Teorema de Mal'cev

Julia Lera Martínez

Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Directora del trabajo:
María Concepción Martínez Pérez

Diciembre de 2023

Introducción

La Teoría de Grupos es una rama del álgebra abstracta que se encarga de estudiar la estructura de los llamados *grupos*, conjuntos con una operación interna que satisface ciertas características. En este trabajo vamos a centrarnos en los grupos nilpotentes, que son una generalización de los grupos abelianos, y probaremos el **Teorema de Mal'cev**, un resultado muy importante relacionado con la extracción de raíces en estos grupos.

Los grupos abelianos son aquellos en los que "el orden de los factores no altera el producto", es decir, los elementos conmutan entre sí. Su nombre fue dado en honor al matemático noruego Niels Henrik Abel. Los números enteros, con la operación de suma, o los reales no nulos, con la operación de producto, son algunos de los ejemplos más tradicionales de este tipo de grupos. Sin embargo, no todos los grupos satisfacen esta condición de conmutatividad. El concepto de *grupos nilpotentes* es una generalización que conserva algunas de las buenas propiedades de los grupos abelianos. Estos grupos se caracterizan por poseer una serie de subgrupos normales tales que los cocientes consecutivos son centrales, en particular, abelianos. Por esta razón, intuitivamente, se dice que son grupos "casi abelianos".

El trabajo está dividido en dos partes:

- El primer capítulo se utiliza para introducir las nociones y conceptos básicos sobre las que desarrollaremos nuestro estudio, así como algunos resultados interesantes. Primero presentamos los conceptos básicos de Teoría de Grupos como la definición formal de grupo, para después definir los grupos resolubles y acabar con los grupos nilpotentes. Haremos un breve comentario sobre la codición de maximalidad, ya que nos será de gran utilidad en el segundo capítulo.

  Un grupo G es resoluble si contiene una serie abeliana, es decir, una serie de subgrupos

  $$1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G,$$

  tales que G_i/G_{i-1} es abeliano. También definiremos el conmutador de dos elementos y los subgrupos conmutadores, los cuales nos permiten construir la serie derivada de G.

  En la siguiente sección definimos los grupos nilpotentes, que son grupos con una serie central, es decir, una serie abeliana donde cada cociente G_i/G_{i-1} además está contenido en el centro de G/G_{i-1}. Usando otra vez subgrupos conmutadores, podemos construir la serie central descendente de G. Por otra parte, si hacemos que los cocientes G_i/G_{i-1} sean exactamente iguales al centro de G/G_{i-1}, obtenemos la serie central ascendente de G. Si nuestro grupo es nilpotente, estas dos series deben terminar en el mismo número de pasos y su longitud es la llamada clase de nilpotencia de G.

  Para acabar la segunda sección, presentamos un ejemplo de grupo nilpotente: las matrices unitriangulares superiores de dimensión n. Nos centramos en el caso $n = 3$, el llamado *grupo de Heisenberg*, y calculamos su serie central descendente.

  En la última sección explicamos lo que significa que un grupo tenga la condición maximal (max). Veremos que, si tenemos un subgrupo normal, nuestro grupo tiene max si y solo si el subgrupo y el correspondiente cociente tienen max. Además, un grupo abeliano tiene max si y solo si es finitamente generado.

- El segundo capítulo profundiza en el problema de encontrar raíces de un elemento dentro de un grupo. Enunciamos el *Teorema de Mal'cev*, que fue desarrollado por el matemático ruso Anatoly Mal'cev en la década de 1940. Este teorema, y su prueba, contribuyó significativamente al entendimiento de la estructura de los grupos nilpotentes y su relación con la radicabilidad.

  En la primera sección, introducimos nuevos conceptos más específicos para la comprensión del teorema. Un grupo G es libre de torsión si no tiene elementos de orden finito, es decir, si dado $g \in G$ tal que $g^n = 1$ para cierto $n > 0$, necesariamente $g = 1$. Con esta definicón, enunciamos un resultado muy importante y conocido en Teoría de Grupos:

  Teorema. *Todo grupo abeliano finitamente generado y libre de torsión es isomorfo a un producto directo de grupos cíclicos.*

  Por otra parte, nuestro grupo G es *radicable* si para todo $g \in G$ y todo número entero positivo n la ecuación $x^n = g$ tiene una solución x en G. Esta propiedad no es común para todos los grupos, ni siquiera para todos los grupos nilpotentes, y esto es lo que motivó el enunciado del *Teorema de Mal'cev*. Por último, demostramos que, si tenemos un grupo nilpotente y libre de torsión, la extracción de raíces, si existe, es única.

  En la segunda sección de este capítulo, enunciamos el *Teorema de Mal'cev*:

  Teorema. *Todo grupo nilpotente G libre de torsión es isomorfo a un subgrupo de otro grupo nilpotente G^* radicable de forma que cada elemento de G^* tiene una potencia positiva en G. Además, el grupo G^* es único salvo isomorfismo.*

  Este grupo G^* se dice *complección de Mal'cev* del grupo G.

- El tercer capítulo está dedicado a la demostración del *Teorema de Mal'cev*. Seguiremos la prueba realizada por el matemático británico Philip Hall en 1969, que se puede resumir como sigue, solo en el caso finitamente generado.

  En la primera parte, refinamos las serie central ascendente de G añadiendo más subgrupos hasta obtener una serie central

  $$1 = G_n \triangleleft G_{n-1} \triangleleft \ldots \triangleleft G_0 = G,$$

  donde cada cociente G_{i-1}/G_i es cíclico infinito, con generador $u_i G_i$. Con esto podemos deducir que cada elemento $a \in G$ puede ser expresado así $a = u_1^{\alpha_1} \ldots u_n^{\alpha_n} = u^\alpha$. Además, probamos que, si $b = u^\beta \in G$ y m es un número entero, existen polinomios γ_i en las variables α_j, β_j y $\omega_i^{(m)}$ en las variables α_j y m tales que

  $$ab = u^\alpha u^\beta = u^\gamma$$
  $$a^m = u^\omega.$$

  Con estos polinomios, definimos $G^{\mathbb{Q}}$ como el conjunto de todos los productos formales u^α con exponentes $\alpha_1, \ldots, \alpha_n$ en $\mathbb{Q}$. Claramente, este conjunto contiene a G. Solo tenemos que probar que $G^{\mathbb{Q}}$ es un grupo nilpotente y radicable como el del enunciado para probar la existencia de la complección de Mal'cev.

  La unicidad se prueba en la segunda parte definiendo un isomorfismo entre $G^{\mathbb{Q}}$ y una complección distinta de la encontrada.

  En la última sección, ampliamos el ejemplo del primer capítulo para ver cómo es su complección. También hablamos de los polinomios de Hall y su aplicación en criptografía.

Finalmente, me gustaría señalar que el problema detrás del Teorema de Mal'cev es básicamente un problema de resolver ciertas ecuaciones. Una ecuación como $nx = a$, donde $n > 0$ y a son enteros, solo tendrá solución x en $\mathbb{Z}$ si n divide a a. Sin embargo, ese no siempre es el caso, y así es como se

introdujeron los números racionales. Análogamente, cuando tenemos una ecuación racional como $x^2 = 2$, tenemos que introducir los números reales, y cuando tenemos una ecuación real como $x^2 = -1$, definimos los números complejos. El problema de extraer raíces de un elemento ha interesado a los matemáticos durante muchas décadas e incluso siglos (como, por ejemplo, el caso de los números imaginarios, que se introdujeron por primera vez en el siglo XVI [4]). Con estas construcciones estamos extendiendo grupos para poder trabajar mejor con ellos. Con esto, es fácil entender la importancia del resultado de Mal'cev, incluso a día de hoy (el artículo [3] de 2017 se basa en la prueba de este teorema dada por P. Hall en 1969 para producir un algoritmo que permite operar de forma eficiente en grupos nilpotentes).

Abstract

This project is included in the branch of Algebra called Group Theory, which focuses on groups and their algebraic structure. In particular, we will consider nilpotent groups. More precisely, our central focus will be Mal'cev's Theorem on the extraction of roots in torsion-free nilpotent groups, and its proof, which helps understand better the structure of these groups.

We first state the grounds from which we will build our a way to the proof. We introduce soluble groups. From there we define nilpotent groups, which can be seen as extensions of abelian groups because of their structure. Both these groups are defined using certain series and these two notions are strongly related since nilpotent groups are also solvable. However the reverse is not true, and one of the reasons that make nilpotent groups interesting is their closer proximity to abelian groups, whilst still maintaining a more rich and complicated structure.

As stated before, nilpotent groups are defined in terms of series, that is why we make a big emphasis on how the subgroups and quotients that form them are and on the properties that they have. We will prove many results about these series, that will help us understand how nilpotent groups are, and also how we can prove the theorem that concerns us.

Once we have our basis, we will change our focus to the extraction of roots in these groups. We will define radicability and prove that in a torsion-free nilpotent group the extraction of roots, if it exists, is unique. We will then present the main theorem of this thesis, Mal'cev's Theorem, which states that a torsion-free nilpotent group G can be embedded in a nilpotent group G^*, in which the extraction of roots is unique, in such a way that every element of G^* has a positive porwer in G. By proving this statement for finitely generated groups, and with the help of some examples, we will learn about the structure of G and how we can extend it so that we can find the roots of its elements.

Finally, I would like to point out that the problem behind Mal'cev's Theorem is basically a problem of solving certain equations. When we have an equation like $nx = a$ where $n > 0$ and a are integers, then we can only find a solution x in $\mathbb{Z}$ if n divides a. However that is not always the case, and that is how the rational numbers where introduced. Similarly, when we have a rational equation like $x^2 = 2$, we have to introduce the real numbers, and when we have a real equation like $x^2 = -1$, we define the complex numbers. The problem of extracting the roots of an element has been interesting for mathematicians for many decades and even centuries (take for example the case of imaginary numbers which were first introduced in the 16th century [4]). These are all just extensions of groups, that give us a bit more space to work with them. Seeing this, it is easy to understand the importance of Mal'cev's result, and why it is still studied to this date (the article [3] from 2017 is based on the proof of this theorem given by P. Hall in 1969, which is used to produce an algorithm to compute in an effective way in these groups).

Índice general

Capítulo 1

Conceptos previos y Grupos Nilpotentes

Antes de empezar vamos a definir algunos conceptos previos que nos ayudarán a entender mejor los resultados que se estudian en este trabajo. Empezamos con lo más básico:

Un *grupo* $G = (G, \cdot)$ es un conjunto no vacío G con una operación interna:

$$\begin{aligned} \cdot : G \times G &\to G \\ (x, y) &\mapsto x \cdot y \end{aligned}$$

tal que:

- es *asociativa*
- tiene *elemento neutro* 1_G
- todo elemento g tiene *inverso* g^{-1}, i.e. $g \cdot g^{-1} = 1_G$

A partir de este punto obviaremos el símbolo $\cdot$ al referirnos a la operación interna de un grupo.

Dos elementos a y b conmutan si $ab = ba$ y, si esto se cumple para todos los elementos de G, se dice que el grupo es *abeliano*.

Este concepto será necesario durante el estudio del Teorema de Mal'cev, al igual que otras nociones que damos por conocidas, como orden o grupo cíclico. También consideramos como básicos algunos resultados primarios sobre la teoría de grupos, pero mencionamos algunos conceptos para situar el marco teórico en el que desarrollamos el trabajo:

Sea G un grupo. Decimos que un subconjuto H de G es un *subgrupo* si es a su vez un grupo con la restricción de la operación de G. Lo denotaremos $H \leqslant G$. En este caso, si x es un elemento cualquiera de G, entonces $xH = \{xh : h \in H\}$ es una *clase lateral izquierda* de H en G. Y, análogamente, Hx es una *clase lateral derecha* de H en G. Un subgrupo N se dice *normal* si para todo $x \in G$ tenemos $xN = Nx$, es decir, $n^x \in N$ para todo $n \in N$. Lo denotaremos $N \trianglelefteq G$. Sea $N \trianglelefteq G$, entonces se puede definir una estructura de grupo en el conjunto de todas las clases de N en G, el cual se llama *grupo cociente* G/N.

Sean G, H dos grupos. Una función $f : G \to H$ se dice *homomorfismo de grupos* si para todo $x, y \in G$ tenemos $f(xy) = f(x)f(y)$. Es fácil probar que el núcleo de un homomorfismo, $ker(f)$, que consiste en los elementos cuya imagen por f es 1, es un subgrupo normal de G.

El *centro* de un grupo G es $Z(G) = \{g \in G \mid xg = gx,\ \forall x \in G\}$.

Sea S un subconjunto (finito o infinito) de elementos de un grupo G. Si todo $y \in G$ puede ser expresado como un producto de un número finito de elementos de S y de sus inversos, entonces decimos que S es un *conjunto generador* de G y lo denotamos así: $G = \langle S \rangle$. Si existe un conjunto generador S de G finito, se dice que G es *finitamente generado*. Además, si el conjunto $\{x_1, \ldots, x_n\}$ genera G de tal forma que $x_1^{r_1} \cdots x_n^{r_n} = 1$ implica que $r_1 = \cdots = r_n = 0$, entonces se dice que $x_1, \ldots, x_n$ forman una *base* de G. No todos los grupos finitamente generados poseen una base.

Lema 1.1. *Sea G un grupo finitamente generado y N un subgrupo normal de G. Entonces G/N es finitamente generado*

Demostración. Es evidente, ya que, si $x_1,\dots,x_k$ generan G, $x_1N,\dots,x_kN$ generan G/N. □

Por último, vamos a dar un resultado muy básico de Teoría de Grupos, cuya demostración, aunque elemental, obviamos por ser demasiado larga:

Lema 1.2. *Todo subgrupo de un grupo abeliano y finitamente generado es finitamente generado.*

1.1. Grupos resolubles

Definición 1.1. Una serie de subgrupos de un grupo G,

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G,$$

se dice *abeliana* si cada cociente G_{i+1}/G_i es abeliano.

Definición 1.2. Un grupo G se dice *resoluble* o *soluble* si tiene una serie abeliana, $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$.

Claramente, si G es abeliano, G es resoluble con serie abeliana $1 \triangleleft G$. Así resolubilidad es una generalización de la conmutatividad. El ejemplo más pequeño de grupo resoluble no abeliano es el grupo simétrico S_3, cuya serie abeliana es $1 \triangleleft \langle(123)\rangle \triangleleft S_3$.

Definición 1.3. La longitud de la serie abeliana más corta de un grupo resoluble G se dice *longitud derivada* de G.

Por tanto, los grupos de longitud derivada 1 son los grupos abelianos.

Definición 1.4. Sea G un grupo cualquiera y sean x_1, x_2 elementos arbitrarios de G. El *conmutador* de x_1 y x_2 es $[x_1,x_2] = x_1^{-1}x_2^{-1}x_1x_2 = x_1^{-1}x_1^{x_2}$ donde $x_1^{x_2} = x_2^{-1}x_1x_2$.

Entonces G es abeliano si y solo si todos los conmutadores de elementos de G son iguales a la identidad. Ampliamos este concepto para más de dos elementos. Definimos un *conmutador simple de peso* $n \geq 2$ de forma recursiva

$$[x_1,x_2,\dots,x_n] = [[x_1,\dots,x_{n-1}],x_n],$$

donde $[x_1] = x_1$ por convención.

Vamos a introducir algunas propiedades básicas de los conmutadores para poder trabajar con ellos.

Lema 1.3. *Supongamos que x,y,z son elementos de un grupo. Entonces:*

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

ii) $[xy,z] = [x,z]^y[y,z], \quad [x,yz] = [x,z][x,y]^z$

iii) $[x,y^{-1}] = \left([x,y]^{y^{-1}}\right)^{-1}, \quad [x^{-1},y] = \left([x,y]^{x^{-1}}\right)^{-1}$

iv) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ *(la identidad de Hall-Witt).*

Demostración. Aplicando la definición de conmutador se puede demostrar i), ii), iii) fácilmente. Para probar iv), definimos $u = xzx^{-1}yx$, $v = yxy^{-1}zy$ y $w = zyz^{-1}xz$. Podemos computar $[x,y^{-1},z]^y = u^{-1}v$, $[y,z^{-1},x]^z = v^{-1}w$ y $[z,x^{-1},y]^x = w^{-1}u$. Y entonces obtenemos:

$$[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = u^{-1}vv^{-1}ww^{-1}u = 1.$$

□

Definición 1.5. Sean X_1, X_2 subconjuntos no vacíos de un grupo G. Definimos el *subgrupo conmutador* de X_1 y X_2 así:

$$[X_1, X_2] = \langle [x_1, x_2] \mid x_1 \in X_1,\ x_2 \in X_2 \rangle .$$

Es decir, es el subgrupo generado por todos los conmutadores de elementos de X_1 y X_2.

Observemos que, por el lema 1.3 (i), el conmutador de dos subconjuntos es simétrico: $[X_1, X_2] = [X_2, X_1]$. Además, si X_1, X_2 son subgrupos normales, el lema 1.3 (iii) implica que $[X_1, X_2]$ también lo es.

Para $n \geq 2$ definimos recursivamente:

$$[X_1, X_2, ..., X_n] = [[X_1, X_2, ..., X_{n-1}], X_n],$$

donde $[X_1] = \langle X_1 \rangle$.

Lema 1.4. *Si X_1, X_2, X_3 son subgrupos normales en G, entonces $[X_1, X_2X_3] = [X_1, X_2][X_1, X_3]$ y $[X_1X_2, X_3] = [X_1, X_3][X_2, X_3]$*

Demostración. $[X_1, X_2X_3]$ esta generado por los conmutadores $[x_1, x_2x_3]$ con $x_1 \in X_1$, $x_2 \in X_2$ y $x_3 \in X_3$. El resultado sigue de usar el apartado *ii*) del lema 1.3. Análogamente, se demuestra la otra igualdad. □

Una vez aclarado el concepto de conmutador, podemos construir series abelianas canónicas para los grupos resolubles.

Definición 1.6. Sea G un grupo. Definimos el *subgrupo derivado o conmutador* de G como $G' = [G, G]$. Formando subgrupos derivados repetidamente, obtenemos una secuencia descendente de subgrupos de G:

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq ... \geq G^{(n)} \geq ...$$

donde $G^{(n+1)} = \left(G^{(n)}\right)'$. La llamaremos *serie derivada* de G.

Teniendo en cuenta la observación realizada tras la definición 1.5, el subgrupo derivado G' es normal en G y, además, G/G' es abeliano, de hecho es el mayor cociente abeliano de G. Vamos a ver esto último. Sea $H \leq G$. Tomamos $[x_1, x_2]$ con $x_1, x_2 \in G$, ya que estos elementos generan el grupo G'. Si el cociente G/H es abeliano, $[x_1, x_2]H = 1$. Por tanto, $[x_1, x_2] \in H$, es decir, $G' \leq H$. Habitualmente se denota $G_{ab} = G/G'$ y se llama *abelianización* de G. Por inducción, es claro que $G^{(n)}$ es un subgrupo normal de G para cada n y cada uno de los cocientes $G^{(n)}/G^{(n+1)}$ en la serie es abeliano.

1.2. Grupos nilpotentes

Definición 1.7. Un grupo G se dice *nilpotente* si tiene una *serie central*, es decir, una serie normal $1 = G_0 \leq G_1 \leq ... \leq G_n = G$ tal que G_{i+1}/G_i está contenido en el centro de G/G_i para $i = 0, 1, ..., n-1$. La longitud de la serie central más corta de G se dice *clase de nilpotencia* de G.

Claramente, si el cociente G_{i+1}/G_i está contenido en el centro de G/G_i, en particular es abeliano y, por tanto, una serie central es también una serie abeliana y, en consecuencia, los grupos nilpotentes son resolubles. Sin embargo, no toda serie abeliana es central: la serie $1 \triangleleft \langle (123) \rangle \triangleleft S_3$ no es central, puesto que $\langle (123) \rangle / 1 = \langle (123) \rangle$ no está contenido en $Z(S_3/1) = 1$. De hecho, es fácil ver que esta es la única serie abeliana de S_3, luego S_3 no es nilpotente. Por tanto, no todo grupo resoluble es nilpotente.

Un grupo nilpotente de clase 0 tiene orden 1 y los grupos nilpotentes de clase 1 son precisamente los grupos abelianos.

Observación. Una serie $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$ es central si y solo si $[G_{i+1}, G] \leq G_i$. Es fácil demostrarlo. La serie es central si y solo si $G_{i+1}/G_i \subseteq Z(G/G_i)$. Esto es equivalente a que $hgG_i = ghG_i$ para todo $h \in G_{i+1}$ y todo $g \in G$, es decir, $[h, g] \in G_i$ para todo $h \in G_{i+1}$ y todo $g \in G$. Por tanto, equivalente a $[G_{i+1}, G] \leq G_i$.

En el caso de la resolubilidad hemos definido una serie canónica. Para la nilpotencia vamos a definir dos. La primera serie, al igual que la serie derivada, es una secuencia descendente de subgrupos conmutadores.

Definición 1.8. Sea G un grupo y definimos $\gamma_1(G) = G$ y $\gamma_{n+1}(G) = [\gamma_n(G), G]$, para $n \geq 1$. La serie $G = \gamma_1(G) \geq \gamma_2(G) \geq ... \geq \gamma_n(G) \geq ...$ se llama la *serie central descendente* de G.

Es claro que la serie es central, basta usar la observación anterior. Al igual que la serie derivada, la serie central descendente no siempre alcanza 1 o termina.

El siguiente resultado nos será de gran utilidad en la prueba de nuestro teorema (3).

Proposición 1.5. *Sea G un grupo nilpotente. Si $G_{ab} = G/G'$ es finitamente generado, entonces, para todo $i = 1, ..., n$, $\gamma_i(G)/\gamma_{i+1}(G)$ también lo es.*

Demostración. Supongamos que X es una familia finita que genera G_{ab}. Observemos que $G' = \gamma_2(G)$, por tanto, el primer cociente de la serie central descendente es finitamente generado. Vamos a ver que entonces $\gamma_2(G)/\gamma_3(G)$ es generado por los elementos de la forma $[x,y]\gamma_3(G)$ con $x\gamma_2(G), y\gamma_2(G) \in X$, por tanto, tiene un número finito de generadores.

Sabemos que $\gamma_2(G)/\gamma_3(G)$ está generado por $[g,h]\gamma_3(G)$ con $g,h \in G$, luego basta con probar que, para todo $g,h \in G$, $[g,h]\gamma_3(G)$ se puede expresar como producto de elementos de la forma $[x,y]\gamma_3(G)$ con $x\gamma_2(G), y\gamma_2(G) \in X$. Como X genera G_{ab}, tenemos:

$$g\gamma_2(G) = x_1 \cdots x_t \gamma_2(G)$$
$$h\gamma_2(G) = y_1 \cdots y_s \gamma_2(G)$$

con $x_i\gamma_2(G), y_j\gamma_2(G) \in X$ para todo $i = 1, \ldots, t$ y todo $j = 1, \ldots, s$.

Vamos a probar el resultado por inducción sobre $t+s$. Sea $t+s = 0$, entonces $g,h \in \gamma_2(G)$, luego $[g,h]\gamma_2(G) = \gamma_2(G)$. Sea ahora $t+s > 0$ y asumimos que el resultado se cumple para $i < t+s$. Como t,s son enteros positivos, uno de ellos es mayor que cero, sin pérdida de generalidad podemos suponer $t > 0$. Ahora podemos poner $g\gamma_2(G) = g_1 x_t \gamma_2(G)$ con $g_1\gamma_2(G) = x_1 \ldots x_{t-1}\gamma_2(G)$. Por la hipótesis de inducción, $[g_1,h]\gamma_3(G)$ es producto de elementos de la forma $[x,y]\gamma_3(G)$ con $x\gamma_2(G), y\gamma_2(G) \in X$. Y lo mismo es cierto para $[x_t,h]\gamma_3(G)$. Además:

$$[g,h]\gamma_3(G) = [g_1x_t,h]\gamma_3(G) = [g_1,h]^{x_t}\gamma_3(G)[x_t,h]\gamma_3(G) = [g_1,h]\gamma_3(G)[x_t,h]\gamma_3(G),$$

donde primero utilizamos el lema 1.3 y después el siguiente hecho:

$$[g_1,h]^{x_t}\gamma_3(G) = [g_1,h][g_1,h]^{-1}[g_1,h]^{x_t}\gamma_3(G) = [g_1,h][[g_1,h],x_t]\gamma_3(G) = [g_1,h]\gamma_3(G).$$

Por tanto, $[g,h]\gamma_3(G)$ también es producto de elementos de la forma $[x,y]\gamma_3(G)$ con $x\gamma_2(G), y\gamma_2(G)$ en X. Como X es finito, las combinaciones de x,y para formar los conmutadores también lo son y $\gamma_2(G)/\gamma_3(G)$ es finitamente generado.

Podemos repetir este proceso con los siguientes cocientes $\gamma_i(G)/\gamma_{i+1}(G)$: si $\gamma_{i-1}(G)/\gamma_i(G)$ está finitamente generado por una familia Y, entonces los elementos de la forma $[x,y]\gamma_{i+1}(G)$ con $x\gamma_2(G) \in X$ e $y\gamma_i(G) \in Y$ generan $\gamma_i(G)/\gamma_{i+1}(G)$. Como X e Y son finitos, sus combinaciones para formar los conmutadores también. Luego, para todo $i = 1, \ldots, n$, el cociente $\gamma_i(G)/\gamma_{i+1}(G)$ es finitamente generado. □

Definición 1.9. La segunda serie canónica asociada a la nilpotencia es la *serie central ascendente*

$$1 = Z_0(G) \leq Z_1(G) \leq ... \leq Z_n(G) \leq ...$$

definida por $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$. En particular, $Z_1(G) = Z(G)$.

En general, la serie central ascendente puede no alcanzar G o siquiera terminar finitamente. Por ejemplo, si $Z_1(G) = 1$ como en el caso de S_3, la serie no crece en absoluto. Si la serie termina, entonces el subgrupo en el que termina se dice *hipercentro* de G.

Proposición 1.6. *Sea $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$ una serie central de un grupo nilpotente G. Entonces:*

i) $\gamma_i(G) \leq G_{n-i+1}$, *para* $0 < i \leq n+1$, *luego* $\gamma_{n+1}(G) = 1$

ii) $G_i \leq Z_i(G)$, *para* $0 \leq i \leq n$, *luego* $Z_n(G) = G$

iii) las series centrales descente y ascendente tienen la misma longitud y este valor común es la clase de nilpotencia de G.

Demostración. Probamos i) por inducción. Para $i = 1$, es claro $\gamma_1(G) = G = G_n$. Supongamos que se cumple hasta $i-1$: $\gamma_{i-1}(G) \leq G_{n-i+2}$. Entonces

$$\gamma_i(G) = [G, \gamma_{i-1}(G)] \leq [G, G_{n-i+2}]$$

ya que la formación de subgrupos conmutadores respeta inclusiones. Como la serie de los G_j es central, $[G, G_{n-i+2}] \leq G_{n-i+1}$ y tenemos que $\gamma_i(G) \leq G_{n-i+1}$.

También probaremos ii) por inducción. El paso $i = 0$ es claro. Supongamos que se cumple hasta $i-1$: $G_{i-1} \leq Z_{i-1}(G)$. Ahora, tomamos $g \in G_i$ y $h \in G$. Entonces

$$[g,h] \in [G_i, G] \leq G_{i-1} \leq Z_{i-1}(G).$$

Por tanto, $ghZ_{i-1}(G) = hgZ_{i-1}(G)$, es decir,

$$gZ_{i-1}(G) \in Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G).$$

Concluimos que $g \in Z_i(G)$, luego $G_i \leq Z_i(G)$.

La última parte es una consecuencia directa de i) y ii). □

De aquí podemos concluir que un grupo es nilpotente si y solo si su serie central descendente termina en el grupo trivial, es decir, si y solo si $\gamma_n(G) = 1$ para algún n. Equivalentemente, su serie central ascendente termina en el grupo original. Esto tiene como consecuencia que, si G es nilpotente y $H \leq G$, entonces H es nilpotente. Para probarlo solo hay que tomar la serie $H \cap \gamma_i(G)$ que claramente es central y termina en 1.

Proposición 1.7. *Sea G un grupo nilpotente y N un subgrupo normal de G. Entonces G/N es nilpotente.*

Demostración. Suponemos que $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ es una serie central de G. Entonces podemos tomar los subgrupos $G_iN/N \leq G/N$, que claramente son normales en G/N. Ahora tomamos gN en G/N y hN en $G_{i+1}N/N$, con $g \in G$, $h \in G_{i+1}$. Como los G_i forman una serie central, $[h,g] \in [G_{i+1}, G] \leq G_i$. Por tanto, $[hN, gN] = [h,g]N \in G_iN/N$, es decir, $[G_{i+1}N/N, G/N] \leq G_iN/N$ y queda probado el resultado. □

Lema 1.8. *Sean H, K, L subgrupos de un grupo G. Si dos subgrupos cualquiera entre $[H,K,L]$, $[K,L,H]$, $[L,H,K]$ están contenidos en un subgrupo normal de G, entonces el tercero también lo está.*

Demostración. Asumimos $[K,L,H], [L,H,K] \leq N$, donde N es un subgrupo normal de G. Utilizando la identidad de Hall-Witt (1.3) tenemos que $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ para cualesquiera $x \in H$, $y \in K$, $z \in L$. Llamaremos $a = [x,y^{-1},z]^y \in [H,K,L]$, $b = [y,z^{-1},x]^z \in [K,L,H]$ y $c = [z,x^{-1},y]^x \in [L,H,K]$. Podemos despejar a de la ecuación de arriba:

$$a = c^{-1}b^{-1} \in [K,L,H][L,H,K] \leq N.$$

Como los elementos de la forma de a generan $[H,K,L]$, tenemos que $[H,K,L] \leq N$. □

Proposición 1.9. *Sea G un grupo e i, j números enteros positivos. Entonces $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$.*

Demostración. Vamos a probarlo por inducción sobre i. Primero, observamos que para $i = 1$:

$$[\gamma_1(G), \gamma_j(G)] = [G, \gamma_j(G)] = \gamma_{j+1}(G),\ \forall j > 0$$

Supongamos que se cumple hasta i, queremos ver que $[\gamma_{i+1}(G), \gamma_j(G)] \leq \gamma_{i+1+j}(G)$ para todo j. Por definición de $\gamma_{i+1}(G)$, tenemos que $[\gamma_{i+1}(G), \gamma_j(G)] = [[G, \gamma_i(G)], \gamma_j(G)]$. Por el lema anterior 1.8, si probamos que los dos subgrupos $[\gamma_i(G), \gamma_j(G), G]$ y $[\gamma_j(G), G, \gamma_i(G)]$ están en $\gamma_{i+j+1}(G)$ (subgrupo normal de G), tendríamos que el tercero también lo está, es decir:

$$[\gamma_{i+1}(G), \gamma_j(G)] \leq \gamma_{i+1+j}(G).$$

El enunciado se cumple para i, luego:

$$[\gamma_i(G), \gamma_j(G), G] = [[\gamma_i(G), \gamma_j(G)], G] \leq [\gamma_{i+j}(G), G] = \gamma_{i+j+1}(G).$$

Además, la hipótesis de inducción es cierta para todo j y por tanto:

$$[\gamma_j(G), G, \gamma_i(G)] = [\gamma_{j+1}(G), \gamma_i(G)] \leq \gamma_{i+j+1}(G).$$

□

Para tener una idea más clara de cómo se comportan los grupos nilpotentes y poder entender mejor el Teorema de Mal'cev, que introduciremos en el capítulo 2, vamos a trabajar con este ejemplo.

Ejemplo 1.10. Sea R un anillo conmutativo con identidad (podemos pensarlo como $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$). Definimos el grupo G de todas las matrices $n \times n$ unitriangulares superiores sobre R, es decir, las matrices con unos en la diagonal y ceros debajo de ella. La operación interna es la multiplicación habitual entre matrices. Podemos asegurar que G es un grupo debido a que el producto de matrices triangulares superiores es otra matriz triangular superior cuyos elementos diagonales son el producto de los correspondientes elementos diagonales de las dos matrices. Se puede ver que este grupo es nilpotente de clase $n-1$.

Vamos a centrarnos en el caso $n = 3$. Este es el llamado *grupo de Heisenberg*:

$$G = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in R \}.$$

Sean dos matrices en G:

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ y } B = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}.$$

Se puede comprobar que su producto será:

$$AB = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \tag{1.1}$$

y, por tanto, el inverso de A será:

$$A^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

Definimos el subgrupo de G:

$$G_2 = \{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in R \}.$$

Además, para todo $M \in G$ y todo $T \in G_2$, (1.1) implica que $MT = TM$. Es decir, G_2 es un subgrupo abeliano y $G_2 \leq Z(G)$.

Por otra parte, en el caso en el que $R = \mathbb{Z}$, las matrices:

$$u_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; u_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \; u_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

claramente generan el grupo G (y en particular u_3 genera el subgrupo G_2) y sus matrices inversas son:

$$u_1^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; u_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \; u_3^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Vamos a calcular los conmutadores de estas matrices generadoras:

$$[u_1,u_2] = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = u_3$$

$$[u_2,u_3] = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1$$

$$[u_1,u_3] = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1$$

Sabiendo esto, se puede deducir que $\gamma_2(G) = [G,G] = G_2$ aplicando la definición de subgrupo conmutador. Entonces $\gamma_3(G) = [G,\gamma_2(G)] = [G,G_2] = 1$ ya que $[u_1,u_3] = [u_2,u_3] = [u_3,u_3] = 1$ y, como u_1, u_2 no conmutan, $G_2 = Z(G)$.

Luego tenemos la serie central descendente de G:

$$\gamma_1(G) = G \triangleright \gamma_2(G) = G_2 \triangleright \gamma_3(G) = 1$$

que termina en un número finito de pasos, es decir, hemos probado que G es nilpotente de clase 2.

Se puede construir un homomorfismo de grupos:

$$\begin{aligned} J : G/G_2 &\to R \oplus R \\ MG_2 &\longmapsto (a,c) \end{aligned}$$

donde $M = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ es un represante de la clase en G/G_2. J está bien definido, puesto que:

$$MG_2 = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} G_2, \text{ debido a } \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & b-ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G_2$$

para cualesquiera $a,b,c \in R$.

Para ver que es un homomorfismo, tomamos $M = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, N = \begin{pmatrix} 1 & a' & 0 \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}$ en G. Entonces

$$MN = \begin{pmatrix} 1 & a+a' & ab' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$

y, aplicando la definición de la operación interna del producto directo, tenemos:

$$J((MN)G_2) = (a+a', b+b') = (a,b)+(a',b') = J(MG_2)+J(NG_2).$$

Por otra parte, $J(MG_2) = J(NG_2)$ si y solo si $a = a'$ y $b = b'$ y, en tal caso, es fácil ver que $MN^{-1} \in G_2$, luego $MG_2 = NG_2$ y J es inyectiva. Y claramente es suprayectiva, por tanto, J es un isomorfismo de grupos y

$$G_{ab} = G/G_2 \cong R \oplus R.$$

1.3. La condición maximal

Vamos a introducir la condición maximal así como algunos resultados relacionados que utilizaremos en la prueba del *Teorema de Mal'cev* (3).

Definición 1.10. Se dice que un grupo G tiene *max* si una de las siguientes condiciones se cumple:

i) toda familia de subgrupos de G tiene algún elemento maximal;

ii) toda serie estrictamente ascendente de subgrupos de G es finita;

iii) todo subgrupo de G es finitamente generado.

Se puede probar que las tres condiciones son equivalentes usando el lema de Zorn. Claramente, si un grupo es finito, tiene max.

Proposición 1.11. *Sea G un grupo y N un subgrupo normal de G. Entonces G tiene max si y solo si tanto N como G/N tienen max.*

Demostración. Los subgrupos de N son en particular subgrupos de G, luego, si G tiene max, N también. Ahora, si tenemos una serie estrictamente ascendente de subgrupos de G/N

$$1 = G_0/N < G_1/N < \ldots < G_n/N < \ldots,$$

en particular, tenemos una serie estrictamente ascendente de subgrupos de G

$$1 = G_0 < G_1 < \ldots < G_n < \ldots$$

Esta serie es finita: existe n tal que $G_n = G_m$ para todo $m \geq n$. Por tanto, $G_n/N = G_m/N$ para todo $m \geq n$ y G/N tiene max.

Para el reverso, tomamos una serie de subgrupos de G: $H_1 < H_2 < \ldots < H_n < \ldots$. De aquí podemos obtener una serie de las mismas características de N y de G/N:

$$H_1 \cap N \leq H_2 \cap N \ldots \leq H_n \cap N \leq \ldots$$
$$H_1N \leq H_2N \leq \ldots \leq H_nN \leq \ldots$$

Como N tiene max, existe i tal que $H_i \cap N = H_n \cap N$ para todo $n \geq i$. De forma similar, existe j tal que $H_jN = H_nN$ para todo $n \geq j$. Entonces, si tomamos $k = max(i, j)$, $H_n \cap N = H_k \cap N$ y $H_nN = H_kN$ para todo $n \geq k$. Recordemos la *ley modular de Dedekind*: Si A, B, C son subgrupos de un grupo G con $A \subset B$, entonces $A(B \cap C) = B \cap AC$. Tomemos $n \geq k$, como $H_n \geq H_k$, podemos usar esta ley y deducimos:

$$H_n = H_n \cap (H_nN) = H_n \cap (H_kN) = H_k(H_n \cap N) = H_k(H_k \cap N) = H_k.$$

□

Proposición 1.12. *Sea G un grupo abeliano. Entonces G tiene max si y solo si es finitamente generado.*

Demostración. Suponemos primero que G tiene max. Si G es cíclico, es finitamente generado. En otro caso, sea $a_1 \in G$ tal que $\langle a_1 \rangle \neq G$. Entonces $\langle a_1 \rangle$ es un subgrupo de G, y elegimos $a_2 \in G \setminus \langle a_1 \rangle$. Si $G = \langle a_1, a_2 \rangle$, ya lo tenemos. Si no, seguimos el proceso y obtenemos una serie estrictamente ascendente de subgrupos de G:

$$1 < \langle a_1 \rangle < \langle a_1, a_2 \rangle < \dots$$

Si G tiene max, la serie es finita, luego existe n tal que $G = \langle a_1, a_2, \dots, a_n \rangle$. El converso es consecuencia del hecho de que los subgrupos de un grupo abeliano y finitamente generado son finitamente generados. □

De aquí se deduce que otro ejemplo de grupos que tienen max son los grupos cíclicos.

Capítulo 2

El Teorema de Mal'cev

2.1. Extracción de raíces en grupos nilpotentes

En la próxima sección (2.2) enunciaremos el Teorema de Mal'cev, que demostraremos posteriormente en el capítulo 3. Antes debemos introducir algunos conceptos sobre grupos radicables y extracción de raíces.

Definición 2.1. Se dice que un grupo G es *libre de torsión* si no tiene elementos de orden finito, es decir, si dado $g \in G$ tal que $g^n = 1$ para cierta $n > 0$, entonces $g = 1$.

El siguiente resultado es un teorema muy importante de Teoría de Grupos y que nos será de gran ayuda más adelante.

Teorema 2.1. *Todo grupo abeliano finitamente generado y libre de torsión es isomorfo a un producto directo de grupos cíclicos.*

Demostración. Sea G un grupo abeliano, finitamente generado y libre de torsión. Entonces existen $x_1, \ldots, x_r$ tales que $G = \langle x_1, \ldots, x_r \rangle$. Veamos que podemos tomar los x_i de manera que formen una base, es decir, $x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} = 1$ con $n_i \in \mathbb{Z}$ para $i = 1, \ldots, r$ si y solo si $n_i = 0$ para cada i.

Claramente, podemos elegir $x_1, \ldots, x_r$ tales que sean una familia generadora minimal, es decir, que ninguno de ellos se pueda expresar en términos de los demás. Supongamos que existen $n_1, \ldots, n_r$ no todos cero de forma que $x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} = 1$. Además, podemos elegir los n_i de forma que $|n_1| + \ldots + |n_r|$ sea lo menor posible entre todas las familias generadoras minimales.

Si todos los n_i excepto uno fueran cero, tendríamos $x_j^{n_j} = 1$ con $n_j \neq 0$, lo que es imposible ya que G es libre de torsión. Por tanto, al menos dos exponentes son distintos de cero. Reordenando si es necesario, podemos suponer que $|n_1| \geq |n_2| > 0$ y, pasando al inverso si es necesario, podemos suponer $n_1 > 0$.

Ahora, si $n_2 > 0$, podemos escribir $x_2' = x_2 x_1$. Entonces $x_2 = x_2' x_1^{-1}$ y, teniendo en cuenta que G es abeliano, llegamos a:

$$1 = x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} = x_1^{n_1 - n_2} (x_2')^{n_2} \cdots x_r^{n_r}.$$

La familia $\{x_1, x_2', x_3, \ldots, x_r\}$ es también generadora minimal y, además:

$$|n_1 - n_2| + |n_2| + \ldots + |n_r| < |n_1| + |n_2| + \ldots + |n_r|,$$

lo que contradice nuestra hipótesis. Para $n_2 < 0$ se prueba igual pero con $x_2' = x_2 x_1^{-1}$.

De aquí se deduce que $x_1, \ldots, x_r$ ha de ser base de G. Con este resultado se puede probar que la función obvia entre G y $\langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_r \rangle$ es un isomorfismo. □

Además, todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$. En conclusión, también se puede decir que G es isomorfo a $\mathbb{Z}^r$, con r el tamaño de la base de G.

Con la definición anterior, podemos introducir la siguiente proposición que relaciona la torsión de un grupo nilpotente con la torsión de los subgrupos de su serie central ascendente.

Proposición 2.2. *Sea G un grupo nilpotente de clase k. Los siguientes enunciados son equivalentes:*

i) G es libre de torsión

ii) $Z(G)$ es libre de torsión

iii) $Z_i(G)/Z_{i-1}(G)$ es libre de torsión para todo $i = 1,...,k$

Demostración. *i)* $\Rightarrow$ *ii)* Es trivial, ya que el centro de un grupo es un subgrupo del mismo.

ii) $\Rightarrow$ *iii)* Para demostrar esto, primero vamos a probar que, si existe un elemento de torsión en $Z_{i+1}(G)/Z_i(G)$, también existirá un elemento de torsión en $Z_i(G)/Z_{i-1}(G)$. Si denotamos como F_i al cociente $Z_i(G)/Z_{i-1}(G)$, entonces para cada $i = 1,\dots,k-1$ existe un homomorfismo injectivo:

$$\theta : F_{i+1} \to Hom(G_{ab}, F_i)$$

donde la imagen de cada $zZ_i(G)$ es un homomorfismo

$$f_z := \theta(zZ_i(G)) : G_{ab} \to F_i$$

tal que $f_z(gG') = [z,g]Z_{i-1}(G)$, donde $z \in Z_{i+1}(G)$, $g \in G$.

Dado un cierto i, probemos que θ es realmente un homomorfismo inyectivo. Primero, deberíamos probar que f_z está bien definida para todo $z \in Z_{i+1}(G)$ y que es un homomorfismo. Lo primero es claro ya que $zZ_i(G) \in Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$, luego $[z,g] \in Z_i(G)$ para todo $g \in G$ y, por tanto, $f_z(gG')$ está en F_i. Veamos que es homomorfismo:

$$f_z(ghG') = [z,gh]Z_{i-1}(G) = [z,h][z,g]^h Z_{i-1}(G) = [z,g]Z_{i-1}(G)[z,h]Z_{i-1}(G) = f_z(gG')f_z(hG'),$$

donde primero usamos el lema 1.3 y después que $[z,g]Z_{i-1}(G), [z,h]Z_{i-1}(G) \in Z_i(G)/Z_{i-1}(G)$ luego conmutan con todo elemento de $G/Z_{i-1}(G)$.

Veamos ahora que θ está bien definido. Si $z_1Z_i(G) = z_2Z_i(G)$, entonces $z_1z_2^{-1} \in Z_i(G)$. Queremos ver que $f_{z_1} = f_{z_2}$. Sea $g \in G$, entonces $f_{z_1}(gG') = f_{z_2}(gG')$ implica que $[z_1,g][z_2,g]^{-1} \in Z_{i-1}(G)$. Como estamos trabajando con la serie central ascendente, tenemos que:

$$[z_1,g][g,z_2]Z_{i-1}(G) = z_1^{-1}g^{-1}z_1z_2^{-1}gz_2Z_{i-1}(G) = z_1^{-1}z_1z_2^{-1}g^{-1}gz_2Z_{i-1}(G) = 1,$$

con lo que queda probado lo que queríamos.

Para ver que θ es homomorfismo tomamos $z_1, z_2 \in Z_{i+1}(G)$ y tenemos que ver $\theta(z_1Z_i(G)\cdot z_2Z_i(G)) = \theta(z_1Z_i(G))\cdot\theta(z_2Z_i(G))$. Esto equivale a probar que $f_{z_1z_2} = f_{z_1}f_{z_2}$, es decir:

$$f_{z_1z_2}(gG') = f_{z_1}(gG')f_{z_2}(gG')$$

para todo $gG' \in G_{ab}$. Usando otra vez las propiedades de los conmutadores vistas en el lema 1.3, obtenemos:

$$f_{z_1z_2}(gG') = [z_1z_2,g]Z_{i-1}(G) = [z_1,g]^{z_2}[z_2,g]Z_{i-1}(G) = [z_1,g][z_2,g]Z_{i-1}(G) = f_{z_1}(gG')f_{z_2}(gG'),$$

donde en la penúltima igualdad hemos considerado que $[z_1,g]Z_{i-1}(G) \in F_i$ y conmuta con los elementos de $G/Z_{i-1}(G)$.

Nos queda ver que θ es inyectivo. Sea $zZ_i(G) \in Z_{i+1}(G)/Z_i(G)$ tal que $f_z = 1$, es decir, $f_z(gG') = 1 = Z_{i-1}(G)$ para todo $g \in G$. Entonces, por la definición de f_z, para todo $g \in G$, tenemos:

$$Z_{i-1}(G) = [z,g]Z_{i-1}(G) \Leftrightarrow zgZ_{i-1}(G) = gzZ_{i-1}(G).$$

Esto implica que $zZ_{i-1}(G) \in Z(G/Z_{i-1}(G)) = F_i$, luego $z \in Z_i(G)$, es decir, $zZ_i(G) = 1$.

Por tanto, si $zZ_i(G) \neq 1$ y $z^nZ_i(G) = 1$ para cierto $n > 0$ y $z \in Z_{i+1}(G)$, entonces $[z^n,g]Z_{i-1}(G) = 1$ para todo $g \in G$, es decir, $[z,g]^nZ_{i-1}(G) = 1$, aplicando las propiedades de los conmutadores y que la serie es central. Sin embargo, como θ es inyectivo, $f_z \neq 1$, es decir, existe $g \in G$ tal que $[z,g]Z_{i-1}(G) \neq 1$.

Hemos probado que, si existe algún elemento de torsión en $F_{i+1} = Z_{i+1}(G)/Z_i(G)$, entonces existe algún elemento de torsión en $F_i = Z_i(G)/Z_{i-1}(G)$. Luego, si para algún $i = 2,\dots,k$, existe un elemento de torsión en $Z_i(G)/Z_{i-1}(G)$, reiterando llegamos a que existe un elemento de torsión en $Z_1(G)/Z_0(G) = Z(G)$. Esto contradice ii).

iii) $\Rightarrow$ *i)* Lo probamos por reducción al absurdo. Sea $g \in G$, tal que $g \neq 1$ y $g^n = 1$. En otras palabras, $g \in G = Z_k(G)$ y $g \notin Z_0(G)$. Por tanto, existe algún valor $i \leq k$ tal que $g \in Z_i(G)$, pero $g \notin Z_{i-1}(G)$. Esto implica que $gZ_{i-1}(G) \neq 1$ y, sin embargo:

$$(gZ_{i-1}(G))^n = g^n Z_{i-1}(G) = 1.$$

Esto contradice que los cocientes de la serie sean libres de torsión. □

Corolario 2.3. *Sea G un grupo nilpotente. Si G es libre de torsión, entonces $G/Z(G)$ también lo es.*

Demostración. Usando la equivalencia *i)* $\Rightarrow$ *iii)* de la proposición anterior (2.2), tenemos que el cociente $Z_i(G)/Z_{i-1}(G)$ es libre de torsión para todo $i = 1,...,k$. Supongamos que $G/Z(G)$ no es libre de torsión. Entonces existe $g \in G$ con $gZ(G) \neq 1$, tal que $(gZ(G))^n = 1$. Es decir, $g^n Z(G) = 1$ o, equivalentemente, $g^n \in Z(G)$. Si $g \notin Z_{k-1}(G)$, como $Z(G) \subset Z_{k-1}(G)$, $(gZ_{k-1}(G))^n = g^n Z_{k-1}(G) = 1$. Pero esto quiere decir que tenemos un elemento de torsión en $Z_k(G)/Z_{k-1}(G)$, lo cual contradice que G sea libre de torsión. Por tanto, $g \in Z_{k-1}(G)$ y podemos repetir el argumento con el siguiente cociente hasta llegar a $g \in Z(G)$. Lo cual contradice nuestra suposición. □

Antes de enunciar el teorema principal de este trabajo, necesitamos introducir algunos conceptos nuevos y probar un último resultado.

Definición 2.2. Sea π un conjunto no vacío de primos. Entonces un grupo G se dice *π-radicable* (o simplemente *radicable* si π es el conjunto de todos los primos) si para todo $g \in G$ y todo π-número positivo n, la ecuación $x^n = g$ tiene una solución x en G. Esto significa que cada elemento de G debe tener una raíz enésima en G para todos los π-números positivos n. Si esta solución es única, se dice que la extracción de raíces es única.

En este contexto, un π-número es un número tal que todos sus divisores están en π.

Definición 2.3. Sea n un entero positivo. Decimos que G es *n-libre de torsión* si $g^n = 1$ implica $g = 1$ para todo $g \in G$.

Definición 2.4. Sea π un conjunto de primos. Se dice que un grupo G es *π-libre de torsión* si es p-libre de torsión para cada primo p en π o, equivalentemente, es n-libre de torsión para cada π-número n.

Si un grupo tiene extracción única de π-raíces, entonces es claramente π-libre de torsión (para la ecuación $x^n = 1$, $x = 1$ es una solución, luego es la única solución). Por tanto, los grupos radicables en los que la extracción de raíces es única son aquellos que son libres de torsión.

Observación. La extracción de raíces no siempre es posible en un grupo libre de torsión. Ese es el caso de los grupos cíclicos infinitos. Por ejemplo, en el grupo $G = \langle 2 \rangle$, la ecuación $x^n = 2^m$ solo tiene solución en G si n divide a m. Sin embargo, todo grupo cíclico infinito es isomorfo a un subgrupo de un grupo radicable libre de torsión, por ejemplo, del grupo multiplicativo de los números racionales $\mathbb{Q}$. Este hecho, que veremos con más detalle en la sección 2.2, se puede generalizar a todos los grupos nilpotentes libres de torsión, dando lugar al *Teorema de Mal'cev*.

Observamos que, si existe, la extracción de raíces siempre es única en un grupo nilpotente y libre de torsión. Esto es una consecuencia directa de la siguiente proposición.

Proposición 2.4. *Sea G un grupo nilpotente y libre de torsión con elementos $a, b \in G$ tales que $a^n = b^n$ para algún $n > 0$. Entonces $a = b$.*

Demostración. Lo probamos por inducción en la clase de nilpotencia k de G. Sea G abeliano ($k = 1$). Entonces:

$$a^n = b^n \Leftrightarrow a^n(b^n)^{-1} = 1 \Leftrightarrow 1 = a^n(b^{-1})^n = (ab^{-1})^n$$

donde en la última igualdad hemos aplicado que G es abeliano. Como G es libre de torsión y $ab^{-1} \in G$, $ab^{-1} = 1$, es decir, $a = b$.

Supongamos ahora que la proposición se cumple para clases de nilpotencia menores que k. Sea G un grupo libre de torsión con clase de nilpotencia k. Entonces $G/Z(G)$ tiene clase de nilpotencia $k-1$ (esto es fácil verlo utilizando la serie central ascendente de G). Además, es libre de torsión por el corolario 2.3. Ahora sean $a, b \in G$ con $a^n = b^n$. En $G/Z(G)$ tenemos

$$(aZ(G))^n = (bZ(G))^n$$

y, por la hipótesis de inducción, $aZ(G) = bZ(G)$. Es decir, existe $z \in Z(G)$ tal que $a = bz$. Teniendo en cuenta que z está en el centro de G:

$$a^n = (bz)^n = bzbz\cdots bz = b^n z^n.$$

Por otra parte, teníamos que $a^n = b^n$, luego podemos concluir que $b^n = b^n z^n$ y, por tanto, $z^n = 1$. Como G es libre de torsión, $z = 1$ y entonces $a = bz = b$. □

2.2. El teorema de Mal'cev

Una vez que hemos presentado los conceptos y los resultados necesarios para entender el teorema de Mal'cev, podemos finalmente enunciarlo, aunque la demostración la realizaremos en el próximo capítulo.

Teorema (Teorema de Mal'cev)**.** *Todo grupo nilpotente G libre de torsión es isomorfo a un subgrupo de un grupo nilpotente G^* en el cual la extracción de raíces es única de forma que cada elemento de G^* tiene una potencia positiva en G. Además, el grupo G^* es único salvo isomorfismos.*

Un grupo con las propiedades de G^* se dice *complección de Mal'cev* o *cubierta radicable* del grupo G.

Si reemplazamos en el enunciado del teorema "libre de torsión" por "π-libre de torsión", con π un conjunto cualquiera de primos, obtenemos que G puede ser incluido en un grupo nilpotente y π-radicable G^*_π.

Ahora siguiendo la observación que hicimos en la sección anterior (2.1), vamos a probar el teorema de Mal'cev cuando nuestro grupo es abeliano y finitamente generado. Si trabajamos con notación aditiva, hemos visto en el teorema 2.1 que $G \cong \mathbb{Z}^r$ para algún r y basta poner $G^* = \mathbb{Q}^r$. Vamos a hacer la demostración en detalle pero con notación multiplicativa, ya que nos ayudará a entender el caso general.

Proposición 2.5. *Sea G un grupo abeliano, libre de torsión y finitamente generado. Entonces existe un grupo abeliano H tal que $G \leqslant H$ y tal que:*

i) para todo n y todo $x \in H$, existe un único elemento $y \in H$ con $y^n = x$ (H es radicable)

ii) para todo $x \in H$ existe $m > 0$ con $x^m \in G$ (cada elemento de H tiene una potencia positiva en G).

Demostración. Como G es abeliano y finitamente generado, aplicando el teorema 2.1, tenemos que es isomorfo a $G_1 \times \cdots \times G_r$, donde r es el orden de G y $G_i = \langle a_i \rangle$ para todo i. Los elementos de G son de la forma $a_1^{\alpha_1} \cdots a_r^{\alpha_r}$, con $\alpha_i \in \mathbb{Z}$.

Llamamos H al conjunto de los productos formales $a_1^{\beta_1} \cdots a_r^{\beta_r}$ donde $\beta_i \in \mathbb{Q}$. Definimos una operación interna en H:

$$(a_1^{\beta_1} \cdots a_r^{\beta_r}) \cdot (a_1^{\gamma_1} \cdots a_r^{\gamma_r}) := a_1^{\beta_1+\gamma_1} \cdots a_r^{\beta_r+\gamma_r}.$$

Primero debemos probar que $(H, \cdot)$ es un grupo y que $G \leqslant H$.

- La operación es claramente asociativa, por la asociatividad de la suma en $\mathbb{Q}$.
- Existe un elemento identidad $1 := a_1^0 \cdots a_r^0$: $1 \cdot (a_1^{\beta_1} \cdots a_r^{\beta_r}) = a_1^{0+\beta_1} \cdots a_r^{0+\beta_r} = a_1^{\beta_1} \cdots a_r^{\beta_r}$.
- Para todo elemento, $a_1^{\beta_1} \cdots a_r^{\beta_r}$, de H existe un inverso en H: $a_1^{-\beta_1} \cdots a_r^{-\beta_r}$.
- Sea $a_1^{\alpha_1} \cdots a_r^{\alpha_r} \in G$, $\alpha_i \in \mathbb{Z} \subset \mathbb{Q}$. Es claro que $a_1^{\alpha_1} \cdots a_r^{\alpha_r} \in H$. Además, la operación de G se define de la misma forma por ser abeliano. Luego $G \leqslant H$.

Ahora veremos que se cumplen las condiciones del teorema.

- H es un grupo abeliano, luego nilpotente.
- Para todo $n > 0$ y todo $x = a_1^{\beta_1} \cdots a_r^{\beta_r} \in H$, el elemento $y = a_1^{\frac{\beta_1}{n}} \cdots a_r^{\frac{\beta_r}{n}} \in H$ es la única solución de la ecuación $y^n = x$.
- Sea $x = a_1^{\beta_1} \cdots a_r^{\beta_r} \in H$. Como $\beta_i \in \mathbb{Q}$, existen $n_i, m_i \in \mathbb{Z}$ tales que $\beta_i = \frac{n_i}{m_i}$ para cada i. Llamando $m := m_1 \cdots m_r$, entonces $x^m = (a_1^{\beta_1} \cdots a_r^{\beta_r})^m \in G$.

□

Capítulo 3

Demostración del Teorema de Mal'cev

Nos disponemos a probar el *Teorema de Mal'cev* para grupos nilpotentes libres de torsión y finitamente generados. El caso general (no necesariamente finitamente generado) queda fuera de los objetivos de este trabajo. Seguiremos los métodos de P. Hall (1969).

Teorema (Teorema de Mal'cev)**.** *Todo grupo nilpotente G libre de torsión es isomorfo a un subgrupo de un grupo nilpotente G^* en el cual la extracción de raíces es única de forma que cada elemento de G^* tiene una potencia positiva en G. Además, el grupo G^* es único salvo isomorfismos.*

3.1. Existencia de la complección

Sea G un grupo nilpotente libre de torsión y finitamente generado. Asumimos que tiene clase de nilpotencia m.

Recordemos que todo grupo abeliano tiene max si y solo si es finitamente generado y que, si N es normal en G, G/N y N tienen max si y solo si G tiene max (lo vimos en la sección 1.3). Por otra parte, por la proposición 1.5 sabemos que $\gamma_i(G)/\gamma_{i+1}(G)$ es finitamente generado para todo $i = 1,\dots n$. Como además los cocientes de una serie central son abelianos por definición, los $\gamma_i(G)/\gamma_{i+1}(G)$ tienen max. En particular, para $i = m$, $\gamma_m(G)/\gamma_{m+1}(G) = \gamma_m(G)$ tiene max. Por tanto, $\gamma_{m-1}(G)$ tiene max. Y de forma recursiva, concluimos que G tiene max. Ahora nos fijamos en la serie central ascendente. Como $Z_i(G)$ es normal en G, para todo $i = 0,1\dots,m$, tanto los subgrupos de la serie como los cocientes $Z_i(G)/Z_{i-1}(G)$ tienen max. Y en consecuencia, como también son abelianos, $Z_i(G)/Z_{i-1}(G)$ son finitamente generados.

Lema 3.1. *Sea A un grupo abeliano, finitamente generado y libre de torsión. Entonces $A \cong \mathbb{Z}^n$. Además, existe una serie $1 = T_0 \trianglelefteq T_1 \trianglelefteq \dots \trianglelefteq T_{n-1} \trianglelefteq T_n = A$ tal que $T_i/T_{i-1} \cong \mathbb{Z}$.*

Demostración. La primera parte ya la vimos en el capítulo anterior (teorema 2.1). Como hicimos entonces, suponemos $A = \langle x_1,\dots,x_n\rangle$, donde $\{x_1,\dots,x_n\}$ es una base de A. Definimos $T_{n-1} := \langle x_1,\dots,x_{n-1}\rangle$, que es un subgrupo de A y, por ser A abeliano, es normal. Por otra parte, definimos:

$$\begin{aligned} \phi : & T_n/T_{n-1} \to \mathbb{Z} \\ & gT_{n-1} \mapsto r_n \end{aligned}$$

donde $g = x_1^{r_1}\dots x_{n-1}^{r_{n-1}}x_n^{r_n}$. Primero, observamos que $gT_{n-1} = hT_{n-1}$ si y solo si sus exponentes en x_n coinciden. Por tanto, la función está bien definida. A partir de ahora, nos centramos en los elementos de la forma $g = x_n^r$. Claramente, ϕ es homomorfismo de grupos, suprayectiva e inyectiva, puesto que tomamos una base de A. Por tanto, ϕ es un isomorfismo y concluimos que $T_n/T_{n-1} \cong \mathbb{Z}$. Por inducción en i se deduce el resultado. □

Ahora consideramos la serie central acendente de G:

$$1 = Z_0(G) \triangleleft Z_1(G) = Z(G) \triangleleft \dots \triangleleft Z_{m-1}(G) \triangleleft Z_m(G) = G,$$

cuyos cocientes son abelianos y finitamente generados, como acabamos de ver, y libres de torsión (aplicando la proposición 2.2). Aplicando el lema anterior sobre $Z(G)$ (abeliano, finitamente generado y libre de torsión), obtenemos que existe una serie

$$1 = T_0^{(1)} \triangleleft T_1^{(1)} \triangleleft \ldots \triangleleft T_{k_1}^{(1)} = Z(G)$$

con $T_{i+1}^{(1)}/T_i^{(1)} \cong \mathbb{Z}$. Hemos refinado la serie entre 1 y $Z(G)$ añadiendo más subgrupos cuyos cocientes son isomorfos a $\mathbb{Z}$.

Podemos repetir este proceso en cada cociente. Sea $i = 1, 2, \ldots, m$, existe una serie:

$$1 = T_0^{(i)}/Z_{i-1}(G) \triangleleft T_1^{(i)}/Z_{i-1}(G) \triangleleft \ldots \triangleleft T_{k_i}^{(i)}/Z_{i-1}(G) = Z_i(G)/Z_{i-1}(G)$$

con $(T_{j+1}^{(i)}/Z_{i-1}(G))\big/(T_j^{(i)}/Z_{i-1}(G)) \cong \mathbb{Z}$. Aplicando el Tercer Teorema de Isomorfía:

$$(T_{j+1}^{(i)}/Z_{i-1}(G))\big/(T_j^{(i)}/Z_{i-1}(G)) \cong T_{j+1}^{(i)}/T_j^{(i)}.$$

Se puede ver que:

$$Z_{i-1}(G) = T_0^{(i)} \triangleleft T_1^{(i)} \triangleleft \ldots \triangleleft T_{k_i}^{(i)} = Z_i(G).$$

Por tanto, uniendo todas estas series, se puede refinar la serie central ascendente a otra serie (que también es central)

$$1 = G_n \triangleleft G_{n-1} \triangleleft \ldots \triangleleft G_0 = G,$$

donde cada cociente $G_{i-1}/G_i \cong \mathbb{Z}$, es decir, es cíclico infinito, digamos con generador $u_i G_i$. Este número n solo depende de G y se llama *longitud de Hirsch* [3].

Vamos a ver que cada elemento a de G tiene una única expresión $a = u_1^{\alpha_1} u_2^{\alpha_2} \cdots u_n^{\alpha_n}$ con α_i entero para todo i.

Supongamos que $a \in G_{n-1}/G_n = G_{n-1} = \langle u_n \rangle$, entonces es claro que $a = u_n^{\alpha_n}$, y esta expresión es única. Si $aG_{n-1} \in G_{n-2}/G_{n-1} = \langle u_{n-1}G_{n-1} \rangle$, entonces $aG_{n-1} = u_{n-1}^{\alpha_{n-1}} G_{n-1}$. Luego $a = u_{n-1}^{\alpha_{n-1}} g$, con $g \in G_{n-1}$. Por tanto, $a = u_{n-1}^{\alpha_{n-1}} u_n^{\alpha_n}$ y esta expresión es única. Supongamos que esto se cumple hasta cierto i. Sea ahora $a \in G_{i-1}$, en particular, $aG_i \in G_{i-1}/G_i = \langle u_i G_i \rangle$, entonces $aG_i = u_i^{\alpha_i} G_i$ y, en consecuencia, $a = u_i^{\alpha_i} g$ con $g \in G_i$. Apicando la hipótesis de inducción, $g = u_{i+1}^{\alpha_{i+1}} \cdots u_n^{\alpha_n}$ y, por tanto, $a = u_i^{\alpha_i} u_{i+1}^{\alpha_{i+1}} \ldots u_n^{\alpha_n}$. Con esto queda demostrado lo que queríamos. Además también hemos probado que $G_i = \langle u_{i+1}, \ldots, u_n \rangle$, para todo $i = 1, \ldots, n$ y, en consecuencia, $G/G_i = \langle u_1 G_i, \ldots, u_i G_i \rangle$.

Siguiendo el ejemplo 1.10 del capítulo anterior, veamos cómo son estos exponentes al hacer el producto de dos elementos del grupo o calcular una potencia de otro.

Ejemplo 3.2. De nuevo, $n = 3$ y escogemos $R = \mathbb{Z}$. Entonces nuestro grupo es:

$$G = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \},$$

que ya vimos que es nilpotente. Como el elemento u_3 del ejemplo 1.10 es de orden infinito, tenemos que $Z(G) = G_2 = \langle u_3 \rangle$ es libre de torsión y, en consecuencia, G es libre de torsión aplicando la proposición 2.2. Estamos en las condiciones del *Teorema de Mal'cev*.

Ahora definimos los subgrupos de G:

$$G_1 = \{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid b, c \in \mathbb{Z} \} \text{ y } G_2 = \{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \}.$$

G_2 es el mismo subgrupo del ejemplo 1.10. Usando las fórmulas del producto, se puede ver fácilmente que son subgrupos de G. Además, $G_1 \triangleleft G$:

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

y $G_2 \triangleleft G_1$, ya que $G_2 = Z(G)$. Tenemos una serie de subgrupos normales de G: $1 = G_3 \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$. Además, consideramos otra vez las matrices:

$$u_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, u_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ y } u_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

y podemos probar que $G/G_1 = \langle u_1 G_1 \rangle$, $G_1/G_2 = \langle u_2 G_2 \rangle$ y $G_2/G_3 = G_2 = \langle u_3 \rangle$. Empezamos tomando una matriz

$$g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

en G. Entonces:

$$gG_1 = u_1^m G_1 \Leftrightarrow u_1^m g^{-1} \in G_1 \Leftrightarrow a - m \cdot 1 = 0,$$

por tanto, $gG_1 = u_1^a G_1$. Análogamente, sea

$$g_1 = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

en G_1, entonces:

$$g_1 G_2 = u_2^m G_2 \Leftrightarrow u_2^m g_1^{-1} \in G_2 \Leftrightarrow c - m \cdot 1 = 0,$$

luego $g_1 G_2 = u_2^c G_2$. Y, por último, sea

$$g_2 = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

en G_2, entonces $g_2 = u_3^m \Leftrightarrow b - m \cdot 1 = 0$, luego $g_2 = u_3^b$.

Por tanto, la serie $1 = G_3 \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$ es central con cocientes consecutivos cíclicos infinitos, y la longitud de Hirsch de G es 3. Observemos que este valor no coincide con la clase de nilpotencia de G, que ya vimos en el primer capítulo que es 2.

De hecho, sea $g \in G$ como antes, podemos escribir: $g = u_1^a u_2^c u_3^b$. Lo comprobamos directamente:

$$u_1^a u_2^c u_3^b = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

En el ejemplo 1.10, vimos que los conmutadores de estas matrices son: $[u_1, u_2] = u_3$, $[u_2, u_3] = 1$ y $[u_1, u_3] = 1$. Por tanto, obtenemos las siguientes identidades:

$$u_1 u_2 = u_2 u_1 u_3 \qquad u_2 u_3 = u_3 u_2 \qquad u_1 u_3 = u_3 u_1$$

Tomamos ahora dos matrices $g = u_1^{\alpha_1} u_2^{\alpha_2} u_3^{\alpha_3}$ y $h = u_1^{\beta_1} u_2^{\beta_2} u_3^{\beta_3}$ en G y, usando las identidades anteriores, calculamos su producto:

$$\begin{aligned} gh &= u_1^{\alpha_1} u_2^{\alpha_2} u_3^{\alpha_3} u_1^{\beta_1} u_2^{\beta_2} u_3^{\beta_3} = u_1^{\alpha_1} u_2^{\alpha_2} u_1^{\beta_1} u_3^{\alpha_3} u_2^{\beta_2} u_3^{\beta_3} \\ &= u_1^{\alpha_1} u_1^{\beta_1} u_2^{\alpha_2} u_3^{-\alpha_2 \beta_1} u_3^{\alpha_3} u_2^{\beta_2} u_3^{\beta_3} = u_1^{\alpha_1 + \beta_1} u_2^{\alpha_2} u_2^{\beta_2} u_3^{-\alpha_2 \beta_1 + \alpha_3} u_3^{\beta_3} \\ &= u_1^{\alpha_1 + \beta_1} u_2^{\alpha_2 + \beta_2} u_3^{\alpha_3 + \beta_3 - \alpha_2 \beta_1} \end{aligned}$$

En la tercera igualdad, para cada u_2 hacemos tantos intercambios como $u_1's$ haya, luego $\alpha_2\beta_1$ intercambios en total. Análogamente obtendríamos:

$$(u_1^{\alpha_1}u_2^{\alpha_2}u_3^{\alpha_3})^{-1} = u_3^{-\alpha_3}u_2^{-\alpha_2}u_1^{-\alpha_1} = u_1^{-\alpha_1}u_2^{-\alpha_2}u_3^{-\alpha_3-\alpha_1\alpha_2}.$$

De aquí se deduce que los exponentes del producto o la exponenciación de elementos de G son poliniomios en los exponentes de esos elementos. Este resultado se va a probar de manera general en los siguientes párrafos.

Pasando al caso general, por conveniencia, escribimos $a = u^\alpha$ para referirnos a $u_1^{\alpha_1}u_2^{\alpha_2}\cdots u_n^{\alpha_n}$. Llamaremos a los α_i *parámetros canónicos* de a con respecto a la base $\{u_1, u_2 \ldots, u_n\}$ de G. Ahora, sea $b \in G$, con $b = u^\beta$, el producto de a y b dará otro elemento en G, digamos $ab = c = u^\gamma$. Aquí los parámetros γ_i son funciones de las $2n$ variables enteras α_j, β_j. De forma similar, si m es un entero, $a^m = u^\omega$, donde los ω_i son funciones de m y las n variables enteras α_j.

Sea F un cuerpo de característica 0 y sea G^F el conjunto de todos los productos formales u^α con exponentes $\alpha_1, \ldots, \alpha_n$ en F. Vimos que todo elemento de G se puede ver como u^α con exponentes enteros. La idea ahora es definir una multiplicación y una exponenciación en G^F usando las funciones γ_i y ω_i mencionadas para G, de la forma obvia, y después probar que G^F es un grupo nilpotente radicable en el cual G se incluye como un subgrupo. Primero hay que demostrar que G^F es un grupo. Para ello, primero necesitamos el siguiente resultado:

Lema 3.3. *Las funciones γ_i son polinomios en las variables α_j, β_j. A su vez, las funciones ω_i son polinomios en m y en las variables α_j. Habitualmente, estos polinomios son conocidos como los* polinomios de Hall.

Demostración. Es claro que los exponentes γ_i dependen de $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$. Tenemos que probar que existen polinomios $f_i(x,y)$ en los $2n$ argumentos $x_1, \ldots, x_n, y_1, \ldots, y_n$ tales que $f_i(\alpha, \beta) = \gamma_i$. Y algo similar se debe cumplir para ω_i^m. Como un polinomio está determinado unívocamente por el valor que toma en cada argumento, identificamos la función γ_i con el polinomio f_i.

Sabemos que $G_i \triangleleft G$, luego podemos considerar su cociente $G/G_i = \langle u_1, \ldots, u_i \rangle$ y observamos:

$$\begin{aligned} abG_i &= u_1^{\alpha_1}\cdots u_i^{\alpha_i}u_1^{\beta_1}\cdots u_i^{\beta_i}G_i \\ cG_i &= u_1^{\gamma_1}\cdots u_i^{\gamma_i}G_i, \end{aligned}$$

como $abG_i = cG_i$, podemos concluir que γ_i depende únicamente de $\alpha_1, \ldots, \alpha_i, \beta_1, \ldots, \beta_i$. Análogamente, ω_i^m depende únicamente de $\alpha_1, \ldots, \alpha_i$ y m.

Sea ahora $n = 1$, entonces G es cíclico infinito y tenemos $\gamma_1(\alpha_1, \beta_1) = \alpha_1 + \beta_1$, $\omega_1^m(\alpha_1) = m\alpha_1$. Sea $n > 1$ vamos a proceder por inducción sobre n. Llamamos Γ_n a la hipótesis que dice que, para cualquier grupo nilpotente finitamente generado con una serie de factores cíclicos de longitud menor o igual que n y subconjunto generador asociado $\{u_1, \ldots, u_n\}$, los exponentes γ_i tales que

$$u_1^{\alpha_1}\cdots u_n^{\alpha_n}u_1^{\beta_1}\cdots u_n^{\beta_n} = u_1^{\gamma_1}\cdots u_n^{\gamma_n}$$

vienen dados por polinomios en $\alpha_1, \ldots, \alpha_i, \beta_1, \ldots, \beta_i$. Análogamente, consideramos la hipótesis Ω_n que afirma que en las condiciones anteriores los ω_i^m son polinomios en m y $\alpha_1, \ldots, \alpha_i$.

Asumimos que Γ_i y Ω_i se cumplen para $i < n$ y vamos a probar que Γ_n también se cumple. Observamos primero que $cG_1 = u_1^{\gamma_1}G_1 = abG_1 = u^{\alpha_1}u^{\beta_1}G_1 = u^{\alpha_1+\beta_1}G_1$, por tanto, $\gamma_1 = \alpha_1 + \beta_1$. En nuestra expresión del producto ab queremos que $u_1^{\alpha_1}$ y $u_1^{\beta_1}$ aparezcan juntos. Para ello usamos

$$u_i^{\alpha_i}u_{i+1}^{\alpha_{i+1}} = u_i^{\alpha_i}u_1^{\beta_1}u_1^{-\beta_1}u_{i+1}^{\alpha_{i+1}}$$

para cada $i = 1, \ldots, n-1$ y llegamos a:

$$\begin{aligned} c = ab = u^\alpha u^\beta &= u_1^{\alpha_1}u_1^{\beta_1}u_1^{-\beta_1}u_2^{\alpha_2}\cdots u_1^{\beta_1}u_1^{-\beta_1}u_n^{\alpha_n}u_1^{\beta_1}u_2^{\beta_2}\cdots u_n^{\beta_n} \\ &= u_1^{\alpha_1+\beta_1}\prod_{i=2}^{n}(u_1^{-\beta_1}u_i^{-\alpha_i}u_1^{\beta_1})^{-1}u_2^{\beta_2}\cdots u_n^{\beta_n} = u_1^{\alpha_1+\beta_1}\prod_{i=2}^{n}(u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1})^{-\alpha_i}u_2^{\beta_2}\cdots u_n^{\beta_n}, \end{aligned} \tag{3.1}$$

donde en la última igualdad utilizamos que $u_1^{-\beta_1}u_i^{-\alpha_i}u_1^{\beta_1} = (u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1})^{\alpha_i}$ para cada i.

Ahora, separamos los u_1 de la expresión $u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1}$ así:

$$u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1} = u_1^{-\beta_1}u_i^{-1}u_1(u_iu_i^{-1})u_1(u_iu_i^{-1})\cdots u_1(u_iu_i^{-1}) = u_1^{-\beta_1}(u_i^{-1}u_1u_i)^{\beta_1}u_i^{-1}. \tag{3.2}$$

Una vez tenemos estos cálculos hechos , vamos a considerar el grupo $H_i \leq G$ generado por $u_1, u_{i+1}, \ldots, u_n$. Este grupo tiene una serie central:

$$1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_{i+1} \triangleleft G_i \triangleleft H_i.$$

Para demostrarlo solo tenenemos que probar que el último cociente es cíclico infinito. Pero esto es trivial ya que, para todo $g \in H_i$, tenemos: $gG_i = u_1^{\alpha_1}u_{i+1}^{\alpha_{i+1}}\cdots u_n^{\alpha_n}G_i = u_1^{\alpha_1}G_i$.

Por tanto, H_i es un grupo nilpotente cuya longitud de la serie es igual a $n-i+1$. Si $i > 1$, podemos suponer que se cumple Ω_{n-i+1} para H_i. Como $[u_1,u_i] \in [G,G_{i-1}] \leq G_i < H_i$, $[u_1,u_i] = u_1^{-1}u_i^{-1}u_1u_i \in H_i$. Pero además, $u_1 \in H_i$, luego $u_i^{-1}u_1u_i \in H_i$. En consecuencia, podemos usar Ω_{n-i+1} para deducir:

$$(u_i^{-1}u_1u_i)^{\beta_1} = u_1^{\beta_1}u_{i+1}^{\phi_{i,1}}\cdots u_n^{\phi_{i,n-i}}, \text{ donde } \phi_{i,j} \text{ son polinomios en } \beta_1. \tag{3.3}$$

El exponente de u_1 se deduce tomando módulo G_i:

$$(u_i^{-1}u_1u_i)^{\beta_1}G_i = u_i^{-1}u_1^{\beta_1}u_iG_i = u_1^{\beta_1}G_i,$$

donde en la primera igualdad deshacemos lo que hicimos en 3.2 y para la segunda solo hay que notar que $[u_1^{\beta_1}, u_i] \in G_i$.

También se cumple Γ_{n-i+1} para G_{i-1}, luego usando esta propiedad y lo que acabamos de ver en 3.2, tenemos:

$$\begin{aligned} u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1} &= u_1^{-\beta_1}(u_i^{-1}u_1u_i)^{\beta_1}u_i^{-1} = u_1^{-\beta_1}u_1^{\beta_1}u_{i+1}^{\phi_{i,1}}\cdots u_n^{\phi_{i,n-i}}u_i^{-1} \\ &= u_i^{-1}u_{i+1}^{\psi_{i,1}}\cdots u_n^{\psi_{i,n-i}}, \text{ con } \psi_{i,j} \text{ polinomios en los } \phi_{i,k} \text{ luego en } \beta_1 \end{aligned}$$

De nuevo, el exponente de u_i se deduce tomando módulo G_i: $u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1}G_i = u_i^{-1}[u_i^{-1},u_1^{\beta_1}]G_i = u_i^{-1}G_i$.

Ahora, volvemos a aplicar Ω_{n-i+1} en el grupo G_{i-1}:

$$(u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1})^{-\alpha_i} = u_i^{\alpha_i}u_{i+1}^{\theta_{i,1}}\cdots u_n^{\theta_{i,n-i}}, \text{ donde } \theta_{i,j} \text{ son polinomios en } \beta_1 \text{ y } \alpha_i.$$

El exponente de u_i se deduce como las otras veces tomando módulo G_i.

Para finalizar, volvemos a la expresión 3.1:

$$\begin{aligned} c = ab &= u_1^{\alpha_1+\beta_1}\prod_{i=2}^{n}(u_1^{-\beta_1}u_i^{-1}u_1^{\beta_1})^{-\alpha_i}u_2^{\beta_2}\cdots u_n^{\beta_n} = u_1^{\alpha_1+\beta_1}\prod_{i=2}^{n}(u_i^{\alpha_i}u_{i+1}^{\theta_{i,1}}\cdots u_n^{\theta_{i,n-i}})u_2^{\beta_2}\cdots u_n^{\beta_n} \\ &= u_1^{\alpha_1+\beta_1}u_2^{\gamma_2}\cdots u_n^{\gamma_n}, \text{ con } \gamma_i \text{ polinomios en } \alpha_2,\cdots,\alpha_n,\beta_1,\beta_2,\cdots,\beta_n \end{aligned}$$

En la última igualdad hemos usado Γ_{n-1} ya que cada factor de $\prod_{i=2}^{n}(u_i^{\alpha_2}u_{i+1}^{\theta_{i,1}}\cdots u_n^{\theta_{i,n-i}})u_2^{\beta_2}\cdots u_n^{\beta_n}$ está en G_1, que es nilpotente con longitud de la serie igual a $n-1$. Queda probado Γ_n.

Nos queda por probar Ω_n: $(u_1^{\alpha_1}\cdots u_n^{\alpha_n})^m = u_1^{\omega_1^m}\cdots u_n^{\omega_n^m}$, donde los exponentes ω_i^m son polinomios en $\alpha_1,\cdots,\alpha_n$ y m. Para ello, inspirándonos en la idea del artículo [3] (p.205), demostramos el siguiente resultado:

Lema 3.4. *Sea $f : \mathbb{N}_0 \to \mathbb{Q}$ una función tal que existe un polinomio g con coeficientes en F que cumple que $f(m) = f(m-1)+g(m-1)$ para todo $m \geq 1$. Entonces f también es un polinomio con coeficientes en F.*

Demostración. Los valores $f(m)$, para $m \geq 0$, están totalmente determinados por $f(0)$ y el polinomio g. Por tanto, basta probar que existe un polinomio p tal que $p(0) = f(0)$ y $p(m) = p(m-1) + g(m-1)$ para cada $m \geq 1$.

Sea $g(x) = c_0 + c_1 x + \cdots + c_l x^l \in F[x]$. Consideramos los *números de Bernoulli* $\{B_k \mid k \in \mathbb{N}_0\}$, una sucesión infinita de números racionales: $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, \ldots$. Estos números satisfacen:

$$\sum_{i=1}^{x-1} i^t = \frac{1}{t+1} \sum_{k=0}^{m} B_k \binom{t+1}{k} x^{t-k+1}, \forall x,t \in \mathbb{N} \tag{3.4}$$

Para todo $t > 0$ definimos:

$$f_t = \sum_{k=0}^{l+1-t} \frac{c_{t+k-1}}{t+k} B_k \binom{t+k}{k} \in F$$

y fijamos $f_0 = f(0)$. Entonces, si ponemos el polinomio $p(x) = f_0 + f_1 x + \ldots + f_{l+1} x^{l+1} \in F[x]$, tenemos que $p(0) = f_0 = f(0)$ y además se puede probar que $p(x) = p(x-1) + g(x-1)$ para todo $x \in \mathbb{N}_0$. Para verlo, primero, observamos que:

$$\begin{aligned}
p(x) &= f_0 + \sum_{t=1}^{l+1} f_t x^t = f_0 + \sum_{t=1}^{l+1} \sum_{k=0}^{l+1-t} \frac{c_{t+k-1}}{t+k} B_k \binom{t+k}{k} x^t \\
&= f_0 + \sum_{j=0}^{l} \sum_{k=0}^{j} \frac{c_j}{j+1} B_k \binom{j+1}{k} x^{j-k+1}, \text{ donde } j = t+k-1 \\
&= f_0 + \sum_{j=0}^{l} c_j \left(\frac{1}{j+1} \sum_{k=0}^{j} B_k \binom{j+1}{k} x^{j-k+1} \right) = f_0 + \sum_{j=0}^{l} c_j \sum_{i=1}^{x-1} i^j, \text{ aquí usamos 3.4} \\
&= f_0 + \sum_{i=1}^{x-1} \sum_{j=0}^{l} c_j i^j = f_0 + \sum_{i=1}^{x-1} g(i)
\end{aligned}$$

En consecuencia, $p(x-1) = f_0 + \sum_{i=1}^{x-2} g(i)$ y entonces $p(x) - p(x-1) = g(x-1)$. □

Ahora, ya podemos probar Ω_n para $m \geq 0$. La propiedad claramente se cumple en G/G_1. Supongamos que se cumple para G/G_{n-1} y probémoslo para G. Teniendo en cuenta que $G_{n-1} \leq Z(G)$, es decir, que u_n es central, los ω_i^m de

$$(u_1^{\alpha_1} \cdots u_n^{\alpha_n})^m = u_1^{\omega_1^m} \cdots u_{n-1}^{\omega_{n-1}^m} u_n^{\omega_n^m}$$

son los mismos que aparecen en G/G_{n-1}, para $1 \leq i \leq n-1$. Por tanto, podemos suponer que son polinomios en m y en los $\alpha_1, \ldots, \alpha_{n-1}$ y solo nos queda verlo para ω_n^m.

Por otra parte, podemos expresar la exponenciación así:

$$\begin{aligned}
(u_1^{\alpha_1} \cdots u_n^{\alpha_n})^m &= (u_1^{\alpha_1} \cdots u_n^{\alpha_n})^{m-1} u_1^{\alpha_1} \cdots u_n^{\alpha_n} \\
&= u_1^{\omega_1^{m-1}} \cdots u_n^{\omega_n^{m-1}} u_1^{\alpha_1} \cdots u_n^{\alpha_n} = u_1^{\gamma_1} \cdots u_n^{\gamma_n},
\end{aligned}$$

donde los γ_i son polinomios en las variables ω_j^{m-1} y α_j. Así que $\omega_n^m = \gamma_n(\omega^{m-1}, \alpha)$, que es un polinomio en las variables α_j y ω_j^{m-1}, y, por inducción en m, los ω_i^{m-1} son polinomios en $m-1$ y α_j.

Teniendo en cuenta de nuevo que u_n es central, se deduce:

$$\omega_n^m = \gamma_n(\omega^{m-1}, \alpha) = \omega_{n-1}^{m-1} + h(\omega^{m-1}, \alpha)$$

Como γ_n y ω_n^{m-1} son polinomios en los α_i y en m, h también lo es. Si consideramos los α_i como constantes, la expresión anterior queda así:

$$\omega_n^m = \omega_n^{m-1} + h(m-1)$$

y, aplicando el lema que acabamos de probar, ω_n^m también es un polinomio en m. Y, volviendo a considerar los α_i como variables, ω_n^m es un polinomio en α_i y m.

Por otra parte, si llamamos $a_1 = u_2^{\alpha_2} \cdots u_n^{\alpha_n}$, a_1 está en G_1, que es un grupo nilpotente de longitud $n-1$, y podemos aplicar Ω_{n-1} para obtener $a_1^{-1} = u_2^{\nu_2} \cdots u_n^{\nu_n}$, con ν_i polinomios en $\alpha_2, \ldots, \alpha_n$. Ahora, usando Γ_n:

$$a^{-1} = a_1^{-1} u_1^{-\alpha_1} = u_1^{\delta_1} \cdots u_n^{\delta_n}, \text{ donde } \delta_i \text{ son polinomios en } \alpha_1, \cdots, \alpha_n.$$

Con esto podemos probar Ω_n para $m < 0$:

$$a^m = (a^{-1})^{-m} = (u_1^{\delta_1} \cdots u_n^{\delta_n})^{-m} = u_1^{\omega_1} \cdots u_n^{\omega_n}, \text{ donde hemos usado } \Omega_n \text{ para } -m > 0.$$

□

Observemos que los coeficientes de estos polinomios deben estar en $\mathbb{Q}$ y, como F tiene característica cero, $\mathbb{Q} \subseteq F$, luego en particular los coeficientes están en F. Que G^F sea el grupo de los productos formales u^α quiere decir que el producto y la exponenciación se definen con los mismos polinomios que en G.

Antes de pasar a la prueba de que G^F es grupo, introducimos el siguiente lema:

Lema 3.5. *Sean p, q dos polinomios en k variables y coeficientes en F. Si $p(u) = q(u)$ para todo $u \in \mathbb{Z}^k$, entonces p y q son el mismo polinomio.*

Demostración. Si $k = 1$, esto es obvio porque estaríamos diciendo que $p - q$, un polinomio en una variable, tiene infinitas soluciones. Ahora supongamos que es cierto para $i < k$. Podemos escribir los polinomios p y q así:

$$p = x_k^r h_r + x_k^{r-1} h_{r-1} + \cdots + x_k h_1 + h_0$$
$$q = x_k^s g_s + x_k^{s-1} g_{s-1} + \cdots + x_k g_1 + g_0,$$

donde h_i, g_j son polinomios en las $n-1$ variables $x_1, \ldots, x_{k-1}$. Para cualquier combinación de $n-1$ enteros $a_1, \ldots, a_{k-1}$, se cumple que $p(a_1, \ldots, a_{k-1}, x_k) = q(a_1, \ldots, a_{k-1}, x_k)$ para todo $x_k \in \mathbb{Z}$. Es decir, fijando esas $n-1$ variables tenemos $p = q$, viéndolo como dos polinomios en una sola variable. Luego $r = s$ y $h_i = g_i$ cuando se evaluan en $\mathbb{Z}^{k-1}$. Por la hipótesis de inducción, los polinomios h_i y g_i son el mismo para todo $i = 0, \ldots, r$ y, por tanto, $p = q$. □

Con estos dos lemas podemos ver que G^F es de hecho un grupo. La ley asociativa se cumple en G, es decir, $(u^\alpha u^\beta)u^\varepsilon = (ab)c = a(bc) = u^\alpha (u^\beta u^\varepsilon)$. Entonces, usando el lema 3.3, para todo i se cumple:

$$\gamma_i(\gamma_1(\alpha_1, \beta_1), \ldots, \gamma_i(\alpha_1, \ldots, \alpha_i, \beta_1, \ldots, \beta_i), \varepsilon_1, \ldots, \varepsilon_i) = \gamma_i(\alpha_1, \ldots, \alpha_i, \gamma_1(\beta_1, \varepsilon_1), \ldots, \gamma_i(\beta_1, \ldots, \beta_i, \varepsilon_1, \ldots, \varepsilon_i)),$$

donde $\alpha_j, \beta_j, \varepsilon_j \in \mathbb{Z}$. Estas identidades polinómicas se cumplen para todo conjunto de variables enteras, luego se cumplen en F (lema 3.5), lo que prueba la asociatividad en G^F. El elemento identidad de G, $1 = u^0$, también lo es en G^F aplicando un razonamiento parecido al anterior. De hecho, para todo $a = u^\alpha \in G^F$, $m \in F$ y todo i, se cumple:

$$\gamma_i(\alpha_1, \ldots, \alpha_i, 0, \ldots, 0) = \gamma_i(0, \ldots, 0, \alpha_1, \ldots, \alpha_i) = \alpha_i,\ \omega_i^{(m)}(0, \ldots, 0) = 0. \tag{3.5}$$

Por último, para todo $a = u^\alpha \in G^F$, su inverso es $a^{-1} = u_n^{-\alpha_n} \cdots u_1^{-\alpha_n}$ y claramente está en G^F. Los exponentes satisfacen:

$$\gamma_i(\alpha_1, \ldots, \alpha_i, \varepsilon_1, \ldots, \varepsilon_i) = 0. \tag{3.6}$$

Además, para cada $i = 0, 1, \ldots, n$, definimos:

$$G_i^F = \{u^\alpha | \alpha_1 = \alpha_2 = \cdots = \alpha_i = 0\}.$$

Claramente, G_i^F es un subgrupo de G^F: contiene la identidad y, si u^α está en G_i^F, su inverso $u^{-\alpha}$ también (usando la expresión 3.5 y 3.6, obtenemos $\varepsilon_j = 0$ para todo $j \leq i$). Obtenemos una serie de G^F:

$$G^F = G_0^F > G_1^F > \cdots > G_n^F = 1.$$

Probemos que esta serie es central. Veamos que G_i^F/G_{i+1}^F está en el centro de G^F/G_{i+1}^F, es decir, que $[u^\alpha, u^\beta] \in G_{i+1}^F$ para todo $u^\alpha \in G_i^F$ y todo $u^\beta \in G^F$. Tenemos que probar que $u^{-\alpha}u^{-\beta}u^\alpha u^\beta \in G_{i+1}^F$. Para exponentes enteros, esto se cumple porque G_i/G_{i+1} está en el centro de G/G_{i+1}. Así que podemos aplicar de nuevo el lema 3.5 y concluir que esto se cumple también en G^F. Esto implica que $G_i^F \triangleleft G^F$. Por tanto, el grupo G^F es nilpotente.

Ahora, para cada $i = 1, \ldots, n$, vamos a definir una función entre el cociente G_{i-1}/G_i y el grupo aditivo de F:

$$\begin{aligned} \phi_i : G_{i-1}^F/G_i^F &\to F \\ u^\alpha G_i^F &\mapsto \alpha_i, \end{aligned}$$

donde $u^\alpha = u_1^{\alpha_1} \cdots u_n^{\alpha_n} \in G_{i-1}^F$, por tanto, $\alpha_1 = \alpha_2 = \cdots = \alpha_{i-1} = 0$. Como hemos tomado representantes en G_{i-1}^F/G_i^F, tenemos que ver que la función esté bien definida:

$$u_i^{\alpha_i} G_i^F = u^\alpha G_i^F = u^\beta G_i^F = u_i^{\beta_i} G_i^F \Leftrightarrow u_i^{-\beta_i} u_i^{\alpha_i} \in G_i^F \Leftrightarrow \alpha_i = \beta_i.$$

Y es obvio que ϕ_i es un isomorfismo, luego $G_{i-1}^F/G_i^F \cong F$, para cada $i = 1, \ldots, n$.

Veamos que, además, G^F tiene la misma clase de nilpotencia, m, que G. Llamemos m' a la clase de nilpotencia de G^F. Tenemos que $G \leq G^F$ y entonces $m \leq m'$. Para probar la otra desigualdad, vamos a ver que si consideramos la complección de Mal'cev de la serie central ascendente de G, obtenemos una serie central de G^F. Tenemos $1 = Z_0(G) \triangleleft Z_1(G) = Z(G) \triangleleft \cdots \triangleleft Z_m(G) = G$ y sabemos que son finitamente generados porque G lo es. En particular, teniendo en cuenta cómo refinamos esta serie para obtener la serie central con cocientes cíclicos $1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$, cada $Z_i(G)$ es finitamente generado por un subconjunto de $\{u_1, \ldots, u_n\}$. Para no complicar la notación, decimos que $Z_i(G)$ es finitamente generado por $\{a_{i,1}, \ldots, a_{i,n_i}\}$ y definimos

$$Z_i(G)^F := \{a_i^\alpha = a_{i,1}^{\alpha_1} \cdots a_{i,n_i}^{\alpha_{n,i}} \mid \alpha_i \in F\}.$$

Claramente, $Z_n(G)^F = G^F$. Queremos ver que $Z_i(G)^F/Z_{i-1}(G)^F$ es central en $G^F/Z_{i-1}(G)^F$, es decir, que

$$[a_i^\alpha, u^\beta] \in Z_{i-1}(G)^F \text{ para todo } a_i^\alpha \in Z_i(G)^F \text{ y todo } u^\beta \in G^F.$$

Pero esta relación se cumple para exponentes enteros y, como cada $a_{i,j}$ denota uno de los generadores u_k de G, esto implica que los polinomios de Hall satisfacen ciertas identidades cuando se evalúan en variables enteras. Por tanto, siempre satisfacen esas identidades y se cumple lo que queremos. La serie $1 = Z_0(G)^F \triangleleft Z_1(G)^F \triangleleft \ldots \triangleleft Z_m(G)^F = G^F$ es central y, en consecuencia, la clase de nilpotencia de G^F debe ser menor o igual que m.

Por último, vamos a considerar el caso en el que $F = \mathbb{Q}$ y vamos a probar que $G^\mathbb{Q}$ cumple las condiciones del Teorema de Mal'cev.

Empezamos probando que todo elemento $a \in G^\mathbb{Q}$ tiene una potencia entera positiva en G. Si $a \in G_{n-1}^\mathbb{Q}$, existe $\alpha_n \in \mathbb{Q}$ tal que $a = u_n^{\alpha_n}$, luego existe un entero $k > 0$ tal que $k\alpha_n \in \mathbb{Z}$. Por tanto, $a^k = u_n^{k\alpha_n}$ está en G_{n-1}, luego en G. Suponemos ahora que esto es cierto para $i < n$ y sea $a \in G^\mathbb{Q}$, entonces $aG_{n-1}^\mathbb{Q}$ está en $G^\mathbb{Q}/G_{n-1}^\mathbb{Q}$, que es nilpotente (proposición 1.7) y de longitud menor que n. Por inducción, existe $k_1 \in \mathbb{Z}_{>0}$ tal que $a^{k_1} G_{n-1}^\mathbb{Q} \in G/G_{n-1}^\mathbb{Q}$. Por tanto, $a^{k_1} = bu_n^\alpha$ para cierto $\alpha \in \mathbb{Q}$ y $b \in G$. Además, existe $k_2 > 0$ entero tal que $\alpha k_2 \in \mathbb{Z}$. Por tanto:

$$a^{k_1 k_2} = (bu_n^\alpha)^{k_2} = b^{k_2} u_n^{\alpha k_2},$$

donde en la última igualdad aplicamos que $G_{n-1}^\mathbb{Q}$ es central en $G^\mathbb{Q}$. Por tanto, para $k = k_1 k_2 > 0$ tenemos que $a^k \in G$.

Veamos ahora que $G^{\mathbb{Q}}$ es radicable, es decir, para todo $b \in G^{\mathbb{Q}}$ y todo k, existe $a \in G^{\mathbb{Q}}$ tal que $a^k = b$. Si $b \in G^{\mathbb{Q}}_{n-1}$, entonces $b = u_n^{\beta}$. Si tomamos $a = u_n^{\frac{\beta}{k}}$, tenemos que $a^k = b$. Ahora, suponemos que esto se cumple para todo $i < n$. Sea $b \in G^{\mathbb{Q}}$. Como hicimos antes, $bG^{\mathbb{Q}}_{n-1}$ está en $G^{\mathbb{Q}}/G^{\mathbb{Q}}_{n-1}$ y podemos aplicar la hipótesis de inducción: existe $cG^{\mathbb{Q}}_{n-1} \in G^{\mathbb{Q}}/G^{\mathbb{Q}}_{n-1}$ tal que $bG^{\mathbb{Q}}_{n-1} = (cG^{\mathbb{Q}}_{n-1})^k = c^k G^{\mathbb{Q}}_{n-1}$. Por tanto, $b = c^k u_n^{\beta}$ para cierto $\beta \in \mathbb{Q}$. Si tomamos $a = cu_n^{\alpha}$ con $\alpha = \frac{\beta}{k}$, podemos ver que:

$$a^k = (cu_n^{\alpha})^k = c^k u_n^{\alpha k} = c^k u_n^{\beta} = b,$$

donde de nuevo usamos que $G^{\mathbb{Q}}_{n-1}$ es central en $G^{\mathbb{Q}}$.

Veamos que, además, la extracción de raíces en $G^{\mathbb{Q}}$ es única, equivalentemente, $G^{\mathbb{Q}}$ es libre de torsión. Como vimos antes $G^{\mathbb{Q}}_{n-1} \cong \mathbb{Q}$, luego es libre de torsión. De igual forma lo es $G^{\mathbb{Q}}_{n-2}/G^{\mathbb{Q}}_{n-1}$. Por inducción, suponemos entonces que $G^{\mathbb{Q}}/G^{\mathbb{Q}}_{n-1}$ es libre de torsión. Luego, si $(u^{\alpha})^k = 1$ para $u^{\alpha} \in G$ y k no nulo, tenemos que $(u^{\alpha}G_{n-1})^k = 1$ y, por la hipótesis, $u^{\alpha}G_{n-1} = 1$. Es decir, $u^{\alpha} \in G_{n-1}$ y, en consecuencia, $u^{\alpha} = 1$.

Queda demostrado que $G^{\mathbb{Q}}$ es una complección de Mal'cev del grupo G y, en consecuencia, la existencia de tal grupo.

3.2. Unicidad de la complección

En esta sección probaremos que esta complección es única salvo isomorfismo.

Sea $\theta : G \to H$ otra inclusión de G en un grupo H que es nilpotente, libre de torsión y radicable. Definimos la función $\theta^* : G^{\mathbb{Q}} \to H$ tal que, si $u^{\alpha} = u_1^{\alpha_1} \cdots u_n^{\alpha_n}$, $\alpha_i \in \mathbb{Q}$, entonces:

$$(u^{\alpha})^{\theta^*} = (u^{\theta})^{\alpha} = (u_1^{\theta})^{\alpha_1} \cdots (u_n^{\theta})^{\alpha_n}.$$

Como H es radicable y libre de torsión, si tenemos un elemento $h \in H$ y $\frac{p}{q} \in \mathbb{Q}$, existe un único $g \in H$ con $g^q = h$. Por tanto, tiene sentido poner $h^{\frac{p}{q}} = g^p$. Esto implica que θ^* está bien definida.

Para probar que θ^* es homomorfismo, necesitamos el siguiente resultado.

Lema 3.6. *Sea H un grupo radicable, nilpotente y libre de torsión. Sean $a, b \in H$ con $[a,b] = 1$. Entonces para todo $\alpha, \beta \in \mathbb{Q}$ se tiene $[a^{\alpha}, b^{\beta}] = 1$.*

Demostración. Sea $\alpha = \frac{p}{q}$ $(p, q \in \mathbb{Z})$ y $a_1 = a^{\frac{1}{q}}$, es decir, a_1 es el único elemento de H tal que $a_1^q = a$. Que $[a,b] = 1$ equivale a que $a^b = a$. Entonces:

$$(a_1^b)^q = (a_1^q)^b = a^b = a$$

y, por unicidad, $a_1^b = a_1$. Si elevamos a p, tenemos:

$$(a^{\alpha})^b = (a_1^p)^b = (a_1^b)^p = a_1^p = a^{\alpha}.$$

Luego, $[a^{\alpha}, b] = 1$.

El mismo razonamiento aplicado a b, β implica que $[a^{\alpha}, b^{\beta}] = 1$. □

Ahora sea L el subgrupo de H generado por

$$\{(u_j^{\theta})^{\alpha_j} \mid \alpha_j \in \mathbb{Q}, \text{ con } 1 \leq j \leq n\}$$

y ponemos también L_i para el subgrupo generado por

$$\{(u_j^{\theta})^{\alpha_j} \mid \alpha_j \in \mathbb{Q}, \text{ con } i < j \leq n\}.$$

Como u_n es central en G y θ es homorfismo, $[u_n^{\theta}, u_j^{\theta}] = 1$ para todo $1 \leq j \leq n$. Esto junto con el lema 3.6 implica que L_{n-1} es central en L, en particular, es normal. Razonando por inducción, suponemos que

$L_{i+1} \trianglelefteq L$. Entonces como G_i/G_{i+1} es central en G/G_{i+1}, el lema 3.6 implica que L_i/L_{i+1} es central en L/L_{i+1} y, en particular, $L_i \trianglelefteq L$.

Tenemos entonces una serie central

$$1 = L_n \triangleleft L_{n-1} \triangleleft \cdots \triangleleft L_{i+1} \triangleleft L_i \triangleleft \cdots L_0 = L$$

con $L_{i-1}/L_i = \{u_i^\alpha L_i \mid \alpha \in \mathbb{Q}\}$ y en estas condiciones se puede repetir la demostración del lema 3.3. Esto no se podía asegurar para H, pero solo nos interesan los elementos de L.

Por tanto, en el subgrupo L también hay unos polinomios, llamémosles δ_i, que determinan cómo es el producto en términos de los u_i^θ. Como θ es un homomorfismo de grupos, estos polinomios coinciden con los correspondientes polinomios de G cuando las entradas son enteros:

$$(u^\theta)^\delta = (u^\theta)^\alpha (u^\theta)^\beta = (u^\alpha)^\theta (u^\beta)^\theta = (u^\alpha u^\beta)^\theta = (u^\gamma)^\theta,$$

es decir, $\delta_i(\alpha_1, \ldots, \alpha_i, \beta_1, \ldots, \beta_i) = \gamma_i(\alpha_1, \ldots, \alpha_i, \beta_1, \ldots, \beta_i)$ para todo $\alpha_j, \beta_j \in \mathbb{Z}$.

Ahora, para probar que θ^* es homomorfismo, queremos ver que:

$$(u^\alpha)^{\theta^*} (u^\beta)^{\theta^*} = (u^\alpha u^\beta)^{\theta^*} = (u^\gamma)^{\theta^*}, \text{ es decir,}$$
$$(u_1^\theta)^{\alpha_1} \cdots (u_n^\theta)^{\alpha_n} (u_1^\theta)^{\beta_1} \cdots (u_n^\theta)^{\beta_n} = (u_1^\theta)^{\gamma_1} \cdots (u_n^\theta)^{\gamma_n}$$

donde todos los exponentes son racionales y los polinomios γ_i son los mismos que los que definen el producto en G. Hemos visto que estos polinomios satisfacen esta identidad para exponentes enteros, luego, aplicando el lema 3.5, la satisfacen también para exponentes racionales. Por tanto, θ^* es homomorfismo de grupos.

Notemos que θ y θ^* coinciden en G. Como θ es una inclusión, $ker(\theta^*) \cap G = 1$. Ahora, tomamos $x \in ker(\theta^*) \leq G^{\mathbb{Q}}$, existe $k \in \mathbb{Z}_{>0}$ tal que $x^k \in G$. Entonces $x^k \in ker(\theta^*)$ por ser θ^* un homomorfismo. Pero entonces $x^k = 1$ y, como G es libre de torsión, $x = 1$. Por tanto, θ^* es inyectivo.

Para terminar, vamos a probar que, si H tiene la propiedad de que todo elemento tiene una potencia entera positiva en G^θ, entonces θ^* es suprayectivo. Ahora sea $h \in H$, entonces $h^k \in G^\theta$ para algún $k > 0$. Por tanto, $h^k \in (G^{\mathbb{Q}})^{\theta^*}$ y existe $g' \in G^{\mathbb{Q}}$ tal que $h^k = g'^{\theta^*}$. Como $G^{\mathbb{Q}}$ es radicable, existe $g \in G^{\mathbb{Q}}$ tal que $g^k = g'$ y, en consecuencia:

$$h^k = g'^{\theta^*} = (g^k)^{\theta^*} = (g^{\theta^*})^k$$

ya que θ^* es homomorfismo. Por lo tanto, la unicidad de la extracción de raíces implica $h = g^{\theta^*}$. Entonces $h \in (G^{\mathbb{Q}})^{\theta^*}$ y concluimos que $H = (G^{\mathbb{Q}})^{\theta^*}$.

Hemos probado que θ^* es un isomorfismo entre H y $G^{\mathbb{Q}}$. Con esto queda probada la unicidad de la complección de Mal'cev y en consecuencia el teorema.

3.3. Comentarios finales

Vamos a ver cómo el *Teorema de Mal'cev* se aplica en nuestro ejemplo de las matrices unitriangulares superiores.

Ejemplo 3.7. Si tenemos una matriz en el grupo G de Heisenberg:

$$B = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}, \text{ con } a', b', c' \in \mathbb{Z},$$

las fórmulas del ejemplo 1.10 implican que su potencia m-ésima ($m \in \mathbb{Z}$) es:

$$B^m = \begin{pmatrix} 1 & ma' & mb' + ma'c' \\ 0 & 1 & mc' \\ 0 & 0 & 1 \end{pmatrix}.$$

Por tanto, si tenemos $A \in G$ una matriz de la forma

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

y m entero, la ecuación $A = B^m$ no tendrá una solución $B \in G$ si m no divide a a. Por tanto, G no es radicable.

Sin embargo, G cumple las condiciones del Teorema de Mal'cev (3), es un grupo nilpotente y libre de torsión, luego tiene una cubierta radicable o complección. Definimos:

$$H = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a,b,c \in \mathbb{Q}\}.$$

Como vimos en (1.10), H es nilpotente de clase 2 y contiene a G. Si consideramos las matrices u_1, u_2, u_3 definidas en (1.10), vemos que para todo $a,b,c \in \mathbb{Q}$:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = u_1^a u_2^c u_3^b$$

De aquí, se deduce que H es la complección de Mal'cev de G.

Para concluir este trabajo hacemos un pequeño comentario sobre cómo este ejemplo puede ser genralizado.

Ejemplo 3.8. Vimos en el primer capítulo (1.10) que el grupo de Heisenberg estaba generado por tres matrices u_1, u_2, u_3 tales que los conmutadores entre ellas satisfacían: $[u_1,u_2] = u_3$, $[u_2,u_3] = 1$ y $[u_1,u_3] = 1$. Sea t entero, podemos ahora considerar otro grupo $G(t)$ generado también por tres elementos $\{u_1,u_2,u_3\}$ de orden infinito, que satisfacen: $[u_1,u_2] = u_3^t$, $[u_2,u_3] = 1$ y $[u_1,u_3] = 1$. Como hicimos para G, podemos encontrar una serie central de $G(t)$:

$$1 \lhd \langle u_3 \rangle \lhd \langle u_3, u_2 \rangle \lhd G(t),$$

donde los cocientes son cíclicos infinitos.

¿Cómo serán los polinomios de Hall en este grupo? Podemos calcularlos, como hicimos en G, usando las relaciones

$$u_1u_2 = u_2u_1u_3^t \qquad u_2u_3 = u_3u_2 \qquad u_1u_3 = u_3u_1.$$

Entonces:

$$u_1^{\alpha_1}u_2^{\alpha_2}u_3^{\alpha_3}u_1^{\beta_1}u_2^{\beta_2}u_3^{\beta_3} = u_1^{\alpha_1}u_2^{\alpha_2}u_1^{\beta_1}u_2^{\beta_2}u_3^{\alpha_3}u_3^{\beta_3} = u_1^{\alpha_1+\beta_1}u_2^{\alpha_2+\beta_2}u_3^{\alpha_3+\beta_3-t\alpha_2\beta_1},$$

con $\alpha_j, \beta_j \in \mathbb{Z}$ y donde en la última igualdad estamos aplicando:

$$u_2^{\alpha_2}u_1^{\beta_1} = \underbrace{u_2\cdots u_2}_{\alpha_2}\underbrace{u_1\cdots u_1}_{\beta_1} = \underbrace{u_2\cdots u_2}_{\alpha_2-1}u_1u_2u_3^{-t}\underbrace{u_1\cdots u_1}_{\beta_1-1} = \underbrace{u_2\cdots u_2}_{\alpha_2-1}u_1u_2\underbrace{u_1\cdots u_1}_{\beta_1-1}u_3^{-t}$$

y esto se repite β_1 veces con cada u_2, es decir, un total de $\alpha_2\beta_1$ veces.

Y, análogamente, obtenemos:

$$(u_1^{\alpha_1}u_2^{\alpha_2}u_3^{\alpha_3})^{-1} = u_1^{-\alpha_1}u_2^{-\alpha_2}u_3^{-\alpha_3-t\alpha_1\alpha_2}.$$

Usando estos polinomios, como hicimos en la prueba del *Teorema de Mal'cev* (3.3), definiríamos la complección de Mal'cev de $G(t)$, $G(t)^{\mathbb{Q}}$.

Esto se puede generalizar aun más. Sea $n > 0$ entero y $t = (t_{i,j,k} \mid 1 \leq i < j < k \leq n) \in \mathbb{Z}^{\binom{n}{3}}$. Usando este valor podemos definir un grupo, al que llamamos $G(t)$, con n generadores, $u_1, \ldots, u_n$, que satisfacen:

$$[u_i, u_j] = u_{j+1}^{t_{i,j,j+1}} \cdots u_n^{t_{i,j,n}}.$$

Este grupo será nilpotente con una serie central de longitud n:

$$G(t) = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n+1} = 1$$

con cocientes consecutivos cíclicos infinitos. De hecho, la longitud de esta serie es exactamente la longitud de Hirsch de $G(t)$.

Se puede encontrar más información sobre estos grupos en el artículo citado en la bibliografía [3], donde además construyen un algoritmo para calcular los polinomios de Hall en función de los $t's$ anteriores y este ha sido implementado en GAP (sistema de cálculo simbólico en grupos).

El interés de los polinomios de Hall es que proporcionan un algoritmo eficiente para multiplicar en grupos nilpotentes libres de torsión. Saber cómo se comporta la multiplicación en un grupo nilpotente tiene una gran utilidad en criptografía, ya que estos grupos se han propuesto como plataforma de diversos protocolos criptográficos (como se ve en el artículo [5]) y para implementarlos es útil tener un algoritmo eficiente para multiplicar.

Bibliografía

[1] JOHN C. LENNOX Y DEREK J.S. ROBINSON, *The Theory of Infinite Soluble Groups*, Oxford University Press, 2004.

[2] DANIEL SEGAL, *Polycyclic Groups (Cambridge Tracts in Mathematics, pp. I-VI)*, Cambridge University Press, 1983.

[3] ALEXANDER CANT Y BETTINA EICK, *Polynomials describing the multiplication in finitely generated torsion-free nilpotent groups*, Journal of Symbolic Computation, Elsevier, 2018

[4] WENHAO CHEN, DAZHENG ZHANG, Y YUTENG ZOU, *Complex numbers and its discovery history*, Highlights in Science, Engineering and Technology (Volume 38, pag. 168-173), 2023

[5] DELARAM KAHROBAEI, ANTONIO TORTORA, MARIA TOTA, *A Closer Look at the Multilinear Cryptography using Nilpotent Groups*, International Journal of Computer Mathematics: Computer Systems Theory (Volume 7, Number 1, pag. 63-67), 2022