Sous-groupes d'indice n et intégrales p-adiques

Daniel Kitachewsky
Emmanuel Lepage
Proposé par François Loeser

25 Juin 2004

Introduction

On s'intéresse ici au décompte des sous-groupes d'indice fini d'un groupe. Afin que ce nombre soit fini pour un indice n fixé, on suppose que le groupe G est de type fini. Pour simplifier (le cas général étant complexe) on le suppose de plus nilpotent.
On est donc amené à considérer une fonction de type arithmétique (i.e. de $\mathbb{N}$ dans $\mathbb{N}$) et l'on veut savoir si son comportement est régulier. Le résultat principal est que la série de Dirichlet associée se décompose suivant les nombres premiers, et que pour chaque nombre premier, la somme de la série correspondante est une fonction rationnelle. Ceci permet de déterminer entièrement la suite que l'on étudiait à partir d'un nombre fini de termes.

Table des matières

Notations

$|S|$ est le cardinal d'un ensemble S.
Pour un groupe G, x,$y \in G$ et S,$T \subset G$,
$\langle S \rangle$ est le sous-groupe engendré par S,
$[x,y] = x^{-1}y^{-1}xy$
$[S,T] = \langle [s,t], s \in S, t \in T \rangle$
$G^n = \langle g^n, g \in G \rangle$ si $n \in \mathbb{Z}$
$Z(G) =$ centre de G
$H \leqq G$: H est un sous-groupe de G
$H \lhd G$: H est un sous-groupe distingué de G
$H \leqq_f G$,$H \lhd_f G$: H est un sous-groupe (resp. un sous-groupe distingué) d'indice fini de G
$\times G_i$: produit cartésien des G_i
Pour un anneau A :
A^* est le groupe des unités de A.
$T_n(A)$ est l'ensemble des matrices triangulaires inférieures à coefficients dans A.

1 Rappels d'algèbre

1.1 Groupes Nilpotents

Définition 1.1 *Un groupe G est dit* nilpotent *s'il existe des sous-groupes distingués $H_0, \ldots, H_n$ tels que*

$$\{1\} = H_0 \leqq H_1 \leqq \cdots \leqq H_n = G$$

et que, pour tout i entre 1 et n, $H_i/H_{i-1} \subset Z(G/H_{i-1})$, ou de façon équivalente $[G,H_i] \subset H_{i-1}$. Les H_i forment alors une suite centrale.

Remarque : Les sous-groupes d'un groupe nilpotent et les quotients d'un groupe nilpotent sont nilpotents.

Définition 1.2 *Pour un groupe G, on définit la suite centrale ascendante par :*

$$Z_0(G) = \{1\}$$
$$Z_i(G) = \pi_i^{-1}(Z(G/Z_{i-1}(G))), \quad i \in \mathbb{N}^*$$

où π_i est la projection canonique de G sur $G/Z_{i-1}(G)$; la suite centrale descendante par :

$$\gamma_1(G) = G$$
$$\gamma_{i+1}(G) = [G,\gamma_i(G)], \quad i \in \mathbb{N}^*$$

Propriétés 1.3
Si la suite centrale ascendante ou descendante est finie, alors c'est une suite centrale.
Si (H_i) est une suite centrale de longueur n, alors $H_i \leqq Z_i$ et $\gamma_{i+1}(G) \leqq H_{n-i}$, pour $0 \leqslant i \leqslant n$.
En particulier, $Z_n(G) = G$ et $\gamma_{n+1}(G) = \{1\}$.
Si G est nilpotent, l'infimum des longueurs des suites centrales est égal à $Inf\{n, Z_n(G) = G\} = Inf\{n, \gamma_{n+1}(G) = \{1\}\}$. Ce nombre est appelé classe de nilpotence de G *et est noté c.*

Dans la suite, on ne considérera que des groupes nilpotents de type fini et sans torsion, que l'on appellera désormais *$\mathcal{T}$-groupes.*

Propriété 1.4
Soit G un $\mathcal{T}$-groupe. Tous ses sous-groupes sont de type fini. Ce sont donc des $\mathcal{T}$-groupes.

Dém. : On ne donne ici qu'une esquisse de démonstration. On note $G_i = \gamma_i(G)$.
Pour $i > 1$ on a un morphisme surjectif

$$\psi_i : (G_{i-1}/G_i) \otimes (G_1/G_2) \longrightarrow G_i/G_{i+1},$$

induit par l'application

$$(G_i g, G_2 h) \longmapsto G_{i+1}\,[g,h]\,.$$

On en déduit par récurrence sur i que G_i/G_{i+1} est de type fini. Comme ce groupe est abélien, tous ses sous-groupes sont de type fini.
Soit H un sous-groupe de G. Les $(HG_{i+1} \cap G_i)/G_{i+1}$ sont de type fini. Soit J_i une famille finie de générateurs. Pour chaque i et chaque $x \in J_i$ on choisit un antécédent par la projection canonique qui soit dans H (quitte à translater par G_{i+1}, ce qui ne change pas le quotient). On obtient ainsi une famille finie de générateurs de H. □

Propriété 1.5
Soit G un $\mathcal{T}$-groupe. $G/Z(G)$ est sans torsion. C'est donc un $\mathcal{T}$-groupe.

Dém. : On commence par montrer que si, pour $x, y \in G$, il existe $n \in \mathbb{Z}$ tel que $x^n = y^n$, alors $x = y$. On procède par récurrence sur c (classe de nilpotence).
Si $c = 1$, G est abélien et sans torsion d'où le résultat.
On suppose le résultat montré pour les classes de nilpotence $< c$. On considère le sous-groupe H engendré par $\gamma_2(G)$ et x. C'est un sous-groupe distingué de G car il contient $\gamma_2(G)$, puisque $G/\gamma_2(G)$ est abélien. On a

$$Z_{c-1}(H) \supset Z_{c-1}(G) \cap H$$

(cela s'établit par récurrence). Or

$$Z_{c-1}(G) \cap H \supset \gamma_2(G) \cap H = \gamma_2(G)$$

H est engendré par $Z_{c-1}(H)$ et x. Dans $H/Z_{c-2}(H)$, x est dans le centre car il commute avec la projection de $Z_{c-1}(H)$ et avec lui-même donc $Z_{c-1}(H) = H$. On peut donc appliquer l'hypothèse de récurrence à H qui est de classe de nilpotence strictement inférieure à celle de G. On a $yxy^{-1} \in H$ puisque H est distingué. De plus

$$\begin{aligned}(yxy^{-1})^n &= yx^ny^{-1} \\ &= y^n\end{aligned}$$

donc $yxy^{-1} = x$: x et y commutent. Comme $x^n = y^n$, $(xy^{-1})^n = 1$ et $x = y$ car G est sans torsion.
Si $x^n \in Z(G)$, pour tout $z \in G$, $(zxz^{-1})^n = zx^nz^{-1} = x^n$ donc $zxz^{-1} = x$ et $x \in Z(G)$, ce qui achève la démonstration. □

Définition 1.6 *Soit G un $\mathcal{T}$-groupe. On appelle* longueur de Hirsch de G, *et on note $h(G)$, le nombre maximal de facteurs infinis monogènes G_i/G_{i-1} dans une tour $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$.*

Propriétés 1.7
Si l'on a une tour composée uniquement de facteurs monogènes, le nombre de facteurs infinis est égal à $h(G)$.
Si $H \leqq G$, $h(H) \leqslant h(G)$.
Si $N \lhd G$ tel que G/N soit sans torsion, $h(G) = h(N) + h(G/N)$.

1.2 Clôtures pro-p et profinie

Définition 1.8 *Un* ensemble dirigé *est un ensemble E partiellement ordonné tel que $\forall\lambda,\mu \in E, \exists\nu \in E$, $\lambda \leqslant \nu$ et $\mu \leqslant \nu$. Un* système inverse *est une famille de groupes $(G_i)_{i\in I}$, telle que I soit dirigé, et une famille de morphismes $(\varphi_{ij} : G_i \longrightarrow G_j)_{j\leqslant i}$ telles que $\forall i$, $\varphi_{ii} = id$ et si $i \leqslant j \leqslant k$, $\varphi_{kj} \circ \varphi_{ji} = \varphi_{ki}$.*
Si (G,φ,I) est un système inverse, on définit la limite inverse de (G,φ,I) par

$$\varprojlim G_i = \left\{ (a_i) \in \prod_{i\in I} G_i,\ \varphi_{ij}(a_i) = a_j \text{ dès que } j \leqslant i \right\}$$

Cette limite est un sous-groupe de $\underset{i\in I}{\times} G_i$

Définition 1.9 *Soit G un $\mathcal{T}$-groupe. La* clôture profinie $\hat{G}$ *de G est la limite inverse de $(G/N,\pi,A)$ où A est l'ensemble des sous-groupes distingués d'indice fini de G ordonné par l'inclusion et π les projections canoniques. La* clôture pro-p $\hat{G}_p$ *est définie de la même manière, mais en ne prenant que les sous-groupes distingués d'indice une puissance de p.*

Propriétés 1.10
G s'injecte dans $\hat{G}$ et les $\hat{G}_p$.
$\hat{G}$ et $\hat{G}_p$ sont compacts pour la topologie induite par la topologie produit (où les G/N sont munis de la topologie discrète).
G est dense dans $\hat{G}$ et $\hat{G}_p$.
G/G^n est isomorphe à $\hat{G}/\hat{G}^n$.

1.3 Nombres p-adiques

Définition 1.11 *L'anneau $\mathbb{Z}_p$ des entiers p-adiques est défini comme la clôture pro-p de $\mathbb{Z}$.*

Propriétés 1.12
$\mathbb{Z}_p$ s'identifie à l'ensemble des séries formelles de la forme

$$\sum_{k=0}^{\infty} a_k p^k, \quad a_k \in \{0,1,\ldots,p-1\}$$

Un élément de $\mathbb{Z}_p$ est inversible si et seulement si $a_o \neq 0$.
Les sous-groupes d'indice fini de $\mathbb{Z}_p$ sont les $p^n\mathbb{Z}_p$. Comme $\mathbb{Z}_p$ est compact, on le munit d'une mesure de probabilité ν (dite mesure de Haar) invariante par translation. On a donc $\nu(p^n\mathbb{Z}_p) = p^{-n}$. On munit de même $\mathbb{Z}_p^n$ d'une mesure de Haar.

2 Propriétés générales des séries de Dirichlet

Tout comme l'on peut déterminer une suite en étudiant la série génératrice associée, nous allons analyser le comportement du nombre a_n de sous-groupes d'un groupe à l'aide de la série de Dirichlet associée. Ainsi, si X est une famille de sous-groupes de G, on lui associe la série

$$\zeta_X(s) = \sum_{H \in X} |G : H|^{-s} = \sum_{n=1}^{\infty} a_n(X) n^{-s} \tag{1}$$

où $a_n(X) = |\{H \in X, |G : H| = n\}|$ (avec la convention $\infty^{-s} = 0$). ζ_X définit alors une fonction analytique sur le demi-plan $\{z \in \mathbb{C}, \mathrm{Re}(s) > \alpha_X\}$, où α_X est l'abscisse de convergence de la série (1). Les abscisses de convergence seront étudiées plus en détail dans la section 2.2.
Voici les familles X de sous-groupes qui seront considérées :

$$\mathcal{S}(G) = \{\text{tous les sous-groupes d'indice fini de } G\},$$
$$\mathcal{N}(G) = \{\text{tous les sous-groupes distingués d'indice fini de } G\}.$$

On notera respectivement

$$\zeta_G = \zeta_{\mathcal{S}(G)}, \quad \alpha_G = \alpha_{\mathcal{S}(G)},$$

$$\zeta_G^{\triangleleft} = \zeta_{\mathcal{N}(G)}, \quad \alpha_G^{\triangleleft} = \alpha_{\mathcal{N}(G)}.$$

L'intérêt majeur d'utiliser de séries de Dirichlet est le fait que, à l'instar de la fonction zêta de Riemann, elle se décomposent en produit d'Euler. À cette fin, on notera

$$X_p = \left\{ H \in X, |G : H| = p^k \text{ pour un } k \in \mathbb{N} \right\},$$

$$\zeta_{G,p} = \zeta_{\mathcal{S}(G)_p}, \quad \zeta_{G,p}^{\triangleleft} = \zeta_{\mathcal{N}(G)_p}.$$

Nous y reviendrons dans la section 2.3.

2.1 Cas abélien

Le cas des $\mathcal{T}$-groupes de classe de nilpotence égale à 1 est facile :

Propriété 2.1
Soit $G = \mathbb{Z}^d$. Alors on a

$$\zeta_G(s) = \zeta_G^{\triangleleft}(s) = \prod_{j=0}^{d-1} \zeta(s-j), \tag{2}$$

$$\zeta_{G,p}(s) = \zeta_{G,p}^{\triangleleft}(s) = \prod_{j=0}^{d-1} (1 - p^j p^{-s})^{-1}. \tag{3}$$

Dém. : Soit $G = \mathbb{Z}^d$ et soit $Z \leqq G$ avec $Z \cong \mathbb{Z}$, $G/Z \cong \mathbb{Z}^{d-1}$. Pour chaque sous-groupe A/Z d'indice fini de G/Z et chaque sous-groupe B d'indice fini de Z, il y a exactement $|\mathrm{Hom}(A/Z, Z/B)| = |Z : B|^{d-1}$ sous-groupes H de G tels que $Z + H = A$ et $Z \cap H = B$. Chacun de ces H a pour indice $|G : A| \cdot |Z : B|$ dans G. En faisant varier A et B, on obtient chaque sous-groupe H de G une et une seule fois. Ainsi on a

$$\begin{aligned} \zeta_G(s) &= \sum_{Z < A \leqq_f G} |G : A|^{-s} \sum_{B \leqq_f Z} |Z : B|^{d-1-s} \\ &= \zeta_{G/A}(s) \zeta_Z(s - (d-1)). \end{aligned}$$

Puisque $Z \cong \mathbb{Z}$, $\zeta_Z(s) = \sum_{n=1}^{\infty} n^{-s} = \zeta(s)$. On établit ainsi (2) par récurrence sur d. (3) s'établit de la même façon en ne considérant que les sous-groupes d'indice une puissance de p. □

2.2 Abscisses de convergence

Propriété 2.2
Pour un $\mathcal{T}$-groupe, $\alpha_G \leqslant h(G)$.

Dém. : On raisonne par récurrence sur $h(G)$.
Si $h(G) = 1$, $G \cong \mathbb{Z}$ et $\alpha_G = 1$ (car ζ_G n'est autre que la fonction zêta de Riemann).
Supposons le résultat montré pour les longueurs de Hirsch plus petites. Soit $Z \leqq Z(G)$ avec $Z \cong \mathbb{Z}$ et G/Z sans torsion. Si $A/Z \leqq_f G/Z$ et $B \leqq_f Z$ alors le nombre de sous-groupes H de G avec $HZ = A$ et $H \cap Z = B$ est au plus

$$|\mathrm{Hom}(A/Z, Z/B)| \leqslant |Z : B|^{h-1}$$

où $h = h(G)$. Donc pour s réel $> h$,

$$\begin{aligned}\zeta_G(s) = \sum |G : H|^{-s} &\leqslant \sum_{A/Z \leqq G/Z} |G : A|^{-s} \sum_{B \leqq Z} |Z : B|^{h-1-s} \\ &= \zeta_{G/Z}(s)\zeta(s - (h-1)).\end{aligned}$$

Le deuxième facteur est fini puisque $s - (h-1) > 1$, et le premier l'est par hypothèse de récurrence. Le résultat s'en suit. □

2.3 Décomposition en produit d'Euler

Propriété 2.3
Soit G un $\mathcal{T}$-groupe. Alors

$$\begin{aligned}\zeta_G = \zeta_{\hat{G}}, \quad \zeta_G^{\triangleleft} = \zeta_{\hat{G}}^{\triangleleft}. \\ \zeta_{G,p} = \zeta_{\hat{G},p}, \quad \zeta_{G,p}^{\triangleleft} = \zeta_{\hat{G},p}^{\triangleleft}.\end{aligned} \tag{4}$$

Dém. : Puisque G est nilpotent, chaque sous-groupe d'indice n de G contient G^n. Ainsi l'isomorphisme naturel $G/G^n \longrightarrow \hat{G}/\hat{G}^n$ induit une bijection entre l'ensemble des sous-groupes d'indice n de G et l'ensemble des sous-groupes d'indice n de $\hat{G}$, de plus les sous-groupes distingués de l'un correspondent aux sous-groupes distingués de l'autre. Cela montre $\zeta_G = \zeta_{\hat{G}}$ et $\zeta_G^{\triangleleft} = \zeta_{\hat{G}}^{\triangleleft}$. □
Pour n entier positif, on note a_n (resp. b_n) le nombre de sous-groupes (resp. sous-groupes distingués) de G d'indice n.

Propriété 2.4
Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ un entier positif décomposé en facteurs premiers. On a

$$a_n = \prod_{i=1}^{r} a_{p_i}^{\alpha_i}, \qquad b_n = \prod_{i=1}^{r} b_{p_i}^{\alpha_i}$$

Dém. : Soit m tel que tous les sous-groupes d'indice k, pour $k|n$, contiennent G^m. Alors $a_k = a_k(G/G^m)$ pour $k|n$ (de même pour b). Or G/G^m est un groupe nilpotent fini, donc il est isomorphe au produit de ses Sylow S_p. Si $H \leqq G/G^m$ d'indice n, alors

$$H \times \prod_{p \neq p_i} S_p \leqq G/G^m$$

d'indice $p_i^{\alpha_i}$. Réciproquement, si $H_i \leqq G/G^m$ est d'indice $p_i^{\alpha_i}$, alors $\bigcap_i H_i \leqq G/G^m$ est d'indice n. □

Corollaire 2.5 *Soit G un $\mathcal{T}$-groupe. Alors*

$$\zeta_G(s) = \prod_p \zeta_{G,p}(s), \qquad \zeta_G^{\triangleleft}(s) = \prod_p \zeta_{G,p}^{\triangleleft}(s)$$

3 Bases de Malcev

Définition 3.1 *Soit G un $\mathcal{T}$-groupe de longueur de Hirsch n. On dit que $(x_1,\ldots,x_n)$ est une base de Malcev de G si la suite des groupes*

$$M_0 = \{1\}, M_1 = \langle x_1\rangle, \ldots, M_n = \langle x_1,\ldots,x_n\rangle$$

est une suite centrale telle que tout élément de M_i s'écrive de façon unique comme $x_1^{a_1}\cdots x_i^{a_i}$ avec $a_j \in \mathbb{Z}$.

Théorème 3.2
Soit G un $\mathcal{T}$-groupe de longueur de Hirsch n. G admet une base de Malcev.

Dém. : On procède par récurrence sur c.
Si $c = 1$, $G \cong \mathbb{Z}^n$, et la base canonique de $\mathbb{Z}^n$ en tant que $\mathbb{Z}$-module convient. On suppose le résultat montré pour les classes de nilpotence $< c$. $G/Z(G)$ est un $\mathcal{T}$-groupe. On considère $(y_1,\ldots,y_k)$ une base de Malcev de $G/Z(G)$. On choisit des antécédents $x_1,\ldots,x_k$ de $y_1,\ldots,y_k$ par la projection canonique, on considère $(x_{k+1},\ldots,x_{k+l})$ une base de Malcev du centre. Alors $(x_{k+1},\ldots,x_{k+l},x_1,\ldots,x_k)$ convient. □

Exemple : on prend $G = \left\{ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_{n-1n} \\ & & & 1 \end{pmatrix}, a_{ij} \in \mathbb{Z} \right\}$. Alors une base de Malcev de G est, en notant $I = I_n$ et E_{ij} les matrices élémentaires, $(I + E_{1n}, I + E_{1n-1}, I + E_{2n}, \ldots, I + E_{12}, I + E_{23}, \ldots, I + E_{n-1n})$.

Théorème 3.3
Soit $(x_1,\ldots,x_n)$ une base de Malcev de G. On convient de noter x^a pour $x_1^{a_1}\cdots x_n^{a_n}$.
Il existe des polynômes μ_i, λ_i, à coefficients dans $\mathbb{Q}$, à respectivement $2n$ et $n+1$ variables, tels que pour tous $a,b \in \mathbb{Z}^n$ et pour tout $k \in \mathbb{Z}$, on ait

$$x^a x^b = x^{\mu(a,b)} \qquad (M_n)$$

$$(x^a)^k = x^{\lambda(a,k)} \qquad (E_n)$$

Dém. : On procède par récurrence sur n, le cas $n = 1$ étant trivial, puisque G est alors abélien.
On suppose $M_1,\dots,M_{n-1},E_1,\dots,E_{n-1}$ déjà démontrés. Montrons M_n. On écrit

$$x^a x^b = x_1^{a_1}\cdots x_{n-1}^{a_{n-1}}\left(\prod_{i=1}^{n-1}(x_n^{a_n}x_i x_n^{-a_n})^{b_i}\right)x_n^{a_n+b_n}$$

$$x_n^{a_n}x_i x_n^{-a_n} = x_i(x_i^{-1}x_n x_i)^{a_n}x_n^{-a_n} \tag{5}$$

Par la propriété de centralité, on obtient une expression de la forme

$$x_i^{-1}x_n x_i x_n^{-1} = \left[x_i,x_n^{-1}\right] = x_1^{c_{i,1}}\cdots x_{i-1}^{c_{i,i-1}},\quad c_{i,j}\in\mathbb{Z}$$

$(x_1,\dots,x_{i-1},x_n)$ est une base de Malcev pour le sous-groupe qu'elle engendre. On a donc, en appliquant E_i,

$$\begin{aligned}(x_i^{-1}x_n x_i)^{a_n} &= (x_1^{c_{i,1}}\cdots x_{i-1}^{c_{i,i-1}}x_n)^{a_n}\\ &= x_1^{\varphi_{i,1}(a_n)}\cdots x_{i-1}^{\varphi_{i,i-1}(a_n)}x_n^{a_n}\end{aligned}$$

En utilisant M_i pour réordonner les termes, on a par (5)

$$\begin{aligned}x_n^{a_n}x_i x_n^{-a_n} &= x_i x_1^{\varphi_{i,1}(a_n)}\cdots x_{i-1}^{\varphi_{i,i-1}(a_n)}\\ &= x^{\tilde{\varphi}_i(a_n)}\end{aligned}$$

On réapplique E_i, puis M_{n-1} pour réordonner les termes :

$$(x_n^{a_n}x_i x_n^{-a_n})^{b_i} = x^{\psi_i(a_n,b_i)}$$

$$\begin{aligned}x^a x^b &= x_1^{a_1}\cdots x_{n-1}^{a_{n-1}}\Big(\prod_{i=1}^{n-1}x^{\psi_i(a_n,b_i)}\Big)x_n^{a_n+b_n}\\ &= x_1^{\mu_1(a,b)}\cdots x_{n-1}^{\mu_{n-1}(a,b)}x_n^{a_n+b_n}\\ &= x^{\mu(a,b)}\end{aligned}$$

en posant $\mu_n(a,b) = a_n + b_n$, ce qui achève la démonstration de M_n.
Passons à la démonstration de E_n. Nous aurons besoin d'un lemme.

Lemme 3.4 *Soit $P = x_1\cdots x_m$, considéré comme un mot, $A_1,\dots,A_k$ une partition de $\{1,\dots,m\}$. Soit C_S le plus petit ensemble contenant les $x_i, i\in\bigcup_{j\in S}A_j$, stable par commutateurs. Soit X_S l'ensemble des $v\in C_S$ qui ont au moins une occurence d'un des $x_k, k\in A_j$, et ce pour chaque $j\in S$.*
On ordonne $\mathcal{P}(\{1,\dots,k\})$ par cardinal puis par ordre lexicographique. Alors on a

$$P = \prod_{S\in\mathcal{P}(\{1,\dots,k\})\setminus\{\varnothing\}} Q_S$$

où Q_S est un produit d'éléments de X_S.

Dém. : On fait d'abord passer les éléments de $X_{\{1\}}$ à gauche en utilisant $x_i x_j = x_j x_i\,[x_i,x_j]$ pour $j \in A_1$, en commençant par les j les plus petits. On fait de même pour les autres parties de $\{1,\ldots,k\}$. □

Soit $S \subset \{1,\ldots,k\}$. On obtient un mot P_S en identifiant, pour $j \notin \bigcup_{k\in S} A_k$, x_j à 1. Alors $P_S = \prod_{T\subset S} Q_T$, ce qui permet de calculer Q_T par récurrence en fonction des P_S.

En particulier, si $m = rn$, et si $P = x_1^r \cdots x_n^r$, avec $A_j = \{j,r+j,\ldots,(n-1)r+j\}$ pour $1 \leqslant j \leqslant r$, alors $P_S = x_1^{|S|}\cdots x_n^{|S|}$. En calculant Q_S par récurrence sur les P_S, on voit que Q_S ne dépend que de S (et pas de r). On pose $Q_S = \tau_{|S|}(x_1,\ldots,x_n)$ (avec $\tau_1(x_1,\ldots,x_n) = x_1\cdots x_n$). Alors $P = \prod_S Q_S$ donne $x_1^r\cdots x_n^r = \tau_1^{C_r^1}\cdots\tau_c^{C_r^c}$.

Revenons à la démonstration de E_n. Pour $r > 0$,

$$(x_1^{a_1}\cdots x_n^{a_n})^r = x_1^{ra_1}\cdots x_n^{ra_n}\tau_2^{-C_r^2}(x_1^{a_1},\ldots,x_n^{a_n})\cdots\tau_c^{-C_r^c}(x_1^{a_1},\ldots,x_n^{a_n})$$

Or $\tau_2,\ldots,\tau_c \in \gamma_2(G) \subset \langle x_1,\ldots,x_{n-1}\rangle$.

Par M_n,

$$\tau_i(x_1^{a_1},\ldots,x_n^{a_n}) = x_1^{\mu_{i,1}(a_1,\ldots,a_n)}\cdots x_{n-1}^{\mu_{i,n-1}(a_1,\ldots,a_n)}$$

avec $\mu_{i,j}$ des polynômes. Donc

$$(\tau_i(x_1^{a_1},\ldots,x_n^{a_n}))^{C_r^i} = x_1^{\mu'_{i,1}(a_1,\ldots,a_n,r)}\cdots x_{n-1}^{\mu'_{i,n-1}(a_1,\ldots,a_n,r)}$$

avec $\mu'_{i,j}$ des polynômes, en appliquant E_{n-1}. Enfin, on applique M_{n-1} pour avoir le résultat pour $r > 0$.

Pour $r < 0$, on utilise $(x_1^{a_1}\cdots x_n^{a_n})^r = (x_n^{-a_n}\cdots x_1^{-a_1})^{-r}$, et les polynômes sont les mêmes. □

Propriété 3.5

Il existe des polynômes κ_i à coefficients dans $\mathbb{Q}$, à $2n$ variables, tels que

$$\forall a,b \in \mathbb{Z}^n, \quad \left[x^a,x^b\right] = x^{\kappa(a,b)}$$

Remarques : On étend facilement les polynômes μ aux produits de n termes par récurrence.

On étend la notion de base de Malcev au complété pro-p de G par

$$x^a = x_1^{a_1}\cdots x_n^{a_n}, \quad a_n \in \mathbb{Z}_p$$

avec la multiplication imposée par μ. Le théorème 3.3 et la proposition restent valables dans $\mathbb{Z}_p$.

4 Formalisme p-adique

4.1 Bonnes bases

Dans cette partie, on se fixe p premier et $(x_1,\dots,x_n)$ une base de Malcev de G. On pose, pour $0 \leqslant i \leqslant n$,

$$G_i = \langle x_1,\dots,x_n\rangle$$

de sorte que les G_i forment une suite centrale à facteurs monogènes infinis. On note $\bar{G}$ le complété pro-p de G, et $\bar{S}$ ou S^- le complété d'un sous-ensemble S de G.

Définition 4.1 *Soit $H \leqq_f \bar{G}$. Un n-uplet $(h_1,\dots,h_n)$ d'éléments de H est appelé une* bonne base *si, pour $1 \leqslant i \leqslant n$,*

$$\langle h_1,\dots,h_i\rangle^- = H \cap \bar{G}_i.$$

Lemme 4.2 *i. Soit $h_i \in \bar{G}_i \setminus \bar{G}_{i-1}$ pour $1 \leqslant i \leqslant n$ et soit $H = \langle h_1,\dots,h_n\rangle^-$. Alors H est d'indice fini dans $\bar{G}$; et $(h_1,\dots,h_n)$ est une bonne base si et seulement si*

$$[h_i,h_j] \in \langle h_1,\dots,h_{i-1}\rangle^- \quad \textit{pour} \quad 1 \leqslant i < j \leqslant n. \tag{6}$$

ii. Supposons (6) vrai et soit $h'_1,\dots,h'_n \in H$. Alors $(h'_1,\dots,h'_n)$ est une bonne base de H si et seulement s'il existe $r_i \in \mathbb{Z}_p^*$ et $w_i \in \langle h_1,\dots,h_{i-1}\rangle^-$ tels que

$$h'_i = w_i h_i \quad \textit{pour} \quad 1 \leqslant i \leqslant n. \tag{7}$$

Dém. : On note $H_i = \langle h_1,\dots,h_i\rangle^-$ pour chaque i. On a :

$$\left|\bar{G}_i : \bar{G}_i \cap H\bar{G}_{i-1}\right| \leqslant \left|\bar{G}_i : H_i\bar{G}_{i-1}\right| = \left|\bar{G}_i : \bar{G}_{i-1}\langle h_i\rangle^-\right| < \infty,$$

d'où

$$\left|\bar{G} : H\right| = \prod_{i=1}^{n} \left|\bar{G}_i : \bar{G}_i \cap H\bar{G}_{i-1}\right| < \infty. \tag{8}$$

Or $(h_i,\dots,h_n)$ est une bonne base si et seulement si $H \cap \bar{G}_i = H_i$ pour chaque i. On a donc (6). Inversement, supposons (6) vrai. Soit $k \leqslant n$, et supposons que $H \cap \bar{G}_i = H_i$ pour chaque $i > k$. Alors $H_{k+1} = H_k\langle h_{k+1}\rangle^-$, puisque (6) implique que $H_k \lhd H$, d'où

$$H \cap \bar{G}_k = (H \cap \bar{G}_{k+1}) \cap \bar{G}_k = H_{k+1} \cap \bar{G}_k = H_k(\langle h_{k+1}\rangle^- \cap \bar{G}_k) = H_k$$

puisque $\langle h_{k+1}\rangle^- \cap \bar{G}_k = 1$. Il s'en suit par récurrence sur k que $H_k = H \cap \bar{G}_k$ pour chaque k. Finalement, $(h'_1,\dots,h'_n)$ est une autre bonne base si et seulement si $\langle h'_1,\dots,h'_i\rangle^- = H_i$ pour chaque i. Puisque $H_{i-1} \lhd H_i$ pour chaque i, c'est équivalent à (7). □

Lemme 4.3 *Soit $h_i \in \bar{G}_i \setminus \bar{G}_{i-1}$ pour $1 \leqslant i \leqslant n$, et soit $H = \langle h_1, \ldots, h_n \rangle^-$. Alors $(h_1, \ldots, h_n)$ est une bonne base et $H \lhd G$ si et seulement si*

$$[h_i, x_j] \in \langle h_1, \ldots, h_{i-1} \rangle^- \quad \text{pour tout } i \text{ et } j.$$

À chaque $H \leqq_f \bar{G}$ on associe l'ensemble $\mathcal{M}(H)$ des matrices M, de taille $n \times n$, à coefficients dans $\mathbb{Z}_p$, tels que $(x^{m_1}, \ldots, x^{m_n})$ soit une bonne base pour H, où les m_i sont les lignes de M. De cette manière, $\mathcal{M}(H) \subset T_n(\mathbb{Z}_p)$ (par la propriété de Malcev), et il est facile de voir que, par (8), que si $M \in \mathcal{M}(H)$ alors

$$|\det M|^{-1} = |G : H|,$$

de plus si $H_i = H \cap \bar{G}_i$ on a

$$\bar{G}_{i-1} H_i = \bar{G}_{i-1} \langle x_i^{m_{ii}} \rangle^-$$

d'où

$$|G_i : G_{i-1} H_i| = |m_{ii}|^{-1}$$

pour tout i.

Lemme 4.4 *Soit $M \in T_n(\mathbb{Z}_p)$. Alors $M \in \mathcal{M}(H)$ pour un certain $H \leqq_f \bar{G}$ si et seulement si $\det M \neq 0$ et pour $1 \leqslant i < j \leqslant n$ il existe $Y_{ij}^1, \ldots, Y_{ij}^{i-1} \in \mathbb{Z}_p$ tels que*

$$\kappa(m_i, m_j) = \mu(\lambda(m_1, Y_{ij}^1), \ldots, \lambda(m_{i-1}, Y_{ij}^{i-1})). \tag{9}$$

Lemme 4.5 *Soit $M \in T_n(\mathbb{Z}_p)$. Alors $M \in \mathcal{M}(H)$ pour un certain $H \lhd_f \bar{G}$ si et seulement si $\det M \neq 0$ et pour $1 \leqslant i, j \leqslant n$ il existe $Y_{ij}^1, \ldots, Y_{ij}^{i-1} \in \mathbb{Z}_p$ tels que*

$$\kappa(m_i, e_j) = \mu(\lambda(m_1, Y_{ij}^1), \ldots, \lambda(m_{i-1}, Y_{ij}^{i-1})), \tag{10}$$

où $(e_1, \ldots, e_n)$ est la base canonique de $\mathbb{Z}^n$.

4.2 Formules intégrales des séries de Dirichlet

Lemme 4.6 *Soit $H \leqq_f \bar{G}$. Alors $\mathcal{M}(H)$ est un ouvert de $T_n(\mathbb{Z}_p)$ de mesure*

$$\nu(\mathcal{M}(H)) = (1 - p^{-1})^n p^{-ne_1} p^{-(n-1)e_2} \cdots p^{-1 \cdot e_n}$$

où, pour chaque i, $p^{e_i} = \left| \bar{G}_i : \bar{G}_{i-1}(H \cap \bar{G}_i) \right|$.

Dém. : On démontre d'abord que $\mathcal{M}(H)$ est ouvert. Il existe $f > 0$ tel que $\bar{G}^{p^f} \leqq H$. Il suffit de montrer que

$$M \in \mathcal{M}(H) \implies M + p^f T_n(\mathbb{Z}_p) \subset \mathcal{M}(H). \tag{11}$$

Soit donc $M \in \mathcal{M}(H)$, soit $r \in p^f\mathbb{Z}_p$ et soit $1 \leqslant l < k \leqslant n$, il suffit de montrer que $M + rE_{kl} \in \mathcal{M}(H)$ (où les E_{kl} sont les matrices élémentaires). Posons $h_i = x^{m_i}$ pour chaque i, $h'_i = h_i$ pour $i \neq k$, et $h'_k = x^{m_k + re_l}$. Alors

$$\begin{aligned} h'_k &= x_1^{m_{k,1}} \cdots x_l^{m_{k,l}} x_l^r x_{l+1}^{m_{k,l+1}} \cdots x_k^{m_{k,k}} \\ &= wh_k \end{aligned}$$

où w est conjugué à x_l^r dans $\bar{G}$, d'où

$$w \in \bar{G}^r \cap \bar{G}_l \subset H \cap \bar{G}_l = \langle h_1, \ldots, h_l \rangle^- \subset \langle h_1, \ldots, h_{k-1} \rangle^-$$

puisque $(h_1, \ldots, h_n)$ est une bonne base pour H. Donc, par le lemme 4.2.ii, $(h'_1, \ldots, h'_n)$ est aussi une bonne base pour H. L'assertion (11) s'en suit.
Maintenant, fixons M et $(h_1, \ldots, h_n)$ comme ci-dessus, et définissons, pour chaque i, l'application $\varphi_i : \mathbb{Z}_p^i \longrightarrow \mathbb{Z}_p^i$ par

$$h_1^{Y_1} \cdots h_i^{Y_i} = x^{\varphi_i(Y_1, \ldots, Y_i), 0, \ldots, 0}.$$

Le lemme 4.2.ii montre que $\mathcal{M}(H)$ est l'ensemble des matrices $n \times n$ N vérifiant

$$n_i = (\varphi_i(Y_1, \ldots, Y_i), 0, \ldots, 0)$$

avec $Y_1, \ldots, Y_{i-1} \in \mathbb{Z}_p$ et $Y_i \in \mathbb{Z}_p^*$, pour $1 \leqslant i \leqslant n$. Par conséquent,

$$\nu(\mathcal{M}(H)) = \prod_{i=1}^{n} \nu(\varphi_i(\mathbb{Z}_p^{i-1} \times \mathbb{Z}_p^*)). \tag{12}$$

Fixons i, et pour $1 \leqslant j,k \leqslant i$ posons

$$\Delta_{jk} = \frac{(\partial \varphi_i)_j}{\partial Y_k}.$$

qui à i fixé est le Jacobien de φ_i. Notons que $(\varphi_i)_j$ est un polynôme en $Y_1, \ldots, Y_i$, c'est-à-dire la j-ième composante de $\mu(\lambda(m_1, Y_1), \ldots, \lambda(m_i, Y_i))$; c'est l'exposant de x_j dans l'expression canonique de $h_1^{Y_1} \cdots h_i^{Y_i}$. Puisque $h_k \in \langle x_1, \ldots, x_k \rangle^-$, cet exposant est indépendant de Y_k dès que $k < j$, ainsi

$$k < j \implies \Delta_{jk} = 0.$$

Puisque $h_j \in \bar{G}_{j-1} x_j^{m_{jj}}$, on a

$$h_1^{Y_1} \cdots h_i^{Y_i} \in \bar{G}_{j-1} x_j^{Y_j m_{jj}} h_{j+1}^{Y_j w_1} \cdots h_i^{Y_i},$$

d'où $\Delta_{jj} = m_{jj}$.
Il suit que

$$|\det \Delta| = |m_{11} m_{22} \cdots m_{ii}| = p^{-(e_1 + \cdots + e_i)}.$$

Ainsi

$$\begin{aligned}\nu(\varphi_i(\mathbb{Z}_p^{i-1}\times\mathbb{Z}_p^*)) &= \int_{\mathbb{Z}_p^{i-1}\times\mathbb{Z}_p^*} |\det\,\Delta|\,d\nu \\ &= p^{-(e_1+\cdots+e_i)}\nu(\mathbb{Z}_p^{i-1}\times\mathbb{Z}_p^*) \\ &= (1-p^{-1})p^{-(e_1+\cdots+e_i)}\end{aligned}$$

ce qui, avec (12), donne le résultat. □

Propriété 4.7
Soit $\mathcal{M}_p$ l'ensemble des $M \in T_n(\mathbb{Z}_p)$ vérifiant les conditions (9), et soit $\mathcal{N}_p$ l'ensemble de ces M satisfaisant (10). Alors

$$\zeta_{G,p}(s) = (1-p^{-1})^{-n}\int_{M\in\mathcal{M}_p} |m_{11}|^{s-n}\,|m_{22}|^{s-(n-1)}\cdots|m_{nn}|^{s-1}\,d\nu \quad (13)$$

$$\zeta^{\triangleleft}_{G,p}(s) = (1-p^{-1})^{-n}\int_{M\in\mathcal{N}_p} |m_{11}|^{s-n}\,|m_{22}|^{s-(n-1)}\cdots|m_{nn}|^{s-1}\,d\nu \quad (14)$$

Dém. : Par le lemme 4.4, $\mathcal{M}_p$ est une réunion disjointe

$$\mathcal{M}_p = \{M\in\mathcal{M}_p,\,\det M = 0\} \cup \bigcup_{H\leqq_f\bar{G}} \mathcal{M}(H).$$

L'intégrande de (13) s'annule dès que $\det M = 0$, et par le lemme 4.6 il est égal à

$$p^{e_1 n}p^{e_2(n-1)}\cdots p^{e_n}p^{-(e_1+\cdots+e_n)s} = (1-p^{-1})^n\nu(\mathcal{M}(H))^{-1}\,|G:H|^{-s}$$

sur $\mathcal{M}(H)$, où $p^{e_i} = \left|\bar{G}_i : \bar{G}_{i-1}(H\cap\bar{G}_i)\right|$. Ainsi le membre de droite de (13) est égal à

$$\begin{aligned}&(1-p^{-1})^{-n}\sum_{H\leqq_f\bar{G}}(1-p^{-1})^n\nu(\mathcal{M}(H))^{-1}\,|G:H|^{-s}\int_{\mathcal{M}(H)}d\nu \\ &= \sum_{H\leqq_f\bar{G}}|G:H|^{-s} = \zeta_{\bar{G}}(s) = \zeta_{G,p}(s).\end{aligned}$$

Le deuxième résultat suit pareillement du lemme 4.5. □

4.3 Théorème de Denef

Théorème 4.8
Soit $\varphi(x)$ une formule du premier ordre (dans le langage des anneaux) sur $\mathbb{Z}_p^n$, $f_1,\ldots,f_n$ des fonctions polynômiales $\mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p$. Alors

$$\int_{\left\{x\in\mathbb{Z}_p^n,\,\varphi(x)\right\}} |f_1(x)|^{s_1}\cdots|f_n(x)|^{s_n}\,d\nu$$

est une fonction rationnelle en $p^{-s_1},\ldots,p^{-s_n}$.

On applique ce théorème aux intégrales (13) et (14) pour avoir le théorème :

Théorème 4.9
$\zeta_{G,p}$ et $\zeta^{\triangleleft}_{G,p}$ sont des fonctions rationnelles en p^{-s}.

Ce théorème dit que les séries de Dirichlet sont des fonctions rationnelles ; or ces séries ne sont autres que des séries entières en p^{-s}, donc on peut facilement récupérer les coefficients de ces séries. C'est là l'intérêt d'utiliser des séries de Dirichlet, car elles se décomposent en produit de séries simples.

Conclusion

La formule intégrale que l'on obtient est surtout d'intérêt théorique car difficile à calculer en pratique. Par un raisonnement similaire, on obtient également une formule intégrale pour les sous-algèbres d'une $\mathbb{Z}$-algèbre non nécessairement associative. On peut se servir de ce résultat pour les $\mathcal{T}$-groupes en considérant des algèbres de Lie associées.

Références

[1] Grunewald, F.J., Segal, D., Smith, G.C. : Subgroups of finite index in nilpotent groups, Invent. Math. **93**, 185-223 (1988)

[2] Grunewald, F.J., Segal, D. : Reflections on the classification of torsion-free nilpotent groups. In : Group Theory : *Essays for Philip Hall*, Grünberg, K.W., Roseblade, J.E., (eds.). New York : Academic Press 1984.

[3] Denef, J. : The rationality of the Poincaré series associated to the p-adic points on a variety. Invent. Math. **77**, 1-23 (1984)

[4] Segal, D. : Polycyclic groups. Cambridge : C.U.P. 1983