Grupos simples

Facultad de Ciencias UNAM

Introducción

En la sección anterior demostramos que si L/F es de Galois, entonces

$$L/F \text{ es separable } \iff \mathrm{Gal}(L/F) \text{ es separable.}$$

Como estamos interesados en estudiar extensiones de la forma L/F donde L es un campo de descomposición sobre F (para demostrar Abel-Ruffini) y en este caso $\mathrm{Gal}(L/F)$ es isomorfo a un subgrupo de S_n (c.f. proposición 2.19.3), entonces es razonable estudiar la resolubilidad de S_n.

El objetivo de esta sección es demostrar que el grupo alternante A_n y el grupo simétrico S_n son resolubles si y solo si $n \leq 4$. Los pasos que seguiremos serán los siguientes:

1. Definiremos el concepto de grupo simple.
2. Demostraremos que "grupo finito simple no-abeliano $\implies$ grupo no resoluble".
3. Demostraremos que A_n es simple si $n \geq 5$.
4. Demostraremos el resultado deseado.

Un recordatorio amistoso

Antes de empezar, recordamos algunos resultados de la sección 2.15.
Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Entonces

1. Si $(i_1 i_2 \cdots i_l) \in S_n$ es un l-ciclo y $\theta \in S_n$ es una permutación, entonces

$$\theta(i_1 i_2 \cdots i_l)\theta^{-1} = \big(\theta(i_1)\theta(i_2)\cdots\theta(i_l)\big)$$

2. Toda permutación en S_n es un ciclo o un producto de ciclos disjuntos.
3. Toda permutación en S_n puede ser escrita como el producto de 2-ciclos.

Grupos simples

Definición

Decimos que un grupo G es **simple** si sus únicos subgrupos normales son los triviales (es decir, $\{e\}$ y G).

Por ejemplo, si p es primo, el teorema de Lagrange implica que los únicos subgrupos de $\mathbb{Z}_p$ (normales o no) son los triviales. En particular, $\mathbb{Z}_p$ es simple si p es primo.

Grupo finito simple no-abeliano $\implies$ grupo no resoluble

Lema 1

Si G es un grupo finito simple no-abeliano, entonces G no es resoluble.

Demostración. Supongamos lo contrario. Es decir, supongamos que G es resoluble. Usando la definición de grupo resoluble, es fácil ver que podemos encontrar un subgrupo normal G_1 de G tal que $G_1 \subsetneqq G$ y $[G_1 : G]$ es primo. Ahora bien, como G es simple y $G_1 \subsetneqq G$, entonces $G_1 = \{e\}$. Por lo tanto,

$$|G| = [G : G_1][G_1 : \{e\}] = [G : G_1]|G_1| = [G : G_1]$$

y en particular, $|G|$ es primo. Esto implica que $G \cong \mathbb{Z}_{|G|}$ y en particular, G es abeliano, contradiciendo la hipótesis. $\square$

Condiciones suficientes para que $H \lhd A_n$ sea A_n

Lema 2

Supongamos que $n \geq 3$ y que H es un subgrupo normal de A_n. Si $H \neq \{e\}$ y H contiene a un 3-ciclo, entonces $H = A_n$.

Demostración. Antes que nada, recordemos que en la proposición 2.15.8 demostramos que A_n es generado por los 3-ciclos si $n \geq 3$. Por eso, para ver que $H = A_n$, basta probar que H contiene a *todos* los 3-ciclos.

Por hipótesis, H contiene a un 3-ciclo, digamos (ijk). Para ver que H contiene a todos los 3-ciclos, supongamos que $i', j', k' \in \{1, \ldots, n\}$ son distintos. Queremos ver que $(i'j'k') \in H$. Para esto, sea θ cualquier permutación tal que

$$\theta(i) = i', \quad \theta(j) = j', \quad \theta(k) = k'.$$

Caso 1. $\theta \in A_n$.

Por el recordatorio 1 tenemos que

$$\theta(ijk)\theta^{-1} = \big(\theta(i)\theta(j)\theta(k)\big) = (i'j'k').$$

Como $\theta \in A_n$, entonces la igualdad anterior y la normalidad de H en A_n implican que $(i'j'k') \in H$.

Caso 2. $\theta \notin A_n$.

Considera $\theta' := \theta(ij)$. Como el producto de dos permutaciones impares es una permutación par, $\theta' \in A_n$ y además

$$(\theta')(ijk)(\theta')^{-1} = \big(\theta'(i)\theta'(j)\theta'(k)\big) = \big(j'i'k'\big) = \big(i'j'k'\big)^{-1}$$

donde las ultimas dos igualdades se pueden verificar directamente. Finalmente, usando la igualdad anterior y la normalidad de H en A_n, obtenemos que $(i'j'k') = (j'i'k')^{-1} \in H$.

En resumen, H contiene a todos los 3-ciclos y por lo tanto, $H = A_n$. $\square$

Un lema técnico para ver que A_n es simple si $n \geq 5$

Lema 3

Supongamos que $n \geq 5$, que $H \lhd S_n$, y que $j_1, j_2, j_3 \in \{1, \ldots, n\}$ son distintos. Si $\sigma \in H \setminus \{e\}$, entonces

$$\sigma^{-1}(j_1 j_2 j_3)^{-1}\sigma(j_1 j_2 j_3) \in H$$

y para toda $j \in \{1, \ldots, n\}$ tenemos que

$$\Big(j \notin \{j_1, j_2, j_3\} \text{ y } \sigma(j) \notin \{j_1, j_2, j_3\}\Big) \implies \Big(\sigma^{-1}(j_1 j_2 j_3)^{-1}\sigma(j_1 j_2 j_3) \text{ fija a } j\Big).$$

Demostración. Primero veamos que $\sigma^{-1}(j_1 j_2 j_3)^{-1}\sigma(j_1 j_2 j_3) \in H$. Para esto, considera la permutación

$$(j_1 j_2 j_3)^{-1}\sigma(j_1 j_2 j_3).$$

Como (i) $(j_1 j_2 j_3) = (j_1 j_2)(j_1 j_3) \in A_n$, (ii) $\sigma \in H$, y (iii) $H \lhd A_n$, entonces

$$(j_1 j_2 j_3)^{-1}\sigma(j_1 j_2 j_3) \in H$$

Usando esto y la pertenencia $\sigma^{-1} \in H$, obtenemos lo deseado.

Resta probar que para toda $j \in \{1, \ldots, n\}$ tenemos que

$$\Big(j \notin \{j_1, j_2, j_3\} \text{ y } \sigma(j) \notin \{j_1, j_2, j_3\}\Big) \implies \Big(\sigma^{-1}(j_1 j_2 j_3)^{-1} \sigma (j_1 j_2 j_3) \text{ fija a } j\Big).$$

Supongamos que $j \in \{1, \ldots, n\}$ es tal que $j \notin \{j_1, j_2, j_3\}$ y $\sigma(j) \notin \{j_1, j_2, j_3\}$. Entonces (calculando directamente)

$$\begin{aligned}
\Big(\sigma^{-1}(j_1 j_2 j_3)^{-1} \sigma (j_1 j_2 j_3)\Big)(j) &= \Big(\sigma^{-1}(j_1 j_2 j_3)^{-1} \sigma\Big)\big((j_1 j_2 j_3)(j)\big) \\
&= \Big(\sigma^{-1}(j_1 j_2 j_3)^{-1} \sigma\Big)(j) \\
&\qquad\qquad\qquad (\text{porque } j \notin \{j_1, j_2, j_3\}) \\
&= \sigma^{-1}\Big((j_1 j_2 j_3)^{-1}\big(\sigma(j)\big)\Big) \\
&= \sigma^{-1}\big(\sigma(j)\big) \qquad (\text{porque } \sigma(j) \notin \{j_1, j_2, j_3\}) \\
&= j.
\end{aligned}$$

□

Teorema 4

El grupo alternante A_n es simple si $n \geq 5$.

Demostración. Supongamos que $H \neq \{e\}$ es un subgrupo normal de A_n. Para ver que A_n es simple, basta probar que $H = A_n$; y para probar que $H = A_n$, basta probar que H contiene a un 3-ciclo (c.f. lema 2).

Para esto, recordemos que por hipótesis $H \neq \{e\}$ y por lo tanto, H contiene a una permutación no trivial, digamos σ. En lo que sigue, construiremos un 3-ciclo en H usando la factorización de σ en ciclos disjuntos (c.f. recordatorio 2). Específicamente, veremos que en cada uno de los siguientes casos, H contiene a un 3-ciclo.

1. Alguno de los ciclos en la factorización de σ tiene longitud ≥ 4.
2. Alguno de los ciclos en la factorización de σ tiene longitud $= 3$.
3. Todo ciclo en la factorización de σ tiene longitud ≤ 2.

Como σ necesariamente satisface alguno de los casos anteriores, tendremos que H contiene a un 3-ciclo.

Caso 1. Alguno de los ciclos en la factorización de σ tiene longitud ≥ 4: Digamos,

$$\sigma = (i_1 i_2 i_3 i_4 \cdots)(\cdots)\cdots$$

Afirmamos que

$$\sigma^{-1}(i_2 i_3 i_4)^{-1}\sigma(i_2 i_3 i_4) = (i_1 i_3 i_4). \tag{1}$$

Primero, notemos que si $j \notin \{i_1, i_2, i_3, i_4\}$, entonces[1] $\sigma(j) \notin \{i_2, i_3, i_4\}$. Usando esto, es fácil ver que el lema 3 implica que

$$\sigma^{-1}(i_2 i_3 i_4)^{-1}\sigma(i_2 i_3 i_4) \text{ fija a toda } j \notin \{i_1, i_2, i_3, i_4\}.$$

Usando esto y evaluando directamente, el lector podrá fácilmente verificar (1). Finalmente, como $\sigma^{-1}(i_2 i_3 i_4)^{-1}\sigma(i_2 i_3 i_4) \in H$ (c.f. lema 3, entonces $(i_1 i_3 i_4) \in H$ y por lo tanto, H contiene a un 3-ciclo en este caso.

[1] Esta implicación depende de que la factorización sea en ciclos *disjuntos*.

Caso 2. Alguno de los ciclos en la factorización de σ tiene longitud $= 3$: Digamos,

$$\sigma = (i_1 i_2 i_3)(i_4 i_5 \cdots) \cdots$$

Afirmamos que

$$\sigma^{-1}(i_2 i_3 i_5)^{-1}\sigma(i_2 i_3 i_5) = (i_1 i_4 i_2 i_3 i_5). \tag{2}$$

Primero notemos que si $j \notin \{i_1, i_2, i_3, i_4, i_5\}$, entonces[2] $\sigma(j) \notin \{i_1, i_2, i_3, i_5\}$. Usando esto, es fácil ver que el lema 3 implica que

$$\sigma^{-1}(i_2 i_3 i_5)^{-1}\sigma(i_2 i_3 i_5) \text{ fija a toda } j \notin \{i_1, i_2, i_3, i_4, i_5\}.$$

Usando esto y evaluando directamente, el lector podrá fácilmente verificar (2). Finalmente, como $\sigma^{-1}(i_2 i_3 i_5)^{-1}\sigma(i_2 i_3 i_5) \in H$ (c.f. lema 3), entonces $(i_1 i_4 i_2 i_3 i_5) \in H$ y por lo tanto, H contiene a un 5-ciclo en este caso. Aplicando el caso anterior[3] a la permutación $(i_1 i_4 i_2 i_3 i_5)$ en vez de a σ, obtenemos un 3-ciclo en H, como deseábamos.

---

[2] Esta implicación depende de que la factorización sea en ciclos *disjuntos*.

[3] Este caso es "alguno de los ciclos en la factorización tiene longitud ≥ 4".

Caso 3. Todo ciclo en la factorización de σ tiene longitud ≤ 2:

Primero notemos que lo σ no puede ser un 2-ciclo porque $\sigma \in H \subset A_n$. Por lo tanto, σ es de la forma

$$\sigma = (i_1 i_2)(i_3 i_4)(\cdots)\cdots$$

De manera análoga a los casos anteriores, el lector podrá fácilmente verificar que

$$\sigma^{-1}(i_2 i_3 i_4)^{-1}\sigma(i_2 i_3 i_4) = (i_1 i_3)(i_2 i_4).$$

De nuevo, como en los casos anteriores, esto demuestra que $(i_1 i_3)(i_2 i_4) \in H$. En lo que sigue, usaremos esta pertenencia para construir un 3-ciclo en H. Supongamos que $i_5 \in$[4] $\{1, \ldots, n\} \setminus \{i_1, i_2, i_3, i_4\}$. Entonces, calculando directamente es facil verificar que

$$\left((i_1 i_3)(i_2 i_4)\right)^{-1}(i_1 i_3 i_5)^{-1}\left((i_1 i_3)(i_2 i_4)\right)(i_1 i_3 i_5) = (i_1 i_5 i_3)$$

y por lo tanto, H contiene a un 3-ciclo en este caso.

Esto concluye la demostración de que H contiene a un 3-ciclo (en cualquier caso), lo cual implica que $H = A_n$. $\square$

[4] Este conjunto es no vació porque $n \geq 5$.

A_n y S_n son resolubles $\iff n \leq 4$

Teorema 5

Los grupos A_n y S_n son resolubles si y solo si $n \leq 4$.

Demostración.

$\Longrightarrow$) Los casos $n = 1, 2$ son triviales. En la sección 2.26 demostramos (directamente) que si $n = 3, 4$, entonces S_n es resoluble. Como (i) A_n es un subgrupo de S_n y (ii) todo subgrupo de un grupo resoluble es resoluble (c.f. proposición 2.26.1), entonces lo anterior implica que S_n es resoluble si $n = 3, 4$.

$\Longleftarrow$) Procedemos por contrapuesta. Es decir, supongamos que $n \geq 5$. Entonces A_n es finito simple[5] no-abeliano[6]. Por el lema 1 esto implica que A_n no es resoluble (si $n \geq 5$). Finalmente, como todo subgrupo de un grupo resoluble es resoluble, lo anterior también implica que S_n no es resoluble (si $n \geq 5$).

□

[5] Por el teorema anterior.

[6] Los 3-ciclos (123) y (124) no conmutan.

Comentario

Finalizamos esta sección usando el teorema anterior para dar una descripción explicita de todos los subgrupos normales de S_n cuando $n \geq 5$. Pero antes de esto, necesitamos un par de lemas.

$H_1 \lhd G$ y $H_2 \leq G \implies H_1 \cap H_2 \lhd H_2$

Lema 6

Supongamos que G es un grupo. Si $H_1 \lhd G$ y $H_2 \leq G$, entonces $H_1 \cap H_2 \lhd H_2$.

Demostración. Supongamos que $x \in H_2$ y que $y \in H_1 \cap H_2$. Queremos demostrar que $x^{-1}yx \in H_1 \cap H_2$. Como $x \in H_2$ y $y \in H_1 \cap H_2 \subset H_2$, entonces $x^{-1}yx \in H_2$ y por lo tanto basta probar que $x^{-1}yx \in H_1$. Sin embargo, esto es consecuencia de que (i) que H_1 es normal en G, (ii) $x \in H_2 \subset G$, y (iii) $y \in H_1 \cap H_2 \subset H$. $\square$

Los subgrupos de S_n que no tienen permutaciones pares

Lema 7

Supongamos que H es un subgrupo de S_n. Si $H \neq \{e\}$ y $H \cap A_n = \{e\}$, entonces existe $\sigma \in S_n \setminus A_n$ tal que $H = \{e, \sigma\}$.

Demostración. Como $H \neq \{e\}$, entonces existe $\sigma \neq e$ tal que $\sigma \in H$. Veamos que $H = \{e, \sigma\}$ (solo resta probar la inclusión "$\subset$"). Procedemos por contradicción. Es decir, supongamos que existe $\tau \in H \setminus \{e, \sigma\}$.

Antes que nada, notemos que si $\tau \in A_n$, entonces las hipótesis $\tau \in H$ y $H \cap A_n = \{e\}$ implican $\tau = e$, contradiciendo $\tau \in H \setminus \{e, \sigma\}$. Por eso, también supongamos que $\tau \notin A_n$. Como $\sigma, \tau \in H$, entonces (i) $\sigma\tau \in H$ y (ii) $\sigma\tau \in$[7] A_n. Entonces $\sigma\tau \in H \cap A_n = \{e\}$ y por lo tanto, $\tau\sigma = e$.

De manera análoga se puede demostrar que $\sigma^2 = e$ y juntando esto con $\tau\sigma = e$, obtenemos $\tau = \sigma$, contradiciendo $\tau \in H \setminus \{e, \sigma\}$. Por lo tanto, $H = \{e, \sigma\}$. Resta probar que $\sigma \in S_n \setminus A_n$; sin embargo, esto es consecuencia inmediata de que $\sigma \neq e$ y $H \cap A_n = \{e\}$. $\square$

[7] Es consecuencia de que (i) σ y τ son impares (pues $H \cap A_n = \{e\}$) y (ii) el producto de dos permutaciones impares es una permutación par.

Los subgrupos normales de S_n

Proposición 8

Supongamos que $n \geq 5$. Si H es un subgrupo normal de S_n, entonces

$$H \in \left\{\{e\}, A_n, S_n\right\}.$$

Demostración. Como $H \lhd S_n$, entonces por el lema 6 $H \cap A_n \lhd A_n$. Mas aun, como $n \geq 5$, entonces A_n es simple y lo anterior implica que $H \cap A_n = \{e\}$ ó $H \cap A_n = A_n$.

Caso 1. $H \cap A_n = A_n$.

Como $H \cap A_n = A_n$, entonces $A_n \subset H$ y por lo tanto,

$$2 = [S_n : A_n] = [S_n : H][H : A_n].$$

Usando esto es fácil verificar que $H = S_n$ ó $H = A_n$.

Caso 2. $H \cap A_n = \{e\}$.

Veamos por contradicción que $H = \{e\}$. Como estamos suponiendo que $H \neq \{e\}$, entonces el lema 7 implica que existe $\sigma \in S_n \setminus A_n$ tal que $H = \{e, \sigma\}$. Como $\sigma \in S_n \setminus A_n$, entonces (por el recordatorio 3) σ es el producto de un numero impar de 2-ciclos, digamos

$$\sigma = (ij)(\cdots)\cdots$$

Ahora bien, supongamos que $k \in \{1, \ldots, n\} \setminus \{i, j\}$ y sea $\theta := (jk)$. Entonces

$$\theta\sigma\theta^{-1} = \theta(ij)(\cdots)\cdots\theta^{-1} = \left(\theta(ij)\theta^{-1}\right)\left(\theta(\cdots)\theta^{-1}\right)\left(\theta\cdots\theta^{-1}\right) = (ik)(\cdots)\cdots$$

donde la ultima igualdad se cumple por (i) el recordatorio 1, (ii) $\theta(i) = i$, y (iii) $\theta(j) = k$.

Acabamos de demostrar que $\theta\sigma\theta^{-1}$ tiene una factorización en 2-ciclos disjuntos en donde (ik) es uno de los factores. En particular, $i \xmapsto{\theta\sigma\theta^{-1}} k$. Por otro lado, como $\sigma = (ij)(\cdots)\cdots$ también es una factorización en 2-ciclos disjuntos, entonces $i \xmapsto{\sigma} j$. Lo anterior implica que $\theta\sigma\theta^{-1} \neq \sigma$ y por lo tanto, $\theta\sigma\theta^{-1} \notin \{e, \sigma\} = H$. Esto contradice $H \lhd S_n$ y por lo tanto $H = \{e\}$.

$\square$