, (1\ 2)\} \subset S_3$ *no es normal puesto que*

$$(1\ 3)^{-1}(1\ 2)(1\ 3) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin K.$$

El núcleo de un homomorfismo es un subgrupo normal...

Proposición (2.5.5)

El núcleo de $f : (G, \star) \to (H, *)$ *es un subgrupo normal de* G*.*

Grupo cociente

Teorema (Grupo cociente)

Si $(G,\star)$ es un grupo y $K \subset G$ es un subgrupo normal entonces el conjunto cociente G/K posee una única estructura de grupo $(G/K,\bar{\star})$ tal que la proyección natural $p\colon G \to G/K$ es un homomorfismo

$$p\colon (G,\star) \longrightarrow (G/K,\bar{\star}).$$

... y todo subgrupo normal es núcleo de un homomorfismo.

Proposición (2.5.6)

El núcleo de la proyección natural $p\colon (G,\star) \to (G/K,\bar{\star})$ es $\operatorname{Ker} p = K$.

La imagen no es un subgrupo normal

Ejemplo (2.5.7)

Si $(G,\star)$ es un grupo y $K \subset G$ es un subgrupo cualquiera, la imagen de la inclusión $i\colon (K,\star) \to (G,\star)$ es $\mathrm{Im}(i) = K$, por tanto la imagen de un homomorfismo en general no es normal en la llegada.

Factorización canónica

Teorema (Factorización canónica)

Todo homomorfismo $f : (G, \star) \to (H, *)$ factoriza como la composición $f = i \circ \bar{f} \circ p$ de un epimorfismo p, un isomorfismo $\bar{f}$ y un monomorfismo i del siguiente modo

$$\begin{array}{ccc} (G, \star) & \xrightarrow{\quad f \quad} & (H, *) \\ \Big\downarrow{\scriptstyle p} & & \Big\uparrow{\scriptstyle i} \\ (G/\operatorname{Ker}(f), \bar{\star}) & \xrightarrow[\bar{f}]{\cong} & (\operatorname{Im}(f), *) \end{array}$$

Aquí p es la proyección natural sobre el cociente e i es la inclusión del subgrupo imagen.

Factorización canónica

Corolario (2.5.8)

Si $f : (G, \star) \to (H, *)$ *es un epimorfismo entonces* $\bar{f} : (G/\operatorname{Ker}(f), \bar{\star}) \to (H, *)$ *es un isomorfismo.*

Corolario (2.5.9)

Si $f : (G, \star) \to (H, *)$ *es un monomorfismo entonces* $\bar{f} : (G, \star) \to (\operatorname{Im}(f), *)$ *es un isomorfismo*

Teorema de Cayley

Teorema (Teorema de Cayley)

Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones. Si el grupo es finito de orden n, entonces es isomorfo a un subgrupo de S_n.