Clase 8: Simplicidad de A_n y Teorema de Jordan-Hölder

§16. Grupos simples y series de composición (continuación):

Recuerdo: Sea G un grupo. Decimos que G es un GRUPO SIMPLE si:
1°) $G \neq \{e\}$
2°) Si $H \trianglelefteq G$ entonces $H = \{e\}$ ó $H = G$.

La vez pasada observamos que:
1) S_n no es simple si $n \geq 3$, pues $A_n \ntrianglelefteq S_n$ normal.
2) $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ es simple ✓
3) A_4 no es simple, pues $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong K \ntrianglelefteq A_4$ normal.

dobles transposiciones $(a,b)(c,d)$

$\boxed{\text{Ejercicio}}$ Probar que A_5 consiste exactamente en la identidad, las dobles transposiciones, los 3-ciclos y los 5-ciclos
[Indicación: Contar! A_5 tiene exactamente $5!/2 = 60$ elementos]

Será útil hoy!

Teorema (Galois, 1832): El grupo alternante A_n es simple para todo $n \geq 5$.

Dem: Sea $H \neq \{e\}$ con $H \trianglelefteq A_n$, i.e., $\forall \sigma \in A_n$ y $\forall \tau \in H$: $\sigma \tau \sigma^{-1} \in H$

Veamos que $H = A_n$:

$\boxed{\text{Paso 1}}$ $A_n = \langle 3\text{-ciclos} \rangle$

Notar que $(a,b)(c,d) = (a,c,b)(a,c,d)$ & $(a,b)(a,c) = (a,c,b)$

⇝ Todo producto par de transp. es producto de 3-ciclos ✓

$\boxed{\text{Paso 2}}$ Todos los 3-ciclos (a,b,c) y dobles transp. $(a,b)(c,d)$ son conjugados en A_n (OK en S_n)

↳ **Idea**: Sup. $\tau_0 = (2,3,1) \in A_n$ y $\tau_0 = \sigma \tau \sigma^{-1}$ con τ 3-ciclo y $\sigma \in S_n$

Como $n \geq 5$: $(2,3,1) = (4,5)\,(2,3,1)\,(4,5) = \underbrace{(4,5)\,\sigma}_{\tilde{\sigma}}\, \tau\, \underbrace{\sigma^{-1}\,(4,5)^{-1}}_{\tilde{\sigma}^{-1}}$

⇝ σ ó $\tilde{\sigma}$ es par, i.e., σ o $\tilde{\sigma} \in A_n$ ✓

Similar : si $(1,2)(3,4) = \sigma \tau \sigma^{-1} = \tilde{\sigma} \tau \tilde{\sigma}^{-1}$ con $\tilde{\sigma} = (1,2)\sigma$

⇝ σ ó $\tilde{\sigma}$ pertenece a A_n ✓

Dem (continuación):

Obs: Paso 2 + $H \trianglelefteq A_n \Rightarrow$ Si H contiene un 3-ciclo entonces contiene todos $\xRightarrow{\text{Paso 1}}$ $H = A_n$

Veamos que H contiene un 3-ciclo:

$\boxed{\text{Paso 3}}$ Si H contiene una ($\Rightarrow$ todas) doble transp. $(a,b)(c,d)$ ó bien un 5-ciclo $\Rightarrow$ H contiene un 3-ciclo.

(Obs: En part, A_5 es simple!)

↳ $(a,b,c) = \underbrace{(a,e)(c,d)}_{\in H} \underbrace{(a,d)(c,e)}_{\in H} \underbrace{(a,b)(d,e)}_{\in H}$

ó bien $(a,b,d) = \underbrace{(a,b,c)(a,b,c,d,e)(a,b,c)^{-1}}_{\in H \trianglelefteq A_n} \underbrace{(a,b,c,d,e)^{-1}}_{\in H}$

$\boxed{\text{Paso 4}}$ $\forall n \geq 6$, A_{n-1} simple $\Rightarrow A_n$ simple

Notar que $\exists\, \sigma \in H$ con $\sigma \neq Id$ y $\sigma(1) = 1$

<u>Dem</u> (continuación):

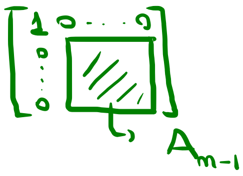
Si $\sigma(1) = i \neq 1$ consideramos $j \notin \{1, i\}$ tq $\sigma(j) \neq j$

↳ Posible pues $\sigma \neq (1, i) \notin A_n$

Como $n \geq 6$, $\exists\, l, m$ con $l \neq m$, $l, m \notin \{1, i, j, \sigma(j)\}$

$$\Rightarrow \tilde{\sigma} := \underbrace{(j, l, m)\, \sigma^{-1} (j, l, m)^{-1}}_{\in H \trianglelefteq A_n} \underbrace{\sigma}_{\in H} \in H \quad \text{y} \quad \left.\begin{array}{l} \tilde{\sigma}(1) = 1 \\ \tilde{\sigma}(j) = l \neq j \end{array}\right\} \rightarrow \tilde{\sigma} \neq Id$$

$\Rightarrow \tilde{\sigma} \in K \cap H$, donde $K := \{\sigma \in A_n \text{ tq } \sigma(1) = 1\} \cong A_{n-1}$ ←



$\Rightarrow K \cap H \neq \{e\}$ y $K \cap H \trianglelefteq K \simeq A_{n-1}$ grupo simple $\Rightarrow K \cap H = K$

ie, $\underbrace{K}_{\text{contiene un 3-ciclo}} \leq H$

$\Rightarrow H$ contiene un 3-ciclo $\Rightarrow H = A_n$ ∎

Corolario: Sea $n \geq 2$. Si $n \neq 4$, los únicos subgrupos normales de S_n son $\{e\}$, A_n y S_n.

Dem: $n = 2$ se verifica "a mano" ✓ Sup que $n = 3$ ó $n \geq 5$.

Si $H \triangleleft S_n \Rightarrow H \cap A_n \triangleleft A_n \overset{\text{galois}}{\Longrightarrow} H \cap A_n = \{e\}$ ó $H \cap A_n = A_n$:

i) $H \cap A_n = A_n$, ie, $A_n \leq H$: $[H : A_n] = |H|/|A_n|$ divide $[S_n : A_n] = \frac{|S_n|}{|A_n|} = 2$ (Lagrange)

$\Rightarrow [H : A_n] = 1 \Leftrightarrow H = A_n$ ✓

ó $[H : A_n] = 2 \Leftrightarrow |H| = |S_n| \Rightarrow H = S_n$ ✓

ii) $H \cap A_n = \{e\}$: $H \hookrightarrow S_n \overset{\pi}{\twoheadrightarrow} S_n / A_n \cong \mathbb{Z}/2\mathbb{Z}$ inyectivo !
(pues $\ker(\pi) \cap H = \{e\}$)

$\Rightarrow H = \{e\}$ ✓ ó bien $|H| = 2$:

Si $|H| = 2$: Sea $\sigma \in H$ tq $\sigma \neq Id$ y escribimos $\sigma = (a,b)(c,d) \cdots$ prod. de transp.

Como $n \geq 3$, $\exists\, c \notin \{a,b\}$ y $\tilde{\sigma} := \underbrace{(a,c)\sigma(a,c)^{-1}}_{\in H \triangleleft S_n}$ cumple $\tilde{\sigma}(c) = b$.

$\Rightarrow \tilde{\sigma} \neq Id$ y $\tilde{\sigma} \neq \sigma$ ↯ pues $\tilde{\sigma} \notin \{Id, \sigma\} = H$. ∎

Def: Una SERIE DE COMPOSICIÓN de un grupo G es una filtración finita

$$G =: G_0 \trianglerighteq\!\!\!\!/\; G_1 \trianglerighteq\!\!\!\!/\; \cdots \trianglerighteq\!\!\!\!/\; G_r = \{e\}$$

tal que cada G_i/G_{i+1} es simple.

Ejemplos:

1. $\mathbb{Z}/6\mathbb{Z}$ admite la serie de composición $\underset{G_0}{\mathbb{Z}/6\mathbb{Z}} \triangleright \underset{G_1}{\mathbb{Z}/3\mathbb{Z}} \triangleright \underset{G_2}{\{0\}}$ con cocientes $G_0/G_1 \simeq \mathbb{Z}/2\mathbb{Z}$ y $G_1\ (= G_1/G_2) \simeq \mathbb{Z}/3\mathbb{Z}$ grupos simples ✓

   Obs: Similar, $\mathbb{Z}/6\mathbb{Z} \triangleright \mathbb{Z}/2\mathbb{Z} \triangleright \{0\}$ con cocientes $\mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}/2\mathbb{Z}$.

2. S_4 admite $S_4 \triangleright A_4 \triangleright K \triangleright \mathbb{Z}/2\mathbb{Z} \triangleright \{e\}$ con cocientes $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ y $\mathbb{Z}/2\mathbb{Z}$ (simples).

3. Si $n=3$ ó $n \geq 5$, S_n admite
   $$S_n \triangleright A_n \triangleright \{e\}$$
   con cocientes $\mathbb{Z}/2\mathbb{Z}$ y A_n (simples!)

4. $\boxed{\text{Ejercicio}}$ $(\mathbb{Z}, +)$ no admite una serie de composición.
   [Indicación: Hay infinitos números primos (Euclides)].

Def: Dos series de composición de un mismo grupo G

$$G = G_0 \rhd G_1 \rhd \dots \rhd G_r = \{e\} \quad y \quad G = G_0' \rhd G_1' \rhd \dots \rhd G_s' = \{e\}$$

son EQUIVALENTES si $r = s$ y $\exists\, \sigma \in S_r$ tq $G_{\sigma(i)} / G_{\sigma(i)+1} \cong G_i' / G_{i+1}'$ $\forall i$.

Obs: Los cocientes G_i / G_{i+1} son llamados los FACTORES SIMPLES de G.
Notar que ellos NO determinan a G (e.g. S_4, $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}/24\mathbb{Z}$ tienen los mismos factores simples!).

Teorema de Jordan-Hölder: Sea G un grupo finito. Entonces:

1) G admite una serie de composición (Hölder 1889).
2) Todas sus series de composición son equivalentes (Jordan 1870).

Camille Jordan
(1838 - 1922)

Otto Hölder
(1859 - 1937)

Lema 2.5.13. — *Sea G un grupo. Sean $H \trianglelefteq G$ y $K \trianglelefteq G$ sub-grupos normales tales que $H \neq K$ y tales que los cocientes G/H y G/K son grupos simples. Entonces, $H \cap K \trianglelefteq H$ y $H \cap K \trianglelefteq K$ son sub-grupos normales. Más aún, $G/H \cong K/(H \cap K)$ y $G/K \cong H/(H \cap K)$.*

$\pi : G \to G/H$

Idea: $\ker(K \xrightarrow{\pi|_K} G/H) \simeq H \cap K \trianglelefteq K \rightsquigarrow K/(H \cap K) \hookrightarrow G/H$ inyectiva.

$K \trianglelefteq G \Rightarrow K/(H\cap K) \trianglelefteq G/H \underset{G/H \text{ simple}}{\rightsquigarrow} K/(H \cap K) \simeq G/H$ OK ✓

ó bien $K/(H \cap K)$ trivial

i.e, $H \cap K = K \iff K \leq H$. $(\star)$

$(\star) \rightsquigarrow H/K$ subgrupo normal (no-trivial! pues $H \neq K$) del grupo simple G/K.

Por un lado: $H/K = G/K$ (pues G/K simple!) y luego $(G/K)/(H/K) = \{e\}$.

Por otro lado: $(G/K)/(H/K) \cong G/H \neq \{e\}$ (pues G/H simple!). ↯

$\boxed{\text{Ejercicio}}$ Completar los detalles (cf. Ejercicio 2.1.33 y 2.1.34 del apunte). ■

Dem de Jordan-Hölder: Existencia: Si G simple, tomar $G = G_0 \triangleright \{e\}$ ✓

Sino, sea $G_1 \trianglelefteq G$ normal de orden maximal $\neq G$

Veamos que G/G_1 es simple:

Dem (continuación):

$\widetilde{H} \lhd G/G_1$ define (vía $\pi: G \twoheadrightarrow G/G_1$) un subgrupo normal $\pi^{-1}(\widetilde{H}) =: H \lhd G$ conteniendo a G_1:

$$|G_1| \text{ maximal} \Rightarrow \begin{cases} H = G_1 \Rightarrow \widetilde{H} = \{e\} \\ H = G \Rightarrow \widetilde{H} = G/G_1 \end{cases} \quad \checkmark$$

Recomenzamos a partir de G_1 y construimos G_2, etc. El proceso se detiene pues $|G| > |G_1| > |G_2|$ y $|G|$ finito ✓

Unicidad: Sup OK para grupos tq $\exists$ serie de largo $\leq r-1$

Sean $G \rhd H_1 \rhd \dots \rhd H_r$ y $G \rhd K_1 \rhd \dots \rhd K_s$ de largos $r \leq s$

$\boxed{\text{Caso 1}}$ $H_1 = K_1$: Hip. Ind aplicada a $H_1 = K_1$

$\Rightarrow (H_2, \dots, H_r) \sim (K_2, \dots, K_s)$ y $r = s$ ✓

Dem (continuación): $\boxed{\text{Caso 2}}$ $H_1 \neq K_1$: Consideran

$$\begin{array}{ccccccccc} G & \triangleright & H_1 & \triangleright & H_2 & \triangleright & \cdots & \triangleright & H_r = \{e\} \\ \| & & \triangleleft & & & & & & \\ & & & & L_2 := H_1 \cap K_1 & \triangleright & \cdots & \triangleright & L_t = \{e\} \\ & & \triangleleft & & & & & & \\ G & \triangleright & K_1 & \triangleright & K_2 & \triangleright & \cdots & \triangleright & K_s = \{e\} \end{array}$$

$\rightsquigarrow$ Lema: H_1/L_2 & K_1/L_2 son simples ❗

$\underset{\text{Hip. Ind con } H_1}{\Rightarrow}$ $(H_2, \ldots, H_r) \sim (L_2, \ldots, L_t)$ y $r = t$ ❗

Así, los cocientes $\{H_1/H_2, \ldots, H_{r-1}/H_r\}$ son $\cong$ a $\{\underbrace{H_1/L_2}_{\overset{\text{Lema}}{\cong} G/K_1}, L_2/L_3, \ldots, L_{r-1}/L_r\}$

Como $t = r$, K_1 admite una serie de comp. $(L_2, \ldots, L_r)$ de largo $r-1$

$\underset{\text{Hip Ind con } K_1}{\Rightarrow}$ $s = r$ y $(K_2, \ldots, K_r) \sim (L_2, \ldots, L_r) \sim (H_2, \ldots, H_r)$ ✓

■

Cultura general El "programa de Gorenstein" tuvo como misión clasificar <u>todos</u> los grupos finitos simples.

$PSL_2(k) := SL_2(k)/\{\lambda I,\ \lambda^2=1\}$

Galois (1832): A_n es simple ($n \geq 5$) & $PSL_2(\mathbb{F}_p)$ es simple ($p \geq 5$)

Cayley (1854): Define la noción de grupo.

(Mathieu, Jordan, Hölder, Sylow, Frobenius, Burnside, Dickson, Hall, Brauer, Chevalley, Suzuki, y muchas otras personas ...)

Gonthier et al. (2012): Se verifica computacionalmente la clasificación!

Todo grupo finito simple es isomorfo a uno de los siguientes:

1) $\mathbb{Z}/p\mathbb{Z}$ con p primo.
2) A_n con $n \geq 5$.
3) Grupos "tipo Lie" (e.g. $PSL_2(\mathbb{F}_p)$).
4) 27 grupos "esporádicos". Eg. El MONSTRUO de Fischer-Griess, de orden $\approx 8 \cdot 10^{53}$