Álgebra II

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán
Arturo Olivares Martos

Granada, 2025

Índice general

1. Grupos resolubles

Este Capítulo trata sobre los grupos resolubles, propiedad interesante de un grupo que tendrá numerosas aplicaciones, como por ejemplo en la solución de ecuaciones por radicales. Sin embargo, la definición de grupo resoluble ha de esperar, pues primero tenemos que hacer un estudio de las "series de un grupo".

1.1. Series de un grupo

Definición 1.1 (Serie de un grupo)**.** Sea G un grupo, una serie de G es una cadena de subgrupos $G_0, G_1, \ldots, G_r$ de forma que:

$$G = G_0 > G_1 > G_2 > \ldots > G_r = \{1\}$$

En dicho caso, diremos que la serie tiene longitud r.

Ejemplo. En S_3, podemos considerar la serie:

$$S_3 > A_3 > \{1\}$$

Definición 1.2 (Refinamiento)**.** Sea G un grupo, si consideramos sobre él dos series:

$$G = H_0 > H_1 > \ldots > H_s = \{1\} \tag{1.1}$$

$$G = G_0 > G_1 > G_2 > \ldots > G_r = \{1\} \tag{1.2}$$

Diremos que (1.2) es un refinamiento de (1.1) si todo grupo que aparece en (1.1) también aparece en (1.2). Ha de ser por tanto $r \geqslant s$.

Decimos que (1.2) es un refinamiento propio de (1.1) si en (1.1) hay grupos que no aparecen en (1.2). En dicho caso, ha de ser $r > s$.

Ejemplo. En A_4, podemos considerar la serie:

$$A_4 > V > \{1\}$$

Un refinamiento propios de la misma es:

$$A_4 > V > \langle (1\ 2)(3\ 4) \rangle > \{1\}$$

Definición 1.3 (Series propia y normal)**.** Sea G un grupo, si consideramos una serie de G:

$$G = G_0 > G_1 > \ldots > G_r = \{1\}$$

- Decimos que es una serie propia si todas las inclusiones entre los subgrupos son propias, es decir, si $G_{k+1} \subsetneq G_k$, para todo $k \in \{0, \dots, r-1\}$.
- Decimos que es una serie normal si todas las relaciones de subgrupo que aparecen son de subgrupo normal, es decir, si $G_k \triangleright G_{k+1}$, para todo $k \in \{0, \dots, r-1\}$.

  En dicho caso, lo notaremos como:

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

Ejemplo. Todas las series anteriores eran series normales propias:

$$S_3 \triangleright A_3 \triangleright \{1\}$$
$$A_4 \triangleright V \triangleright \{1\}$$
$$A_4 \triangleright V \triangleright \langle(1\ 2)(3\ 4)\rangle \triangleright \{1\}$$

Definición 1.4 (Índices y factores de una serie)**.**
Dada una serie normal de un grupo G:

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

- Llamamos factores de la serie a los cocientes:

$$G_{k-1}/G_k \qquad \forall k \in \{1, \dots, r\}$$

- Llamamos índices de la serie a los correspondientes índices de los factores. Si i_k es el índice del factor G_{k-1}/G_k para todo $k \in \{1, \dots, r\}$, entonces notaremos:

$$G = G_0 \overset{i_1}{\triangleright} G_1 \overset{i_2}{\triangleright} \dots \overset{i_r}{\triangleright} G_r = \{1\}$$

Ejemplo. Por ejemplo, en la serie:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

Tenemos los factores:

$$S_3/A_3 \cong C_2$$
$$A_3/\{1\} \cong A_3$$

Y los índices:

$$S_3 \overset{2}{\triangleright} A_3 \overset{3}{\triangleright} \{1\}$$

Si consideramos ahora la serie:

$$A_4 \overset{3}{\triangleright} V \overset{2}{\triangleright} \langle(1\ 2)(3\ 4)\rangle \overset{2}{\triangleright} \{1\}$$

Los factores que obtenemos son:

$$A_4/V \qquad V/\langle(1\ 2)(3\ 4)\rangle \qquad \langle(1\ 2)(3\ 4)\rangle/\{1\}$$

Definición 1.5. Sea G un grupo, si tenemos dos series normales de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$
$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$$

Se dice que son isomorfas si $r = s$ y existe $\sigma \in S_r$ de forma que:

$$G_{k-1}/G_k \cong H_{\sigma(k)-1}/H_{\sigma(k)} \qquad \forall k \in \{1, \ldots, r\}$$

Ejemplo. En $\mathbb{Z}/24\mathbb{Z}$ consideramos las series:

$$\mathbb{Z}/24\mathbb{Z} \rhd 2\mathbb{Z}/24\mathbb{Z} \rhd 4\mathbb{Z}/24\mathbb{Z} \rhd 8\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$
$$\mathbb{Z}/24\mathbb{Z} \rhd 3\mathbb{Z}/24\mathbb{Z} \rhd 6\mathbb{Z}/24\mathbb{Z} \rhd 12\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$

Que son dos series isomorfas, para la permutación $\sigma = (1\ 2\ 3\ 4)$

1.1.1. Series de composición

Pasamos ya al estudio de las series que nos interesarán, que son las series de composición.

Definición 1.6 (Serie de composición)**.** Una serie de G se dice que es una serie de composición de G si es una serie normal sin refinamientos normales propios.
En una serie de composición, será usual referirnos a los factores como factores de composición, y a los índices como índices de composición.

Ejemplo. Ejemplos de series de composición son:

- Las dos series anteriores sobre $\mathbb{Z}/24\mathbb{Z}$ son series de composición.
- Anteriormente vimos que la serie $A_4 \rhd V \rhd \{1\}$ no era de composición, ya que podíamos refinarla más: $A_4 \rhd V \rhd \langle(1\ 2)(3\ 4)\rangle \rhd \{1\}$, aunque ya esta última sí que es de composición.

Por ahora, para estudiar si una serie es o no de composición, no nos queda otra que realizar un análisis exhaustivo del retículo de subgrupos del grupo que consideremos, analizando solo las inclusiones de subgrupos que sean normales, algo que mostraremos en los siguientes ejemplos.

Ejemplo. Sea $\mathbb{K}$ un cuerpo, sobre $\mathrm{GL}_2(\mathbb{K})$ consideramos las matrices triangulares superiores::

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{K}^*, b \in \mathbb{K} \right\}$$

Que tiene infinitos elementos y no es un grupo abeliano, ya que:

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$$

Si consideramos ahora:

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{K} \right\}$$

Tenemos que $T \rhd U \rhd \{1\}$ es una serie de composición.

Notemos que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

Si ahora para $n > 2$ cogemos como T el conjunto de las matrices triangulares superiores y luego cogemos:

$$N = \{\text{matrices triangulares superiores con diagonal de ceros}\}$$
$$U_r = I + N^r$$

Tomando potencias los elementos van subiendo en la diagonal. Podemos considerar:

$$T \rhd U_1 \rhd U_2 \rhd \ldots \rhd U_n = I$$

Ejemplo. Tratamos de buscar cuántas series de composición hay en los siguientes grupos:

- En S_3, recordamos que el retículo de subgrupos que teníamos era:

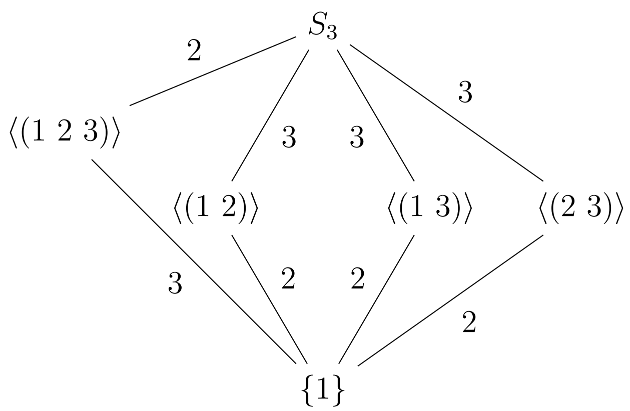


Figura 1.1: Diagrama de Hasse para los subgrupos de S_3.

  Como $A_3 = \langle(1\ 2\ 3)\rangle \lhd S_3$ (por tener índice 2) y ningún otro subgrupo de S_3 es normal salvo el trivial, la única serie de composición de S_3 es:

$$S_3 \rhd A_3 \rhd \{1\}$$

- En D_4:

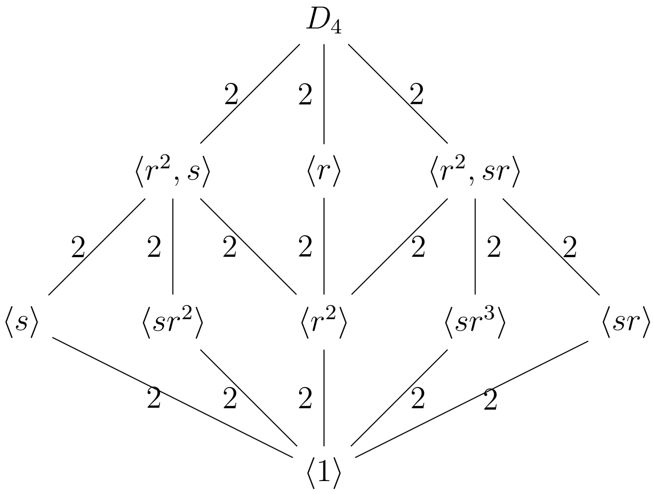
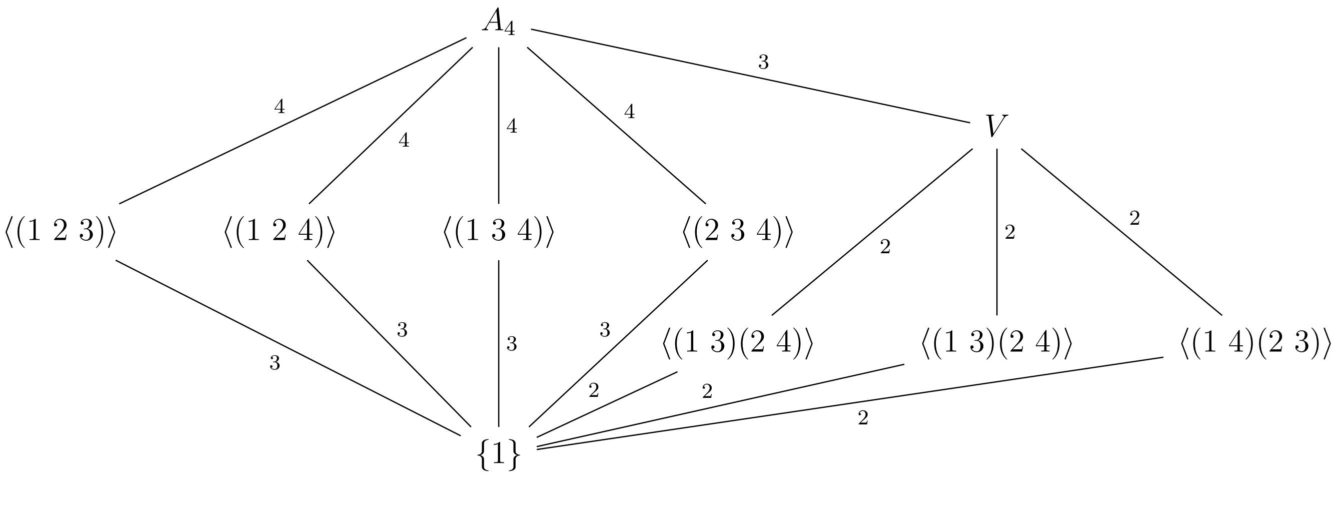


Figura 1.2: Diagrama de Hasse para los subgrupos de D_4.

Como todos los índices del grafo son 2, todas las relaciones de inclusión mostradas en el grafo en realidad son relaciones de normalidad ($\lhd$), por lo que tenemos 7 series de composición distintas (una por cada forma que tengamos de llegar desde D_4 hasta $\{1\}$ en el grafo mediante caminos descendientes):

$$\begin{gathered}
D_4 \rhd \langle r^2, s\rangle \rhd \langle sr^2\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, s\rangle \rhd \langle s\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, s\rangle \rhd \langle r^2\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle r^2\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr^3\rangle \rhd \{1\}\\
D_4 \rhd \langle r\rangle \rhd \langle r^2\rangle \rhd \{1\}
\end{gathered}$$

- Para A_4:

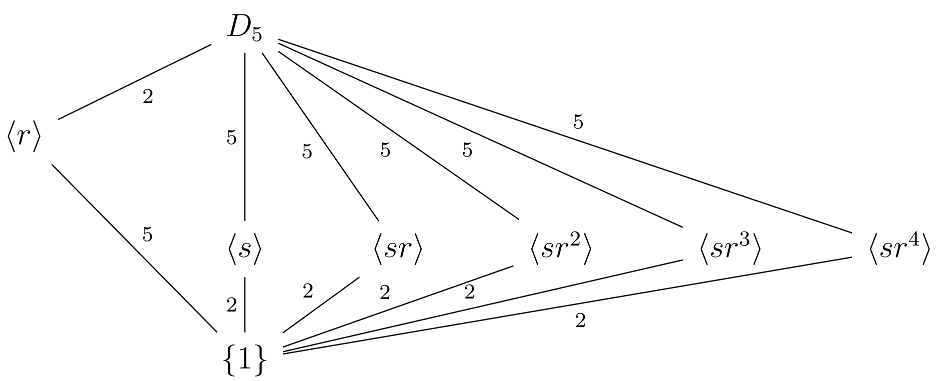


Como $V \lhd A_4$, tenemos como series de composición:

$$A_4 \rhd V \rhd \langle (1\ 2)(3\ 4) \rangle \rhd \{1\}$$
$$A_4 \rhd V \rhd \langle (1\ 3)(2\ 4) \rangle \rhd \{1\}$$
$$A_4 \rhd V \rhd \langle (2\ 3)(2\ 3) \rangle \rhd \{1\}$$

Además, como ninguna de las relaciones $\langle (i\ j\ k) \rangle < A_4$ es normal, no tenemos más series de composición.

- En $D_5 = \langle r, s \mid r^5 = s^2 = 1, sr = r^4 s \rangle$ tenemos:



Solo tenemos la serie de composición:

$$D_5 \rhd \langle r \rangle \rhd \{1\}$$

Ya que D_5 no tiene más subgrupos normales, a parte del trivial.

- En el grupo de los cuaternios:

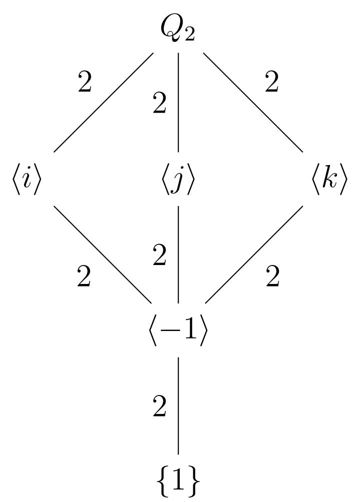


Figura 1.3: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

Como todas las aristas del grafo están numeradas con índice 2, todas las relaciones de subgrupo son normales, por lo que tenemos 3 series de composición, una por cada camino posible:

$$Q_2 \rhd \langle i \rangle \rhd \langle -1 \rangle \rhd \{1\}$$
$$Q_2 \rhd \langle j \rangle \rhd \langle -1 \rangle \rhd \{1\}$$
$$Q_2 \rhd \langle k \rangle \rhd \langle -1 \rangle \rhd \{1\}$$

- En $S_3 \times \mathbb{Z}_2$: Por una parte, en S_3 teníamos una única serie de composición:

  $$S_3 \rhd A_3 \rhd \{1\}$$

  Y en $\mathbb{Z}_2$ la única opción a considerar es $\mathbb{Z}_2 \rhd \{0\}$. Podemos considerar ahora las series de composición resultantes de considerar todas las combinaciones:

  $$S_3 \times \mathbb{Z}_2 \rhd S_3 \times \{0\} \rhd A_3 \times \{0\} \rhd \{(1,0)\}$$
  $$S_3 \times \mathbb{Z}_2 \rhd A_3 \times \mathbb{Z}_2 \rhd A_3 \times \{0\} \rhd \{(1,0)\}$$
  $$S_3 \times \mathbb{Z}_2 \rhd A_3 \times \mathbb{Z}_2 \rhd \{1\} \times \mathbb{Z}_2 \rhd \{(1,0)\}$$

  Que obtenemos primero variando algunos y luego otras. Esto es posible ya que los subgrupos del producto eran productos de subgrupos, en el Teorema **??**.

  Como $\text{mcd}(6,2) = 2 \neq 1$, vamos a tener que hay subgrupos que no son producto de uno por producto de otro, por lo que tendremos otra serie de composición:

  $$S_3 \times \mathbb{Z}_2 \overset{2}{\rhd} H_1 \overset{2}{\rhd} H_2 \overset{3}{\rhd} \{1\}$$

  Con $H_1, H_2 < S_3 \times \mathbb{Z}_2$ que no especificaremos pero diremos que $H_1 \cong S_3$ y $H_2 \cong A_3$.

Definición 1.7 (Grupo simple)**.** Un grupo G se dice simple si no es trivial y no tiene subgrupos normales propios

Ejemplo. $\mathbb{Z}_3$ es un grupo simple, ya que su retículo de subgrupos es:

$$\begin{array}{c} \mathbb{Z}_3 \\ | \\ \{0\} \end{array}$$

Un resultado que veremos luego (el Teorema de Abel) nos dirá que los grupos A_n para $n \geqslant 5$ son grupos simples.

Resultados sobre series de composición

Proposición 1.1. *Un grupo abeliano es simple si y solo si es un grupo cíclico de orden primo.*

Demostración. Por doble implicación:

$\Longleftarrow$) Si G es cíclico de orden primo, no va a tener subgrupos propios, por lo que será simple.

$\Longrightarrow$) Si G es abeliano, entonces todos sus subgrupos serán normales. Si es simple, no tendrá subgrupos propios (ya que si no serían normales, luego no sería simple). Sea $1 \neq x \in G$, sabemos que $\langle x \rangle < G$, de donde ($\{1\} \neq \langle x \rangle$ y G no tiene subgrupos propios) $G = \langle x \rangle$, por lo que G es cíclico.

Si $|G| = nm$, entonces $1 \neq \langle x^m \rangle < G$, por lo que G tendría subgrupos propios, luego no sería simple. Por tanto, $|G|$ ha de ser primo.

$\square$

Ejemplo. Estudiando un poco el caso de grupos cíclicos infinitos, si $G = \mathbb{Z}$, un grupo cíclico finito, $\mathbb{Z}$ no es simple, ya que tiene subgrupos propios (que además son normales, por ser $\mathbb{Z}$ abeliano).

Proposición 1.2. *Si un grupo G tiene una serie de composición, entonces sus factores de composición son grupos simples.*

Demostración. Sea una serie de composición de longitud r:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\} \tag{1.3}$$

Supongamos que existe un índice $i \in \{1, \ldots, r\}$ de forma que G_{i-1}/G_i no sea un grupo simple. En cuyo caso, existirá un subgrupo propio normal suyo no trivial $\{1\} \neq H \lhd G_{i-1}/G_i$. Si usamos ahora el Tercer Teorema de Isomorfía considerando la proyección $p_i : G_{i-1} \to G_{i-1}/G_i$, tenemos que:

$$p_i^*(H) \lhd G_{i-1}$$

Además, como H es un subgrupo del cociente, tenemos que $\{G_i\} \subseteq H$, luego:

$$G_i = \ker(p_i) = p_i^*(G_i) \subseteq p_i^*(H) \lhd G_{i-1}$$

Y por ser $G_i \lhd G_{i-1}$, deducimos que también $G_i \lhd p_i^*(H)$. Hemos encontrado un subgrupo normal de G que estaría entre G_i y G_{i-1}:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_{i-1} \rhd p_i^*(H) \rhd G_i \rhd \ldots \rhd G_r = \{1\} \tag{1.4}$$

Por lo que (1.4) es un refinamiento de (1.3), que era una serie de composición, <u>contradicción</u>, que venía de suponer que un factor de la serie de composición no era simple. $\square$

Proposición 1.3. *Todo grupo finito tiene una serie de composición.*

Demostración. Sea G un grupo finito, distinguimos casos:

- Si G es el grupo trivial, es fácil hayar la serie de composición.
- Si G es simple, entonces no tiene subgrupos normales propios, por lo que tiene una única serie de composición:

$$G \rhd \{1\}$$

- Si $|G| = p$ primo, vimos en la Proposición **??** que entonces G es cíclico, y la Proposición 1.1 nos dice que G es simple, por lo que estamos en el caso anterior.

- Si $|G|$ no es primo y G no es simple, por inducción sobre $n = |G|$, suponemos que es cierto para todo grupo H con $|H| < |G|$ (observemos que el punto anterior nos sirve como caso base).

  Como G es finito, tiene un número finito de subgrupos, entre los que podemos encontrar (por ser G no simple) G_1, un subgrupo normal propio maximal[1] de G. Como $|G_1| < |G|$ (G_1 es subgrupo propio), por hipótesis de inducción tenemos una serie de composición para G_1:

  $$G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

  Además, como G_1 era el subgrupo normal maximal de G, sabemos que no existe $H \lhd G$ con $G_1 \lhd H \lhd G$, por lo que la serie:

  $$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

  Es de composición. □

Teorema 1.4 (de Refinamiento de Schreier)**.** *Sea G un grupo, dos series normales de G tienen refinamientos isomorfos.*

Demostración. Consideramos dos series normales de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_{i-1} \rhd G_i \rhd \ldots \rhd G_r = \{1\} \tag{1.5}$$

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_{j-1} \rhd H_j \rhd \ldots \rhd H_s = \{1\} \tag{1.6}$$

Fijado $i \in \{1, \ldots, r\}$, tenemos $G_i \lhd G_{i-1} < G$, y para todo $j \in \{1, \ldots, s\}$ tenemos $H_j \lhd H_{j-1} < G$, donde podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo la siguiente relación entre los grupos:

$$G_{ij} = G_i(H_j \cap G_{i-1}) \lhd G_i(H_{j-1} \cap G_{i-1}) = G_{ij-1} \qquad \forall j \in \{1, \ldots, s\}$$

En los casos extremos (es decir, en $j = 0$ y $j = s$), tendremos:

$$\begin{aligned} G_{i0} &= G_i(H_0 \cap G_{i-1}) = G_iG_{i-1} = G_{i-1} \\ G_{is} &= G_i(H_s \cap G_{i-1}) = G_i\{1\} = G_i \end{aligned}$$

De esta forma, tenemos para todo $i \in \{1, \ldots, r\}$ que:

$$G_{i-1} = G_{i0} \rhd G_{i1} \rhd \ldots \rhd G_{is-1} \rhd G_{is} = G_i$$

Que podemos meter en todos los eslabones de la serie (1.5):

$$\begin{aligned} G = G_0 = G_{10} \rhd G_{11} \rhd \ldots \rhd G_{1s} = G_1 = G_{20} \rhd G_{21} \rhd \ldots \rhd G_{2s} = G_2 = G_{30} \rhd \ldots \\ \ldots \rhd G_{r-1s} = G_{r-1} = G_{r0} \rhd \ldots \rhd G_{rs} = G_r = \{1\} \end{aligned}$$

[1] Es decir, que no existe $K \lhd G$ con $G_1 \lhd K$.

Obteniendo un refinamiento de longitud $r(s+1)-(r-1)=rs+1$:
En cada eslabón (teníamos r) hemos metido $s+1$ eslabones, de los que se repetían ($G_{is}=G_{i+1,0}$, para $i\in\{0,\dots,r-1\}$) $r-1$ eslabones.

Si repetimos el procedimiento para la serie (1.6), fijado $j\in\{1,\dots,s\}$, para todo $i\in\{0,\dots,r\}$ podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo que:

$$H_{ij}=H_j(G_i\cap H_j-1)\lhd H_j(G_{i-1}\cap H_{j-1})=H_{i-1j}\qquad \forall i\in\{1,\dots,r\}$$

En los casos extremos tendremos:

$$\begin{aligned}H_{0j}&=H_{j-1}\\H_{rj}&=H_j\end{aligned}$$

Por lo que para todo $j\in\{1,\dots,s\}$, tenemos:

$$H_{j-1}=H_{0j}\rhd H_{1j}\rhd\dots\rhd H_{r-1j}\rhd H_{rj}=H_j$$

Y podemos obtener un refinamiento de (1.6) al igual que hicimos antes, metiendo la cadena superior entre cada uno de los eslabones de la serie original:

$$\begin{aligned}G=H_0=H_{01}\rhd H_{11}\rhd\dots\rhd H_{r1}=H_1=H_{02}\rhd H_{12}\rhd\dots\rhd H_{r2}=G_2=H_{03}\rhd\dots\\ \dots\rhd H_{rs-1}=H_{s-1}=H_{0s}\rhd H_{1s}\rhd\dots\rhd H_{rs}=H_s=\{1\}\end{aligned}$$

Que tiene longitud $s(r+1)-(s-1)=rs+1$, al igual que antes.

Ahora, por la segunda parte del Cuarto Teorema de Isomorfía, tenemos que:

$$\frac{G_{ij-1}}{G_{ij}}=\frac{G_i(H_j\cap G_{i-1})}{G_i(H_j\cap G_{i-1})}\cong\frac{H_j(G_{i-1}\cap H_{j-1})}{H_j(G_i\cap H_{j-1})}=\frac{H_{i-1j}}{H_{ij}}$$

Por lo que los dos refinamientos encontrados son isomorfos. □

Ejercicio. Se pide calcular un refinamiento isomorfo aplicando el método de Schreier a las dos siguientes series normales:

$$\begin{aligned}G=G_0\rhd G_1\rhd G_2\rhd G_3=\{1\}\\G=H_0\rhd H_1\rhd H_2=\{1\}\end{aligned}$$

Teorema 1.5 (Jordan-Holder)**.** *Si un grupo G admite una serie de composición, cualquier serie normal puede refinarse a una serie de composición.*

Además, dos series de composición de un mismo grupo son isomorfas siempre.

Demostración. Tomamos una serie de composición de G:

$$G=G_0\rhd G_1\rhd\dots\rhd G_r=\{1\}$$

Y también una serie normal de G:

$$G=H_0\rhd H_1\rhd\dots\rhd H_s=\{1\}$$

Por el Teorema de Schreier (la serie de composición es normal), existe un refinamiento de ambos isomorfo. Sin embargo, como la primera serie es de composición, su refinamiento coincide con ella misma. Para la segunda serie, obtendremos un refinamiento isomorfo a la primera:

$$G = \overline{G_0} \triangleright \overline{G_1} \triangleright \ldots \triangleright \overline{G_r} = \{1\}$$

□

Con este último Teorema de Jordan-Holder se tiene claro ya el interés en las series de composición, ya que cada grupo admite un única (salvo isomorfismos) serie de composición.

Podemos pensar en calcular series de composición de un grupo conocida una serie de composición en un grupo isomorfo, resultado que podemos esperar que sea cierto (y que de hecho vamos a probar a continuación); sin embargo, el recíproco no es cierto en general: si tenemos dos series de composición, una de un grupo G y otra de otro grupo K que son isomorfas, en general G y K no van a ser isomorfos.

Ejemplo. Por ejemplo, anteriormente vimos en un ejemplo que la única serie de composición que podemos considerar en S_3 es:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

En $\mathbb{Z}_6$, que no es isomorfo a S_3 por ser abeliano, si observamos su retículo:

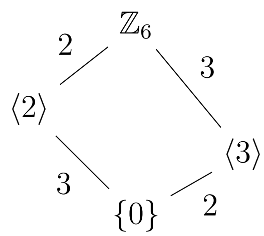


Figura 1.4: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_6$.

Vemos que una serie de composición de $\mathbb{Z}_6$ es:

$$\mathbb{Z}_6 \triangleright \langle 2\rangle \triangleright \{0\}$$

Además, sabemos ahora por el Teorema de Jordan-Holder que $\mathbb{Z}_6$ no tiene más series de composición, ya que la otra posibilidad sería la serie:

$$\mathbb{Z}_6 > \langle 3\rangle > \{0\}$$

Pero como esta no es isomorfa a la primera y sabemos que todas las series de composición de un mismo grupo son isomorfas, sabemos que esta segunda no es de composición. Veamos que las series:

$$S_3 \overset{2}{\triangleright} A_3 \overset{3}{\triangleright} \{1\}$$
$$\mathbb{Z}_6 \overset{2}{\triangleright} \langle 2\rangle \overset{3}{\triangleright} \{0\}$$

Son isomorfas. Para ello, basta ver que:

$$S_3/A_3 \cong \mathbb{Z}_2 \cong Z_6/\langle 2\rangle$$
$$A_3/\{0\} \cong A_3 \cong \mathbb{Z}_3 \cong \langle 2\rangle \cong \langle 2\rangle/\{0\}$$

Proposición 1.6. *Sean G y K dos grupos isomorfos, entonces todas las series de composición de G son isomorfas a todas las series de composición de K.*

El objetivo principal de esta asignatura es clasificar los grupos finitos. Como estos grupos van a tener series de composición cuyos factores serán grupos simples, nos centraremos en clasificar los grupos simples, para luego clasificar los grupos finitos.

La teoría de clasificación de grupos simples comenzó en 1960 y fue completada en 2004, con una demostración de 15000 páginas en lo que se conoce como el "Teorema enorme". En la demostración intervinieron matemáticos como Gorestein (1923 - 1992). Esta clasificación de los grupos simples se hizo en:

- 18 familias infinitas de grupos simples.
- 26 grupos simples, llamados grupos esporádicos.

  Como curiosidad, el grupo esporádico más pequeño tiene orden 7920 y el más grande, 10^{54}.

Cualquier grupo finito simple pertenece a una de estas 18 familias, o es isomorfo a alguno de los 26 grupos esporádicos.

Entre las 18 familias de grupos simples destacamos 2, que son las que nos interesan por ahora:

- Los grupos cíclicos de orden primo, que ya hemos demostrado que se tratan de grupos simples.
- Los grupos alternados A_n con $n \geqslant 5$.

Veremos ahora este segundo resultado, en el ya prometido Teorema de Abel.

Teorema 1.7 (de Abel)**.** *A_n es simple, para $n \geqslant 5$.*

Demostración. Sea $\{1\} \neq N \lhd A_n$, veamos que ha de ser $N = A_n$. En la Proposición **??** vimos que dado[2] $j \in X_n \setminus \{1, 2\}$, teníamos que:

$$A_n = \langle (1\ 2\ j)\rangle$$

Y la demostración terminará viendo que N contiene a un elemento de esta forma. Bajo estas hipótesis, sabemos que va a existir (por ser N finito) $1 \neq \sigma \in N$, la permutación de N que mueve menos elementos. Por ser σ par (estamos en A_n), ha de mover más de dos elementos. Veamos que mueve exactamente 3:

[2]Donde $X_n = \{1, 2, \ldots, n\}$.

1. Si σ es producto de ciclos disjuntos de longitud 2: supongamos que σ mueve, al menos, los elementos x_1, x_2, x_3 (distintos entre sí), con lo que podemos escribir:

$$\sigma = (x_1\ x_2)(x_3\ x_4)\dots$$

Sea $\tau = (x_3\ x_4\ x_5)$ para ciertos $x_4, x_5 \in X_n$ distintos de x_1, x_2, x_3 y distintos entre sí, definimos:

$$\sigma_1 = (x_3\ x_4\ x_5)\sigma(x_3\ x_4\ x_5)^{-1} \in N$$

σ_1 está en N por ser $N \lhd A_n$. Si consideramos:

$$[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N$$

- Supongamos que σ mueve a x_5, en cuyo caso:

$$\begin{aligned} \sigma &= (x_1\ x_2)(x_3\ x_4)(x_5\ \sigma(x_5))\dots \\ \sigma_1 &= (x_1\ x_2)(x_3\ \sigma(x_5))(x_4\ x_5)\dots \end{aligned}$$

  Con lo que:

$$[\tau, \sigma] = (x_3\ \sigma(x_5))(x_4\ x_5)(x_3\ x_4)(x_5\ \sigma(x_5))$$

  Luego $[\tau, \sigma]$ deja fijos a x_1 y x_2 y mueve a los mismos que movía σ. Por ello, $[\tau, \sigma] \in N$ y $[\tau, \sigma]$ mueve menos elementos que σ, contradicción, que viene de suponer que σ mueve a x_5.

- Si suponemos que σ no mueve a x_5:

$$\sigma_1 = (x_1\ x_2)(x_4\ x_5)$$

  Tenemos:

$$[\tau, \sigma] = (x_3\ x_5\ x_4)$$

  Que mueve menos elementos que σ, contradicción.

Por tanto, σ no puede ser producto de transposiciones, ya que llegamos a contradicciones.

2. Si σ tiene un ciclo de longitud mayor o igual que 3 en el que mueve a x_1, x_2 y x_3:

$$\begin{aligned} \tau &= (x_3\ x_4\ x_5) \\ \sigma_1 &= \tau\sigma\tau^{-1} \in N \end{aligned}$$

Supongamos que σ mueve más de 3 elementos, por lo que mueve al menos (por ser una permutación par) 5. En dicho caso:

$$\sigma_1 = (x_1\ x_2\ x_4\ \dots) \neq \sigma$$

Por lo que:

$$[\tau, \sigma] = \sigma_1\sigma^{-1} \in N$$

Y $[\tau, \sigma]$ deja fijos a los mismos que σ y a x_2. En dicho caso, tenemos que $[\tau, \sigma]$ mueve menos que σ.

En definitiva, concluimos que σ contiene a un ciclo de longitud 3, a saber: $(i\ j\ k)$, todos ellos elementos distintos.

- Si $i, j, k, 1, 2$ son todos distintos:

$$(1\ i)(2\ j)(i\ j\ k)(1\ i)(2\ j) = (1\ 2\ k) \in N$$

- Si $i = 1$ y $j, k, 2$ fueran distintos, $\exists h$ distinto de los anteriores de forma que:

$$(2\ j)(k\ h)(1\ j\ k)(2\ j)(k\ h) = (1\ 2\ h) \in N$$

- Si $i = 2$ y $j, k, 1$ fueran distintos, $\exists h$ distintos de los anteriores de forma que:

$$\ldots = (1\ 2\ h) \in N$$

En definitiva, N contiene al generador de A_n, de donde:

$$N = \langle (1\ 2\ j) \rangle = A_n$$

$\square$

1.2. Grupos resolubles

Antes de pasar con la definición de grupos resolubles, hemos de respasar ciertos conceptos relacionados con la operación de conmutador que ya definimos sobre los elementos de G, recordamos que era la aplicación $[\cdot, \cdot] : G \times G \to G$ dada por:

$$[x, y] = xy(yx)^{-1} = xyx^{-1}y^{-1} \qquad \forall x, y \in G$$

1.2.1. Preliminares

Sobre el conmutador solo vimos la Proposición **??**, que nos decía que dados dos elementos h, k de un grupo G:

$$hk = kh \Longleftrightarrow [h, k] = 1$$

Proposición 1.8. *Sea G un grupo y $x, y \in G$, se verifican:*

i) $[x, y]^{-1} = [y, x]$.

ii) $z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}]$, $\forall z \in G$.

Demostración. Veamos cada apartado:

i) Basta con ver:

$$[x, y][y, x] = xy(yx)^{-1}yx(xy)^{-1} = xy(xy)^{-1} = 1$$

ii) Sea $z \in G$, basta aplicar la definición del conmutador:

$$\begin{aligned} z[x,y]z^{-1} &= zxy(yx)^{-1}z^{-1} = zxy(x^{-1}y^{-1}z^{-1}) \\ [zxz^{-1}, zyz^{-1}] &= zxz^{-1}zyz^{-1}(zyz^{-1}zxz^{-1})^{-1} = zxyz^{-1}(zx^{-1}y^{-1}z^{-1}) \\ &= zxy(x^{-1}y^{-1}z^{-1}) \end{aligned}$$

□

Proposición 1.9. *Sea G un grupo, el conjunto:*

$$\langle [x,y] \mid x,y \in G \rangle$$

es un subgrupo normal de G.

Demostración. Llamando Λ a dicho conjunto, para ver que es un subgrupo, si $a,b \in \Lambda$, entonces $\exists n,m \in \mathbb{Z}$ de forma que:

$$a = ([x,y])^n \qquad b = ([x,y])^m$$

En dicho caso:

$$ab^{-1} = ([x,y])^n([x,y])^{-m} = ([x,y])^{n-m}$$

Con $n-m \in \mathbb{Z}$, por lo que $ab^{-1} \in \Lambda$, de donde $\Lambda < G$.

Ahora, para ver que $\Lambda \lhd G$, sea $a \in \Lambda$, existirán $n \in \mathbb{Z}$, $x,y \in G$ de forma que $a = ([x,y])^n$. Sea $z \in G$:

- Si $n = 1$:

$$z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}] \in \Lambda$$

- Si $n = -1$:

$$z([x,y])^{-1}z^{-1} = z[y,x]z^{-1} = [zyz^{-1}, zxz^{-1}] \in \Lambda$$

- Supuesto para $n-1$, para n:

$$z([x,y])^n z^{-1} = z[x,y]z^{-1}z([x,y])^{n-1}z^{-1} = (z[x,y]z^{-1})(z([x,y])^{n-1}z^{-1})$$

  Con $z[x,y]z^{-1} \in \Lambda$ por ser $[x,y] \in \Lambda$ y $z([x,y])^{n-1}z^{-1} \in \Lambda$ por hipótesis de inducción. Como $\Lambda < G$, concluimos que $z([x,y])^n z^{-1} \in \Lambda$. Escribiendo $m = -n$:

$$\left(z([x,y])^m z^{-1}\right)^{-1} = z^{-1}([x,y])^{-m}z \in \Lambda$$

  Por ser $\Lambda < G$, concluimos que $z([x,y])^m z^{-1} \in \Lambda$.

En definitiva, $\Lambda \lhd G$. □

Definición 1.8 (Subgrupo conmutador)**.** Sea G un grupo, llamamos subgrupo conmutador de G al subgrupo:

$$[G,G] = \langle [x,y] \mid x,y \in G \rangle$$

Observemos que como $hk = kh \iff [h,k] = 1$, este grupo está generado por los conmutadores de los elementos que no conmutan entre sí:

$$[G,G] = \langle [x,y] \mid xy \neq yx \rangle$$

Proposición 1.10. *Sea G un grupo, $G/[G,G]$ es abeliano. Más aún, es el menor subgrupo normal de G que hace que el cociente sea abeliano. Es decir, si $N \lhd G$:*

$$G/N \text{ es abeliano} \Longleftrightarrow [G,G] < N$$

$G/[G,G]$ recibe el nombre de grupo abelianizado de G.

Demostración. Si demostramos la doble implicación, como $[G,G] < [G,G]$, tendremos que $G/[G,G]$ es abeliano, por lo que solo tenemos que probar esto:

$\Longrightarrow$) Si consideramos la proyección al cociente $p : G \to G/N$, sea $a \in [G,G]$, entonces existirán $n \in \mathbb{Z}$ y $x, y \in G$ de forma que:

$$a = ([x,y])^n$$

Si calculamos la imagen de a por p (que recordamos que es un homomorfismo):

$$\begin{aligned} p(a) = (p([x,y]))^n = \left(p\left(xy(yx)^{-1}\right)\right)^{-1} &= (p(xy))^n(p(yx))^{-n} \\ &\overset{(*)}{=} (p(x))^n(p(y))^n(p(y))^{-n}(p(x))^{-n} = 1 \end{aligned}$$

Donde en $(*)$ hemos usado que G/N es abeliano. Tenemos que $a \in \ker(p) = N$.

$\Longleftarrow$) Sean $x, y \in G$, entonces:

$$xy(yx)^{-1} = [x,y] \in [G,G] < N$$

Pero:

$$(xN)(yN) = xyN = yxN = (yN)(xN) \Longleftrightarrow xy(yx)^{-1}N = N$$

Por lo que $(xN)(yN) = (yN)(xN)$, para todos $x, y \in G$.

□

Corolario 1.10.1. *Si G es un grupo:*

$$G \text{ abeliano} \Longleftrightarrow [G,G] = \{1\}$$

Demostración. Como $G \cong G/\{1\}$:

$$G \text{ abeliano} \Longleftrightarrow G/\{1\} \text{ abeliano} \Longleftrightarrow [G,G] < \{1\} \Longleftrightarrow [G,G] = \{1\}$$

□

Ejercicio. Se pide comprobar que:

$$\begin{aligned} [A_3, A_3] &= \{1\} \\ [S_3, S_3] &= A_3 \\ [A_4, A_4] &= V \end{aligned}$$

1.2.2. Definición

Definición 1.9 (Serie derivada)**.** La serie derivada de un grupo G es la cadena de subgrupos normales:

$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd \ldots$$

Donde:

$$G^{(k+1)} = [G^{(k)}, G^{(k)}]$$

De esta forma, el subgrupo $G' = [G, G]$ recibe el nombre de subgrupo derivado de G, o primer derivado de G.

Un grupo G se dice <u>resoluble</u> si existe un índice k de forma que $G^{(k)} = \{1\}$. Es decir, la serie derivada de G alcanza el $\{1\}$.

Ejemplo. Veamos que:

- Si G es abeliano, entonces G es resoluble:

  $$G' = [G, G] = \{1\}$$

  Por lo que la serie derivada es:

  $$G \rhd G' = \{1\}$$

- S_3 es resoluble:

  $$\begin{aligned} S_3' &= [S_3, S_3] = A_3 \\ S_3'' &= A_3' = [A_3, A_3] = \{1\} \end{aligned}$$

  Y la serie derivada es:

  $$S_3 \rhd A_3 \rhd \{1\}$$

- A_4 es resoluble:

  $$\begin{aligned} A_4' &= [A_4, A_4] = V \\ A_4'' &= V' = [V, V] = \{1\} \end{aligned}$$

  Y la serie derivada es:

  $$A_4 \rhd V \rhd \{1\}$$

- S_4 es resoluble, ya que $S_4' = [S_4, S_4] = A_4$ y ya tenemos la serie de A_4:

  $$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

  En general, si G es un grupo cuyo grupo derivado es resoluble, entonces G será resoluble.

- A_5 no es resoluble:
$$A_5' = [A_5, A_5] \neq \{1\}$$
Ya que A_5 no es abeliano, pero como A_5 es simple, no tiene subgrupos normales propios, con lo que $A_5' = A_5$. La serie derivada será:
$$A_5 \rhd A_5 \rhd A_5 \rhd \ldots$$
En general, ningún grupo no abeliano y simple es resoluble.

- S_n no es resoluble para $n \geqslant 5$, ya que:
$$[S_n, S_n] = A_n \qquad \forall n \geqslant 3$$
Y como ya vimos lo que le pasa a A_n para $n \geqslant 5$, la serie derivada de S_n será:
$$S_n \rhd A_n \rhd A_n \rhd \ldots$$

Teorema 1.11 (Caracterización de grupos resolubles para grupos finitos)**.**
Si G es un grupo finito, son equivalentes:

i) *G es resoluble.*

ii) *G tiene una serie normal con factores abelianos.*

iii) *Los factores de composición de G son cíclicos de orden primo.*

iv) *G tiene una serie normal con factores cíclicos.*

Demostración. Veamos todas las implicaciones:

$i) \Longrightarrow ii)$ Si G es resoluble, la serie derivada será de la forma:
$$G = G^0 \rhd G' \rhd \ldots \rhd G^{(r)} = \{1\}$$
Que es una serie normal con factores abelianos, ya que los factores son de la forma:
$$G^{(k-1)}/G^{(k)} = G^{(k-1)}/\left[G^{(k-1)}, G^{(k-1)}\right]$$
Que ya vimos en la Proposición 1.10 que siempre era un grupo abeliano.

$ii) \Longrightarrow iii)$ Si tenemos una serie normal con factores abelianos:
$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{1\}$$
Por el Teorema de Jordan-Holder, podemos refinarla a una serie de composición, donde nos fijaremos ahora en lo que pasa entre dos eslabones de la serie original:
$$\ldots \rhd G_r \rhd H_{r1} \rhd H_{r2} \rhd \ldots \rhd H_{rs} \rhd G_{r+1} \rhd \ldots$$
Por hipótesis los factores son abelianos, es decir, los grupos:
$$G_{k-1}/G_k \qquad \forall k \in \{1, \ldots, s\}$$

son abelianos. Por consiguiente, como todo subgrupo de un grupo abeliano también es abeliano, tenemos que los siguientes cocientes también son abelianos:

$$H_{r1}/G_{r+1} \quad H_{r2}/G_{r+1} \quad \cdots \quad H_{rs}/G_{r+1} \quad < \quad G_r/G_{r+1}$$

Por tanto, los factores:

$$G_r/H_{r1} \cong \frac{G_r/G_{r+1}}{H_{r1}/G_{r+1}}$$
$$H_{r1}/H_{r2} \cong \frac{H_{r1}/G_{r+1}}{H_{r2}/G_{r+1}}$$
$$\vdots$$
$$H_{rs-1}/H_{rs} \cong \frac{H_{rs-1}/G_{r+1}}{H_{rs}/G_{r+1}}$$

Son abelianos, por ser isomorfos a un cociente de un grupo abeliano. En definitiva, todos los factores de composición son abelianos, finitos y simples (por ser factores de composición), luego son cíclicos de orden primo, por la Proposición 1.1.

iii) $\Longrightarrow$ *iv)* Como las series de composición son, en particular, series normales, cualquier[3] serie de composición de G será normal con factores cíclicos.

iv) $\Longrightarrow$ *i)* Consideramos una serie normal con factores cíclicos (luego abelianos):

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Veamos que $G^{(k)} < G_k$, para todo $k \in \{1, \ldots, r\}$: como G_{k-1}/G_k es abeliano por ser un factor, entonces por la Proposición 1.10:

$$[G_{k-1}, G_{k-1}] = G^{(k)} < G_k$$

En particular:

$$G^{(r)} < G_r = \{1\}$$

Y tenemos ya que la serie derivada alcanza el mínimo:

$$G = G^0 \rhd G' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Por lo que G es resoluble.

□

Ejemplo. Aplicaciones del Teorema son:

- Vimos ya que S_4 era resoluble, veámoslo de otra forma:

$$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

Es una serie normal con factores cíclicos abelianos:

$$S_4/A_4 \qquad A_4/V \qquad V/\{1\}$$

[3]Gracias al Teorema de Jordan-Holder.

- En D_n:
$$D_n \rhd \langle r \rangle \rhd \{1\}$$
Es una serie normal con factores cíclicos abelianos, luego D_n es resoluble.

Una estrategia muy usada a la hora de comprobar si un grupo es resoluble o no es buscar si nuestro grupo tiene un subgrupo normal resoluble que haga que el cociente sea resoluble, con lo que podemos aplicar el tercer apartado de la siguiente Proposición:

Proposición 1.12. *Se verifica que:*

i) *Todo subgrupo de un grupo resoluble es resoluble.*

ii) *Todo cociente de un grupo resoluble es resoluble.*

iii) *Si $N \lhd G$ y N y G/N son resolubles, entonces G es resoluble.*

Demostración. Veamos cada una:

i) Supongamos que la serie derivada de G es:
$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(r)} = \{1\}$$
Si $H < G$, entonces $H^{(k)} < G^{(k)}$ para todo $k \in \{1, \ldots, r\}$. Como tenemos que $G^{(r)} = \{1\}$, tendremos que $H^{(r)} = \{1\}$, por lo que H es resoluble.

ii) Supuesto que G es resoluble con la serie anterior, consideramos $N \lhd G$. Por inducción, tendremos que:
$$\left({}^{G}\!/\!_{N}\right)^{(k)} = {}^{G^{(k)}N}\!/\!_{N}$$
Y como $G^{(r)} = \{1\}$, entonces:
$$\left({}^{G}\!/\!_{N}\right)^{(r)} = \{1\} \Longrightarrow G/N \text{ resoluble}$$

iii) Si $N \lhd G$ y G/N son resolubles: por ser G/N resoluble, entonces $\exists s$ de forma que:
$${}^{G^{(s)}N}\!/\!_{N} = \left({}^{G}\!/\!_{N}\right)^{(s)} = \{1\}$$
En dicho caso:
$$G^{(s)} < N$$
Y como N es resoluble, $\exists t$ de forma que $N^{(t)} = \{1\}$. En dicho caso:
$$G^{(s+t)} < N^{(t)} = \{1\}$$

□

Para concluir los resultados sobre grupos resolubles, veamos qué pasa con el producto de grupos resolubles:

Corolario 1.12.1. *Cualquier producto finito de grupos resolubles es resoluble.*

Demostración. Suponiendo que G_1 y G_2 son resolubles, cada uno tendrá su serie derivada. Tenemos:

$$G_2 \cong \{1\} \times G_2 < G_1 \times G_2$$

Con $\{1\} \times G_2$ resoluble por ser isomorfo a G_2. Además, $\{1\} \times G_2 \lhd G_1 \times G_2$. Busquemos el cociente:

$$G_1 \times G_2 / \{1\} \times G_2 \cong G_1$$

Que es resoluble, por lo que usando el apartado 3 de la Proposición superior, concluimos que $G_1 \times G_2$ es resoluble.

Por hipótesis de inducción, fijada una coordenada, movemos todas las demás. $\square$

2. $G-$conjuntos y p-grupos

Definición 2.1. Sea G un grupo y X un conjunto no vacío, una acción[1] de G sobre X es una aplicación:

$$\begin{array}{rccc} ac: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & ac(g,x) \end{array}$$

Que verifica:

i) $ac(1,x) = x \quad \forall x \in X$.

ii) $ac(g, ac(h,x)) = ac(gh,x) \quad \forall x \in X, \quad \forall g,h \in G$.

En dicho caso, diremos que G actúa[2] (o que opera) sobre X.

Si G actúa sobre X, diremos que este conjunto X es el $G-$conjunto a izquierda. A la aplicación ac se le llama aplicación de la $G-$estructura.

Notación. Si $ac : G \times X \to X$ es una acción de G sobre X, es común denotar:

$$ac(g,x) = {}^g x = g \cdot x = g * x$$

En este documento, usaremos la notación $ac(g,x) = {}^g x$.

Ejemplo. Ejemplos de acciones son:

1. Tenemos la <u>acción trivial</u>: $ac : G \times X \to X$ dada por $ac(g,x) = x \ \forall g \in G, x \in X$.

2. La <u>acción por restricción</u> de un subgrupo $H < G$ sobre X

$$\begin{tikzcd} ac : H \times X \arrow[rr] \arrow[dr, "i_{X1}"'] & & X \\ & G \times X \arrow[ur, "ac_G"'] & \end{tikzcd}$$

3. La <u>acción natural</u> de S_n sobre $X = \{1, \ldots, n\}$ será:

$$\begin{gathered} ac : S_n \times X \to X \\ (\sigma, i) \longmapsto ac(\sigma, i) = {}^\sigma i = \sigma(i) \end{gathered}$$

[1] En realidad esta es la definición de acción por la izquierda, pero no vamos a trabajar con las acciones por la derecha, por lo que hablaremos simplemente de acciones.

[2] En realidad deberíamos decir que "G actúa por la izquierda sobre X".

Proposición 2.1. *Sea G un grupo y X un conjunto no vacío, dar una acción de G sobre X equivale a dar un homomorfismo de grupos de G en* $\mathrm{Perm}(X)$.

Demostración. Veamos que es posible:

- Por una parte, dada una acción de G sobre X, $ac : G \times X \to X$, podemos definir la aplicación:
$$\begin{array}{rccc} \phi: & G & \longrightarrow & \mathrm{Perm}(X) \\ & g & \longmapsto & \phi(g) \end{array}$$
Donde $\phi(g)$ es una aplicación $\phi(g) : X \longrightarrow X$ dada por:
$$\phi(g)(x) = {}^g x \qquad \forall x \in X$$
Veamos en primer lugar que ϕ está bien definida, es decir, que $\phi(g) \in \mathrm{Perm}(X)$ para cada $g \in G$. Para ello, veamos antes que ϕ cumple:
  - $\phi(1) = id_X$, ya que la aplicación $x \mapsto ac(1, x)$ es la aplicación identidad en X, por ser ac una acción de G sobre X.
  - $\phi(g)\phi(h) = \phi(gh)$, ya que al evaluar en cualquier $x \in G$:
  $$(\phi(g)\phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)({}^h x) = {}^g({}^h x) \overset{(*)}{=} {}^{gh}x = \phi(gh)(x)$$
  Donde en $(*)$ hemos usado que ac es una acción de G sobre X.

  Ahora, veamos que dado $g \in G$, la aplicación $\phi(g)$ es biyectiva (es decir, está en $\mathrm{Perm}(X)$), ya que su aplicación inversa es $\phi(g^{-1})$:
$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$
  Y anteriormente vimos que $\phi(1) = id_X$, por lo que $\phi(g) \in \mathrm{Perm}(X)$, para todo $g \in G$ y la aplicación ϕ está bien definida.

  Además, por las dos propiedades anteriores, tenemos que ϕ es un homomorfismo de grupos.

- Sea $\phi : G \to \mathrm{Perm}(X)$ un homomorfismo de grupos, definimos la acción $ac : G \times X \to X$ dada por:
$$ac(g, x) = \phi(g)(x) = {}^g x \qquad \forall g \in G, x \in X$$
Veamos que es una acción:
$$\begin{aligned} {}^1x &= \phi(1)(x) = x \\ {}^g({}^h x) &= \phi(g)(\phi(h)x) = \phi(gh)(x) = {}^{(gh)}x \end{aligned}$$

Este homomorfismo ϕ se conoce como la representación de G por permutaciones. □

Podemos calcular el núcleo de ϕ, que recibirá el nombre núcleo de la acción.
$$\ker(\phi) = \{g \in G \mid \phi(g) = id_X\} = \{g \in G \mid {}^g x = x \quad \forall x \in X\}$$

Definición 2.2. Si $\ker(\phi) = \{1\}$, decimos que la acción es fiel.

Ejemplo. Ejemplos de representaciones por permutaciones de acciones son:

1. Si consideramos la acción trivial, la representación de G por permutaciones será:
$$\phi(g) = id_X$$
2. En la acción por restricción, sea $H \subseteq G$:
$$\begin{tikzcd} H \arrow[r, "i"] \arrow[rr, bend right, "\phi_H"'] & G \arrow[r, "\phi"] & Perm(X) \end{tikzcd}$$
3. En el caso de la acción natural, $\phi(g) = id_X$.
4. En el caso de la acción de D_4 sobre $X = \{1, 2, 3, 4\}$:
$$ac : G \times X \to X$$
$$ac(g, x) = {}^g x = \phi(g)(x)$$
Tendremos:
$$\phi : G \to \text{Perm}(X) = S_4$$
$$\phi(r) = (1\ 2\ 3\ 4)$$
$$\phi(s) = (2\ 4)$$
ϕ es inyectiva, por lo que será una acción fiel.

   A partir de ahora, consideramos $X = G$.
5. La acción por traslación se define como:
$$ac : G \times G \to G$$
$$ac(g, h) = {}^g h = gh$$
La representación asociada será:
$$\phi : G \to \text{Perm}(X)$$
$$\phi(g)(h) = gh$$
$\{g \in G \mid gh = h \quad \forall h \in G\} = \ker(\phi) = \{1\}$, por lo que se trata de una acción fiel.

Teorema 2.2 (Cayley)**.** *Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración.
$$\phi / \ker(\phi) \cong Im(\phi)$$
De donde $\phi \cong Im(\phi)$, por ser una acción fiel. □

Ejemplo. Podemos considerar las traslaciones de G sobre conjuntos especiales:

- La acción por traslación de G sobre $\mathcal{P}(G)$ es:

$$ac : G \times \mathcal{P}(G) \to \mathcal{P}(G)$$
$$(g, A) \longmapsto ac(g, A) = {}^{g}A = gA = \{ga \mid a \in A\} \subseteq G$$

- Podemos también hacer la acción por traslación en el cociente por las clases laterales por la izquierda: si $H < G$, consideramos el cociente de G sobre $G/_{H}\sim$:

$$ac : G \times G/_{H}\sim \to G/_{H}\sim$$
$$ac(g, xH) = {}^{g}xH = gxH$$

6. La acción por conjugación se define como la aplicación

$$ac : G \times G \to G$$
$$ac(g, h) = {}^{g}h = ghg^{-1}$$

Que es una acción ya que:

$${}^{1}h = 1h1^{-1} = h$$
$${}^{g}({}^{h}l) = ghl(gh)^{-1} = g(hlh^{-1})g^{-1}$$

El homomorfismo asociado es:

$$\phi : G \to \text{Perm}(X)$$
$$\phi(g)(h) = ghg^{-1} \qquad \forall g, h \in G$$

Y a $\phi(g)$ lo llamábamos (en el ej 14 de la relación 4, φ_g) automorfismo interior definido por G, con imagen:

$$Im(\phi) = Int(G)$$

El núcleo en este caso es:

$$\ker(\phi) = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg \quad \forall h \in G\} = Z(G)$$

7. La acción por conjugación en partes de G se define como:

$$ac : G \times \mathcal{P}(G) \to \mathcal{P}(G)$$
$$ac(g, A) = {}^{g}A = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G$$

8. Podemos definir la acción por conjugación también de G sobre $Subg(G)$:

$$Subg(G) = \{H \subseteq G \mid H < G\}$$

$$ac : G \times Subg(G) \to Subg(G)$$
$$ac(g, H) = {}^{g}H = gHg^{-1} < G$$

A gHg^{-1} lo llamaremos subgrupo conjugado de G.