

Álgebra II

FACULTAD
DE
CIENCIAS
UNIVERSIDAD DE GRANADA



Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

Álgebra II

Los Del DGIIM, losdeldgiim.github.io

José Juan Urrutia Milán

Granada, 2025

Índice general

1. Grupos resolubles	5
1.1. Series de un grupo	5
1.1.1. Series de composición	7
1.1.2. Resultados sobre series de composición	12
1.2. Grupos resolubles	21
1.2.1. Preliminares	21
1.2.2. Definición	23
2. G-conjuntos y p-grupos	31
2.1. Órbitas de un elemento	35
2.1.1. Acción por traslación	40
2.1.2. Acción por conjugación	41
2.1.3. Acción por conjugación sobre subgrupos	44
2.2. p -grupos	45
2.2.1. p -subgrupos de Sylow	49
3. Clasificación de grupos abelianos finitos	57
3.1. Clasificación de grupos abelianos no finitos	63
3.1.1. Forma Normal de Smith de una matriz	66
4. Clasificación de grupos de orden bajo	73
4.1. Grupos abelianos	73
4.2. Producto semidirecto	73

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 con 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, \dots, G_r de forma que:

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

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:

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

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

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 $r \geq s$.

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

Ejemplo. En A_4 , podemos considerar la serie:

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

Un refinamiento propio 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 :

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

- 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:

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

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 grupos cocientes:

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

- Llamamos índices de la serie a los correspondientes órdenes de los factores.

Si $i_k = [G_{k-1} : G_k]$ 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:

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

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:

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

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

$$\begin{aligned} G &= G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\} \\ G &= H_0 \triangleright H_1 \triangleright \dots \triangleright H_s = \{1\} \end{aligned}$$

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

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

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

$$\begin{aligned} \mathbb{Z}/24\mathbb{Z} &\triangleright 2\mathbb{Z}/24\mathbb{Z} \triangleright 4\mathbb{Z}/24\mathbb{Z} \triangleright 8\mathbb{Z}/24\mathbb{Z} \triangleright 24\mathbb{Z}/24\mathbb{Z} = \{0\} \\ \mathbb{Z}/24\mathbb{Z} &\triangleright 3\mathbb{Z}/24\mathbb{Z} \triangleright 6\mathbb{Z}/24\mathbb{Z} \triangleright 12\mathbb{Z}/24\mathbb{Z} \triangleright 24\mathbb{Z}/24\mathbb{Z} = \{0\} \end{aligned}$$

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

$$\begin{aligned} \mathbb{Z}/24\mathbb{Z} &\stackrel{2}{\triangleright} 2\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 4\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 8\mathbb{Z}/24\mathbb{Z} \stackrel{3}{\triangleright} 24\mathbb{Z}/24\mathbb{Z} = \{0\} \\ \mathbb{Z}/24\mathbb{Z} &\stackrel{3}{\triangleright} 3\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 6\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 12\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 24\mathbb{Z}/24\mathbb{Z} = \{0\} \end{aligned}$$

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, ya que los índices no permiten introducir más subgrupos a la serie.
- Anteriormente vimos que la serie $A_4 \triangleright V \triangleright \{1\}$ no era de composición, ya que podíamos refinarla más: $A_4 \triangleright V \triangleright \langle (1 \ 2)(3 \ 4) \rangle \triangleright \{1\}$, 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 $\text{GL}_2(\mathbb{K})$ 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 $T \triangleright U \triangleright \{1\}$ 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:

$$T \triangleright U_1 \triangleright U_2 \triangleright \dots \triangleright U_n = I$$

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:

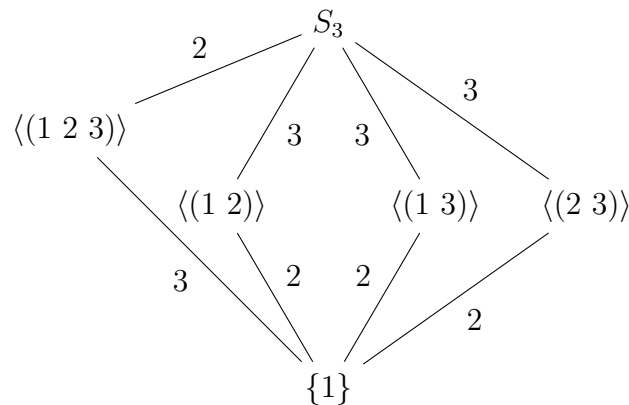


Figura 1.1: Diagrama de Hasse para los subgrupos de S_3 .

Como $A_3 = \langle (1\ 2\ 3) \rangle \triangleleft S_3$ (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:

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

- En D_4 :

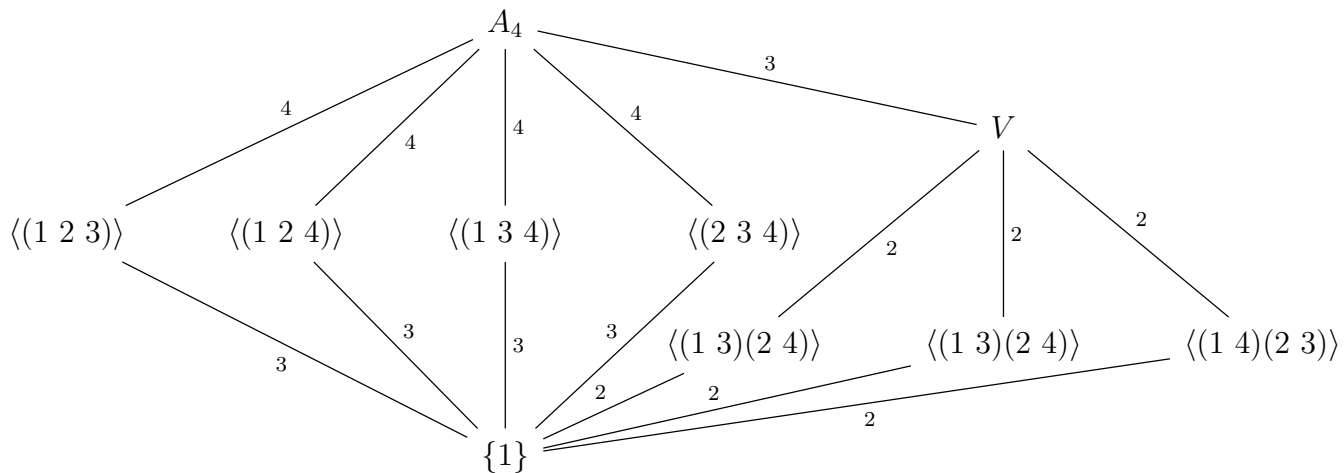


Figura 1.2: Diagrama de Hasse para los subgrupos de D_4 .

Como todos los índices del grafo son 2, todas las relaciones de inclusión mostradas en el grafo en realidad son relaciones de normalidad (\triangleleft), 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):

$$\begin{aligned}
 D_4 &\triangleright \langle r^2, s \rangle \triangleright \langle s \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, s \rangle \triangleright \langle sr^2 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, s \rangle \triangleright \langle r^2 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, sr \rangle \triangleright \langle r^2 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, sr \rangle \triangleright \langle sr \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, sr \rangle \triangleright \langle sr^3 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r \rangle \triangleright \langle r^2 \rangle \triangleright \{1\}
 \end{aligned}$$

■ Para A_4 :



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

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

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

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

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

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



Solo tenemos la serie de composición:

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

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:

$$Q_2 \triangleright \langle i \rangle \triangleright \langle -1 \rangle \triangleright \{1\}$$

$$Q_2 \triangleright \langle j \rangle \triangleright \langle -1 \rangle \triangleright \{1\}$$

$$Q_2 \triangleright \langle k \rangle \triangleright \langle -1 \rangle \triangleright \{1\}$$

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

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

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

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

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

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

Que obtenemos primero variando algunos y luego otras. Esto es posible ya que el producto de subgrupos es subgrupo del producto, como vimos en la Proposición ??.

Sin embargo, como $\text{mcd}(6, 2) = 2 \neq 1$, el Teorema ?? no puede asegurarnos que todos los subgrupos de $S_3 \times \mathbb{Z}_2$ sean producto de subgrupos, y de hecho vamos a tener que hay subgrupos del producto que no son producto de subgrupos de cada coordenada, por lo que tendremos otra serie de composición, que tendrá la forma:

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

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 $n \geq 5$ son grupos simples.

1.1.2. Resultados sobre series de composición

Proposición 1.1 (Caracterización de los grupos abelianos simples).

Un grupo es abeliano y simple si y solo si es de orden primo.

Demostración. Por doble implicación:

\Leftarrow) Si G es un grupo de orden p primo, vimos en la Proposición ?? que entonces es cíclico, luego abeliano. Además, por ser de orden primo, no tendrá subgrupos propios (ya que sus órdenes serían distintos de p y de 1 y dividirían a p), por lo que también será simple.

\Rightarrow) 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.

Veamos ahora que G es finito: como vimos en el Teorema ??, G ha de ser isomorfo a \mathbb{Z} o a \mathbb{Z}_n para algún $n \in \mathbb{N}$. Supongamos que G no es finito, con lo que $G \cong \mathbb{Z}$, pero G es simple (por hipótesis) y \mathbb{Z} no, pues tiene subgrupos propios (por ejemplo, $2\mathbb{Z}$). Como la propiedad de “ser simple” se preserva por isomorfismos, G no puede ser isomorfo a \mathbb{Z} , luego tendremos que $G \cong \mathbb{Z}_n$ para algún $n \in \mathbb{N}$, por lo que G es finito.

Veamos ahora que $|G|$ es primo. Si no lo fuese, tendríamos $|G| = nm$. 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.

□

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

Proposición 1.2 (Caracterización de series de composición). *Sea G un grupo, una serie normal es de composición si y solo si sus factores son grupos simples.*

Demostración. Consideramos una serie normal de longitud r :

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

Y demostraremos que la serie no es de composición si y solo si tiene un factor que no es un grupo simple:

\Rightarrow) Si la serie no es de composición, podemos encontrar $H < G$ de forma que la serie:

$$G = G_0 \triangleright \dots \triangleright G_{k-1} \triangleright H \triangleright G_k \triangleright \dots \triangleright G_r = \{1\}$$

Sea un refinamiento normal propio de la serie de partida. Si consideramos la proyección al cociente de los grupos:

$$G_{k-1} \triangleright H \triangleright G_k$$

Llegamos a que:

$$p_*(G_{k-1}) = G_{k-1}/G_k \triangleright p_*(H) = H/G_k \triangleright p_*(G_k) = \{G_k\}$$

Y ninguna de estas inclusiones es una igualdad, ya que:

- Si $G_{k-1}/G_k = H/G_k$, entonces $G_{k-1} = H$ y el refinamiento anterior no era propio.
- Si $H/G_k = \{G_k\}$, entonces $H = G_k$ y el refinamiento anterior no era propio.

En definitiva, hemos encontrado un subgrupo normal propio de G_{k-1}/G_k , por lo que este factor no es un grupo simple.

\Leftarrow) Si existe $k \in \{1, \dots, r\}$ de forma que G_{k-1}/G_k no es un grupo simple, entonces dicho grupo tendrá un subgrupo propio normal suyo:

$$\{G_k\} = \{1\} \neq H \triangleleft G_{k-1}/G_k$$

Si usamos el Tercer Teorema de Isomorfía considerando la proyección al cociente $p_k : G_{k-1} \rightarrow G_{k-1}/G_k$, tenemos que:

$$p_k^*(H) \triangleleft G_{k-1}$$

Además, como $H < G_{k-1}/G_k$, tendremos que $G_k \in H$, luego:

$$G_k = \ker(p_k) = p_k^*(\{G_k\}) \subseteq p_k^*(H) \triangleleft G_{k-1}$$

Y por ser $G_k \triangleleft G_{k-1}$, deducimos que también $G_k \triangleleft p_k^*(H)$. Hemos encontrado un subgrupo normal de G que estaría entre G_k y G_{k-1} :

$$G = G_0 \triangleright \dots \triangleright G_{k-1} \triangleright p_k^*(H) \triangleright G_k \triangleright \dots \triangleright G_r = \{1\}$$

Además, este refinamiento de la serie normal es propio, ya que:

- Si fuese $p_k^*(H) = G_k$, tendríamos que $H = \{G_k\}$.
- Si fuese $p_k^*(H) = G_{k-1}$, tendríamos que $H = G_{k-1}/G_k$.

Ambos casos son imposibles, puesto que H era un subgrupo propio de G_{k-1}/G_k . Hemos encontrado un refinamiento normal propio de la serie de partida, por lo que esta no era de composición.

□

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

Demostración. Sea G un grupo finito, distinguimos casos:

- Si G es simple o trivial, entonces no tiene subgrupos normales propios, por lo que tiene una única serie de composición:

$$G \triangleright \{1\}$$

- Si $|G| = p$ primo, 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 maximal¹ de G . Como $|G_1| < |G|$ (G_1 es subgrupo propio), por hipótesis de inducción tenemos una serie de composición para G_1 :

$$G_1 \triangleright G_2 \triangleright \dots \triangleright G_r = \{1\}$$

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

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_r = \{1\}$$

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 :

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{i-1} \triangleright G_i \triangleright \dots \triangleright G_r = \{1\} \quad (1.3)$$

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_{j-1} \triangleright H_j \triangleright \dots \triangleright H_s = \{1\} \quad (1.4)$$

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

$$G_{ij} = G_i(H_j \cap G_{i-1}) \triangleleft G_i(H_{j-1} \cap G_{i-1}) = G_{ij-1} \quad \forall j \in \{1, \dots, s\}$$

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

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

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

$$G_{i-1} = G_{i0} \triangleright G_{i1} \triangleright \dots \triangleright G_{is-1} \triangleright G_{is} = G_i$$

Que podemos meter en todos los eslabones de la serie (1.3):

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

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.

¹Es decir, que no existe $G_1 \neq K \triangleleft G$ con $G_1 \triangleleft K$.

Si repetimos el procedimiento para la serie (1.4), 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:

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

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:

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

Y podemos obtener un refinamiento de (1.4) al igual que hicimos antes, metiendo la cadena superior entre cada uno de los eslabones de la serie original:

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

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. \square

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

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

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 :

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

Y también una serie normal de G :

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

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:

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

Por tanto, tendremos que $\exists \sigma \in S_r$ de forma que:

$$G_k/G_{k+1} \cong \overline{G_{\sigma(k)}}/\overline{G_{\sigma(k)+1}} \quad \forall k \in \{0, \dots, r-1\}$$

Como la primera serie era de composición, los factores G_k/G_{k+1} son simples, y como esta propiedad se conserva por isomorfismos (compruébese), los factores $\overline{G_k}/\overline{G_{k+1}}$ también serán simples, de donde deducimos que el refinamiento de la serie normal que hemos encontrado es de composición. \square

Con este último Teorema de Jordan-Holder se tiene claro ya el interés en las series de composición, ya que cada grupo admite una 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 isomorfas, una de un grupo G y otra de otro grupo K , 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:

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

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

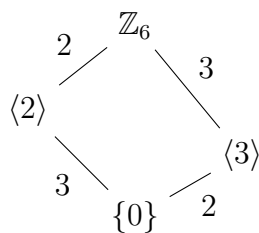


Figura 1.4: Diagrama de Hasse para los subgrupos de \mathbb{Z}_6 .

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

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

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. Vemos finalmente que las series:

$$\begin{aligned} S_3 &\stackrel{2}{\triangleright} A_3 \stackrel{3}{\triangleright} \{1\} \\ \mathbb{Z}_6 &\stackrel{2}{\triangleright} \langle 2 \rangle \stackrel{3}{\triangleright} \{0\} \end{aligned}$$

son isomorfas. Para ello, basta ver que:

$$\begin{aligned} S_3/A_3 &\cong \mathbb{Z}_2 \cong \mathbb{Z}_6/\langle 2 \rangle \\ A_3/\{1\} &\cong A_3 \cong \mathbb{Z}_3 \cong \langle 2 \rangle \cong \langle 2 \rangle/\{0\} \end{aligned}$$

Veamos ahora que dos grupos isomorfos siempre tienen una serie de composición isomorfa. Sin embargo, antes de ello, hemos de destacar un resultado que no vimos en el Capítulo anterior pero que puede demostrarse fácilmente con las herramientas introducidas en el mismo.

Lema 1.6. Sean G y K dos grupos, $f : G \rightarrow K$ un isomorfismo de grupos y $H \triangleleft G$, entonces:

$$G/H \cong K/f_*(H)$$

Demostración. En primer lugar, hemos de demostrar que $f_*(H) \triangleleft K$. Para ello:

- Como $H < G$ y f es un homomorfismo, por la Proposición ??, tenemos que $f_*(H) < K$.
- Ahora, si $y \in K$ y $h' \in f(H)$, existirán $x \in G$ y $h \in H$ de forma que:

$$f(x) = y \quad f(h) = h'$$

En cuyo caso:

$$yh'y = f(x)f(h)(f(x))^{-1} = f(xhx^{-1}) \in f(H)$$

Ya que por ser $H \triangleleft G$, tenemos que $xhx^{-1} \in H$.

Ahora, podemos considerar los grupos cocientes G/H y $K/f_*(H)$, junto con las proyecciones $p_G : G \rightarrow G/H$ y $p_K : K \rightarrow K/f_*(H)$. Si definimos $g : G \rightarrow K/f_*(H)$ como $g = p_K \circ f$:

$$g(x) = p_K(f(x)) = f(x)f_*(H) \quad \forall x \in G$$

Es un homomorfismo, como composición de homomorfismos. Si observamos el siguiente diagrama:

$$\begin{array}{ccc} G & \xrightarrow{p_G} & G/H \\ f \downarrow & \searrow g & \downarrow \varphi \\ K & \xrightarrow{p_K} & K/f_*(H) \end{array}$$

Figura 1.5: Situación de los grupos.

Podemos aplicar la Propiedad Universal del grupo cociente sobre g , obteniendo que existe un único homomorfismo $\varphi : G/H \rightarrow K/f_*(H)$ que hace que el diagrama conmute. Como vimos en el Teorema ??:

- Como g es sobreyectiva por ser composición de aplicaciones sobreyectivas, tenemos que φ es sobreyectiva.
- Calculemos $\ker(g)$, sea $x \in \ker(g)$:

$$f(x)f_*(H) = p_K(f(x)) = g(x) = f_*(H)$$

Entonces, $f(x) \in f_*(H)$, de donde $x \in H$. La inclusión $H \subseteq \ker(g)$ es clara, por lo que $H = \ker(g)$, de donde deducimos que φ es inyectiva.

□

Proposición 1.7. 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 .

Demostración. Como todas las series de composición de G son isomorfas entre sí y todas las series de composición de K también (por el Teorema de Jordan-Holder), basta ver que hay una serie de composición de G que es isomorfa a una serie de composición de K . Para ello, como $G \cong K$, ha de existir un isomorfismo de grupos $f : G \rightarrow K$. Sea

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

una serie de composición de G , si denotamos:

$$H_k = f_*(G_k) \quad \forall k \in \{0, \dots, r\}$$

Tendremos entonces una serie normal en K :

$$K = H_0 \triangleright H_1 \triangleright \dots \triangleright H_r = \{1\}$$

Por el Lema anterior, tenemos que:

$$G_k/G_{k+1} \cong H_k/H_{k+1} \quad \forall k \in \{0, \dots, r-1\}$$

Además, como la serie de G era de composición, sus factores serán grupos simples, de donde los factores H_k/H_{k+1} serán también grupos simples, por lo que la serie obtenida en K es de composición, y son series isomorfas. □

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 Gorenstein (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 $n \geq 5$.

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

Teorema 1.8 (de Abel). A_n es simple, para $n \geq 5$.

Demostración. Sea $\{1\} \neq N \triangleleft A_n$, veamos que ha de ser $N = A_n$. En la Proposición ?? vimos que dado² $j \in X_n \setminus \{1, 2\}$, 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:

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 $N \triangleleft A_n$. 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 .

²Donde $X_n = \{1, 2, \dots, n\}$.

- 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 , si definimos:

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

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, $\exists h$ distinto de los anteriores de forma que:

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

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

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

□

1.2. Grupos resolubles

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

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

1.2.1. Preliminares

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

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

Proposición 1.9. Sea G un grupo y $x, y \in G$, se verifican:

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

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

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 1.10. 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, por la definición de subgrupo generado por un subconjunto, es claro que $\Lambda < G$. Para ver la normalidad, sea $\lambda \in \Lambda$ y $z \in G$, existirán $x_1, \dots, x_n, y_1, \dots, y_n \in G$ y $\gamma_1, \dots, \gamma_n \in \{\pm 1\}$ de forma que:

$$\lambda = ([x_1, y_1])^{\gamma_1} \dots ([x_n, y_n])^{\gamma_n}$$

Por lo que:

$$\begin{aligned} z\lambda z^{-1} &= z([x_1, y_1])^{\gamma_1} \dots ([x_n, y_n])^{\gamma_n} z^{-1} = z([x_1, y_1])^{\gamma_1} z^{-1} z \dots z^{-1} z ([x_n, y_n])^{\gamma_n} z^{-1} \\ &= ([zx_1z^{-1}, zy_1z^{-1}])^{\gamma_1} \dots ([zx_nz^{-1}, zy_nz^{-1}])^{\gamma_n} \end{aligned}$$

Ya que para los γ_k positivos tendremos que:

$$z([x_k, y_k])^{\gamma_k} z^{-1} = [zx_k z^{-1}, zy_k z^{-1}] = ([zx_k z^{-1}, zy_k z^{-1}])^{\gamma_k}$$

Y para los γ_k negativos tendremos:

$$z([x_k, y_k])^{\gamma_k} z^{-1} = [zy_k z^{-1}, zx_k z^{-1}] = ([zx_k z^{-1}, zy_k z^{-1}])^{\gamma_k}$$

□

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 1.11. 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 $N \triangleleft G$:

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

$G/[G, G]$ 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:

\implies) Si consideramos la proyección al cociente $p : G \rightarrow G/N$, sean $x, y \in G$, observemos que:

$$\begin{aligned} p([x, y]) &= p(xy(yx)^{-1}) = p(xy)p((yx)^{-1}) = p(x)p(y)(p(yx))^{-1} \\ &= p(x)p(y)(p(y)p(x))^{-1} \stackrel{(*)}{=} p(x)p(y)(p(y))^{-1}(p(x))^{-1} = 1 \end{aligned}$$

Donde en $(*)$ hemos usado que G/N es abeliano. De esta forma, vemos que $[x, y] \in \ker(p) = N$, para todo $x, y \in G$, de donde $[G, G] < N$.

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

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

Por lo que $xy(yx)^{-1}N = N$, y si multiplicamos por yxN a la derecha obtenemos que:

$$(xN)(yN) = xyN = yxN = (yN)(xN)$$

Como x e y eran arbitrarios, concluimos que G/N es abeliano.

□

Corolario 1.11.1. Si G es un grupo:

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

Demostración. Como $G \cong G/\{1\}$:

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

□

Lema 1.12. Sea B un grupo y $A < B$, entonces $[A, A] < [B, B]$.

Demostración. Por la definición del subgrupo conmutador, si definimos:

$$S_A = \{[x, y] \mid x, y \in A\}$$

$$S_B = \{[x, y] \mid x, y \in B\}$$

De la relación $A \subseteq B$ tenemos que $S_A \subseteq S_B$, y como:

$$[A, A] = \langle S_A \rangle \quad [B, B] = \langle S_B \rangle$$

Tendremos que $[A, A] \subseteq [B, B]$, de donde $[A, A] < [B, B]$.

□

1.2.2. Definición

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

$$G = G^0 \triangleright G' \triangleright G'' \triangleright \dots \triangleright G^{(k)} \triangleright \dots$$

Donde:

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \quad \forall k \in \mathbb{N}$$

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 resoluble si existe un índice k de forma que $G^{(k)} = \{1\}$. Es decir, la serie derivada de G alcanza el $\{1\}$.

Ejercicio. Se pide comprobar que:

$$[A_3, A_3] = \{1\} \quad [S_3, S_3] = A_3 \quad [A_4, A_4] = V \quad [S_n, S_n] = A_n \quad n \geq 3$$

Ejemplo. Veamos ejemplos de grupos que son resolubles, y de algunos que no lo son.

- Si G es abeliano, entonces G es resoluble, ya que:

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

Por lo que la serie derivada de cualquier grupo abeliano G es:

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

- S_3 es resoluble, ya que:

$$\begin{aligned} S'_3 &= [S_3, S_3] = A_3 \\ S''_3 &= A'_3 = [A_3, A_3] = \{1\} \end{aligned}$$

Y la serie derivada es:

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

- 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:

$$A_4 \triangleright V \triangleright \{1\}$$

- S_4 es resoluble, ya que $S'_4 = [S_4, S_4] = A_4$ y ya tenemos la serie de A_4 :

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

En general, si G es un grupo de forma que su k -ésimo grupo derivado es resoluble para cierto $k \in \mathbb{N}$, 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 ha de ser $A'_5 = A_5$. La serie derivada será por tanto:

$$A_5 \triangleright A_5 \triangleright A_5 \triangleright \dots$$

En general, ningún grupo no abeliano y simple es resoluble.

- S_n no es resoluble para $n \geq 5$, ya que:

$$[S_n, S_n] = A_n \quad \forall n \geq 3$$

Y como ya vimos lo que le pasa a A_n para $n \geq 5$, la serie derivada de S_n será:

$$S_n \triangleright A_n \triangleright A_n \triangleright \dots$$

Teorema 1.13 (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:

$i) \implies ii)$ Si G es resoluble, la serie derivada será de la forma:

$$G = G^0 \triangleright G' \triangleright \dots \triangleright G^{(r)} = \{1\}$$

Que es una serie normal con factores abelianos, ya que los factores son de la forma:

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

Que ya vimos en la Proposición 1.11 que siempre era un grupo abeliano.

$ii) \implies iii)$ Si tenemos una serie normal con factores abelianos:

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

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:

$$\dots \triangleright G_r \triangleright H_{r1} \triangleright H_{r2} \triangleright \dots \triangleright H_{rs} \triangleright G_{r+1} \triangleright \dots$$

Por hipótesis los factores son abelianos, es decir, los grupos:

$$G_{k-1}/G_k \quad \forall k \in \{1, \dots, s\}$$

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

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

Por tanto, los factores:

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

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.

$iii) \implies iv)$ Como las series de composición son, en particular, series normales, cualquier³ serie de composición de G será normal con factores cíclicos.

³Gracias al Teorema de Jordan-Holder.

$iv) \implies i)$ Consideramos una serie normal con factores cíclicos:

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

Donde los grupos G_k/G_{k+1} son cíclicos, para todo $k \in \{0, \dots, r-1\}$, luego abelianos. Veamos que $G^{(k)} < G_k$, para todo $k \in \{1, \dots, r\}$:

- Para $k = 1$: como el cociente G/G_1 es abeliano, tenemos por la Proposición 1.11 que $G' = [G, G] < G_1$.
- Supuesto que $G^{(k)} < G_k$, veámoslo para $k + 1$: Como tenemos por hipótesis que $G^{(k)} < G_k$, si consideramos el grupo derivado a ambos lados gracias al Lema 1.12, tendremos que:

$$G^{(k+1)} = (G^{(k)})' < G'_k = [G_k, G_k]$$

Y finalmente, como el cociente G_k/G_{k+1} es abeliano, deducimos por la Proposición anterior que $G'_k = [G_k, G_k] < G_{k+1}$. En definitiva, tenemos $G^{(k+1)} < G_{k+1}$.

Una vez probado esto, en particular, tenemos que:

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

De donde deducimos que el r -ésimo grupo derivado de G es trivial, con lo que G es resoluble.

□

Observación. Notemos que en el Teorema superior podríamos haber demostrado que $i) \iff ii)$ para cualquier grupo G (no necesariamente finito):

- En la demostración $i) \implies ii)$ no se usó que G era finito.
- En la demostración $iv) \implies i)$ en realidad no se usó que G tuiera una serie normal con factores cíclicos, sino que las hipótesis puede relajarse a que G tenga una serie normal con factores abelianos. Además, en esta tampoco usamos que G era finito.

Ejemplo. Aplicaciones del Teorema son:

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

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

Es una serie normal con factores cíclicos abelianos:

$$S_4/A_4 \cong \mathbb{Z}_2 \quad A_4/V \cong \mathbb{Z}_2 \quad V/\{1\} \cong V \text{ abeliano}$$

- En D_n :

$$D_n \triangleright \langle r \rangle \triangleright \{1\}$$

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, para la cual hemos de introducir dos Lemas previos.

Lema 1.14. *Sea G un grupo, $H < G$ y $N \triangleleft G$, entonces:*

$$\left[\frac{HN}{N}, \frac{HN}{N} \right] = \frac{[H, H]N}{N}$$

Lema 1.15. *Sea G un grupo y $N \triangleleft G$, entonces:*

$$\left(\frac{G}{N} \right)^{(k)} = \frac{G^{(k)}N}{N} \quad \forall k \in \mathbb{N}$$

Demostración. Por inducción sobre $k \in \mathbb{N}$:

- Para $k = 0$, como $G = GN$ y $G = G^{(0)}$, tendremos que:

$$\frac{G}{N} = \frac{GN}{N}$$

- Supuesto para k , para $k + 1$:

$$\begin{aligned} \left(\frac{G}{N} \right)^{(k+1)} &= \left(\left(\frac{G}{N} \right)^{(k)} \right)' = \left[\left(\frac{G}{N} \right)^{(k)}, \left(\frac{G}{N} \right)^{(k)} \right] \stackrel{(*)}{=} \left[\frac{G^{(k)}N}{N}, \frac{G^{(k)}N}{N} \right] \\ &\stackrel{(**)}{=} \frac{[G^{(k)}, G^{(k)}]N}{N} = \frac{G^{(k+1)}N}{N} \end{aligned}$$

Donde en $(*)$ usamos la hipótesis de inducción y en $(**)$ el Lema anterior. \square

Proposición 1.16. *Se verifica que:*

- i) Todo subgrupo de un grupo resoluble es resoluble.*
- ii) Todo cociente de un grupo resoluble es resoluble.*
- iii) Si $N \triangleleft G$ y N y G/N son resolubles, entonces G es resoluble.*

Demostración. Veamos cada una:

- i)* Supongamos que la serie derivada de G es:

$$G = G^0 \triangleright G' \triangleright G'' \triangleright \dots \triangleright G^{(r)} = \{1\}$$

Si $H < G$, entonces $H^{(k)} < G^{(k)}$ para todo $k \in \{1, \dots, r\}$, gracias al Lema 1.12. Como tenemos que $G^{(r)} = \{1\}$, tendremos que $H^{(r)} = \{1\}$, por lo que H es resoluble.

ii) Supuesto que G es resoluble, su serie derivada será de la forma:

$$G = G^0 \triangleright G' \triangleright \dots \triangleright G^{(r)} = \{1\}$$

Si consideramos $N \triangleleft G$, vimos en el Lema anterior que:

$$(G/N)^{(k)} = \frac{G^{(k)}N}{N} \quad \forall k \in \mathbb{N}$$

Y como $G^{(r)} = \{1\}$, tenemos que:

$$(G/N)^{(r)} = \frac{G^{(r)}N}{N} = \{1\}$$

De donde G/N es resoluble.

iii) Por ser G/N resoluble, sabemos que $\exists s \in \mathbb{N}$ de forma que:

$$\frac{G^{(s)}N}{N} = (G/N)^{(s)} = \{1\}$$

Por lo que tendremos $G^{(s)} < N$. Por ser N resoluble, $\exists t \in \mathbb{N}$ de forma que $N^{(t)} = \{1\}$. En dicho caso, tendremos que, aplicando el Lema 1.12:

$$G^{(s+t)} < N^{(t)} = \{1\}$$

Por lo que G es resoluble. □

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

Corolario 1.16.1. *Cualquier producto finito de grupos resolubles es resoluble.*

Demostración. Suponiendo que G_1 y G_2 son dos grupos resolubles, si consideramos:

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

Tenemos que $\{1\} \times G_2$ es resoluble, por ser $\{1\} \times G_2 \cong G_2$. Si observamos el cociente:

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

es resoluble, por ser G_1 resoluble. Por la Proposición anterior, concluimos que $G_1 \times G_2$ es resoluble. Por una sencilla inducción, lo demostramos para productos finitos de grupos resolubles. □

Proposición 1.17. *Sea G un grupo resoluble y $f : G \rightarrow H$ un homomorfismo, entonces $f(G)$ es resoluble.*

Demostración. Como G es resoluble, entonces tendrá una serie normal con factores abelianos:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = \{1\}$$

Como la imagen de grupos normales por homomorfismos conservan la normalidad (compruébese), tenemos:

$$f(G) = f(G_0) \triangleright f(G_1) \triangleright f(G_2) \triangleright \cdots \triangleright f(G_n) = f(\{1\}) = \{1\}$$

Veamos ahora que $f(G_k)/f(G_{k+1})$ es abeliano para todo $k \in \{0, \dots, n-1\}$. Como G_k/G_{k+1} es abeliano, para cada par $x_1, x_2 \in G_k$ se tiene que:

$$\begin{aligned} x_1x_2G_{k+1} = x_2x_1G_{k+1} &\implies x_1x_2(x_2x_1)^{-1} \in G_{k+1} \\ &\implies f(x_1x_2(x_2x_1)^{-1}) = f(x_1x_2)f(x_2x_1)^{-1} \in f(G_{k+1}) \\ &\implies f(x_1x_2)f(G_{k+1}) = f(x_2x_1)f(G_{k+1}) \\ &\implies f(x_1)f(x_2)f(G_{k+1}) = f(x_2)f(x_1)f(G_{k+1}) \end{aligned}$$

Por tanto, $f(G)$ es resoluble. □

2. G -conjuntos y p -grupos

Definición 2.1. Sea G un grupo y X un conjunto no vacío, una acción¹ de G sobre X es una aplicación:

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

Que verifica:

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

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

En dicho caso, diremos que G actúa² (o que opera) sobre X .

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

Notación. Si $ac : G \times X \rightarrow X$ 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 $ac(g, x) = {}^g x$. Con esta, las propiedades que ha de cumplir una aplicación $ac : G \times X \rightarrow X$ para ser una acción son:

$$i) \quad {}^1 x = x \quad \forall x \in X.$$

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

Ejemplo. Si G es un grupo y X es un conjunto no vacío, ejemplos de acciones de G sobre X son:

1. La acción trivial:

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

2. Si tenemos una acción $ac : G \times X \rightarrow X$ y $H < G$, podemos considerar la acción por restricción $ac : H \times X \rightarrow X$, dada por:

$$ac(h, x) = ac(i(h), x) \quad \forall h \in H, x \in X$$

Donde consideramos la aplicación inclusión $i : H \rightarrow G$ dada por $i(h) = h$, para todo $h \in H$.

¹En 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.

²En realidad deberíamos decir que “ G actúa por la izquierda sobre X ”.

3. Dado $n \in \mathbb{N}$, si $X = \{1, \dots, n\}$ y $G = S_n$, la acción natural de S_n sobre X será la acción $ac : S_n \times X \rightarrow X$ dada por:

$$ac(\sigma, k) = {}^\sigma k = \sigma(k) \quad \forall \sigma \in S_n, k \in X$$

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 $\text{Perm}(X)$.

Demostración. Veamos que es posible:

- Por una parte, dada una acción de G sobre X , $ac : G \times X \rightarrow X$, podemos definir la aplicación:

$$\begin{aligned} \phi : G &\longrightarrow \text{Perm}(X) \\ g &\longmapsto \phi(g) \end{aligned}$$

Donde $\phi(g)$ es una aplicación $\phi(g) : X \rightarrow X$ dada por:

$$\phi(g)(x) = {}^g x \quad \forall x \in X$$

Veamos en primer lugar que ϕ está bien definida, es decir, que $\phi(g) \in \text{Perm}(X)$ 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 $x \in G$:

$$(\phi(g)\phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)({}^h x) = {}^g({}^h x) \stackrel{(*)}{=} {}^{gh} x = \phi(gh)(x)$$

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 $\text{Perm}(X)$), 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 $\phi(g) \in \text{Perm}(X)$, 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 $\phi : G \rightarrow \text{Perm}(X)$ un homomorfismo de grupos, definimos la aplicación $ac : G \times X \rightarrow X$ dada por:

$$ac(g, x) = \phi(g)(x) \quad \forall g \in G, x \in X$$

Veamos que es una acción:

$$\begin{aligned} ac(1, x) &= \phi(1)(x) = x \quad \forall x \in X \\ ac(g, ac(h, x)) &= \phi(g)(\phi(h)(x)) = \phi(gh)(x) = ac(gh, x) \quad \forall x \in X, \quad \forall g, h \in G \end{aligned}$$

□

Definición 2.2 (Representación por permutaciones). Sea G un grupo y X un conjunto no vacío, si tenemos una acción de G sobre X , el homomorfismo ϕ dado por esta acción según la Proposición 2.1 recibirá el nombre de representación de G por permutaciones.

Además, llamaremos a $\ker(\phi)$ núcleo de la acción, ya que:

$$\ker(\phi) = \{g \in G \mid \phi(g) = id_X\} = \{g \in G \mid {}^g x = x \quad \forall x \in X\}$$

En el caso de que $\ker(\phi) = \{1\}$, diremos que la acción es fiel.

Ejemplo. A continuación, dados varios ejemplos de acciones, consideraremos en cada caso su representación por permutaciones:

1. La representación por permutaciones de la acción trivial es el homomorfismo $\phi : G \rightarrow Perm(X)$ dado por:

$$\phi(g) = id_X \quad \forall g \in G$$

2. Si tenemos un conjunto no vacío X y una acción $ac : G \times X \rightarrow X$ sobre un grupo G que tiene asociada una representación por permutaciones ϕ , entonces la acción por restricción $ac : H \times X \rightarrow X$ tendrá asociada como representación por permutaciones el homomorfismo $\phi_H : H \rightarrow Perm(X)$ dado por:

$$\phi_H = \phi \circ i$$

Siendo $i : H \rightarrow G$ la aplicación inclusión.

3. En el caso de la acción natural de S_n sobre $X = \{1, \dots, n\}$, tenemos que la representación por permutaciones es el homomorfismo $\phi : S_n \rightarrow Perm(X)$ dado por:

$$\phi(\sigma) = \sigma \quad \forall \sigma \in S_n$$

Es decir, $\phi = id_{S_n}$.

4. Sea G un grupo, podemos definir la acción por traslación como:

$$\begin{aligned} ac : G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

Y el homomorfismo asociado a la acción como representación por permutaciones será $\phi : G \rightarrow Perm(G)$ dado por:

$$\phi(g)(h) = gh \quad \forall g, h \in G$$

Como además:

$$\ker(\phi) = \{g \in G \mid gh = h \quad \forall h \in G\} = \{1\}$$

Tenemos que es una acción fiel.

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

Demostración. Sea G un grupo, consideramos la acción por traslación:

$$\begin{aligned} ac : G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

Y su representación por permutaciones, $\phi : G \rightarrow \text{Perm}(G)$ dado por:

$$\phi(g)(h) = gh \quad \forall g \in G, \forall h \in G$$

Como la acción por traslación es una acción fiel, tendremos que $\ker(\phi) = \{1\}$ y aplicando el Primer Teorema de Isomorfía sobre ϕ , obtenemos que:

$$G \cong G/\{1\} \cong \text{Im}(\phi)$$

Donde $\text{Im}(\phi) = \phi_*(G)$, que en la Proposición ?? vimos que es un subgrupo de $\text{Perm}(G)$. \square

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

- La acción por traslación de G sobre $\mathcal{P}(G)$ será $ac : G \times \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ dada por:

$$ac(g, A) = gA = \{ga \mid a \in A\} \subseteq G \quad \forall A \in \mathcal{P}(G)$$

- Podemos también considerar la acción por traslación en el cociente por las clases laterales por la izquierda³: si $H < G$, consideramos el cociente de G sobre H por la izquierda y la acción $ac : G \times G/H \rightarrow G/H$ dada por:

$$ac(g, xH) = {}^g(xH) = gxH = \{gxh \mid h \in H\}$$

- La acción por conjugación se define como $ac : G \times G \rightarrow G$ dada por:

$$ac(g, h) = {}^gh = ghg^{-1}$$

Que es una acción, ya que:

$$\begin{aligned} {}^1h &= 1h1^{-1} = h \quad \forall h \in G \\ {}^g({}^hl) &= g{}^hlg^{-1} = ghlg^{-1}g^{-1}ghl(gh)^{-1} = {}^{gh}l \quad \forall g, h, l \in G \end{aligned}$$

El homomorfismo asociado es:

$$\begin{aligned} \phi : G &\rightarrow \text{Perm}(G) \\ \phi(g)(h) &= ghg^{-1} \quad \forall g, h \in G \end{aligned}$$

El núcleo en este caso es:

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

- La acción por conjugación en partes de G se define como la aplicación $ac : G \times \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ dada por:

$$ac(g, A) = {}^gA = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G \quad \forall A \in \mathcal{P}(G)$$

³No es necesario considerar $H \triangleleft G$, ya que solo consideramos conjuntos no vacíos, por lo que no es necesario que el cociente tenga estructura de grupo.

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

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

Como la aplicación $ac : G \times Subg(G) \rightarrow Subg(G)$ dada por:

$$ac(g, H) = {}^gH = gHg^{-1} < G$$

Ya que en la Proposición ?? vimos que gHg^{-1} era un subgrupo de G , al que llamaremos subgrupo conjugado de G .

2.1. Órbitas de un elemento

Definición 2.3 (Órbita). Sea G un grupo y X un G -conjunto, definimos en X una relación de equivalencia \sim (compruébese) dada por:

$$y \sim x \iff \exists g \in G \mid y = {}^gx$$

La clase de equivalencia de cada $x \in X$ se llama órbita de x , denotada por:

$$Orb(x) = \{y \in X \mid \exists g \in G \text{ con } y = {}^gx\}$$

Como estamos considerando una acción, será equivalente escribir:

$$Orb(x) = \{y \in X \mid \exists g \in G \text{ con } {}^gy = x\}$$

Tenemos de esta forma que el conjunto cociente X/\sim es el conjunto formado por las órbitas de todos los elementos de X :

$$X/\sim = \{Orb(x) \mid x \in X\}$$

Ejemplo. Sobre $X = \{1, 2, 3, 4\}$: En S_4 consideramos $ac : S_4 \times X \rightarrow X$, la acción natural de S_4 sobre X :

$$ac(\sigma, k) = {}^\sigma k = \sigma(k)$$

- Si tenemos $H = \langle (1 \ 2 \ 3) \rangle$, queremos calcular las órbitas de los elementos de H . Recordamos que:

$$Orb(x) = \{y \in X \mid \exists \sigma \in H \text{ con } \sigma(y) = x\}$$

Es decir, pensamos en $Orb(x)$ como en los elementos de X desde los que podemos llegar a x con una permutación de H . De esta forma:

$$Orb(1) = \{1, 2, 3\}$$

$$Orb(2) = \{1, 2, 3\}$$

$$Orb(3) = \{1, 2, 3\}$$

$$Orb(4) = \{4\}$$

- En A_4 :

$$A_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\}$$

Como tenemos todos los 3-ciclos:

$$\text{Orb}(1) = X$$

Y también tendremos que $\text{Orb}(k) = X$, para $k \in X$.

- En V , que contiene a todos los 2-ciclos, la situación será la misma:

$$\text{Orb}(k) = X \quad \forall k \in X$$

- En $H = \langle (1\ 2\ 3\ 4) \rangle$ sucede lo mismo:

$$\text{Orb}(k) = X \quad \forall k \in X$$

Definición 2.4. Si el conjunto de órbitas X/\sim es unitario, decimos que la acción es transitiva.

Este nombre se debe a que dados $x, y \in X$, siempre $\exists g \in G$ de forma que:

$$y = {}^g x$$

Definición 2.5 (Estabilizador). Sea G un grupo y X un G -conjunto, definimos el grupo de estabilizadores de $x \in X$ en G como:

$$\text{Stab}_G(x) = \{g \in G \mid {}^g x = x\}$$

También se le llama grupo de isotropía.

Para justificar por qué a $\text{Stab}_G(x)$ le llamábamos grupo de estabilizadores de x en G , es necesaria la siguiente Proposición:

Proposición 2.3. Sea G un grupo y X un G -conjunto:

$$\text{Stab}_G(x) < G \quad \forall x \in X$$

Demostración. Fijado $x \in X$, es claro que $\text{Stab}_G(x) \subseteq G$. Vemos que:

- $1 \in \text{Stab}_G(x)$, ya que ${}^1 x = x$ por definición de acción.
- Si $g \in \text{Stab}_G(x)$, supongamos que $g^{-1} \notin \text{Stab}_G(x)$, con lo que ${}^{g^{-1}} x = y \in X$ con $y \neq x$. En dicho caso:

$$x = {}^1 x = {}^{g^{-1}g} x = {}^{g^{-1}} ({}^g x) = {}^{g^{-1}} x = y$$

Llegamos a una contradicción, luego $g^{-1} \in \text{Stab}_G(x)$ para todo $g \in \text{Stab}_G(x)$.

- Finalmente, si $g, h \in \text{Stab}_G(x)$, entonces:

$$^{gh}x = {}^g({}^hx) = {}^gx = x$$

Por lo que $gh \in \text{Stab}_G(x)$.

□

Ejemplo. Si nuevamente sobre $X = \{1, 2, 3, 4\}$ volvemos a considerar la acción natural de S_4 sobre X :

- En $H = \langle (1\ 2\ 3) \rangle$, recordamos que:

$$\text{Stab}_H(x) = \{\sigma \in H \mid \sigma(x) = x\}$$

Es decir, el grupo de estabilizadores de x en H son los elementos de H que dejan fijo el elemento x . De esta forma:

$$\text{Stab}_H(1) = \{1\}$$

$$\text{Stab}_H(2) = \{1\}$$

$$\text{Stab}_H(3) = \{1\}$$

$$\text{Stab}_H(4) = H$$

- En A_4 :

$$\text{Stab}_{A_4}(1) = \{1, (2\ 3\ 4), (2\ 4\ 3)\} = \langle (2\ 3\ 4) \rangle$$

$$\text{Stab}_{A_4}(2) = \langle (1\ 3\ 4) \rangle$$

$$\text{Stab}_{A_4}(3) = \langle (1\ 2\ 4) \rangle$$

$$\text{Stab}_{A_4}(4) = \langle (1\ 2\ 3) \rangle$$

- En V :

$$\text{Stab}_V(k) = \{1\} \quad \forall k \in X$$

- En $H = \langle (1\ 2\ 3\ 4) \rangle$:

$$\text{Stab}_H(k) = \{1\} \quad \forall k \in X$$

Vamos a poder establecer una relación entre el orden de las órbitas y del conjunto cociente.

Proposición 2.4. Sea G un grupo finito que actúa sobre X , entonces para cada $x \in X$, $\text{Orb}(x)$ es un conjunto finito y:

$$|\text{Orb}(x)| = [G : \text{Stab}_G(x)]$$

En particular, el cardinal de la órbita es un divisor del orden de G .

Demostración. Fijado $x \in X$, si consideramos $\text{Stab}_G(x) < G$ y las clases laterales por la izquierda⁴, $G / \text{Stab}_G(x) \sim$, definimos la aplicación $\phi : G / \text{Stab}_G(x) \sim \longrightarrow \text{Orb}(x)$ dada por:

$$\phi(g\text{Stab}_G(x)) = {}^gx \quad \forall g\text{Stab}_G(x) \in G / \text{Stab}_G(x) \sim$$

⁴No consideramos el conjunto cociente porque no sabemos si $\text{Stab}_G(x)$ es un subgrupo normal en G o no.

- Veamos que está bien definida. Para ello, sean $g, g' \in G$ de forma que:

$$gStab_G(x) = g'Stab_G(x)$$

Entonces, existirá $h \in Stab_G(x)$ de forma que $g = g'h$. En dicho caso:

$$\phi(gStab_G(x)) = {}^gx = {}^{g'h}x = {}^{g'}({}^hx) = {}^{g'}x = \phi(g'Stab_G(x))$$

- Veamos que es sobreyectiva: sea $y \in Orb(x)$, entonces $\exists g \in G$ de forma que:

$$y = {}^gx$$

Por lo que $y = \phi(gStab_G(x))$.

- Para la inyectividad, sean $g, g' \in G$ de forma que:

$${}^gx = \phi(gStab_G(x)) = \phi(g'Stab_G(x)) = {}^{g'}x$$

Entonces, podemos escribir:

$$x = {}^{g^{-1}}({}^gx) = {}^{g^{-1}}({}^{g'}x) = {}^{g^{-1}g'}x$$

De donde concluimos que $g^{-1}g' \in Stab_G(x)$, por lo que $gStab_G(x) = g'Stab_G(x)$.

En definitiva, acabamos de probar que $Orb(x)$ es biyectivo con $G/Stab_G(x) \sim$, por lo que tienen el mismo cardinal. Además:

- Por ser G finito y $Stab_G(x) < G$, tenemos que:

$$|Orb(x)| = [G : Stab_G(x)] = \frac{|G|}{|Stab_G(x)|}$$

Por lo que $Orb(x)$ es un conjunto finito.

- Despejando de la igualdad superior, tenemos que:

$$|Orb(x)||Stab_G(x)| = |G|$$

Por lo que $|Orb(x)|$ es un divisor de $|G|$.

□

Observación. La demostración es cierta sin suponer que G sea un grupo finito, pero entonces solo podemos poner como tesis que $Orb(x)$ es biyectivo con $G/Stab_G(x) \sim$, para todo $x \in X$.

Proposición 2.5. *Sea G un grupo que actúa sobre X , si $x, y \in X$ están en la misma órbita, entonces $Stab_G(x)$ y $Stab_G(y)$ son subgrupos conjugados.*

Demostración. Si x e y están en la misma órbita, entonces $Orb(x) = Orb(y)$, por lo que $\exists g \in G$ de forma que $y = {}^gx$. En dicho caso, también tenemos que $x = {}^{g^{-1}}y$. Veamos que:

$$Stab_G(x) = g^{-1}Stab_G(y)g$$

Para ello:

\subseteq) Sea $h \in \text{Stab}_G(x)$, queremos ver que $h \in g^{-1}\text{Stab}_G(y)g$, para lo que bastará ver que $ghg^{-1} \in \text{Stab}_G(y)$:

$$ghg^{-1}y = {}^ghx = {}^gx = y$$

\supseteq) Sea $h \in \text{Stab}_G(y)$, queremos ver que $g^{-1}hg \in \text{Stab}_G(x)$:

$$g^{-1}hgx = g^{-1}hy = g^{-1}y = x$$

□

Definición 2.6. Sea G un grupo y X un G -conjunto, un elemento $x \in X$ se dice que es fijo por la acción si ${}^gx = x$, $\forall g \in G$.

Consideramos el conjunto de todos los elementos que se quedan fijos por todos los elementos de G :

$$\text{Fix}(X) = \{x \in X \mid {}^gx = x, \quad \forall g \in G\}$$

Proposición 2.6. Sea G un grupo y X un G -conjunto, si $x \in X$, entonces:

$$x \in \text{Fix}(X) \iff \text{Orb}(x) = \{x\} \iff \text{Stab}_G(x) = G$$

Demostración. Si recordamos las definiciones de estos tres conjuntos:

$$\begin{aligned} \text{Orb}(x) &= \{y \in X \mid \exists g \in G \text{ con } {}^gy = x\} \\ \text{Stab}_G(x) &= \{g \in G \mid {}^gx = x\} \\ \text{Fix}(X) &= \{x \in X \mid {}^gx = x \quad \forall g \in G\} \end{aligned}$$

Veamos todas las implicaciones:

$$x \in \text{Fix}(X) \implies \text{Orb}(x) = \{x\}$$

Si $y \in \text{Orb}(x)$, entonces $\exists g \in G$ con ${}^gy = x$, por lo que:

$$y = g^{-1}gy = g^{-1}({}^gy) = g^{-1}x \stackrel{(*)}{=} x$$

Donde en $(*)$ usamos que $x \in \text{Fix}(X)$. Concluimos que $\text{Orb}(x) = \{x\}$.

$$\text{Orb}(x) = \{x\} \implies \text{Stab}_G(x) = G$$

Sea $g \in G$, si consideramos $y = {}^gx$, entonces $y \in \text{Orb}(x) = \{x\}$, de donde $y = x$ y $g \in \text{Stab}_G(x)$.

$$\text{Stab}_G(x) = G \implies x \in \text{Fix}(X)$$

$${}^gx = x \quad \forall g \in G$$

De donde deducimos que $x \in \text{Fix}(X)$.

□

Observación. Si tenemos un grupo G y un G -conjunto X , recordamos que tenemos definida sobre X una relación de equivalencia \sim , con la que anteriormente definimos los órbitas de los elementos. En el caso de que X sea un conjunto finito y tenga n elementos:

$$X = \{x_1, \dots, x_n\}$$

Por ser \sim una relación de equivalencia, tenemos una partición de X , lo que nos da la igualdad:

$$|X| = \sum_{k=1}^n |Orb(x_k)|$$

Para simplificarla usando propiedades ya vistas, sabemos que puede haber órbitas unitarias:

$$Orb(x) = \{x\} \iff x \in Fix(x)$$

Por tanto, podemos simplificar la igualdad superior, eliminando de ella todas las órbitas unitarias. Para ello, si Γ contiene un único representante de cada una de las órbitas de elementos que no son puntos fijos ($\Gamma \subseteq X \setminus Fix(X)$):

$$|X| = \sum_{k=1}^n |Orb(x_k)| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)|$$

Y aplicando finalmente la Proposición 2.4, llegamos a que:

$$|X| = \sum_{k=1}^n |Orb(x_k)| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)| = |Fix(X)| + \sum_{y \in \Gamma} [G : Stab_G(y)]$$

A continuación, lo que haremos será estudiar los conjuntos $Orb(\cdot)$, $Stab_G(\cdot)$ y $Fix(X)$ para ciertos ejemplos comunes de acciones.

2.1.1. Acción por traslación

Sea G un grupo no trivial, la acción por traslación se define como $ac : G \times G \rightarrow G$ dada por:

$$ac(g, h) = {}^g h = gh \quad \forall g, h \in G$$

De esta forma, tenemos que:

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = gh\} = G \quad \forall h \in G$$

Ya que fijado $k \in G$ y dado $h \in G$, siempre podemos tomar $g = kh^{-1} \in G$ para tener que ${}^g h = gh = k$.

$$\begin{aligned} Stab_G(h) &= \{g \in G \mid gh = {}^g h = h\} = \{1\} \quad \forall h \in G \\ Fix(G) &= \{h \in G \mid gh = {}^g h = h \quad \forall g \in G\} = \emptyset \end{aligned}$$

Observación. Observemos que la acción por traslación cuenta con las mismas cualidades que tiene una traslación entre dos espacios vectoriales, pensando en que primero fijamos un vector $v \in V$ para luego definir una aplicación $t_v : V \rightarrow V'$. De esta forma:

- Fijado cualquier vector v , t_v siempre será sobreyectiva. Esto se pone de manifiesto al decir que $Orb(h) = G$ para todo $h \in G$.
- La única traslación que mantiene fijo un punto es la correspondiente al vector 1, que deja fijos todos los puntos, $Stab_G(h) = \{1\} \forall h \in G$.
- Como hay traslaciones que no mantienen fijos ningún punto (todas salvo la trivial), no hay ningún punto que permanezca invariante ante todas ellas, $Fix(G) = \emptyset$.

2.1.2. Acción por conjugación

Sea G un grupo, la acción por conjugación se define como $ac : G \times G \rightarrow G$ dada por:

$$ac(g, h) = {}^g h = ghg^{-1} \quad \forall g, h \in G$$

Preliminares

Antes de estudiar los subconjuntos notables de esta acción, definimos ciertos conjuntos y vemos propiedades de estos que nos ayudarán a entender la acción.

Definición 2.7 (Centralizador). Sea G un grupo y $S \subseteq G$, llamamos centralizador de S en G al conjunto:

$$C_G(S) = \{x \in G \mid xs = sx \quad \forall s \in S\}$$

Definición 2.8 (Normalizador). Sea G un grupo y $S \subseteq G$, llamamos normalizador de S en G al conjunto:

$$N_G(S) = \{x \in G \mid xS = Sx\}$$

Proposición 2.7. Sea G un grupo y $S \subseteq G$, se verifica:

- i) $N_G(S) < G$.
- ii) $C_G(S) \triangleleft N_G(S)$.
- iii) Si $S < G$, entonces $S \triangleleft N_G(S)$.

Demostración. Demostramos cada apartado:

i) Sean $x, y \in N_G(S)$, entonces tendremos que:

$$\begin{aligned} xS = Sx &\implies xSx^{-1} = S \\ yS = Sy &\implies S = y^{-1}Sy \end{aligned}$$

En dicho caso:

$$(xy^{-1})S(xy^{-1})^{-1} = (xy^{-1})S(yx^{-1}) = x(y^{-1}Sy)x^{-1} = xSx^{-1} = S$$

De donde deducimos que $(xy^{-1})S = S(xy^{-1})$, por lo que $xy^{-1} \in N_G(S)$ y $N_G(S) < G$.

ii) Hemos de ver primero que $C_G(S) < N_G(S)$:

- En primer lugar, si $x \in C_G(S)$:

$$xS = \{xs \mid s \in S\} = \{sx \mid s \in S\} = Sx$$

Por lo que $x \in N_G(S)$ y se tiene que $C_G(S) \subseteq N_G(S)$.

- Ahora, si $x, y \in C_G(S)$, entonces:

$$\begin{aligned} xs = sx &\implies xsx^{-1} = s \\ ys = sy &\implies s = y^{-1}sy \quad \forall s \in S \end{aligned}$$

Lo que nos permite escribir:

$$(xy^{-1})s(xy^{-1})^{-1} = x(y^{-1}sy)x^{-1} = xsx^{-1} = s \quad \forall s \in S$$

De donde deducimos que $xy^{-1} \in C_G(S)$, por lo que $C_G(S) < N_G(S)$.

Para la normalidad, dado $x \in C_G(S)$ y $g \in N_G(S)$, queremos ver que se cumple $y = gxg^{-1} \in C_G(S)$. Para ello, dado $s \in S$, vemos que:

$$ys = (gxg^{-1})s \stackrel{(*)}{=} gxs'g^{-1} = gs'xg^{-1} \stackrel{(**)}{=} s(gxg^{-1}) = sy$$

Donde en $(*)$ usamos que como $g \in N_G(S)$, también tenemos que $g^{-1} \in N_G(S)$, con lo que $\exists s' \in S$ de forma que:

$$g^{-1}s = s'g^{-1}$$

Y en $(**)$ deshacemos este proceso, ya que multiplicando la igualdad superior por derecha e izquierda por g , llegamos a que:

$$g^{-1}s = s'g^{-1} \implies gg^{-1}sg = gs'g^{-1}g \implies sg = gs'$$

En definitiva, de $ys = sy$ deducimos que $y = gxg^{-1} \in C_G(S)$, para todo $x \in C_G(S)$ y todo $g \in N_G(S)$, de donde $C_G(S) \triangleleft N_G(S)$.

iii) Si suponemos además que $S < G$, por una parte tenemos que:

$$sS = S = Ss \quad \forall s \in S$$

De donde deducimos que $S \subseteq N_G(S)$ y por ser $S < G$, tenemos que $S < N_G(S)$. Para la normalidad, si $g \in N_G(S)$, tendremos entonces que:

$$gS = Sg \implies gSg^{-1} = S$$

De donde deducimos que $S \triangleleft N_G(S)$.

□

Proposición 2.8. Sea G un grupo, $H, K < G$ con $H \subseteq K$, entonces:

$$H \triangleleft K \iff K < N_G(H)$$

De esta forma, el normalizador $N_G(H)$ se caracteriza como el mayor subgrupo de G en el que H es normal.

Demostración. Por ser $H, K < G$ con $H \subseteq K$, tenemos ya que $H < K$. Por una caracterización que vimos de los subgrupos normales:

$$H \triangleleft K \iff kHk^{-1} = H \quad \forall k \in K \iff kH = Hk \quad \forall k \in K \iff K \subseteq N_G(H)$$

Y por ser $K < G$, $K \subseteq N_G(H) \iff K < N_G(H)$. \square

Ejercicio. Para terminar de comprender las propiedades del centralizador y del normalizador, se pide probar que si G es un grupo y $H < G$:

$$\begin{aligned} H \triangleleft G &\iff G = N_G(H) \\ H \subseteq Z(G) &\iff G = C_G(H) \end{aligned}$$

Subconjuntos notables

Estudiadas ya las propiedades del centralizador y del normalizador, estamos ya en condiciones de estudiar los conjuntos notables de la acción por conjugación:

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = ghg^{-1}\} = \{ghg^{-1} \mid g \in G\} = Cl_G(h) \quad \forall h \in G$$

De esta forma, llamaremos a la órbita de h por la acción por conjugación la clase de conjugación de h en G .

$$Stab_G(h) = \{g \in G \mid {}^g h = ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = C_G(h)$$

El estabilizador de h en G coincide con el centralizador de h en G , y como la órbita de h coincidía con la clase de conjugación de h en G , por la Proposición 2.4, tenemos que:

$$|Cl_G(h)| = |Orb(h)| = [G : Stab_G(h)] = [G : C_G(h)] \quad \forall h \in G$$

Y en el caso de que G sea finito:

$$|Cl_G(h)| |C_G(h)| = |G|$$

Para los puntos fijos:

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

Ejemplo. Calcular las clases de conjugación de los elementos de D_4 :

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} = \{s^i r^j \mid i \in \{0, 1\} \ j \in \{0, 1, 2, 3\}\}$$

Vemos que:

$$\begin{aligned} Cl_{D_4}(1) &= \{s^i r^j 1 (s^i r^j)^{-1}\} = \{1\} \\ Cl_{D_4}(r) &= \{s^i r^j r (s^i r^j)^{-1}\} = \{s^i r^j r r^{-j} s^{-i}\} = \{s^i r s^i\} = \{r, srs\} = \{r, r^3\} \\ Cl_{D_4}(r^2) &= \{s^i r^2 s^i\} = \{r^2\} \\ Cl_{D_4}(s) &= \{s, sr^2\} \\ Cl_{D_4}(sr) &= \{sr, sr^3\} \end{aligned}$$

Fórmula de clases

Podemos particularizar la fórmula anteriormente obtenida:

$$|X| = |Fix(X)| + \sum_{y \in \Gamma} [G : Stab_G(y)]$$

Para la acción por conjugación, obteniendo la **fórmula de clases**:

$$|G| = |Z(G)| + \sum_{y \in \Gamma} [G : C_G(y)]$$

Donde podemos pensar en Γ en el conjunto formado por los representantes de las órbitas con más de un elemento.

Esta última podemos generalizarla para cualquier subgrupo $H \triangleleft G$, obteniendo la **fórmula de clases general**:

$$|H| = |H \cap Z(G)| + \sum_{y \in \Gamma} [G : C_G(y)]$$

2.1.3. Acción por conjugación sobre subgrupos

Sea G un grupo, la acción por conjugación sobre sus subgrupos viene definida⁵ por $ac : G \times Subg(G) \rightarrow Subg(G)$ dada por:

$$ac(g, H) = {}^gH = gHg^{-1} \quad \forall g \in G, \quad \forall H \in Subg(G)$$

Veamos que:

$$Orb(H) = \{K \in Subg(G) \mid \exists g \in G \text{ con } gHg^{-1} = {}^gH = K\} = \{gHg^{-1} \mid g \in G\}$$

Es decir, la órbita de un subgrupo está formado por todos sus conjugados.

Observación. Sea G un grupo, $H \in Subg(G)$, si consideramos la acción por conjugación sobre subgrupos, tenemos que:

$$Orb(H) = \{H\} \iff H \triangleleft G$$

Esto se debe a que:

$$Orb(H) = \{H\} \iff \{gHg^{-1} \mid g \in G\} = \{H\} \iff H \triangleleft G$$

Donde la última equivalencia se tiene gracias a la Proposición ??, donde vimos una caracterización de los subgrupos normales.

El estabilizador:

$$Stab_G(H) = \{g \in G \mid {}^gH = H\} = \{g \in G \mid gH = Hg\} = N_G(H)$$

Vemos finalmente los subgrupos que quedan fijos mediante la acción:

$$Fix(Subg(G)) = \{H < G \mid gHg^{-1} = {}^gH = H \quad \forall g \in G\} = \{H < G \mid H \triangleleft G\}$$

Coincide con el conjunto de subgrupos normales de G .

Y tendremos que:

$$|Orb(H)| = [G : N_G(H)]$$

⁵está bien definida gracias a la Proposición ??

2.2. p -grupos

Definición 2.9 (p -grupo). Si p es un número primo, un grupo G se dice que es un p -grupo si todo elemento de G distinto del neutro tiene orden una potencia de p . Si G es un grupo, diremos que $H < G$ es un p -subgrupo de G si H es un p -grupo.

Ejemplo. \mathbb{Z}_8 es un ejemplo de 2-grupo, ya que sus elementos son:

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

Calculamos los órdenes de todos los elementos, sabiendo que (Proposición ??):

$$O(x) = \frac{n}{\text{mcd}(x, n)} \quad \forall x \in \mathbb{Z}_n$$

Por lo que:

$$\begin{array}{llll} O(1) = 8 = 2^3 & O(2) = 4 = 2^2 & O(3) = 8 = 2^3 & O(4) = 2 \\ O(5) = 8 = 2^3 & O(6) = 4 = 2^2 & O(7) = 8 = 2^3 & \end{array}$$

Teorema 2.9 (de Cauchy). Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p , y por tanto tendrá un p -subgrupo de orden p .

Demostración. Si consideramos:

$$X = \{(a_1, a_2, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = 1\}$$

Si $|G| = n$, entonces $|X| = n^{p-1}$, ya que elegimos libremente las $p - 1$ primeras coordenadas (variación con repetición):

$$a_1, a_2, \dots, a_{p-1} \in G \quad \text{arbitrarios}$$

Y la última viene condicionada:

$$a_p = (a_1, a_2, \dots, a_{p-1})^{-1}$$

Sea $\sigma = (1 \ 2 \ \dots \ p) \in S_p$, consideramos $H = \langle \sigma \rangle = \{1, \sigma, \dots, \sigma^{p-1}\} \subseteq S_p$. Consideramos también la acción $ac : H \times X \rightarrow X$ dada por (compruébese que es una acción):

$$ac(\sigma^k, (a_1, a_2, \dots, a_p)) = (a_{\sigma^k(1)}, a_{\sigma^k(2)}, \dots, a_{\sigma^k(p)}) \quad \forall (a_1, \dots, a_p) \in X, \forall \sigma^k \in H$$

Por la Proposición 2.4, tenemos que:

$$|Orb(z)| = [H : \text{Stab}_H(z)] = \frac{|H|}{|\text{Stab}_H(z)|} \quad \forall z \in X$$

De donde tenemos que $|Orb(a_1, \dots, a_p)|$ es un divisor de $|H|$, $\forall (a_1, \dots, a_p) \in X$. En dicho caso, $|Orb(a_1, \dots, a_p)| \in \{1, p\}$, por ser $|H| = p$. Por tanto, las órbitas de un elemento serán unitarias o bien tendrán cardinal p .

Por tanto, sean r el número de órbitas con un elemento y s el número de órbitas con p elementos, entonces $(|\Gamma| = s)$:

$$n^{p-1} = |X| = |\text{Fix}(X)| + \sum_{y \in \Gamma} |\text{Orb}(y)| = r + \sum_{y \in \Gamma} p = r + sp$$

Veamos ahora cómo son los elementos de $\text{Orb}(a_1, \dots, a_p)$:

$$\begin{aligned} \text{Orb}(a_1, \dots, a_p) &= \left\{ \sigma^k(a_1, \dots, a_p) \mid k \in \{0, \dots, p-1\} \right\} \\ &= \{(a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots, (a_p, a_1, \dots, a_{p-1})\} \end{aligned}$$

Por tanto, la órbita será unitaria si y solo si $a_1 = a_2 = \dots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geq 1$), como $\text{Orb}(1, 1, \dots, 1)$. Busquemos más: por hipótesis, $p \mid n$ y además $r = n^{p-1} - sp$, de donde $p \mid r$, por lo que $r \geq 2$ (ya que lo divide un primo).

En conclusión, $\exists a \in G \setminus \{1\}$ de forma que $\text{Orb}(a, a, \dots, a)$ es unitaria, de donde $a^p = 1$, por lo que $O(a) = p$.

Finalmente, sea $x \in \langle a \rangle \setminus \{1\}$, tenemos entonces que $1 \neq O(x) \mid p$, por lo que $O(x) = p$ y tenemos que todo elemento del subgrupo $\langle a \rangle$ es de orden p . En definitiva, $\langle a \rangle$ es un p -subgrupo de G de orden p . \square

Corolario 2.9.1. *Sea G un grupo finito y p un número primo:*

$$G \text{ es un } p\text{-grupo} \iff \exists n \in \mathbb{N} \text{ con } |G| = p^n$$

Demostración. Veamos la doble implicación.

\Leftarrow) Si $|G| = p^n$ para cierto $n \in \mathbb{N}$, entonces tendremos que $O(x) \mid p^n$ para todo $x \in G$, de donde $O(x) = p^k$ para cierto $k \in \mathbb{N}$, luego G es un p -grupo.

\Rightarrow) Suponemos que q es un primo que divide al orden de $|G|$, luego por el Teorema de Cauchy debe existir $x \in G$ de forma que $O(x) = q$. En dicho caso, como G es un p -grupo, $q = p^r$ para cierto $r \in \mathbb{N}$, de donde (q y p son primos) $r = 1$ y $q = p$.

De esta forma, el único primo que divide a $|G|$ es p , luego $|G| = p^n$, para algún $n \in \mathbb{N}$. \square

Teorema 2.10 (de Burnside). *Si G es un p -grupo finito no trivial, entonces $|Z(G)| \geq p$, y en particular, $|Z(G)| \neq \{1\}$.*

Demostración. Distinguimos casos:

- Si G es abeliano, $Z(G) = G$ y tenemos que $|Z(G)| = |G| = p^n$ para cierto $n \in \mathbb{N}$, por lo que $|Z(G)| \geq p$. En particular, $Z(G) = G$ no es trivial.
- Si G es no abeliano, entonces $Z(G) < G$ y por la fórmula anterior de clases:

$$p^n = |G| = |Z(G)| + \sum_{h \in \Gamma} [G : C_G(h)]$$

Como G es finito, $[G : C_G(h)]$ divide a $|G| = p^n$ para cualquier $h \in \Gamma$ y para cierto $n \in \mathbb{N}$. Es decir:

$$[G : C_G(h)] = p^k \quad \text{para algún } k \in \mathbb{N}, \quad \forall h \in \Gamma$$

En ningún caso puede ser $k = 0$, ya que diríamos que $C_G(h) = G$ y:

$$C_G(h) = \{g \in G \mid gh = hg\}$$

De donde $h \in Z(G)$, por lo que h no estaría en $\Gamma \subseteq G \setminus Z(G)$.

En dicho caso, $p \mid [G : C_G(h)]$ para todo $h \in \Gamma$, $p \mid |Z(G)|$ (despejar $|Z(G)|$ de la anterior igualdad), de donde $|Z(G)| \geq p$.

□

Lema 2.11. *Si G es un grupo y $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Como $G/Z(G)$ es cíclico, existirá $z \in G$ de forma que:

$$Z/Z(G) = \langle zZ(G) \rangle$$

Sean $x, y \in G$, si consideramos su proyección al cociente, tendremos que $\exists n, m \in \mathbb{Z}$ de forma que:

$$xZ(G) = z^n Z(G) \quad yZ(G) = z^m Z(G)$$

Es decir, $\exists a, b \in Z(G)$ de forma que $x = z^n a$ y $y = z^m b$. Por tanto:

$$xy = z^n a z^m b = z^n z^m ab = z^{n+m} ba = z^m z^n ba = z^m b z^n a = yx$$

□

Corolario 2.11.1. *Si G es un grupo y p es un número primo, si $|G| = p^n$, entonces:*

$$|Z(G)| \neq p^{n-1}$$

En particular, todos los grupos de orden p^2 son abelianos.

Demostración. Supongamos que $|G| = p^n$ y que $|Z(G)| = p^{n-1}$. De esta forma:

$$|G/Z(G)| = p$$

En dicho caso, $G/Z(G)$ es cíclico, luego G es abeliano (por el Lema anterior). En dicho caso, G coincide con su centro, $G = Z(G)$, luego $p^n = p^{n-1}$, contradicción.

En particular, si G es un grupo con $|G| = p^2$ con p primo, como $Z(G) < G$, $|Z(G)|$ a de dividir a p^2 , luego:

- Si $|Z(G)| = 1$, entonces $Z(G) = 1$, que contradice a Burnside.
- $|Z(G)| = p$ no puede ser, por lo que acabamos de probar.
- La única posibilidad es que $|Z(G)| = p^2$, de donde $Z(G) = G$.

□

Observación. Notemos que ahora sabemos que todos los grupos de orden un primo al cuadrado son resolubles, por ser abelianos.

Teorema 2.12. *Sea G un grupo finito con $|G| = n$ y sea p un número primo, entonces para toda potencia p^k que divida a n , existe un subgrupo $H < G$ con orden $|H| = p^k$.*

Demostración. Por inducción sobre k :

- Si $k = 1$: tenemos el Teorema de Cauchy.
- Primera hipótesis de inducción: el resultado es cierto para todo $l < k$: si p^l divide a $|G|$, entonces $\exists H < G$ con $|H| = p^l$.
Veamos qué ocurre con k , es decir, si $|G| = p^k r = n$ para cierto $r \in \mathbb{N}$.

Por inducción sobre r :

- Si $r = 1$: tomamos $H = G$.
- Segunda hipótesis de inducción: si $r > 1$, suponemos el resultado cierto para todo grupo de orden divisible por p^k que sea de la forma $p^k m$ con $m < r$, es decir, $\exists H < G$ con $|H| = p^k$, veamos qué ocurre con G :

Para ello, distinguimos casos:

- Si existe $K < G$, $K \neq G$ de forma que $p \nmid [G : K]$. En dicho caso: $|G| = [G : K]|K|$ y $p^k \mid |G|$, entonces p^k dividirá a $|K|$. Usando la Segunda Hipótesis de inducción, tendremos $H < K < G$ de forma que $|H| = p^k$.
- Si para cualquier $K < G$, $K \neq G$ se tiene que $p \mid [G : K]$, entonces usando la fórmula de las clases:

$$|Z(G)| = |G| - \sum_{h \in \Gamma} [G : C_G(h)]$$

Y como p divide a todos los $[G : C_G(h)]$, concluimos que $p \mid |Z(G)|$. Por el Teorema de Cauchy, podemos encontrar $K < Z(G)$ de forma que $|K| = p$.

Por ser $K \subseteq Z(G)$, entonces $K \triangleleft G$ y podemos considerar el conjunto cociente G/K , con orden:

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{p}$$

De donde $p^{k-1} \mid |G/K|$.

Por la Primera Hipótesis de inducción, existe otro $L < G/K$ con $|L| = p^{k-1}$. Por el Tercer Teorema de Isomorfía, sabemos que $\exists K' \triangleleft H < G$ de forma que:

$$L = H/K$$

De donde:

$$|H| = |H/K||K| = p^{k-1}p = p^k$$

□

Ejemplo. Por ejemplo, si G es un grupo de la forma $|G| = 24 = 2^3 \cdot 3$, tendremos un subgrupo de orden 2, otro de orden 4, otro de orden 8 y otro de orden 3.

2.2.1. p -subgrupos de Sylow

En 1872, un noruego llamado Peter LM Sylow (1832-1918) definió unos grupos y llegó a unos resultados sobre ellos. En este documento, sus Teoremas no tendrán demostraciones muy elaboradas, como consecuencia de la teoría que venimos ya desarrollando desde el inicio.

Definición 2.10 (p -subgrupos de Sylow). Si G es un grupo finito y p un número primo que divide a $|G|$, un p -subgrupo de Sylow de G es un p -subgrupo de G cuyo orden es la máxima potencia de p que divide a $|G|$.

Es decir, si $|G| = p^k m$ con $\text{mcd}(p, m) = 1$ y p primo, un p -subgrupo $H < G$ es de Sylow si $|H| = p^k$.

Corolario 2.12.1 (Primer Teorema de Sylow). *Para todo grupo finito G y todo divisor primo p de su orden, existe al menos un p -subgrupo de Sylow.*

Demostración. Es evidente a partir del Teorema 2.12. □

Ejemplo. Si tenemos un grupo G con $|G| = 24 = 2^3 \cdot 3$, vamos a tener:

- $P < G$ un 2-subgrupo de Sylow, con $|P| = 8$.
- $Q < G$ un 3-subgrupo de Sylow, con $|Q| = 3$.

Observación. Si G es un grupo y p es un número primo con:

$$|G| = p^k m \quad \text{mcd}(p, m) = 1$$

Y P es un p -grupo de Sylow con $P < H < G$, entonces usando la fórmula de los índices:

$$[G : P] = [G : H][H : P]$$

En dicho caso, $[H : P] \mid [G : P] = m$, por lo que p no dividirá a $[H : P]$. Además:

$$[G : H] \mid [G : P] \implies p \nmid [G : H]$$

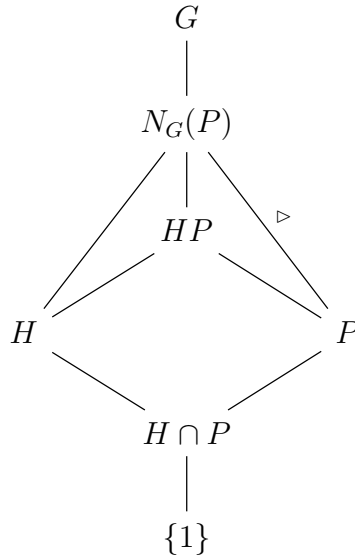
Es decir, si encontramos un grupo que contiene a P como subgrupo, p no dividirá a dichos índices.

El siguiente Lema también recibe el nombre de Segundo Teorema de Sylow, aunque nos reservamos este nombre para el resultado que se demuestra a partir del Lema.

Lema 2.13. *Si P es un p -subgrupo de Sylow de un grupo finito G y H es un p -subgrupo de $N_G(P)$, entonces H está contenido en P .*

Es decir, los p -subgrupos del normalizador de un p -subgrupo de Sylow estarán contenidos en dicho subgrupo.

Demostración. Como $P \triangleleft N_G(P)$ y $H < N_G(P)$, tenemos que $HP < N_G(P)$ y $H \cap P < H$. Estamos en la situación:



Por el Segundo Teorema de Isomorfía:

$$HP/P \cong H/H \cap P$$

Ahora, si $r = [HP : P] = [H : H \cap P]$, entonces $p \nmid r$. Ahora, como $r = [H : H \cap P]$ y como H es un p -subgrupo, $p^k \mid r$ para cierto $k \in \mathbb{N}$ (como es un p -grupo, tendremos $k > 0$). Como $p \nmid r$ (por la observación anterior) y $p^k \mid r$, entonces $r = 1$, de donde $HP = P$ y $H < P$. \square

Teorema 2.14 (Segundo Teorema de Sylow). *Sea G un grupo finito, p un número primo, supongamos que $|G| = p^k m$ con $\text{mcd}(p, m) = 1$ y n_p denota el número de p -subgrupos de Sylow de G , entonces:*

- i) *Todo p -subgrupo de G está contenido (como subgrupo) en un p -subgrupo de Sylow de G .*
- ii) *Cualesquiera dos p -subgrupos de Sylow de G son conjugados.*
- iii) *$n_p \mid m$ y $n_p \equiv 1 \pmod{p}$.*

Demostración. Demostramos cada apartado:

- i) Si llamamos $S = \text{Syl}_p(G) = \{P \mid P \text{ es un } p\text{-subgrupo de Sylow de } G\}$, consideramos la acción por conjugación $G \times S \rightarrow S$ dada por:

$$ac(g, P) = {}^gP = gPg^{-1} \in S$$

Sea $P_1 \in S$, estudiemos su órbita y su estabilizador:

$$\begin{aligned} \text{Orb}(P_1) &= \{gP_1g^{-1} \mid g \in G\} \\ \text{Stab}_G(P_1) &= \{g \in G \mid gP_1g^{-1} = P_1\} = N_G(P_1) \end{aligned}$$

Tenemos:

$$\begin{aligned} |Orb(P_1)| &= [G : N_G(P_1)] \\ P_1 &< N_G(P_1) < G_1 \\ [G : P_1] &= [G : N_G(P_1)][N_G(P_1) : P_1] \end{aligned}$$

Por lo que $|Orb(P_1)|$ divide a $[G : P_1] = m$. En definitiva:

$$\text{mcd}(|Orb(P_1)|, p) = 1$$

Ahora, veamos que todo p -subgrupo está contenido en un p -subgrupo de Sylow. Para ello, sea H un p -subgrupo de G , consideramos la acción sobre la órbita de $P_1 \in S$, $H \times Orb(P_1) \rightarrow Orb(P_1)$, dada por:

$$ac(h, P) = {}^hP = hPh^{-1} \in Orb(P_1)$$

Tendremos:

$$Stab_H(P) = \{h \in H \mid hPh^{-1} = P\} = H \cap N_G(P) < H$$

Además, también tendremos que $H \cap N_G(P) < P$, ya que si H es un p -subgrupo de $N_G(P)$, entonces $H < P$. En definitiva:

$$Stab_H(P) = H \cap N_G(P) < H \cap P < H \cap N_G(P)$$

De donde tenemos que $N_G(P) = H \cap P$. Usando la fórmula de la órbita:

$$|Orb(P_1)| = \sum_P [H : Stab_H(P)] = \sum_P [H : H \cap P]$$

De donde cada sumando divide a $|H|$ con H un p -subgrupo de P , por lo que $|H|$ es una potencia de p . Sin embargo, como $p \nmid |Orb(P_1)|$ (su máximo común divisor era 1), ha de existir un grupo $P \in Orb(P_1)$ (notemos que P es un p -subgrupo de Sylow. De hecho, P es un conjugado de P_1) de forma que:

$$[H : H \cap P] = 1$$

Por lo que $H \cap P = H$ y $H < P$.

ii) Veamos ahora que cualesquiera dos p -subgrupos de Sylow de G son conjugados. Para ello, sean P_1, P_2 dos p -subgrupos de Sylow de G , antes vimos (el lema) que si $H = P_2 < G$, entonces H está contenido en un subgrupo de Sylow, por lo que $\exists P$, un p -subgrupo de Sylow, conjugado de P_1 (por *i*)) de forma que $P_2 < P$, pero $|P| = |P_2|$, luego $P_2 = P$.

iii) Veamos ahora que $n_p \mid m$ y que $n_p \equiv 1 \pmod{p}$.

En el apartado *ii*) hemos visto que $Orb(P_1) = S$, luego:

$$n_p = |S| = |Orb(P_1)| = [G : N_G(P_1)]$$

Por lo que $n_p \mid m$.

Si en el apartado i) tomamos $H = P_1$ (el de la demostración anterior):

$$n_p = |\text{Orb}(P_1)| = \sum_P [P_1 : P_1 \cap P]$$

Por lo que $[P_1 : P_1 \cap P] = 1$ y los demás eran múltiplos de p , deducimos que $n_p \equiv 1 \pmod{p}$.

□

Ejemplo. Vamos a calcular grupos de Sylow:

- En $C_n = \langle x \mid x^n = 1 \rangle$ para cierto $n \in \mathbb{N}$, por el Primer Teorema de Sylow tendremos grupos de Sylow de las potencias máximas de los primos que aparecen en la factorización de n . Es decir, si n se descompone como:

$$n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$$

Para cada $k \in \{1, 2, \dots, m\}$, existe un p_k -subgrupo de Sylow, que será cíclico y tendrá orden $p_k^{t_k}$, luego los subgrupos de Sylow serán de la forma: $C_{p_k^{t_k}}$.

- En S_3 , como $|S_3| = 6 = 2 \cdot 3$, tendremos 2-subgrupos de Sylow y 3-subgrupos de Sylow. Veamos cuántos tenemos:
 - 2-subgrupos de Sylow, es decir, subgrupos de orden 2 de S_3 . Como $n_2 \mid 3$ y ha de ser $n_2 \equiv 1 \pmod{2}$, tendremos que n_2 valdrá 1 o 3.

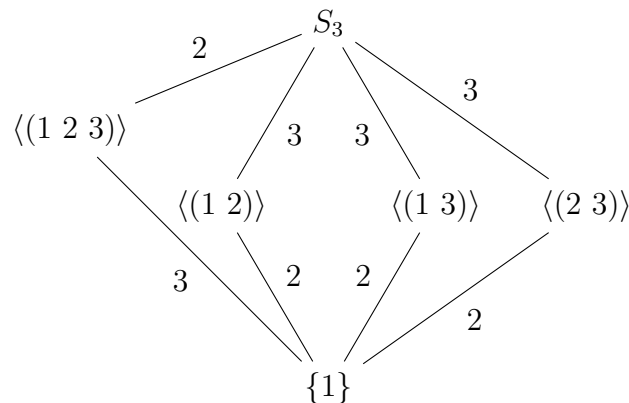


Figura 2.1: Diagrama de Hasse para los subgrupos de S_3 .

como los 3 subgrupos de la derecha son conjugados entre sí (compruébe-se), tendremos que $n_2 = 3$.

- Los 3-subgrupos de Sylow será un subgrupo de orden 3 de S_3 , que será el único que hay: $\langle (1\ 2\ 3) \rangle = A_3 \triangleleft S_3$.

Si queremos verlo por el Segundo Teorema de Sylow:

$$n_3 \equiv 1 \pmod{3} \quad \left. \begin{array}{l} n_3 \mid 2 \end{array} \right\} \implies n_3 = 1$$

- En A_4 , tenemos $|A_4| = 12 = 2^3 \cdot 3$. Tendremos:
 - 2-subgrupo de Sylow de orden 4. Busquemos por el Segundo Teorema de Sylow:

$$\left. \begin{array}{l} n_2 \mid 3 \\ n_2 \equiv 1 \pmod{2} \end{array} \right\} \implies n_2 \in \{1, 3\}$$

Concluimos que $n_2 = 1$, de donde el 2-subgrupo de Sylow es V , que era normal en A_4 .

- 3-subgrupo de Sylow de orden 3:

$$\left. \begin{array}{l} n_3 \mid 4 \\ n_3 \equiv 1 \pmod{3} \end{array} \right\} \implies n_3 \in \{1, 4\}$$

Y serán los subgrupos de A_4 generados por los 3-ciclos.

- En S_4 , $|S_4| = 24 = 2^3 \cdot 3$:
 - Para los 2-subgrupos:

$$\left. \begin{array}{l} n_2 \mid 3 \\ n_2 \equiv 1 \pmod{2} \end{array} \right\} \implies n_2 \in \{1, 3\}$$

Si suponemos que $n_2 = 1$, sea Q un grupo con $|Q| = 8$ que sea el 2-subgrupo de Sylow. En dicho caso, todas las trasposiciones deben estar contenidas en Q (por ser de orden 2), pero todas las trasposiciones generan a S_4 , luego $Q = S_4$, contradicción.

Por tanto, tenemos $n_2 = 3$, tenemos 3 2-subgrupos de Sylow: Q_1, Q_2 y Q_3 . El grupo de Klein V es un 2-subgrupo, y es normal en S_4 . Por tanto, va a estar contenido en algún Q_k ($k \in \{1, 2, 3\}$). Supongamos que $V < Q_1$. Como todos ellos son conjugados, $\exists \alpha, \beta \in S_4$ de forma que:

$$\begin{aligned} Q_2 &= \alpha Q_1 \alpha^{-1} \\ Q_3 &= \beta Q_1 \beta^{-1} \end{aligned}$$

Y si multiplicamos (como $V \triangleleft S_4$):

$$\begin{aligned} V &= \alpha V \alpha^{-1} < \alpha Q_1 \alpha^{-1} = Q_2 \\ V &= \beta V \beta^{-1} < \beta Q_1 \beta^{-1} = Q_3 \end{aligned}$$

De donde deducimos que $V < Q_k$ para todo $k \in \{1, 2, 3\}$. Los Q_k contendrán a V y a alguna transposición:

$$\begin{aligned} Q_1 &= V \langle (1 \ 2) \rangle \\ Q_2 &= V \langle (1 \ 3) \rangle \\ Q_3 &= V \langle (1 \ 4) \rangle \end{aligned}$$

- Para los 3-subgrupos de Sylow:

$$\left. \begin{array}{l} n_3 \mid 8 \\ n_3 \equiv 1 \pmod{3} \end{array} \right\} \implies n_3 \in \{1, 4\}$$

Los subgrupos de orden 4 de S_4 son:

$$\langle (1\ 2\ 3) \rangle, \langle (1\ 2\ 4) \rangle, \langle (1\ 3\ 4) \rangle, \langle (2\ 3\ 4) \rangle$$

Que son los 3-subgrupos de Sylow.

Corolario 2.14.1. *Sea P un p -subgrupo de Sylow de un grupo finito G . Entonces:*

$$P \text{ es el } \text{único } p\text{-subgrupo de Sylow} \iff P \triangleleft G$$

Demostración. Por doble implicación:

\implies) Si P es el único, como todos los conjugados de P son subgrupos de Sylow, tendremos que:

$$gPg^{-1} = P \quad \forall g \in G$$

Que era la caracterización de subgrupo normal de G .

\impliedby) Supuesto que $P \triangleleft G$, sea Q otro p -subgrupo de Sylow, como P y Q han de ser conjugados, sabemos que $\exists g \in G$ de forma que $gPg^{-1} = Q$, pero por ser $P \triangleleft G$, tenemos también que $P = gPg^{-1}$, luego:

$$P = gPg^{-1} = Q$$

□

Ejemplo. Todo grupo de orden 35 es resoluble.

Demostración. Sea G un grupo con $|G| = 35 = 5 \cdot 7$, vemos que:

$$\left. \begin{array}{l} n_7 \mid 5 \\ n_7 \equiv 1 \pmod{5} \end{array} \right\} \implies n_7 = 1$$

En dicho caso, tenemos un único 7-subgrupo de Sylow $H < G$, que además es normal y tendrá orden 7. En dicho caso, sabemos que será isomorfo a \mathbb{Z}_7 . Como los grupos abelianos son resolubles, tenemos que H es resoluble. Si consideramos el cociente:

$$|G/H| = 5$$

Por lo que $G/H \cong \mathbb{Z}_5$ y G/H será resoluble por ser isomorfo a un grupo abeliano. Deducimos que G es resoluble, por existir $H \triangleleft G$ y ser H y G/H resolubles. □

Se puede demostrar de forma análoga que ciertos grupos de cierto orden son siempre resolubles.

Teorema 2.15. *Sea G un grupo finito en el que todos sus subgrupos de Sylow son normales, entonces G es el producto directo interno de sus subgrupos de Sylow:*

$$G = \prod_{H \in \text{Syl}(G)} H$$

Demostración. En la caracterización de producto directo interno para una cantidad finita de subgrupos (Teorema ??), vimos que G era producto directo interno de todos ellos (los llamaremos H_i con $i \in \{1, \dots, n\}$) si y solo si:

- $H_i \triangleleft G$ para todo $i \in \{1, \dots, n\}$.
- $H_1 H_2 \dots H_n = G$.
- $(H_1 \dots H_{i-1}) \cap H_i = \{1\}$ para todo $i \in \{2, \dots, k\}$

Basta pues, demostrar estos 3 puntos. Supuesto que $|G| = p_1^{n_1} \dots p_k^{n_k}$, llamamos P_i al único p_i -subgrupo de Sylow, para todo $i \in \{1, \dots, k\}$.

- Por hipótesis, tendremos que $P_i \triangleleft G$ para todo $i \in \{1, \dots, k\}$.
- También:

$$|P_1 P_2 \dots P_k| = |P_1| |P_2| \dots |P_k| = |G|$$

De donde concluimos que $P_1 P_2 \dots P_k = G$.

- Fijado $i \in \{2, \dots, k\}$, veamos que $(P_1 \dots P_{i-1}) \cap P_i = \{1\}$. Para ello, sea $x \in (P_1 \dots P_{i-1}) \cap P_i$, tenemos:

$$\left. \begin{array}{l} O(x) \mid |P_1 \dots P_{i-1}| = p_1^{n_1} \dots p_{i-1}^{n_{i-1}} \\ O(x) \mid |P_i| = p_i^{n_i} \end{array} \right\} \implies O(x) = 1 \implies x = 1$$

□

Observación. Notemos que cualquier grupo abeliano finito es producto directo interno de sus subgrupos de Sylow, ya que en cualquier grupo abeliano los subgrupos son normales.

3. Clasificación de grupos abelianos finitos

El objetivo final del tema es demostrar los teoremas de estructura de los grupos abelianos finitos, que permiten clasificar todos estos grupos según su orden (para cada orden tendremos una clasificación), salvo isomorfismos.

Serán de especial relevancia varios resultados que ya hemos visto:

- $C_n \times C_m \cong C_{nm} \iff \text{mcd}(n, m) = 1$, en la Proposición ??.
- Si $|G| = p_1^{n_1} \dots p_k^{n_k}$ y G tenía un único P_i p_i -subgrupo de Sylow para cada $i \in \{1, \dots, k\}$, entonces $G \cong P_1 \times P_2 \times \dots \times P_k$.

Como trabajaremos con subgrupos abelianos, recordamos que la notación que usábamos para el producto directo de grupos abelianos era \oplus .

Teorema 3.1 (Estructura de los p -grupos abelianos finitos).

Sea A un p -grupo abeliano finito con orden $|A| = p^n$ para $n \geq 1$, entonces existen enteros $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$ de forma que:

$$\beta_1 + \beta_2 + \dots + \beta_t = n \quad y \quad A \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \dots \oplus C_{p^{\beta_t}}$$

Además, esta expresión es única, es decir, si existen $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_s \geq 1$ de forma que:

$$\alpha_1 + \alpha_2 + \dots + \alpha_s = n \quad y \quad A \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \dots \oplus C_{p^{\alpha_s}}$$

entonces $s = t$ y $\alpha_k = \beta_k$, para todo $k \in \{1, \dots, t\}$.

Observación. Notemos que lo que estamos haciendo es tomar particiones de n de la forma β_i , y este Teorema nos dice que el p -grupo puede escribirse de forma única salvo isomorfismos como producto de ciertos subgrupos cíclicos.

Es decir, existen tantos p -grupos abelianos de orden p^n como particiones tengamos del número n .

Ejemplo. Por ejemplo:

- Grupos abelianos finitos de orden $8 = 2^3$, tenemos como particiones:

$$\begin{aligned} 3 &\implies A \cong C_8 \\ 1, 2 &\implies A \cong C_4 \oplus C_2 \\ 1, 1, 1 &\implies A \cong C_2 \oplus C_2 \oplus C_2 \end{aligned}$$

- Los grupos abelianos finitos de orden $81 = 3^4$, tenemos como particiones:

$$\begin{aligned} A &\cong C_{81} \\ A &\cong C_{27} \oplus C_3 \\ A &\cong C_9 \oplus C_9 \\ A &\cong C_9 \oplus C_3 \oplus C_3 \\ A &\cong C_3 \oplus C_3 \oplus C_3 \oplus C_3 \end{aligned}$$

Teorema 3.2 (Estructura de los grupos abelianos finitos).

Sea A un grupo abeliano finito con $|A| = p_1^{\gamma_1} \dots p_k^{\gamma_k}$ siendo p_i primo $\forall i \in \{1, \dots, k\}$, entonces:

$$A \cong \bigoplus_{i=1}^k \left(\bigoplus_{j=1}^{t_i} C_{p_i}^{n_{ij}} \right)$$

Donde para cada $i \in \{1, \dots, k\}$ tenemos:

$$\begin{aligned} n_{i1} &\geq n_{i2} \geq \dots \geq n_{it_i} \geq 1 \\ n_{i1} + n_{i2} + \dots + n_{it_i} &= r_i \end{aligned}$$

Y la descomposición es única salvo el orden.

Esta última recibe el nombre de descomposición cíclica primaria, y a los $p_i^{n_{ij}}$ con $i \in \{1, \dots, k\}$ y $j \in \{1, \dots, t_i\}$ se les llama divisores elementales de A .

Demostración. Si A es abeliano y finito, entonces todos sus p -subgrupos de Sylow son normales, luego podemos escribir:

$$A = P_1 \oplus P_2 \oplus \dots \oplus P_k$$

Siendo P_1, P_2, \dots, P_k el conjunto de todos sus p -subgrupos de Sylow, de forma que $|P_i| = p_i^{r_i}$, para todo $i \in \{1, \dots, k\}$. Como cada P_i es un p_i -subgrupo abeliano finito, aplicando el Teorema 3.1, podemos escribir:

$$P_i = \bigoplus_{j=1}^{t_i} C_{p_i}^{n_{ij}} \quad \forall i \in \{1, \dots, k\}$$

De donde tenemos la expresión de la tesis.

A cada P_i con $i \in \{1, \dots, k\}$ lo llamaremos componente p_i -primaria de A . \square

Ejemplo. Si tenemos un subgrupo finito abeliano A con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$, veamos los divisores elementales:

Div. elementales	Descomp. cíclica primaria
$2^3 \ 3^2 \ 5$	$C_8 \oplus C_9 \oplus C_5$
$2^2 \ 2 \ 3^2 \ 5$	$C_4 \oplus C_2 \oplus C_9 \oplus C_5$
$2 \ 2 \ 2 \ 3^2 \ 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$
$2^3 \ 3 \ 3 \ 5$	$C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8$
$2 \ 2^2 \ 3 \ 3 \ 5$	$C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5$
$2 \ 2 \ 2 \ 3 \ 3 \ 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$

Serían todas las descomposiciones cíclicas primarias de A . Es decir, A será isomorfo a cualquiera de esos.

Sin embargo, si recordamos la Proposición ??, esto nos llevará a la descomposición cíclica, donde observaremos por ejemplo que:

$$\begin{aligned}
 C_8 \oplus C_9 \oplus C_5 &\cong C_{360} \\
 C_4 \oplus C_2 \oplus C_9 \oplus C_5 &\cong C_{180} \oplus C_2 \\
 C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5 &\cong C_{90} \oplus C_2 \oplus C_2 \\
 C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8 &\cong C_{120} \oplus C_3 \\
 C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5 &\cong C_{60} \oplus C_6 \\
 C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5 &\cong C_{30} \oplus C_6 \oplus C_2
 \end{aligned}$$

Ahora, usaremos que:

$$C_n \times C_m \cong C_{nm} \iff \text{mcd}(n, m) = 1$$

Teorema 3.3 (Descomposición cíclica de un grupo abeliano finito).

Si A es un grupo abeliano finito, entonces:

$$A \cong C_{d_1} \oplus C_{d_2} \oplus \dots \oplus C_{d_t}$$

Donde los d_i son enteros positivos de forma que:

$$d_1 d_2 \dots d_t = |A|$$

Y $d_i \mid d_j$ para cada $j \leq i$. Además, la descomposición es única salvo el orden, para cada partición.

Demostración. Supuesto que $|A| = p_1^{r_1} \dots p_k^{r_k}$, si usamos la descomposición que nos da el Teorema 3.2:

$$A \cong \bigoplus_{i=1}^k \left(\bigoplus_{j=1}^{t_i} C_{p_i}^{n_{ij}} \right)$$

Para ciertos:

$$\begin{aligned}
 n_{i1} &\geq n_{i2} \geq \dots \geq n_{it_i} \geq 1 \\
 n_{i1} + n_{i2} + \dots + n_{it_i} &= r_i
 \end{aligned}$$

Sea $t = \max t_1, t_2, \dots, t_k$, si $t_i < l \leq t$, tendremos entonces que $n_{il} = 0$.

Lo que estamos haciendo es dada una partición, como por ejemplo la $\{2, 2^2, 3^2, 5\}$, denotar por t_i al número de particiones de cada número y por n_{ij} a los exponentes de cada una de las particiones, construyendo la tabla:

$$\left\{ \begin{array}{c|cc} t_1 & n_{11} & n_{12} \\ t_2 & n_{21} & n_{22} \\ t_3 & n_{31} & n_{32} \end{array} \right.$$

De esta forma, tenemos:

$$\begin{pmatrix} p_1^{n_{11}} & p_2^{n_{21}} & \dots & p_k^{n_{k1}} \\ p_1^{n_{12}} & p_2^{n_{22}} & \dots & p_k^{n_{k2}} \\ \vdots & \vdots & \ddots & \vdots \\ p_1^{n_{1k}} & p_2^{n_{2k}} & \dots & p_k^{n_{kk}} \end{pmatrix}$$

Y A es la suma directa de los cíclicos con órdenas las entradas de las columnas. Si tomamos el producto por columnas obtenemos la cíclica primaria y si la hacemos por filas la que estamos interesados:

$$\begin{aligned} d_1 &= p_1^{n_{11}} p_2^{n_{21}} \dots p_k^{n_{k1}} \\ &\vdots \\ d_t &= p_1^{n_{1t}} p_2^{n_{2t}} \dots p_k^{n_{kt}} \end{aligned}$$

Efectivamente, tendremos que:

$$d_1 d_2 \dots d_t = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} = |A|$$

Como $n_{ij} \geq n_{i,j+1}$, tendremos entonces que $d_i \mid d_j$, para todo $j \leq i$. Además, tendremos que:

$$\begin{aligned} C_{d_1} &\cong C_{p_1^{n_{11}}} \oplus C_{p_2^{n_{21}}} \oplus \dots \oplus C_{p_k^{n_{k1}}} \\ &\vdots \\ C_{d_t} &\cong C_{p_1^{n_{1t}}} \oplus C_{p_2^{n_{2t}}} \oplus \dots \oplus C_{p_k^{n_{kt}}} \end{aligned}$$

De donde $A \cong C_{d_1} \oplus C_{d_2} \oplus \dots \oplus C_{d_t}$. La unicidad viene de la unicidad dada por la descomposición del Teorema 3.2. \square

Los d_i reciben el nombre de factores invariantes.

Ejemplo. Sea A un grupo abeliano finito con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$:

- Para la partición $\{2^3, 3^2, 5\}$, tenemos que:

$$A \cong C_8 \oplus C_9 \oplus C_5$$

Los factores invariantes serán:

$$d_1 = 2^3 \cdot 3^2 \cdot 5$$

Por lo que la descomposición cíclica será $A \cong C_{360}$.

- Para la partición $\{2^2, 2, 3^2, 5\}$, la descomposición cíclica primaria fue:

$$A \cong C_4 \oplus C_2 \oplus C_9 \oplus C_5$$

En este caso, tendremos $t = \max\{2, 1, 1\} = 2$, por lo que tendremos dos factores invariantes:

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

Por lo que tendremos (los productos de las filas):

$$\begin{aligned} d_1 &= 2^2 \cdot 3^2 \cdot 5 = 180 \\ d_2 &= 2 \cdot 1 \cdot 1 = 2 \end{aligned}$$

Y la descomposición cíclica es:

$$A \cong C_{180} \oplus C_2$$

- Para la descomposición $\{2, 2, 2, 3^2, 5\}$, tenemos:

$$A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$$

Y tendremos $t = 3$:

$$\begin{pmatrix} d_1 = & 2 & 3^2 & 5 \\ d_2 = & 2 & 1 & 1 \\ d_3 = & 2 & 1 & 1 \end{pmatrix}$$

Por lo que:

$$A \cong C_{90} \oplus C_2 \oplus C_2$$

- Para $\{2^3, 3, 3, 5\}$:

$$A \cong C_8 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

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

Y la descomposición cíclica será:

$$A \cong C_{120} \oplus C_3$$

- Para $\{2^2, 2, 3, 3, 5\}$:

$$A \cong C_4 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

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

Por lo que tenemos la descomposición cíclica:

$$A \cong C_{60} \oplus C_6$$

- Para $\{2, 2, 2, 3, 3, 5\}$:

$$A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$$

Tenemos:

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

Y:

$$A \cong C_{30} \oplus C_6 \oplus C_2$$

En el caso particular de que todos los primos tengan exponente 1:

Corolario 3.3.1. Si A es un grupo abeliano finito con $|A| = p_1 p_2 \dots p_k = n$, entonces salvo isomorfismo, el único grupo abeliano de orden n es el cíclico C_n .

Demostración. Utilizando el Teorema 3.2, podemos escribir:

$$A \cong C_{p_1} \oplus C_{p_2} \oplus \dots \oplus C_{p_k}$$

Y como $\text{mcd}(p_i, p_j) = 1$ para cada $i, j \in \{1, \dots, k\}$ con $i \neq j$, tenemos que:

$$C_{p_1} \oplus C_{p_2} \oplus \dots \oplus C_{p_k} = C_{p_1 p_2 \dots p_k} = C_n$$

□

Ejemplo. Sea A un grupo abeliano finito con $|A| = 580 = 2^2 \cdot 3^2 \cdot 5$, busquemos clasificarlo según la descomposición cíclica:

Descomposición	desc. cíclica primaria	factores invariantes	desc. cíclica
$\{2^2, 3^2, 5\}$	$C_4 \oplus C_9 \oplus C_5$	$2^2 \cdot 3^2 \cdot 5 = 180$	C_{180}
$\{2, 2, 3^2, 5\}$	$C_2 \oplus C_2 \oplus C_9 \oplus C_5$	$d_1 = 2 \cdot 9 \cdot 5 = 90$ $d_2 = 2$	$C_{90} \oplus C_2$
$\{2^3, 3, 3, 5\}$	$C_4 \oplus C_3 \oplus C_3 \oplus C_5$	$d_1 = 2^2 \cdot 3 \cdot 5 = 60$ $d_2 = 3$	$C_{60} \oplus C_3$
$\{2, 2, 3, 3, 5\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$	$d_1 = 2 \cdot 3 \cdot 5 = 30$ $d_2 = 2 \cdot 3 = 6$	$C_{30} \oplus C_6$

Ejemplo. Listar los órdenes de todos los elementos de un grupo de orden 8. Sea A un grupo abeliano finito de orden 8, entonces lo podemos clasificar en:

- C_8 :
 - Los elementos $\{1, 3, 5, 7\}$ tienen orden 8.
 - $O(0) = 1$.
 - $O(2) = 8/\text{mcd}(2, 8) = 4 = O(6)$.
 - $O(4) = 2$.
- $C_4 \oplus C_2$, aplicamos que $O(a, b) = \text{mcm}(O(a), O(b))$: Como los órdenes de los elementos en C_4 son: $\{1, 2, 4\}$ y en C_2 son $\{1, 2\}$, las posibilidades son: $\{1, 2, 4\}$:
 - $O(0, 0) = 1$.
 - $O(0, 1) = 2$.
 - $O(1, b) = 4 = O(3, b), \forall b \in C_2$
 - $O(2, b) = 2, \forall b \in C_2$.
- $C_2 \oplus C_2 \oplus C_2$, los órdenes son $\{1, 2\}$ y todos tienen orden 2 salvo el elemento $(0, 0, 0)$, que tiene orden 1.

Ejemplo. Listar los órdenes de todos los elementos de un grupo abeliano A de orden 12.

Sea A con $|A| = 12 = 2^2 \cdot 3$, tenemos $A \cong \mathbb{Z}_{12}$ o $A \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

- En \mathbb{Z}_{12} :

- $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$.
- $O(2) = 6$.
- $O(3) = 4 = O(9)$.
- $O(4) = 3 = O(8)$.
- $O(6) = 2$.

■ En $\mathbb{Z}_6 \oplus \mathbb{Z}_2$:

$$O(a, b) = \text{mcm}(\text{Div}(6), \text{Div}(2)) = \text{mcm}(\{1, 2, 3, 6\}, \{1, 2\}) = \{1, 2, 3, 6\}$$

El orden de los elementos de \mathbb{Z}_6 son:

- $U(\mathbb{Z}_6) = \{1, 5\}$, luego $O(1) = O(5) = 6$.
- $O(2) = 3 = O(4)$.
- $O(3) = 2$.
- $O(0) = 1$.

Ahora:

- $O(0, 0) = 1$.
- $O(1, b) = O(5, b) = 6 \ \forall b \in \mathbb{Z}_2$.
- $O(3, b) = 2 \ \forall b \in \mathbb{Z}_2$.
- $O(2, 0) = O(4, 0) = 3$.
- $O(2, 1) = O(4, 1) = 6$.

3.1. Clasificación de grupos abelianos no finitos

Buscamos hallar la descomposición cíclica y la descomposición cíclica primaria de dos grupos cualesquiera. Para ello, recordamos varias definiciones que ya vimos.

Notación. Como trabajaremos con grupos abelianos finitos, usaremos la notación aditiva.

Definición 3.1. Un grupo abeliano A se dice que es finitamente generado si existe un conjunto:

$$X = \{x_1, \dots, x_r\} \subseteq A$$

De forma que para todo $a \in A$, existirán $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ de forma que:

$$a = \sum_{k=1}^r \lambda_k x_k$$

En dicho caso, diremos que X es un sistema de generadores de A , y notaremos:

$$A = \langle x_1, \dots, x_r \rangle$$

Definición 3.2 (Base). Sea A un grupo abeliano, un conjunto de generadores $X = \{x_1, \dots, x_r\}$ de A es una base si son \mathbb{Z} -linealmente independientes.

En dicho caso A es un grupo abeliano libre de rango r .

Observación. Observemos que si A es un grupo abeliano libre de rango r , entonces tendremos que:

$$A \cong \mathbb{Z}^r$$

Además, si $H < A$, tendremos entonces que $H \cong \mathbb{Z}^s$, para cierta $s \leq r$.

De esta forma, si A es un grupo finitamente generado, podemos descomponerlo en:

$$A \cong F \oplus T(A)$$

Que será la descomposición estándar de A . F será un grupo abeliano libre de rango finito y:

$$T(A) = \{a \in A \mid O(a) < +\infty\}$$

Que recibe el nombre de subgrupo de torsión de A .

Proposición 3.4. *El subgrupo de torsión de un grupo es un grupo abeliano finito.*

De esta forma, existirán $r \geq 0$ y d_1, \dots, d_s con $d_i \mid d_j$ con $j \leq i$ de forma que:

$$d_1 d_2 \dots d_s = |T(A)|$$

Por lo que:

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \dots \oplus \mathbb{Z}_{d_s}$$

- Llamaremos r al rango de A .
- A los d_i los llamaremos factores invariantes de A .

Ejemplo. Si tomamos:

$$A = \langle x, y, z \mid x^3 = y^4, x^2 z = z^{-1} y, xy = yx, xz = zx, yz = zy \rangle$$

Si lo escribimos en notación aditiva:

$$A = \langle x, y, z \mid 3x = 4y, 2x + z = y - z, x + y = y + x, x + z = z + x, y + z = z + y \rangle$$

Si nos olvidamos de las últimas y pensamos que el grupo es abeliano, así como despejando:

$$A = \langle x, y, z \mid 3x - 4y = 0, 2x - y + 2z = 0 \rangle$$

Y tenemos el sistema:

$$M = \begin{pmatrix} 3 & -4 & 0 \\ 2 & -1 & 2 \end{pmatrix}$$

Tenemos 3 incógnitas y $rg(M) = 2$, un Sistema Compatible Indeterminado, con un parámetro libre. Veremos que transformaremos M en:

$$\begin{pmatrix} 3 & -4 & 0 \\ 2 & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

Que es la forma normal de Smith (parecido a Hermite pero en \mathbb{Z}). De esta forma, tendremos que:

$$A \cong \mathbb{Z} \oplus \{0\} \oplus \mathbb{Z}_2 \cong \mathbb{Z} \oplus \mathbb{Z}_2$$

Sea:

$$A = \left\langle x_1, x_2, \dots, x_n \mid \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{array} \right\rangle$$

con n generadores y $m \leq n$ relaciones siendo. Sea:

$$X = \{e_1, \dots, e_n\}$$

Consideramos $F = \langle X \rangle$, que será $F \cong \mathbb{Z}^r$. La descomposición estándar de A será:

$$A = F + T(A)$$

Si definimos:

$$\begin{aligned} \varphi: F &\longrightarrow A \\ e_i &\longmapsto x_i \end{aligned}$$

Tenemos que φ está bien definida, así como que es sobreyectiva. Tendremos:

$$\ker(\varphi) < F$$

Por lo que:

$$\ker(\varphi) \cong \mathbb{Z}^m$$

De esta forma, si $\{y_1, \dots, y_m\}$ es una base de $\ker(\varphi)$, cumplirá que (basta aplicar φ):

$$\begin{cases} a_{11}e_1 + a_{12}e_2 + \dots + a_{1n}e_n = y_1 \\ \vdots \\ a_{m1}e_1 + a_{m2}e_2 + \dots + a_{mn}e_n = y_m \end{cases}$$

De esta forma, tenemos:

$$\ker(\varphi) \xrightarrow{i} F \rightarrow A$$

De forma que la matriz:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

A la que llamaremos matrices de relaciones del grupo, que nos lleva el vector (y_1, \dots, y_m) en (x_1, \dots, x_n) , tras multiplicar por (e_1, \dots, e_n) , y tendremos aplicando Teoremas de Isomorfía que:

$$A \cong F / \ker(\varphi)$$

Esta matriz la convertiremos en la forma normal de Smith.

Como los factores invariantes eran productos de primos, no nos podrá salir ningún 1, por lo que esos unos los eliminaremos, ya que como factores invariantes han de ser mayor que 1.

Ejemplo. En $A = \mathbb{Z} \oplus \mathbb{Z}_2$, una base para \mathbb{Z} es:

$$X = \{1\}$$

Y un sistema de generadores para $\mathbb{Z} \oplus \mathbb{Z}_2$ es:

$$\{(1, 1)\}$$

3.1.1. Forma Normal de Smith de una matriz

Ejemplo. Una forma de Hermite por filas es:

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

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

Las operaciones elementales sobre matrices eran:

- Intercambiar filas.
- Multiplicar una fila por un número.
- Sumar un múltiplo de una fila a otra.

Al hacer la forma normal de Smith podemos encontrar dos matrices P y Q regulares de forma que:

$$PAQ = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_s \\ & & & & 0 \end{pmatrix}$$

De forma que $d_i \mid d_{i+1}$. P contenía las transformaciones elementales por filas y Q por columnas.

Ejemplo. Si consideramos:

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix}$$

Como mcd de todos los elementos es 1, tenemos que poner un 1 arriba (consejo: no hacer ceros hasta poner un 1). Para ello, hacemos la cuarta fila más la segunda:

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 1 & 6 & 0 \end{pmatrix}$$

Si nos la llevamos a la primera posición:

$$\begin{pmatrix} 1 & 6 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

Ahora, hacemos ceros en la primera fila, salvo el 1. Restamos a la primera la cuarta multiplicada por 3:

$$\begin{pmatrix} 1 & 0 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

Como el mcd es 2, hay que sacar un 2 en la posición 2, 2. Para ello, intercambiamos las filas segunda y cuarta:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 6 \\ 0 & -4 & -6 \end{pmatrix}$$

Hacemos ceros:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Como el mcd es 6 y tenemos un 6, hemos terminado. Hemos conseguido la forma normal de Smith.

Ejemplo. Calcular el rango de A y todos los grupos abelianos no isomorfos de orden igual que la torsión.

$$A = \left\langle x, y, z, t \mid \begin{array}{l} 14x + 4y + 4z + 14t = 0 \\ -6x + 4y + 4z + 10t = 0 \\ -16x - 4y - 4z - 20t = 0 \end{array} \right\rangle$$

Calculamos la forma normal de Smith de la matriz:

$$\begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \xrightarrow{F'_1 = -(F_1 + F_3)} \begin{pmatrix} 2 & 0 & 0 & 6 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \xrightarrow{C_4 - 3C_1}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ -6 & 4 & 4 & 28 \\ -16 & -4 & -4 & 28 \end{pmatrix} \xrightarrow{\substack{F_2 + 3F_1 \\ F_3 + 8F_1}} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & 28 \\ 0 & -4 & -4 & 28 \end{pmatrix} \xrightarrow{F_2 + F_3}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 56 \\ 0 & -4 & -4 & 28 \end{pmatrix} \xrightarrow{F_2 \leftrightarrow F_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -4 & -4 & 28 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{F'_2 = -F_2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & -28 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{C_3 + 7C_2}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{C_3 - C_2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{C_3 \leftrightarrow C_4} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 56 & 0 \end{pmatrix}$$

Por tanto, el rango de A es (el número de incógnitas menos el rango de la matriz)

3. Ahora, la descomposición cíclica sería:

$$T(A) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{56}$$

Y la descomposición cíclica primaria:

$$T(A) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_7$$

Y tendremos:

$$A \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{56} \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_7$$

Para ello, buscamos los grupos G con orden $2 \cdot 4 \cdot 8 \cdot 7 = 448 = 2^6 \cdot 7$ y descartamos el isomorfo a $T(A)$:

Divisores elementales	Factores invariantes
$2^6, 7$	448
$2, 2^5, 7$	2, 224
$2, 2, 2^4, 7$	2, 2, 112
$2, 2, 2, 2, 2^3, 7$	2, 2, 2, 56
$2, 2, 2, 2, 2, 2^2, 7$	2, 2, 2, 2, 28
$2, 2, 2, 2, 2, 2, 2, 7$	2, 2, 2, 2, 2, 14
$2, 2^2, 2^3, 7$	2, 4, 56
$2^2, 2^2, 2^2, 7$	4, 4, 28
$2^3, 2^3, 7$	8, 56
$2^2, 2^4, 7$	4, 112
$2, 2, 2^2, 2^2$	2, 2, 4, 28

¿Hay algún elemento de orden infinito en A ? Sí:

$$(1, 0, 0, 0)$$

¿Hay algún elemento de orden 56? Sí:

$$(0, 0, 0, 1)$$

¿Hay algún elemento de orden 8? Sí:

$$(0, 0, 0, 7)$$

O también:

$$(0, 1, 1, 7)$$

Ejemplo. Forma normal de Smith de:

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

Como no está en forma normal, hemos de añadir elementos para poder hayar el 2:

$$2 = \text{mcd}(4, 6, 8)$$

$$\begin{aligned}
& \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_2+F_1} \begin{pmatrix} 4 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2-C_1} \begin{pmatrix} 4 & -4 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \\
& \begin{pmatrix} -4 & 4 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 4 & 0 \\ -4 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 4 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \\
& \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 8 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 8 \\ 0 & -8 & 8 \end{pmatrix} \longrightarrow \\
& \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 8 \\ 0 & 0 & 24 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 24 \end{pmatrix}
\end{aligned}$$

Ejemplo. Sea G un grupo abeliano de orden n y $l(G)$ su longitud (la longitud de su serie de composición). Si la descomposición en factores primos de n es:

$$n = p_1^{r_1} \dots p_r^{e_r}$$

Entonces:

$$l(G) = e_1 + \dots + e_r$$

Y los factores de composición son:

$$fact(G) = (C_{p_1}, \cdot^{e_1}, C_{p_1}, C_{p_2}, \cdot^{e_2}, C_{p_2}, \dots, C_{p_r}, \cdot^{e_r}, C_{p_r})$$

Como:

$$G \cong (C_{p_1}^{\alpha_{11}} \oplus \dots \oplus C_{p_1}^{\alpha_{1n_1}}) \oplus \dots \oplus (C_{p_r}^{\alpha_{r1}} \oplus \dots \oplus C_{p_r}^{\alpha_{rn_1}})$$

Para:

$$\begin{aligned}
\alpha_{11} &\geq \dots \geq \alpha_{1n_1} \geq 1 & \alpha_{11} + \dots + \alpha_{1n_1} &= e_1 \\
&\vdots & &\vdots \\
\alpha_{r1} &\geq \dots \geq \alpha_{rn_1} \geq 1 & \alpha_{r1} + \dots + \alpha_{rn_1} &= e_r
\end{aligned}$$

Como G es abeliano, los factores de composición son cíclicos.

Para conseguir la serie de composición, lo que haremos será considerar la descomposición de G en suma de grupos cíclicos y en cada paso, iremos quitando un grupo cíclico:

$$\begin{aligned}
G_1 &= (C_{p_1}^{\alpha_{12}} \oplus \dots \oplus C_{p_1}^{\alpha_{1n_1}}) \oplus \dots \oplus (C_{p_r}^{\alpha_{r1}} \oplus \dots \oplus C_{p_r}^{\alpha_{rn_1}}) \\
G_2 &= (C_{p_1}^{\alpha_{13}} \oplus \dots \oplus C_{p_1}^{\alpha_{1n_1}}) \oplus \dots \oplus (C_{p_r}^{\alpha_{r1}} \oplus \dots \oplus C_{p_r}^{\alpha_{rn_1}}) \\
&\vdots \\
G_{n_1} &= (C_{p_2}^{\alpha_{21}} \oplus \dots \oplus C_{p_2}^{\alpha_{2n_2}}) \oplus \dots \oplus (C_{p_r}^{\alpha_{r1}} \oplus \dots \oplus C_{p_r}^{\alpha_{rn_1}}) \\
&\vdots
\end{aligned}$$

Ejemplo. Sea A un grupo con $|A| = 40 = 2^3 \cdot 5$:

Descomposición	Descomp. cíclica primaria	Factores invariantes	Descomp. cíclica
$2^3, 5$	$C_8 \oplus C_5$	40	C_{40}
$2, 2^2, 5$	$C_2 \oplus C_4 \oplus C_5$	2, 20	$C_2 \oplus C_{20}$
$2, 2, 2, 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_5$	2, 2, 10	$C_2 \oplus C_2 \oplus C_{10}$

Como $l(A) = 4$ por el ejercicio anterior, series de composición serán:

$$\begin{aligned} C_{40} \triangleright C_{20} \triangleright C_{10} \triangleright C_5 \triangleright \{1\} \\ C_{40} \triangleright C_8 \triangleright C_4 \triangleright C_2 \triangleright \{1\} \end{aligned}$$

Los factores de composición de la primera son:

$$C_{40}/C_{20} \cong C_2 \quad C_{20}/C_{10} \cong C_2 \quad C_{10}/C_5 \cong C_2 \quad C_5/\{1\} \cong C_5$$

Ejemplo. Sea:

$$G = \langle a, b, c \mid \begin{array}{l} 2a - 6b + 18c = 0 \\ 6a + 6c = 0 \end{array} \rangle$$

Y sea:

$$H = \mathbb{Z}^3 / \langle (1, -9, 3), (1, -7, 1), (1, -1, 1) \rangle$$

Tenemos la matriz:

$$\begin{pmatrix} 2 & -6 & 18 \\ 6 & 0 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & -6 & 18 \\ 0 & 18 & -48 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 48 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix} \longrightarrow$$

Por lo que G tiene rango 1 y sus descomposiciones cíclica y cíclica primaria son:

$$G \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Con H tenemos lo mismo:

$$\begin{pmatrix} 1 & 1 & 1 \\ -9 & -7 & -1 \\ 3 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ -9 & 2 & 8 \\ 3 & -2 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & -2 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 0 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Por lo que:

$$H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$$

y H no tiene parte libre. Tendremos:

$$l(H) = 3$$

Los factores de composición serán $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

$$\begin{aligned} G &\not\cong H \\ T(G) &\cong T(H) = H \end{aligned}$$

¿Cuáles son los elementos de orden 6 de H ? Tiene al menos:

$$O(a, 1) = O(a, 5) = 6 \quad \forall a \in \mathbb{Z}_2$$

También tendremos:

$$O(1, 2) = \text{mcm}(O(1), O(2)) = \text{mcm}(2, 3) = 6$$

¿ G tiene elementos de orden 6? Sí, los mismos pero con un 0 en primera coordenada.

4. Clasificación de grupos de orden bajo

Clasificar grupos es una tarea dura y difícil, por lo que nos centraremos en grupos de orden bajo.

4.1. Grupos abelianos

Sabemos ya clasificar los grupos abelianos de orden menor o igual que 15:

Orden	Grupo
1	$\{1\}$
2	C_2
3	C_3
4	$C_2 \oplus C_2, C_4$
5	C_5
6	C_6
7	C_7
8	$C_2 \oplus C_2 \oplus C_2, C_2 \oplus C_4 \oplus C_8$
9	$C_9, C_3 \oplus C_3$
10	C_{10}
11	C_{11}
12	$C_{12}, C_6 \oplus C_2$
13	C_{13}
14	C_{14}
15	C_{15}
\vdots	\vdots

En general, si $|G| = p$ primo, tendremos C_p .

Si el grupo no es finito, nos dan la presentación y también sabemos clasificarlos. Nos centraremos por tanto en los grupos no abelianos.

4.2. Producto semidirecto

Será una especie de producto que nos permitirá escribir muchos grupos no abelianos. Con esta herramienta podremos escribir muchos grupos no abelianos (aunque no todos).

Ejemplo. En el Capítulo ?? vimos que $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ es isomorfo a:

$$Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$$

Es decir, teníamos una aplicación (gracias a Teorema de Dyck) $f : Q_2 \rightarrow Q_2^{\text{abs}}$ dada por:

$$f(x) = i \quad f(y) = j$$

Que además era un epimorfismo, porque $Q_2^{\text{abs}} = \langle i, j \rangle$. Veamos que $|Q_2^{\text{abs}}| = 8$, de una forma distinta que contar elementos:

Demostración. Como $x^4 = 1$, si consideramos $H = \langle x \rangle$, tendremos que $|H| \leq 4$. Ahora, como:

$$yxy^{-1} = x^{-1} \in H$$

Tenemos que $H \triangleleft Q_2^{\text{abs}}$. Si escribimos Q_2^{abs} en su partición de clases:

$$Q_2^{\text{abs}} \cong H \cup yH$$

Ya que $y \notin H$, de donde al tomar cocientes:

$$Q_2^{\text{abs}}/H \cong \langle yH \rangle$$

Ahora, como:

$$(yH)^2 = y^2H = x^2H = H$$

Llegaremos a que:

$$|Q_2^{\text{abs}}/H| \leq 2$$

Si aplicamos el Primer Teorema de Isomorfía sobre f :

$$Q_2^{\text{abs}}/\ker(f) \cong \text{Im}(f) = Q_2$$

De donde $|Q_2^{\text{abs}}| = |Q_2| |\ker(f)| \geq 8$. Concluimos que $|Q_2^{\text{abs}}| = 8$. \square

El hecho de introducir Q_2^{abs} en el Capítulo ?? fue para ahora generalizar lo que hacíamos con Q_2 a todo grupo, con el producto semidirecto.

Definición 4.1 (Grupos dicíclicos). Para cada $k \in \mathbb{N} \setminus \{0\}$, definimos el k -ésimo grupo dicíclico como el grupo:

$$Q_k = \langle x, y \mid x^{2k} = 1, y^2 = x^k, yxy^{-1} = x^{-1} \rangle$$

Ejemplo. Veamos que:

- Para $k = 1$:

$$Q_1 = \langle x, y \mid x^2 = 1, y^2 = x, yxy^{-1} = x \rangle$$

Nos preguntamos qué grupo es. Si tratamos de describir los elementos, obtenemos:

$$\{1, x, y, xy\} = \{1, y, y^2, y^3\}$$

Es decir, $Q_1 \cong C_4$.

- Observemos que si $k = 2$, obtenemos Q_2^{abs} .

- Para $k \geq 3$, tendremos que tiene un cociente isomorfo a D_k , por lo que no será abeliano. Sin embargo, podemos acotar el orden de Q_k :

$$2k \leq |Q_k| \leq 4k \quad \forall k \geq 3$$

Y si k es impar, tendremos que $|Q_k| = 4k$.

Demostración. Si recordamos al grupo diédrico de orden k :

$$D_k = \langle r, s \mid r^k = s^2 = 1, sr = r^{-1}s \rangle$$

Tenemos que $r^{2k} = (r^k)^2 = 1$ y tenemos la primera relación. Para la segunda, tenemos que $s^2 = 1 = r^k$. Finalmente, $sr = r^{-1}s$ nos da la tercera (compruébese). Podemos aplicar el Teorema de Dyck, que nos da un homomorfismo $f : Q_k \rightarrow D_k$ de forma que:

$$f(x) = r \quad f(y) = s$$

Además, sabemos que f es un epimorfismo, ya que $D_k = \langle r, s \rangle$. Por el Primer Teorema de Isomorfía aplicado a f , podemos asegurar que:

$$Q_k / \ker(f) \cong D_k$$

Por tanto, el dicíclico de orden k no será abeliano.

\geq) Sabemos que $|D_k| = 2k$, y por el epimorfismo anterior, sabemos que $2k$ divide a $|Q_k|$, de donde $2k \leq |Q_k|$.

\leq) Usando que $x^{2k} = 1$, si tomamos $H = \langle x \rangle$, tenemos que:

$$|H| = |\langle x \rangle| \leq 2k$$

Como también tenemos que:

$$yxy^{-1} = x^{-1} \in H$$

Tendremos que $H \triangleleft Q_k$, de donde al considerar el cociente, tendremos al igual que antes que:

$$Q_k/H \cong \langle yH \rangle$$

De esta forma:

$$(yH)^2 = y^2H = x^kH = H$$

Por lo que $y^2 \notin yH$ y:

$$|Q_k/H| \leq 2$$

De donde deducimos que:

$$|Q_k| = |Q_k/H||H| \leq 4k$$

Suponiendo ahora que $k = 2t + 1$ para cierto $t \in \mathbb{N}$, consideramos el cíclico de orden 4:

$$C_4 = \langle a \mid a^4 = 1 \rangle$$

1. Tenemos que:

$$(a^2)^{2k} = (a^4)^k = 1$$

2. Además:

$$(a^2)^k = a^{2k} = a^{4t+2} = a^2$$

3. Finalmente:

$$aa^2 = a^3 = a^2a = (a^2)^{-1}a$$

Por el Teorema de Dyck, podemos construir el homomorfismo $f : Q_k \rightarrow C_4$ dado por:

$$f(x) = a^2 \quad f(y) = a$$

Que de hecho es un epimorfismo, ya que $C_4 = \langle a \rangle$. Al igual que antes:

$$Q_k / \ker(f) \cong C_4$$

De donde llegamos a que 4 divide a $|Q_k|$. Como además $2k$ divide a $|Q_k|$, tenemos que $\text{mcm}(2k, 4)$ divide a $|Q_k|$ y, como k era impar, tendremos que:

$$\text{mcm}(2k, 4) = 4$$

De donde $4k \leq |Q_k|$, que con la desigualdad anterior nos da la igualdad. \square

Ejemplo. Grupos no abelianos de orden 12 conocíamos:

- A_4 .
- D_6 .

Y ahora conocemos Q_3 . Próximamente veremos que estos grupos son los únicos, salvo isomorfismo.

Definición 4.2 (Producto semidirecto). Dados dos grupos, K , H y una acción $\theta : H \rightarrow \text{Aut}(K)$, consideramos el conjunto producto cartesiano:

$$G = K \times H = \{(k, h) \mid k \in K, h \in H\}$$

Sobre el que definimos la siguiente operación:

$$(k_1, h_1)(k_2, h_2) = (k_1^{h_1}k_2, h_1h_2)$$

Se verifica que $K \times H$ con esta operación tiene estructura de grupo, al que llamaremos **producto semidirecto de K por H relativo a θ** , que denotaremos por:

$$K \rtimes_{\theta} H$$

Teorema 4.1. *Se verifica que $K \times H$ con esta operación tiene estructura de grupo*

Demostración. Veamos:

- El elemento $(1, 1)$ es el neutro:

$$\begin{aligned}(k, h)(1, 1) &= (k^h 1, h) = (k, h) \\ (1, 1)(k, h) &= (1, {}^1k, h) = (k, h) \\ \forall (k, h) &\in K \times H\end{aligned}$$

- Para el inverso, dado $(k, h) \in K \times H$, el inverso será:

$$\begin{aligned}(k, h)^{-1} &= ({}^{h^{-1}}k^{-1}, h^{-1}) \\ (k, h)({}^{h^{-1}}k^{-1}, h^{-1}) &= \left(k^h ({}^{h^{-1}}k^{-1}), hh^{-1}\right) = \left(k^{hh^{-1}}k^{-1}, 1\right) = (kk^{-1}, 1) = (1, 1)\end{aligned}$$

□

Ejemplo. Veamos:

- Si $\theta = 1$, tenemos que el producto semidirecto coincide con el producto directo:

$$\theta(1)(h) = {}^1h = h \quad \forall h \in H$$

De donde:

$$(k_1, h_1)(k_2, h_2) = (k_1 {}^{h_1}k_2, h_1 h_2) = (k_1 k_2, h_1 h_2) \quad \forall (k_1, h_1), (k_2, h_2) \in K \times H$$

- Veamos cómo escribir S_3 como producto semidirecto:

$$S_3 \cong C_3 \rtimes_{\theta} C_2$$

Tenemos los elementos:

$$C_3 \times C_2 = \{(x, y) \mid x \in C_3, y \in C_2\}$$

Buscamos qué homomorfismo $\theta : C_2 \rightarrow \text{Aut}(C_3)$ hemos de coger. Será:

$$\theta(y)(x) = x^{-1} \quad \forall y \in C_2, \forall x \in C_3$$

Ya que $\text{Aut}(C_3) \cong C_2 = \{1, x\}$. Los elementos serán:

$$C_3 \rtimes_{\theta} C_2 = \langle x, y \mid x^3 = 1, y^2 = 1, \text{algo} \rangle$$

Con $|C_3 \rtimes_{\theta} C_2| = 6$. Los grupos que conocemos de orden 6 son S_3 y C_6 , que podemos distinguir en función de si el grupo es abeliano o no. Veamos que no lo es:

$$\begin{aligned}(x^2, y)(1, y) &= (x^2 {}^y1, y^2) = (x^2, 1) \\ (1, y)(x^2, y) &= (1 {}^yx^2, y^2) = (x, 1)\end{aligned}$$

Como $x \neq x^2$, no es conmutativo, por lo que $C_3 \rtimes_{\theta} C_2 \cong D_3$. Por tanto, completamos la presentación pensando en la de D_3 :

$$C_3 \rtimes_{\theta} C_2 = \langle x, y \mid x^3 = 1, y^2 = 1, xy = yx^{-1} \rangle$$

En definitiva, el único producto semidirecto de dos grupos de orden 6 es S_3 .

- Veamos que $Q_3 = C_3 \rtimes_{\theta} C_4$. De nuevo, el homomorfismo a considerar será:

$$\begin{aligned} \theta : C_4 &\longrightarrow \text{Aut}(C_3) \\ y &\longmapsto \theta(y)(x) = x^{-1} \end{aligned}$$

Tendremos:

$$C_3 \rtimes_{\theta} C_4 = \langle x, y \mid x^3 = 1, y^4 = 1, yx = x^{-1}y \rangle$$

Y queremos ver el isomorfismo con:

$$Q_3 = \langle c, d \mid c^6 = 1, d^2 = c^3, dc = c^{-1}d \rangle$$

- Si $n \geq 3$, si consideramos $\theta : C_2 \rightarrow \text{Aut}(C_n)$ dado por:

$$\theta(y)(x) = x^{-1} \quad \forall x \in C_n, y \in C_2$$

Tendremos que $C_n \rtimes_{\theta} C_2 \cong D_n$.

Definición 4.3. En el producto semidirecto, definimos:

$$\begin{array}{ccccc} K & \xrightarrow{\lambda_1} & K \rtimes H & \xleftarrow{\lambda_2} & H \\ & & \downarrow \pi & & \\ & & H & & \end{array}$$

Por:

$$\begin{aligned} \lambda_1(k) &= (k, 1) \\ \lambda_2(h) &= (1, h) \\ \pi(k, h) &= h \end{aligned}$$

Proposición 4.2. *Se verifica que:*

1. $\lambda_1, \lambda_2, \pi$ son homomorfismos de grupos.
2. $\pi\lambda_1$ es trivial.
3. $\pi\lambda_2 = id_H$.

De forma análoga a la propiedad universal del producto directo, podemos tener la propiedad universal para el producto semidirecto.

La siguiente Proposición nos será de utilidad para clasificar grupos haciéndolos isomorfo a un producto semidirecto, a partir del orden.

Proposición 4.3. *Sea G un grupo y $K, H < G$ con $K \triangleleft G$, $KH = G$ y $K \cap H = \{1\}$, sea $\theta : H \rightarrow \text{Aut}(K)$ un homomorfismo que nos da la acción $ac : H \times K \rightarrow K$ por conjugación¹:*

$$\theta(h)(k) = hkh^{-1} \quad \forall h \in H, \forall k \in K$$

Entonces, $K \rtimes_{\theta} H \cong G$.

¹La condición $K \triangleleft G$ nos dice que θ está bien definida

Demostración. Definiremos la aplicación $f : K \rtimes_{\theta} H \rightarrow G$ dada por:

$$f(k, h) = kh \quad \forall k \in K, \forall h \in H$$

Veamos que es un isomorfismo:

- f es sobreyectiva, ya que $G = KH$, de donde cualquier elemento $g \in G$ se escribe como $g = kh$ para ciertos $k \in K$, $h \in H$.
- Para la inyectividad, si $f(k_1, h_1) = f(k_2, h_2)$, entonces $k_1 h_1 = k_2 h_2$, de donde $k_2^{-1} k_1 = h_2 h_1^{-1}$:
 - $k_2^{-1} k_1 \in K$.
 - $h_2 h_1^{-1} \in H$.

Y como $H \cap K = \{1\}$, concluimos que $k_1 = k_2$ y $h_1 = h_2$, de donde f es inyectiva.

- Para ver que f es un homomorfismo, si $(k_1, h_1), (k_2, h_2) \in K \rtimes_{\theta} H$:

$$\begin{aligned} f((k_1, h_1)(k_2, h_2)) &= f(k_1 {}^{h_1}k_2, h_1 h_2) = f(k_1 h_1 k_2 h_1^{-1}, h_1 h_2) \\ &= k_1 h_1 k_2 h_1^{-1} h_1 h_2 = k_1 h_1 k_2 h_2 = f(k_1, h_1) f(k_2, h_2) \end{aligned}$$

□

Definición 4.4. Si G verifica las condiciones de la Proposición anterior, decimos que G es producto semidirecto interno de K y H .

Definición 4.5 (Complemento de un subgrupo). Si $K < G$, un subgrupo $H < G$ se llama complemento para K en G si $G = KH$ con $K \cap H = \{1\}$.

Observación. Con esta última definición, tendremos que G será un producto semidirecto interno de dos subgrupos propios si y solo si algún subgrupo normal propio tiene un complemento.

Ejemplo. Esto último no siempre será posible. Por ejemplo, si G es simple, no tendrá subgrupos normales propios, por lo que no será producto semidirecto interno de dos subgrupos.

Si G es un grupo que sí tiene subgrupos normales propios, tampoco somos capaces siempre de poner como un producto semidirecto. Por ejemplo, Q_2 no es un producto semidirecto interno de subgrupos propios. Si recordamos su diagrama de Hasse:

$$\begin{aligned} \langle i \rangle \cap \langle j \rangle &= \{1, -1\} \\ \langle i \rangle \cap \langle k \rangle &= \{1, -1\} \\ \langle j \rangle \cap \langle k \rangle &= \{1, -1\} \end{aligned}$$

Dado un subgrupo normal, no seremos capaces de complementarlo con otro.

Ejemplo. Para cualquier grupo K , si tomamos $H = \text{Aut}(K)$ y $\theta = 1_{\text{Aut}(K)}$, si tomamos:

$$K \rtimes_{\theta} \text{Aut}(K) = \text{Hol}(K)$$

Al que llamaremos grupo holomorfo de K .

Por ejemplo:

$$\text{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2) = S_4$$