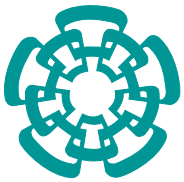


Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Matemáticas

El Grupo de Nottingham

Tesis que presenta

Jesus Angel Lara Rivera

para obtener el Grado de
Maestro en Ciencias
en la Especialidad de
Matemáticas

Director de Tesis: Dr. Jacob Mostovoy

Ciudad de México, Julio 2017

AGRADECIMIENTOS

A mi familia, mis padres Angel Lara e Ines Rivera y mi hermano Carlos Eduardo; a ellos por todo su amor, cariño, apoyo, enseñanzas, en fin, simplemente gracias por todo.

A mis compañeros y amigos del posgrado con los que he pasado grandes y maravillosos momentos, en especial a Rodo, Isidro, la Dra. Bárbara, Gustavo, Christo, Lalo, Fa y Raul. Sin ustedes, esto no hubiera sido divertido. Y a Isaac, gracias amigo por todo los consejos, la ayuda y los ratos que hemos pasado.

A mi gran amigo y paisano, Alejandro Flores; gracias por el apoyo que me has brindado en todo.

Un enorme agradecimiento a mi tutor, el Dr. Mostovoy, por su paciencia, guía y pláticas de las que siempre salía motivado a continuar.

Gracias también al personal administrativo del departamento; Adriana, Anabel, Norma y Roxana.

Un gran agradecimiento al Consejo Nacional de Ciencia y Tecnología (CONACYT) por el apoyo económico proporcionado que me permitió realizar mis estudios.

Y a ella, Laila F. Z. H.; por tanto amor y comprensión. Eres un gran pilar para mí. Gracias, Bonita.

Dedicado a mis padres
Angel Lara Angel
y
Ma. Ines Rivera Valencia

ÍNDICE GENERAL

RESUMEN

El grupo de series formales bajo la sustitución, también conocido como el grupo de Nottingham, es un objeto que ha llamado la atención de la comunidad matemática debido a varias propiedades interesantes que cumple. En este trabajo hablamos sobre este grupo, algunos resultados interesantes y unas generalizaciones.

ABSTRAC

The group of formal powers series under substitution, also know like Nottingham group, is a objet that has caught the attention of math community due many intersting properties that satisfies. In this work, we talk about this group, some interesting results and generalizations.

INTRODUCCIÓN

En este trabajo, abordaremos teoremas interesantes que se relacionan con el grupo de Nottingham. Por ejemplo, un resultado nos dice que en el grupo de Nottingham sobre $\mathbb{F}_p$, podemos encajar cierta familia de grupos. El primer resultado con ésta filosofía fue hecho por Johnson en [7]. El probó el siguiente resultado para $char(R) = 0$.

Proposición. $\mathcal{N}(t, R)$ *contiene una copia de* $\mathbf{F}_2$.

Aquí, $\mathcal{N}(t, R)$ denota el grupo de Nottigham sobre R, un anillo conmutativo con 1. Después Leedham-Green y Weiss probaron que cualquier p-grupo finito se encaja en $\mathcal{N}(t, \mathbb{F}_p)$ y con ayuda de esto, Camina ([1]) prueba el siguiente resultado.

Teorema. *Cualquier pro-p grupo con base numerable puede ser encajado en* $\mathcal{N}(t, \mathbb{F}_p)$ *como un subgrupo cerrado.*

La demostración del resultado de Johnson puede verse en [7] mientras que el resultado de Camina se analiza en el capítulo 3.

El trabajo se divide de la siguiente manera:

En el capítulo 1, abordamos la teoría de campos locales, grupos profinitos y una forma de asociar una estructura de Lie a un grupo cualquiera a traves de filtraciones, las cuales son funciones definidas en el grupo con imagen en los reales positivos.

En el capítulo 2, introducimos el objeto principal del trabajo, el grupo de Nottigham, el cual es un grupo de series formales donde la operación está dada por la composición de series con coeficientes en un anillo conmutativo con identidad R. Vemos algunas propiedades que cumple y calculamos la estructura de Lie asociada a una filtración que aparece de manera natural en el grupo. Esta filtración es llamada *profundidad*.

En el capítulo 3, presentamos uno de los resultados más interesantes sobre el grupo de Nottingham, el Teorema de Camina, ya mencionado arriba.

En el capítulo 4, desarrollamos tres ejemplo de generalizaciones al grupo de Nottigham y calculamos las estructuras de Lie asociadas a una filtración que generalizada la *profundidad* a estos casos.

Capítulo 1
Preliminares

En este capítulo veremos algunos resultados preliminares necesarios para el desarrollo de este trabajo.

1.1 Campos Locales

Los campos con los que trabajaremos son los $\mathbb{F}_p((X))$ los cuales son campos locales. Por ello, en esta sección abordaremos la teoria necesaria de campos.

Sea F un campo y sea $\nu : F^* \to \mathbb{Z}$ un epimorfismo de grupos. Ponemos $\nu(0) = +\infty$.

Definición 1.1. *Si ν cumple*

$$\nu(\alpha + \beta) \geq \text{mín}\{\nu(\alpha), \nu(\beta)\}, \tag{1.1}$$

decimos que ν es una valuación discreta en F y a F lo llamamos campo de valuación discreta.

Observación 1.1. *Hay una definición más general para una valuación discreta en la que se pide que la imagen de ν sea un subgrupo aditivo de $\mathbb{R}$ que sea isomorfo a $\mathbb{Z}$ (por ejemplo $p^{-1}\mathbb{Z}$). Sin embargo, siempre podemos regresar al caso de la definición haciendo la composición de ν con el isomorfismo.*

Por cómo se define ν tenemos la siguiente proposición:

Proposición 1.1. *Sean*

$$A = \{x \in F \mid \nu(x) \geq 0\} \tag{1.2}$$

y

$$I = \{x \in F \mid \nu(x) > 0\} \tag{1.3}$$

Entonces A es un anillo e I un ideal.

Demostración. Tenemos que $\nu(xy) = \nu(x) + \nu(y)$, entonces A es cerrado bajo el producto y por la desigualdad (1.1) es cerrado bajo la suma. Nótese que $\nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1}) = \nu(x) - \nu(x) = 0$, con lo que podemos ver que $\nu(-1) = 0$. Con esto tenemos que $\nu(x) = \nu(-x)$, es decir, hay inversos aditivos en A.

Que I sea ideal se sigue de que ν es homomorfismo y la desigualdad (1.1). □

Nótese que $a \in A$ es invertible si y sólo si $\nu(a) = 0$; con esto tenemos:

1. Si $\pi \in A$ es tal que $\nu(\pi) = 1$, entonces $I = \langle \pi \rangle$: si $\nu(x) = \nu(y)$, entonces xy^{-1} en F tiene valuación 0. Así, existe un $u \in ker(\nu)$ tal que $x = uy$. En particular $u\pi^{\nu(x)} = x$. Esto prueba $I = \langle \pi \rangle$.
2. I es un ideal maximal de A. Más aún, es el único ideal maximal y A es un dominio de ideales principales. Para cada ideal J de A, existe un $s \in J$ de valuación mínima. Tómese s como generador y con el argumento anterior se tiene que $J = \langle s \rangle$. En particular, tomando como generador a $\pi^{\nu(s)}$ tenemos que todo ideal de A es de la forma $\langle \pi^n \rangle$ y está contenido en I.
3. I es el único ideal primo en A. Esto por la forma de los ideales.

Definición 1.2. *Definimos*

- *Un anillo de valuación discreta como un dominio de ideales principales Noetheriano que tiene un único ideal primo.*
- *El campo residual de F como $k_\nu = A/I$.*
- *Un elemento uniformizante (o primo) π como un generedor de I.*

Observación 1.2. *Tenemos lo siguiente*

- *A es anillo de valuación discreta con I ideal maximal.*
- *Cualquier elemento uniformizante es no nilpotente.*
- *Dado un anillo de valuación discreta A tenemos una función ν asociada la cual definimos como $\nu(x) = n$ si y sólo si $x = \pi^n u$, con u invertible. Esta función se extiende a una valuación discreta en $Q(A)$ (el campo de cocientes de A) como $\nu(a/b) = \nu(a) - \nu(b)$. Más aún, si K es un campo de valuación discreta con A_K anillo de valuación discreta, entonces $Q(A_K) = K$ con la misma valuación.*

Los campos (o anillos) de valuación discreta los podemos dotar de una topología asociada a la valuación. La topología en F es la I-ádica; esto es, $\{I^n\}$ forma sistema de bases para las vecindades de 0. Con esto, podemos definir convergencia y sucesiones de Cauchy.

Definición 1.3. *Sea $S = \{x_i\}$ una sucesión en F.*

1. *Decimos que S converge a $x \in F$ si para todo $n \in \mathbb{N}$, existe un $M \in \mathbb{N}$, tal que si $j > M$, entonces $x_j - x \in I^n$.*
2. *Decimos que S es una sucesión de Cauchy si para todo $n \in \mathbb{N}$, existe un $m \in \mathbb{N}$, tal que si $j, i > m$, entonces $x_i - x_j \in I^n$.*

Observación 1.3. *También podemos darle topología a F mediante el valor absoluto dado por ν. Defini-*

mos el valor absoluto asociado a ν como $|x| = a^{\nu(x)}$, para algún $a \in (0,1)$. Lo importante de esto es que ambas topologías coinciden, la topología dada por $|\cdot|$ y la I-ádica. Esto puede verse por cómo se define el valor absoluto, ya que $|x-y| < \epsilon$, implica $|x-y| = a^{\nu(x-y)} < \epsilon$, lo que hace que $x - y \in I^N$, para N tal que $\nu(x-y) > N$ y $\epsilon > a^N$.

Proposición 1.2. *$|\cdot|$ como arriba es un valor absoluto en F.*

La demostración se sigue de la definición de valuación (1.1 (p. 1)), salvo la desigualdad triangular, la cual pasa primero por la siguiente desigualdad.

Definición 1.4. *Un valor absoluto que cumple $|x+y| \leq \sup\{|x|, |y|\}$ se llama no-arquimediano o ultramétrico.*

El valor absoluto $|\cdot|$, asociado a ν, es ultramétrico en F. Esto por la propiedad 1) de la Definición 1.1 (p. 1).

Si F es completo respecto a la topología dada por $|\cdot|$ (o la I-ádica), decimos que es un campo de valuación discreta completo.

Proposición 1.3. *La ν está unicamente determinada en un campo de valuación discreta completo.*

Esto se sigue del siguiente lema.

Lema 1.1. *Dos topologías en F definidas por dos valuaciones discretas ν_1, ν_2 coinciden si y sólo si $\nu_1 = \nu_2$.*

Demostración. Si las valuaciones son iguales, claramente se tiene que las topologías lo son.

Supongamos que las topologías son iguales. Sean π_1 y π_2, dos elementos uniformizantes para ν_1 y ν_2, respectivamente. Nótese que $\alpha^n \to 0$ si y sólo si $\nu(\alpha) > 0$. Entonces, $\nu_1(\alpha) > 0$ si y sólo si $\nu_2(\alpha) > 0$. Por ello, $\nu_1(\pi_2) \geq 1$ y $\nu_2(\pi_1) \geq 1$. Si $\nu_1(\pi_2) > 1$, tenemos $\nu_2(\pi_1\pi_2^{-1}) > 0$. Luego, $\nu_1(\pi_1\pi_2^{-1}) > 0$; esto es, $\nu_1(\pi_2) < 1$. Así, $\nu_1(\pi_2) = 1$. Por lo tanto, $\nu_1 = \nu_2$. □

Definición 1.5. *Un campo local es un campo de valuación discreta completo donde el campo residual es finito.*

Es un hecho que los campos con los que estamos trabajando, dada la topología $I-$ádica, son localmente compactos.

Proposición 1.4. *Sea K un campo de valuación discreta. K es localmente compacto si y sólo si k_v es finito y K completo; es decir, es campo local.*

Demostración. Primero, nótese que I^n es cerrado para cada n. Para ver esto, sea $\{a_j\}$ una sucesión en I^n y supongamos que converge a a. Esto singnifica que existe un N tal que $a_i - a \in I^n$, para todo $i > N$. Como $a_i \in I^n$ se tiene que $a \in I^n$. Esto incluye a $I^0 = A$.

($\Rightarrow$) Si K es localmente compacto, entonces es completo. Como sabemos I^n forma un sistema de vecindades para cero. Entonces I^n es compacto para algún n. Multiplicando por π^{-n} tenemos $\pi^{-n}(I^n) = A$, lo que muestra que A es compacto. Así A/I es discreto (si p es la proyección al cociente, entonces $p^{-1}(a) = a + I$ es abierto) y compacto, por ello finito.

($\Leftarrow$) De la Observación 1.3 (p. 2) las topologías coinciden. Por cómo se define la completación vía la topología I-ádica, tenemos que si A es el anillo de valuación discreta de K, $\varprojlim A/I^n = \widehat{A}$ es la cerradura de A en $\widehat{K}$. Como $K = \widehat{K}$ por ser completo y A cerrado, entonces $\widehat{A} = A$. Además, A/I^n es finito pues $A/I^n = \sum_{j=1}^{j-1} \pi^j A/I$; es decir, $\widehat{A}$ es límite inverso de conjuntos finitos, entonces es compacto[1]. Así K es locamente compacto.

□

Teorema 1.1. *Cualquier campo local de caracteristica p es isomorfo a un campo de series formales de potencias en una variable con coeficientes en un campo finito.*

La demostración puede verse en [11] capítulo I, sección 4, Teorema 8.

En la demostración se obtiene más, ya que las series de potencias a las que es isomorfo el campo tiene coeficientes en el campo residual.

Sea L/F una extensión finita de un campo de valuación discreta completo F con valuación ν_F. Tenemos el siguiente resultado sobre la extensión y la valuación ν_F.

Proposición 1.5. *La valuación ν_F puede extenderse de manera única a una valuación discreta en L, ν_L de tal forma que L es completo. Además, el campo residual de F se puede ver como un subcampo del campo residual de L.*

La demostración puede verse en Serre [10] capítulo 2 Proposición 3.

La siguiente definición la usaremos más adelante.

Definición 1.6. *Decimos que la extensión L/F es totalmente ramificada si $k_L = k_F$.*

1.1.1 EJEMPLOS

Sólo daremos los dos ejemplos más importantes dentro de la teoria de campos locales.

En un campo local el valor absoluto se llama normalizado si $|x| = q^{-\nu(x)}$ con q la cardinalidad del campo residual. Aquí tomaremos los ejemplos normalizados.

[1] Se ve en la sección de grupos profinitos.

EL CAMPO $\mathbb{Q}_p$

Consideremos p un primo fijo. Definimos sobre cada número racional $\frac{a}{b} \in \mathbb{Q}$, la valuación ν_p como

$$\nu_p\left(\frac{a}{b}\right) = n, \text{ si } \frac{a}{b} = p^n \frac{a'}{b'} \text{ con } (a', p) = (b', p) = 1.$$

Proposición 1.6. *ν_p definida como arriba es una valuación en $\mathbb{Q}$.*

El anillo de valuación discreta asociado a ν_p, en $\mathbb{Q}$, es la localización $\mathbb{Z}_{(p)}$.

Observación 1.4. *$\mathbb{Q}$ no es completo respecto a ν_p. Denotemos por $|x|_p$ la norma dada por ν_p. Para ver que no es completo, considere a entero, con $1 < a < p-1$, y defina $x_n = a^{p^n}$.*

1. *x_n es de Cauchy: por el pequeño teorema de Fermat vemos que $a^p - a = pm_1$, $a^{p^2} - a^p = pm_2, \ldots$, $a^{p^r} - a^{p^{r-1}} = pm_r$. Sumando obtenemos $a^{p^r} - a = pm$, o $a^{p^r} = pm + a$. Entonces, elevando a la p^N, tenemos*

$$a^{p^{N+r}} - a^{p^N} = (pm)^{p^N} + \sum_{i=1}^{p^N} \binom{p^N}{i} (pm)^{p^N - i} a^i. \tag{1.4}$$

   Cada sumando aporta almenos N potencias de p. Entonces, $|a^{p^{N+r}} - a^{p^N}| \leq p^{-N}$.

2. *x_n no converge: supongamos que si y sea x el límite. Entonces,*

$$x = \lim x_j = \lim x_{j+1} = \lim x_j^p = (\lim x_j)^p = x^p. \tag{1.5}$$

   Además $|x-a|_p = p^{-\nu(x-a)} < p^{-\nu(a)} = 1$. Es claro que si $|y|_p < 1$, $p|y$. Así $p|x-a$. Por (1.5), $x = 1$ (no puede ser cero pues $|x_n|_p = 1$). Sea $1 - a = pb$. Escribamos $a = pb' + 1$. Si $b' > 0$, entonces $p \leq a$. Si $b' \leq 0$, entonces $a \leq 1$. Ambas contradicciones.

La completación de $\mathbb{Q}$ respecto a esta valuación es el campo de los números $p-$ádicos denotado $\mathbb{Q}_p$. El anillo de valuación discreta asociado a $\mathbb{Q}_p$ es el anillo de los enteros $p-$ádicos denotado por $\mathbb{Z}_p$.

De este ejemplo podemos ver que no hay una única manera de completar un campo de valuación discreta.

EL CAMPO $\mathbb{F}_p((X))$

Consideremos $K = \mathbb{F}((X))$, las series de Laurent de cola finita con coeficientes en $\mathbb{F}_p$. K es un campo de valuación discreta. La valuación está dada como sigue: Si $a \in K$, entonces $a = \sum_{j \geq n} a_j X^j$, con $a_n \neq 0$. Definimos $\nu(a) = n$.

Proposición 1.7. *K con ν es un campo de valuación discreta.*

Esta se sigue sólo de la definición de producto en K. Nótese que $A = \mathbb{F}_p[[X]]$ y por la Observación 1.2 (p. 2) $Q(A) = \mathbb{F}_p((X))$.

A diferencia del ejemplo anterior, K es completo. Por ello ν es la única valuación en la que K es completo.

1.1.2 OBSERVACIONES SOBRE $\mathbb{F}_p((X))$

Denotemos, como antes, $K = \mathbb{F}_p((X))$ y $A = \mathbb{F}_p[[X]]$. Sean $H(\mathbb{F}_p) = \{\sum_{j\geq 1} a_j X^j \mid a_1 \neq 0\}$ y $Aut(A)$ el grupo de automorfismos de A. Es fácil ver que $H(\mathbb{F}_p)$ es un grupo bajo la sustitución[2].

Proposición 1.8. $H(\mathbb{F}_p) \cong Aut(A)$.

Demostración. Que los elementos de $H(\mathbb{F}_p)$ son automorfismos de A se prueba en el capítulo siguiente[3]. Sea $f \in Aut(A)$. Entonces, f queda completamente determinado por su acción en X. Como $f(X) \in A$, se tiene $f : X \mapsto \sum_{j\geq 1} f_j X^j$. Si $f_1 = 0$, entonces f es no es invertible, pues el inverso tendría que mandar $X \mapsto \sum g_i X^i$, pero $f^{-1} \circ f : X \mapsto cX^2 + \ldots$; es decir, mandaria a algo que por lo menos empieza en la potencia cuadrada. Así $f_1 \neq 0$. □

Sea $Aut(K)$ el grupo de automorfismos de K, entonces

Proposición 1.9. $Aut(K) \cong Aut(A)$.

Demostración. Por la Observación 1.2 (p. 2) $Q(A) = K$. Entonces todo automorfismo de A puede extenderse a uno en K. Si $f \in Aut(K)$ entonces podemos restringir a $f|_A$ y como los automorfismos preservan la valuación, entonces $f|_A(x) \in A$ (se muestra abajo). □

Sea $f \in Aut(K)$ y defina ν_f como $\nu_f(x) = \nu(f(x))$. Entonces, ν_f es una valuación en K y por ser K completo tenemos que $\nu = \nu_f$ (Proposición 1.3 (p. 3)). Se sigue que f preserva la valuación, entonces $f^{-1}(I^n) = I^n$; es decir, f es continuo. Sea $Aut_c(K)$ el grupo de automorfismos continuos de K, por lo anterior tenemos

Proposición 1.10. $Aut_c(K) = Aut(K)$.

[2] La demostración es análoga a la de la Proposición 2.1 (p. 20).

[3] La demostración es análoga a la de inversos en la Proposición 2.1 (p. 20).

1.2 GRUPOS PROFINITOS Y PRO-p GRUPOS

El estudio de los grupos profinitos inicia en la Teoria de Galois: cuando uno trabaja con subextensiones finitas de una extension de Galois, uno observa que el grupo de Galois de la extensión puede construirse como límite inverso del sistema dado por los grupos de Galois de todas las subextensiones finitas de la extensión. Como se sabe, tales grupos son finitos. Grupos construidos como límites inversos de grupos finitos son llamados grupos profinitios. Todo lo visto en esta sección se puede consultar en [3].

1.2.1 GRUPOS PROFINITOS

Definición 1.7. *Un grupo topológico que es Hausdorff, compacto y donde los subgrupos abiertos forman una base para la topología se llama profinito.*

Observación 1.5. *Es claro que en un grupo topológico cualquier subgrupo que contiene un conjunto abierto es abierto. Así, la condición de que los subgrupos forman una base para las vecindades de 1 es equivalente a que cualquier conjunto abierto que contiene a 1 contiene un subgrupo abierto.*

Proposición 1.11. *Sea G un grupo profinito. Entonces:*

1. *Cualquier subgrupo abierto de G es cerrado, tiene índice finito en G y contiene un subgrupo normal abierto.*
2. *Un grupo cerrado es abierto si y sólo si es de índice finito.*
3. *La familia de todos los subgrupos abiertos de G intersectan en $\{1\}$.*
4. *Una sucesión en G converge si y sólo si es de Cauchy; es decir, G es completo.*

Una sucesión $\{g_j\}$ es de Cauchy en G si para cada $N \leq G$ abierto, existe un $n = n(N)$ tal que $g_i g_j^{-1} \in N$, para todo $i, j \geq n$.

Demostración.

1. Las clases laterales forman una cubierta abierta de G. Por compacidad se tiene el resultado.
2. La ida es por compacidad. El regreso, del hecho de que multiplicar es un isomorfismo en un grupo topológico.
3. Por compacidad y 1.
4. Por compacidad, existe una subsucesión convergente $\{g_{j_k}\}$. Sea g el límite. Sea N un subgrupo normal abierto de G. Entonces, la vecindad gN de g cumple que para todo n_1, $g_{j_k} \in gN$, para todo $k \geq n_1$. De la misma forma, existe un n_2 tal que $g_i \in g_j N$, para todo $i, j \geq n_2$. Tomando $n = \text{máx}\{n_1, j_{n_1}\}$, tenemos que que $g_i \in g_j N = gN$, para $i, j \geq n$.

□

Tenemos una segunda definición de grupo profinito, esta se basa en la construcción de límite inverso.

Sea $\{G_\alpha\}$ un sistema inverso de subgrupos finitos con la topología discreta. Entonces , $\prod G_\alpha$ tiene la topología producto y $\varprojlim G_\alpha$ se vuelve un grupo topológico.

Sea $\mathcal{G}$ una familia de subgrupos normales de G ordenados por la inclusión. Entonces, los cocientes $\{G/N \mid N \in \mathcal{G}\}$ forman un sistema inverso con las funciones definidas como $[a]_N \mapsto [a]_M$, tomar la clase del representante.

Proposición 1.12. *Si G es un grupo profinito, entonces, G es topologicamente isomorfo a $\varprojlim G/N$, donde el sistema es $\{G/N \mid N \triangleleft G$ abierto$\}$. A la inversa, el límite inverso de un sistema de grupos finitos es un grupo profinito.*

Demostración. Sea $D = \varprojlim G/N$. Tenemos una la función $J : G \to \prod G/N$, dada por $J : g \mapsto (gN)_N$. Como todos los subgrupos normales intersectan en 1 (Proposición 3 (p. 7)), esta es inyectiva. Tenemos $J(G) \leq D$. Sea $(g_N N) \in D$. Entonces cualquier colección finita de clases $g_N N$ tiene intersección no vacia. Como las clases son cerradas (N lo son) y son subconjuntos de un espacio compacto G, tenemos que existe $1 \neq g \in \cap_{N \triangleleft G} g_N N$, N abiertos. De donde $J(g) = (g_N N)$. Probaremos que J es continua.

Sean $M \triangleleft G$ abierto y

$$U(M) = \prod_{N \not\geq M} G/N \times \prod_{N \geq M} \{1\} \leq \prod G/N.$$

Entonces, los subgrupos $U(M) \cap D$ forman una base para las vecindades de 1 en D y para cada M, $J^{-1}(U(M)) = M$, el cual es abierto en G. Como una función continua y biyectiva entre un conjunto compacto y uno Hausdorff es un homeomorfismo, tenemos el resultado.

Para la inversa, consideremos una sistema inverso de grupos finitos $\{G_\alpha\}_{\alpha \in A}$, cada uno con la topología discreta. Entonces, $\prod G_\alpha$ es Hausdorff y por el teorema de Tychonoff es compacto. Si $1 \in U$ es un abierto, entonces contiene un conjunto de la forma

$$U(S) = \prod_{\alpha \notin S} G_\alpha \times \prod_{\alpha \in S} \{1\},$$

para $S \subset A$ finito, esto por cómo se define la topología producto. Esto prueba que $\prod G_\alpha$ es profinito. Todas las propiedades son heredables, sólo falta probar que $D = \varprojlim G_\alpha$ es cerrado.

Sea $\widehat{g} \in \prod G_\alpha - D$. Entonces existe un $\nu > \mu$ en A, tal que $\pi_{\nu\mu}(g_\nu) \neq g_\mu$. Así, $\widehat{g}U(\nu, \mu)$ es una vecindad abierta de $\widehat{g}$ en $\prod G_\alpha$ y $\widehat{g}U(\nu, \mu) \cap D = \emptyset$. De lo contrario tendríamos un $h = (h_\alpha)$ tal que $g_\mu = h_\mu = \pi_{\nu\mu}(h_\nu) = \pi_{\nu\mu}(g_\nu)$. Es decir, $\prod G_\alpha - D$ es abierto en $\prod G_\alpha$. □

EJEMPLO: LA COMPLETACIÓN PROFINITA

Sea G un grupo y A una familia de subgrupos normales de G con índice finito. Como antes, la familia $\{G/N \mid N \in A\}$ forma un sistema inverso de grupos finitos. Entonces,

$$\widehat{G}_A = \varprojlim_{N \in A} G/N,$$

es un grupo profinito. Nótese que la función natural $G \to \widehat{G}_A$ tiene como kernel $\bigcap_{N \in A} N = K$.

Proposición 1.13. *G/K se encaja como un subgrupo denso en $\widehat{G}_A$.*

$\widehat{G}_A$ es una completación profinita de G. Cuando A son todos los subgrupos normales de G con índice finito, decimos que $\widehat{G}_A$ es *la* completación profinita de G.

Un hecho que nos ayudará más adelante es el siguiente .

Proposición 1.14. *Si G es un grupo profinito finitamente generado*[4] *y $m \geq 1$ entero, entonces G tiene sólo un número finito de subgrupos de índice m.*

Demostración. Supongamos que G es topologicamente generado por d elementos. Entonces, tenemos a lo más $(m!)^d$ homomorfismos continuos de G en el grupo simétrico Σ_m (con la topología discreta). Si $H \leq G$ abierto tal que $[G : H] = m$, entonces la representación de la permutación de G en las clases laterales derechas de H es continua, y la imagen inversa de una permutación es la intersección de m conjuntos abiertos de la forma $x^{-1}Hy$ y H es exactamente la imagen inversa en G de un punto estabilizador en Σ_m. Entonces, no hay más que $m(m!)^d$ posibilidades para H. □

1.2.2 PRO-p GRUPOS

Los pro-p grupos son los grupos profinitos que nos interesan por el resultado principal del trabajo.

Definición 1.8. *Un pro-p grupo es un grupo profinito en el cual cualquier subgrupo abierto normal tiene índice una potencia de p.*

Observación 1.6. *De la definición vemos que todo subgrupo abierto tiene índice una potencia de p, por la Proposición 1.11 (p. 7).*

Como un pro$-p$ grupo es un grupo profinito, este se puede ver como límite inverso de grupos finitos, pero de grupos finitos particulares.

[4] En el caso de grupos topológicos decimos que un grupo G es generado por X si $G = \overline{\langle X \rangle}$

Proposición 1.15. *Un grupo topológico G es un pro$-p$ grupo si y sólo si G es topologicamente isomorfo a un límite inverso de $p-$grupos finitos.*

Demostración. Si G es un pro$-p$ grupo, entonces $G \cong \varprojlim G/N$ (1.12 (p. 8)), donde los N son subgrupos normales abiertos de G. Entonces tienen índice una potencia de p.

Para la inversa, supongamos que $G \cong \varprojlim_{\alpha \in A} G_\alpha$, con cada G_α $p-$grupo finito. Entonces, G es un grupo profinito (1.12 (p. 8)). Ahora, cualquier subgrupo abierto de G contiene un subgrupo de la forma

$$G(S) = G \cap \left(\prod_{\alpha \notin S} G_\alpha \times \prod_{\alpha \in S} \{1\} \right),$$

para algún $S \subset A$ finito. Como

$$[G : G(S)] | \prod_{\alpha \in S} |G_\alpha|,$$

esto implica que cualquier subgrupo abierto de G tiene índice igual a una potencia de p. □

EJEMPLOS

1. Los enteros $p-$ádicos $\mathbb{Z}_p$ forman un grupo profinito. Por cómo se define la completación en $\mathbb{Q}$, de ν_p, tenemos $\mathbb{Z}_p = \widehat{\mathbb{Z}_{(p)}} = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, es decir, son un pro$-p$ grupo.
2. La pro$-p$ completación se define como tomar la completación profinita para el conjunto de todos subgrupos normales con índice una potencia de p.
3. Sea X un conjunto finito no vacío. El pro$-p$ grupo libre en X se define como la pro$-p$ completación del grupo libre en X.[5]

Cerramos esta sección con unos resultados que usaremos más adelante.

Proposición 1.16. *Si G es pro$-p$ grupo finitamente generado, entonces todo sugrupo de índice finito en G es abierto.*

La demostración se puede ver en [3], Capítulo 1 Teorema 1.17.

Corolario 1.1. *Cualquier homomorfismo de grupos de un pro$-p$ grupo finitamente generado a un grupo profinito es continuo.*

[5]Este cumple con una propiedad unviersal, pero para ello necesitamos definir lo que se entiende como 1-convergencia en un grupo, la cual es esencial para definir el análogo de grupos libres en grupos profinitos. Pero para este caso es suficiente lo mecionado en el ejemplo.

Demostración. Sean G un pro$-p$ grupo finitamente generado, H un grupo profinito y $f : G \to H$ un homomorfismo de grupos. Sea $K \leq H$ un subgrupo abierto, entonces $f^{-1}(K)$ es un subgrupo de índice a lo más $[H : K]$ en G, así por la Proposición 1.16 $f^{-1}(K)$ es abierto en G. Como los subgrupos abiertos forman una base para las vacindades de 1 en H, entonces f es continuo. □

Y como corolario de este resultado tenemos

Corolario 1.2. *Si G es un pro-p grupo finitamente generado, cualquier automorfismo de G como grupo, es un automorfismo topológico.*

1.3 FILTRACIONES Y SERIES CENTRALES EN GRUPOS

Aquí estudiamos la forma de asociar una estructura de Lie a un grupo cualquiera.

Notación: Usamos la notación para los conmutadores $\mathbf{c}(a,b) = aba^{-1}b^{-1}$ (grupo), $[A,B] = AB - BA$ (álgebra) y en un álgebra de Lie denotamos el producto por $(x,y) \mapsto [xy]$. Para los subgrupos usamos $\mathbf{c}(H,L) = \langle\{\mathbf{c}(h,l)|h \in H, l \in L\}\rangle$, donde $\langle X\rangle$ es el subgrupo generado por X.

Definición 1.9. *Una filtración en un grupo G es una función $\omega : G \to \mathbb{R} \cup \{+\infty\}$ que satisface lo siguiente:*

1. $\omega(1) = +\infty$.
2. $\omega(g) > 0$ *para todo* $g \in G$.
3. $\omega(gh^{-1}) \geq \text{ínf}\{\omega(g), \omega(h)\}$.
4. $\omega(\mathbf{c}(g,h)) \geq \omega(g) + \omega(h)$.

Observación 1.7. *La condición 3) implica $\omega(g) = \omega(g^{-1})$. Lo cual se obtiene viendo que $\omega(x^{-1}) = \omega(1x^{-1}) \geq \omega(x) = \omega(1(x^{-1})^{-1}) \geq \omega(x^{-1})$.*

Para $r \geq 0$ definimos los siguientes subconjuntos de G:

- $G_r = \{g \in G \mid \omega(g) \geq r\}$
- $G_r^+ = \{g \in G \mid \omega(g) > r\}$

Observación 1.8. *$G_0 = G_0^+ = G$, para todo r se tiene que $G_r^+ \subset G_r$ y si $r \geq s$, entonces $G_r \subset G_s$ y $G_r^+ \subset G_s^+$; es decir, las sucesiones $\{G_r^+\}$ y $\{G_r\}$ son decrecientes.*

Proposición 1.17. *G_r y G_r^+ son subgrupos normales de G.*

Demostración. La condición 3) en la Definición 1.9 (p. 11) muestra que ambos son subgrupos de G (pues $\omega(gh^{-1}) \geq \text{ínf}\{\omega(g), \omega(h)\} \geq r$ (respectivamente $> r$)). Para ver que G_r es normal, tómese $g \in G$ y $h \in G_r$, entonces, por ser ω una filtración, tenemos

$$\omega(ghg^{-1}h^{-1}) \geq \omega(h) + \omega(g) \geq r + \omega(g) > r. \tag{1.6}$$

Así, $ghg^{-1}h^{-1} \in G_r^+$; esto es, $ghg^{-1} = xh \in G_r$, para algún $x \in G_r^+$. La misma cuenta muestra que G_r^+ es normal en G (al tomar $h \in G_r^+$ cambia $\geq$ por $>$ en la desigualdad central de (1.6 (p. 12))). □

Estos grupos nos ayudarán a formar los bloques con los que construiremos una estructura de Lie para G.

Definición 1.10. *Para $r \geq 0$, definimos*

$$\mathtt{gr}_{\omega,r}(G) = G_r / G_r^+, \tag{1.7}$$

$$\mathtt{gr}_{\omega}(G) = \sum_r \mathtt{gr}_{\omega,r}(G). \tag{1.8}$$

Observación 1.9. *$\mathtt{gr}_{\omega,r}(G)$ es un grupo abeliano. Además, si $\pi_r : G_r \to \mathtt{gr}_{\omega,r}(G)$, es la función cociente, entonces $\pi_r(h) = \pi_r(ghg^{-1})$, para todo $g \in G$.*
La demostración de la Proposición 1.17 (p. 11) mostró que $\mathbf{c}(g,h) \in G_r^+$, para todo $g \in G$ y todo $h \in G_r$, de esto se siguen ambos hechos.

Ahora consideraremos a $\mathtt{gr}_{\omega,r}(G)$ como $\mathbb{Z}-$módulo.

Proposición 1.18. *La función $c_{r,s} : G_r \times G_s \to G_{r+s}$, definida como $c_{r,s}(g,h) = \mathbf{c}(g,h)$, induce una función bilineal $\overline{c}_{r,s} : \mathtt{gr}_{\omega,r}(G) \times \mathtt{gr}_{\omega,s}(G) \to \mathtt{gr}_{\omega,r+s}(G)$, definida como $\overline{c}_{r,s}(g,h) = \pi_{r+s}(\mathbf{c}(g,h))$*

Antes de la demostración unas identidades que serán de utilidad.

Lema 1.2. *Para cualesquiera $g, h, x, y \in G$ se tiene:*

1) $\mathbf{c}(xy,z) = x\mathbf{c}(y,z)x^{-1}\mathbf{c}(x,z)$.

2) $\mathbf{c}(x,yz) = \mathbf{c}(x,y)y\mathbf{c}(x,z)y^{-1}$.

Demostración. 1) $\mathbf{c}(xy,z) = xyzy^{-1}x^{-1}z^{-1} = x(yzy^{-1}z^{-1})x^{-1}(xzx^{-1}z^{-1}) = x\mathbf{c}(y,z)x^{-1}\mathbf{c}(x,z)$

2) Del hecho $\mathbf{c}(y,x) = (\mathbf{c}(x,y))^{-1}$, obtenemos

$$\mathbf{c}(x,yz) = (\mathbf{c}(yz,x))^{-1} = (y\mathbf{c}(z,x)y^{-1}\mathbf{c}(y,x))^{-1} = \mathbf{c}(x,y)y\mathbf{c}(x,z)y^{-1}.$$

□

Regresando a la proposición:

Demostración. 1) $\bar{c}_{r,s}$ está bien definida: sean $\pi_r(g) = \pi_r(h)$ y $\pi_s(a) = \pi_s(b)$. Por el Lema 1.2 tenemos

$$\begin{aligned}
\pi_{r+s}(\mathbf{c}(g,a)) &= \pi_{r+s}(\mathbf{c}(xh,a)), \text{ donde } x = gh^{-1} \in G_r^+, \\
&= \pi_{r+s}(x\mathbf{c}(h,a)x^{-1}\mathbf{c}(x,a)), \\
&= \pi_{r+s}(x\mathbf{c}(h,a)x^{-1}) + \pi_{r+s}(\mathbf{c}(x,a)), \ \mathtt{gr}_{r+s}(G) \text{ es abeliano}, \\
&= \pi_{r+s}(\mathbf{c}(h,a)), \ \pi_{r+s}(\mathbf{c}(x,a)) = 0, \text{ porque } \mathbf{c}(x,a) \in G_{r+s}^+.
\end{aligned}$$

De forma análoga (usando la parte 2 del Lema 1.2) $\pi_{r+s}(\mathbf{c}(g,a)) = \pi_{r+s}(\mathbf{c}(g,b))$ y con ambas obtenemos $\pi_{r+s}(\mathbf{c}(g,a)) = \pi_{r+s}(\mathbf{c}(h,b))$.

2) Es bilineal: Sean $g, h \in G_r$ y $a, b \in G_s$, entonces

$$\begin{aligned}
\pi_{r+s}(\mathbf{c}(gh,a)) &= \pi_{r+s}(g\mathbf{c}(h,a)g^{-1}\mathbf{c}(g,a)), \\
&= \pi_{r+s}(g\mathbf{c}(h,a)g^{-1}) + \pi_{r+s}(\mathbf{c}(g,a)), \\
&= \pi_{r+s}(\mathbf{c}(g,a)) + \pi_{r+s}(\mathbf{c}(h,a)).
\end{aligned}$$

$$\begin{aligned}
\pi_{r+s}(\mathbf{c}(g,ab)) &= \pi_{r+s}(\mathbf{c}(g,a)a\mathbf{c}(g,b)a^{-1}), \\
&= \pi_{r+s}(\mathbf{c}(g,a)) + \pi_{r+s}(a\mathbf{c}(g,b)a^{-1}), \\
&= \pi_{r+s}(\mathbf{c}(g,a)) + \pi_{r+s}(\mathbf{c}(g,b)).
\end{aligned}$$

Por como está definida $\bar{c}_{r,s}$, esto prueba la proposición. □

Observación 1.10. *Las funciones $\bar{c}_{r,s}$ se puede extender linealmente a $\bar{c} : \mathtt{gr}_\omega(G) \times \mathtt{gr}_\omega(G) \to \mathtt{gr}_\omega(G)$, considerando a $\mathtt{gr}(G)$ como $\mathbb{Z}-$módulo.*

Definición 1.11. *Un anillo de Lie es un $\mathbb{Z}-$módulo en el cual hay un corchete de Lie[6] definido. Si consideramos R-módulo, para un anillo R, donde hay un corchete de Lie definido, decimos que es una R-álgebra de Lie.*

Teorema 1.2. *$\mathtt{gr}_\omega(G)$ es anillo de Lie con $[\cdot\ \cdot] := \bar{c}(\cdot,\cdot)$ como corchete de Lie.*

Como antes, un lema que nos ayudará en los cálculos.

Lema 1.3. *Sea G un grupo con elemento identidad e. Entonces, para cualesquiera $x, y, z \in G$, tenemos*

$$\mathbf{c}(\mathbf{c}(x,y), yzy^{-1})\mathbf{c}(\mathbf{c}(y,z), zxz^{-1})\mathbf{c}(\mathbf{c}(z,x), xyx^{-1}) = e.$$

Demostración. Al desarrollar cada factor tenemos:

- $\mathbf{c}(\mathbf{c}(x,y), yzy^{-1}) = (xyx^{-1}zx)(y^{-1}x^{-1}yz^{-1}y^{-1}) = AB^{-1}$.
- $\mathbf{c}(\mathbf{c}(y,z), zxz^{-1}) = (yzy^{-1}xy)(z^{-1}y^{-1}zx^{-1}z^{-1}) = BC^{-1}$.

[6]Recuerde que un corchete de Lie es una función bilineal $(a,b) \mapsto [ab]$ que satisface $[aa] = 0$ y la identidad de Jacobi.

- $\mathbf{c}(\mathbf{c}(z,x),xyx^{-1}) = (zxz^{-1}yz)(x^{-1}z^{-1}xy^{-1}z^{-1}) = CA^{-1}$.

Entonces, $\mathbf{c}(\mathbf{c}(x,y),yzy^{-1})\mathbf{c}(\mathbf{c}(y,z),zxz^{-1})\mathbf{c}(\mathbf{c}(z,x),xyx^{-1}) = AB^{-1}BC^{-1}CA^{-1} = e$. □

Ahora la demostración del teorema.

Demostración. Sea $A \in \mathrm{gr}_\omega(G)$. Por definición $A = \sum_r A_r$. Demostraremos *i*) $[AA] = 0$ y *ii*) que $[\cdot\,\cdot]$ satisface la identidad de Jacobi. La bilinealidad ya se tiene:

i) Por la bilinealidad de $[\cdot\,\cdot]$, es suficiente probar que $[A_rA_r] = 0$ y $[A_rA_s] = -[A_sA_r]$. Sea a_r, a_s tales que $\pi_r(a_r) = A_r$ y $\pi_s(a_s) = A_s$. Entonces,

$$[A_rA_r] = \overline{c}(\pi_r(a_r),\pi_r(a_r)) = \pi_{2r}(c_{r,r}(a_r,a_r)) = \pi_{2r}(e) = 0.$$

Y

$$\begin{aligned}
[A_rA_s] &= \overline{c}_{r,s}(\pi_r(a_r),\pi_s(a_s)),\\
&= \pi_{r+s}(c_{r,s}(a_r,a_s)),\\
&= \pi_{r+s}(c_{s,r}(a_s,a_r)^{-1}),\\
&= -\pi_{r+s}(c_{s,r}(a_s,a_r)),\\
&= \overline{c}_{s,r}(\pi_s(a_s),\pi_r(a_r)),\\
&= -[A_sA_r].
\end{aligned}$$

Por la bilinealidad de $[\cdot\,\cdot]$ tenemos que $[AA] = 0$.

ii) Sean $A, B, C \in \mathrm{gr}_\omega(G)$. Denotemos $J(A,B,C) := [[AB]C] + [[BC]A] + [[CA]B]$. Es claro que J es trilineal, entonces es suficiente probar que $J(A_r,B_s,C_t) = 0$. Sean a, b, c tales que $\pi_r(a) = A_r$ y análogo para b y c. Denotemos $\lambda = r+s+t$, entonces

$$\begin{aligned}
J(A_r,B_s,C_t) &= \pi_\lambda(c_{r+s,t}(c_{r,s}(a,b),c)) + \pi_\lambda(c_{s+t,r}(c_{s,t}(b,c),a))\\
&\quad +\pi_\lambda(c_{t+r,s}(c_{t,r}(c,a),b)),\\
&= \pi_\lambda(c_{r+s,t}(c_{r,s}(a,b),bcb^{-1})) + \pi_\lambda(c_{s+t,r}(c_{s,t}(b,c),cac^{-1}))\\
&\quad +\pi_\lambda(c_{t+r,s}(c_{t,r}(c,a),aba^{-1})),\\
&= \pi_\lambda(c_{r+s,t}(c_{r,s}(a,b),bcb^{-1})\cdot c_{s+t,r}(c_{s,t}(b,c),cac^{-1})\cdot c_{t+r,s}(c_{t,r}(c,a),aba^{-1})),\\
&= \pi_\lambda(\mathbf{c}(\mathbf{c}(a,b),bcb^{-1})\cdot \mathbf{c}(\mathbf{c}(b,c),cac^{-1})\cdot \mathbf{c}(\mathbf{c}(c,a),aba^{-1})),\ \text{por el lema,}\\
&= \pi_\lambda(e) = 0.
\end{aligned}$$

□

Esta es la manera en que podemos asociar una estructura de Lie a un grupo. Sin embargo, las filtraciones en las que nos enfocarémos son las "enteras", las cuales abordaremos en la siguiente sección.

1.3.1 FILTRACIONES ENTERAS

Diremos que una filtración $\omega : G \to \mathbb{R} \cup \{+\infty\}$ es *entera* si $\omega(G - \{1\}) \subset \mathbb{Z}$.

Proposición 1.19. *Sea G un grupo. Tenemos una correspondencia uno a uno entre:*

1) Filtraciones enteras,

2) Sucesiones decrecientes $\{G_n\}_{n\in\mathbb{N}}$ de subgrupos de G tales que:

i) $G_1 = G$.

ii) $\mathbf{c}(G_n, G_m) \subset G_{n+m}$.

Observación 1.11. *Una sucesión como en 2) debe ser de subgrupos normales: si $g \in G_n$ y $h \in G = G_1$, entonces $\mathbf{c}(h,g) \in G_{n+1} \subset G_n \Rightarrow hgh^{-1} = \mathbf{c}(h,g)g \in G_n$. Es decir, $G_n \lhd G$.*

Ahora la demostración de la Proposición 1.19.

Demostración. ($\Rightarrow$) Se sigue del la definición de filtración (1.9 (p. 11)) y la Observación 1.8 (p. 11).

($\Leftarrow$) Definimos $\omega(g) = \sup\{n \mid g \in G_n\}$. Vamos a probar que ω es una filtración.

La parte 1 y 2 de la Definición 1.9 (p. 11) son inmediatas, además de que $\omega(g) = \omega(g^{-1})$. Sean $m, n \in \mathbb{N}$ y supongamos que $m \leq n$. Si $g \in G_n$ y $h \in G_m$, entonces $g \in G_m$ y $gh^{-1} \in G_m$. Esto nos da $\omega(gh^{-1}) \geq \text{ínf}\{\omega(g), \omega(h)\}$. Si $n = +\infty$ ó $m = +\infty$ la desigualdad es clara. Por la condición *ii)* tenemos que $\mathbf{c}(g,h) \in G_{n+m}$ y se tiene 4). Por construcción ω es entera.

□

Definición 1.12. *Una sucesión $\{H_k\}$ de subgrupos de G que cumplen con la condición 2 de la Proposición 1.19 (p. 15) la llamaremos serie fuertemente central. Si sólo satisface $\mathbf{c}(G, H_j) \subset H_{j+1}$, la llamaremos serie central.*

1.3.2 EJEMPLOS

Damos dos ejemplos de serie central: La "serie central descendente", la cual es fuertemente central y de donde derivamos el nombre de las series, y la "serie de dimensión".

Para ver un ejemplo de una filtración no entera, ver la sección 4.3 (p. 46) del capítulo 4.

EJEMPLO: SERIE CENTRAL DESCENDENTE

Definición 1.13. *Sea G un grupo. Definimos $\gamma_1(G) = G$ y $\gamma_n(G) = \mathbf{c}(G, \gamma_{n-1}(G))$.*

Proposición 1.20. *Sea G un grupo. Entonces, $\{\gamma_n(G)\}$ cumple con 2) de la Proposición 1.19 (p. 15). Más aún, si $\{H_n\}$ también lo cumple, entonces $\gamma_n(G) \subset H_n$ para toda $n \in \mathbb{N}$.*

Demostración. La condición $i)$ se sigue por definición. Vamos a probar $ii)$ por inducción en n. Sea m fijo. Entonces, para $n = 1$, tenemos

$$\mathbf{c}(G, \gamma_m(G)) = \mathbf{c}(\gamma_1(G), \gamma_m(G)) = \gamma_{m+1}(G) \subset \gamma_m(G).$$

Esto también prueba que es una sucesión decreciente.

Supongamos el hecho para $n > 1$. Por el Lema 1.3 (p. 13) tenemos

$$\begin{aligned} \mathbf{c}(\gamma_n(G), \gamma_m(G)) &= \mathbf{c}(\mathbf{c}(G, \gamma_{n-1}(G)), \gamma_m(G)), \\ &\subset \mathbf{c}(\mathbf{c}(\gamma_{n-1}(G), \gamma_m(G)), G) \cdot \mathbf{c}(\mathbf{c}(\gamma_m(G), G), \gamma_{n-1}(G)), \\ &\subset \mathbf{c}(\gamma_{n+m-1}(G), G) \cdot \mathbf{c}(\gamma_{m+1}(G), \gamma_{n-1}(G)), \\ &\subset \gamma_{n+m}(G) \cdot \gamma_{n+m}(G) = \gamma_{n+m}(G). \end{aligned}$$

Ahora, si $\{H_n\}$ cumple 2) de la Proposición 1.19 (p. 15), entonces $H_1 = \gamma_1(G)$. Supongamos que $\gamma_n(G) \subset H_n$ para $n > 1$. Entonces,

$$\gamma_{n+1}(G) = \mathbf{c}(G, \gamma_{n-1}(G)) \subset \mathbf{c}(H_1, H_n) \subset H_{n+1}.$$

□

EJEMPLO: SERIE DE DIMENSIÓN

Sea R un anillo conmutativo con 1 y G un grupo. El anillo del grupo sobre R es el R-álgebra

$$R[G] = \left\{ \sum_{g \in G} \alpha_g g \mid \alpha_g \in R, \forall g \in G \text{ y } \alpha_g \neq 0, \text{ para un número finito} \right\},$$

donde las operaciones están dadas por

$$\left(\sum_{g \in G} \alpha_g g \right) + \left(\sum_{g \in G} \beta_g g \right) = \sum_{g \in G} (\alpha_g + \beta_g) g,$$

$$\left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{h \in G} \beta_h h \right) = \sum_{l \in G} \left(\sum_{gh = l} \alpha_g \beta_h \right) l.$$

Definimos $\varepsilon : R[G] \to R$, dado por $\varepsilon(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g$, el cual es un homomorfismo de anillos.

Definición 1.14. *ε es llamado homomorfismo de aumentación y $\Delta_R(G) = ker(\varepsilon)$ ideal de aumentación.*

Escribiremos Δ por $\Delta_R(G)$ y $1g$ por g en $R[G]$. Para $g \in G$ definimos

$$\omega(g) := \sup\{k \mid g - 1 \in \Delta^k\}.$$

Observación 1.12. *ω está bien definida; esto porque $G \hookrightarrow \mathcal{U}(R[G])$, las unidades de $R[G]$. Así, para todo g existe un $n \in \mathbb{N}$ tal que $g - 1 \in \Delta^n$.*

Proposición 1.21. *ω es una filtración entera en G.*

Demostración. Por definición de ω, es claro que $\omega(1) = \infty$ y $\omega(g) > 0$, para todo $g \in G$. Además, tenemos que $\omega(g) = \omega(g^{-1})$. Esto se obtiene de que, si $\omega(g) = n$, entonces $g^{-1} - 1 = g^{-1}(1 - g) \in \Delta^n$.

Supongamos que $\omega(g) = n$ y $\omega(h) = m$, con $m < n$. Como $\{\Delta^n\}$ es decreciente, $g - 1, h - 1 \in \Delta^m$. Entonces,

$$(g-1)(h^{-1}-1) = gh^{-1} - 1 - (g-1) - (h^{-1}-1) \in \Delta^m,$$

con lo que $gh^{-1} - 1 \in \Delta^m$. Así,

$$\omega(gh^{-1}) \geq \text{ínf}\{\omega(g), \omega(h)\}.$$

Si $n = +\infty$ ó $m = +\infty$, la demostración es la misma.

Con los mismos valores vemos que

$$[g-1, h-1] \in \Delta^{n+m}, \text{ y}$$

$$[g-1, h-1] = [g,h] - [1,h] - [g-1,1] = [g,h].$$

Por ser Δ^{n+m} ideal, tenemos que $[g,h]x \in \Delta^{n+m}$, para todo $x \in R[G]$. Tomando $x = g^{-1}h^{-1}$ tenemos que $\mathbf{c}(g,h) - 1 \in \Delta^{n+m}$. Por lo que $\omega(\mathbf{c}(g,h)) \geq \omega(g) + \omega(h)$. □

Definición 1.15. *Para $n \in \mathbb{N}$, definimos*

$$D_{n,R}(G) := \{g \in G \mid \omega(g) \geq n\}$$

el n-ésimo subgrupo de dimensión de G sobre R.

Por lo anterior, $D_{n,R}(G)$ es una serie fuertemente central y tenemos que $\gamma_n(G) \subset D_{n,R}(G)$.

Problemas interesantes que aparecen sobre las series de dimensión, y las potencias del ideal de aumentación, son el identificar a los $D_{n,R}(G)$, calcular Δ^n/Δ^{n+1} y describir la interseción de los Δ^n.

Capítulo 2

El Grupo de Nottingham

En este capítulo definiremos el grupo de Nottingham, tema central en este trabajo.

Considere R un anillo conmutativo con identidad y sea $\mathcal{N}(t,R) \subset R[[t]]$ dado por

$$\mathcal{N}(t,R) = \left\{ t + a_2 t^2 + a_3 t^3 + \dots \mid a_j \in R \right\}.^1 \tag{2.1}$$

Uno de los primeros en trabajar con este conjunto fue Jennnings en [6] quien prueba que bajo la operación dada por la substitución (formal) forma un grupo, da una forma para el conmutador y prueba los conjuntos $\mathcal{N}(t,R)_m := \{t + a_m t^m + a_{m+1} t^{m+1} ...\}$ forman una serie central. Además, cuando R es un campo de característica cero, encuentra una familia de grupos uniparamétricos que generan a todo el grupo y que topológicamente está generado por los dos primeros grupos de la familia.

Posterior al trabajo de Jennings, Johnson y su alumno York prueban varios resultados de la estructura del grupo. El hecho de que es isomorfo a un límite inverso, que en el caso de que $R = \mathbb{F}_p$ nos dice que es un pro-p grupo.

2.1 Primeras Definiciones

Toda esta sección sigue ideas de Jennings ([6]) y Johnson ([7]).

Sea R un anillo conmutativo con identidad. Considere

$$\mathcal{N}(t,R) := \left\{ t + a_2 t^2 + a_3 t^3 + \cdots \mid a_j \in R \right\} \subset R[[t]].$$

Si $\alpha, \beta \in \mathcal{N}(t,R)$, definimos la operación como $\alpha\beta := \alpha(\beta)$ (substitución formal); esto es, si $\alpha = t + \sum a_j t^j$ y $\beta = t + \sum b_j t^j$, entonces $\alpha\beta = \beta + \sum a_j \beta^j$. Así obtenemos

- $\alpha\beta \in \mathcal{N}(t,R)$.

[1] Nótese que es muy parecido a $H(\mathbb{F}_p)$, salvo que aquí $a_1 = 1$. Ver 1.1.2 (p. 6).

- Si $\alpha\beta = t + \sum c_j t^j$, entonces los coeficientes del producto son

$$\begin{aligned} c_2 &= a_2 + b_2, \\ c_k &= a_k + b_k + \sum_{j\geq 2}^{k-1} a_j \phi_j(b_2, \ldots, b_{k-1}), \text{ con } k > 2, \end{aligned} \tag{2.2}$$

  donde ϕ_j son polinomios.

Por ejemplo, la forma de los primeros coeficientes es

$$\begin{aligned} c_2 &= a_2 + b_2, \\ c_3 &= a_3 + b_3 + a_2(2b_2), \\ c_4 &= a_4 + b_4 + a_2(b_2^2 + 2b_3) + a_3(3b_2), \\ c_5 &= a_5 + b_5 + a_2(2b_2b_3 + 2b_4) + a_3(3b_2^2 + 3b_3) + a_4(4b_2). \end{aligned}$$

En general, son de la forma

$$\phi_j(b_2, \ldots, b_{k-1}) = \sum_{j_1 + j_2 + \cdots + j_{k-1} = k} b_{j_1} b_{j_2} \ldots b_{j_{k-1}}, \text{ con } 1 < j_i \leq k-1.$$

La asociatividad de este producto es clara y tenemos un elemento neutro dado por $1 = t$. Bajo esta operación el inverso de $\alpha = t + \sum a_j t^j$, si existiera, digamos $\eta = t + \sum x_j t^j$, debe cumplir $\alpha\eta = 1 = t$. Por las identidades (2.2) se obtiene

$$\begin{aligned} 0 &= a_2 + x_2, \\ 0 &= a_k + x_k + \sum_{j\geq 2}^{k-1} a_j \phi_j(x_2, \ldots, x_{k-1}), \text{ con } k > 2. \end{aligned} \tag{2.3}$$

Tal sistema tiene solución

$$\begin{aligned} x_2 &= -a_2, \\ x_k &= -a_k - \sum_{j\geq 2}^{k-1} a_j \phi_j(a_2, \ldots, a_{k-1}), \text{ con } k > 2. \end{aligned} \tag{2.4}$$

Por esto, $\eta \in \mathcal{N}(t, R)$ y por construcción $\alpha\eta = t = 1$. Con esto garantizamos la existencia de inversos derechos para cualquier elemento en $\mathcal{N}(t, R)$. Así, η tiene un inverso derecho, digamos γ. Entonces,

$$\eta\alpha = \eta\alpha(1) = \eta\alpha(\eta\gamma) = \eta(\alpha\eta)\gamma = \eta\gamma = 1. \tag{2.5}$$

Es decir, $\eta = \alpha^{-1}$. Con esto hemos probado el siguiente resultado.

Proposición 2.1. *$\mathcal{N}(t, R)$ es un grupo con la operación anterior.*

Tal grupo tiene un nombre especial.

Definición 2.1. *El grupo $\mathcal{N}(t,R)$ se llama el grupo de Nottingham sobre R. El grupo de Nottingham clásico es definido sobre $R = \mathbb{F}_p$.*

La siguiente observación nos muestra otra forma de pensar en $\mathcal{N}(t,R)$.

Observación 2.1. *Como se vio en la sección 1.1.2 (p. 6), $\mathcal{N}(t,R) \subset H(R) \cong Aut(R[[t]])$; es decir, podemos considerar a $\mathcal{N}(t,R)$ encajado en $Aut(R[[t]])$. Observe que la demostración dada en Proposición 1.8 (p. 6) funciona igual para el caso de un anillo R: sea $\alpha \in \mathcal{N}(R,t)$. Entonces, α define un homomorfismo f como $f(t) = \alpha(t) = t + \sum a_j t^j$, y extendemos la acción de f a todo $R[[t]]$. Es claro que f es un automorfismo por ser α invertible y $fg \mapsto g(f(t)) = (g \circ f)(t)$.*

2.1.1 FILTRACIÓN EN $\mathcal{N}(t,R)$

Para $k \in \mathbb{N}$, considere $L_k := \{t + \sum_{j>k} a_j t^j\} \subset \mathcal{N}(t,R)$. Hay una filtración natural para $\mathcal{N}(t,R)$ asociada a los L_k

Definición 2.2. *Definimos la «profundidad» de $\alpha \in \mathcal{N}(t,R)$ como $D(\alpha) = k$ si y sólo si $\alpha \in L_k \setminus L_{k+1}$.*

Observación 2.2. *Es claro que $D(1) = \infty$ y que D está bien definida ya que dado un α, existe único k, tal que $\alpha \in L_k / L_{k+1}$. Además, la definición es equivalente a decir que $D(\alpha) = k$ si y sólo si $\alpha = t + \sum_{j>k} a_j t^j$, con $a_{k+1} \neq 0$.*

Probaremos que D es, en efecto, una filtración. Antes un lema que nos dice la naturaleza del conmutador en este grupo dada la profundidad de los elementos.

Lema 2.1. *Sean $\alpha = t + at^{n+1} + \dots$ y $\beta = t + bt^{m+1} + \dots$ en $\mathcal{N}(t,R)$. Entonces,*

$$\mathbf{c}(\alpha,\beta) = t + ab(m-n)t^{m+n+1} + Q(\alpha,\beta,m+n+1), \tag{2.6}$$

donde $Q(\alpha,\beta,m+n+1)$ es una serie donde sus coeficientes son productos de los coeficientes de α y β y $D(t + Q(\alpha,\beta,m+n+1)) > m+n+1$.

Demostración. Escribiremos $Q = Q(\alpha,\beta,n+m+1)$ y sólo nos importa de éste termino que su profundidad esté acotada por abajo. Al hacer el producto de α con β obtenemos

$$\alpha\beta = \beta + a(\beta)^{n+1} + \sum_{j \geq n+1} a_j(\beta)^j = \beta + \alpha - t + ab(n+1)t^{m+n+1} + Q \tag{2.7}$$

Por las ecuaciones 2.4 (p. 20), tenemos que $\alpha^{-1} = t - at^{n+1} + \ldots$, así

$$\begin{aligned}\alpha\beta\alpha^{-1} &= \beta\alpha^{-1} + \alpha\alpha^{-1} - \alpha^{-1} + ab(n+1)(\alpha^{-1})^{m+n+1} + Q(\alpha^{-1}),\\ &= \left(\alpha^{-1} + \beta - t - ab(m+1)t^{m+n+1} + Q\right) + t - \alpha^{-1} + ab(n+1)t^{m+n+1} + Q,\\ &= \beta + ab(n-m)t^{m+n+1} + Q. \end{aligned} \tag{2.8}$$

Entonces,

$$\begin{aligned}\mathbf{c}(\alpha,\beta) &= \alpha\beta\alpha^{-1}\beta^{-1},\\ &= \beta\beta^{-1} + ab(n-m)(\beta^{-1})^{m+n+1} + Q(\beta^{-1}),\\ &= t + ab(n-m)t^{m+n+1} + Q.\end{aligned}$$

□

Proposición 2.2. *D es una filtración entera en $\mathcal{N}(t,R)$.*

Demostración. 1) y 2) son inmediatos de la definición de filtración (1.9 (p. 11)). 3) se sigue de las ecuaciones 2.4 (p. 20) y 2.7 (p. 21); y 4) del lema anterior. □

Es claro que $\mathcal{N}(t,R)_m = L_m$. Así, la sucesión $\{L_m\}_{m\in\mathbb{N}}$ es una serie fuertemente central y como $\bigcap L_m = \{t\}$, obtenemos el siguiente resultado.

Corolario 2.1. *$\mathcal{N}(t,R)$ es residualmente nilpotente.*

Sea $\mathcal{N}_k = \mathcal{N}(t,R)/L_k$. Denotamos $[g]_k$ la clase de g en $\mathcal{N}_k$ y definimos $\varphi_{k+1} : \mathcal{N}_{k+1} \to \mathcal{N}_k$, por $\varphi_{k+1}([g]_{k+1}) = [g]_k$, para $k > 0$. Tenemos que φ_k está bien definida por ser $\{L_k\}_k$ decreciente. Así, $\{\mathcal{N}_k, \varphi_k\}$ forma un sistema inverso.

Observación 2.3. *Cada clase $[g]_k$ contiene un único polinomio de grado a lo más k: si $\alpha = t + a_2t^2 + \ldots$ y $\beta = t + b_2t^2 + \ldots$, entonces $[\alpha]_k = [\beta]_k$ si y sólo si $D(\alpha\beta^{-1}) = k$. Ahora, β^{-1} tiene coeficientes*

$$\begin{aligned}x_2 &= -b2.\\ x_j &= -b_j - \sum_{i\geq 2}^{j-1} b_i\phi_i(b_2,\ldots,b_{j-1}).\end{aligned}$$

Así que $\alpha\beta^{-1}$ tiene coeficientes

$$\begin{aligned}c_2 =& a_2 + x_2 = a_2 - b_2.\\ c_k =& a_k + x_k + \sum_{l\geq 2}^{k-1} a_l\phi_l(x_2,\ldots,x_{k-1}),\\ =& a_k - b_k - \sum_{j\geq 2}^{k-1} b_j\phi_j(b_2,\ldots,b_{k-1}) + \sum_{l\geq 2}^{k-1} a_l\phi_l(x_2,\ldots,x_{k-1}).\end{aligned}$$

Observe que para tener $D(\alpha\beta^{-1}) = k+1$ es necesario que $c_2 = c_3 = \cdots = c_k = 0$. Esto implica que $a_2 = b_2$. Sustituyendo en c_3 se llega a $0 = c_3 = a_3 - b_3 - b_2(2b_2) + a_2(2b_2) = a_3 - b_3$. Continuando obtenemos que $c_j = 0$ implica $a_j = b_j$, para $2 \leq j \leq k$. Esto muestra que dos elementos α, β se relacionan si coinciden hasta grado k.

Ponga $M = \varprojlim \mathcal{N}_k$ y sean $\psi_k : M \to \mathcal{N}_k$, dadas por M. Entonces, podemos probar un resultado de Johnson en [7], a saber, $\mathcal{N}(t, R)$ es un límite inverso.

Proposición 2.3. $M \cong \mathcal{N}(t, R)$

Demostración. Para cada k, sea $\pi_k : \mathcal{N}(t, R) \to \mathcal{N}_k$, la función cociente. Es claro que $\pi_k = \varphi_k \circ \pi_{k+1}$, así por la propiedad universal de M, existe único morfismo $h : \mathcal{N}(t, R) \to M$, tal que $\pi_k = \psi_k \circ h$.

- h es inyectiva: sea $g \in \mathcal{N}(t, R)$ tal que $h(g) = 1$. Entonces, para todo k, $[t]_k = \psi_k(h(g)) = \pi_k(g)$; es decir, $g \in L_k$ para todo k. Por el Corolario 2.1 (p. 22), $g = t$.
- h es sobreyectiva: sea $z \in M$. Entonces, $\psi_k(z) = t + z_2 t^2 + \cdots + z_k t^k$ (el representante de la clase), con $z_k \in R$. Como $\psi_k = \phi_{k+1} \circ \psi_{k+1}$ y de la observación anterior tenemos que $\psi_{k+1}(z) - \psi_k(z) = z_{k+1} t^{k+1}$, para todo k. Definimos $\alpha = t + \sum_{j \geq 2} z_j t^j$ y obtenemos $\psi_k(h(\alpha)) = \pi_k(\alpha) = \psi_k(z)$, para todo k. Así $h(\alpha) = z$.

□

Este resultado nos dirá, al combinarlo con otro, que en el caso clásico ($R = \mathbb{F}_p$), el grupo de Nottingham es un grupo profinito; es decir, $\mathcal{N}(t, R)$ es un grupo topológico, Hausdorff , compacto y donde L_k nos da un sistema de bases para las vecindades de $1 = t$.

Uno puede notar que la condición de ser residualmente nilpotente implica que el grupo puede encajarse en un límite inverso como arriba. Esto es importante por cómo se define la completación profinita de un grupo (ver1.2.1 (p. 9)).

2.2 $char(R) = 0$

Calcularemos el anillo de Lie asociado a D, usando la construcción vista en el capítulo 1 (1.3 (p. 11)), dejando el caso de $char = p$ para la siguiente sección.

El anillo de Lie asociado a D

Sean $\alpha, \beta \in L_m$ con $\alpha = t + at^{m+1} + \ldots$ y $\beta = t + bt^{m+1} + \ldots$. Por la ecuación 2.7 (p. 21) tenemos que

$$\alpha\beta^{-1} = t + (a - b)t^{m+1} + \ldots \tag{2.9}$$

Entonces, $\alpha\beta^{-1} \in L_{m+1}$ si y sólo si $a = b$. Así, una clase en $\mathtt{gr}_{D,m}(\mathcal{N}(t,R))$ depende sólo del coeficiente del término t^{m+1}.

Consideremos $\tau_m(a) = t + at^{m+1} \in L_m$. Abusando de la notación, escribiremos $\tau_m(a)$ como la clase de equivalencia en $\mathtt{gr}_{D,m}(\mathcal{N}(t,R))$.

Proposición 2.4. *$\{\tau_m(a) \mid a \in R\}$ es un grupo abeliano y $\{\tau_m(a) \mid a \in R\} = \mathtt{gr}_{D,m}(\mathcal{N}(t,R))$*

Demostración. Para $a, b \in R$, tenemos

$$\begin{aligned}\tau_m(a)\tau_m(b) &= t + bt^{m+1} + a(t + bt^{m+1})^{m+1},\\ &= t + bt^{m+1} + at^{m+1},\\ &= t + (a+b)t^{m+1},\\ &= \tau_m(a+b).\end{aligned}$$

Se sigue que la multiplicación es conmutativa, $\tau_m(a)^{-1} = \tau_m(-a)$ y $\tau_m(0) = t$ es el neutro. Así, $\{\tau(a)|a \in R\} \subset \mathtt{gr}_{D,m}(\mathcal{N}(t,R))$ es un subgrupo. Pero como se mencionó arriba, una clase sólo depende del coeficiente de t^{m+1}; esto es, para cada clase $g \in \mathtt{gr}_{D,m}(\mathcal{N}(t,R))$ existe $a \in R$, único, tal que $g = \tau_m(a)$. Por ello se tiene la igualdad. □

Con esto, $\mathtt{gr}_{D,m}(\mathcal{N}(t,R)) \cong R\langle t^{m+1}\rangle$ y

$$\begin{aligned}\bar{c}_{m,n}(\tau_m(a), \tau_n(b)) &= [\mathbf{c}(\tau_m(a), \tau_n(b))]_{n+m}\\ &= t + ab(m-n)t^{m+n+1}\\ &= \tau_{m+n}(ab(m-n))\end{aligned} \tag{2.10}$$

Observación 2.4. *En la ecuación de arriba, denotamos $[x]_N$ la clase en $\mathtt{gr}_{D,N}(\mathcal{N}(t,R))$. Esto porque $\tau_n(a) = [\tau_n(a)]_n$, pero si cambiamos de clase, $[\tau_n(a)]_N^{-1} \neq [\tau_n(-a)]_N$, ya que $\tau_n(a)^{-1} = t - at^n + \ldots$; es decir, pueden aparecen más términos al cambiar de clase.*

Así, $\mathtt{gr}_D(\mathcal{N}(t,R))$ es la suma directa de $R\langle t^{n+1}\rangle$ con $n \geq 1$;

$$\mathtt{gr}_D(\mathcal{N}(t,R)) = \bigoplus_{k\geq 1} R\langle t^{k+1}\rangle^2, \tag{2.11}$$

y el corchete de Lie está dado por

$$[t^{n+1}t^{m+1}] = (n-m)t^{n+m+1}. \tag{2.12}$$

[2] Recuerde que $t^1 = 1$, en $\mathcal{N}(t,R)$

2.3 $R = \mathbb{F}_p$

En esta sección daremos algunos resultados sobre el grupo de Nottingham clásico, esto es, cuando $R = \mathbb{F}_p$. La gran mayoría de los resultados e ideas se deben a Jennings [6], Johnson [7] y Camina [1] y [2].

Sea D la filtración natural en $\mathcal{N}(t, R)$ y L_m los subgrupos dados por D. Entonces, como en la sección anterior, tenemos que

$$\mathtt{gr}_{D,m}(\mathcal{N}(t, R)) = L_k / L_{k+1} = R\langle t^{k+1} \rangle,$$

y el conmutador está dado por $[t^{n+1}, t^{m+1}] = (n - m)t^{n+m+1}$. Así, para el caso de caracteristica p, el corchete es cero si $n \equiv m \mod p$. Esto se relaciona con el primer álgebra de Witt W; ésta álgebra se define sobre $\mathbb{F}_p$ con base $\{\lambda_0, \ldots \lambda_{p-1}\}$ y el conmutador está dado por

$$[\lambda_i, \lambda_j] = (i - j)\lambda_{i+j},$$

donde el subíndice se toma módulo p. W tiene la siguiente estructura de graduada

$$W = \bigoplus_{j=0}^{p-1} \mathbb{F}_p\langle \lambda_j \rangle.$$

Con esto, es claro ver que

$$\mathtt{gr}_D(\mathcal{N}(t, R)) \cong \bigoplus_{j>0} \mathbb{F}_p\langle \lambda_{j \bmod p} \rangle \otimes t^j.$$

Como se mencionó antes, la Proposición 2.3 (p. 23) y el siguiente resultado nos dan el hecho de que $\mathcal{N}(t, R)$ es un pro-p grupo.

Proposición 2.5. $|\mathcal{N}(t, R)/L_m| = p^{m-1}$.

Demostración. Se sigue de que todo elemento en $\mathcal{N}(t, R)/L_m$ es de la forma $t + \sum_{j>1}^{m} a_j t^j$. □

Corolario 2.2. *$\mathcal{N}(t, \mathbb{F}_p)$ es un pro-p grupo.*

También, al considerar al grupo de Nottingham como subgrupo de los automorfismos de $\mathbb{F}_p((t))$ obtenemos

Proposición 2.6. $[\mathcal{N}(t, \mathbb{F}_p((t))) : Aut(\mathbb{F}_p((t)))] = p - 1$

Demostración. Se sigue de los automorfismos de $\mathbb{F}_p((t))$ son los de la forma $t \mapsto \sum_{n\geq 1} a_n t^n$ (ver 1.1.2 (p. 6)). □

En la siguiente sección abordaremos los teoremas que llamaron mucho la atención de los matemáticos hacia este grupo. Tales resultado nos dicen que en el grupo de Nottingham podemos encajar ciertos grupos. El primer resultado con ésta filosofía fue hecho por Johnson ([7]). Él probó el siguiente resultado para $char(R) = 0$.

Proposición 2.7. *$\mathcal{N}(t, R)$ contiene una copia de $\mathbf{F}_2$.*

Después Leedham-Green y Weiss probaron que cualquier p-grupo finito se encaja en $\mathcal{N}(t, \mathbb{F}_p)$ y con ayuda de esto, Camina ([1]) prueba el siguiente resultado.

Teorema 2.1. *Cualquier pro-p grupo con base numerable[3] puede ser encajado en $\mathcal{N}(t, \mathbb{F}_p)$ como un subgrupo cerrado.*

La demostración del resultado de Johnson puede verse en [7] mientras que el resultado de Camina se prueba en el siguiente capítulo.

[3]Decimos que G tiene base numerable si existe una base para las vecindades de 1 numerable.

Capítulo 3
Teorema de Camina

En este capítulo abordaremos la demostración de un teorema de Camina en [1], uno de los resultados más interesantes sobre el grupo de Nottingham. Además, usamos un resultado por Lubotzky y Wilson presentado en [8].

Nota: Aquí p denota un primo cualquiera fijo y k un campo de caracteristica p. Además, usando la Observación 2.1 (p. 21), pensaremos a $\mathcal{N}(t, \mathbb{F}_p) = \mathcal{N}(t)$ como un subgrupo de $Aut(\mathbb{F}_p((t))$ y otras veces como el grupo de potencias formales bajo la sustitución.

3.1 Dos Teoremas de Witt

Tomaremos los resultados de Witt en [1] y los comentarios hechos por Camina sobre los mismos.

En pocas palabras, los teoremas de Witt nos garantizan la posibilidad, y la forma, de construir extensiones de campos de caracteristica p, en los cuales, los grupos de Galois son isomorfos a p-grupos dados.

Sea k un campo de característica p. Denotemos como k^+ el grupo aditivo de k y $\overline{k}$ la cerradura algebraica de k. Sea $\wp : \overline{k}^+ \to \overline{k}^+$, el homomorfismo de grupos aditivos, definido por $\wp(x) = x^p - x$. Entonces, $\wp(k) \leq k^+$. Witt probó lo siguiente:

Teorema 3.1 (Witt). *Sea $\wp(k) \leq G \leq k^+$ con $[\wp(G) : G] < \infty$. Entonces,*

$$Gal(k(\wp^{-1}(G))/k) \cong G/\wp(k).$$

Más aún, para cualquier extensión abeliana K de k de exponente p existe un grupo G tal que $K = k(\wp^{-1}(G))$.

Las siguientes dos observaciones son hechas por Camina en [1].

Observación 3.1. .
Para el caso de un p-grupo cualquiera, Witt construye extensiones usando el caso abeliano (Teorema 3.1) y un proceso de inducción tomando las siguientes hipótesis:

Hipótesis 1. *Supongamos que P es un $p-$grupo finito con subgrupo de Frattini*[1] $\Phi(P) \neq \emptyset$. *Sea L un subgrupo cíclico de P de orden p que satisface $L \leq Z(P) \cap \Phi(P)$ (con $Z(P)$ centro de P). Supongamos que tenemos un isomorfismo $M \cong Gal(K/k)$, para alguna extensión K de k, donde $M \cong P/L$. Entonces, para construir una extensión de Galois de k, con grupo de Galois isomorfo a P, hacemos lo siguiente:*

1. *Fijamos un conjunto de representantes de M en P de tal manera de que si $M = \{a, b, \dots\}$, entonces los representantes son $\{z_a, z_b, \dots\}$. Con esto, definimos $l_{a,b}, \dots \in L$ tales que $z_a z_b = l_{a,b} z_{ab}$.*
2. *Tomemos un isomorfismo explícito $J : M \to Gal(K/k)$, $a \mapsto x$, $b \mapsto y$.*
3. *Escojamos un caracter aditivo χ de L; esto es, $\chi : L \to K^+$, homomorfismo de grupos.*
4. *Elegimos un conjunto $\{\delta_x | x \in Gal(K/k)\} \subset K$ tal que*
$$\chi(l_{a,b}) = \delta_x + x\delta_y - \delta_{xy}, \quad \forall x, y \in Gal(K/k). \tag{3.1}$$
5. *Elijamos $\gamma \in K$ tal que $\wp(\delta_x) = (x-1)\gamma$, para todo $x \in Gal(K/k)$.*
6. *Resolvemos la ecuación $\wp(t) = \gamma$, y adjuntamos la raíz $\theta \in \overline{K}$ a K. La extensión $\widehat{K} = K(\theta)$ es la buscada.*

Además, la representación como producto cruzado de $Gal(\widehat{K}/k)$ está dada como sigue: sea $f \in L$ y $h \in Gal(K/k)$. Se definen $\overline{f}$ y w_h en $Gal(\widehat{K}/k)$
$$\overline{f}(\theta) = \theta + \chi(f), \quad \overline{f} = id|_K,$$
y
$$w_h(\theta) = \theta + \delta_h, \quad w_h(z) = h(z), \quad \forall z \in K.$$

Nos referiremos a esta observación como el método de Witt o algoritmo de Witt.

Denotemos con $d(P)$ al número de generadores de P y definimos N tal que $[k : \wp(k)] = p^N$. En caso de que $[k : \wp(k)] = \infty$, ponemos $N = \infty$. Con esto, Witt prueba lo siguiente.

Teorema 3.2 (Witt)**.** *Sea P un $p-$grupo finito y k un campo de caracteristica p. Entonces, hay una extensión de Galois $\widehat{K}$ de k tal que $Gal(\widehat{T}/k) \cong P$ si y sólo si $d(P) \leq N$.*

Ahora la segunda observación.

Observación 3.2. .

- *Al identificar $P \cong Gal(\widehat{K}/k)$ y $M \cong Gal(K/k)$ tenemos que el homomorfismo $\pi : P \to P/L \cong M$ es restringir a K; esto es, $\pi(f) = f|_K$, con $f \in Gal(\widehat{K}/k)$.*
- *Para $k = \mathbb{F}_p((T))$ las extensiones obtenidas por el método de Witt son totalmente ramificadas siempre que supongamos que la extensión abeliana con la que iniciamos la construcción lo es.*

[1] El subgrupo de Frattini de un p-grupo es la intersección de todos los subgrupos maximales.

3.2 LEMAS

En esta sección, probaremos unos resultados que nos ayudarán en la demostración del teorema de Camina.

Proposición 3.1. *Sean* $\Psi : \mathbb{F}_p((t)) \to \mathbb{F}_p((t))/\wp(\mathbb{F}_p((t))) = A$, *la función al cociente de* $\mathbb{F}_p-$*espacios vectoriales y*

$$B = \{1\} \cup \{t^j \mid -j \in \mathbf{Z}^+ \text{ y } j \equiv 0 \mod p\}.$$

Entonces $\Psi(B)$ *es una base para* A *como* $\mathbb{F}_p-$*espacio vectorial.*

Demostración. Es claro que $\Psi(B)$ es un conjunto linealmente independiente. Para probar que es generador, nótese que $t^n = \wp(-\sum_{j\geq 0} t^{np^j})$, para toda $n \in \mathbb{N}$. Entonces, toda potencia positiva es cero en el cociente. □

Observación 3.3. *Otra forma de escribir éste resultado es la siguiente: para todo* $x \in \mathbb{F}_p((t))\backslash\wp(\mathbb{F}_p((t)))$ *existen* $\widehat{x}, \mu \in \mathbb{F}_p((t))$ *tales que* $x = \widehat{x} + \wp(\mu)$ *y con* $\nu(\widehat{x}) \leq 0$. *Además, si* $\nu(\widehat{x}) < 0$, *entonces* $\nu(\widehat{x}) \not\equiv 0 \mod (p)$. *Aquí* ν *denota la valuación normalizada de* $\mathbb{F}_p((t))$.

Además, si la raíz de γ, *para* $\wp(X) = \gamma$ *en 6) de la Observación 3.1 (p. 27), da una extensión totalmente ramificada, entonces* $\nu(\widehat{\gamma}) < 0$.

El primer resultado que va en la dirección del teorema 2.1 (p. 26) es el siguiente.

Teorema 3.3 (Leedham-Green, Weiss)**.** *El grupo de Nottingham* $\mathcal{N}(t, \mathbb{F}_p) = \mathcal{N}$ *contiene una copia de cualquier p-grupo finito.*

Demostración. Sea P un $p-$grupo finito. Por el Teorema 3.2 (p. 28) y el Lema 3.1 (p. 29), existen una extensión K del campo $\mathbb{F}_p((t))$ tal que $P \cong Gal(K/\mathbb{F}_p((t)))$. Como K es una extensión finita y totalmente ramificada (por Observación 3.2 (p. 28)) de $\mathbb{F}_p((t))$, se tiene, por Teorema 1.1 (p. 4), que $K \cong \mathbb{F}_p((t))$. Así $P \leq Aut(\mathbb{F}_p((t)))$. Por la Proposición 2.6 (p. 25), $\mathcal{N}$ tiene indice $p-1$ en $Aut(\mathbb{F}_p((t)))$. Por el principio del palomar $\mathcal{N} \cap P \neq \{1\}$. Sea $|\mathcal{N} \cap P| = p^m$, para $m \leq n$, donde $|P| = p^n$. Si $m < n$, entonces hay un $q \leq p-1$ tal que $qp^m = p^n$, lo cual es una contradicción si $q \neq 1$. Entonces, $n = m$ y $P \leq \mathcal{N}$. □

Para el siguiente lema vamos a suponer la siguiente hipótesis para poder demostrarlo.

Hipótesis 2. *Supongamos que* $\mathbb{F}_p((\widehat{T}))$ *es una extensión finita y separable de* $\mathbb{F}_p((T))$ *de grado p. Sea* ν_T *la valuación usual de* $\mathbb{F}_p((T))$; *esto es,* $\nu_T(T) = 1$. *Entonces,* ν_T *puede extenderse de manera única a una valuación de* $\mathbb{F}_p((\widehat{T}))$ *con* $\nu_T(\widehat{T}) = \dfrac{1}{p}$.

Esta hipótesis implica dos cosas:

1. T debe tener una expresión, en $\widehat{T}$, de la forma $T = \sum_{j\geq p} a_j \widehat{T}^j$, donde $a_j \in \mathbb{F}_p$ y $a_p \neq 0$.
2. Para tal expresión, existe un u tal que a_u es el primer coeficiente, en la expresión de T, tal que $u \not\equiv 0 \mod p$. De lo contrario, T seria una potencia de p en $\mathbb{F}_p((\widehat{T}))$, lo cual nos dice que la extensión es inseparable, una contradicción.

Lema 3.1. *Bajo las condiciones de la hipótesis:*

a) Si $g \in Gal(\mathbb{F}_p((\widehat{T}))/\mathbb{F}_p((T))) \cap \mathcal{N}(\widehat{T})$, y está dado por $g(\widehat{T}) = \widehat{T} + \sum_{j\geq k+1} \alpha_j \widehat{T}^j$ y $\alpha_{k+1} \neq 0$, entonces $u = k(p-1) + p$.

b) Sea $g \in \mathcal{N}(\widehat{T})$ con $g(\widehat{T}) = \widehat{T} + \sum_{j\geq n+1} \alpha_j \widehat{T}^j$, $\alpha_{n+1} \neq 0$, y $g(T) = T + \sum_{j\geq m+1} \beta_j T^j$, $\beta_{m+1} \neq 0$. También supongamos que $u = q(p-1) + p$, con $q > m$. Entonces $n = m$.

Demostración. a) Es claro que $g(T) = T$. Entonces, viendo a $T = T(\widehat{T})$ en $Aut(\mathbb{F}_p((\widehat{T})))$, tenemos que $g(T) = g(T(\widehat{T})) = (g \circ T)(\widehat{T}) = (T \cdot g)(\widehat{T})$ (ver 2.1 (p. 21)). Así,

$$\sum_{i\geq p} a_i \widehat{T}^i = \sum_{i\geq p} a_i (\widehat{T} + \sum_{j\geq k+1} \alpha_j \widehat{T}^j)^i. \tag{3.2}$$

Al desarrollar obtenemos

$$\sum_{i\geq p} a_i \widehat{T}^i = \sum_{i\geq p} a_i \widehat{T}^i + O(\widehat{T}). \tag{3.3}$$

Entonces, $O(\widehat{T}) = 0$. Si $pm_1 \ldots, pm_l$ son las potencias entre p y u en $T(\widehat{T})$, se tiene

$$O(\widehat{T}) = a_p \alpha_{k+1} \widehat{T}^{(k+1)p} + \sum_{e=1}^{l} m_e a_{pm_e} \alpha_{k+1} \widehat{T}^{pm_e+kp} + u a_u \alpha_{k+1} \widehat{T}^{u+k} + \ldots \tag{3.4}$$

Aquí, el primer y tercer término que aparecen son los de menor grado en los que se garantiza que sus coeficientes son no nulos. Para que $O(\widehat{T}) = 0$ es necesario que estos se anulen entre si; es decir, $(k+1)p = u + k$, como queríamos.

b) Tenemos lo siguiente

$$\begin{array}{rcl} T + \sum_{j\geq k+1} \beta_j T^j & = & g(T), \\ & = & g(\sum_{i\geq p} a_i \widehat{T}^i), \\ & = & \sum_{i\geq p} a_i g(\widehat{T})^i, \\ T + \sum_{j\geq m+1} b_j T^j & = & T + Q(T, g, p+k). \end{array}$$

Recuerde que $T = T(\widehat{T})$ y donde $Q(T, g, p+k)$ es como en el Lema 2.1 (p. 21). El término de menor grado del lado izquierdo es $\beta_{m+1} a_p^{m+1} \widehat{T}^{p(m+1)}$. En el lado derecho, al desarrollar, obtenemos $a_p \alpha_{n+1} \widehat{T}^{(n+1)p} + u a_u \alpha_{n+1} \widehat{T}^{u+n} \ldots$.
Tenemos las siguientes posibilidades:

a) Si $a_p\alpha_{n+1}\widehat{T}^{(n+1)p} + ua_u\alpha_{n+1}\widehat{T}^{u+n} = 0$, entonces, por cómo es u, $n = q$ y como $q > m$, y estos términos son los de menor grado, implica que $\beta_{m+1}a_p^{m+1} = 0$. Contradicción.

b) Si $\beta_{m+1}a_p^{m+1}\widehat{T}^{p(m+1)} = ua_u\alpha_{n+1}\widehat{T}^{u+n}$, tenemos que $p(m+1) = u+n$, ó $pm+p-n = u = q(p-1)+p$. Así, $pm-n = q(p-1)$. También debe pasar que $(n+1)p > (m+1)p$, de donde $m < n$ (de lo contrario, se tendría el tercer inciso) lo que lleva a $m(p-1) = pm-m > pm-n = q(p-1)$. Contradicción.

c) Entonces, sólo tenemos $\beta_{m+1}a_p^{m+1}\widehat{T}^{p(m+1)} = a_p\alpha_{n+1}\widehat{T}^{(n+1)p}$, de donde obtenemos $m = n$.

□

Ya vimos que el grupo de Nottingham contiene un copia de cualquier $p-$grupo finito (3.3 (p. 29)). Ahora, por razones que quedarán claras más adelante, analizaremos, en términos de D, dónde están los elementos de los p-grupos. Para ello, empezaremos con el caso cíclico[2]. Denotaremos por D_x la profundidad en $\mathcal{N}(x)$.

Sea C_p un grupo cíclico de orden p. Usando el algoritmo de Witt (Observación 3.1 (p. 27)) en C_p, el cual cumple las hipotesis necesarias[3], tenemos que existe una extensión K de $\mathbb{F}_p((t))$ tal que $Gal(K/\mathbb{F}_p((t))) \cong C_p$.

Recordemos cómo construímos a K: en la hipótesis de la Observación 3.1 (p. 27) $L = C_p$, entonces necesitamos una extensión $F/\mathbb{F}_p((t)$ tal que $Gal(F/\mathbb{F}_p((t))) \cong C_p/L = \{1\}$. Así, podemos usar $F = \mathbb{F}_p((t))$. Entonces, el elemento γ, del inciso *5)* del método de Witt (5 (p. 28)), se toma en $\mathbb{F}_p((t))\backslash\wp(\mathbb{F}_p((t)))$ [4]. Al calcular una raíz θ, de $\gamma = \wp(X)$, en la cerradura algebraica de $\mathbb{F}_p((t))$, y adjuntarla a $\mathbb{F}_p((t))$, obtenemos $\mathbb{F}_p((t))(\theta) = K$. Como nuestra extensión F es totalmente ramificada, $K = \mathbb{F}_p((T))$ para alguna T.

$\mathbb{F}_p((T))$ es una extensión de Galois de grado p, así que podemos extender la valuación ν de $\mathbb{F}_p((t))$ a $\mathbb{F}_p((T))$ de manera que $\nu(T) = \dfrac{1}{p}$ (Ver Hipótesis 2 (p. 29)). Además, podemos escoger el elemento γ, del método de Witt, de tal forma que $\nu(\gamma) = -n$, con $n \in \mathbb{N}$ y $(n,p) = 1$[5]. Como $\wp(\theta) = \gamma$, entonces $\nu(\wp(\theta)) = \nu(\gamma) = -n$.

- Si $\nu(\theta) \geq 0$, se tiene $-n = \nu(\theta^p - \theta) \geq \text{ínf}\{p\nu(\theta), \nu(\theta)\} \geq \nu(\theta)$. Contradicción.
- Entonces, $\nu(\theta) < 0$ y

$$-n = \nu(\theta^p(1-\theta^{1-p})) = p\nu(\theta) + \nu(1-\theta^{1-p}) \tag{3.5}$$

[2]Camina en [1] atribuye este resultado a Weiss.

[3]El grupo de Frattini para este caso se define como $\Phi(P) = P$.

[4]De lo contrario la raíz θ de $\wp(X) = \gamma$ estaría en $\mathbb{F}_p((t))$.

[5]Podemos considerar a γ o a $\widehat{\gamma}$, como en la Observación 3.3 (p. 29). Esto porque si θ es solución a $\wp(X) = \gamma$, entonces $\theta - \mu$ lo es para $\widehat{\gamma}$ y ambas generan la misma extensión.

Ahora, $\nu(\theta^{1-p}) = (1-p)\nu(\theta) > 0$, entonces $\theta^{1-p} \in I_\nu$, en la ν extendida. Así, $1-\theta^{1-p}$ es invertible; es decir, de valuación cero. Por esto, de la ecuación 3.5, obtenemos $\nu(\theta) = -\frac{n}{p}$.

Como $(n,p) = 1$, existen $c, d \in \mathbb{Z}$ tal que $cp - dn = 1$. Usando que $K = \mathbb{F}_p((T)) = \mathbb{F}_p((t))(\theta)$, $T = \sum a_i \theta^i t^j$. Sin pérdida de generalidad podemos suponer que $T = \theta^d t^c$, esto porque los automorfismos de $\mathbb{F}_p((T))$ preservan la valuación (ver sección 1.1.2 (p. 6)). Así

$$\nu(T) = w(\theta^d t^c) = d\nu(\theta) + c\nu(t) = \frac{-dn}{p} + c = \frac{-dn + cp}{p} = \frac{1}{p}.$$

Es decir, $K = \mathbb{F}((T))$, para $T = \theta^d t^c$.

Sea $\langle g \rangle = Gal(\mathbb{F}_p((T))/\mathbb{F}_p((t)))$. Entonces, $\langle g \rangle \subset \mathcal{N}(T)$ pues g es de orden p en $Aut(F_p((T)))$ (como en la demostración de Teorema 3.3 (p. 29)). Por la última parte de la Observación 3.1 (p. 27) podemos asumir que $g(\theta) = \theta + 1$. Entonces,

$$\begin{aligned} g(T) &= g(\theta^d t^c) = (\theta+1)^d t^c = \left(\sum_{i=0}^{d} \binom{d}{i} \theta^{d-i}\right) t^c = \sum_{i=0}^{d} \binom{d}{i} \frac{T}{\theta^i}, \\ &= T + d\frac{T}{\theta} + \ldots \frac{T}{\theta^d}. \end{aligned}$$

Así, $\nu\left(\frac{T}{\theta^x}\right) = \nu(T) - x\nu(\theta) = \frac{1+xn}{p}$ y buscamos el mínimo de esta expresión para $x = 1 \ldots d$. Esto se obtiene en $x = 1$; es decir, la menor potencia de T en la expresión de $(g - id)(T)$ es T^{n+1}, con lo que tenemos el siguiente resultado.

Lema 3.2 (Weiss)**.** *Sea g el generador del grupo $Gal(\mathbb{F}_p((T))/\mathbb{F}_p((t)))$, entonces $D_T(g) = n$*

Ahora vamos a probar que la profundidad no cambia en las extensiones. Para esto procedemos por inducción en la potencia de la cardinalidad de un $p-$grupo. El caso $n = 1$ es el lema anterior.

Sea P un $p-$grupo de orden p^n y K una extensión de $\mathbb{F}_p((t))$ que cumplen las Hipótesis 1 (p. 28). Como $P/L \cong Gal(K/\mathbb{F}_p((t)))$ y $|P/L| < p^n$, por inducción $K = \mathbb{F}_p((T))$ y es totalmente ramificada. Entonces, por el algoritmo de Witt (3.1 (p. 27)) $\widehat{K} = K(\theta) = \mathbb{F}_p((\widehat{T}))$, para una variable $\widehat{T}$.

Si $g \in Gal(\mathbb{F}_p((\widehat{T}))/\mathbb{F}_p((t)))$, entonces $g \in \mathcal{N}(\widehat{T})$ por tener orden una potencia de p.

Ahora, por la Observación 3.2 (p. 28) tenemos que el homomorfismo al cociente $P \to P/L$ induce un homomorfismo

$$\pi : Gal(\mathbb{F}_p((\widehat{T}))/\mathbb{F}_p((t))) \to Gal(\mathbb{F}_p((T))/\mathbb{F}_p((t))), \tag{3.6}$$

el cual es sólo restringir a $\mathbb{F}_p((T))$.

Teorema 3.4. *Sea $g \in Gal(\mathbb{F}_p((\widehat{T}))/\mathbb{F}_p((t)))$ con $\pi(g) \neq id$. Entonces, existe un γ, y por ello una extensión $\widehat{K} = \mathbb{F}_p((\widehat{T}))$, tal que*

$$D_T(\pi(g)) = D_{\widehat{T}}(g). \tag{3.7}$$

Antes una observación.

Observación 3.4. *Dado $\gamma \in \mathbb{F}_p((T))$, como en el método de Witt, siempre podemos modificarlo para que su valuación sea tan pequeña como queramos.*

Demostración. Para esto, es suficiente sumar un elemento b, con valuación muy pequeña, que esté en la imagen de $\widehat{i} : \mathbb{F}_p((t))/\wp(\mathbb{F}_p((t))) \to \mathbb{F}_p((T))/\wp(\mathbb{F}_p((T)))$, función inducida por la inclusión $i : \mathbb{F}_p((t)) \to \mathbb{F}_p((T))$. Que esté en la imagen de $\widehat{i}$ es para garantizar que sea solución de la ecuación en el inciso 5) de la Observación 3.1 (p. 27). Para ver que siempre podemos elegir un elemento como éste, es necesario ver que la imagen de $\widehat{i}$ tiene dimensión infinita como $\mathbb{F}_p$-espacio, esto por la base dada en el Lema 3.1 (p. 29). Para ver que la imagen tiene dimensión infinita, es suficiente ver que el kernel tiene dimensión finita. Para eso, veamos lo siguiente:

1. $\ker(\widehat{i}) = \dfrac{\mathbb{F}_p((t)) \cap \wp(\mathbb{F}_p((T)))}{\wp(\mathbb{F}_p((t)))}$.
2. Dado $y \in \mathbb{F}_p((t)) \cap \wp(\mathbb{F}_p((T)))$, existen $f \in \mathbb{F}_p((t))$ y $\mu \in \mathbb{F}_p((T))$ tales que $f = y = \wp(\mu)$. Esto quiere decir que μ es raíz de la ecuación $f = \wp(X)$. Nótese que $\mu + j$ sigue siendo raíz de la ecuación para $j \in \mathbb{F}_p$. Dado $\sigma \in G = Gal(\mathbb{F}_p((T))/\mathbb{F}_p((t)))$, tenemos $\sigma(y) = y$, no se altera la ecuación, pero como $\mu \in \mathbb{F}_p((T))$, $\sigma(\mu)$ debe ser raíz; es decir, σ permuta las raíces de la ecuación. Así $\sigma(\mu) = \mu + x_\sigma$.
3. Defina $\widetilde{y} : G \to \mathbb{F}_p$, como $\widetilde{y}(\sigma) = x_\sigma$. Es claro que es un homomorfismo.
4. La función $y \mapsto \widetilde{y}$ es una transformación lineal de $\mathbb{F}_p$-espacios, lo cual se obtiene de que $\wp$ lo sea.
5. $\ker(y \mapsto \widetilde{y}) = \wp(\mathbb{F}_p((t)))$, pues la única manera de que $\widetilde{y}(\sigma) = 0$, para todo $\sigma \in G$, es que $\mu \in \mathbb{F}_p((t))$.

Así, $ker(\widehat{i}) \subset \hom(G, \mathbb{F}_p)$, el cual es finito. Esto implica que $ker(\widehat{i})$ es de dimensión finita sobre $\mathbb{F}_p$. □

Ahora la demostración del teorema.

Demostración. Supongamos que ν es la valuación de $\mathbb{F}_p((T))$ y la extendemos a $\mathbb{F}_p((\widehat{T}))$ como $\nu(\widehat{T}) = 1/p$. Como en la Observación 3.3 (p. 29), dado $\gamma \in \mathbb{F}_p((T))$, tenemos μ, $\widehat{\gamma} \in \mathbb{F}_p((T))$ tales que $\gamma = \widehat{\gamma} + \wp(\mu)$, con $\nu(\widehat{\gamma}) = -n$, $n \in \mathbb{N}$ y n no multiplo de p.

Por la observación anterior (3.4), podemos escoger γ tal que $\nu(\gamma) < -D_T(g)$. Sea $L = \langle l \rangle$ como en las Hipótesis 1 (p. 28). Entonces, podemos construir una $\widehat{T}$ tal que $\mathbb{F}_p((T))(\theta) = \mathbb{F}_p((\widehat{T}))$ y obtener que $D_{\widehat{T}}(\bar{l}) = n$, como en el Lema 3.2 (p. 32). Así,

$$\bar{l}(\widehat{T}) = \widehat{T} + \sum_{j \geq n+1} \alpha_j \widehat{T}^j, \quad \alpha_{n+1} \neq 0.$$

Como la extensión $\mathbb{F}_p((\widehat{T}))$ es de grado p, por Hipótesis 2 (p. 29), $T = \sum_{i \geq p} a_i \widehat{T}^i$, con $a_p \neq 0$. Como en el Lema 3.1 (p. 30), tenemos que el primer elemento no nulo y con índice no multiplo de p, a_u, cumple que $u = n(p-1) + p$.

Ahora, si $D_T(\pi(g)) = m$, $D_{\widehat{T}}(g) = n_1$ y como $-n = \nu(\gamma) < -D_T(g) = -m$, entonces $n > m$, con $u = n(p-1) + p$. Por la parte b) del Lema 3.1 (p. 30), tenemos que $m = n_1$; esto es, $D_T(\pi(g)) = D_{\widehat{T}}(g)$. □

3.3 EL TEOREMA DE CAMINA

Ahora el tema central del trabajo.

Lubotzky y Wilson en [8] prueban lo siguiente.

Teorema 3.5 (Lubotzky y Wilson)**.** *Existe un pro-p grupo 2-generado en el cual todo pro-p grupo con base numerable puede ser encajado.*

Usando este teorema y el siguiente resultado obtenemos como corolario el Teorema 2.1 (p. 26)

Teorema 3.6 (Camina)**.** *Cualquier pro-p grupo finitamente generado puede ser encajado como un subgrupo cerrado en $\mathcal{N}$.*

Demostración. Sea P un pro-p grupo finitamente generado por $X = \{x^1, \ldots, x^r\}$; esto es $P = \overline{\langle X \rangle}$. Por la Proposición 1.15 (p. 10) $P \cong \varprojlim P_m$, donde los P_m forman un sistema inverso de p-grupos finitos indexados por $\mathbb{N}$ (Proposición 1.14 (p. 9)). Por el método de Witt, P_m se encaja en $\mathbb{F}_p((T_m))$ y podemos contruir las extensiones de tal forma que $\mathbb{F}_p((T_m))$ sea extensión propia de $F_p((T_{m+1}))$.

Para cada $x^\alpha \in X$, pongamos $x^\alpha = (s_j^\alpha) \in \varprojlim P_m$, con $s_m^\alpha \in P_m$. Usando el encaje $P_m \hookrightarrow \mathcal{N}(T_m)$, entonces $s_m^\alpha \mapsto o_m^\alpha \in \mathcal{N}(T_m)$. Definamos $f_m : \mathcal{N}(T_m) \to \mathcal{N}(T)$, como $g(T_m) \mapsto g(T)$; es decir,

$$T_m + \sum \alpha_i T_m^i \mapsto T + \sum \alpha_i T^i,$$

donde $\mathcal{N}(T)$ es el grupo de Nottingham para alguna variable T. Es claro que los f_m son isomorfismos y que $D_T(f_m(g)) = D_{T_m}(g)$, para todo $g \in \mathcal{N}(T_m)$. Entonces, cada generador x^α define una sucesión de elementos en $\mathcal{N}(T)$.

$$\begin{array}{ccccccccc} x^\alpha & \mapsto & (s_m^\alpha) & \overset{\pi_m}{\longmapsto} & s_m^\alpha & \overset{f_m}{\longmapsto} & o_\alpha & \mapsto & f_m(o_m^\alpha) = y_m^\alpha \\ \Uparrow & & \Uparrow & & \Uparrow & & \Uparrow & & \Uparrow \\ P & & \varprojlim P_m & & P_m & & \mathcal{N}(T_m) & & \mathcal{N}(T) \end{array}$$

Así, $\{y_m^\alpha\}$ es la sucesión asociada a x^α en $\mathcal{N}(T)$. Consideremos la sucesión

$$\Gamma := \{(y_m^1, \ldots, y_m^r)\} \text{ en } \underbrace{\mathcal{N}(T) \times \cdots \times \mathcal{N}(T)}_{r-veces} =: \mathcal{N}(T)^{\times r}.$$

Por el teorema de Tychonoff, $\mathcal{N}^{\times r}$ es compacto. Así, Γ tiene una subsucesión $Y = \{(y_{m_i}^1, \ldots, y_{m_i}^r)\}$ convergente. Sea $z = (z^1, \ldots, z^r) = \lim Y$. Sea $LP = LP(\eta_1, \ldots, \eta_r)$ el pro-p grupo libre en r generadores. Como P está generado por r elementos, entonces, para cada $h \in P$ existe $w \in LP$ tal que $w(X) = w(x^1, \ldots, x^r) = h$.

Definimos $F : P \to \mathcal{N}(T)$ como $F(h) = w(z)$. Veamos que F está bien definida.

Antes, note que $w : \mathcal{N}(T)^{\times r} \to \mathcal{N}(T)$ es continua. Para esto tenemos dos casos:

1. Si w es de longitud finita: la continuidad se sigue de que $\mathcal{N}(T)$ es un grupo topológico.
2. Si w es de longitud infinita[6]: tenemos que w es continua porque $\pi_m \circ w : \mathcal{N}(T)^{\times r} \to \mathcal{N}(T)/\mathcal{N}(T)_m$ lo son, para cada m.

Para ver que F está bien definida, es suficiente ver que si $w(X) = 1$, entonces $w(z) = 1$. Pero esto se sigue de la continuidad de w; si $w(X) = 1$, entonces

$$\begin{array}{rcl} w(s_m^1, \ldots, s_m^r) & = & 1, \text{ luego} \\ w(y_m^1, \ldots, y_m^r) & = & 1, \text{ para toda } m, \text{ con lo que} \\ w(y_{m_i}^1, \ldots, y_{m_i}^r) & = & 1, \text{ así} \end{array}$$

$$w(z) = w(\lim Y) = \lim w(Y) = 1.$$

Por ello, F está bien definida y es un homomorfismo. Por el Corolario 1.1 (p. 10) es continua.

Para la inyectividad, sea $h \neq 1$ y $h = w(X) \in P$. Entonces, $F(h) = w(z) = \lim w(Y)$. Como $h \neq 1$, $w(s_m^1, \ldots, s_m^r) \neq 1$ para m grande, lo que implica $w(y_m^1, \ldots y_m^r) \neq 1$, para la misma m. Así, $Y_i = (y_{m_i}^1, \ldots, y_{m_i}^r)$ tiene profundidad $D_T(Y_i) = d_i$. Pero por el Teorema 3.4 (p. 33), $d = d_i = d_{i+j}$, $\forall j > 0$. Por lo tanto

$$D_T(F(h)) = D_T(w(z)) = D_T(\lim w(Y)) = \lim D(w(Y)) = d.$$

[6]Lo entendemos como un límite. Recordemos que los grupos profinitos son completos (Proposición 1.11 (p. 7))

Entonces, $F(h) \neq T$ en $\mathcal{N}(T)$; es decir, es inyectiva. Como P es compacto y $\mathcal{N}(T)$ Hausdorff, un resultado clásico de topología nos dice que una función continua entre un espacio compacto y uno Hausdorff tiene imagen compacta. Como $\mathcal{N}(T)$ es compacto (Definición 1.7 (p. 7)), entonces la imagen es cerrada. Se sigue que $F(P)$ es cerrado. □

Corolario 3.1 (Camina)**.** *Cualquier pro-p grupo con base numerable puede ser encajado como un subgrupo cerrado de* $\mathcal{N}(T)$*.*

Capítulo 4
Generalizaciones

El grupo de Nottingham se puede generalizar a una variedad de contextos. En este capítulo consideraremos tres generalizaciones: el caso de coeficientes y la variable no conmutativos, el caso de una variable no asociativa y el caso de series de potencias con las potencias no necesariamente enteros. En los tres casos demostramos que las series de potencias bajo sustitución forman un grupo y calculamos su álgebra de Lie asociada. Además, probamos que en los primeros casos, el grupo es residualmente nilpotente.

4.1 Caso No Conmutativo

Sean R un anillo no conmutativo con identidad y T una variable que no conmuta con algunos elementos en $R - \{1, 0\}$. Tenemos lo siguiente:

- Un monomio de grado n es una expresión de la forma $a_0 T a_1 T a_2 T \dots T a_n$, con $a_j \in R$. Aquí no excluimos las potencias de T, pues $T^n = \underbrace{1T1T\dots1T1}_{n-veces}$.
- Dos monomios $a_0 T a_1 T a_2 T \dots T a_n$ y $b_0 T b_1 T b_2 T \dots T b_m$ son iguales si $n = m$ y $a_k = b_k$, para todo $k = 0, \dots n$.
- Un polinomio de grado n es una expresión de la forma

$$a + \sum a_{i_0} T a_{i_1} + \sum a_{j_0} T a_{j_1} T a_{j_2} + \cdots + \sum a_{k_0} T \dots T a_{k_n}$$

  donde la sumas son finitas.[1]
- Una serie formal es una suma infinita de la forma

$$a + \sum a_{i_0} T a_{i_1} + \sum a_{j_0} T a_{j_1} T a_{j_2} + \dots,$$

  donde la sumas son finitas.

Notación: Sea $I = (i_0, \dots, i_n) \in \mathbb{N}^{n+1}$ un vector de índices. Diremos que I tiene longitud n, denotado como $|I| = n$, si $I \in \mathbb{N}^{n+1}$. Usaremos la notación $a_I(T) := a_{i_0} T a_{i_1} T \dots T a_{i_n}$, con $a_{i_r} \in R$ y $\sum_{|I|=k} a_I(T)$ indica una suma de monomios de grado k.

[1] Así, los monomios de grado n, como $\mathbb{Z}$-módulos, son isomorfos a $R^{\otimes(n+1)}$, el producto tensorial sobre $\mathbb{Z}$

Con esta notación dos monomios $a_I(T)$ y $b_J(T)$ son iguales si y sólo si $J = I = (i_o, \dots, i_n)$ y $a_{i_k} = b_{i_k}$, para todo $k = 0, \dots n$.

Como lo que nos interesan son las sustituciones, emplearemos la siguiente forma para abreviarlas: sean $n, k \in \mathbb{N}$, con $1 \leq k \leq n$; $I = (i_0, \dots, i_n)$ y $X_1, \dots X_k$ algunas variables. Definimos

$$a_I(T)[(X_1)_{j_1}, \dots, (X_k)_{j_k}] := a_{i_0} T \dots T a_{j_1 - 1} X_1 a_{j_1} T \dots T a_{j_k - 1} X_k a_{j_k} T \dots a_{i_{n-1}} T a_{i_n}, \tag{4.1}$$

donde $j_1, \dots, j_k \in \{1, \dots, n\}$ son distintos. Esto es, sustituimos X_l en la posición j_l, $l = 1, \dots k$. No es necesario que $j_1 < j_2 < \dots < j_k$ aunque eso parece en 4.1.

Consideremos $R[[T]]$ las series de potencias en la variable T; esto es, dado $s \in R[[T]]$, entonces $s = a + \sum_{n \geq 1} \sum_{|I|=n} a_I(T)$. Es claro que $R[[T]]$ es un anillo (R-álgebra) no conmutativo con 1, ya que $[T, 1] = 0$. Definimos $\mathcal{N}_{nc}(T, R)$ de manera análoga al grupo de Nottingham:

$$\mathcal{N}_{nc}(T, R) := \left\{ \alpha \in R[[T]] \;\middle|\; \alpha = T + \sum_{n \geq 2} \sum_{|I|=n} a_I(T) \right\}. \tag{4.2}$$

Tomemos la misma operación que antes; si $\alpha, \beta \in \mathcal{N}_{nc}(T, R)$ y $\alpha = T + \sum_{n \geq 2} \sum_{|I|=n} a_I(T)$, definimos $\alpha\beta = \alpha(\beta) = \beta + \sum_{n \geq 2} \sum_{|I|=n} a_I(\beta)$, la cual es asociativa. Si $\beta = T + \sum_{m \geq 2} \sum_{|J|=n} b_J(T)$, entonces, al desarrollar, obtenemos

$$\alpha\beta = \beta + \alpha - T + \sum_{n \geq 2} \sum_{|I|=n} \left\{ \sum_{l=1}^{n} \sum_{1 \leq r_1 < \dots < r_l \leq n} \left(\sum_{\nu \in F} \sum_{|J_1|=\nu_1} \cdots \sum_{|J_l|=\nu_l} a_I(T)[(b_{J_1})_{r_1} \dots, (b_{J_l})_{r_l}] \right) \right\}, \tag{4.3}$$

donde $F \subset (\mathbb{N} - \{1\})^l$, es el conjunto de todos los posibles grados.

Observación 4.1. *La ecuación 4.3 se sigue de que*

$$a_I(T + \theta) = a_{i_0}(T + \theta) a_{i_1} \dots a_{i_{n-1}}(T + \theta) a_{i_n} = a_I(T) + \sum_{k=1}^{|I|} \sum_{1 \leq r_1 < \dots < r_l \leq |I|} a_I(T)[(\theta)_{r_1}, \dots, (\theta)_{r_k}], \tag{4.4}$$

donde la suma sobre los $r's$ son todos las posibles sustituciones que uno puede hacer de los b_{J_i} en $a_I(T)$, la suma de l son la cantidad de sustituciones que se están haciendo en $a_I(T)$, por eso $1 \leq l \leq n = |I|$; y la suma sobre los ν son los grados de los monomios que se están sustituyendo.

Sea $\gamma = \alpha\beta$. Denotemos por C_k, $k > 1$, la suma de todos los monomios de grado k en γ. Así, deducimos de la ecuación 4.3 (p. 38) que

$$C_2 = \sum_{|J|=2} b_J(T) + \sum_{|I|=2} a_I(T), \tag{4.5}$$

$$C_k = \sum_{|J|=k} b_J(T) + \sum_{|I|=k} a_I(T) + \sum_{s=2}^{k-1} \sum_{|J|=s} \sum_{l=1}^{s} \sum_{\substack{J_1, \dots, J_l \\ |I| + \sum |J_e| - l = k}} \sum_{1 \leq r_1 < \dots < r_l \leq s} a_I(T)[(b_{J_1}(T))_{r_1}, \dots, (b_{J_l}(T))_{r_l}].$$

Vemos que $|I| + \sum |J_e| - l = k$ se debe a que cada vez que sustituimos un monomio de grado $|J_e|$ sumamos su grado, pero esto nos cuesta un lugar, que se traduce en restar 1 al grado de $a_I(T)$. Como sustituimos l monomios, restamos esta cantidad. Al final, igualamos a k, porque buscamos l monomios cuyas suma grados satisfagan dicha ecuación; esto es, que el resultado sea de grado k.

Como antes, $\mathcal{N}_{nc}(T, R)$ conjunto forma un grupo con la operación de sustitución.

Proposición 4.1. *$\mathcal{N}_{nc}(T, R)$ es un grupo con la operación definida arriba.*

Demostración. La operación es cerrada, asociativa y T juega el papel de neutro de la operación. Tómese $\alpha \in \mathcal{N}_{nc}(T, R)$. Queremos encontrar un $x = T + \sum_m \sum_J x_J(T)$ para el cual $\alpha x = T$. Por la primera ecuación en 4.5 (p. 38), obtenemos que los conjuntos de índices deben de ser iguales, y si $I = J$, entonces $-a_I(T) = x_I(T)$. Para $k > 2$, se complica encontrar una forma explícita de calcular los monomios necesarios, pero se puede hacer lo siguiente: de las ecuaciones 4.5 (p. 38), vemos que para k

$$\sum_{|J|=k} x_J(T) = -\sum_{|I|=k} a_I(T) + E(a_{I'}(T), k) \tag{4.6}$$

donde $E(a_{I'}(T), k)$ es la serie de grado k (todos sus monomios son de grado k), cuyos coeficientes son productos de los coeficientes de $a_{I'}$, donde I' corre sobre los índices en α de longitud $\leq k - 1$, dada en la segunda ecuación de 4.5 (p. 38). Escriba $-\sum_{|I|=k} a_I(T) + E(a_{I'}(T), k) = \sum_{|N|=k} e_N(T)$, después de simplificar, si fuera posible. Entonces, el inverso se halla haciendo que $\{J's\} = \{N's\}$ y $x_N(T) = -e_N(T)$. Por construcción $\alpha x = T$. Del argumento dado por la ecuación 2.5 (p. 20) obtenemos que $x = \alpha^{-1}$, es el inverso. □

Tal vez no sea fácil calcular los inversos, pero podemos tener una idea de cómo son sus términos de mínimo grado distintos de T.

Observación 4.2. *De las ecuaciones 4.5 uno obtiene que si $\alpha = T + \sum_{|I|=n} a_I(T) + \ldots$, entonces $\alpha^{-1} = T - \sum_{|I|=n} a_I(T) + \ldots$. Esto se sigue de que si no aparecen términos de grado menor a n, el tercer término de la segunda ecuación en las ecuaciones 4.5 es cero.*

Al igual que antes, definimos $L_k := \{T + \sum_{n>k} \sum_{|I|=n} a_I(T)\}$ y $D_{nc}(\alpha) := n$ si y sólo si $\alpha \in L_n / L_{n+1}$, la «profundidad» de α. Es claro que $D_{nc}(T) = \infty$. Probaremos que es una filtración y calcularemos el anillo de Lie asociado a ésta. Para tal efecto, es necesario conocer el comportamiento del conmutador en el grupo. El siguiente lema nos dice cómo es éste.

Lema 4.1. *Sean $\alpha = T + \sum_{|I|=n} a_I(T) + \ldots$ y $\beta = T + \sum_{|J|=m} b_J(T) + \ldots$. Entonces,*

$$\mathbf{c}(\alpha, \beta) = T + \sum_{|I|=n} \sum_{|J|=m} \sum_{\substack{r=1 \\ s=1}}^{n,m} \{a_I(T)[(b_J(T))_r] - b_J(T)[(a_I(T))_s]\} + E(\alpha, \beta, m + n - 1), \tag{4.7}$$

donde $E(\alpha, \beta, n+m-1) =: E \in R[[T]]$ *donde sus coeficientes son productos de los coeficientes de* α *y* β*, y satisface* $D_{nc}(T+E) \geq m+n$.

Demostración. Seguiremos los mismos pasos de la demostración del Lema 2.1 (p. 21). Por la ecuación 4.3 (p. 38)

$$\begin{aligned}
(\alpha\beta)\alpha^{-1} &= \left(\beta+\alpha-T+\sum_{|I|=n}\sum_{|J|=m}\sum_{r=1}^{n} a_I(T)[(b_J(T))_r]+E'\right)\alpha^{-1},\\
&=\beta\alpha^{-1}+\alpha\alpha^{-1}-\alpha^{-1}+\left(\sum_{|I|=n}\sum_{|J|=m}\sum_{r=1}^{n} a_I(T)[(b_J(T))_r]\right)(\alpha^{-1})+E'(\alpha^{-1}),\\
&=\left(\beta+\alpha^{-1}-T-\left(\sum_{|J|=m}\sum_{|I|=n}\sum_{s=1}^{m} b_J(T)[(a_I(T))_s]\right)+E''\right)+\\
&\quad T-\alpha^{-1}+\left(\sum_{|I|=n}\sum_{|J|=m}\sum_{r=1}^{n} a_I(T)[(b_J(T))_r]+E'''\right)+E',\\
&=\beta-\sum_{|J|=m}\sum_{|I|=n}\sum_{s=1}^{m} b_J(T)[(a_I(T))_s]+\sum_{|I|=n}\sum_{|J|=m}\sum_{r=1}^{n} a_I(T)[(b_J(T))_r]+E,\\
&=\beta+\sum_{|J|=m}\sum_{|I|=n}\sum_{\substack{r=1\\s=1}}^{n,m}\{a_I(T)[(b_J(T))_r]-b_J(T)[(a_I(T))_s]\}+E,
\end{aligned}$$

con $E = E' + E'' + E'''$. Se sigue que,

$$\begin{aligned}
\mathbf{c}(\alpha,\beta) &= \beta\beta^{-1}+\sum_{|J|=m}\sum_{|I|=n}\sum_{\substack{r=1\\s=1}}^{n,m}\{a_I(T)[(b_J(T))_r]-b_J(T)[(a_I(T))_s]\}(\beta^{-1})+E(\beta^{-1})\\
&=T+\sum_{|J|=m}\sum_{|I|=n}\sum_{\substack{r=1\\s=1}}^{n,m}\{a_I(T)[(b_J(T))_r]-b_J(T)[(a_I(T))_s]\}+E.
\end{aligned}$$

□

Observación 4.3. $D_{nc}(\mathbf{c}(\alpha,\beta)) \geq n+m+1$ *si* $D_{nc}(\alpha) = n$ *y* $D_{nc}(\beta) = m$.

Con todo esto, tenemos el siguiente resultado, ya esperado, sobre D_{nc}.

Proposición 4.2. D_{nc} *es una filtración en* $\mathcal{N}_{nc}(T,R)$.

Demostración. Por definición D_{nc} cumple 1) y 2) de la definición de filtración (1.9 (p. 11)). 3) se sigue de la ecuación 4.3 (p. 38) y la Observación 4.2 (p. 39); 4) se sigue del lema anterior (4.1 (p. 39)). □

Es claro que $\mathcal{N}_{nc}(T,R)_k = L_k$ y $\{\mathcal{N}_{nc}(T,R)_k\}_{k\in\mathbb{N}}$ es una serie central. Además, $\bigcap L_k = \{T\}$. Tenemos el siguiente resultado.

Proposición 4.3. *$\mathcal{N}_{nc}(T,R)$ es residualmente nilpotente.*

Una última observación sobre este caso.

Observación 4.4. *Hay dos subgrupos conocidos para este caso. Estos son al considerar series donde todos los monomios tiene último coeficiente $a_n = 1$ y al considerar el primer coeficiente $a_0 = 1$.*

4.1.1 ANILLO DE LIE ASOCIADO A D_{nc}

Antes, una observación sobre las clases de equivalencia en $\mathcal{N}_{nc}(T,R)/L_k$.

Observación 4.5. *$\mathcal{N}_{nc}(T,R)/L_k = \{T + \sum_{j\geq 2}^{k}\sum_{|I|=j} a_I(T)\}$. Esto porque para que dos elementos $\alpha,\beta \in \mathcal{N}_{nc}(T,R)$ estén relacionados, es necesario que $D_{nc}(\alpha\beta^{-1}) > k$. Así, por las ecuaciones 4.5 (p. 38), y un desarrollo análogo al de la Observación 2.3 (p. 22), uno obtiene que $C_2 = \cdots = C_k = 0$ implica que los índices en cada grado, hasta grado k, de α y β sean iguales, y que $a_I(T) = b_I(T)$, con $|I| = j$ y $2 \leq j \leq k$.*

Así,

$$\mathtt{gr}_{D_{nc},k}(\mathcal{N}_{nc}(T,R)) = L_k/L_{k+1} = \left\{ T + \sum_{|I|=k+1} a_I(T) \right\} \cong R^{\otimes(k+2)}. \tag{4.8}$$

Entonces,

$$\mathtt{gr}_{D_{nc}}(\mathcal{N}_{nc}(T,R)) \cong \bigoplus_{k\geq 1} R^{\otimes(k+2)}, \tag{4.9}$$

donde el corchete de Lie está dado por

$$\left[\left(\sum_{|I|=n} a_I(T) \right) \left(\sum_{|J|=m} b_J(T) \right) \right] = \sum_{|I|=n}\sum_{|J|=m}\sum_{\substack{r=1\\s=1}}^{n,m} \{a_I(T)[(b_J(T))_r] - b_J(T)[(a_I(T))_s]\}. \tag{4.10}$$

4.2 CASO NO ASOCIATIVO

Aquí trabajaremos con una variable x que es no asociativa. Llamaremos una palabra de longitud n en x al producto, en alguna forma, de x consigo mismo n veces y la denotaremos como $w_n(x)$. Al conjuntos de todas las palabras de longitud n lo denotamos como W_n. La palabra de longitud cero es 1. Así, tenemos que $W_1 = \{x\}$, $W_2 = \{x^2\}$, $W_3 = \{x(x^2), (x^2)x\}, \ldots$

Un polinomio de grado n en x es una expresión de la forma

$$\sum_{j=0}^{n} \sum_{w_j \in W_j} a_{j,w_j} w_j(x), \tag{4.11}$$

mientras que una serie es de la forma

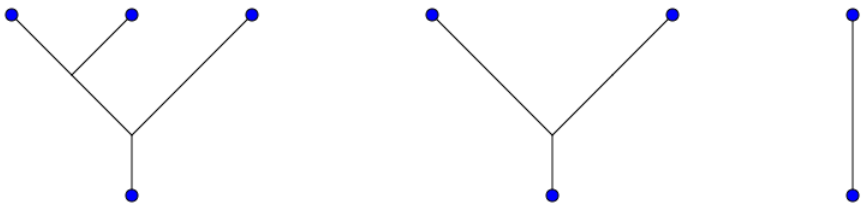
$$\sum_{j\geq 0} \sum_{w_j \in W_j} a_{j,w_j} w_j(x). \tag{4.12}$$

Aquí no hacemos distinción sobre la finitud de la segunda suma, pues vemos que $|W_j| < \infty$, para todo j.

ÁRBOLES BINARIOS PLANOS CON RAÍZ Y POTENCIAS DE x

Definición 4.1. *Un árbol binario plano con raíz es una gráfica orientada con sólo una raíz y cada vértice distinto a la raíz es trivalente; esto es, tiene una raíz y dos hojas. Decimos que v es un vértice (o punto) interior de la gráfica G si $\#\{A \in E(G) \mid \{v\} \cap A\} > 1$, donde $E(G)$ es el conjunto de aristas de G.*

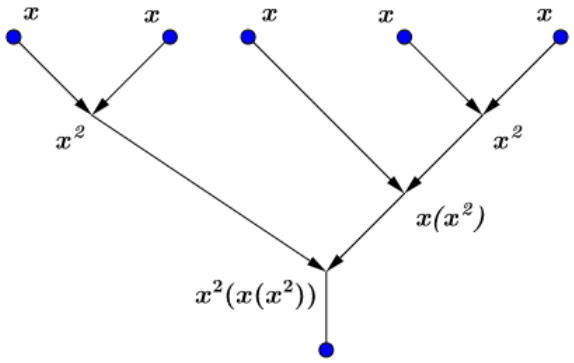
Decimos que un arbol binario plano con raíz tiene $n+1$ hojas si el número de vértices interiores es n. Por ejemplo, la imagen de abajo muestra dos árboles binarios planos con raíz de 3 hojas.



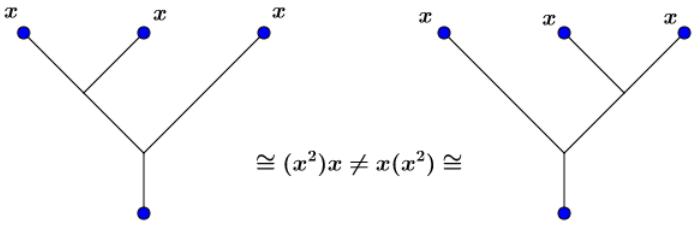
De ahora en adelante llamaremos sólo árboles o $n-$árboles a los árboles binarios planos con raíz de $n+1$ hojas, donde cada hoja es un vértice no interior distinto de la raíz. Denotemos como T_n al conjunto de todos los $n-$árboles.

Proposición 4.4. *Hay una biyección entre W_{n+1} y T_n*

Tal relación se da colocando en cada hoja la variable x y haciendo la multiplicación de arriba hacia abajo siguiendo la orientación de las aristas hasta la raíz. La siguente imagen muestra un ejemplo de cómo realizar el producto.



Esta descripción en efecto de los productos como árboles nos identifica perfectamente cada monomio de grado n. Por ejemplo la siguiente imagen tenemos dos 3-árboles distintos y vemos que sus respectivos monomios son distintos.



El número de $n-$árboles es el $n-$ésimo número de Catalan, el cual es $c_n = \frac{1}{n+1}\binom{2n}{n}$. Entonces, para cada n tenemos un número finito de monomios mónicos en x pues $|W_n| = |T_{n-1}| = c_{n-1}$.

Tenemos una operación básica en los árboles la cual es unir las raíces para formar otro arbol binario, esto se traduce en multiplicar sus respectivos monomios asociados. De la misma forma, hacer sustitución en los monomios; esto es $w_j(w_i)$, es "pegar" el árbol asociado a w_i en cada hoja de w_j.

Como nos interesan las sustituciones usamos, como en la sección anterior, la siguiente notación: Sea w una palabra (de alguna longitud), entonces $w(x)[(A_1)_{r_1}, \dots (A_k)_{r_k}]$ significa sustituir los A_j en las "posiciones" r_j, con $1 \leq r_j \leq$ longitud de w. Como w representa un árbol, entendemos la "posición" j como la $j-$ésima hoja contando de izquierda a derecha. Con esto tenemos

$$w_n(x+\theta) = w_n(x) + \sum_{l=1}^{n} \sum_{1 \leq r_1 < \dots < r_l \leq n} w_n(x)[(\theta)_{r_1}, \dots (\theta)_{r_l}], \tag{4.13}$$

donde la primera suma significa el número de sustituciones.

Nos interesa son las series de potencias en la variable x. Sea R un anillo conmutativo con 1. Definimos

$$\mathcal{N}_{NA}(R,x) := \{x + \sum_{k>1} \sum_{w_k \in W_k} a_{k,w_k} w_k(x) \mid a_{k,w_k} \in R\} \tag{4.14}$$

Entonces, al igual que antes, definimos la operación de dos elementos $\alpha = x + \sum_{i\geq 2} \sum_{w_i \in W_i} a_i w_i(x)$ y $\beta = x + \sum_{j\geq 2} \sum_{w_j \in W_j} b_j w_j(x)$ en $\mathcal{N}_{NA}(R,x)$ como

$$\begin{aligned}
\alpha\beta =& \beta + \sum_{i\geq 2} \sum_{w_i \in W_i} a_i w_i(\beta), \\
=& \beta + \sum_{i\geq 2} \sum_{w_i \in W_i} a_i w_i \left(x + \sum_{j\geq 2} \sum_{w_j \in W_j} b_j w_j(x) \right), \\
=& \beta + \sum_{i\geq 2} \sum_{w_i \in W_i} a_i \Bigg(w_i(x) + \\
& \sum_{l=1}^{i} \left(\sum_{1\leq r_1 < \ldots < r_l \leq i} \left(\sum_{j_1,\ldots j_l \geq 2} \left(\sum_{w_{j_1} \in W_{j_1}, \ldots, w_{j_l} \in W_{j_l}} b_{j_1} \ldots b_{j_l} w_n(x) [(w_{j_1}(x))_{r_1}, \ldots, (w_{j_l}(x))_{r_l}] \right) \right) \right) \Bigg), \\
=& \beta + \alpha - x + \sum_{i\geq 2} \sum_{w_i \in W_i} \left(\sum_{r=1}^{i} \sum_{j\geq 2} \sum_{w_j \in W_j} a_i b_j w_i(x) [(w_j(x))_r] \right) + \ldots
\end{aligned} \tag{4.15}$$

(4.16)

El último término que aparece en la última linea es el sumando $l = 1$ de la suma en la línea anterior.

Como antes, tenemos el siguiente resultado.

Proposición 4.5. *$\mathcal{N}_{NA}(R,x)$ con la operación definida por la sustitución forma un grupo.*

Demostración. La operación es asociativa y tiene como 1 a x. Para hallar al inverso usamos el mismo argumento que en la Proposición 4.1 (p. 39). □

Observación 4.6. *Al igual que antes, si $\alpha = x + \sum_{w_n \in W_n} a_n w_n(x) + \ldots$, entonces*

$$\alpha^{-1} = x - \sum_{w_n \in W_n} a_n w_n(x) + \ldots$$

Como vamos a calcular el anillo de Lie asociado a D_{NA}, necesitamos conocer el conmutador del grupo $\mathcal{N}_{NA}(R,x)$. Éste tiene una estructura similar al caso no conmutativo.

Lema 4.2. *Sean $\alpha = x + \sum_{i\geq n} \sum_{w_i \in W_i} a_i w_i(x)$ y $\beta = x + \sum_{j\geq m} \sum_{w_j \in W_j} b_j w_j(x)$. Entonces,*

$$\mathbf{c}(\alpha,\beta) = x + \sum_{w_n \in W_n} \sum_{w_m \in W_m} \left(\sum_{r=1}^{n} a_i b_j w_i(x) [(w_j(x))_r] - \sum_{s=1}^{m} b_j a_i w_j(x) [(w_i(x))_s] \right) \tag{4.17}$$

Demostración. La demostración es seguir los mismos pasos que en la demostración del Lema 4.1 (p. 39), sólo usando la ecuación 4.15 (p. 44) junto a la observación anterior (4.6). □

Definimos para cada $k > 0$, $L_k = \{\alpha \in \mathcal{N}_{NA}(R,x) \mid \alpha = x + \sum_{w_{k+1}\in W_{k+1}} a_{k+1}w_{k+1}(x)\}$, y el análogo a la «profundidad» en el grupo de Nottingham:

$$D_{NA}(\alpha) = k \text{ si y sólo si } \alpha \in L_k - L_{k+1}. \tag{4.18}$$

Es claro que D_{NA} está bien definido, pues sólo existe un k para el que se cumple 4.18.

Proposición 4.6. *D_{NA} es una filtración en $\mathcal{N}_{NA}(R,x)$.*

Demostración. La propiedades de la Definición 1.9 (p. 11) se siguen por definición 1) y 2), 3) de la ecuación 4.15 (p. 44) y 4) del Lema 4.2 (p. 44). □

Para terminar esta sección, vea que $L_k = \mathcal{N}_{NA}(R,x)_k$ y $\bigcap L_k = \{x\}$. Así, por ser $\{\mathcal{N}_{NA}(R,x)_k\}_{k\in\mathbb{N}}$ una serie central, tenemos lo siguiente.

Proposición 4.7. *$\mathcal{N}_{NA}(R,x)$ es residualmente nilpotente.*

4.2.1 ANILLO DE LIE ASOCIADO A D_{NA}

Para cada $k > 0$,

$$\mathtt{gr}_{D_{NA},k}(\mathcal{N}_{NA}(R,x)) = L_k/L_{k+1} = \left\{ x + \sum_{w_{k+1}\in W_{k+1}} a_{k+1}w_{k+1}(x) \right\}, \tag{4.19}$$

es un $R-$módulo generado por W_{k+1} (o por T_k). Denotemoslo por $R\langle W_{k+1}\rangle$. Entonces, el anillo de Lie es

$$\mathtt{gr}_{D_{NA}}(\mathcal{N}_{NA}(R,x)) = \bigoplus_{k>0} L_k/L_{k+1} \cong \bigoplus_{k>0} R\langle W_{k+1}\rangle, \tag{4.20}$$

y el corchete de Lie está dado por

$$[AB] = \sum_{w_n\in W_n}\sum_{w_m\in W_m}\left(\sum_{r=1}^{n} a_i b_j w_i(x)[(w_j(x))_r] - \sum_{s=1}^{m} b_j a_i w_j(x)[(w_i(x))_s]\right), \tag{4.21}$$

donde $A = \sum_{w_n\in W_n} a_n w_n(x) \in R\langle W_{n-1}\rangle$ y $B = \sum_{w_m\in W_m} b_m w_m(x) \in R\langle W_{m-1}\rangle$.

4.3 POTENCIAS REALES

En este caso consideraremos potencias de números reales. Sea

$$S_\infty := \{\{\alpha_j\} \mid \alpha_j \in \mathbb{R} \text{ y } \alpha_1 = 1 < \alpha_2 < \alpha_3 < \ldots \to \infty\}. \tag{4.22}$$

Para cada elemento $\{\alpha_j\} \in S_\infty$, definimos

$$\sum_{j\geq 1} a_{\alpha_j} t^{\alpha_j} = t + \sum_{j>1} a_{\alpha_j} t^{\alpha_j}, \tag{4.23}$$

donde $a_{\alpha_j} \in \mathbb{R}$. Por simplicidad escribiremos $a_j = a_{\alpha_j}$.

Definimos el siguiente conjunto

$$\mathcal{N}_{\mathbb{R}}(t) = \left\{ t + \sum_{j>1} a_j t^{\alpha_j} \mid \{\alpha_j\} \in S_\infty \right\} \tag{4.24}$$

Al igual que antes, damos un producto en este conjunto. Sean $\alpha, \beta \in \mathcal{N}_{\mathbb{R}}(t)$, dados por $\alpha = t + \sum_{i>1} a_i t^{\alpha_i}$ y $\beta = t + \sum_{j>1} b_j t^{\beta_j}$, entonces

$$\alpha \cdot \beta = \alpha\beta = \beta + \sum_{i>1} a_i (\beta)^{\alpha_i}.$$

Para desarrollar $(\beta)^{\alpha_j}$ es necesario la siguiente definición.

Definición 4.2 (Binomio de Newton Generalizado)**.** *Para $\alpha \in \mathbb{R}$, definimos*

$$\binom{\alpha}{k} := \begin{cases} \dfrac{\alpha(\alpha-1)\ldots(\alpha-k+1)}{k!}, & \text{para } k > 0. \\ 1, & k = 0. \end{cases}$$

Y con esto tomamos

$$(x+y)^\alpha := \sum_{k\geq 0} \binom{\alpha}{k} x^{\alpha-k} y^k. \tag{4.25}$$

Usando esto

$$\begin{aligned}
\alpha\beta &= \beta + \sum_{i\geq 1} a_i(\beta)^{\alpha_i} \\
&= \beta + \sum_{i>1} a_i \left(t + \sum_{j>1} b_j t^{\beta_j} \right)^{\alpha_i}, \\
&= \beta + \sum_{i>1} a_i \left[\sum_{k\geq 0} \binom{\alpha_i}{k} t^{\alpha_i - k} \left(\sum_{j>1} b_j t^{\beta_j} \right)^k \right], \\
&= \beta + \sum_{i>1} a_i \sum_{k\geq 0} \binom{\alpha_i}{k} t^{\alpha_i - k} \left(\sum_{j_1,\ldots,j_k} b_{j_1} \ldots b_{j_k} t^{\sum_{l=1}^k \beta_{j_l}} \right), \\
&= \beta + \sum_{i>1} \sum_{k\geq 0} \sum_{j_1,\ldots,j_k} \binom{\alpha_i}{k} a_i b_{j_1} \ldots b_{j_k} t^{\alpha_i - k + \sum_{l=1}^k \beta_{j_l}}, \text{ entonces} \\
\alpha\beta &= \beta + \alpha - t + \sum_{i>1} \sum_{k>0} \sum_{j_1,\ldots,j_k} \binom{\alpha_i}{k} a_i b_{j_1} \ldots b_{j_k} t^{\alpha_i - k + \sum_{l=1}^k \beta_{j_l}}. \qquad (4.26)
\end{aligned}$$

Notemos que $\alpha_i - k + \sum_{l=1}^k \beta_{j_l} \to +\infty$ si $i \to +\infty$, pues $a_i \to +\infty$ y también cuando $k \to +\infty$ ya que $\alpha_i - k + \sum_{l=1}^k \beta_{j_l} \geq a_i - k + k \min\{b_{j_l}\} = a_i + k(\min\{b_{j_l}\} - 1)$. Así, siempre podemos arreglar esta serie para que sea un elemento de $\mathcal{N}_{\mathbb{R}}(t)$. Entonces, tenemos un producto asociativo con identidad $1 = t$. Para hallar inversos, supongamos que $X = t + \sum x_i t^{\theta_i} \in \mathcal{N}_{\mathbb{R}}(t)$ es tal que $X\alpha = t$. Entonces de 4.26 tenemos

$$\begin{aligned}
t = X\alpha &= \alpha + X - t + \sum_{i>1} \sum_{k>0} \sum_{j_1,\ldots,j_k} \binom{\theta_i}{k} x_i a_{j_1} \ldots a_{j_k} t^{\theta_i - k + \sum_{l=1}^k \alpha_{j_l}}. \\
0 &= \sum_{j>1} a_j t^{\alpha_j} + \sum_{i>1} x_i t^{\theta_i} + \sum_{i>1} \sum_{k>0} \sum_{j_1,\ldots,j_k} \binom{\theta_i}{k} x_i a_{j_1} \ldots a_{j_k} t^{\theta_i - k + \sum_{l=1}^k \alpha_{j_l}}. \qquad (4.27)
\end{aligned}$$

Aquí, los grados mínimos son los de α_2 y θ_2, de cada parte. Igualandolos obtenemos $x_2 = -a_2$. Despúes, sustituyendo "hacia arriba", obtenemos el sumando $i = 2$ en 4.27 es

$$\sum_{k>0} \sum_{j_1,\ldots,j_k} \binom{\alpha_2}{k} (-a_2) a_{j_1} \ldots a_{j_k} t^{\alpha_2 - k + \sum_{l=1}^k \alpha_{j_l}} = -\alpha_2 a_2^2 t^{2\alpha_2 - 1} + \ldots.$$

Lo que se hace, es comparar las potencias de grado menor, estas son $2\alpha_2 - 1$ y α_3. La menor igualamos con θ_3. Con esto tendremos ahora el sumando $i = 3$ del último término de 4.27. Continuamos de la misma manera, tomando la menor potencia de ese sumando y comparando lo con la menor de los sumandos conocidos, el cual siempre se puede elegir por cómo son las sucesiones. Este proceso inductivo nos lleva a la construcción del inverso izquierdo para α. Por un argumento análogo al de la ecuación 2.5 (p. 20) obtenemos la existencia de inversos para

este producto. Nótese que, como antes, el inverso siempre tiene la forma $\alpha^{-1} = t - a_2 t^{\alpha_2} + \dots$. Entonces, tenemos el resultado esperado.

Proposición 4.8. *$\mathcal{N}_{\mathbb{R}}(t)$ junto con la operación de sustitución forma un grupo.*

Al igual que antes, definimos en $\mathcal{N}_{\mathbb{R}}(t)$ la función «profundidad», $D_{\mathbb{R}}$, como

$$D_{\mathbb{R}}(t + at^{\alpha} + \dots) = \alpha - 1,$$

con α mínimo tal que $a \neq 0$. Es claro que siempre existe tal α y la única manera en que no, es que $t + at^{\alpha} + \dots = t$. En tal caso $D_{\mathbb{R}}(t) = +\infty$.

Proposición 4.9. *$D_{\mathbb{R}}$ es una filtración en $\mathcal{N}_{\mathbb{R}}(t)$ con imagen $\mathbb{R}^+$.*

Para probar esta proposición necesitamos conocer la forma del conmutador.

Lema 4.3. *Sean $A = t + at^{\alpha} + \dots$ y $B = t + bt^{\beta} + \dots$. Entonces,*

$$\mathbf{c}(A, B) = t + ab(\alpha - \beta)t^{\alpha+\beta-1} + \dots \tag{4.28}$$

Demostración. La demostración es análoga a la del Lema 2.1 (p. 21). Por 4.26 (p. 47) tenemos

$$\begin{aligned} AB &= B + A - t + \sum_{i>1} \sum_{k>0} \sum_{j_1,\dots,j_k} \binom{\alpha_i}{k} a_i b_{j_1} \dots b_{j_k} t^{\alpha_i - k + \sum_{l=1}^{k} \beta_{j_l}}, \\ &= B + A - t + \alpha a b t^{\alpha - 1 + \beta} + E, \end{aligned} \tag{4.29}$$

donde E es la serie que queda al quitar el término de menor grado de la última serie de la expresión de arriba. Como $A^{-1} = t - at^{\alpha} + \dots$ tenemos que

$$\begin{aligned} ABA^{-1} &= BA^{-1} + AA^{-1} - A^{-1} + \alpha a b (A^{-1})^{\alpha - 1 + \beta} + E(A^{-1}), \\ &= \left(A^{-1} + B - t + \beta(-a) b t^{\beta - 1 + \alpha} + E' \right) + t - A^{-1} + \alpha a b t^{\alpha - 1 + \beta} + E'' + E(A^{-1}), \\ &= B + ab(\alpha - \beta) t^{\alpha + \beta - 1} + E + E' + E'', \end{aligned} \tag{4.30}$$

con E, E' y E'' series que aparecen al desarrollar. Ponga $Q = E + E' + E''$. Entonces, al multiplicar por B^{-1} a 4.30 obtenemos

$$\mathbf{c}(A, B) = BB^{-1} + ab(\alpha - \beta)(B^{-1})^{\alpha+\beta-1} + Q(B^{-1}) = t + ab(\alpha - \beta)t^{\alpha+\beta-1} + \dots$$

□

Ahora la demostración de la Proposición 4.9.

Demostración. La propiedad 1 y 2 de la Definición 1.9 (p. 11) son inmediatas. 3 se sigue de cómo definimos los inversos y la ecuación 4.26 (p. 47), y 4 del Lema anterior. □

Observación 4.7. *En esta generalización obtenemos $\mathcal{N}(\mathbb{R}, t) \leq \mathcal{N}_{\mathbb{R}}(t)$, lo cual no se garantiza en los otros dos casos, por la naturaleza de la variable.*

4.3.1 ANILLO DE LIE ASOCIADO A $D_{\mathbb{R}}$

Es claro que, dado $\alpha \in \mathbb{R}^{\geq 0}$, entonces

$$\mathtt{gr}_{D_{\mathbb{R}},\alpha}(\mathcal{N}_{\mathbb{R}}(t)) = L_\alpha / L_\alpha^+ \cong \mathbb{R}\langle t^{\alpha+1}\rangle. \tag{4.31}$$

Con lo que obtenemos el anillo de Lie de $D_{\mathbb{R}}$

$$\mathtt{gr}_{D_{\mathbb{R}}}(\mathcal{N}_{\mathbb{R}}(t)) = \bigoplus_{\alpha\in\mathbb{R}^{\geq 0}} \mathbb{R}\langle t^{\alpha+1}\rangle, \tag{4.32}$$

y corchete $[t^{\alpha+1}t^{\beta+1}] = (\alpha - \beta)t^{\alpha+\beta+1}$.

Capítulo 5
Conclusiones

El trabajo deja muchas preguntas para futuras investigaciones sobre los temas que aparecen aquí.

- En el capítulo 1, tenemos preguntas sobre el tipo de relaciones que hay entre dos anillos de Lie asociados a filtraciones distintas.
- En el capítulo 2, las investigaciones recientes sobre el grupo de Nottingham y su relaciones con teoría de números.
- En el capítulo 3, generalizaciones sobre los resultados aquí dados.
- En el capítulo 4, seguir el estudio de las diferentes generalizaciones que se trabajaron.

BIBLIOGRAFÍA

[1] Camina, R., *Subgroups of the Nottingham group*, **J. Algebra 196**, (1997), 101-113.

[2] Camina,R., *The Nottingham Group*, **New Horizons in pro-p Groups**, eds: M.P.F. du Sautoy, D. Segal, & A. Shalev, Birkhauser, (2000).

[3] Dixon, J. D., du Sautoy M. P. F., Mann A., Segal D., *"Analytic pro-p Groups"*, **London Math. Soc. Lectures Series Vol. 157, Cambridge University Press**, 2nd edition 1999

[4] du Sautoy M., Fesenko I., *Where the Wild Things Are: Ramification Groups and the Nottingham Group*, **New Horizons in pro-p Groups**, eds: M.P.F. du Sautoy, D. Segal, & A. Shalev, Birkhauser, (2000).

[5] Fesenko, Ivan B.; Vostokov, Sergei V., *Local fields and their extensions*, **Translations of Mathematical Monographs**, 121 (Second ed.), Providence, RI: American Mathematical Society (2002).

[6] Jennigs, S. A., *Substitution groups of formal power series*, **Canad. J. Math. & (1954), 325-340**

[7] Johnson, D. L., *The group of formal powers series under substitution*, **J. Austral. Math. Soc. 45 (1988), 296-302.**

[8] Lubotzky A., Wilson J. S. ,*"An embedding theorem for profinite groups"*, **Arch. Math. 42 (1984), 296-302**

[9] Serre, J-P., *"Lie algebras and Lie groups"* 1964 Lecture given at Harvard University, **Lecture Notes in Mathematics, Springer-Verlag**, 2nd edition 1992.

[10] Serre, J-P., *"Local Fields"*, **Graduate Texts in Mathematics; 67, Springer-Verlag**, 1980.

[11] Weil A., *"Basic Number Theory"*, **Springer-Verlag, Berlin**, 1967.