Teoría de Grupos
y
Álgebras de Lie

Belén Citoler Berdala

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Conchita Martínez Pérez
26 de Noviembre de 2018

Prólogo

En este trabajo se presentan dos estructuras que son los grupos y las álgebras de Lie. Aparentemente diferentes por definición, cuando se comienza a profundizar en ellas, se observa que disponen de similares resultados y propiedades, por lo que resulta natural preguntarse si existe alguna forma directa de relacionarlas.

La manera usual es mediante grupos de Lie. Un *grupo de Lie* es una variedad diferencial real que es también un grupo cuya operación e inversión son funciones diferenciables. Además puede ser una variedad diferencial compleja, en ese caso las funciones de la operación y su inversa deben ser analíticas.

Muchos problemas de álgebras de Lie se pueden transformar en cuestiones de grupos de Lie [6] y surge la idea de una relación entre álgebras y grupos de Lie, efectivamente se pueden asociar álgebras de Lie a grupos de Lie.

Sin embargo, en este trabajo trataremos las siguientes relaciones: el *álgebra de Lie asociado a un grupo* y la *Correspondencia de Mal'cev.*

Resumen

Group theory is applied in every part of mathematics and in others sciences like physics. Also, Lie algebras are of central importance and play an important role in modern physics.

The aim of this project is present an introduction to both the theory of groups and theory of Lie algebras, and also to the interactions between them. We will define the notions of solvable and nilpotent groups and central and derived series. Then, we will consider the analogous of these notions in the theory of Lie algebras and see many similaries between them. Finally, we will be able to associate a Lie algebra to a group and show a correspondence that can be used to transfer information between these two structures. Next, we describe more in detail the content of each chapter.

In Chapter 1, we introduce some basic definitions as the notions of abelian groups, normal groups, quotient group or free group. In addition, we will see commutators of a group which can be seen as an operation between two elements of a group,

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

and also we will see the commutator subgroups. The commutator subgroup of a group with itself, $[G,G]$, can be used to measure how far is the group from being commutative. We will see useful properties of commutators, as *Hall-Witt Identity* or *Three Subgroups' Lemma*.

All of the propositions and theorems we deal with, help us to know if these groups are nilpotent and/or solvable. We will see a lot of examples that we are going to develop and apply some of properties and theorems studied. Some examples that we will show are:

- *Dihedric group*, we will show that it is solvable but not nilpotent.
- Square matrices of size $n \times n$. Let R be $\mathbb{Z}$ or a field K, we denote by $T_n(R)$ to upper triangular matrices group, by $UT_n(R)$ unitriangular matrices group and by $D_n(R)$ to diagonal matrices group, all of them with elements in R. We will see that $T_n(R)$ is *semidirect product* of the group of $UT_n(R)$ and $D_n(R)$. This example together with the next one demonstrate that $T_n(R)$ is solvable.
- Let R be $\mathbb{Z}$ or a field K, we will see that $UT_n(R)$ is nilpotent and solvable whatever dimension. The fact that n is arbitrary makes the computation more complicated. In fact, in chapter 1 we consider the case $n = 3$ only and the general case will be proven in chapter 3.

Then, in chapter 2 we will focus on Lie algebras. The main advantage of Lie algebras over groups is that they are linear. On the other hand, groups can be studied through their actions on spaces and this can be used to prove statements that can be more difficult for Lie algebras. A Lie algebra is an algebra with an intern binary operation which is bilinear but not associative. Very often, one considers Lie algebras over a field K, which are vector spaces. Though less general, these Lie algebras are easier to manipulate.

Many definitions and properties about Lie algebras are analogous to definitions in groups but with some differences. We will define commutators, homomorphisms... and we will see that like we have

subgroups in group theory, we have subalgebras in Lie algebras theory. Also, the notion of normal subgroup in group theory corresponds to the notion of ideal in the theory of Lie algebras. We will define quotient Lie algebras. We also should take associativity into account. Some calculations are complicated in Lie algebras because they do not have the associative property. We will also define the notion of central and derived series and also of solvable and nilpotent Lie algebras (and of nilpotency class). Furthermore, we will define graded Lie algebra.

As an important example, we have the Lie algebra of square upper triangular matrices of size $n \times n$ with zeros in main diagonal and whose elements belong to a commutative ring. These matrices are called *null-triangular* and denoted by nt_n. We will see that this Lie algebra is nilpotent, its nilpotent class $n-1$. Also we will see that it is a graded Lie algebra.

Because of the number of similarities of the properties and behaviour of these structures, it is natural to think that one can relate them in a more precise way. We could think about some kind of association between them in order to take the best properties of each one. So, in Chapter 3, we will see two different ways of match these structures.

First one is the *Lie algebra associated to a group*. We are going to use a series defined previously, that is the lower central series.

Definition. Let G a group and $\gamma_i(G)$ the elements of its lower central series, we define the *associated $\mathbb{Z}$-Lie algebra of G* as follows

$$L(G) = \bigoplus_{i=1}^{\infty}(\gamma_i(G)/\gamma_{i+1}(G)),$$

with

$$[g+\gamma_i(G), h+\gamma_j(G)]_{L(G)} = [g,h]_G + \gamma_{i+j}(G)$$

We will see that the Lie algebra associated to the group of unitriangular matrices with entries in $\mathbb{Z}$ is the Lie algebra of null-triangular matrices in $\mathbb{Q}$, $nt_n(\mathbb{Q})$.

For an abelian group A, we denote by $A \otimes \mathbb{Q}$ the $\mathbb{Q}$-vector space obtained by extending scalars in A (we define this construction in chapter 3). Also we will define the $\mathbb{Q}$*-Lie algebra* as

$$L_{\mathbb{Q}}(G) = \bigoplus_{i=1}^{\infty}((\gamma_i(G)/\gamma_{i+1}(G)) \otimes \mathbb{Q})$$

considering Lie bracket before and where $\{\gamma_i(G)\}_{\mathbb{N}}$ means the lower central series of G.

The second way to relate groups and Lie algebras that we are going to see is by *Mal'Cev Correspondence*. That is a bijective application between $UT_n(\mathbb{Q})$ and $nt_n(\mathbb{Q})$. In addition, this correspondence can be used for many groups, not only $UT_n(\mathbb{Q})$ because every nilpotent and finitely generated group is isomorphic to a subgrop of $UT_n(\mathbb{Z})$. Unfortunately, the proof of this result is out of the reach of this project so we state it without proof. In this way, finitely generated nilpotent groups are isomophic to a subgroup of $UT_n(\mathbb{Q})$ and we could calculate the image of that subgroup in order to obtain the Lie subalgebra, then we work with that algebra, see its properties and take advantages of the Lie algebras. As *Mal'Cev Correspondence* is bijective, we could come back and we will see it better in an example.

Índice general

Capítulo 1

Teoría de Grupos

En este capítulo veremos algunas definiciones básicas relacionadas con el concepto de grupo, veremos también nociones como la de conmutadores, subgrupo derivado, series y diversas propiedades que nos van a servir para llegar a resultados muy interesantes. Este capítulo está basado en [2], [5] y [4].

1.1. Grupos y conmutadores

Definición 1.1. Sea G un conjunto no vacío y $*$ una operación asociativa interna de $G \times G$ en G. Diremos que $(G,*)$ es un *grupo* si existe $e \in G$ tal que $g * e = e * g = g$, para todo $g \in G$ (elemento neutro) y para cada $g \in G$ existe $h \in G$ tal que $g * h = h * g = e$ (todo elemento de G posee inverso en G).

Observación 1.2. Una consecuencia sencilla de esta definición es que el neutro es único y también lo es el inverso de un elemento. A partir de ahora vamos a denotar $g * h$ como gh por convenio.

Definición 1.3. Sea G un grupo,

- decimos que es *abeliano* si $gh = hg$ para todo $g,h \in G$.
- Sea H un subconjunto de elementos de G no vacío tal que $gh \in H$ y $g^{-1} \in H$ para todo $g,h \in H$, entonces H se denomina *subgrupo* y se denota $H \leqslant G$.
- Si H es un subgrupo de G, llamamos *coclase a izquierda (respectivamente a derecha)* a $xH = \{xh | h \in H\}$ (respectivamente $Hx = \{hx | h \in H\}$). Si no se especifica nada, se entiende que es a izquierda.
- Sea $N \leqslant G$, decimos que N es *normal* si para todo $x \in G$ se tiene $x^{-1}gx \in N$ $\forall g \in N$, se denota como $N \trianglelefteq G$. En este caso, las coclases a izquierda coinciden con las coclases a derecha y en el conjunto de las coclases se puede definir una estructura de grupo por $xN \cdot gN := xgN$. Este grupo se dice *grupo cociente* y se denota G/N.
- Un subgrupo H de G se dice *central* si para todo $h \in H$ y todo $g \in G$ se tiene $gh = hg$. El centro de un grupo de G es
$$Z(G) = \{h \in G \mid gh = hg \text{ para todo } g \in G\}.$$
Es fácil probar que $Z(G)$ es subgrupo normal de G y que un subgrupo H es central en G si y sólo si $H \leq Z(G)$. Además se define el *centralizador* de un subgrupo H de G como
$$Z_G(H) = \{g \in G \mid gh = hg \text{ para todo } h \in H\}.$$
- Llamamos *orden de* G al número de elementos de G y se denota por $|G|$.
- Dado X un subconjunto de G, definimos el subgrupo generado por X, $\langle X \rangle$, como la intersección de todos los subgrupos de G que contienen a X. Notemos que este también es subgrupo ya que una intersección arbitraria de subgrupos es subgrupo.

- Sean G_1 y G_2 grupos. Se define un *homomorfismo* φ como una aplicación entre G_1 *y* G_2, $\varphi : G_1 \longrightarrow G_2$ tal que $\forall a, b \in G_1$ se tiene $\varphi(ab) = \varphi(a)\varphi(b)$.
- Si φ es un homomorfismo biyectivo, se dice que φ es un *isomorfismo*. En ese caso, G_1 *y* G_2 son *isomorfos* y se denota por $G_1 \cong G_2$. Si además $G_1 = G_2$, entonces se dice que φ es un *automorfismo*.

Ejemplo 1.4. Sea N subgrupo normal en G y $g \in G$. La aplicación

$$\begin{array}{ccc} N & \longrightarrow & N \\ n & \longmapsto & g^{-1}ng \end{array}$$

es un automorfismo de N.

Ejemplo 1.5. Consideremos el conjunto de todas las matrices cuadradas regulares de tamaño $n \times n$ con entradas en un cuerpo K, que se denota como $GL(n,K)$ y veamos que es un grupo con la multiplicación usual entre matrices como operación.
Para ello, tenemos que comprobar que cumple las condiciones de la definición. La matriz identidad $I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \in GL(n,K)$ es el elemento neutro de la multiplicación ya que $AI_n = I_nA = A$, $\forall A \in GL(n,K)$. Como todas las matrices de $GL(n,K)$ son regulares, para cada $A \in GL(n,K)$ existe $B \in GL(n,K)$ tal que $AB = I_n = BA$, luego tenemos la segunda condición de la definición.
Por lo tanto $GL(n,K)$ es grupo con la operación multiplicación usual entre matrices para todo $n \in \mathbb{N}$ y para todo cuerpo K.

Ejemplo 1.6. Dado un cuerpo K, también se puede considerar el grupo de las matrices diagonales con elementos en K,

$$D_n = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \middle| \, a_i \in K \right\}.$$

D_n es un grupo abeliano considerando la operación multiplicación ya que K es un cuerpo.

Presentamos a continuación un grupo de gran interés que vamos a desarrollar a lo largo de todo el trabajo.

Ejemplo 1.7. Sea $R = \mathbb{Z}$ o un cuerpo K, denotamos por $UT_n(R)$ al conjunto de las matrices triangulares superiores de tamaño $n \times n$ con unos en la diagonal, cuyos elementos están en R. A este conjunto también se le denomina como *matrices unitriangulares de tamaño* $n \times n$. Teniendo en cuenta que al multiplicar dos matrices unitriangulares se obtiene otra matriz unitriangular, se deduce que este conjunto es un grupo con la operación multiplicación usual entre matrices.

Definición 1.8. Sea $X = \{x_1,\ x_2, \ldots,\ x_n\}$ y $X^{-1} = \{x_1^{-1},\ x_2^{-1}, \ldots,\ x_n^{-1}\}$ conjuntos de símbolos. Llamamos *letras* a los elementos de $X \cup X^{-1}$. A las yuxtaposiciones de letras las llamamos *palabras*, incluyendo la palabra vacía.

Una palabra es *reducida* si no tiene subpalabras de la forma $x_ix_i^{-1}$ ó $x_i^{-1}x_i$. Una *reducción* consiste en eliminar subpalabras de esta forma.

El conjunto de palabras reducidas con la operación de yuxtaposición seguida de posibles reducciones es un grupo que se llama *grupo libre en* X y se denota por $F(X)$, el elemento neutro es la palabra vacía.

Sea $R \subseteq F(X)$. El grupo $G = \langle X|R\rangle$ se define como el cociente de $F(X)$ por el subgrupo normal generado por R, es decir, el menor subgrupo normal que contiene a los elementos de R. Una expresión de este tipo se dice una presentación del grupo G. Los elementos de X se dicen generadores y los de R relaciones. Intuitivamente, G es el menor grupo que contiene a los elementos de X en el que se cumplen las relaciones $r = 1$ para cada $r \in R$.

Ejemplo 1.9. [Grupo Diédrico] Sea G el grupo diédrico de 12 elementos. Hay varias formas de definirlo, todas ellas equivalentes. La primera sería considerar los movimientos del plano que fijan un hexágono regular, teniendo como operación la composición y como elemento neutro la identidad. También lo podemos ver mediante la siguiente presentación donde el elemento a corresponde a una simetría y el elemento b a un giro.

$$G = D_6 = \langle a,b \mid a^2 = b^6 = 1, aba = b^5 \rangle = \{1,a,b,b^2,b^3,b^4,b^5,ab,ab^2,ab^3,ab^4,ab^5\}.$$

Definición 1.10. Sea G un grupo y $x_1,x_2 \in G$. Llamamos *conmutador de* x_1 *y* x_2 a

$$[x_1,x_2] = x_1^{-1}x_2^{-1}x_1x_2.$$

De manera inductiva, el *conmutador de* $x_1,\ldots,x_n$ se define como $[x_1,\ldots,x_n] = [[x_1,\ldots,x_{n-1}],x_n]$, y se dice que es un conmutador de *peso* o *longitud* n.

Los conmutadores se utilizan a menudo en las presentaciones de grupos. A continuación podemos ver dos ejemplos cuya definición contiene conmutadores.

Ejemplo 1.11. Consideramos $G = \langle a,b,c | a^3 = b^3 = c^3 = 1, [a,b] = c, [a,c] = [b,c] = 1 \rangle$.
Se puede ver que G es isomorfo a $UT_3(\mathbb{Z}_3)$.

Ejemplo 1.12. Si consideramos el grupo del Ejemplo 1.11 sin las condiciones del orden de los elementos obtenemos $H = \langle a,b,c | [a,b] = c, [a,c] = [b,c] = 1 \rangle$ denominado *Grupo de Heisenberg*. Se puede probar que es isomorfo a $UT_3(\mathbb{Z})$.

Proposición 1.13. *Dados x,y,z elementos de un grupo tenemos:*

- $[x,y] = [y,x]^{-1}$
- $[x,y]^z = [x^z,y^z]$
- $[x,y^{-1}] = ([x,y]^{y^{-1}})^{-1}$
- $[xy,z] = [x,z][x,z,y][y,z]$
- $[x,y^{-1},z]^y \cdot [y,z^{-1},x]^z \cdot [z,x^{-1},y]^x = 1$ *(Identidad de Hall-Witt)*

Demostración. Las cuatro primeras propiedades son consecuencia directa de la definición,

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

$$[x^z,y^z] = z^{-1}x^{-1}zz^{-1}y^{-1}zz^{-1}xzz^{-1}yz = z^{-1}x^{-1}y^{-1}xyz = [x,y]^z.$$

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

$$[x,z][x,z,y][y,z] = x^{-1}z^{-1}xz[x^{-1}z^{-1}xz,y]y^{-1}z^{-1}yz =$$

$$= y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz = (xy)^{-1}z^{-1}xyz = [xy,z].$$

Para la última propiedad, calculemos el primer factor

$$[x,y^{-1},z]^y = y^{-1}[x,y^{-1}]^{-1}z^{-1}[x,y^{-1}]zy = y^{-1}(x^{-1}yxy^{-1})^{-1}z^{-1}x^{-1}yxy^{-1}zy = x^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zy.$$

De manera análoga obtenemos

$$[y,z^{-1},x]^z = y^{-1}z^{-1}yx^{-1}y^{-1}zyz^{-1}xz$$

y también
$$[z,x^{-1},y]^x = z^{-1}x^{-1}zy^{-1}z^{-1}xzx^{-1}yx.$$

Multiplicando los tres factores tenemos

$$[x,y^{-1},z]^y \cdot [y,z^{-1},x]^z \cdot [z,x^{-1},y]^x =$$
$$= x^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zyy^{-1}z^{-1}yx^{-1}y^{-1}zyz^{-1}xzz^{-1}x^{-1}zy^{-1}z^{-1}xzx^{-1}yx = 1.$$

□

Definición 1.14. Sea G un grupo y X_1, X_2 subgrupos de G. Definimos el *conmutador de los subgrupos X_1 y X_2* como
$$[X_1,X_2] = \langle [x_1,x_2] | x_1 \in X_1, x_2 \in X_2 \rangle.$$

Análogamente podemos definir $[X_1,\ldots,X_n] = \langle [x_1,\ldots,x_n] | x_i \in X_i \rangle$, siendo $X_1,\ldots,X_n$ subgrupos de G.

Sea M un conjunto. Diremos que un conmutador es un *conmutador simple* de elementos de M si es de la forma
$$[x_1,x_2,\ldots,x_n]$$
con los $x_i \in M$. Notemos que un conmutador de la forma $[x_1x_2,x_3]$ con $x_1,x_2,x_3 \in M$ no es simple a menos que x_1x_2 esté en M.

En el caso en el que $X_1 = X_2 = G$ ponemos $G' = [G,G]$. Si G es abeliano, $G' = 1$. Por tanto, el tamaño de G' nos puede dar una idea de lo lejos que está un grupo de ser abeliano.

Observación 1.15. Notemos que $[X_1,X_2]$ no contiene solo todos los conmutadores de elementos de cada X_1 y X_2, sino también los productos de esos conmutadores. A menudo el producto de dos conmutadores se puede escribir como un solo conmutador, pero se puede probar que no siempre es así, además el grupo finito de menor orden en el que existen dos conmutadores cuyo producto no es un conmutador tiene orden 96. Esto fue probado por el matemático Robert Guralnick [1].

Lema 1.16 (Lema de los Tres Subgrupos)**.** *Sean G un grupo, A,B,C subgrupos de G y N un subgrupo normal en G. Si $[[A,B],C] \leq N$ y $[[B,C],A] \leq N$, entonces $[[C,A],B] \leq N$.*

Demostración. Considerando G/N, podemos asumir $N = 1 = [[A,B],C] = [[B,C],A]$. Sean $a \in A$, $b \in B$, $c \in C$. Por la *Identidad de Hall-Witt* de la Proposición 1.13 se tiene
$$[a,b^{-1},c]^b \cdot [b,c^{-1},a]^c \cdot [c,a^{-1},b]^a = 1.$$

El primer factor pertenece a $[[A,B],C]^b = 1^b = 1$ y por tanto es igual a 1. Análogamente el segundo pertenece a $[[B,C],A]^c$ y por tanto es igual a uno. Lo que implica que $[c,a^{-1},b]^a = 1 \Rightarrow [c,a^{-1},b] = 1^{a^{-1}} = 1$. Reemplazando a por a^{-1}, tenemos $[c,a,b] = 1$ para todo $a \in A, b \in B, c \in C$. Por lo tanto, $[c,a] \in Z_G(B)$ para todo $c \in C, a \in A$, siendo $Z_G(B)$ el centralizador de B en G, es decir el subgrupo que contiene los elementos de G que conmutan con todos los de B. Debido a que $[C,A]$ está generado por elementos de la forma $[c,a]$ con $c \in C$ y que $Z_G(B)$ es un subgrupo, se tiene $[C,A] \in Z_G(B)$, y por lo tanto $[C,A,B] = 1$. □

1.2. Series de grupos

A continuación, vamos a definir algunas series importantes de subgrupos que existen para todo grupo y que nos van a ser de gran utilidad a lo largo de todo el trabajo.

Definición 1.17. La *serie central descendente* de un grupo G se define inductivamente como $\gamma_1(G) = G, \gamma_{k+1}(G) = [\gamma_k(G), G]$ para todo $k \in \mathbb{N}$.

Proposición 1.18. *Sea G un grupo y $N \trianglelefteq G$, entonces $\gamma_k(N) \trianglelefteq G$. Además, dado un automorfismo α de G tal que $\alpha(N) = N$ se tiene que $(\gamma_k(N))^\alpha = \gamma_k(N)$, para todo $k \geq 1$.*

Demostración. Basta probar la segunda afirmación, ya que la primera es el caso particular en el que $n^\alpha = g^{-1}ng$ para $g \in G$. Procedemos por inducción sobre k. Para $k = 1$ tenemos que $\gamma_1(N) = N$, luego podemos suponer que es cierto para $1 \leq i \leq k-1$. Veamos que se cumple para k.

$\gamma_k(N)$ está generado por $[h,n]$ con $h \in \gamma_{k-1}(N)$ y $n \in N$. Luego basta ver que $[h,n]^\alpha \in \gamma_k(N)$.

$$[h,n]^\alpha = (h^{-1})^\alpha (n^{-1})^\alpha h^\alpha n^\alpha = [h^\alpha, n^\alpha] \in \gamma_k(N)$$

ya que $h^\alpha \in \gamma_{k-1}(N)$ por inducción y $n^\alpha \in N$ por ser N α-invariante.

□

Ejemplo 1.19. Sea S_5 el grupo simétrico de grado 5, es decir, el conjunto de las permutaciones de un conjunto $\Omega = \{1,2,3,4,5\}$ de cinco elementos con elemento neutro la identidad y con el producto dado por la composición. Una trasposición es una permutación que consiste en intercambiar dos elementos de Ω y fija el resto. Se puede probar que toda permutación de Ω puede expresarse como producto de trasposiciones y que aunque dicha expresión no es única sí lo es la paridad. El grupo alternado $G = A_5$ se define como el conjunto de permutaciones de orden par, que son aquellas que se pueden escribir como producto de un número par de trasposiciones. Sabemos que A_5 es simple, es decir, los únicos subgrupos normales que tiene son 1 y G. Debido a la Proposición 1.18 tomando $N = G$ y teniendo en cuenta que $\gamma_1(G) = G'$, se tiene $G' \trianglelefteq G$. Como G es simple, $G' = 1$ o $G' = G$. Como G no es abeliano tenemos $G' \neq 1$ y por tanto $G' = G$.

Proposición 1.20. *Sea G un grupo, tenemos $\gamma_i(G) \geq \gamma_{i+1}(G)$ y además $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$.*

Demostración. Se procede por inducción sobre i.

Para $i = 1$ es obvio ya que $\gamma_1(G) = G$.

Suponemos cierto para $i-1$. Veamos para $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [\gamma_{i-1}(G), G] = \gamma_i(G)$. Luego $\gamma_i(G) \geq \gamma_{i+1}(G)$ para todo i.

Para la segunda afirmación, consideramos $i, j \in \mathbb{N}$, se procede por inducción sobre j. Si $j = 1$ se tiene $[\gamma_i(G), \gamma_1(G)] = [\gamma_i(G), G] = \gamma_{i+1}(G)$. Por definición y por hipótesis de inducción tenemos para $j-1$, $[\gamma_i(G), \gamma_{j-1}(G)] \leq \gamma_{i+j-1}(G)$ para todo i. De aquí se deduce,

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

y también,

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

Por el *Lema de los Tres Subgrupos* (1.16) tenemos que $[G, \gamma_i(G), \gamma_{j-1}(G)] \leq \gamma_{i+j}(G)$ y $[\gamma_i(G), \gamma_{j-1}(G), G] \leq \gamma_{i+j}(G)$ implican $[\gamma_{j-1}(G), G, \gamma_i(G)] \leq \gamma_{i+j}(G)$ y por tanto,

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

es decir,

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

como queríamos probar. □

Proposición 1.21. *Sea G un grupo, se tiene que $G^{(i)}/G^{(i+1)}$ y $\gamma_i(G)/\gamma_{i+1}(G)$ son abelianos. Además este último es central en $G/\gamma_{i+1}(G)$.*

Demostración. Sean $xG^{(i+1)}, yG^{(i+1)} \in G^{(i)}/G^{(i+1)}$, con $x, y \in G^{(i)}$. Tenemos

$$[xG^{(i+1)}, yG^{(i+1)}] = x^{-1}y^{-1}xyG^{(i+1)} = [x,y]G^{(i+1)} = G^{(i+1)},$$

luego $G^{(i)}/G^{(i+1)}$ es abeliano.

Para la última afirmación tenemos que ver que los elementos de $\gamma_i(G)/\gamma_{i+1}(G)$ conmutan con todos los elementos de $G/\gamma_{i+1}(G)$. Para ello, tomamos $x\gamma_{i+1}(G)$ tal que $x \in \gamma_i(G)$, y $y \in G$. Observemos que

$$[x\gamma_{i+1}(G), y\gamma_{i+1}(G)] = [x,y]\gamma_{i+1}(G) = \gamma_{i+1}(G)$$

ya que $[x,y] \in \gamma_{i+1}(G)$.

Por último, notemos que como $\gamma_i(G)/\gamma_{i+1}(G)$ es central en $G/\gamma_{i+1}(G)$ por fuerza ha de ser abeliano. □

Definición 1.22. La *serie central ascendente* de un grupo G se define inductivamente como $\zeta_1(G) = Z(G)$ con $Z(G)$ centro de G, $\zeta_{k+1}(G)/\zeta_k(G) = Z(G/\zeta_k(G))$.

Definición 1.23. La *serie derivada* de un grupo G es $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$ tal que $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$. Si existe un valor de d tal que $G^{(d+1)} = 1$, el menor valor posible en esas condiciones se llama *longitud derivada* de G.

Definición 1.24. Sea G un grupo y $G = G_0 \leq G_1 \ldots$ una serie, entonces se dice que la serie se *estabiliza* cuando existe un número natural n tal que $G_i = G_n$ para todo $i \geq n$.

Definición 1.25. Se dice que la serie central descendente o serie derivada *termina* si existe $n \in \mathbb{N}$ tal que $G_i = 1$ para $i \geq n$, siendo G_k el elemento k de la serie correspondiente. En ese caso, también se dice que las series llegan a 1.

Definición 1.26. Si existe $n \in \mathbb{N}$ tal que $G_i = G$ para $i \geq n$ con G_k el elemento k de la serie central ascendente, entonces se dice que la serie *termina* o que la serie llega a G.

Observación 1.27. En el caso de que G sea finito cualquier serie se estabiliza, pero puede terminar o no.

Observación 1.28. La serie central ascendente está relacionada con la serie central descendente. Si una de ellas termina, lo hará también la otra (lo veremos con más detalle en la Proposición 1.39).

Proposición 1.29. *Sea G un grupo, entonces G' es normal en G y G/G' es abeliano. Además si $N \trianglelefteq G$ es tal que el cociente G/N es abeliano, entonces $G' \leq N$.*

Demostración. La primera parte del enunciado es una consecuencia directa de la Proposición 1.18 y por la Proposición 1.21, G/G' es abeliano.

Supongamos $N \trianglelefteq G$ es un subgrupo tal que G/N abeliano. Sea $[x,y] \in G'$ se tiene que

$$[xN, yN] = x^{-1}y^{-1}xyN = [x,y]N = N$$

por ser G/N abeliano, luego $[x,y]$ pertenece a N y tenemos $G' \leq N$. □

Las series que más vamos a utilizar van a ser la serie central descendente y la serie derivada, debido a que son más sencillas de calcular. Vamos a calcular estas series para alguno de los ejemplos que hemos visto anteriormente.

Ejemplo 1.30. [Grupo diédrico] Consideramos el grupo del Ejemplo 1.9. Veamos cómo es la serie central descendente. Comencemos por el primer término, para ello vamos a calcular algunos conmutadores.

$[a,b] = a^{-1}b^{-1}ab = ab^{-1}ab = bb = b^2$

$\left[a,b^2\right] = ab^{-2}ab^2 = b^4$

$\left[a,b^3\right] = ab^{-3}ab^3 = b^6 = 1$

$\left[a,b^4\right] = ab^{-4}ab^4 = b^2$

De aquí deducimos que $1, b^2, b^4 \in G'$. Sospechamos que no hay más elementos en G'. Vamos a utilizar la Proposición 1.29. Denotamos $N = \{1, b^2, b^4\}$, veamos que $N \trianglelefteq G$.

Sea $x \in G$ arbitrario. Notemos que es suficiente probar que $(b^2)^x \in N$ para deducir que $N \trianglelefteq G$ ya que $(b^4)^x = ((b^2)^2)^x = ((b^2)^x)^2$. Basta probarlo para $x = a$ y $x = b$:

- Si $x = a \Longrightarrow (b^2)^x = (b^2)^a = ab^2a = b^4 \in N$.
- Si $x = b \Rightarrow (b^2)^x = b^{-1}b^2b = b^2 \in N$.

Por tanto, $N \trianglelefteq G$. Veamos ahora si G/N es abeliano. Primero calculamos los elementos de G/N:

$$\begin{aligned} N &= \{1, b^2, b^4\} \\ aN &= \{a, ab^2, ab^4\} \\ bN &= \{b, b^3, b^5\} \\ abN &= \{ab, ab^3, ab^5\} \end{aligned}$$

Por lo tanto, $G/N = \{N, aN, bN, abN\}$. Veamos que es abeliano. Tenemos,

$$bNaN = baN = \{ba, bab^2, bab^4\} = \{ab^5, ab, ab^3\} = abN = aNbN.$$

Luego G/N es abeliano. Resumiendo, tenemos $N \trianglelefteq G$ y sabemos que G/N es abeliano, luego $G' \leq N$ por la Proposición 1.29. Sabemos que $1, b^2, b^4 \in G'$ y $N = \{1, b^2, b^4\}$ por lo que deducimos que $G' = N$.

Por lo tanto tenemos, $\gamma_1(G) = G$ y $\gamma_2(G) = G' = [G,G] = N$. Calculemos $\gamma_3(G)$.

$\gamma_3(G) \overset{def}{=} [G, G'] = \langle [x,y] \,|\, x \in G, y \in G' \rangle$

$\left[a,b^2\right] = b^4 \in \gamma_3(G) \Rightarrow b^2 \in \gamma_3(G)$. Además $\gamma_3(G) \leq \gamma_2(G) = N$. Por lo que $\gamma_3(G) = \gamma_2(G)$.

Luego, se deduce que $\gamma_i(G) = N$, $\forall i \geq 2$.

Veamos ahora cual es su serie derivada. Ya hemos calculado $G' = [G,G] = \gamma_2(G) = \{1, b^2, b^4\}$. Por definición $G'' = [G', G']$, luego $G'' = 1$ ya que b^2 y b^4 conmutan. Por tanto, $G' = \{1, b^2, b^4\}$ y $G^{k)} = 1$, $\forall k \geq 2$. Podemos verlo mejor en un diagrama.

$$\begin{array}{l} \text{G} \\ \Big| \\ G' = \{1, b^2, b^4\} \\ \Big| \\ 1 \end{array}$$

Ejemplo 1.31. Consideremos el grupo del Ejemplo 1.11. Vamos a calcular su serie central descendente. Vamos a utilizar el mismo procedimiento que en el ejemplo anterior. Calculamos algunos conmutadores para intuir cómo puede ser G'.

$$[a,b] = a^{-1}b^{-1}ab = a^2b^2ab = a^2babcb = a^2abcbcb = a^3cb^2bc = c^2$$

$$[ab,b] = b^{-1}a^{-1}b^{-1}abb = b^2a^2b^2ab^2 = b^2c^2b = c^2$$

$$[a,b] \cdot [a,b] = c^2c^2 = c$$

Luego $c, c^2 \in G'$. Sospechamos que $G' = \{1, c, c^2\}$. Vamos a denotar N a ese conjunto. Es trivial ver que N es subgrupo de G. Como c conmuta con a y b (obviamente también con sí mismo), vamos a tener que para todo $x \in G$, $x^{-1}cx = cx^{-1}x = c \in N$ y por consiguiente, $x^{-1}c^2x = x^{-1}cxx^{-1}cx = c^2 \in N$. Luego N es normal en G. Probemos que G/N es abeliano. Como G/N está generado por aN y bN (notemos que $cN = N$), basta con probar que aN y bN conmutan.

$$\begin{aligned} aN &= \{a, ac, ac^2\} \\ bN &= \{b, bc, bc^2\} \\ aNbN = abN &= \{ab, abc, abc^2\} \\ bNaN = baN &= \{ba, bac, bac^2\} \end{aligned}$$

En efecto, G/N es abeliano. Por la Proposición 1.29 tenemos que $G' \leq N$. Pero como $N = \{1, c, c^2\} \leq G'$ obtenemos la igualdad, $N = G'$.

Tenemos $\gamma_1(G) = G$ y $\gamma_2(G) = [G, G] = G' = N = \{1, c, c^2\}$. Calculemos $\gamma_3(G) = [G, G']$
$[a, c] = 1$
$[b, c] = 1$

Tanto c como c^2 conmutan con todos los elementos de G, por lo que $[G, G'] = 1$, es decir, $\gamma_3(G) = 1$ y por tanto $\gamma_i(G) = 1\ \forall i \geq 3$.

Calculemos su serie derivada. Ya tenemos el primer término $G' = \{1, c, c^2\}$. Por definición $G'' = [G', G']$. Se ve que $G'' = 1$ ya que c conmuta con sí mismo y todas sus potencias y c^2 también. Luego $G^{(i)} = 1\, \forall i \geq 2$.

Ejemplo 1.32. Consideremos el grupo $UT_3 = UT_3(K)$ con K un cuerpo. Veamos cómo es la serie central descendente.

Sean $g, h \in UT_3$, de forma $g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ y $h = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$. Se puede ver que, $g^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$ y $h^{-1} = \begin{pmatrix} 1 & -d & df-e \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix}$. Haciendo cuentas tenemos

$$[g, h] = g^{-1}h^{-1}gh = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -d & df-e \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix} gh =$$

$$= \begin{pmatrix} 1 & -a-d & df-e+af+ac-b \\ 0 & 1 & -c-f \\ 0 & 0 & 1 \end{pmatrix} gh = \begin{pmatrix} 1 & -d & -cd+df-e+af \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix} h = \begin{pmatrix} 1 & 0 & -dc+af \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Sospechamos que $\gamma_2(UT_3)$ puede ser $\left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| a \in K \right\}$. A este conjunto lo vamos a denotar por N. Veamos que es normal en UT_3.

Sean $g \in N$, $x \in UT_3$, veamos que $x^{-1}gx$ pertenece a N. El elemento x es de la forma $x = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$.

Por lo tanto, $x^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$. De la misma manera, $g = \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, luego $g^{-1} = \begin{pmatrix} 1 & 0 & -d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Calculando tenemos, $x^{-1}gx = \begin{pmatrix} 1 & -a & d+ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} x = \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = g \in N$, y por lo tanto N es normal en UT_3.

Ahora tenemos que ver UT_3/N es abeliano para así poder aplicar la Proposición 1.29 de manera análoga a los ejemplos anteriores.

Sean $g_1, g_2 \in UT_3$, tenemos que ver que $g_1g_2N = g_2g_1N$. Probar esto es equivalente a ver que $g_1^{-1}g_2^{-1}g_1g_2$ pertenece a N.

Utilizando las cuentas del principio del ejercicio tenemos $g_1^{-1}g_2^{-1}g_1g_2 = \begin{pmatrix} 1 & 0 & -dc+af \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in N$.

Por lo tanto, UT_3/N es abeliano y aplicando la Proposición 1.29, tenemos $UT_3' \leq N$.

Sabiendo que $N \leq \gamma_2(UT_3)$ y $UT_3' = \gamma_2(UT_3)$, tenemos la igualdad. Luego,

$$\gamma_2(UT_3) = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a \in K \right\}.$$

Vamos a calcular $\gamma_3(UT_3) = [UT_3, UT_3']$. Sea $g \in UT_3$ y $h \in UT_3'$ teniendo en cuenta los cálculos anteriores se tiene, $[g,h] = \begin{pmatrix} 1 & 0 & -d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$. Luego, $\gamma_3(UT_3) = 1$ y por tanto, UT_3 es nilpotente.

Resumiendo tenemos

- $\gamma_1(UT_3) = UT_3$
- $\gamma_2(UT_3) = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$
- $\gamma_3(UT_3) = 1$

Por lo tanto,

$$\gamma_1(UT_3)/\gamma_2(UT_3) = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \gamma_2(UT_3) \right\} \cong (K^2, +)$$

siendo este último un espacio vectorial de dimensión 2 sobre K, esto es debido a las dos siguientes propiedades,

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

$$\begin{pmatrix} 1 & a_1 & 0 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & 0 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1+a_2 & a_1b_2 \\ 0 & 1 & b_1+b_2 \\ 0 & 0 & 1 \end{pmatrix},$$

notemos que ésta última matriz en el cociente anterior se corresponde con $\begin{pmatrix} 1 & a_1+a_2 & 0 \\ 0 & 1 & b_1+b_2 \\ 0 & 0 & 1 \end{pmatrix}$.

Además, $\begin{pmatrix} 1 & a_1 & 0 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} \gamma_2(UT_3) = \begin{pmatrix} 1 & a_2 & 0 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} \gamma_2(UT_3) \Leftrightarrow a_1 = a_2$ y $b_1 = b_2$. Para probarlo es suficiente ver que

$$\begin{pmatrix} 1 & a_1 & 0 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_2 & 0 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_2 & c \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

entonces se tiene que $c = 0$, $a_1 = a_2$, $b_1 = b_2$.

Además, como $\gamma_3(UT_3) = 1$ y teniendo en cuenta la forma de las matrices de $\gamma_2(UT_3)$, se deduce que

$$\gamma_2(UT_3)/\gamma_3(UT_3) = \gamma_2(UT_3) \cong (K,+)$$

Para visualizar la serie central descendente vamos a utilizar el siguiente diagrama:

$$\begin{array}{r|l} \gamma_1(UT_3) = UT_3 & \\ & \cong K^2 \\ \gamma_2(UT_3) & \\ & \cong K \\ \gamma_3(UT_3) = 1 & \end{array}$$

Vamos a ver un resultado que simplifica el cálculo de la serie central descendente y que utilizaremos en el último capítulo para generalizar lo que se ha hecho aquí al caso de n arbitrario.

Lema 1.33. *Sea G un grupo y $k \in \mathbb{N}$, se tiene:*

a) *$\gamma_k(G)$ contiene todos los conmutadores de peso mayor o igual a k de elementos de G.*

b) *$\gamma_k(G)$ está generado por los conmutadores simples de peso exactamente k de elementos de G.*

c) *Si $G = \langle M \rangle$, entonces $\gamma_k(G)$ está generado por los conmutadores simples de peso mayor o igual a k de los elementos de $M \cup M^{-1}$.*

d) *Si $G = \langle M \rangle$, entonces $\gamma_k(G)/\gamma_{k+1}(G)$ está generado por conmutadores simples de peso k de los elementos de $M \cup M^{-1}$.*

Demostración. a) Como $\gamma_i(G) \geq \gamma_{i+1}(G)$ para todo i por la Proposición 1.20, es suficiente probar que cada conmutador de peso exactamente k pertenece a $\gamma_k(G)$. Procedemos por inducción sobre k. Para $k = 1$ se cumple ya que $\gamma_1(G) = G$. Sea $c = [x_1,\ldots,x_k] = [[x_1,\ldots,x_{k-1}],\ x_k] = [c_1,\ c_2]$ con $c_1 \in \gamma_{k-1}(G)$ y $c_2 \in \gamma_1(G) = G$. Por definición $[c_1,c_2] \in \gamma_k(G)$. Y por tanto, hemos obtenido lo que queríamos.

b) Definimos $N_k = \langle [g_1,\ldots,g_k] | g_1,\ldots,g_k \in G \rangle$. Por a) tenemos $N_k \leq \gamma_k(G)$. Probemos por inducción que $\gamma_k(G) \leq N_k$. Para $k = 1$ sabemos $N_1 = G = \gamma_1(G)$. Ahora suponemos para $i \leq k-1$ que $\gamma_i(G) \leq N_i$. La Proposición 1.13 implica que para todo $g \in G$, tenemos $[g_1,\ldots,g_k]^g = [g_1^g,\ldots,g_k^g] \in N_k$, luego N_k es normal en G. Para cualquier $g \in G$ tenemos $[[g_1,\ldots,g_{k-1}],g] \in N_k$, lo que implica que $[N_{k-1},G] \leq N_k$. Luego $\gamma_k(G) = [\gamma_{k-1}(G),G] \leq [N_{k-1},G] \leq N_k$. Y por tanto, tenemos la igualdad, $\gamma_k(G) = \langle [g_1,\ldots,g_k] | g_i \in G \rangle$.

c) Usando b) y teniendo en cuenta el cuarto apartado de la Proposición 1.13, se tiene c).

d) Por c) $\gamma_k(G)$ está generado por conmutadores $a_t = [x_1,\ldots,x_t]$ con $t \geq k$, y $x_i \in M \cup M^{-1}$. Si $t > k$ tenemos $a_t \in \gamma_{k+1}(G)$ y por lo tanto $a_t\gamma_{k+1}(G) = \gamma_{k+1}(G)$. Y por tanto en $\gamma_k(G)/\gamma_{k+1}(G)$ sólo nos quedan los a_t con $t = k$. □

1.3. Grupos resolubles y nilpotentes

Definición 1.34. Decimos que G es *resoluble* si existe una serie $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ con $G_i \trianglelefteq G$ en la que cada cociente G_{i+1}/G_i es abeliano, $n \in \mathbb{N}$.

Observación 1.35. Todo grupo abeliano es resoluble.

Proposición 1.36. *Un grupo G es resoluble si y solo si su serie derivada termina.*

Demostración. Si la serie derivada termina es obvio que G es resoluble.

Si es resoluble sabemos que existe $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ con $G_i \trianglelefteq G$ y cada cociente G_i/G_{i+1} abeliano. Procedemos por inducción sobre n para probar que su serie derivada termina. Para $n = 0$ es trivial. Por inducción podemos suponer que la serie derivada de G_{n-1} termina ya que este grupo es resoluble. Sabemos $G_{n-1} \trianglelefteq G$ y G/G_{n-1} es abeliano. Luego por la Proposición 1.29, $G' \leq G_{n-1}$. Luego, $G^{(i+1)} = (G')^{(i)} \leq G_{n-1}^{(i)}$. Y por tanto, la serie derivada de G también termina. □

Definición 1.37. Decimos que G es *nilpotente* si existe una serie $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ tal que G_{i+1}/G_i está contenido en el centro de G/G_i.

El menor valor de c con $\gamma_{c+1}(G) = 0$ se denomina *clase de nilpotencia* de G. Las series que cumplen que cada cociente G_{i+1}/G_i es central en G/G_i se denominan *series centrales*.

Observación 1.38. Notemos que si G es abeliano, entonces es nilpotente. Además, la serie central descendente de cualquier grupo es efectivamente una serie central, lo hemos probado en la Proposición 1.21.

Proposición 1.39 (Definiciones equivalentes a nilpotente)**.** *Sea G un grupo, son equivalentes:*

i) G es nilpotente.

ii) Su serie central descendente llega a 1.

iii) Su serie central ascendente llega a G.

Demostración. Veamos $i) \Rightarrow ii)$, para ello suponemos que existe una serie $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ tal que $G_{i+1}/G_i \subseteq Z(G/G_i)$ para $0 \leq i \leq n-1$. Observemos que $G_{i+1}/G_i \subseteq Z(G/G_i) \Leftrightarrow [G_{i+1}/G_i,\, G/G_i] = 1 \Leftrightarrow ([G_{i+1},\, G]\, G_i)/G_i = 1 \Leftrightarrow [G_{i+1},\, G] \leq G_i$, es decir,

$$G_{i+1}/G_i \subseteq Z(G/G_i) \Leftrightarrow [G_{i+1},\, G] \leq G_i \tag{1.1}$$

para todo $i \leq n-1$.

Veamos por inducción sobre i, que $\gamma_i(G) \leq G_{n-i+1}$, para $i = 1$ tenemos $\gamma_1(G) = G = G_{n-1+1}$. Suponemos que es cierto para i, veamos si se cumple para $i+1$. Aplicando (1.1) con $n-i$ en lugar de i, tenemos $[G_{n-i+1}, G] \leq G_{n-i}$. Por lo tanto, $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [G_{n-i+1}, G] \leq G_{n-i}$. Luego tenemos,

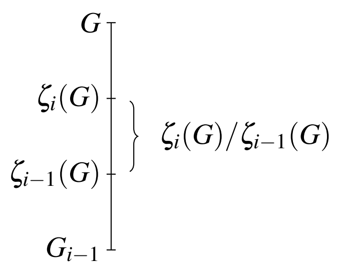
$$\gamma_{i+1}(G) \leq G_{n-i}. \tag{1.2}$$

Por lo tanto, $\gamma_{n+1}(G) \leq G_0 = 1$, es decir, la serie central descendente termina.

$ii) \Rightarrow i)$ Consecuencia de la Proposición 1.21.

$iii) \Rightarrow i)$ Es trivial ya que la serie central ascendente es una serie central

$i) \Rightarrow iii)$ Suponemos que G es nilpotente, luego existe una serie $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ tal que G_{i+1}/G_i está contenido en el centro de G/G_i. Vamos a probar que $G_i \leq \zeta_i(G)$ para todo $i \geq 0$.



Procedemos por inducción sobre i. Para $i = 0$ tenemos $G_0 = 1 = \zeta_0(G)$. Suponemos cierto para $1 \leq k \leq i-1$. Veamos que se cumple también para i. Por la definición de serie central ascendente sabemos $\zeta_i(G)/\zeta_{i-1}(G) = Z(G/\zeta_{i-1}(G))$. Por otro lado, también sabemos que G_i/G_{i-1} es central en G/G_{i-1}, lo que es equivalente a decir que para todo $g \in G_i$ y todo $x \in G$, tenemos $g^x G_{i-1} = gG_{i-1}$. Por hipótesis de inducción $G_{i-1} \leq \zeta_{i-1}(G)$, luego $g^x\zeta_{i-1}(G) = g\zeta_{i-1}(G)$, luego $g\zeta_{i-1}(G) \in Z(G/\zeta_{i-1}(G)) = \zeta_i(G)/\zeta_{i-1}(G)$.

Por lo tanto

$$G_i \leq G_i\zeta_{i-1}(G) \leq \zeta_i(G)$$

tal y como queríamos probar.

□

Teorema 1.40. *Si G es un grupo nilpotente, entonces G es resoluble.*

Demostración. Veamos por inducción que $G^{(i)} \leq \gamma_{i+1}(G)$ para todo $i \geq 0$, es decir, que G es resoluble ya que si G es nilpotente, la serie central descendente termina y por tanto la serie derivada también. Si $i = 0$ es trivial ya que $G^{(0)} = \gamma_1(G) = G$.

Suponemos que es cierto para i. Se tiene $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [\gamma_{i+1}(G), G] = \gamma_{i+2}(G)$. Como G es nilpotente tenemos $\gamma_{c+1}(G) = 1$ para algún c, y entonces $G^{(c)} = 1$, y por tanto G es resoluble.

□

Observación 1.41. El recíproco no es cierto, un contraejemplo lo vamos a ver en el Ejemplo 1.42.

Debido a que ya hemos calculado las respectivas series central descendente y derivada en los ejemplos utilizados anteriormente, nos va a ser fácil ver si son nilpotentes y/o resolubles.

Ejemplo 1.42 (Diédrico)**.** Volvamos de nuevo al grupo del Ejemplo 1.30. Hemos calculado su serie central descendente $\gamma_1(G) = G, \gamma_i(G) = \{1, b^2, b^4\} \forall i \leq 2$, se puede ver que no llega a 1, por lo tanto, $G = D_6$ no es nilpotente. También conocemos su serie derivada y tenemos $G' = \{1, b^2, b^4\}$ y $G^{i)} = 1 \forall i \leq 2$. Por tanto, G es resoluble. Luego, G es un grupo resoluble pero no nilpotente.

Ejemplo 1.43. Consideremos el grupo del Ejemplo 1.31. Veamos que es resoluble y nilpotente.

Recordemos cómo es su serie descendente,

$$\gamma_1(G) = G, \quad \gamma_2(G) = \{1, c, c^2\}, \quad \gamma_i(G) = 1 \text{ para todo } i \geq 3.$$

Como la serie central descendente llega a 1, G es nilpotente y por el Teorema 1.40 también resoluble.

Lema 1.44. *Sea G un grupo, si existe un subgrupo N normal en G tal que G/N y N son resolubles, entonces G es resoluble.*

Demostración. Por ser N y G/N resolubles, existen N_i y H_i tales que

$$1 = N_0 \trianglelefteq \ldots \trianglelefteq N_m = N$$

$$1 = H_0/N \trianglelefteq \ldots \trianglelefteq H_n/N = G/N$$

con N_{i+1}/N_i y con H_{j+1}/H_j abelianos para $0 \leq i \leq m-1$ y $0 \leq j \leq n-1$. Consideramos el homomorfismo

$$\begin{array}{rccc} \alpha: & G & \longrightarrow & G/N \\ & g & \longmapsto & gN \end{array}$$

Definimos $G_i = N_i$ para $0 \leq i \leq m-1$, $G_m = N_m = N = (H_0/N)^{\alpha^{-1}}$, y $G_i = (H_{i-m}/N)^{\alpha^{-1}}$ para $m+1 \leq i \leq n+m$ de manera que se tiene

$$1 = G_0 \trianglelefteq \ldots \trianglelefteq G_m \trianglelefteq \ldots \trianglelefteq G_{m+n} = G$$

Notemos que G_{i+1}/G_i es abeliano para todo i: si $i < m$ es trivial y si $i \geq m$ tenemos

$$[(H_{j+1}/N)^{\alpha^{-1}}, (H_j/N)^{\alpha^{-1}}] = [H_{j+1}/N, H_j/N]^{\alpha^{-1}} = N^{\alpha^{-1}} = N,$$

y por tanto G_{i+1}/G_i es abeliano. □

Ejemplo 1.45. Con el fin de simplificar la notación, vamos a dar por hecho que los elementos de todas las matrices de este ejemplo pertenecen a un cuerpo K. Consideramos el grupo de las matrices triangulares superiores no singulares de tamaño $n \times n$,

$$T_n = \left\{ \begin{pmatrix} a_{11} & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix} \middle| a_{11}, \ldots, a_{nn} \neq 0 \right\}$$

y el grupo de las matrices unitriangulares superiores sobre el cuerpo K

$$UT_n = \left\{ \begin{pmatrix} 1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \right\}$$

La operación de estos grupos es la multiplicación usual en matrices.

Es trivial que $UT_n \cap D_n = I_n$, con D_n el grupo de las matrices diagonales no singulares. Veamos que $T_n = D_n \cdot UT_n$, es decir, que para todo g en T_n, existe $d \in D_n, u \in UT_n$ tales que $g = du$. Basta observar que

$$\underbrace{\begin{pmatrix} a_1 & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix}}_{g} = \underbrace{\begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix}}_{d} \underbrace{\begin{pmatrix} 1 & a_{12}a_1^{-1} & \cdots & a_{1n}a_1^{-1} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1n}\, a_{n-1}^{-1} \\ 0 & \cdots & 0 & 1 \end{pmatrix}}_{u}$$

Notemos que $a_i \neq 0$ para $1 \leq i \leq n$ ya que g es invertible y por tanto, existe a_i^{-1} ya que K es un cuerpo. Luego, en efecto

$$T_n = D_n \cdot UT_n.$$

Veamos ahora UT_n es normal en T_n, para ello vamos a utilizar que $T_n = D_n \cdot UT_n$. Tenemos que ver que dados $v \in UT_n,\ g \in T_n$ también se tiene $g^{-1}vg \in UT_n$.

Por lo anterior sabemos que existe $d \in D_n$, $u \in UT_n$ tal que $g = du$. Por lo que $g^{-1}vg = u^{-1}d^{-1}vdu$, luego basta probar $d^{-1}vd \in UT_n$. Sabemos que d es de la forma $\begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix}$ con $0 \neq a_1, \ldots, a_n$, por lo que $d^{-1} = \begin{pmatrix} a_1^{-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n^{-1} \end{pmatrix}$. Además sabemos que $v = \begin{pmatrix} 1 & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$. Vamos a ver qué forma tiene el elemento $d^{-1}vd$,

$$d^{-1}vd = \begin{pmatrix} a_1^{-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n^{-1} \end{pmatrix} \begin{pmatrix} 1 & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} =$$

$$\begin{pmatrix} a_1^{-1} & \cdots & a_1^{-1}v_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n^{-1} \end{pmatrix} \begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & u_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$$

Por lo que $d^{-1}vd \in UT_n$. Es decir, $UT_n \trianglelefteq T_n$.
En estas condiciones se dice que T_n es *producto semidirecto* de UT_n y D_n, se denota

$$T_n = D_n \ltimes UT_n.$$

Esto es válido $\forall n \in \mathbb{N}$ y K cuerpo.
Segundo Teorema de Isomorfía: dados un grupo G, un subgrupo H y un subgrupo normal en G, se tiene que $(HN)/N \cong H/(H \cap N)$. Entonces, considerando lo visto en este ejemplo, tenemos

$$T_n/UT_n = D_nUT_n/UT_n \cong D_n/(D_n \cap UT_n) = D_n$$

y sabemos que D_n es abeliano. Luego por la Proposición 1.29 tenemos que $T_n' \leq UT_n$.

Más adelante, veremos que es UT_n es nilpotente, y por tanto resoluble, además hemos visto que el cociente de T_n y UT_n es isomorfo a D_n y este es abeliano y por tanto resoluble. Por lo que por el Lema 1.44 tenemos que T_n es resoluble.

Capítulo 2

Álgebras de Lie

En este capítulo introduciremos la noción de *álgebra de Lie* y veremos algunas de sus propiedades siguiendo un desarrollo análogo al que hemos hecho para grupos. Todos los conceptos y propiedades de este capítulo están basados en las lecturas [2] y [5]. En el próximo capítulo analizaremos la relación de las álgebras de Lie con los grupos.

2.1. Primeros conceptos y ejemplos

Definición 2.1. Un espacio vectorial L sobre un cuerpo K, con una operación binaria interna bilineal

$$\begin{array}{rccc} [\cdot,\cdot]: & L\times L & \longrightarrow & L \\ & (x,y) & \longmapsto & [x,y] \end{array}$$

tal que satisface:

i) $[[x,y],z]+[[z,x],y]+[[y,z],x]=0$ (*Identidad de Jacobi*)

ii) $[x,x]=0\ \forall x\in L$

se denomina *K-álgebra de Lie*. Si se sobreentiende el cuerpo en el que estamos, diremos solamente *álgebra de Lie*.

Definición 2.2. Un *anillo de Lie* es un grupo abeliano con una operación binaria interna que cumple

$$[a+b,c]=[a,c]+[b,c]$$

y también las propiedades i) y ii) anteriores.

Observación 2.3. La principal característica de las álgebras o anillos de Lie es que el corchete no es asociativo, es decir, en general

$$[[a,b],c]\neq[a,[b,c]].$$

Esta falta de asociatividad complica en ocasiones los cálculos.

Observación 2.4. Todo anillo de Lie se puede ver como una $\mathbb{Z}$-álgebra de Lie. Así, de ahora en adelante diremos simplemente álgebra de Lie para referirnos a una R-álgebra de Lie y se sobreentenderá que R es o bien $\mathbb{Z}$ o bien un cuerpo K que solo especificaremos si es necesario.

Observación 2.5. Toda K-álgebra de Lie es también un anillo de Lie (es decir, una $\mathbb{Z}$-álgebra) pero no al revés.

Observación 2.6. Las álgebras de Lie tienen la propiedad anticonmutativa, es decir, $[a,b]=-[b,a]$ para todo $a,b\in L$. Para verlo desarrollamos por bilinealidad el siguiente conmutador

$$[a+b,\ a+b]=[a,a]+[a,b]+[b,a]+[b,b]=0$$

ya que $[x,x]=0$ para todo $x\in L$, por lo que nos queda $[a,b]+[b,a]=0$.

Como consecuencia de esta observación, en un anillo de Lie también se cumple

$$[a,b+c] = [a,b]+[a,c]$$

para todo a,b,c en el anillo de Lie. Es decir, el corchete, al igual que para una K-álgebra, es bilineal.

Observación 2.7. Para no dar lugar a confusión con la notación usada por conmutadores de grupos, en los casos en los que sea necesario, denotaremos $[\cdot,\cdot]_L$ al corchete de un álgebra de Lie L, también denotaremos por $[\cdot,\cdot]_G$ al conmutador en un grupo G.

Definición 2.8. Un álgebra de Lie L es abeliana si $[x,y] = 0$ para todo $x,y \in L$.

Ejemplo 2.9. Sea V un espacio vectorial sobre un cuerpo K, definimos $[\cdot,\cdot]$ mediante $[A,B] = 0$ para todo A, $B \in V$. Este es un ejemplo de álgebra de Lie abeliana.

Ejemplo 2.10. Sea $L = Mat(n,R)$ el conjunto de todas las matrices cuadradas de tamaño $n \times n$ sobre $R = K$ cuerpo o $R = \mathbb{Z}$. Consideramos el *corchete de Lie* en L definido como

$$[A,B]_L := AB-BA \ \forall A,B \in Mat(n,R).$$

Notemos que esta operación es obviamente bilineal y que

$$[A,A] = AA-AA = 0.$$

Veamos que también se satisface la *Identidad de Jacobi*. Sean $A,B,C \in Mat(n,R)$, teniendo en cuenta que los *corchetes de Lie* son bilineales tenemos,

$$[[A,B],C]+[[C,A],B]+[[B,C],A] = [AB-BA,C]+[CA-AC,B]+[BC-CB,A] =$$

$$= [AB,C]-[BA,C]+[CA,B]-[AC,B]+[BC,A]-[CB,A] =$$

$$= ABC-CAB-BAC+CBA+CAB-BCA-ACB+BAC+BCA-ABC-CBA+ACB = 0.$$

Luego, $Mat(n,R)$ con este corchete es un álgebra de Lie.

Definición 2.11. Veamos algunos tipos de aplicaciones entre álgebras de Lie.

- Un *homomorfismo* h es una aplicación entre dos R-álgebras de Lie que es o bien un homomorfismo de R-espacios vectoriales si R es cuerpo o un homomorfismo de grupos abelianos de $R = \mathbb{Z}$ y además, preserva el corchete de Lie, es decir,

$$\begin{array}{rccc} h: & L_1 & \longrightarrow & L_2 \\ & x & \longmapsto & h(x) \end{array}$$

  tal que $h(ax+y) = ah(x)+h(y) \ \forall a \in R, x,y \in L_1$ y $h([x,y]) = [h(x),h(y)]$.

- Un *isomorfismo* es un homomorfismo que es biyectivo. Si existe un isomorfismo entre dos álgebras de Lie se dice que L_1 y L_2 son isomorfas, en este caso, se denota por $L_1 \cong L_2$.

- Un *automorfismo* es un isomorfismo donde $L_1 = L_2$.

Ejemplo 2.12. Sean L_1, L_2 K-álgebras de Lie abelianas de la misma dimensión con K cuerpo, entonces L_1 y L_2 son isomorfas.

Como L_1, L_2 son espacios vectoriales con la misma dimensión, existe un isomorfismo de espacios vectoriales $h : L_1 \to L_2$, es decir h es una biyección tal que $h(ax+y) = ah(x)+h(y)$ para todo $a \in K, x,y \in L_1$, nos falta ver $h([x,y]) = [h(x),h(y)]$. Al ser las dos álgebras abelianas tenemos

$$h([x,y]_{L_1}) = h(0) = 0 = [h(x),h(y)]_{L_2}.$$

Vamos a ver algunas propiedades de álgebras de Lie que son similares, aunque no iguales a las de grupos.

Definición 2.13. Sean K cuerpo y L un K-álgebra de Lie, se llama *subálgebra de Lie* de L a un subespacio vectorial S tal que $[x,y] \in S\ \forall x,y \in S$.

Sea L un $\mathbb{Z}$-álgebra de Lie, se denomina *subálgebra de Lie* de L a un subgrupo abeliano S tal que satisface $[x,y] \in S\ \forall x,y \in S$.

Definición 2.14. Sea L un álgebra de Lie y sea X un subconjunto de L, la subálgebra generada por X se define como la menor subálgebra que contiene a X y se denota por $\langle X \rangle$.
Se denota por $_+\langle X \rangle$ al subgrupo aditivo generado por el subconjunto X. En general $_+\langle X \rangle \subseteq \langle X \rangle$.

Definición 2.15. Sea L un R-álgebra de Lie, un *ideal* de L es un subespacio vectorial S en el caso $R = K$ cuerpo o un subgrupo abeliano si $R = \mathbb{Z}$, tal que $[x,y] \in S\ \forall x \in S, y \in L$. La notación va a ser igual que para anillos, es decir $S \trianglelefteq L$.

Como consecuencia de la Observación 2.6, todo ideal a derecha también lo es a izquierda, por ese motivo no hemos hecho distinción entre ideal a derecha, a izquierda o bilátero en la definición de ideal.

Definición 2.16. Sea L una K-álgebra de Lie e $I \trianglelefteq L$ un ideal. En el espacio vectorial/subgrupo cociente L/I definimos

$$[a+I, b+I] := [a,b] + I$$

Se puede comprobar que esta operación está bien definida y que por tanto L/I es también un K-álgebra de Lie.

Definición 2.17. De manera análoga a lo que se hace para grupos, se puede definir la noción de álgebra libre sobre un conjunto X, que se denota $L(X)$. Dado un subconjunto $S \subseteq L(X)$, se denota por $R < X \mid S >$ al cociente de $L(X)$ por el ideal generado por S (es decir, por el menor ideal de $L(X)$ que contiene a S). Al igual que sucede para subgrupos normales, una intersección arbitraria de ideales es también ideal.

Una expresión del tipo $L = R < X \mid S >$ se dice presentación del álgebra L por generadores y relaciones.

Ejemplo 2.18. Un ejemplo sencillo de álgebra de Lie expresada por generadores y relaciones es:

$$L = K < u,v,w | [u,v] = [v,w] = [u,w] = 0 >$$

con K cuerpo. De hecho, es fácil ver que se trata del álgebra de Lie abeliana de dimensión 3.

Definición 2.19. Sean A y B dos subconjuntos de un álgebra de Lie L, definimos el conmutador de A y B como

$$[A,B] =_+ \langle [a,b] | a \in A,\, b \in B \rangle\,.$$

También se puede ampliar este concepto a varios subconjuntos. Para eso, vamos a utilizar la siguiente notación. Dados elementos $a_1, \ldots, a_n$ en un álgebra de Lie L, definimos inductivamente

$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$

Dados $A_1, \ldots, A_n$ subconjuntos de un álgebra de Lie L, ponemos:

$$[A_1, \ldots, A_n] =_+ \langle [a_1, \ldots, a_n] | a_i \in A_i \rangle\,.$$

Lema 2.20. *Sean A y B ideales de un álgebra de Lie L, entonces $[A,B]$ también es un ideal de L.*

Demostración. Basta probar que $[[a,b],l] \in [A,B]\ \forall a \in A,\, b \in B,\, l \in L$. Por la *Identidad de Jacobi* tenemos que $[[a,b],l] = [[a,l],b] + [a,[b,l]]$. Como $[a,l] \in A, [b,l] \in B$ se tiene que $[[a,b],l] \in [A,B]$. $\square$

Observación 2.21. Como podemos ver, muchas definiciones y propiedades de álgebras de Lie son análogas a las vistas en el capítulo anterior sobre grupos, pero hay algunas diferencias. Por definición, el conmutador de dos subgrupos es subgrupo, mientras que aunque A y B sean subálgebras, el corchete no tiene por qué serlo.

Definición 2.22. Sea L un álgebra de Lie, se dice $\mathbb{N}$-*graduada* si es suma directa de espacios o subgrupos abelianos L_i con $i \geq 0$ tales que $[L_i, L_j] \leq L_{i+j}$ para todo $i, j \in \mathbb{N}$, es decir,

$$L = \bigoplus_i L_i.$$

En este trabajo, nos referiremos a las álgebras de Lie que cumplan esta condición simplemente como *graduadas*.

Las álgebras de Lie graduadas son una familia relevante, en especial porque aparecen de forma natural asociadas a un grupo. Veremos ejemplos en la sección siguiente.

2.2. Series, nilpotencia y resolubilidad para álgebras de Lie

Las nociones de nilpotencia, resolubilidad, serie central y derivada para álgebras de Lie son análogas a las de grupos.

Definición 2.23. La *serie central descendente de un álgebra de Lie L* se define inductivamente como $\gamma_1(L) = L, \gamma_{k+1}(L) = [\gamma_k(L), L]$.

Al segundo elemento de esta serie se denota por $L' = \gamma_2(L) = [L, L]$.

Proposición 2.24. *Sea L álgebra de Lie, entonces L' es un ideal en L y L/L' es una álgebra de Lie abeliana.*

Demostración. Si $x = [x_1, x_2]$, entonces $[x, y] = [[x_1, x_2], y] \in L'$ para todo $y \in L$. Como por definición L' es cerrado para la suma, es un ideal. Veamos que L/L' es una álgebra de Lie abeliana. Sean $x + L', y + L' \in L/L'$ con $x, y \in L$, como $[x, y]$ está en L', se tiene

$$[x + L', y + L']_{L/L'} = [x, y]_L + L' = L'$$

y por tanto L/L' es abeliana. □

Proposición 2.25. *Sea L un álgebra de Lie, entonces $[\gamma_m(L), \gamma_n(L)] \leq \gamma_{m+n}(L)$.*

Demostración. Sean $m, n \in \mathbb{N}$, se procede por inducción sobre n. Si $n = 1$ es trivial. Por definición y por hipótesis de inducción tenemos para $n-1$, $[\gamma_m(L), \gamma_{n-1}(L)] \leq \gamma_{m+n-1}(L)$ para todo m. De aquí se deduce

$$[L, \gamma_m(L), \gamma_{n-1}(L)] = [\gamma_{m+1}(L), \gamma_{n-1}(L)] \leq \gamma_{m+1+n-1}(L) = \gamma_{m+n}(L),$$

y también,

$$[\gamma_m(L), \gamma_{n-1}(L), L] \leq [\gamma_{m+n-1}(L), L] = \gamma_{m+n}(L).$$

Por la *Identidad de Jacobi* tenemos que $[L, \gamma_m(L), \gamma_{n-1}(L)] \leq \gamma_{m+n}(L)$ y $[\gamma_m(L), \gamma_{n-1}(L), L] \leq \gamma_{m+n}(L)$ implica $[\gamma_{n-1}(L), L, \gamma_m(L)] \leq \gamma_{m+n}(L)$ y por tanto,

$$[\gamma_m(L), \gamma_n(L)] = [\gamma_n(L), \gamma_m(L)] = [\gamma_{n-1}(L), L, \gamma_m(L)] \leq \gamma_{m+n}(L).$$

□

Definición 2.26. Un álgebra de Lie es *nilpotente de clase* $\leq c$ si $\gamma_{c+1}(L) = 0$. El menor valor de c con $\gamma_{c+1}(L) = 0$ se llama la *clase de nilpotencia* de L.

Definición 2.27. Se define inductivamente la *serie derivada de un álgebra de Lie L* mediante $L^{(k+1)} = [L^{(k)}, L^{(k)}]$ con $L^{(1)} = [L, L]$

Definición 2.28. Un álgebra de Lie L es *resoluble de longitud derivada* $\leq$ d si $L^{(d)} = 0$. El menor valor de d tal que $L^{(d+1)} = 0$ es la *longitud derivada* de L.

Veamos que mediante la serie central descendente de un álgebra de Lie siempre podemos construir un álgebra de Lie graduada.

Ejemplo 2.29. Sea L un álgebra de Lie. Sea $\gamma_1(L) \supseteq \gamma_2(L) \supseteq \cdots$ la serie central descendente L. Se define

$$\mathrm{grad}(L) := \gamma_1(L)/\gamma_2(L) \oplus \gamma_2(L)/\gamma_3(L) \oplus \cdots$$

como espacio vectorial o grupo abeliano. En este conjunto vamos a definir un corchete de Lie mediante,

$$[A + \gamma_{i+1}(L),\ B + \gamma_{j+1}(L)]_{\text{grad }(L)} = [A, B]_L + \gamma_{i+j+1}(L)$$

con $A \in \gamma_i(L)$, $B \in \gamma_j(L)$. Está bien definido ya que $[A, B]_L \in \gamma_{i+j}(L)/\gamma_{i+j+1}(L)$.

Ejemplo 2.30 (Matrices null-triangulares)**.** Sea $R = \mathbb{Z}$ o un cuerpo, consideramos el conjunto de las matrices cuadradas de dimensión n, con elementos en R tales que los elementos en la diagonal principal y por debajo de la misma son todos 0. Este conjunto se denota por $nt_n(R)$,

$$nt_n(R) = \left\{ \left. \begin{pmatrix} 0 & * & \cdots & * \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & \cdots & 0 \end{pmatrix}_{n \times n} \right| * \in R \right\}$$

con el corchete de Lie

$$[A, B] = [A, B]_L = AB - BA$$

es un álgebra de Lie. Para verlo basta razonar de forma análoga a como hemos hecho en el Ejemplo 2.10. Además, es fácil ver, que no es un álgebra de Lie abeliana.

Se puede probar que es nilpotente y graduada. Esto lo veremos en el Capítulo 3 para cualquier n.

Vamos a probarlo en el caso $n = 3$ y para cualquier anillo conmutativo R. Notemos que $nt_n(R)$ es un grupo abeliano si consideramos la operación suma, pero si consideramos la operación multiplicación usual entre matrices no lo es, ya que no tiene elemento neutro ($I_n \notin nt_n(R)$) y además las matrices de $nt_n(R)$ no son regulares. Comencemos calculando la serie central descendente, procedemos de manera análoga a los ejemplos del capítulo anterior. Consideramos $A, B \in\ nt_3(R)$, luego

$$A = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{pmatrix},$$

y por tanto,

$$[A, B] = \begin{pmatrix} 0 & 0 & af \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & dc \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & af - dc \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Se puede ver que $\gamma_2(nt_3(R)) = \left\{ \left. \begin{pmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right| a \in R \right\}$ ya que

$$\begin{pmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \left[\begin{pmatrix} 0 & a & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \right]$$

y $\gamma_3(nt_3(R)) = 0$, ya que $[A,B] = 0$ para todo $A \in \gamma_2(nt_3(R))$ y $B \in nt_3(R)$. Por lo tanto, $nt_3(R)$ es un álgebra de Lie nilpotente con clase de nilpotencia 2.

Además podemos considerar $L_1 = \left\{ \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \right\}$ y $L_2 = \left\{ \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$.

Se tiene

$$nt_3(R) = L_1 \bigoplus L_2$$

y como $[L_1, L_1] \subseteq L_2$ y $[L_i, L_2] = 0$ para $i = 1, 2$, deducimos que $nt_3(R)$ es un álgebra de Lie graduada.

Capítulo 3

Relación entre grupos y álgebras de Lie

En este capítulo vamos a ver dos formas de relacionar la teoría de grupos con la de álgebras de Lie mediante el *anillo de Lie asociado a un grupo* y la *Correspondencia de Mal'cev*. Estas relaciones nos sirven para pasar de una estructura a otra y por tanto, deducir propiedades de una de ellas estudiando la otra. La información acerca de la *Correspondencia de Mal'cev* está basada en la lectura de [3], el resto del capítulo se fundamenta en el libro [2].

3.1. Anillo de Lie asociado a un grupo

Definición 3.1. Sea G un grupo y $\gamma_i(G)$ los términos de la serie central descendente de G. Se define el *anillo de Lie asociado a G* como el grupo abeliano

$$L(G) = \bigoplus_{i=1}^{\infty} (\gamma_i(G)/\gamma_{i+1}(G)).$$

con el corchete de Lie inducido por

$$[g+\gamma_i(G), h+\gamma_j(G)]_{L(G)} = [g,h]_G + \gamma_{i+j}(G)$$

Observación 3.2. Notemos que como cada cociente $\gamma_i(G)/\gamma_{i+1}(G)$ es abeliano trabajamos con notación aditiva. Veamos que está bien definido, es decir, tenemos que ver que es un grupo abeliano tal que para todo $x,y,z \in L(G)$ se tiene

- $[[x,y],z]+[[z,x],y]+[[y,z],x] = 0$
- $[x,x] = 0$
- $[x+y,z] = [x,z]+[y,z]$

Sea $g \in \gamma_{i-1}(G)$ se tiene $[g+\gamma_i(G), g+\gamma_i(G)]_{L(G)} = [g,g]_G + \gamma_{2i}(G) = \gamma_{2i}(G) \in \gamma_{2i}(G)/\gamma_{2i+1}(G)$, luego tenemos $[x,x] = 0$ para todo $x \in L(G)$.

Sean $h \in \gamma_{j-1}(G)$ y $f \in \gamma_{k-1}(G)$ se tiene

$$[[g+\gamma_i(G), h+\gamma_j(G)]_{L(G)}, f+\gamma_k(G)]_{L(G)} + [[f+\gamma_k(G), g+\gamma_i(G)]_{L(G)}, h+\gamma_j(G)]_{L(G)} +$$
$$+[[h+\gamma_j(G), f+\gamma_k(G)]_{L(G)}, g+\gamma_i(G)]_{L(G)} =$$
$$= [[g,h]_G+\gamma_{i+j}(G), f+\gamma_k(G)]_{L(G)} + [[f,g]_G+\gamma_{k+i}(G), h+\gamma_j(G)]_{L(G)} + [[h,f]_G+\gamma_{j+k}(G), g+\gamma_i(G)]_{L(G)} =$$
$$= [[g,h]_G,f]_G + [[f,g]_G,h]_G + [[h,f]_G,g]_G + \gamma_{i+j+k}(G) = \gamma_{i+j+k}(G)$$

ya que G es grupo y cumple la *Identidad de Hall-Witt*. Falta ver la última propiedad, sean $g,h \in \gamma_{i-1}(G)$ y $f \in \gamma_i(G)$,

$$[g+\gamma_i(G)+h+\gamma_i(G), f+\gamma_j(G)]_{L(G)} = [g+\gamma_i(G), f+\gamma_j(G)]_{L(G)} + [h+\gamma_i(G), f+\gamma_j(G)]_{L(G)}$$

Luego tenemos que $L(G)$ está bien definido. Además tomando $L_i = \gamma_i(G)/\gamma_{i+1}(G)$ para $i \geq 1$ y por la Proposición 2.25 se tiene que es un álgebra de Lie graduada.

3.2. Extensión de escalares en grupos abelianos y $\mathbb{Q}$-álgebra de Lie asociada a un grupo

Sea B un grupo abeliano libre de torsión, es decir, tal que si $0 \neq n \in \mathbb{Z}$ y $0 \neq b \in B$ entonces $nb \neq 0$. Vamos a 'añadir inversos' para transformar B en un $\mathbb{Q}$-espacio vectorial. Sea

$$B \otimes \mathbb{Q} = \{(b,n) | b \in B,\ 0 \neq n \in \mathbb{Z}\} / \sim$$

donde

$$(b,n) \sim (b',n') \text{ si } n'b = nb'.$$

Intuitivamente, estamos representando mediante el par (b,n) el elemento que podríamos denotar por $\frac{1}{n}b$. Se puede comprobar que es una relación de equivalencia.

En $B \otimes \mathbb{Q}$ definimos una operación interna, que denotamos por $+$, tal que

$$(b,n) + (b_1,n_1) := (n1b + nb_1, nn_1).$$

También definimos el producto por un escalar de la siguiente manera: Sea $\frac{s}{t} \in \mathbb{Q}$, y sea $(b,n) \in B \otimes \mathbb{Q}$ ponemos

$$\frac{s}{t} \cdot (b,n) := (sb, tn).$$

Se puede ver que estas operaciones están bien definidas y que $B \otimes \mathbb{Q}$ es un $\mathbb{Q}$-espacio vectorial.

Sea A un grupo abeliano, su subgrupo de torsión es

$$T(A) := \{a \in A |\ na = 0 \text{ para algún } 0 \neq n \in \mathbb{Z}\}$$

Se tiene $T(A) \trianglelefteq A$ ya que en un grupo abeliano todos los subgrupos son normales. Además $A/T(A)$ es libre de torsión.

Definimos

$$A \otimes \mathbb{Q} := (A/T(A)) \otimes \mathbb{Q}$$

Ejemplo 3.3. Si A es un grupo abeliano finitamente generado, entonces $A = T(A) \otimes \mathbb{Z}^n$ luego $A/T(A) = \mathbb{Z}^n$. Y por tanto $A \otimes \mathbb{Q} = (\mathbb{Z}^n) \otimes \mathbb{Q} = \mathbb{Q}^n$

Definición 3.4. Sea G un grupo y $\gamma_i(G)$ los términos de la serie central descendente de G. Se define la *$\mathbb{Q}$-álgebra de Lie de G* como

$$L_{\mathbb{Q}}(G) = \bigoplus_{i=1}^{\infty} ((\gamma_i(G)/\gamma_{i+1}(G)) \otimes \mathbb{Q})$$

con el corchete generado por el que hemos definido anteriormente.

3.3. Matrices unitriangulares y null-triangulares

A continuación, consideramos el grupo de las matrices unitriangulares en R y el álgebra de Lie de las matrices null-triangulares sobre R, siendo $R = \mathbb{Z}$ ó un cuerpo K.

En esta sección vamos a calcular la serie central descendente de $UT_n(R)$ y veremos que $UT_n(R)$ es un grupo nilpotente. Además, probaremos que $L_{\mathbb{Q}}(UT_n(\mathbb{Z})) = nt_n(\mathbb{Q})$. Para ello vamos a considerar unas matrices especiales que nos van a ayudar a probar todas estas propiedades.

A partir de ahora vamos a denotar $G = UT_n(R)$ con $R = \mathbb{Z}$ ó un cuerpo K y $L = nt_n(\mathbb{Q})$.

Definición 3.5. Sean $1 \leq i < j \leq n$ y sea $\alpha \in R$, denotamos por E_{ij} la matriz cuadrada de tamaño $n \times n$, con todos sus elementos ceros excepto el que se encuentra en la fila i y columna j, que tiene un 1 en dicha posición.

Definición 3.6. Sea $\alpha \in R$, definimos $e_{ij\alpha} = I_n + \alpha E_{ij}$, esta matriz es la que tiene 1 en los elementos de la diagonal y además, el valor α en la posición $\{i, j\}$. Es fácil ver que $e_{ij\alpha}^{-1} = I_n - \alpha E_{ij} = e_{i,j,-\alpha}$.

$$E_{ij} = \begin{array}{c c} & j \\ i & \begin{pmatrix} 0 & & & & \vdots & \\ & \ddots & & & \vdots & \\ \cdots & \cdots & \ddots & \cdots & 1 & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \end{array}, \qquad e_{ij\alpha} = \begin{array}{c c} & j \\ i & \begin{pmatrix} 1 & & & & \vdots & \\ & \ddots & & & \vdots & \\ \cdots & \cdots & \ddots & \cdots & \alpha & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} \end{array}$$

Definición 3.7. Sea $1 \leq s \leq n-1$, denotamos

$$X_s = \{e_{ij\alpha} | \alpha \in R, j - i \geq s\}$$

Observación 3.8. Es fácil ver que $X_1 \supseteq X_2 \supseteq \cdots \supseteq X_{n-1}$.

Lema 3.9. *Se tiene*

$$E_{ij} \cdot E_{kl} = \begin{cases} 0 & si\ j \neq k \\ E_{il} & si\ j = k \end{cases}$$

Demostración. Denotamos por a_{pr}, b_{rq} las entradas (p,r) y (r,q) de las matrices E_{ij} y E_{kl} respectivamente. La entrada (p,q) del producto es

$$m_{pq} = \sum_{r=1}^{n} a_{pr} b_{rq},\ con\ a_{pr} = 1\ si\ p = i, r = j\ y\ b_{rq} = 1\ si\ r = k,\ q = l,$$

en el resto de los casos a_{pr} y b_{rq} son cero. □

Lema 3.10. *Se tiene*

$$e_{ij\alpha} \cdot e_{kl\beta} = \begin{cases} e_{ij\alpha} + \beta E_{kl} & si\ j \neq k \\ e_{ij\alpha} + \beta E_{jl} + \alpha\beta E_{il} & si\ j = k \end{cases}$$

Demostración. Tenemos

$$e_{ij\alpha} \cdot e_{kl\beta} = (I_n + \alpha E_{ij}) \cdot (I_n + \beta E_{kl}) = I_n + \beta E_{kl} + \alpha E_{ij} + \alpha E_{ij} \cdot \beta E_{kl} = e_{ij\alpha} + \beta E_{kl} + \alpha\beta E_{ij} \cdot E_{kl}.$$

Utilizando el Lema 3.9 obtenemos el resultado. □

Lema 3.11. *Sea M una matriz de tamaño $n \times n$, entonces $E_{ij}M$ es la matriz con todo ceros excepto la fila i, donde tiene la fila j de M.*

Además $e_{ij\alpha}M$ es la matriz que se obtiene al sumar a la fila i de M la fila j multiplicada por α.

Demostración. La primera frase es trivial. Para la segunda, observemos que $e_{ij\alpha}M = M + \alpha E_{ij}M$. □

Como consecuencia de estos lemas, podemos ver cómo son tanto los conmutadores de las matrices $e_{ij\alpha}$, como los corchetes de Lie de las matrices E_{ij}. Para no confundirnos vamos a denotar por $[\cdot,\cdot]_G$ los conmutadores y por $[\cdot,\cdot]_L$ los corchetes de Lie.

Lema 3.12.

$$[E_{ij},E_{kl}]_L = \begin{cases} 0 & si\ j \neq k \text{ y } l \neq i \\ E_{il} & si\ j = k \\ -E_{kj} & si\ l = i \end{cases}$$

Demostración. Por definición tenemos $[E_{ij},E_{kl}]_L = E_{ij}E_{kl} - E_{kl}E_{ij}$. Por los lemas anteriores, para que $E_{ij}E_{kl}$ sea distinto de 0, tenemos que tener $j = k$ y esto implica $i < l$ y por tanto i distinto de l, es decir $E_{kl}E_{ij} = 0$, y por tanto $[E_{ij},E_{kl}]_L = E_{il}$. Análogamente, si $i = l$ entonces $j \neq k$, luego $[E_{ij},E_{kl}]_L = -E_{kj}$. Finalmente, si $j \neq k$ y $l \neq i$, tenemos $[E_{ij},E_{kl}]_L = 0+0 = 0$. □

Lema 3.13.

$$[e_{ij\alpha},e_{kl\beta}]_G = \begin{cases} I_n & si\ j \neq k \text{ y } l \neq i \\ e_{il\alpha\beta} & si\ j = k \\ e^{-1}_{kj\alpha\beta} & si\ l = i \end{cases}$$

Demostración. Observemos que

$$e^{-1}_{ij\alpha} = I_n - \alpha E_{ij}.$$

Tenemos,

$$[e_{ij\alpha},e_{kl\beta}]_G = (I_n - \alpha E_{ij})(I_n - \beta E_{kl})(I_n + \alpha E_{ij})(I_n + \beta E_{kl}) =$$

$$= (I_n - \beta E_{kl} - \alpha E_{ij} + \alpha\beta E_{ij}E_{kl})(I_n + \beta E_{kl} + \alpha E_{ij} + \alpha\beta E_{ij}E_{kl}).$$

Notemos que $E_{ab}E_{cd} \neq 0$ si y sólo si $b = c$. Luego, si $j \neq k$ y $i \neq l$, todos los dobles productos que nos aparecen van a ser cero y por tanto se tiene $[e_{ij\alpha},e_{kl\beta}]_G = I_n + \beta E_{kl} + \alpha E_{ij} - \beta E_{kl} - \alpha E_{ij} = I_n$.

Si $j = k$, entonces $i \neq l$ y tenemos $[e_{ij\alpha},e_{kl\beta}]_G = I_n + \beta E_{kl} + \alpha E_{ij} + \alpha\beta E_{il} - \beta E_{kl} - \alpha E_{ij} - \alpha\beta E_{il} + \alpha\beta E_{il} = I_n + \alpha\beta E_{il} = e_{il\alpha\beta}$.

Finalmente, si $l = i$, entonces $[e_{ij\alpha},e_{kl\beta}]_G = I_n + \beta E_{kl} + \alpha E_{ij} - \beta E_{kl} - \alpha\beta E_{kj} - \alpha E_{ij} = I_n - \alpha\beta E_{kj} = e^{-1}_{kj\alpha\beta}$. □

Notación. Sea $1 \leq s \leq n-1$. Denotamos por N_s al conjunto

$$\left\{ \left. \begin{pmatrix} 1 & \overbrace{0\cdots0}^{s-1} & \overbrace{a_{1s+1}\cdots a_{1n}}^{n-s} \\ & & \ddots \quad a_{n-s\,n} \\ & & 0 \\ & \ddots & \vdots \\ & & 0 \\ & & 1 \end{pmatrix} \right| \; a_{ij} \in R \right\}$$

Para $s = n$ consideramos $N_n = 1$. Se puede ver $G = N_1 \supseteq N_2 \supseteq \cdots \supseteq N_{n-1} \supseteq 1 = N_n$.

Lema 3.14. *Sea $1 \leq s \leq n-1$, entonces:*

1. *N_s está generado por X_s*

2. *X_s es igual al conjunto de los conmutadores simples no triviales de longitud mayor o igual que s en los elementos de X_1. Además, todo conmutador simple de longitud $\geq n$ es igual a I_n*

3. *$N_s = \gamma_s(G)$ para $1 \leq s \leq n$*

Demostración. Para ver 1) vamos a utilizar el Lema 3.11. Primero, vamos a comprobar que una matriz cualquiera de N_s se puede formar a partir de la identidad sumando filas multiplicadas por un escalar. Sea $M \in N_s$. Partimos de I_n, la idea es ir añadiendo ordenadamente filas multiplicadas por escalares de manera que se vayan formando las entradas de M. Sea $a_{1,s+1}$ el elemento $\{1,s+1\}$ de M, por el Lema 3.11 se obtiene que el producto $e_{1s+1a_{1,s+1}}I_n$ es igual a la matriz identidad pero con el elemento $a_{1,s+1}$ en la posición $\{1,s+1\}$. Para añadir $a_{1,s+2}$ bastará multiplicar $e_{1s+2a_{1,s+2}}$ por la matriz obtenida anteriormente. Procedemos así hasta tener una matriz cuya primera fila es igual a la de M. Luego se sigue con la siguiente fila, de manera que la matriz que resulta es exactamente M. Por tanto, M es producto de $e_{ij\alpha}$ para algunos i,j,α. De aquí se deduce que N_s está generado por X_s. A la inversa, notemos que un producto arbitrario de elementos de X_s está en N_s.

Veamos 2), procedemos por inducción sobre s. Para $s=1$ es trivial. Suponemos, por hipótesis de inducción que X_{s-1} es el conjunto de los conmutadores simples no triviales de longitud mayor o igual que $s-1$ de elementos de X_1.

Sea $e_{pq\alpha} \in X_s$, luego $q-p \geq s$ y por tanto $q-1-p \geq s-1$. Esto implica $e_{pq-1\alpha} \in X_{s-1}$, es decir, $e_{pq-1\alpha}$ es un conmutador de longitud mayor o igual que $s-1$ de elementos de X_1. Notemos que por el Lema 3.13 se tiene $e_{pq\alpha} = [e_{pq-1\alpha}, e_{q-1q}]_G$. Además $e_{q-1q,1} \in X_1$, luego $e_{pq\alpha}$ es un conmutador de longitud s en X_1. Por tanto se tiene que X_s está contenido en el conjunto formado por los conmutadores simples de longitud mayor o igual que s en X_1.

Sea $g \neq 1$ un conmutador simple de longitud s en los elementos de X_1, luego g es de la forma $[h,x]_G$ siendo $x \in X_1$ y h un conmutador simple de longitud $s-1$ que por hipótesis de inducción está en X_{s-1}. Por tanto, $g = [h,x]_G = [e_{ij\alpha}, e_{kl\beta}]_G$ y los índices i,j,k,l cumplen $j-i \geq s-1$ y $l-k \geq 1$, es decir $j-i+l-k \geq s$.

Si $j=k$ se tiene que $[e_{ij\alpha}, e_{kl\beta}]_G = e_{i,l,\alpha\beta}$, como $l-i \geq s$, g está en X_s.

Si $i=l$ se tiene que $[e_{ij\alpha}, e_{kl\beta}]_G = e^{-1}_{k,j,\alpha\beta} = e_{kj-\alpha\beta}$, como $j-k \geq s$, g está en X_s. Como $g \neq 1$, estas son las únicas posibilidades que tenemos que considerar. Luego X_s está formado por lo conmutadores no triviales de longitud $\geq s$ de elementos de X_1.

Finalmente, sea g un conmutador simple de longitud n en X_1. Entonces g es de la forma $g = [x_1,x_2]_G$ con x_1 conmutador de longitud $n-1$ y $x_2 \in X_1$. Luego, $x_1 \in X_{n-1}$, es decir $x_1 = e_{ij\alpha}$ con $j-i \geq n-1$. Como $1 \leq i < j \leq n$, se tiene $i=1$ y $j=n$, por lo tanto, $x_1 = e_{1n\alpha}$. También sabemos que $x_2 = e_{kl\beta}$ con $1 \leq k < l \leq n$, luego $n \neq k$ y $l \neq 1$, por tanto, por el Lema 3.13 se tiene $g = [x_1,x_2]_G = I_n$. Análogamente pasará con los conmutadores simples de longitud mayor que n.

3) es consecuencia de 1) y 2) por el Lema 1.33. □

Teorema 3.15. *$UT_n(R)$ es nilpotente.*

Demostración. Basta aplicar el Lema 3.14. □

Observación 3.16. En realidad la demostración sirve para cualquier anillo conmutativo R que tenga 1.

A continuación, vamos a ver una serie de resultados que nos permitirán probar que la $\mathbb{Q}$-álgebra de Lie asociada a $UT_n(\mathbb{Z})$ es el álgebra $nt_n(\mathbb{Q})$ de las matrices null-triangulares. Para empezar vamos a determinar la $\mathbb{Q}$-álgebra de Lie asociada a la serie descendente de $UT_n(\mathbb{Z})$ y $UT_n(\mathbb{Q})$.

Definición 3.17. Definimos

$$L_s(R) = \left\{ \left(\begin{array}{ccccc} \overbrace{0\cdots0}^{s} & * & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & 0 \\ & & & & * \\ & & & & 0 \\ & & & & \vdots \\ & & & & 0 \end{array} \right) \middle| * \in R \right\} \text{ para } s = 1,\ldots,n-1 \text{ y } L_n(R) = 0.$$

Por simplicidad ponemos L_s en lugar de $L_s(R)$. Tenemos que L_s es un R-módulo libre, es decir, si $R=\mathbb{Z}$ es un grupo abeliano libre y si $R=K$ con K cuerpo entonces L_s es un K-espacio vectorial. En ambos casos L_s tiene base E_{ii+s}, $1\leq i\leq n-s$.

Lema 3.18. *$L=nt_n(\mathbb{Q})=L_1\bigoplus\cdots\bigoplus L_{n-1}$ es un álgebra de Lie graduada (K-álgebra si $R=K$)*

Demostración. Es suficiente ver que $[L_s,L_t]_L\subseteq L_{s+t}$, para ello basta probarlo para los elementos de la base, luego consideramos

$$[E_{ii+s},E_{jj+t}]_L=\begin{cases}E_{ii+s+t} & \text{si } i+s=j\\ -E_{jj+t+s} & \text{si } j+t=i\\ 0 & \text{en otro caso}\end{cases}$$

por tanto, en todos los casos está en L_{s+t}. □

Lema 3.19. *Sea $G=UT_n(R)$ con $R=\mathbb{Z}$ ó un cuerpo K, entonces $\gamma_s(G)/\gamma_{s+1}(G)\cong L_s(R)$ para $1\leq s\leq n-1$ y el corchete de Lie inducido por los conmutadores de G es precisamente $[\cdot,\cdot]_L$.*

Demostración. Notemos que $\gamma_s(G)/\gamma_{s+1}(G)$ es un R-módulo libre generado por las clases $e_{ii+s}+\gamma_{s+1}(G)$ con $1\leq i\leq n-s$. Consideramos la aplicación

$$\begin{array}{rccc}\varphi: & \gamma_s(G)/\gamma_{s+1}(G) & \longrightarrow & L_s\\ & e_{ii+s}+\gamma_{s+1}(G) & \longmapsto & E_{ii+s}\end{array}$$

Entonces φ es una biyección entre bases y por tanto induce un isomorfismo. Además

$$\varphi([e_{ii+s}+\gamma_{s+1}(G),e_{jj+t}+\gamma_{t+1}(G)]_{L(G)})=\varphi([e_{ii+s},e_{jj+t}]_G+\gamma_{s+t+2}(G))=\begin{cases}0 & \text{si } j\neq i+s, i\neq j+t\\ E_{ij+t} & \text{si } j=i+s\\ -E_{ji+s} & \text{si } j+t=s\end{cases}$$

Por otro lado,

$$[\varphi(e_{ii+s}+\gamma_{s+1}(G)),\varphi(e_{jj+t}+\gamma_{t+1}(G))]_{L(G)}=[E_{ii+s},E_{jj+t}]_L=\begin{cases}E_{ij+t} & \text{si } i+s=j\\ -E_{ji+s} & \text{si } j+t=s\\ 0 & \text{si } j\neq i+s, i\neq j+t\end{cases}$$

□

Lo que probamos en estos dos últimos lemas es que el álgebra de Lie $nt_n(\mathbb{Q})$ es graduada y que además es el álgebra de Lie asociado a $UT_n(R)$ con $R=\mathbb{Z}$ o un cuerpo K.

3.4. La correspondencia de Mal'cev

Una de las ventajas de la *correspondencia de Mal'cev* es que podemos traspasar resultados y propiedades de forma explícita entre la teoría de grupos y la de álgebras de Lie. Las álgebras de Lie son lineales y esto hace más sencillos de resolver algunos problemas. Al contrario, los grupos actúan en espacios y esto permite probar algunos resultados de forma geométrica. Esta asociación permite, a veces, aprovechar las ventajas de las dos estructuras.

La *correspondencia de Mal'cev* es una aplicación entre el grupo $UT_n(\mathbb{Q})$ y el álgebra de Lie $nt_n(\mathbb{Q})$ que se puede utilizar para asociar una $\mathbb{Q}$-álgebra de Lie nilpotente a cada grupo nilpotente finitamente generado (aunque no veremos todos los detalles de esta asociación).

Sea $A=I_n+B\in UT_n(\mathbb{Q})$ con $B\in nt_n(\mathbb{Q})$, se define

$$\begin{array}{rccc}\log: & UT_n(\mathbb{Q}) & \longrightarrow & nt_n(\mathbb{Q})\\ & A & \longmapsto & \log A=B-\frac{1}{2}B^2+\cdots+(-1)^n\frac{B^{n-1}}{n-1}\end{array}$$

Sea $C \in nt_n(\mathbb{Q})$ se define,

$$\begin{array}{rccl} \exp: & nt_n(\mathbb{Q}) & \longrightarrow & UT_n(\mathbb{Q}) \\ & C & \longmapsto & \exp C = I_n + C + \dfrac{C^2}{2!} + \cdots + \dfrac{C^{n-1}}{(n-1)!} \end{array}$$

Estas aplicaciones son inversas una de la otra y por tanto son biyecciones. Para verlo, observemos que si $D \in nt_n(\mathbb{R})$, entonces $D^n = 0$. Por tanto tenemos el desarrollo en serie de potencias de las funciones log y exp y basta tener en cuenta que exp $(\log(x)) = x$ y $\log(\exp(x)) = x$.

Definición 3.20. Sea $V \subseteq nt_n(\mathbb{Q})$ un subconjunto. Denotamos por $\mathbb{Q}V$ el subespacio generado por V. Si V es cerrado para el corchete de Lie de $nt_n(\mathbb{Q})$, entonces $\mathbb{Q}V$ es una $\mathbb{Q}$-álgebra de Lie.

Solo hemos definido esta correspondencia para el grupo $UT_n(\mathbb{Q})$ y el álgebra $nt_n(\mathbb{Q})$. Sin embargo se puede aplicar a cualquier grupo nilpotente finitamente generado y a cualquier álgebra nilpotente finitamente generada gracias a los dos resultados siguientes cuya demostración queda fuera del objetivo de este trabajo:

Teorema 3.21. *[3, Capítulo 6 - Teorema 2] Sea $G \leq UT_n(\mathbb{Q})$ un subgrupo y sea* $\log(G) = \{\log(A) \mid A \in G\}$. *Entonces $\mathbb{Q}\log(G)$ es un subanillo de Lie de $nt_n(\mathbb{Q})$. Al contrario, si $L \leq nt_n(\mathbb{Q})$ es una subálgebra de Lie, entonces* exp $(\mathbb{Q}L) \leq UT_n(\mathbb{Q})$ *es un subgrupo.*

Observación 3.22. Sea $G \leq UT_n(\mathbb{Q})$, entonces el álgebra $L_{\mathbb{Q}}(G)$ es un álgebra de Lie graduada. En cambio, $\log(G) \subseteq nt_n(\mathbb{Q})$ es un álgebra de Lie no necesariamente graduada.

Proposición 3.23. *[3, Capítulo 5 - Teorema 2] Sea G un grupo nilpotente finitamente generado libre de torsión, entonces G es isomorfo a un subgrupo de $UT_n(\mathbb{Z})$.*

Teorema 3.24. *[8][9](Teorema de Ado-Iwasawa) Toda K-álgebra de Lie de dimensión finita es un álgebra de Lie de matrices en K con $[\cdot,\cdot]$ el corchete de Lie de las matrices.*

Una álgebra nilpotente finitamente generada es de dimensión finita y además en ese caso, es isomorfa a un subálgebra de $nt_n(K)$.

Definición 3.25. Sea $G \leq UT_n(\mathbb{Q})$, la *complección de Mal'cev* de G es el grupo

$$\hat{G} := \exp\,(\mathbb{Q}\log(G)) \leq UT_n(\mathbb{Q})$$

Notemos que $G \leq \hat{G}$.

Veamos en un ejemplo cómo funciona esta correspondencia.

Ejemplo 3.26. Sea

$$S = \left\{ \left. \begin{pmatrix} 1 & 0 & \cdots & 0 & a_1 \\ & \ddots & \ddots & \vdots & a_2 \\ & & \ddots & 0 & \vdots \\ & & & \ddots & a_{n-1} \\ 0 & & & & 1 \end{pmatrix} \right| a_i \in \mathbb{Z} \right\}$$

notar que $S \leq UT_n(\mathbb{Z})$. Se observa fácilmente que S está generado como grupo por matrices de la forma $e_{in} = I_n + E_{in}$ con $1 \leq i \leq n-1$.

Luego tenemos $E_{in}^2 = 0$ ya que $i < n$ y por tanto se tiene $\log(e_{in}) = E_{in}$. Estas matrices generan un $\mathbb{Q}$-espacio que está contenido en $\mathbb{Q}\log S$, que a su vez está contenido en $nt_n(\mathbb{Q})$.

Ejemplo 3.27. Sea

$$L =_{\mathbb{Q}} \langle x_1, x_2, x_3, x_4, x_5 | [x_1, x_3] = x_4, [x_1, x_4] = x_5, [x_2, x_3] = x_5 \rangle$$

Se puede ver en [7] que L no es isomorfa a grad(L). Además L cumple lo siguiente: Existe G grupo nilpotente tal que: grad$(L) = L_{\mathbb{Q}}(G)$, $L = \log(G)$. Como $L \neq$ grad(L), se deduce que log $(G) \neq L_{\mathbb{Q}}(G)$

Bibliografía

[1] ARTURO MAGIDIN, https://mathoverflow.net/questions/44269/commutator-subgroup-does-not-consist-only-of-commutators/44276#44276

[2] E.I. KHUKHRO, *p-Automorphisms of Finite p-Groups*, London Mathematical Society Lecture Note Series 246, Cambridge University Press, 2004.

[3] DANIEL SEGAL, *Polycyclic groups*, Cambridge tracts in mathematics. Cambridge University Press, 2004.

[4] KIYOSHI IGUSA, *Solvable groups*, http://people.brandeis.edu/~igusa/Math101b/solv.pdf, disponible en http://people.brandeis.edu/~igusa/Math101b.

[5] DEREK J.S. ROBINSON, *Graduate Texts in Mahtematics, A course in the Theory of Groups*, 2.ª ed., Editorial Board, 1996.

[6] WOLFGANG ZILLER, *Lie groups*, https://www.math.upenn.edu/~wziller/math650/LieGroupsReps.pdf, disponible en https://www.math.upenn.edu/~wziller/.

[7] YVES CORNULIER *Gradings on Lie algebras, systolic growth, and cohopfian properties of nilpotent groups*, Bulletin de la Société mathématique de France 144(4):693-744 (2016).

[8] *Ado's theorem*, https://terrytao.wordpress.com/2011/05/10/ados-theorem/

[9] *Iwasawa's theorem*, http://www.math.clemson.edu/~jimlb/CourseNotes/iwasawa.pdf