# Algebra Abstracta I

Nicholas Mc-Donnell

2do semestre 2017

# Índice general

**1. Grupos** **3**

1.1. Grupos . . . 3

1.1.1. Grupos . . . 4

1.1.2. Motivación para estudiar esto: . . . 4

1.2. Subgrupos . . . 5

1.2.1. Subgrupos triviales . . . 5

1.3. Relación de equivalencia y particiones . . . 6

1.3.1. Relación de equivalencia . . . 6

1.3.2. Meta . . . 9

1.4. Restricción de morfismos a subgrupos . . . 10

1.5. Producto de grupos . . . 10

1.5.1. Porqué es grupo? . . . 11

**2. Simetrías** **13**

2.1. Simetrías en figuras planas . . . 13

2.2. Acciones de grupo . . . 14

2.2.1. Acción en clases laterales . . . 16

2.3. . . . 17

# Capítulo 1

# Grupos

## 1.1. Grupos

Una operación en un conjunto $S$ es una función.

$$S \times S \to S$$

$$(a, b) \mapsto ab$$

Ejemplo: $S =$ Matrices de $n \times n$
La multiplicación y la suma son operaciones en este conjunto.
La operación puede ser asociativa: $(ab)c = a(bc)$
Esto implica que se le puede dar un y solo un sentido a $a_1 \cdot a_2 \cdot ... \cdot a_n$
La operación es conmutativa: $ab = ba$
Ejemplo: Dado un conjunto $T$

$$S = \{\text{funciones de } T \text{ en } T\}$$

En este conjunto la operación de composición es asociativa.
La operación tiene identidad (o neutro) para la operación en $S$ es el clásico neutro y es único:

$$\exists e : \forall a, ae = ea = a$$

Lo operación tiene inverso, con identidad $e$: $\forall a \exists a^{-1} : aa^{-1} = a^{-1}a = e$

**Lema 1.1.1.** *Si la operación es asociativa, esto implica que los inversos son únicos.*

*Demostración.*

$$b \cdot a = a \cdot b = e = a \cdot b' \quad /b\cdot$$

$$(b \cdot a) \cdot b = (b \cdot a) \cdot b' \quad /\text{Propiedad asociativa}$$

$$e \cdot b = e \cdot b'$$

$$b = b'$$

Además, si $a$ y $b$ tienen inverso y la operación es asociativa, esto implica que $ab$ tiene inverso:

$$(ab)^{-1} = b^{-1}a^{-1} \qquad \square$$

### 1.1.1. Grupos

**Definición 1.1.1.** Un grupo es un conjunto $G$ con operación asociativa e identidad, tal que todo elemento tiene inverso.

Ejemplo: $GL_n \begin{pmatrix} \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C} \end{pmatrix} = \{M \in \text{Matrices} \begin{pmatrix} \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C} \end{pmatrix} : det(M) \neq 0\}$ (Grupo general lineal)
Este es un grupo no abeliano con el producto.

**Definición 1.1.2** (Orden)**.** El orden de un grupo $G$ es su cardinalidad $|G|$

Sea $T$ un conjunto (no vacío).

$$S_{|T|} = \{\text{Las biyecciones de } T \text{ en si mismo}\}$$

Entonces, $(S_{|T|}, \circ)$ es un grupo.
Explicación:

- Asociatividad, esta aparece como propiedad de la composición de las funciones
- Identidad, $e = 1|_T$, la función identidad (biyectiva)
- Dada $f : T \to T$ biyección $\implies \exists f^{-1} : T \to T$ tal que $f \circ f^{-1} = f^{-1} \circ f = 1|_T$

Si $|T| = n$ finito, $S_{|T|}$ = grupo de simetría de $n$ elementos. Y $|S_n| = n!$.

### 1.1.2. Motivación para estudiar esto:

Resolver: $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$ por radicales, donde $a_i \in \mathbb{Q}$
Existe cierta manera de asociar un grupo a $p(x)$.
$Gal(p) = Gal(K|\mathbb{Q}$ donde $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ (cuerpo).

**Teorema 1.1.2.** *Sea $f(x) \in \mathbb{Q}[x]$ irreducible:*

$$f(x) \textit{ se resuelve por radicales} \iff Gal(f) \textit{ es soluble}$$

*Ser soluble es la siguiente propiedad:*

$$\exists 1 \lhd G_1 \lhd G_2 \lhd ... \lhd Gal(f) : G_{i+1}/G_i \textit{ es grupo abeliano y } G_i \textit{ subgrupo de } G_i + 1$$

Ejemplo: $f(x) = 2x^5 - 10x + 5$
$Gal(f)$ es isomorfo a $S_5$, pero $S_5$ no es soluble, lo que implica que $f(x) = 0$ no se resuelve por radicales (fórmula).

## 1.2. Subgrupos

Def: Sea $G$ un grupo, $H \subset G$ es subgrupo $\iff$ $H$ es grupo (con la misma operación).

### 1.2.1. Subgrupos triviales

Sea $(G, \cdot)$ grupo y $e$ su neutro. $(G, \cdot) < (G, \cdot)$ y $(\{e\}, \cdot) < (G, \cdot)$ (Notación de subgrupo).

#### Subgrupos de $(\mathbb{Z}, +)$

Los pares son subgrupo de $(\mathbb{Z}, +)$, además los múltiplos de $n$ son subgrupo de $(\mathbb{Z}, +)$
$b\mathbb{Z} := \{bk, k \in \mathbb{Z}\}$

**Proposición 1.2.1.** *Todo subgrupo de $\mathbb{Z}$ es de la forma $b\mathbb{Z}$ ($H < \mathbb{Z} \iff H = b\mathbb{Z}$)*

*Demostración.*

1. Caso: $H$ sin números positivos $\iff$ $H = \{0\} = 0\mathbb{Z}$, esto es por los inversos (sin positivos no hay negativos)

2. Caso: $H$ tiene números positivos $\implies \exists m \in \mathbb{Z}^+ : \forall a > 0 \in H \implies m \leq a$
   Demostrar que $H = m\mathbb{Z}$.

$\supseteq$
Clausura e inducción ($\forall x \in H \implies x \in m\mathbb{Z}$) y también tirar inversos.
$\subseteq$
Todo elemento de $H$ es divisible por $m$.
Sea $a \in H$ no divisible por $m \implies a = mc + r$ con $0 < r < m$
Como $a \in H, m \in H \implies mc \in H \implies -mc \in H$
Por clausura $a - mc = r \in H$. Pero por buen orden es el más pequeño.

$$\rightarrow\leftarrow$$

$\square$

#### Subgrupos Generados

Sea $(G, \cdot)$ grupo y $S \subseteq G$, con $S \neq \emptyset$.
$< S >= \bigcap_{S \subseteq H < G} =$ es el subgrupo más pequeño que contiene a $S$.

**Subgrupos generados por un elemento**

Subgrupo de $G$ generado por $x$

$$< x >:= \{e, x^1, x^{-1}, x^2, x^{-2}, ...\}$$

**Lema 1.2.2.**

$$x \in G, (G, \cdot)$$

$\{Los\ K\ tal\ que\ x^k = e\}$ *es subgrupo de* $\mathbb{Z}$

**Definición 1.2.1** (Centro)**.** Si $G$ es grupo, el centro de $G$ es:

$$Z(G) = \{z \in G : zg = gz\, \forall g \in G\} \trianglelefteq G$$

Si $g \in G, z \in Z \implies gzg^{-1} = z$

## 1.3. Relación de equivalencia y particiones

**Definición 1.3.1** (Partición)**.** Sea $S \neq \emptyset$ conjunto. Una partición $P$ de $S$ es una subdivisión $S$ en un subconjuntos disjuntos.

Ejemplos:
$\{1, 3\}, \{2, 5\}, \{4\}$ es partición de $\{1, 2, 3, 4, 5\}$
Pares e impares en $\mathbb{Z}$

### 1.3.1. Relación de equivalencia

**Definición 1.3.2** (Relaciones de equivalencia)**.** Una <u>relación de equivalencia</u> en $S$ es una forma de relacionar elementos de $S$, $a \sim b$, tal que:

(1) Si $a \sim b, b \sim c \implies a \sim c$ (transitivo)

(2) Si $a \sim b \implies b \sim a$ (simétrico)

(3) $a \sim a$ (reflexivo)

Ejemplo:
Los isomorfismos particionan el conjunto de objetos. Luego tenemos un conjunto que clasifica los objetos.
En Matemáticas <u>clasificamos</u>. Cómo?
Buscamos <u>isomorfismos</u> entre objetos que se presentan en formas distintas, pero estructuralmente son lo mismo.
Dado $S \neq \emptyset$
Partición de $S \equiv$ una relación de equivalencia

Despues de particionar se crea un nuevo conjunto, $\overline{S} = S/\sim =$ Conjunto de las particiones.
Ejemplo:
$\mathbb{Z} \to \overline{\mathbb{Z}} = \{\text{pares, impares}\}, \text{impares} = \overline{1}, \overline{-1}, \overline{3}, \text{pares} = \overline{0}, \overline{-2}, \overline{2}$
Queremos: $\overline{a} + \overline{b} = \overline{a+b}$
$\therefore$ Siempre hay un función sobreyectiva:

$$S \to \overline{S}$$

$$a \mapsto \overline{a}$$

Cualquier función entre conjuntos $S \xrightarrow{\varphi} T$ define una partición en $S : a \sim b$ si $\varphi(a) = \varphi(b)$

$$\therefore \overline{S} = \{\varphi^{-1}(t) : t \in T\}$$

Asá tenemos morfismo biyectivo (isomorfismo)

$$\overline{S} \xrightarrow{\overline{\varphi}} \Im(\varphi)$$

Volviendo a grupos: Sea $\varphi : G \to G'$ morfismo entre grupos.
Ejemplo:

$$\mathbb{C}^\times \xrightarrow{\varphi} \mathbb{R}^\times_{>0} \quad \varphi(a) = |a|$$

$$\varphi(a \cdot b) = |a \cdot b| = |a| \cdot |b| = \varphi(a) \cdot \varphi(b)$$

Esta partición es $\{z \in \mathbb{C}^\times : |z| = r, r \in \mathbb{R}_{>0}\}$
Notar que: $\ker(\varphi) = \{z \in \mathbb{C}^\times : |z| = 1\}$
Proposición: $G \xrightarrow{\varphi} G'$ morfismo de grupo con kernel $N$. Sean $a, b \in G \implies$

$$\varphi(a) = \varphi(b) \iff a = b \cdot n \quad \text{para algún } n \in N$$

$$\iff a \cdot b^{-1} \in N$$

Notación: $aN = \{an : n \in N\}$
$|aN| = |N|$
Dem:

$$N \to aN$$

$$n \mapsto an$$

$$(\text{Inyectiva}) \quad an = an' \implies n = n'$$

$$(\text{Sobreyectiva}) \quad an' \in aN \implies \varphi n' = an'$$

Dem:

$$\varphi(a) = \varphi(b) \iff \varphi(a)\varphi(b)^{-1} = e$$

$$\iff \varphi(ab^{-1}) = e$$

$$\iff ab^{-1} \in \ker(\varphi) = N$$

Def: Dado $H \leq G, a \in G$.

$$aH = \{a \cdot h : h \in H\}$$

se llama clase lateral izquierda. (clases laterales derechas $Ha$)
Proposición: Dado $H \leq G$, las clases laterales izquierdas particionan $G$.
Ejemplos:

- Si $G$ es abeliano $\implies aH = Ha \quad \forall a \in G \implies$ la misma partición.

- $S_3$ = permutaciones de 3 elementos $\iff$ simetráas del triángulo equilátero
  Si $H = \{1|, \sigma_1\} =< \sigma_1 >$

Tarea: verificar que clases laterales coinciden o no coinciden.
Notación: la cardinalidad de las clases laterales se denota por $[G : H]$ (indice de $H$ en $G$)

**Corolario: Teorema de Lagrange**

Si $G$ es finito y $H \leq G \implies |H| \cdot [G : H] = |G|$
En particular: $|H| \,|\, |G|$
Más particular, $|a| \,|\, |G| \quad \forall a \in G$
Corolario: Si $G$ tiene orden $p$ primo y $a \in G \setminus \{e\} \implies G =< a >$
En efecto, $G$ es isomorfo a $\mathbb{Z}/p\mathbb{Z}$.
Dem:
Si $a \neq e \implies |a| \neq 1$
Pero $|a| \,|\, |G| = p$ primo $\implies G =< a > \implies |a| = p$

$$\therefore \{a, a^2, a^3, ..., a^{p-1}, e\} = G =< a >$$

Isomorfismo:

$$\mathbb{Z}/p\mathbb{Z} \to G$$

$$\bar{i} \mapsto a^i$$

$\mathbb{Z}/p\mathbb{Z}$

Sea $n \in \mathbb{Z}_{>0}$.
En $\mathbb{Z}$ definir la relacion de equivalencia:

$$a \sim b \iff a - b \text{ es divisible por } n$$

$$\therefore \mathbb{Z}/n\mathbb{Z} = \{i\mathbb{Z} : i \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

Tarea: la suma designada por $\overline{a} + \overline{b} = \overline{a+b}$ no depende de $a, b$ sino de su clase.

$$\therefore (\mathbb{Z}/n\mathbb{Z}, +) \text{ es un grupo de } n \text{ elementos, y } \mathbb{Z}/n\mathbb{Z} = < \overline{1} >$$

Tarea: $G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg$ y para $g, g' \in G$ $gH \cap f'H = \emptyset$ o $gH = g'H$, por relación de equivalencia ($a \sim b \iff a = bh$ para algún $h \in H$)
Notación: $[G : H] = \#$ de clases lat. izq.$=\#$ de clases lat. der.

$$\therefore |G| = [G : H] \cdot |H|$$

### 1.3.2. Meta

Dado $n > 0$ entero. Cuántos grupos $G$ existen $|G| = n$?
Si $n$ es primo $\implies$ hay sólo 1
Si $n = 4 \implies$ hay sólo 2

$$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Si $n = 6 \implies$ hay sólo 2

$$\mathbb{Z}/6\mathbb{Z}, S_3$$

Si $n = 8 \implies$ hay 5.

**Corolario**

Sea $\varphi : G \to G'$ morfismo entre grupos finitos

$$\implies \ker(\varphi) \trianglelefteq G, \varphi(G) \trianglelefteq G'$$

$$|G| = |\ker \varphi| \cdot [G : \ker \varphi] = |\ker \varphi| \cdot |\varphi(G)|$$

Prop: $H \trianglelefteq G \iff$ Toda clase lateral izquierda es derecha $\iff gH = Hg \forall g \in G$
Dem: Tenemos siempre

$$gh = (ghg^{-1})g \forall g \in G$$

Suponer $H \triangleleft G \implies ghg^{-1} \in H \implies gH \subseteq Hg$. También

$$hg = g(g^{-1}hg) \forall g \in G$$

$$\implies Hg \subseteq gH \implies gH = Hg$$

Si $H \ntriangleleft G \implies \exists ghg^{-1} \notin H$

$$\implies gh \in Hg$$

$$\therefore Hg \neq gH$$

$Hg = g'H$? No, ya que las clases laterales izquierda y derecha particionan. Luego, si $Hg = g'H$

$$\implies g \in g'H \text{ y } g \in gH$$

$$\implies g'H \cap gH \neq \emptyset \implies g'H = gH$$

$$\rightarrow\leftarrow$$

## 1.4. Restricción de morfismos a subgrupos

Obs: $K, H \leq G \implies K \cap H \leq H$

$$K \lhd G \implies K \cap H \lhd H$$

Obs: $\varphi : G \to G'$ morfismo

$$\implies \varphi|_H : H \to G' \quad \text{es morfismo}$$

Prop: $\varphi : G \to G'$ morfismo, $h' \leq G$. Sea $\varphi^{-1}(H') = \tilde{H}$

(a) $\tilde{H} \leq G$

(b) $H' \lhd G' \implies \tilde{H} \lhd G$

(c) $\tilde{H}$ contiene a $\ker \varphi$

(d) $\varphi|_H : \tilde{H} \to H'$ tiene kernel $\ker \varphi$

Dem: p.d. $\tilde{H} \leq G$

1. $e \in \tilde{H}$ ya que $\varphi(e) = e' \in H'$

2. $x, y \in \tilde{H} \implies \varphi(xy) = \varphi(x)\varphi(y) \in H'$

3. $x \in \tilde{H} \implies x^{-1} \in \tilde{H}$

## 1.5. Producto de grupos

Def: Dados $g, G'$ grupos, podemos formar un <u>nuevo grupo</u>:

$$G \times G' = \{(g, g') : g \in G, g' \in G'\}$$

Con la operación:

$$(a, b) \cdot_{G \times G'} (c, d) = (a \cdot_G b, c \cdot_{G'} d)$$

### 1.5.1. Porqué es grupo?

(a) Identidad: $(e, e')$

(b) Invertibilidad: Para $(a, b), (a, b)^{-1} = (a^{-1}, b^{-1})$

Ejemplos:

- $S_3 \times \mathbb{Z}/2\mathbb{Z}$ es un grupo de orden 12 y no es abeliano
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ es grupo de orden 4 y <u>no</u> es $\mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ es grupo abeliano de orden 6.
  Notar que es generado por el $(1, 1)$, por lo que es isomorfo a $\mathbb{Z}/6\mathbb{Z}$

Sean $n, m$ coprimos enteros

$$\implies \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m, \mathbb{Z}$$

# Capítulo 2

# Simetrías

## 2.1. Simetrías en figuras planas

**Definición 2.1.1** (Isometría)**.** Una función $m : \mathbb{R}^2 \to \mathbb{R}^2$ es una <u>isometría</u> si preserva distancia, es decir $\forall p, q \in \mathbb{R}^2$

$$dist(P,Q) = dist(m(P), m(Q))$$

**Proposición 2.1.1.** $m : \mathbb{R}^2 \to \mathbb{R}^2$ *isometría*

$$\implies m\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + M \begin{bmatrix} x \\ y \end{bmatrix}$$

$$Con\ M^t M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

*Notar que* $\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = m\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix}\right)$

*Demostración.*

$$\mathbb{R}^2 \xrightarrow{m} \mathbb{R}^2 \xrightarrow{-m\begin{bmatrix} 0 \\ 0 \end{bmatrix}} \mathbb{R}^2$$

$$T = \text{ isometría con } T\begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\therefore \text{ Sea } v \in \mathbb{R}^2 \setminus \mathbf{0}, T(v)$$

$$T(\lambda v) = \lambda T(v) \quad (ejercicio)$$

$$T(u+v) = T(u) + T(v)$$

Luego $T$ es transformación lineal: $\exists M \in M_{2\times 2}$

$$T\begin{bmatrix} x \\ y \end{bmatrix} = M\begin{bmatrix} x \\ y \end{bmatrix}, M = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$$

$$M\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix} \implies A^2 + B^2 = 1$$

$$M\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} C \\ D \end{bmatrix} \implies C^2 + D^2 = 1$$

$$\begin{bmatrix} A \\ B \end{bmatrix} \cdot \begin{bmatrix} C \\ D \end{bmatrix} = 0 \implies AC + BD = 0$$

$$\therefore \begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$ □

**Corolario.** *Isometrías son biyecciones*

**Corolario.** *Isometrías forman un grupo con la composición.*

**Definición 2.1.2** (Simetría)**.** Sea $F \subseteq \mathbb{R}^2$ una figura. Una <u>simetría</u> es una isometría tal que

$$m(F) = F$$

$$Sim(F) \leq Sim(\mathbb{R}^2$$

## 2.2. Acciones de grupo

**Definición 2.2.1.** $G =$ Grupo, $S \neq \emptyset$ conjunto. Sea $G \times S \to S, (g, s) \mapsto g \cdot s$ tal que:

(a) $e \cdot s = s, \forall s \in S$

(b) $(gg') \cdot s = g \cdot (g' \cdot s) \forall g, g' \in G, \forall s \in S$

Si tenemos esto decimos que $G$ actua en $S$

$$(GS)$$

Ejemplos:

- $F \subseteq \mathbb{R}^2$ figura.

$$Sim(F) = G, S = F$$

$$\therefore GS$$

$$G \times S \to S$$

$$(g,p) \mapsto g \cdot p = g(p)$$

- $G = \mathbb{Z}/2\mathbb{Z}, S = \mathbb{C}\ GS$ por conjugación

$$\{0,1\} \times \mathbb{C} \to \mathbb{C}$$

$$0 \cdot z = z$$

$$1 \cdot z = \bar{z}$$

**Observación 2.2.1.** Si $GS$ y $g \in G$

$$\implies m_g : S \to S, m_g(s) = g \cdot s \quad \text{y es biyección:}$$

- Inyectiva:

$$g \cdot s = g \cdot s' \quad /g^{-1}\cdot$$

$$g^{-1} \cdot (g \cdot s) = g^{-1} \cdot (g \cdot s') \implies e \cdot s = e \cdot s'$$

$$\implies s = s'$$

- Sobreyectiva: Dado $s \in S$, $g \cdot ? = s \therefore ? = g^{-1} \cdot s$

Lo principal de $GS$ es que particiona a $S$ en órbitas.

$$O_s = \{s' \in S : g \cdot s = s' \text{ para algún } g \in G\}$$

Ejemplo: $G = D_4, S = \square$, $D_4$ verlo como $Sim(\square)$
Las órbitas de $G \circlearrowleft S$ definen una relación de equivalencia:

$$s \sim s' \iff s' = g \cdot s \exists g \in G$$

$$\therefore S \text{ es unión de órbitas disjuntas}$$

**Definición 2.2.2.** Si $S$ es una órbita $\implies$ decimos que $G$ actua <u>transitivamente</u>. $\iff$ Dados $s, s' \in S \exists g \in G$ tal que $s = g \cdot s'$

Ejemplo: $Sim(\mathbb{R}^2$ actua en $\mathbb{R}^2$ transitivamente.

**Definición 2.2.3.** El <u>estabilizador de $s \in S$</u> es $G_s = \{g \in G : g \cdot s = s\}$

Ejemplo: $G_{(0,0)}$ para $G = Sim(\mathbb{R}^2) \circlearrowleft \mathbb{R}^2$

$$\therefore G_{(0,0)} = \{M \in Mat_{2\times 2}(\mathbb{R}) : M^t M = Id\} = \text{ grupo ortogonal } = O(2,\mathbb{R})$$

**Observación 2.2.2.** $G_s \leq G$

Ejemplo: $G = Sim(\mathbb{R}^2), S = \{\triangle \in \mathbb{R}^2\} \implies$ las órbitas son los $\triangle_s$ congruentes.

$$G_\triangle = \{e\} \quad G_{\triangle \text{ (equilátero)}} \simeq S_3$$

$$G_{\triangle \text{ (isosceles)}} \simeq \mathbb{Z}/2\mathbb{Z}$$

### 2.2.1. Acción en clases laterales

**Definición 2.2.4.** $H \leq G \implies$ clases laterales izquierdas particionan $G$
Notación: part.$= G/H$
$G$ actua en $G/H$!

$$G \times G/H \to G/H$$

$$(g, aH) \mapsto gaH = g \cdot aH$$

es acción y transitiva.

**Proposición 2.2.1.** *$G \circlearrowleft S, s \in S, H = G_s, O_s$ la órbita de $s$. Luego $G/H \xrightarrow{\varphi} O_s, \varphi(aH) = a \cdot s$ es biyección.*

*Demostración.*

- Bien definido: Sean $aH = bH \iff \exists h \in H : b = ah$

$$\implies b \cdot s = ah \cdot s = a \cdot (h \cdot s) = a \cdot s$$

- Inyectiva:

$$a \cdot s = b \cdot s \implies s = a^{-1}b \cdot s \implies a^{-1}b \in G_s = H$$

$$\iff aH = bH$$

- Sobreyectiva: Si $g \cdot s \in O_s \implies \varphi(gH) = gs$

□

**Proposición 2.2.2.**

$$G \circlearrowleft S, s \in S, \exists a \in G : s' = a \cdot s$$

*(a)* $aG_s = \{g \in G : g \cdot s = s'\}$

*(b)* $G_{s'} = aG_s a^{-1}$

*Demostración.* (a) Si $b \in aG_s \implies b = ah$ para algún $h \in G_s$

$$\implies b \cdot s = ah \cdot s = a \cdot (h \cdot s) = a \cdot s = s' \implies b \in \text{Derecha}$$

$$b \in \text{Derecha}, b \cdot s = s' = a \cdot s \implies a^{-1}bs = s$$

$$a^{-1}b \in G_s \implies b \in aG_s$$

(b) Si $h \in G_s$

$$\implies h \cdot s' = s' \implies h \cdot (a \cdot s) = a \cdot s$$

$$\implies a^{-1}ha \cdot s = s \implies a^{-1}ha \in G_s$$

$$\implies h \in aG_sa^{-1}$$

$$h \in aG_sa^{-1}$$

$$\implies h = ah'a^{-1} \implies h \cdot s' = ah'a^{-1} \cdot s' = ah'a^{-1} \cdot as = s' \qquad \square$$

Ejemplo: Sea $(a, b) \in \mathbb{R}^2$

$$\therefore G_{(a,b)} = t_{(a,b)} G_{(0,0)} t_{(a,b)}^{-1}$$

$$G_{(a,b)} = \{f \in Sim(\mathbb{R}^2) : f(x, y) = t^{-1}(M(t_{(a,b)}(x, y)))\}$$

## 2.3.

**Teorema 2.3.1.** *Todo grupo finito $G$ de $SO_3$ es uno de los siguientes:*

- $C_k$ : *grupo ciclico de orden $k$*
- $D_k$ : *Diedral de orden $2k$ (isometrías de un poligono regular de $k$ lados)*
- $T$ : *Tetraedral; 12 rotaciones de llevar un tetraedro en si mismo.*
- $O$ : *Octaedral; 24 rotaciones que llevan un cubo o un octaedro en si mismo.*
- $I$ : *Icosaedral; 60 rotaciones que llevan dodecaedros o icoseaedros en si mismo.*

*Demostración.* Sea $G \leq SO_3$ finito: $|G| = N$
Si $g \in G$ y $g \neq Id \implies g$ fija 2 puntos en la esfera.

$$P = \{Pg, P'gLg \in G\} = \text{Polos de } G$$

$G \circlearrowright P : G$ envia polos en polos.

*Demostración.* $p \in P, g \in G$. Necesitamos $gp \in P$ fijo por algún $g' \in G$. Asumir $x \neq Id, x \in G$ tal que $xp = p \implies gxg^{-1}(gp) = gp$ $\square$

<u>La Idea</u> es contar polos. Creemos que hay $2n - 2$ polos, pero no ya que el estabilizador de $p \in P$ es ciclico de orden $r_p$.

$$G_p \text{ es cíclico}$$

$$\therefore |O_p| = \frac{|G|}{|G_p|}$$

Digamos que $|O_p| = n_p$

$$r_p \cdot n_p = N$$

# elementos en $G$ con $p$ polo $= r_p - 1$

$$\implies \sum_{p\in P}(r_p - 1) = 2(N-1)$$

Dividir $P$ en órbitas:

$$O_1, ..., O_s$$

disjuntas: $|O_i| = n_i$

$$\therefore \sum_{i=1}^{s} n_i(r_i - 1) = 2N - 2$$

Como $r_i n_i = N$, entonces

$$\sum_{i=1}^{s} \frac{N}{r_i}(r_i - 1) = 2N - 2$$

$$\therefore 2 - \frac{2}{N} = \sum_{i=1}^{s}\left(1 - \frac{1}{r_i}\right)$$

Notar que:

$$2 - \frac{2}{N} < 2 \text{ y } 1 - \frac{1}{r_i} \geq \frac{1}{2}$$

$$\therefore 2 > \frac{1}{2}s \implies 4 > s \implies s \leq 3$$

(1 órbitas): $2 - 2/N = 1 - 1/r_1$, $2 - 2/N \geq 1$ y $1 - 1/r_1 < 1$

$$\rightarrow\leftarrow$$

Por lo que no existe este caso.

(2 órbitas): $s = 2$

$$2 - \frac{2}{N} = 1 - \frac{1}{r_1} + 1 - \frac{1}{r_2}$$

$$\implies \frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2}$$

Pero $r_i \leq N$

$$\therefore r_1 = r_2 = N$$

$$\therefore n_1 = n_2 = 1$$

$$\therefore G_p = G = G_{p'}$$

Rotaciones $2\pi/N$

(3 órbitas): $s = 3$

$$\frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1$$

Asumir que $r_1 \leq r_2 \leq r_3$

$$\therefore r_1 = 2$$

(I) Asumimos $r_1 = r_2 = 2, r_3 = r$

$$\therefore N = 2r \implies n_3 = 2.$$

$$O_3 = \{p, p'\}$$

$$\therefore G \simeq D_r$$

(II) Asumimos $r_1 = 2, r_i \geq 3$, pero $r_2 \geq 4, r_3 \geq 4 \implies \rightarrow\leftarrow$ y $r_2 = 3, r_3 \geq 6 \implies \rightarrow\leftarrow$

$$\therefore r_2 = 3$$

$\square$