Tema2-AII.pdf

jaliriop

Álgebra II

2º Grado en Matemáticas

Facultad de Ciencias
Universidad de Granada

2 GRUPOS: DEFINICIÓN Y EJEMPLOS

Definición: Un <u>grupo</u> es un par $(G, *)$ donde G es un conjunto no vacío, y $*$ es una ley de composición, es decir, una aplicación binaria

$$* : G \times G \longrightarrow G$$
$$(x,y) \longmapsto x * y$$

verificando los siguientes axiomas:

1) Asociatividad $\quad x*(y*z) = (x*y)*z \quad \forall x,y,z \in G$
2) Existencia de elemento neutro $\quad \exists e \in G \mid e*x = x \quad \forall x \in G$
3) Existencia de elemento simétrico $\quad \forall x \in G \ \exists x' \in G \mid x' * x = e$

Si además se verifica

4) Conmutatividad $\quad x*y = y*x \quad \forall x,y \in G$

tenemos un <u>grupo abeliano</u>

Definición: Se llama <u>orden</u> del grupo $(G, *)$ al cardinal del conjunto G y lo notamos $|G|$. Si $|G|$ es finito, decimos que G es un <u>grupo finito</u>.

Objetivos del curso:

- Clasificar (salvo isomorfismos) todos los grupos abelianos finitos.
- Clasificar (salvo isomorfismos) todos los grupos de orden ≤ 15

24/9/19

Notación: La ley de composición la notaremos por $xy \leftrightarrow x*y$. Notaremos al neutro por $1 \leftrightarrow e$ y al simétrico por $x^{-1} \leftrightarrow x'$ (inverso). Si el grupo es abeliano, notaremos la ley de composición $x+y \leftrightarrow x*y$. En tal caso, el neutro será $0 \leftrightarrow e$ y al simétrico $-x \leftrightarrow x'$ (opuesto)

Definición: En un grupo finito $G = \{x_1, x_2, \dots, x_n\}$ donde $x_1 = 1$ (neutro), la tabla de grupo (o de Cayley) es la matriz cuadrada $n \times n$ que en la entrada (i,j) tiene el producto $x_i x_j$

G	x_1	x_2	$\dots$	x_j	$\dots$	x_n
x_1						
x_2						
$\vdots$						
x_i				$x_i x_j$		
$\vdots$						
x_n						

La matriz es simétrica si, y solo si, el grupo es abeliano.

Ejemplos:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ con $+$ son grupos abelianos
- $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Q}^+$, $\mathbb{R}^+$ con el producto son grupos abelianos
- $\{1, -1, i, -i\} \subseteq \mathbb{C}$ con el producto es un grupo abeliano.
- $\mathcal{M}_2(\mathbb{R})$ con la suma es un grupo abeliano
- $GL_2(\mathbb{R}) = \{\text{matrices invertibles}\}$ es un grupo no abeliano con el producto.
- $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ con la suma es un grupo abeliano
- Cualquier espacio vectorial con la suma es un grupo abeliano
- $U(\mathbb{Z}_n) = \mathbb{Z}_n^{\times} = \{\text{unidades de } \mathbb{Z}_n\} = \{\bar{a} \in \mathbb{Z}_n \mid \exists\, \bar{b} \in \mathbb{Z}_n \text{ con } \bar{a}\bar{b} = 1\} =$
  $= \{\bar{a} \in \mathbb{Z}_n \mid \text{m.c.d.}(a,n) = 1\}$ con el producto, es un grupo
- Dado $n \geq 1$, $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\cos\left(\frac{2k\pi}{n}\right) + i\,\text{sen}\left(\frac{2k\pi}{n}\right),\ k = 0, 1, \dots, n-1\}$ con el producto es un grupo.
- Si $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p primo), entonces $SL_2(k) = \{\text{matrices invertibles de } \det = 1\} \equiv$ grupo lineal especial es un grupo con el producto, pero no abeliano.
- Si G y H son grupos, entonces $G \times H$ con la multiplicación componente a componente $(x,y)(x',y') = (xx', yy')$ es un grupo.

Proposición: Sea G un grupo (usamos yuxtaposición como producto pero mantenemos e como neutro). Se verifican:

i) $\forall x \in G \Rightarrow xx^{-1} = e$

ii) $\forall x \in G \Rightarrow xe = x$

iii) El neutro es único.

iv) El simétrico de cualquier elemento es único

v) Propiedad cancelativa $\Rightarrow \forall x, y, z \in G$ $\quad xy = xz \Rightarrow y = z$ $\quad yx = zx \Rightarrow y = z$

vi) $e^{-1} = e$

vii) $\forall x \in G \quad (x^{-1})^{-1} = x$

viii) $\forall x, y \in G \Rightarrow (xy)^{-1} = y^{-1}x^{-1}$

ix) $\forall x, y \in G \quad \exists$ únicos $u, v \in G$ / $xu = y \wedge vx = y$

Es decir, $\exists$ solución única de las ecuaciones $xX = y$, $Xx = y$.

DEMOSTRACIÓN:

i) $x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1} = e \cdot x^{-1} = x^{-1}$

$e = (x^{-1})^{-1}x^{-1} = (x^{-1})^{-1}\left(x^{-1}(xx^{-1})\right) = \left((x^{-1})^{-1}x^{-1}\right)(xx^{-1}) = e(xx^{-1}) = xx^{-1}$

ii) $xe = x(x^{-1}x) = (xx^{-1})x = ex = x$

iii) Supongamos que e y e' son neutros $\Rightarrow e = ee' = e'$

iv) Si x' y x^{-1} son inversos de x, entonces

$x' = x'e = x'(xx^{-1}) = (x'x)x^{-1} = ex^{-1} = x^{-1}$

v) Si $xy = xz$

$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$

vi) $ee = e \Rightarrow e = e^{-1}$

vii) $xx^{-1} = e \Rightarrow x = (x^{-1})^{-1}$

viii) $(y^{-1}x^{-1})(xy) = \left((y^{-1}x^{-1})x\right)y = \left(y^{-1}(x^{-1}x)\right)y = (y^{-1}e)y = y^{-1}y = e$

$\Rightarrow (xy)^{-1} = y^{-1}x^{-1}$

ix) $u = x^{-1}y$, $v = yx^{-1}$ son soluciones

Observación: Si $x_1, x_2, \dots, x_n \in G$, definimos $\prod_{i=1}^{n} x_i = x_1 x_2 \dots x_n$ recurrentemente

$x_1x_2x_3 = (x_1x_2)x_3 \Rightarrow \prod_{i=1}^{n} x_i = \left(\prod_{i=1}^{n-1} x_i\right) x_n$

Proposición: Sean $x_1, x_2, \dots, x_m, \dots, x_n \in G$. Entonces

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{m} x_i \prod_{i=m+1}^{n} x_i$$

DEMOSTRACIÓN: Inducción:

$x_1x_2x_3 = (x_1x_2)x_3 = x_1(x_2x_3)$

$x_1x_2\dots x_n \begin{cases} m = n-1 & x_1x_2\dots x_n = (x_1\dots x_{n-1})x_n \\ m < n-1 & x_1x_2\dots x_n = (x_1x_2\dots x_{n-1})x_n = \end{cases}$

$= \left((x_1\dots x_m)(x_{m+1}\dots x_{n-1})\right)x_n =$

$= (x_1\dots x_m)\left((x_{m+1}\dots x_{n-1})x_n\right) =$

$= (x_1\dots x_m)(x_{m+1}\dots x_n)$

En particular, podemos considerar p/c potencia n-ésima de x con $n>0$ como $x^n = \underbrace{x \dots x}_{n \text{ veces}}$

Extendemos a $\mathbb{Z}$

$$x^n = \begin{cases} x^n & n>0 \\ 1 & n=0 \\ (x^{-1})^n & n<0 \end{cases}$$

Se verifican, por tanto, $x^n x^m = x^{n+m}$ y $(x^n)^m = x^{nm}$ $\forall n,m \in \mathbb{Z}$

Con la notación aditiva:

$$nx = \underbrace{x + \dots x + x}_{n \text{ veces}} \longrightarrow nx = \begin{cases} nx & n>0 \\ 0 & n=0 \\ (-n)(-x) & n<0 \end{cases} \quad n \in \mathbb{Z} \quad \begin{array}{l} nx + mx = (n+m)x \\ n(mx) = (nm)x \end{array}$$

Definición: En un grupo G, el orden de un elemento $x \in G$ es el menor entero positivo n (si existe) tal que $x^n = 1$ $(nx = 0)$. Si no existe se dice que el orden de x es ∞. Lo notaremos por $O(x)$

Ejemplos:

- $O(x) = 1 \iff x = 1$
- $\forall x \in \mathbb{Q}, \mathbb{Z}, \mathbb{R}$ $(+)$ $\Rightarrow$ $O(x) = \infty$ si $x \neq 0$
- $\mathbb{R}^*, \mathbb{Q}^*$ (producto) $\Rightarrow$ $O(-1) = 2$, $O(x) = \infty$ $\forall x \neq \pm 1$
- $\mathbb{C}^*$ (producto), $O(i) = 4$
- En $\mathbb{Z}_9$ $(+)$, $O(\bar{6}) = 3$
- En $\mathbb{Z}_7^* = U(\mathbb{Z}_7)$ (producto), $O(\bar{2}) = 3$, $O(\bar{3}) = 6$
- En cualquier grupo G, $O(x) = O(x^{-1})$ $\forall x \in G$.

GRUPOS DIÉDRICOS D_n.

27/9/19

Supongamos $n \geq 3$.

Denotaremos $D_n = \{$ simetrías del polígono regular de n lados $\}$

$\equiv$ movimientos rígidos del plano (isometrías) que llevan el polígono regular en sí mismo.

D_n es un grupo con la composición de movimientos.

Cualquiera de estos movimientos está determinado por 3 puntos no alineados. Entonces numeramos 1, 2 dos vértices adyacentes y 3 el centro del polígono (invariante) luego, el movimiento queda determinado por la imagen de 1 o 2.

$$\left.\begin{array}{l} 1 \longmapsto \{1, 2, \ldots, n\} \\ 2 \longmapsto \text{adyacente a la imagen de } 1 \end{array}\right\} \Rightarrow |D_n| \leq 2n$$

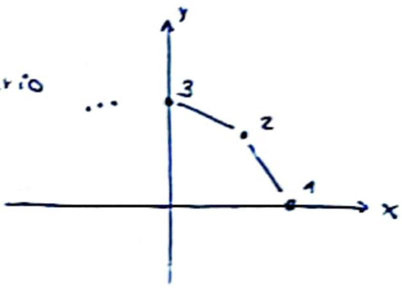
$$\left.\begin{array}{l} * \ r_k \equiv \text{rotación de ángulo } \frac{2k\pi}{n} \quad 0 \leq k \leq n-1 \\ * \ \text{reflexiones en los } n \text{ ejes de simetría del polígono} \end{array}\right\} |D_n| = 2n$$

- • n impar (ejes unen vértices con el punto medio del lado opuesto)
- • n par ($n/2$ ejes unen puntos medios de lados opuestos; $n/2$ ejes unen vértices opuestos)

Notación:

Llamaremos $r \equiv$ rotación en sentido antihorario de ángulo $\frac{2\pi}{n}$

$s \equiv$ reflexión en el eje que une el vértice 1 con el centro.



Entonces se tiene

1. - $1, r, r^2, \ldots, r^{n-1}$ son distintos y $r^n = 1$ $(\Rightarrow O(r) = n)$
2. - $s^2 = 1$ $(\Rightarrow O(s) = 2)$

- $s \neq r^i$ $\forall i \in \{1, \ldots, n-1\}$ (s fija el 1 y r^i no)
- $sr^i \neq sr^j$ $0 \leq i, j \leq n-1,\ i \neq j$ (si $sr^i = sr^j \Rightarrow r^i = r^j$)

  $\{sr^i\}$ reflexiones de orden 2.

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

3. - $sr = r^{-1}s$ $\quad ((sr)^2 = 1 \Rightarrow srsr = 1 \Rightarrow sr = r^{-1}s) \Rightarrow$ No abeliano.

- Por inducción $sr^i = r^{-i}s$
- $\forall$ elemento de D_n tiene una representación única en la forma $s^i r^j$ $\quad i \in \{0, 1\}$, $j \in \{0, \ldots, n-1\}$

- Usando (1), (2) y (6), tenemos que $(s^i r^j)(s^k r^l) = s^u r^w$

Ejemplo: D^{12}

$$(sr^9)(sr^6) = sr^9sr^6 = \underbrace{ss}_{1}\overset{r^3}{r^{-9}}r^6 = r^3r^6 = r^9$$

Definición: Un conjunto de generadores de un grupo G es un subconjunto $S \subseteq G$ tal que todo elemento de G puede escribirse como un producto finito de elementos de S y sus inversos. En tal caso, escribiremos $G = \langle S \rangle$, y diremos que S genera a G o que G está generado por S. ($\forall x \in G$. $x = s_1^{\delta_1} s_2^{\delta_2} \dots s_r^{\delta_r}$, $s_i \in S$ y $\delta_i = \pm 1$)

Si $S = \{x_1, \dots, x_n\}$, entonces $G = \langle S \rangle = \langle x_1, \dots, x_n \rangle$

Si $S = \{x_1\} \rightsquigarrow G = \langle x_1 \rangle$ y diremos que G es un grupo cíclico

Ejemplos:

- $D_n = \langle r, s \rangle$
- $\mathbb{Z} = \langle 1 \rangle$

Definición: Si un grupo G está generado por un subconjunto S y existe un conjunto de relaciones en G (entendiendo por relación una ecuación en los elementos de $S \cup \{1\}$) $R_1, R_2, \dots, R_m$ tal que cualquier otra relación puede deducirse de estas, diremos que S y el conjunto $\{R_1, \dots, R_m\}$ constituyen una presentación de G, y lo denotaremos

$G = \langle S \mid R_1, \dots, R_m \rangle$

Ejemplos:

- $D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ sr = r^{-1}s \rangle$

  $D_3 = \langle r, s \mid r^3 = 1,\ s^2 = 1,\ sr = r^{-1}s \rangle$

  Extensiones sin significado geométrico $\begin{cases} D_1 = \langle s \mid s^2 = 1 \rangle = \{1, s\}\ (\cong \mathbb{Z}_2) \\ D_2 = \langle r, s \mid r^2 = 1,\ s^2 = 1,\ sr = rs \rangle = \{1, r, s, sr\}\ (\cong \mathbb{Z}_2 \times \mathbb{Z}_2) \end{cases}$

- $C_n = \langle x \mid x^n = 1 \rangle = \{1, x, x^2, \dots, x^{n-1}\}\ (\cong \mathbb{Z}_n)$

  grupo cíclico de orden n abstracto

- $V^{abs} = \langle x, y \mid x^2 = 1,\ y^2 = 1,\ xy = yx \rangle = \{1, x, y, xy\}$

  $(\cong D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2)$

  grupo de Klein abstracto.

- $Q_2^{abs} = \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ yx = x^{-1}y \rangle = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$

  grupo abstracto de los cuaternios

  $(\cong$ grupo de matrices de $GL_2(\mathbb{C}))$

  $(\cong Q_2$ cuaternios$)$

$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$

$$\begin{cases} 1 \cdot 1 = 1 \\ 1 \cdot a = a \quad \forall a \in Q_2 \\ (-1)(-1) = 1 \\ (-1) \cdot a = -a \quad \forall a \in Q_2 \\ i^2 = j^2 = k^2 = -1 \\ ij = k \quad jk = i \quad ki = j \\ ji = -k \quad kj = -i \quad ik = -j \end{cases}$$

$\begin{cases} \text{neutro} \\ 1 \text{ elemento de orden } 2 \\ 6 \text{ elementos de orden } 4 \end{cases}$

GRUPOS SIMÉTRICOS S_n.

$X \rightsquigarrow Perm(X) = \{$permutaciones de $X\}$

$X = \{1, 2, \dots, n\} \rightsquigarrow Perm(X) = S_n$. $\qquad |S_n| = n!$

$\sigma \in S_n \rightsquigarrow \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ representación matricial de una permutación.

Dados $\sigma, \tau \in S_n$, en general $\sigma\tau \neq \tau\sigma \Rightarrow$ No abelianos.

Las permutaciones del tipo $a_i \longmapsto a_{i+1}$ las

notaremos $\sigma = (1\ 2\ 3\ 4\ 5) \equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

Estas permutaciones se llaman <u>ciclos</u>. $\qquad$ 30/9/19

Definición: la <u>longitud</u> de un ciclo es el número de elementos que permuta.

Si la longitud de un ciclo σ es t, entonces σ es un <u>t-ciclo</u>. Notaremos la longitud como $\ell(\sigma)$

El orden de un ciclo es su longitud.

Los ciclos de longitud 2 son traspoiciones.

Dos ciclos se dicen disjuntos si los elementos que permutan son disjuntos.

Si $\sigma = (a_1\ a_2 \dots a_m) \Rightarrow \sigma^{-1} = (a_m \dots a_2\ a_1)$

Ejemplo:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix} \in S_{13}$$

$$\overset{\shortparallel}{(1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9)}$$

Es usual no escribir los ciclos de longitud 1.

$\underset{n}{S_n} \ni \sigma$ descompuesto en ciclos $\underset{\substack{\text{no escribiendo} \\ \text{los ciclos de} \\ \text{long} = 1}}{\rightsquigarrow}$ $\sigma \in S_m$ $m \geq n+1$

$n+1 \longmapsto n+1$
$n+2 \longmapsto n+2$
$\dots$

Ejemplo: $(1\ 2)(1\ 3) = (1\ 3\ 2)$
$(1\ 3)(1\ 2) = (1\ 2\ 3)$ $\rightarrow$ S_n no es abeliano $\forall n \geq 3$

Ejemplo: Dado el ejemplo anterior:

$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9\ 6)$

Proposición: Toda permutación $\sigma \in S_n$, $\sigma \neq 1$, se expresa como producto de ciclos disjuntos

$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$ con γ_i disjuntos con $\ell(\gamma_i) \geq 2$

y esta descomposición es única salvo el orden de los factores.

DEMOSTRACIÓN:

Sea $X = \{1, 2, \dots, n\}$ y en X definimos la siguiente relación binaria:

$y, x \in X$ $\quad yRx \Leftrightarrow \exists m \in \mathbb{Z} \mid y = \sigma^m(x)$

R es una relación de equivalencia $\rightsquigarrow X/_R = \{\text{clases de equiv}\}$

Dado $x \in X \Rightarrow C = \{\sigma^m(x) \mid m \in \mathbb{Z}\}$ que es un conjunto finito.

Por ser finito, $\exists r \mid \sigma^r(x) = x$

Sea m el menor entero positivo tal que $\sigma^m(x) = x$

En tal caso $C = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)\}$, que tiene m elementos.

Sea $\gamma = (x \ \ \sigma(x) \ \ \sigma^2(x) \dots \sigma^{m-1}(x))$ de modo que $\gamma(y) = \sigma(y)$ si $y \in C$ y $\gamma(y) = y$ si $y \notin C$

Si $C_1, C_2, \dots, C_k$ son las distintas clases de equivalencia, sea $\gamma_1, \gamma_2, \dots, \gamma_k$ los correspondientes ciclos asociados a cada clase.

Veamos que $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$. (si existiera γ_i tal que $l(\gamma_i) = 1$, lo suprimimos).

Si $y, z \in X$ tales que $\sigma(y) = z \Rightarrow y, z \in C_i \mid \gamma_i(y) = z$

$$\left.\begin{array}{l} \gamma_j(y) = y \\ \gamma_j(z) = z \end{array}\right. \text{ si } j \neq i$$

$$\left.\begin{array}{l} \sigma(y) = z \\ \gamma_1 \gamma_2 \dots \gamma_i \dots \gamma_k(y) = z \end{array}\right\} \sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

Supongamos ahora que $\sigma = \beta_1 \beta_2 \dots \beta_L$ con β_i ciclos disjuntos. Entonces el conjunto de elementos que permuta β_j corresponde exactamente a una cierta clase de equivalencia C_i, y como de estas hay k, entonces $L = k$ y además $\beta_j = \gamma_i$

Luego, salvo el orden, ambas descomposiciones son iguales.

Corolario: El orden de una permutación es el mínimo común múltiplo de las longitudes de los ciclos disjuntos en que descompone.

DEMOSTRACIÓN:

Si $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$ y puesto que al ser disjuntos los ciclos se tiene que $\gamma_i \gamma_j = \gamma_j \gamma_i$, entonces

$$\sigma^n = (\gamma_1 \gamma_2 \dots \gamma_k)^n = \gamma_1^n \gamma_2^n \dots \gamma_k^n$$

Así que $\sigma^n = 1 \iff \gamma_1^n = \gamma_2^n = \dots = \gamma_k^n = 1 \iff n$ es múltiplo común de $O(\gamma_i)$, $i \in \{1, \dots, k\}$

y si $n = O(\sigma)$, entonces $n = \text{m.c.m.}(O(\gamma_1), \dots, O(\gamma_k)) =$

$$= \text{m.c.m.}(l(\gamma_1), \dots, l(\gamma_k)).$$

Definición: $\forall \sigma, \tau \in S_n \Rightarrow \tau \sigma \tau^{-1} \equiv$ conjugado de σ

Proposición: Si γ es un ciclo de longitud n, todo conjugado suyo vuelve a ser un ciclo de longitud n:

$\forall \tau \in S_n \quad \tau\gamma\tau^{-1} \equiv n$-ciclo.

DEMOSTRACIÓN:

Veamos que si $\gamma = (x_1\ x_2 \dots x_n)$, entonces $\forall \tau \in S_n$

$$\tau\gamma\tau^{-1} = (\tau(x_1)\ \ \tau(x_2)\ \dots\ \tau(x_n)).$$

$\forall y \in$ si $\tau^{-1}(y) = x \neq x_i\ \forall i \Rightarrow y \xmapsto{\tau^{-1}} x \xmapsto{\gamma} x \xmapsto{\tau} y$

si $\tau^{-1}(y) = x_i$ para algún $i \Rightarrow \underset{\tau(x_i)}{\overset{\shortparallel}{y}} \xmapsto{\tau^{-1}} x_i \xmapsto{\gamma} x_{i+1} \longmapsto \tau(x_{i+1})$

Ejemplo: $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$

$\tau = (2\ 5\ 3)$

$\tau\sigma\tau^{-1} = (1\ 12\ 8\ 10\ 4)(5\ 13)(3\ 11\ 7)(6\ 9)$

1/10/19

Ejemplo:

S_2 $\{1,2\}$ $\begin{cases} 1 \\ (1\ 2) \end{cases}$

S_3 $\{1,2,3\}$ $\begin{cases} 1 \\ (1\ 2),\ (1\ 3),\ (2\ 3) \\ (1\ 2\ 3),\ (1\ 3\ 2) \end{cases}$

S_4 $\{1,2,3,4\}$ $\begin{cases} 1 & 1 \\ (1\ 2),\ (1\ 3), \dots & 6 \\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4), \dots & 3 \\ (1\ 2\ 3),\ (1\ 3\ 2), \dots & 8 \\ (1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3), \dots & 6 \end{cases}$

Proposición: Cualquier permutación de S_n es producto de trasposiciones.

DEMOSTRACIÓN:

Si γ es cualquier ciclo $(x_1\ x_2 \dots x_m)$ se tiene que $(x_1\ x_2 \dots x_m) = (x_1\ x_m)(x_1\ x_{m-1}) \dots (x_1\ x_3)(x_1\ x_2)$ y entonces basta usar que toda permutación es producto de ciclos disjuntos.

Observación: La descomposición como producto de trasposiciones no es única.

$(x_1\ x_2\ \dots\ x_m) = (x_1\ x_2)\dots(x_{m-1}\ x_m) = (x_1\ x_m)\dots(x_1\ x_2)$

Sean $(x_1, x_2, \dots, x_n$ variables independientes y consideremos la expresión
$$\Delta = \prod_{1\leq i<j\leq n} (x_i - x_j)$$

Para cada $\sigma \in S_n$, sea $\sigma(\Delta) = \prod_{1\leq i<j\leq n} (x_{\sigma(i)} - x_{\sigma(j)})$

Ejemplo: $n=4$

$\Delta = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$

$\sigma = (1\ 2\ 3\ 4)$

$\sigma(\Delta) = (x_2-x_3)(x_2-x_4)(x_2-x_1)(x_3-x_4)(x_3-x_1)(x_4-x_1)$

En $\sigma(\Delta)$ aparece (x_i-x_j) ó (x_j-x_i), $i<j$, pero no ambos por ser σ una biyección.

Cambiando x_j-x_i por $-(x_i-x_j)$ tenemos que Δ y $\sigma(\Delta)$ tienen los mismos factores pero, eventualmente, distinto signo. Es decir, $\sigma(\Delta) = \pm\Delta$

Definición: La aplicación $\varepsilon : S_n \longrightarrow \{1,-1\}$ definida por
$$\varepsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma(\Delta) = \Delta \\ -1 & \text{si } \sigma(\Delta) = -\Delta \end{cases} \quad \forall \sigma\in S_n$$

la llamaremos aplicación signatura o paridad.

Si $\varepsilon(\sigma) = 1$, σ es par, y si $\varepsilon(\sigma) = -1$, σ es impar.

Evidentemente, $\sigma(\Delta) = \varepsilon(\sigma)\cdot\Delta$.

Proposición: La aplicación $\varepsilon : S_n \longrightarrow \{1,-1\}$ verifica que
$\forall \tau, \sigma \in S_n \Rightarrow \varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma)$
(ε es un homomorfismo de grupos).

DEMOSTRACIÓN:

Sean $\tau, \sigma \in S_n$.

$$(\tau\sigma)(\Delta) = \prod_{1\leq i<j\leq n} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)}) = \varepsilon(\tau\sigma)\,\Delta$$

$$\|$$

$$\tau(\sigma(\Delta))$$

Si suponemos que $\varepsilon(\sigma) = (-1)^k$ es que $\sigma(\Delta)$ tiene k factores de la forma $x_j - x_i$ con $i<j$, y por tanto, $\tau(\sigma(\Delta))$ tendrá k factores de la forma $x_{\tau(j)} - x_{\tau(i)}$ con $i<j$. Cambiándole el signo $\Rightarrow$ $x_{\tau(i)} - x_{\tau(j)}$ tenemos que

$$\tau(\sigma(\Delta)) = \varepsilon(\sigma)\cdot \prod_{1\leq i<j\leq n} (x_{\tau(i)} - x_{\tau(j)}) = \varepsilon(\sigma)\cdot\varepsilon(\tau)\cdot\Delta$$

$n=4$
$\sigma=(1\ 2\ 3\ 4)$
$\tau=(4\ 2\ 3)$

Es decir, $\varepsilon(\tau\sigma) = \varepsilon(\sigma)\,\varepsilon(\tau)$.

Corolario: El producto de permutaciones satisface la regla de los signos. Esto es

	PAR	IMPAR
PAR	PAR	IMPAR
IMPAR	IMPAR	PAR

Corolario: Las trasposiciones son permutaciones impares y ε es sobreyectiva.

DEMOSTRACIÓN:

$\varepsilon((1,2)) = -1$ porque intercambia 1 y 2 y los demás los fija.

Ahora, $\forall (i\ j) \Rightarrow (i\ j) = \lambda(1\ 2)\lambda$ donde $\lambda \Rightarrow \begin{cases} i \longleftrightarrow 1 \\ j \longleftrightarrow 2 \\ \text{fija el resto} \end{cases}$

Así que $\varepsilon((i\ j)) = \varepsilon(\lambda(1\ 2)\lambda) = \underbrace{(\varepsilon(\lambda))^2}_{1} \cdot \underbrace{\varepsilon(1\ 2)}_{-1} = -1$

Corolario: Una permutación $\sigma \in S_n$ es par o impar si, y solo si, σ se descompone como producto de un número par o impar de trasposiciones, respectivamente.

Puesto que cualquier m-ciclo es producto de m-1 trasposiciones, tenemos:

Corolario: Un m-ciclo es par (impar) $\iff$ m es impar (par)

Corolario: Una permutación es impar si, y solo si, el número de ciclos de longitud par que aparecen en su descomposición es impar.

Observación:

Sea $A_n = \{$ permutaciones pares de $S_n \} \subseteq S_n$.

A_n es un grupo (grupo alternado)

Sean $\sigma_1, \sigma_2, \dots, \sigma_t$ todas las permutaciones pares y consideremos $\sigma_1(1\ 2), \sigma_2(1\ 2), \dots, \sigma_t(1\ 2)$.

Todas estas permutaciones $\sigma_i(1\ 2)$ $\forall i \in \{1, 2, \dots, t\}$. son distintas, y son impares. Veamos que estas son todas las impares. Si ρ es una permutación impar, $\rho(1\ 2)$ es par, luego $\rho(1\ 2) = \sigma_i$ para cierto $i \Rightarrow \rho = \sigma_i(1\ 2)$

Por tanto, hay igual número de pares y de impares, luego $|A_n| = \frac{n!}{2}$

GRUPOS DE MATRICES 4/10/19

Si $\mathbb{K}$ es un cuerpo, se denota

$GL_n(\mathbb{K}) = \mathcal{U}(\mathcal{M}_n(\mathbb{K})) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid \exists B \in \mathcal{M}_n(\mathbb{K})$ con $AB = I = BA\}$

grupo lineal de grado n sobre $\mathbb{K}$.

Sabemos que $A \in GL_n(\mathbb{K}) \iff \det(A) \neq 0 \iff$ filas o columnas linealmente indep.

Sea $\mathbb{K}$ un cuerpo finito con q elementos.

Veamos cuque $|GL_n(\mathbb{K})| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$

número posibles de 1ª filas; 2ª fila; última fila.

COMBINATORIA

Ejemplo: Si $\mathbb{K} = \mathbb{Z}_2$ $|GL_2(\mathbb{Z}_2)| = (2^2-1)(2^2-2) = 6$

$|GL_3(\mathbb{Z}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168$

Si $\mathbb{K} = \mathbb{Z}_3$ $|GL_2(\mathbb{Z}_3)| = (3^2-1)(3^2-3) = 48$

$SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \mid \det(A) = 1\} \equiv$ grupo lineal especial

Razonaremos luego que $|SL_n(\mathbb{K})| = \dfrac{|GL_n(\mathbb{K})|}{q-1}$ si $\mathbb{K}$ es finito con ... elementos.

Definición: dados dos grupos G y H, un homomorfismo de G en H es una aplicación $f: G \to H$ tal que $f(xy) = f(x)f(y)$ $\forall x, y \in G$. G es el dominio de f y H es el codominio.

Lema: Si $f: G \to H$ es un homomorfismo de grupos, entonces:

i) $f(1) = 1$

ii) $f(x^{-1}) = f(x)^{-1}$ $\forall x \in G$

DEMOSTRACIÓN:

i) $f(1) = f(1 \cdot 1) = f(1)f(1) \Rightarrow f(1) = 1$

ii) $1 = f(1) = f(x x^{-1}) = f(x)f(x^{-1}) \Rightarrow f(x^{-1}) = f(x)^{-1}$

- $Im(f) = f_*(G) = \{f(x) \mid x \in G\} \subseteq H$ imagen de f
- $\ker(f) = \{x \in G \mid f(x) = 1\} \subseteq G$ núcleo de f

Ejemplo:

(1) $id_G: G \longrightarrow G$ es un homomorfismo

(2) $f: G \longrightarrow H \mid f(x) = 1$ $\forall x \in G$ es el homomorfismo cero

(3) $\exp: (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$ es un homomorfismo
$x \longmapsto e^x$

(4) $\det: GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^*$ es un homomorfismo
Además, $\ker(\det) = SL_n(\mathbb{K})$

(5) La composición de homomorfismos es un homomorfismo.

(6) $\varepsilon: S_n \longrightarrow \{1, -1\}$ es un homomorfismo, entendiendo $\{1, -1\}$ como la versión multiplicativa del grupo $\mathbb{Z}_2$.
Además, $\ker(\varepsilon) = A_n$ el grupo alternado.

(7) Si V es un espacio vectorial de dimensión n sobre $\mathbb{K}$,
$Aut(V) \cong GL_n(\mathbb{K})$
↑
... fismos de V en V.

Definición: Sea $f: G \to H$ un homomorfismo de grupos. Se dice que f es un

- monomorfismo si f es inyectiva
- epimorfismo si f es sobreyectiva
- isomorfismo si f es biyectiva.

Si $dom(f) = cod(f)$, f se dice un endomorfismo.
Si f es un endomorfismo isomorfo, entonces f es un automorfismo. Lo notaremos $Aut(G) = \{f: G \to G \mid f \text{ automorfismo}\}$.

Proposición: Sea $f: G \to H$ un homomorfismo de grupos. Entonces:

i) f es isomorfismo $\iff \exists f^{-1}: H \to G$ homomorfismo $\mid ff^{-1} = id_H$
$f^{-1}f = id_G$

ii) f es un monomorfismo $\iff$ $ker(f) = 1$

DEMOSTRACIÓN:

i) Solo hay que comprobar que f^{-1} es un homomorfismo de grupos

ii) $\Leftarrow$] Supongamos que $ker(f) = 1$
Si $x, y \in G \mid f(x) = f(y) \overset{?}{\Rightarrow} x = y$

$$f(x)f(y)^{-1} = 1$$
$$f(xy^{-1}) = 1$$
$$xy^{-1} \in ker(f)$$
$$xy^{-1} = 1 \Rightarrow x = 1$$

$\Rightarrow$]

Proposición:

i) Si $X, Y \neq \emptyset$ y $f: X \to Y$ es una biyección con X, Y finitos, entonces $Perm(X) \cong Perm(Y)$

ii) $Aut(G)$ es un grupo con la composición.

iii) Si $f: G \to H$ es un isomorfismo, entonces $|G| = |H|$.

iv) Si $G \cong H$, entonces G es abeliano $\Leftrightarrow$ H es abeliano.

v) $\forall x \in G$ si $f: G \to H$ es un isomorfismo, entonces $O(f(x)) = O(x)$

DEMOSTRACIÓN:

i) $\sigma \in Perm(X) \longmapsto f \circ \sigma \circ f^{-1} \in Perm(Y)$

$Y \xrightarrow{f^{-1}} X \xrightarrow{\sigma} X \xrightarrow{f} Y$ Ejercicio

Ejemplo: $S_3 \not\cong \mathbb{Z}_6$ $\qquad (\mathbb{R}^*, \cdot) \not\cong (\mathbb{R}, +)$

no abeliano $\quad$ abeliano $\qquad O(-1) = 2 \quad \nexists$ elementos de orden 2

Teorema (de Dyck): Sea G un grupo finito de orden n para el cual tenemos una presentación $G = \langle S \mid R_1, \dots, R_k \rangle$ donde $S = \{s_1, \dots, s_m\}$. Sea H otro grupo y $\{r_1, \dots, r_m\} \subseteq H$, y supongamos que cualquier relación satisfecha en G por los s_i $\forall i \in \{1, \dots, m\}$ es también satisfecha en H cuando los s_i se sustituyen por los r_i. Entonces podemos asegurar que $\exists \varphi: G \to H$ homomorfismo de grupos $\mid \varphi(s_i) = r_i$ $\forall i \in \{1, \dots, m\}$. Además, si $\{r_1, \dots, r_m\}$ es un sistema de generadores de H, φ es sobreyectiva.

Si además $|G| = |H|$, entonces φ es un isomorfismo.

Ejemplos:

7/10/19

(1) $C_n = \langle x \mid x^n = 1 \rangle$
$\mathbb{Z}_n = \langle \bar{1} \rangle \quad n\bar{1} = \bar{0}$

$\exists! \varphi: C_n \to \mathbb{Z}_n$ homomorfismo, $x \longmapsto \bar{1}$

$\mathbb{Z}_n$ está generado por 1, $|\mathbb{Z}_n| = |C_n|$ $\Big\}$ isomorfismo

(2) $V^{abs} = \langle x, y \mid x^2 = 1, \ y^2 = 1, \ xy = yx \rangle$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \rangle$

$V^{abs} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$
$x \longmapsto (\bar{1}, \bar{0})$
$y \longmapsto (\bar{0}, \bar{1})$

homomorfismo
$\Downarrow$
isomorfismo

(3) $V = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2,3)\} = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$

$$\begin{aligned} V^{ab} &\longrightarrow V \\ x &\longmapsto (1\,2)(3\,4) \\ y &\longmapsto (1\,3)(2\,4) \end{aligned}$$

(4) $D_3 = \langle r, s \mid r^3 = 1,\ s^2 = 1,\ sr = r^{-1}s \rangle$

S_3

$$\begin{aligned} D_3 &\xrightarrow{\varphi \text{ iso}} S_3 \\ r &\longmapsto (1\,2\,3) \\ s &\longmapsto (1\,2) \end{aligned}$$

$(1\,2\,3)^3 = 1$

$(1\,2)^2 = 1$

$(1\,2)(1\,2\,3) \overset{?}{=} (1\,2\,3)^{-1}(1\,2)$

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1\,3\,2)(1\,2)$

$(2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$|D_3| = |S_3|$

En general,

$$\begin{aligned} D_n &\xrightarrow{\varphi} S_n \\ r &\longmapsto (1\,2 \ldots n) \\ s &\longmapsto \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & n & n-1 & \ldots & 2 \end{pmatrix} \end{aligned}$$

φ homomorfismo inyectivo. no sobreyectivo ($|D_n| = 2n \neq n! = |S_n|$)

(5) $Q_2^{ab} = \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ yx = x^{-1}y \rangle$

$$\begin{aligned} Q_2^{ab} &\xleftrightarrow{\varphi} Q_2 = \{\pm 1, \pm i, \pm j, \pm k\} \\ x &\longmapsto i \\ y &\longmapsto j \end{aligned}$$

$|Q_2^{ab}| = |Q_2|$

φ isomorfismo.

(6) Sea $k \geq 3 \mid k|n$ ← k divide a n

Entonces $\exists$ homomorfismo

$$\begin{aligned} D_n &\xrightarrow{\varphi} D_k = \langle r_1, s_1 \mid r_1^k = 1 = s_1^2,\ s_1r_1 = r_1^{-1}s_1 \rangle \\ r &\longmapsto r_1 \\ s &\longmapsto s_1 \end{aligned}$$

φ es sobreyectivo, pero no es inyectivo.