Clase 5. Órbitas, Conjugación, Fórmula de clases y p-grupos

§10. Órbitas (continuación):

Ejemplos:

① La acción $GL_n(k) \curvearrowright V \cong k^n$ es fiel: Sea $e_1, \dots, e_n$ base canónica de k^n, si $Av = v \ \forall v \in k^n \leadsto Ae_i = e_i \ \forall i = 1, \dots, n \Rightarrow A = I_n$ ✓

Pero NO es transitivo.: Hay dos órbitas, $\{0\}$ y $k^n \setminus \{0\}$. ← Ejercicio (completar bases)

② La acción (fiel) del grupo ortogonal $O_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ tiene las siguientes órbitas:

Si $x = 0$ en $\mathbb{R}^n \Longrightarrow O_n(\mathbb{R}) \cdot x = \{0\}$

Si $x \neq 0$ y si $y = Ax$ con $A \in O_n(\mathbb{R})$

$\Rightarrow \|y\|^2 = \|Ax\|^2 = \langle Ax, Ax \rangle = \langle x, x \rangle = \|x\|^2$

$R := \|x\|$

$\Rightarrow$ La órbita de x es la esfera $\{y \in \mathbb{R}^n \text{ tq } \|y\| = R\} \underset{\text{difeomorfa}}{\cong} S^{n-1}$

[Indicación: x y $\|x\| e_n$ en la misma órbita]

$\boxed{\text{Ejercicio}}^*$ Si $x \neq 0 \Rightarrow O_n(\mathbb{R})_x \cong O_{n-1}(\mathbb{R})$ y en part $O_n(\mathbb{R})/O_{n-1}(\mathbb{R}) \underset{\text{difeo}}{\cong} S^{n-1}$

③ La acción $SL_2(\mathbb{R}) \curvearrowright \mathbb{H}$, $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \longmapsto \frac{az+b}{cz+d}$ NO es fiel, pues el kernel de la acción es $\{\pm Id\}$.

$\rightsquigarrow PSL_2(\mathbb{R}) := SL_2(\mathbb{R}) / \{\pm Id\}$ actúa fielmente en $\mathbb{H}$.

$\boxed{\text{Ejercicio}}^*$ La acción $SL_2(\mathbb{R}) \curvearrowright \mathbb{H}$ es transitiva

④ Espacio proyectivo: Sea k un cuerpo y consideremos la acción

$$k^\times \curvearrowright k^{n+1} \setminus \{0\}, \quad \lambda \cdot (x_0, \dots, x_n) := (\lambda x_0, \dots, \lambda x_n)$$

cuyo cociente $k^\times \setminus (k^{n+1} \setminus \{0\}) = \{\text{rectas vectoriales en } k^{n+1}\}$ es llamado ESPACIO PROYECTIVO de dimensión n sobre k, denotado $\mathbb{P}^n(k)$.

La clase $[(x_0, \dots, x_n)] =: [x_0, \dots, x_n]$ representa la recta l en k^{n+1} de vector director $(x_0, \dots, x_n) \neq 0$.

Cultura general (Más detalles en MAT426 "Curvas Algebraicas")

Sea $f : k^{n+1} \to k$ una función $\neq$ constante. Entonces $f([x_0, \dots, x_n])$ <u>NO</u> está bien def,

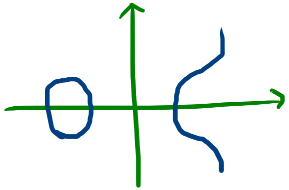
pero la <u>ecuación</u> $f([x_0, \dots, x_n]) = 0$ tiene sentido en $\mathbb{P}^n(k)$ si

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n) \quad \forall \lambda \neq 0 \quad , \text{ie}, f \text{ homogénea de grado } d \in \mathbb{Z}$$

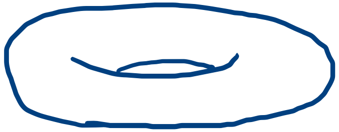
E.g. En $\mathbb{P}^2(k)$, la ecuación cúbica (que depende de $a, b \in k$)

$$E := \{ [x, y, z] \in \mathbb{P}^2(k) \text{ tq } y^2 z = x^3 + axz^2 + bz^3 \}$$

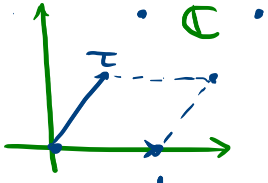
define una CURVA ELÍPTICA (si $\Delta := -16(4a^3 + 27b^2) \neq 0$).



$k = \mathbb{R}$



$\simeq$



$k = \mathbb{C}$

$E \cong \mathbb{C}/\Lambda \quad , \Lambda \cong \mathbb{Z}^2$

<u>Hecho</u>: Se puede dotar a $E \subseteq \mathbb{P}^2(k)$ de estructura de grupo abeliano !

($\rightsquigarrow$ Criptografía)

(5) Sea $\sigma \in S_n$ permutación $\Rightarrow \langle\sigma\rangle \curvearrowright \{1,2,\dots,n\}$ y luego

$$\{1,\dots,n\} = \underset{\text{unión disjunta}}{\bigsqcup_{i=1}^{r}} \underset{\text{órbitas de } \langle\sigma\rangle}{O_i} \rightsquigarrow \sigma_i(x) := \begin{cases} \sigma(x) & \text{si } x \in O_i \\ x & \text{si } x \notin O_i \end{cases}$$

↳ "CICLO CON SOPORTE O_i"

Por definición, $\sigma_i\sigma_j = \sigma_j\sigma_i$ y $\sigma = \sigma_1 \cdots \sigma_r$

$\Rightarrow$ "Toda $\sigma \in S_n$ se escribe de manera única como producto de ciclos disjuntos"

Eg. $\sigma = (4,5,1,3,2) \in S_5 \rightsquigarrow \sigma = \underbrace{(1,4,3)}_{\sigma_1}\underbrace{(2,5)}_{\sigma_2}$ y $\operatorname{ord}(\sigma) = \operatorname{mcm}(3,2) = 6$

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

Consecuencia: Dado que un ciclo de largo l tiene orden l se tiene que $\operatorname{ord}(\sigma) = \operatorname{mcm}\{\operatorname{ord}(\sigma_1),\dots,\operatorname{ord}(\sigma_r)\}$, con $\sigma = \sigma_1 \cdots \sigma_r$ como antes.

↳ $\boxed{\text{Ejercicio}}$ Calcular el orden de todos los elementos de A_4.

Teorema de Cayley (1854): Todo grupo finito es subgrupo de algún S_n.
En part, dado $N \in \mathbb{N}^{\geq 1}$ existen finitos G tq $|G| = N$, módulo isomorfismo.

Dem: La acción $G \curvearrowright G$, $g \cdot x := gx$ es fiel ✓

$\Rightarrow G \hookrightarrow \operatorname{Biy}(G) \cong S_{|G|}$ es inyectivo ∎

§ 11. Conjugación: Sea G un grupo arbitrario.

Hay otra acción natural $G \curvearrowright G$ dada por la CONJUGACIÓN:

$$g \cdot x := g x g^{-1}$$

En este caso, dados $x \in G$ llamamos

a) $G_x \overset{\text{dy}}{=} \{ g \in G \text{ tq } g \cdot x = x \iff gx = xg \} =: C_G(x)$ CENTRALIZADOR de x.

b) $G \cdot x \overset{\text{dy}}{=} \{ g x g^{-1}, g \in G \} =: c(x)$ CLASE DE CONJUGACIÓN de x.

$\boxed{\text{Ejercicio}}^{*}$ (cf MAT210): Describir las clases de conjugación de $GL_2(\mathbb{C})$.

Obs: 1) De manera general, la "conjugación preserva propiedades". Por ejemplo, si $r \in O_3(\mathbb{R})$ rotación resp. a una recta L y $\tau \in O_3(\mathbb{R})$ $\Rightarrow$ $\tau r \tau^{-1}$ es la rotación (mismo ángulo) resp. a la recta $\tau(L) \subseteq \mathbb{R}^3$.

2) Si $H_1, H_2 \leq G$ y $\exists\, g \in G$ tq $g H_1 g^{-1} = H_2 \Rightarrow H_1 \cong H_2$

3) $H \trianglelefteq G$ normal $\overset{\text{dy}}{\iff} g H g^{-1} = H \ \forall g \in G$, i.e., H invariante por conj.

Proposición 2.2.8. — *Si* $\sigma = (a_1 \cdots a_k) \in \mathfrak{S}_n$ *es un* k*-ciclo y* $\tau \in \mathfrak{S}_n$, *entonces*

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_k)). \qquad (2) \qquad (\star)$$

Por ende, todos los k*-ciclos son conjugados en* $\mathfrak{S}_n$. *Más aún, las clases de conjugación de* $\mathfrak{S}_n$ *están en biyección con las particiones de* n:

$$n = k_1 + \cdots + k_r,\ r \in \mathbb{N},\ 1 \le k_1 \le \cdots \le k_r.$$

Dem: si $x \notin \{\tau(a_1), \ldots, \tau(a_k)\} \Rightarrow \tau^{-1}(x) \notin \{a_1, \ldots, a_k\} \Rightarrow \tau\sigma\tau^{-1}(x) = x$.

si $x = \tau(a_i) \Rightarrow \tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1}) \rightsquigarrow (\star)$ OK ✓

En gral, si $\sigma = \sigma_1 \cdots \sigma_r$ producto de ciclos disjuntos de largos $1 \le k_1 \le \ldots \le k_r$

$\Rightarrow \quad \tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1}) \quad (\star\star)$

$\sigma_i\sigma_j = \sigma_j\sigma_i$ producto de ciclos disjuntos de largos $1 \le k_1 \le \ldots \le k_r$

Recíprocamente, $(\star) + (\star\star) \Rightarrow$ Permutaciones corresp. a la misma partición son conj. ∎

Ejemplos:

① S_2: Particiones de $n = 2$: $1 + 1$ y 2

Clases de conjugacion: $\{Id\}$ y $\{(1,2)\}$

② S_3: Particiones de $n = 3$: $1+1+1$, $1+2$ y 3

Clases de conjugación: $\{Id\}$, $\{(1,2), (1,3), (2,3)\}$ y $\{(1,2,3), (1,3,2)\}$

③ S_4: Particiones de $n=4$: $1+1+1+1$, $1+1+2$, $2+2$, $1+3$ y 4

Clases de conjugación: $\{Id\}$, 6 Transposiciones (i,j), 3 "doble transp." $(i,j)(k,l)$, 8 3-ciclos (a,b,c), 6 4-ciclos (a,b,c,d)

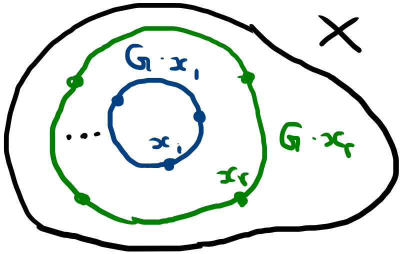
$\boxed{\text{Ejercicio}}$ Describir las clases de conjugación de S_5.
Describir los elementos de A_4 usando este método.

§12. Fórmula de clases y p-grupos

Proposición 2.2.10 (Fórmula de clases). — *Sea G un grupo finito actuando sobre un conjunto finito X. Entonces*

$$\operatorname{card}(X) = \sum_{x\in R} [G : G_x],$$

donde $R \subseteq X$ es un conjunto que contiene exactamente un punto de cada órbita.



$R = \{x_1, \dots, x_r\}$

Dem: X es unión disjunta de las órbitas $G\cdot x$.

Como $G/G_x \xrightarrow[\text{biy}]{\sim} G\cdot x$ y $\operatorname{Card}(G/G_x) \overset{\text{dy}}{=} [G : G_x] \rightsquigarrow$ fórmula ✓ ■

Terminología: Un elemento $x \in X$ es un PUNTO FIJO de $G \curvearrowright X$ si $g \cdot x = x \quad \forall g \in G$ (ie, $G_x = G \iff G \cdot x = \{x\}$)

$$X^G := \{x \in X \text{ punto fijo de } G \curvearrowright X\}$$

Ejemplo: Sea k un cuerpo y $k^\times \curvearrowright k^{n+1}$, $\lambda \cdot (x_0, \ldots, x_n) = (\lambda x_0, \ldots, \lambda x_n)$.

$\rightsquigarrow$ Origen único punto fijo y si $x \in k^{n+1} \setminus \{0\} \Rightarrow G_x = \{1\}$

Si $k = \mathbb{F}_p$: $\operatorname{Card}(k^{n+1}) = p^{n+1}$ Recuerdo: $G/G_x \xrightarrow{\simeq} G \cdot x \Rightarrow \operatorname{Card}(G \cdot x) = [G : G_x]$

$\hookrightarrow x = 0$: $k^\times \cdot x = \{0\} \Rightarrow [G : G_x] = 1$

$\hookrightarrow x \neq 0$: $k^\times \cdot x = \{x, 2x, \ldots, (p-1)x\} \Rightarrow [G : G_x] = p - 1$

$\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$

Fórmula de clases: $\operatorname{card}(k^{n+1}) = p^{n+1} = \sum_{x \in R} [G : G_x] = 1 + (p-1) \underbrace{\# \{\text{rectas vectoriales en } k^{n+1}\}}_{\operatorname{Card}(\mathbb{P}^n(\mathbb{F}_p))}$

$$\Rightarrow \operatorname{Card}(\mathbb{P}^n(\mathbb{F}_p)) = \frac{p^{n+1} - 1}{p - 1} = 1 + p + p^2 + \cdots + p^n.$$

Def: Sea p primo y G grupo finito. Decimos que G es un p- GRUPO si $|G| = p^n$ para cierto $n \in \mathbb{N}^{\geq 1}$.

Proposición 2.2.13. — *Sea G un grupo finito.*

1. *Si un p-grupo G actúa sobre X, entonces*
$$\mathrm{card}(X^G) \equiv \mathrm{card}(X) \mod p.$$
En particular, si p no divide a $\mathrm{card}(X)$ entonces $X^G \neq \emptyset$. (i.e., $\exists$ al menos 1 punto fijo)
2. *Si G es un p-grupo, el centro $Z(G)$ de G no se reduce al singleton $\{e\}$.*

Dem: ① Si $x \in X^G \Rightarrow G \cdot x = \{x\}$ y $[G : G_x] = 1$

$$\Rightarrow \mathrm{Card}(X) = \sum_{x \in R} [G : G_x] = \mathrm{Card}(X^G) + \sum_{x \in R - X^G} \underbrace{[G : G_x]}_{>1 \text{ pues } x \notin X^G}$$

$x \in R - X^G \Rightarrow [G : G_x] > 1$ y divide $|G| = p^n$ (Lagrange) $\Rightarrow p$ divide $[G : G_x]$

$\Rightarrow \mathrm{Card}(X) \equiv \mathrm{Card}(X^G) \mod p$ ✓

② La acción $G \curvearrowright G = X$, $g \cdot x = g x g^{-1}$ tiene $X^G \overset{\text{def}}{=} Z(G)$

$\overset{①}{\Rightarrow} |Z(G)| \equiv |G| \equiv 0 \pmod p$ y $|Z(G)| > 1$ pues $e \in Z(G)$.

∎