Étude de groupes nilpotents agissant par transformations algébriques complexes

Marc Abboud

18 Juillet 2018

Mémoire de M2 sous la direction de Serge Cantat.

Résumé

Dans ce mémoire, on s'intéresse à l'action de groupe nilpotents sur des variétés algébriques complexes. Nous allons voir comment la dimension de la variété donne des informations sur la structure du groupe. Pour cela nous allons utiliser une méthode de changement de corps de base. Lorsque le groupe est fini, on passe du corps des complexes à un corps fini pour pouvoir appliquer des lemmes de comptage. Lorsque le groupe est infini de type fini, on passe du corps des complexes à $\mathbf{Z}_p$ pour pouvoir utiliser des outils analytiques.

Remerciements Je remercie Serge Cantat pour m'avoir guidé dans mon travail durant ce semestre, pour ses conseils qui m'ont aidé dans beaucoup de situations.

Table des matières

Première partie

Introduction

Ce mémoire porte sur l'étude de l'action de groupe nilpotents sur des variétés algébriques complexes. Il a deux aspects principaux : Premièrement, l'outil principal développé et utilisé le long de ce mémoire est le passage du corps des complexes à un autre corps ayant des propriétés arithmétiques particulières. Le second point est le contrôle des groupes nilpotents par la dimension de l'espace sur lequel ils agissent. On explicite dans cette introduction les théorèmes prouvés dans ce mémoire lorsque la variété algébrique sur lequel le groupe agit est l'espace affine.

1 Sur les groupes finis

1.1 Structure des groupes finis d'automorphismes de l'espace affine

Ici on suppose donné un groupe G fini qui agit par automorphisme polynomiaux sur l'espace affine $\mathbf{A}^d_{\mathbf{Q}}$. On cherche à montrer comment la dimension d de l'espace affine permet de borner la taille du groupe G. Il est naturel de s'intéresser d'abord au cas d'une action linéaire, on a alors le théorème de Minkowski :

Théorème 1.1 ([Ser09], 5.1)**.** *Soit p un nombre premier et G un p-sous-groupe de $GL_d(\mathbf{Q})$ de cardinal p^α, alors*

$$\alpha \leq M(d,p) = \left\lfloor \frac{d}{p-1} \right\rfloor + \left\lfloor \frac{d}{p(p-1)} \right\rfloor + \left\lfloor \frac{d}{p^2(p-1)} \right\rfloor + \cdots$$

Et le cas d'égalité est atteint.

La preuve de ce théorème utilise le passage de $\mathbf{C}$ vers un corps fini où l'on peut calculer le cardinal du groupe des matrices inversibles.

On montre dans ce mémoire que cette même borne s'applique pour une action par automorphisme polynomiaux.

Théorème 1.2. *Soit p un nombre premier et G un p-sous-groupe de $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{A}^d)$ de cardinal p^α, alors*

$$\alpha \leq M(d,p) = \left\lfloor \frac{d}{p-1} \right\rfloor + \left\lfloor \frac{d}{p(p-1)} \right\rfloor + \left\lfloor \frac{d}{p^2(p-1)} \right\rfloor + \cdots$$

La preuve utilise aussi le passage sur les corps finis. On montre d'abord que G est isomorphe à un sous-groupe de $\mathrm{Aut}(\mathbf{A}^d_F)$ où F est un corps fini de caractéristique différente de p et ce pour deux raisons : la première est que sur F, G a un point fixe. La deuxième est que l'on peut alors linéariser l'action de G autour de ce point fixe pour appliquer le théorème de Minkowski.

Remarque 1.3. Ce théorème et son optimalité donne le fait qu'il n'existe pas de plongement

$$\mathrm{Aut}(\mathbf{A}^m_{\mathbf{Q}}) \hookrightarrow \mathrm{Aut}(\mathbf{A}^n_{\mathbf{Q}})$$

si $m > n$, comme on le verra dans la partie 5.

1.2 Le résultat de Prokhorov-Shramov

Dans leur article [PS16], Prokhorov et Shramov montre modulo la conjecture de Borisov-Alexeev-Borisov un résultat de contrôle sur les sous-groupes finis des transformations birationnelles d'une variété rationnellement connexe. Leur résultat est vrai modulo la conjecture BSB qui a été prouvé depuis.

Théorème 1.4. *En supposant la conjecture de Borisov, Alexeevn Borisov vraie en dimension n, alors il existe une constante $L = L(n)$ tel que pour toute variété rationnellement connexe X de dimension n définie sur un corps k de caractéristique 0 et pour tout nombre premier $p > L$, tout p-sous-groupe fini de* $\mathrm{Bir}(X)$ *est abélien et engendré par au plus n éléments.*

Depuis l'écriture de [PS16] la conjecture BSB a été démontré et ce théorème est donc vrai.

Ce résultat a des aspects plus forts que la borne de Minkowski pour les automorphismes polynomiaux car on considère une classe plus générale de variété que l'espace affine et surtout, on ne considère pas les automorphismes mais les transformations birationnelles. De plus on a une information sur la structure des groupes finis et pas seulement sur leurs cardinaux et on ne se restreint pas au corps des rationnels donc ce théorème est plus général. Cependant, dans le cas particulier des automorphismes de l'espace affine définis sur $\mathbf{Q}$, ce résultat est moins fort car on a une information pour les nombres premiers assez grand et une borne moins forte.

Sur les groupes nilpotents de type fini

La suite du mémoire est consacrée au contrôle des groupes nilpotents de type fini agissant par automorphismes algébriques sur une variété quasi-projective complexe.

Dans le cas où G est un groupe nilpotent de type fini agissant sur $\mathbf{A}^d_{\mathbf{C}}$. On montre que l'indice de résolubilité virtuel de G est plus petit que d.

Ici, on ne va pas regarder l'action de G sur des corps finis mais on va effectuer un changement de base pour se ramener sur $\mathbf{Z}_p$. On utilise le fait que tout corps de type fini sur $\mathbf{Q}$ se plonge dans $\mathbf{Q}_p$ de sorte que l'on puisse choisir un nombre fini d'éléments dont l'image sera dans $\mathbf{Z}_p$. On montre ce fait dans la partie 7.1.

Dans le cas de l'espace affine, tout est très simple. G étant de type fini son action est défini sur un anneau R de type fini sur $\mathbf{Z}$. On peut donc plonger R dans $\mathbf{Z}_p$ de sorte que l'action de G est définie sur $\mathbf{Z}_p$. Maintenant, G agit par automorphisme polynomiaux et donc en particulier par difféomorphisme analytique sur $\mathbf{Z}_p^d$. On peut donc utiliser la théorie de l'analyse p-adique pour étudier l'action de G. En particulier, on regardera les champs de vecteurs associés aux éléments de G et l'algèbre de Lie qu'ils engendrent pour obtenir le résultat suivant :

Théorème 1.5. *Si G est un groupe nilpotent de type fini qui agit sur $\mathbf{A}^d_{\mathbf{C}}$ par automorphisme polynomiaux, alors*

$$d \geq \mathrm{vdl}(G).$$

où $\mathrm{vdl}(G)$ *est l'indice de résolubilité virtuel de G.*

On étudiera enfin en dernière partie l'optimalité de ce théorème en regardant une classe particulière de groupe nilpotent, le groupe F_n/D_2, le quotient du groupe libre à n générateurs par son second groupe dérivé.

Théorème 1.6. *Soit $n \geq 2$ un entier, alors le groupe F_n/D_2 agit fidèlement sur une variété de dimension* 2.

On montrera en fait que l'on peut plonger F_n/D_2 dans un groupe de matrice 3×3.

Deuxième partie
Etude des groupes finis

Dans cette première partie, nous allons voir comment la donnée d'une action d'un groupe fini sur une variété algébrique complexe nous donne des informations sur son cardinal. L'outil primordial utilisé dans les preuve de cette partie est le passage du corps des complexes vers un corps fini.

2 Quelques résultats préliminaires

2.1 Sur les groupes finis

Nous allons travailler dans ce texte avec des p-groupes. On rappelle dans cette section quelques résultats sur ceux-ci.

Définition 2.1. Soit G un groupe et p un nombre premier.

- On dit que c'est un *p-groupe* si le cardinal de G est une puissance de p. En particulier, Le groupe trivial est un p-groupe.
- Soit H un sous-groupe de G, alors H est un *p-sous-groupe* de G si c'est un p-groupe.

Lemme 2.2. *Tout p-groupe non trivial admet un élément d'ordre p.*

Démonstration. Soit G un p-groupe et $x \in G$ non trivial, alors x est d'ordre $p^l \leq |G|$ avec $l \geq 1$. Et alors $x^{p^{l-1}}$ est d'ordre p. □

Lemme 2.3. *Le centre d'un p-groupe non trivial n'est jamais réduit à l'élément neutre.*

Démonstration. Soit G un p-groupe, alors G agit sur lui-même par conjugaison. L'orbite de l'élément neutre est réduite à un élément et par l'équation aux classes il existe au moins un autre point fixe (et en fait au moins p-1 autre points fixes). □

Lemme 2.4. *Soit G un p-groupe de cardinal p^ℓ, alors pour tout $0 \leq t \leq \ell, G$ possède un sous-groupe d'indice p^t.*

Démonstration. On fait la preuve par récurrence sur ℓ, si $\ell = 0$ ou $\ell = 1$ c'est vrai. Maintenant, on suppose $|G| = p^\ell$ avec $\ell \geq 2$. Soit $t \leq \ell$, par le lemme précédent, le centre $Z(G)$ de G est un p-sous-groupe non trivial de G. Par le lemme 2.2, il existe $x \in Z(G)$ non trivial d'ordre p. Le sous-groupe engendré par x est distingué dans G et on a le morphisme de groupes $\pi : G \twoheadrightarrow {}^G/_{<x>} =: G'$. On a $|G'| = p^{\ell-1}$ et par récurrence il existe un sous-groupe H' de G' de cardinal p^{t-1}. On définit alors $H := \pi^{-1}(H')$, c'est un sous-groupe de G de cardinal p^t car chaque fibre est de cardinal p. □

On définit dans la partie 7.4, la notion de groupes nilpotents et les propriétés de bases de ces groupes.

Théorème 2.5. *Soit p un nombre premier. Tout p-groupe est nilpotent.*

Démonstration. La preuve se fait par récurrence sur le cardinal du groupe en utilisant le fait que le centre d'un p-groupe non trivial n'est jamais trivial.

Si G est trivial, c'est vrai. Si G est de cardinal p aussi car alors G est cyclique et isomorphe à $\mathbf{Z}/p\mathbf{Z}$ qui est abélien.

Supposons G de cardinal p^ℓ avec $\ell \geq 2$, alors $Z(G)$ est abélien donc nilpotent. De plus, $Z(G)$ est non trivial donc par récurrence $G/Z(G)$ est nilpotent. Ceci implique que G est nilpotent car $Z(G)$ est central. □

Définition 2.6. Soit G un groupe fini et p un nombre premier. On note α la valuation p-adique de $|G|$. Un *p-sous groupe de Sylow* de G est un sous-groupe $H \subset G$ de cardinal p^α.

Théorème 2.7 (Théorème de Sylow)**.** *Soit G un groupe fini et p un facteur premier de $|G|$. En notant α la valuation p-adique de G, on a*

1. *G contient un p-sous-groupe de Sylow.*
2. *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow.*
3. *Tous les p-sous-groupes de G sont conjugués dans G.*
4. *Le nombre de p-sous-groupes de Sylow de G divise $\frac{|G|}{p^\alpha}$ et est congru à 1 modulo p.*

2.2 Arithmétique et Algèbre

2.2.1 Idéaux maximaux

Théorème 2.8. *Soit A un anneau commutatif et I un idéal strict de A, alors il existe un idéal maximal contenant I. En particulier, avec $I = \{0\}$, on voit que tout anneau commutatif admet un idéal maximal.*

Démonstration. Ceci découle du lemme de Zorn. En effet, soit X l'ensemble des idéaux stricts contenant A. X est ordonné par l'inclusion et est non vide car $I \in X$. De plus, si on prend une suite croissante $(J_k)_{k\in K}$ d'éléments de X, alors l'idéal $J := \bigcup_{k\in K}$ en est un majorant. En effet, J est un idéal car c'est une union d'idéaux croissants, de plus c'est un idéal strict car pour tout $k \in K$, 1 n'appartient pas à I_k donc 1 n'appartient pas à J. Par le lemme de Zorn, X admet un élément maximal et c'est un idéal maximal par définition. □

Théorème 2.9 (Nullstellensatz)**.** *Soit k un corps et A une k-algèbre de type fini. Soit $\mathfrak{m}$ un idéal maximal de A, alors $A/\mathfrak{m}$ est une extension finie de k.*

Théorème 2.10 (Nullstellensatz, deuxième version)**.** *Soit k un corps algébriquement clos et $f_1, ..., f_n \in k[X_1, ..., X_d]$ des polynômes, alors le système $(f_i = 0)_{1\leq i\leq n}$ n'a pas de solutions dans k si et seulement si l'idéal $(f_1, ..., f_n)$ est égal à $k[X_1, ..., X_n]$.*

Théorème 2.11. *Soit A une $\mathbf{Z}$-algèbre de type fini et $\mathfrak{m}$ un idéal maximal de A,alors $A/\mathfrak{m}$ est un corps fini.*

Démonstration. On note $\mathfrak{n} := \mathbf{Z} \cap \mathfrak{m}$. Comme c'est un idéal premier de $\mathbf{Z}$, on a $\mathfrak{n} = 0$ ou bien $\mathfrak{n} = p\mathbf{Z}$ avec p premier.

Montrons que $\mathbf{A}/\mathfrak{m}$ est une extension finie du corps des fractions de $\mathbf{Z}/\mathfrak{n}$. A est une $\mathbf{Z}$-algèbre de type fini donc il existe $a_1, ..., a_s \in A$ tel que tout élément de A s'écrive comme polynôme à coefficients entiers en les a_i. Notons $\overline{a_i}$ l'image de a_i dans $A/\mathfrak{m}$, il est clair que tout élément de $A/\mathfrak{m}$ s'écrit comme polynôme à coefficients dans $\mathbf{Z}/\mathfrak{n}$ en les $\overline{a_i}$. Donc $A/\mathfrak{m}$ est un corps qui est une Frac($\mathbf{Z}/\mathfrak{n}$)-algèbre de type fini. Par le Nullstellensatz, on a que $A/\mathfrak{m}$ est une extension finie de Frac($\mathbf{Z}/\mathfrak{n}$).

Supposons que $\mathfrak{n} = 0$, alors $A/\mathfrak{m}$ est une extension finie de $\mathbf{Q}$. On en prend une base $e_1, ..., e_n$ comme $\mathbf{Q}$-espace vectoriel, alors il existe un entier q tel que $\forall i, q\overline{a_i} \in \mathbf{Z}e_1 \oplus ... \oplus \mathbf{Z}e_n$ et $\forall k, l, qe_k \cdot e_l \in \mathbf{Z}e_1 \oplus ... \oplus \mathbf{Z}e_n$. Et donc, $\mathbf{Q}e_1 \oplus ... \oplus \mathbf{Q}e_n = A/\mathfrak{m} \subset \mathbf{Z}[\frac{1}{q}]e_1 \oplus ... \oplus \mathbf{Z}[\frac{1}{q}]e_n$ c'est absurde.

Donc il existe un nombre premier p tel que $\mathfrak{n} = p\mathbf{Z}$ et alors $A/\mathfrak{m}$ est une extension finie de $\mathbf{Z}/p\mathbf{Z}$ donc est un corps fini. □

2.2.2 Résultats arithmétiques

Théorème 2.12 (Dirichlet)**.** *Soient a et m deux entiers premiers entre eux. Il existe alors une infinité de nombre premiers p tel que $p \equiv m \mod a$.*

Proposition 2.13. *Soit n un entier naturel et p un nombre premier, alors*

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

où v_p est la valuation p-adique standard.

Démonstration. On remarque tout d'abord que la somme de droite est finie. Ensuite, on fait le calcul :

$$\begin{aligned} v_p(n!) = \sum_{k=1}^{n} v_p(k) &= \sum_{t \geq 1} t \left| \left\{ 1 \leq x \leq n \;\middle|\; p^t \mid x \text{ et } p^{t+1} \nmid x \right\} \right| \\ &= \sum_{t \geq 1} t \left(\left\lfloor \frac{n}{p^t} \right\rfloor - \left\lfloor \frac{n}{p^{t+1}} \right\rfloor \right) \\ &= \sum_{t \geq 1} t \left\lfloor \frac{n}{p^t} \right\rfloor - \sum_{t \geq 2} (t-1) \left\lfloor \frac{n}{p^{t+1}} \right\rfloor = \sum_{t \geq 1} \left\lfloor \frac{n}{p^t} \right\rfloor \end{aligned}$$

□

3 Un p-groupe a un point fixe

Théorème 3.1. *Soit p un nombre premier et G un p-sous-groupe de $\mathrm{Aut}_k(\mathbf{A}^d)$ avec k un corps algébriquement clos de caractéristique différente de p, alors G a un point fixe.*

Démonstration. **Premier cas : $k = \overline{\mathbf{F}_\ell}$**

Supposons tout d'abord que $k = \overline{\mathbf{F}_\ell}$ est la clôture algébrique d'un corps fini avec $l \wedge p = 1$. Il existe $q > 0$ tel que l'action de G est définie sur $\mathbf{F}_{\ell^q}$. Mais alors G agit sur $\mathbf{A}^d(\mathbf{F}_{\ell^q}) = (\mathbf{F}_{\ell^q})^d$ qui est de cardinal ℓ^{qd}. Par l'équation aux classes, on a une orbite qui consiste d'un seul point, c'est un point fixe de G.

Cas général

Comme G est fini il existe un anneau $\Lambda \subset k$ de type fini sur $\mathbf{Z}$ au-dessus duquel l'action de G est définie. Tout élément g de G est défini par un unique d-uplet de polynômes $(P_{g,i})_{1 \leq i \leq d} \in \mathbf{Q}[X_1, ..., X_d]^d$ tel que $g = (P_{1,g}, ..., P_{d,g})$. Si G n'a pas de points fixes cela veut dire que le système

$$x_i - P_{g,i}(x_1, \ldots, x_d) = 0 \quad (g \in G, 1 \leq i \leq d)$$

n'a pas de solutions sur $\mathbf{C}$. Par le Nullstellensatz 2.10, il existe des polynômes $Q_{g,i}$ tels que

$$\sum_{1\leq i\leq d, g\in G} (x_i - P_{g,i}(x_1,...,x_d))Q_{g,i}(x_1,...,x_d) = 1 \tag{1}$$

Ajoutons à Λ les coefficients des $Q_{g,i}$ et $1/p$. Cela donne un anneau de type fini $\Lambda' \supset \Lambda$. Soit $\mathfrak{m}$ un idéal maximal de Λ', on sait par le théorème 2.11 que $\Lambda'/\mathfrak{m} = \mathbf{F}_l$ est un corps fini de caractéristique différente de p car p est inversible dans Λ'. Donc si on note G' l'image de G, c'est un p-sous-groupe (de cardinal inférieur ou égal à $|G|$) de $\mathrm{Aut}_{\overline{\mathbf{F}_l}}(\mathbf{A}^d)$ qui n'a pas de point fixe par (1). C'est absurde. □

Ce théorème nous dit qu'un p-groupe ne peut pas agir librement sur une variété algébrique définie sur un corps de caractéristique différente de p. Ce résultat est faux en caractéristique p.

Théorème 3.2. *Soit G un p-groupe, il existe une action libre de G sur $\mathbf{A}^d_{\overline{\mathbf{F}_p}}$ avec $d = \frac{|G|(|G|-1)}{2}$.*

Démonstration. On note $N = |G|$. Il est connu que G se plonge dans le groupe symétrique $\mathfrak{S}_N$ en considérant l'action de G sur lui-même par translation. On a de plus une injection $\varphi : \mathfrak{S}_N \hookrightarrow GL_N(\mathbf{F}_p)$ où pour $\sigma \in \mathfrak{S}_n$, $\varphi(\sigma)$ est l'application linéaire qui envoie le i-ème vecteur de la base canonique sur le $\sigma(i)$-ème vecteur. On identifie G avec son image dans $GL_N(\mathbf{F}_p)$. On considère maintenant le sous-groupe :

$$T_N(\mathbf{F}_p) := \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in GL_N(\mathbf{F}_p) \right\}$$

C'est un p-sous-groupe de Sylow de $GL_N(\mathbf{F}_p)$ car $|GL_N(\mathbf{F}_p)| = p^{\frac{N(N-1)}{2}} \prod_{i=1}^N (p^i - 1)$ et $|T_N(\mathbf{F}_p)|$ est égal à $p^{\frac{N(N-1)}{2}}$. Or, G est contenu dans un p-sous-groupe de Sylow H qui est conjugué à $T_N(\mathbf{F}_p)$ par le théorème de Sylow (2.7). Donc, on a un plongement $G \hookrightarrow T_N(\mathbf{F}_p)$.

Enfin, on définit $d := \frac{N(N-1)}{2}$ et on identifie

$$\mathbf{A}^d(\overline{\mathbf{F}_p}) = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in GL_N(\overline{\mathbf{F}_p}) \right\}$$

G agit alors de façon polynomiale sur $\mathbf{A}^d(\overline{\mathbf{F}_p})$ par multiplication matricielle et cette action est libre. On obtient une action libre de G sur $\mathbf{A}^d_{\overline{\mathbf{F}_p}}$. □

4 Borne des sous-groupes finis de $GL_d(\mathbf{Q})$

Théorème 4.1. *Soit p un nombre premier et G un p-sous-groupe de $GL_d(\mathbf{Q})$ de cardinal p^α, alors*

$$\alpha \leq M(d,p) = \left\lfloor \frac{d}{p-1} \right\rfloor + \left\lfloor \frac{d}{p(p-1)} \right\rfloor + \left\lfloor \frac{d}{p^2(p-1)} \right\rfloor + \cdots = \left\lfloor \frac{d}{p-1} \right\rfloor + v_p\left((\left\lfloor \frac{d}{p-1} \right\rfloor ! \right)$$

Remarque 4.2. On observe que le nombre $M(d,p)$ est nul pour tout nombre premier p plus grand que $d+1$. Ainsi, l'entier $M(d) := \prod_{p\in\mathcal{P}} M(d,p)$, où $\mathcal{P}$ est l'ensemble des nombres premiers est bien défini. On peut alors déduire une borne sur les sous-groupes finis de $GL_d(\mathbf{Q})$.

Corollaire 4.3. *Soit G un sous-groupe fini de $GL_d(\mathbf{Q})$, alors $|G|$ divise $M(d)$. En particulier, $|G| \leq M(d)$*

Démonstration. Il suffit de montrer que pour tout nombre premier p, on a $v_p(|G|) \leq v_p(M(d)) = M(d,p)$. Ainsi, p un nombre premier et $\alpha := v_p(|G|)$. Par le théorème de Sylow (2.7), G admet un p-sous-groupe H de cardinal p^α. Par le théorème 4.1, on a $\alpha \leq M(d,p) = v_p(M(d))$, ce qui conclut la preuve du corollaire. □

Preuve du théorème. **Cas** $p \neq 2$

On va montrer que G peut être vu comme un sous groupe d'un groupe linéaire sur un corps fini. Pour cela, soit N assez grand tel que $G \subset GL_d(\mathbf{Z}[1/N])$, alors pour tout nombre premier ℓ assez grand, la réduction modulo ℓ de G est bien définie et est injective. De plus, on peut choisir ℓ de sorte qu'il soit un générateur de $(\mathbf{Z}/p^2\mathbf{Z})^*$. En effet, ce groupe est cyclique et soit x un générateur. On sait par le théorème de Dirichlet que l'ensemble des nombres premiers ℓ tels que $\ell \equiv x \mod p^2$ est infini. On peut donc en choisir un suffisamment grand tel que $G \hookrightarrow GL_d(\mathbf{F}_\ell)$.

Or, $|GL_d(\mathbf{F}_\ell)| = \ell^{\frac{d(d-1)}{2}} \prod_{i=1}^d (\ell^i - 1)$, donc $|G| = p^\alpha$ divise ce nombre. Nous allons donc étudier la valuation p-adique de $\prod_{i=1}^d (\ell^i - 1)$.

Tout d'abord, si $\ell^i \equiv 1 \mod p$, alors $\ell^{ip} - 1 = (\ell^i - 1)\sum_{j=0}^{p-1} \ell^{ij}$. Or, p divise $\ell^i - 1$, donc $\sum_{j=0}^{p-1} \ell^{ij} \equiv \sum_{j=0}^{p-1} 1 \equiv 0 \mod p$. Donc $\ell^{ip} \equiv 1 \mod p^2$. Ainsi, par le choix de ℓ, on a $p(p-1)$ qui divise ip, donc $p-1$ divise i. On vient de montrer que $p/(\ell^i - 1) \Rightarrow (p-1)/i$ (c'est ici que l'hypothèse $p \neq 2$ est utilisée). On suppose donc dans la suite que $p-1$ divise i. Par notre choix de ℓ, on a que si p ne divise pas i, alors $\varphi(p^2) = (p-1)p$ ne divise pas i et donc p^2 ne divise pas $\ell^i - 1$. Ainsi, $v_p(\ell^i - 1) = 1$. De manière générale, on a le

Lemme 4.4. *Avec ℓ et p choisi comme précédemment. Si $p-1$ divise i, alors*

$$v_p(\ell^i - 1) = 1 + v_p(i)$$

Preuve du lemme. On montre ce résultat par récurrence sur $v_p(i)$. Si $v_p(i) = 0$, c'est vrai par ce qui a été fait au-dessus.

On écrit $i = (p-1)p^{k+1}m$ avec $p \nmid m$ et on suppose le résultat vrai pour $v_p(i) = k$, alors en notant $s = \ell^{(p-1)m}$:

$$(s^{p^{k+1}} - 1) = (s^{p^k} - 1)\sum_{j=0}^{p-1} s^{jp^k}$$

Par hypothèse de récurrence, on a $v_p(s^{p^k} - 1) = 1 + k$ et il existe $u \in \mathbf{N}$ avec $p \nmid u$ tel que $s^{p^k} = 1 + up^{k+1}$. Et on a,

$$\begin{aligned} A_k := \sum_{j=0}^{p-1} s^{jp^k} &= \sum_{j=0}^{p-1}\sum_{t=0}^{j}\binom{j}{t}u^t p^{(k+1)t} \\ &= p + \sum_{j=1}^{p-1} jup^{k+1} + \sum_{j=0}^{p-1}\sum_{t=2}^{j}\binom{j}{t}u^t p^{(k+1)t} \\ &= p + \underbrace{\frac{u(p-1)}{2}p^{k+2} + \sum_{j=0}^{p-1}\sum_{t=2}^{j}\binom{j}{t}u^t p^{(k+1)t}}_{\text{divisible par } p^2 \text{ car } k\geq 0 \text{ et } p\neq 2} \end{aligned}$$

Donc $v_p(A_k) = 1$ ce qui conclut la preuve du lemme. □

Ainsi, on a l'inégalité

$$\begin{aligned} \alpha &\leq \sum_{p-1|i, 1\leq i\leq d} (1+v_p(i)) = \sum_{k=0}^{+\infty}(1+k)\,\mathrm{Card}\left\{1\leq i\leq d \;\middle|\; (p-1)p^k | i \text{ et } (p-1)p^{k+1} \nmid i\right\} \\ &= \sum_{k\geq 0}(1+k)\left(\left\lfloor \frac{d}{(p-1)p^k}\right\rfloor - \left\lfloor \frac{d}{(p-1)p^{k+1}}\right\rfloor\right) \\ &= \sum_{k\geq 0}(1+k)\left\lfloor \frac{d}{(p-1)p^k}\right\rfloor - \sum_{k\geq 1} k\left\lfloor \frac{d}{(p-1)p^k}\right\rfloor \\ &= \left\lfloor \frac{d}{p-1}\right\rfloor + \sum_{k\geq 1}\left\lfloor \frac{d}{(p-1)p^k}\right\rfloor \end{aligned}$$

Ce qui est la borne voulue.

Cas $p = 2$ Plonger G dans un groupe linéaire ne suffit pas, il est nécessaire de le plonger dans un groupe orthogonal pour avoir la borne souhaitée. On a le

Lemme 4.5. *Soit G un sous-groupe fini de $GL_d(\mathbf{Q})$, il existe une forme quadratique définie positive à coefficients entiers sur $\mathbf{Q}^d$ telle que G est un sous-groupe de $O(q)$.*

Démonstration. On prend la forme quadratique définie positive telle que $\forall x \in \mathbf{Q}^d, q(x) = x_1^2 + \cdots + x_d^2$ et on définit $q' = \sum_{g\in G} q\circ g$ qui est stable par G et définie positive. Quitte à multiplier q' par une constante on peut la prendre à coefficients entiers. □

Nous allons avoir besoin dans la preuve de calculer le cardinal d'un groupe orthogonal sur un corps fini.

Théorème 4.6. *Soit F un corps fini de caractéristique différente de 2 de cardinal q et Q une forme quadratique sur F non dégénérée, alors on a*

$$|O_{2k}(F,Q)| = 2q^{k(k-1)}(q^k-1)\prod_{i=1}^{k-1}(q^{2i}-1) \quad \textit{si le discriminant de } Q \textit{ est un carré}$$

$$|O_{2k}(F,Q)| = 2q^{k(k-1)}(q^k+1)\prod_{i=1}^{k-1}(q^{2i}-1) \quad \textit{sinon}$$

$$\textit{et } |O_{2k+1}(F,Q)| = 2q^{k^2}\prod_{i=1}^{k}(q^{2i}-1)$$

Remarque 4.7. Sur les corps finis, une forme quadratique non dégénérée est déterminée à conjugaison près par son discriminant, il y a donc potentiellement deux classes de groupe orthogonal. Cependant, en dimension impaire on peut montrer que ce sont les mêmes, alors qu'en dimension paire il y a bien deux classes de groupes orthogonaux non isomorphes car de cardinaux différents. C'est pour cela qu'il y a une distinction de cas en dimension paire. Pour une preuve détaillée de ce théorème voir [Gro02], théorème 9.11.

On choisit donc une forme quadratique non dégénérée sur $\mathbf{Q}^d$ à coefficients entiers et on choisit ℓ un nombre premier assez grand avec $\ell \equiv \pm 3 \mod 8$ tel que G s'injecte dans $GL_d(\mathbf{F}_\ell)$ et que ℓ ne divise pas le discriminant et les coefficients de q. Alors G s'injecte en fait dans le groupe orthogonal $O_d(\mathbf{F}_\ell, q)$.

Remarque 4.8. On a $(\ell^{2k}-1) = (\ell^k-1)(\ell^k+1)$. Donc $v_2(\ell^k \pm 1) \leq v_2(\ell^{2k}-1)-1$, car ℓ^k+1 et ℓ^k-1 sont pairs . Finalement, si on note $|G| = 2^\alpha$, on a par le théorème 4.6

$$\alpha \leq 1 + \sum_{i=1}^{k} v_2(\ell^{2i}-1) \text{ si } d = 2k+1$$

$$\text{et } \alpha \leq \sum_{i=1}^{k} v_2(\ell^{2i}-1) \text{ si } d = 2k$$

On calcule les valuations qui interviennent :

Lemme 4.9. *Si $\ell \equiv \pm 3 \mod 8$, on a*

$$v_2(\ell^{2i}-1) = 3 + v_2(i)$$

Démonstration. On montre ce résultat par récurrence sur $v_2(i)$.

Si i est impair, alors

$$\begin{aligned}\ell^{2i}-1 &= (\ell^2-1)\sum_{j=0}^{i-1}\ell^{2j} \\ &= (\ell-1)(\ell+1)\underbrace{\sum_{j=0}^{i-1}\ell^{2j}}_{\equiv 1 \mod 2}\end{aligned}$$

On a $\ell^{2i} \equiv 1 \mod 8$ donc $v_2(\ell^{2i}-1) \geq 3$ d'une part. D'autre part, comme $\ell \equiv \pm 3 \mod 8$, on a $v_2(\ell \pm 1) \leq 2$, donc $v_2(\ell^2-1) \leq 4$. Mais 4 divise $\ell-1$ si et seulement si 4 ne divise pas $\ell+1$, donc $v_2(\ell^2-1) \leq 3$ et on a l'égalité.

Supposons que le résultat soit vrai pour $v_2(i) = q$ et on écrit $i = 2^{q+1}m$ avec m impair, alors

$$\ell^{2i} - 1 = (\ell^{2^{q+1}m} - 1)(\ell^{2^{q+1}m} + 1)$$

Par hypothèse de récurrence, on a $v_2(\ell^{2^{q+1}m} - 1) = 3 + q$ et $\ell^{2^{q+1}m} + 1$ qui est pair mais pas divisible par 4 car $\ell^{2^{q+1}m} - 1$ l'est. On obtient donc bien $v_2(\ell^{2i} - 1) = 3 + q + 1$ et la formule est vraie par récurrence. □

On peut maintenant finir la preuve dans le cas $p = 2$.

Cas $d = 2k + 1$ On a par la remarque précédente :

$$\begin{aligned}
\alpha &\leq 1 + \sum_{i=1}^{k} v_2(\ell^{2i} - 1) = 1 + \sum_{i=1}^{k} (3 + v_2(i)) \\
&= 1 + 3k + \sum_{i=1}^{k} v_2(i) = 1 + 3k + v_2(k!) \\
&= 1 + 3k + \sum_{t \geq 1} \left\lfloor \frac{k}{2^t} \right\rfloor \quad \text{par la proposition 2.13} \\
&= 1 + 3k + \sum_{t \geq 1} \left\lfloor \frac{(d-1)}{2^{t+1}} \right\rfloor \leq 1 + 3k + \sum_{t \geq 2} \left\lfloor \frac{d}{2^t} \right\rfloor
\end{aligned}$$

Et on conclut car $1 + 3k = \frac{3d}{2} - \frac{1}{2} = d + \frac{d-1}{2} = d + \left\lfloor \frac{d}{2} \right\rfloor$.

Cas $d = 2k$ On a de façon analogue

$$\begin{aligned}
\alpha &\leq 3k + v_2(k!) \\
&= 3k + \sum_{t \geq 1} \left\lfloor \frac{k}{2^t} \right\rfloor = 3k + \sum_{t \geq 1} \left\lfloor \frac{d}{2^{t+1}} \right\rfloor
\end{aligned}$$

On conclut car $3k = \frac{3d}{2} = d + \frac{d}{2}$.

□

Remarque 4.10. Dans le cas $p = 2$, on aurait pu remplacer le corps $\mathbf{F}_\ell$ par $\mathbf{F}_{\ell^t}$ avec t impair. En effet, si on note $q = \ell^t$, alors G a un point fixe $m' \in \mathbf{A}_d(\mathbf{F}_q)$ par l'équation aux classes et le morphisme $G \to GL_d(\mathbf{F}_q)$ induit par m' est aussi injectif avec le même argument que celui de la preuve. De plus, $q \equiv \pm 3 \mod 8$ et pour tout i, $v_2(q^{2i} - 1) = v_2(\ell^{2ti} - 1) = 3 + v_2(ti) = 3 + v_2(i)$, car t est impair. Donc $v_2(|O_d(\mathbf{F}_\ell, Q)|) = v_2(|O_d(\mathbf{F}_q, Q)|)$ et on aboutit à la même borne sur le cardinal de G.

On a aussi le fait que cette borne est optimale.

Proposition 4.11 ([Ser07], 1.4)**.** *Soit p un nombre premier et $d \geq 1$, il existe un p-sous-groupe G de $GL_d(\mathbf{Q})$ tel que*

$$v_p(|G|) = M(d, p).$$

Démonstration. Le groupe symétrique S_p admet une représentation fidèle sur l'espace vectoriel $V_1 = \{(x_1, .., x_p) \in \mathbf{R}^p \mid x_1 + ... + x_p = 0\}$ de dimension $p-1$. On note $r = \left\lfloor \frac{d}{p-1} \right\rfloor$. On considère l'espace vectoriel $V = V_1 \oplus \cdots \oplus V_r$ somme directe de r copies de V_1. Soit S le produit semi-direct de S_r et $(S_p)^r$ où S_r permute les copies de S_p. S a une représentation fidèle sur V qui est de dimension $r(p-1) \leq n$. Donc S est un sous-groupe de $GL_{r(p-1)}(\mathbf{Q})$ et donc un sous-groupe de $GL_n(\mathbf{Q})$. Calculons maintenant la valuation p-adique du cardinal de S :

$$v_p(|S|) = v_p(r!) + v_p((p!)^r) = r + v_p(r!) = \left\lfloor \frac{d}{p-1} \right\rfloor + \left\lfloor \frac{d}{p(p-1)} \right\rfloor + ... = M(d,p)$$

N'importe quel p-Sylow donne un p-sous-groupe de $GL_n(\mathbf{Q})$ de cardinal $M(d,p)$. □

5 Borne de Minkowski sur les p-groupes d'automorphismes polynomiaux

On montre dans cette section que la borne que l'on trouve sur les p-groupes de matrices est la même pour les p-groupes finis de $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{A}^d)$. La preuve utilise un mélange de la preuve de Minkowski et de l'existence d'un point fixe pour un p-groupe en caractéristique différente de p.

Théorème 5.1. *Soit p un nombre premier et G un p-sous-groupe de $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{A}^d)$ de cardinal p^α, alors*

$$\alpha \leq M(d,p) = \left\lfloor \frac{d}{p-1} \right\rfloor + \left\lfloor \frac{d}{p(p-1)} \right\rfloor + \left\lfloor \frac{d}{p^2(p-1)} \right\rfloor + \cdots$$

Nous allons déduire ce théorème du résultat suivant :

Théorème 5.2. *Soit p un nombre premier et G un p-sous-groupe de $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{A}^d)$.*

- *Si $p \neq 2$, on peut plonger G dans $GL_d(\mathbf{F}_l)$ avec ℓ un nombre premier générateur de $(\mathbf{Z}/p^2\mathbf{Z})^*$.*
- *Si $p = 2$, on peut plonger G dans $O_d(\mathbf{F}_q, f)$, avec $q = l^{2t+1}$, ℓ un nombre premier congru à $\pm 3 \mod 8$ et f une forme quadratique non dégénérée sur $\mathbf{F}_q$.*

Ce théorème permet bien de trouver les bornes voulues sur les cardinaux car :

- Dans le cas $p \neq 2$, on obtient donc G comme un p-sous-groupe de $GL_n(\mathbf{F}_\ell)$ avec ℓ premier et générateur de $(\mathbf{Z}/p^2\mathbf{Z})^*$. On peut donc conclure comme pour la preuve de la borne de Minkowski sur les sous-groupes de $GL_d(\mathbf{Q})$.
- Dans le cas $p = 2$, on conclut par la remarque 4.10.

Démonstration. **Cas** $p \neq 2$.

Les coefficients des polynômes définissant les éléments de G sont à coefficients rationnels. On peut donc les voir dans un anneau de la forme $\mathbf{Z}[\frac{1}{N}]$. Ainsi, pour tout nombre premier ℓ avec $\ell > N$, la réduction modulo ℓ a un sens, car N est inversible modulo ℓ. On obtient donc un morphisme de groupes ρ_ℓ : $G \to \mathrm{Aut}_{\mathbf{F}_\ell}(\mathbf{A}^d)$. On montre qu'on peut choisir ℓ de sorte que ρ_ℓ soit injectif. Pour tout $g \in G$, il existe $x_g \in \mathbf{Q}^d$ tel que $g(x_g) \neq x_g$, ainsi pour tout nombre premier ℓ_g assez grand, on a $g(x_g) \not\equiv x_g \mod \ell_g$. Comme G est fini, on peut trouver un nombre premier ℓ commun à tous les éléments de g. On va supposer, comme dans la preuve des bornes de Minkowski que ℓ est un générateur de $(\mathbf{Z}/p^2\mathbf{Z})^*$ ce qui est possible par le théorème de Dirichlet.

On a donc montré qu'on peut voir G comme un p-sous-groupe de $\mathrm{Aut}_{\mathbf{F}_\ell}(\mathbf{A}^d)$ pour un ℓ bien choisi. Dans la suite, on remplace G par son image dans $\mathrm{Aut}_{\mathbf{F}_l}(\mathbf{A}^d)$. G agit alors sur $\mathbf{A}^d(\mathbf{F}_\ell) = (\mathbf{F}_\ell)^d$ qui est

de cardinal ℓ^d. Par l'équation aux classes et comme $\ell \wedge p = 1$, on a une orbite qui consiste en un point. C'est un point fixe $\mathbf{F}_\ell$-*rationnel* pour l'action de G que l'on note $m = (m_1, \ldots, m_d)$. On va maintenant plonger G dans le groupe $GL_d(\mathbf{F}_\ell)$.

On définit le morphisme de groupe :

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & GL_d(\mathbf{F}_\ell) \\ & g & \longmapsto & D_m g \end{array}$$

C'est bien un morphisme car m est fixe par G.

Tout élément g de G s'écrit par des polynômes $g = (P_1, \ldots, P_d)$. En décomposant chaque polynôme en polynôme homogène et en changeant de coordonnées pour que m soit l'origine (ce qui est possible car m est $\mathbf{F}_\ell$-rationnel) on obtient la décomposition :

$$g(z_1, \ldots, z_d) = D_m g(z_1, ..., z_d) + \sum_{j=2}^{N} A_j(z_1, \ldots, z_d)$$

Avec A_j la partie homogène de degré j de g. Montrons alors que φ est injectif, soit $g \in \ker \varphi$ avec $g \neq \mathrm{id}$, alors g s'écrit

$$g(z_1, ..., z_d) = \mathrm{id}(z_1, ..., z_d) + A_{j_0}(z_1, \ldots, z_d) + A_g(z_1, ..., z_d)$$

avec j_0 le plus petit indice j tel que A_j soit non nul et A_g les termes de degrés supérieurs à $j_0 + 1$, on itère g :

$$\begin{aligned} g^2(z_1, ..., z_d) =& \mathrm{id}(z_1, ..., z_d) + A_{j_0}(z_1, ..., z_d) + A_g(z_1, ..., z_d) \\ &+ A_{j_0}\left((\mathrm{id}(z_1, ..., z_d) + A_{j_0}(z_1, ..., z_d) + A_g(z_1, ..., z_d)\right) + A_g(g(z_1, ..., z_d)) \\ =& \mathrm{id}(z_1, ..., z_d) + 2A_{j_0}(z_1, ..., z_d) + (\text{termes de degré supérieurs}) \end{aligned}$$

En itérant le calcul, on obtient

$$\forall n \geq 0, \quad g^n(z_1, ..., z_d) = \mathrm{id}(z_1, ..., z_d) + nA_{j_0}(z_1, \ldots, z_d) + (\text{termes de degrés supérieurs})$$

Mais pour $n = p^\alpha$, on a $g^{p^\alpha} = \mathrm{id}$ ce qui impose $p^\alpha A_{j_0} = 0$. Comme ℓ ne divise pas p^α, on obtient $A_{j_0} = 0$, c'est absurde.

On a donc bien un plongement de G dans $GL_d(\mathbf{F}_l)$ avec ℓ un nombre premier générateur de $(\mathbf{Z}/p^2\mathbf{Z})^*$.

Cas $p = 2$ On cherche comme dans le cas linéaire à plonger G dans un groupe orthogonal. Soient $\mathbf{t} = (t_1, \ldots, t_d) \in \mathbf{C}^d$, on note $B^{\mathbf{t}}$ la forme bilinéaire symétrique définie par la matrice diagonale $\mathrm{Diag}(t_1, \ldots, t_d)$ dans la base canonique. Pour tout $g \in G$, on définit un champ de forme bilinéaire symétrique $g^*(B^{\mathbf{t}})$ par

$$\forall x \in \mathbf{A}_d(\mathbf{Q}), \forall u, v \in T_x(\mathbf{A}_d), \quad g^*(B^{\mathbf{t}})_x(u, v) = B^{\mathbf{t}}(D_x g(u), D_x g(v))$$

Et on définit $A_x^{\mathbf{t}}$ la matrice associée dans la base canonique à la forme bilinéaire symétrique $\sum_{g \in G} g^*(B^{\mathbf{t}})_x$. On regarde le polynôme $P(\mathbf{t}; x) = \det(A_x^{\mathbf{t}}) \in \mathbf{Q}[t_1, ..., t_d, x_1, ..., x_d]$ où $x = (x_1, .., x_d)$. On cherche à trouver un corps fini $\mathbf{F}_q$ de caractéristique $\ell \equiv \pm 3 \mod 8$ et des scalaires $t_1, ..., t_d$ tels que pour $m \in \mathbf{A}^d(\mathbf{F}_q)$ un point fixe pour l'action de G, on ait $P(\mathbf{t}; m) \neq 0$ dans F_q. Dans ce cas, on aura que G est un 2-sous-groupe du groupe orthogonal d'une forme quadratique non dégénérée sur $\mathbf{F}_q$.

Pour cela, il suffit de trouver un corps fini $\mathbf{F}_q$ dans lequel le système suivant a une solution :

$$(\mathcal{P}) \quad \begin{cases} P(\mathbf{t}; x) = 1 \\ P_i^g(x) - x_i = 0, \quad \forall g \in G, 1 \leq i \leq d \end{cases}$$

où les polynômes P_i^g sont ceux tels que $g = (P_1^g, ..., P_d^g)$.

Remarque 5.3. Pour tout nombre premier ℓ assez grand, le système $(\mathcal{P})$ est bien défini dans tout corps de caractéristique ℓ. En effet, il suffit de prendre ℓ plus grand que tous les dénominateurs des coefficients des polynômes qui interviennent dans ce système.

Supposons que $(\mathcal{P})$ n'ait pas de solutions dans $\mathbf{C}$, alors par le Nullstellensatz (2.10), il existe des complexes μ, et $(\lambda_i^g)_{g\in G, 1\leq i\leq d}$ tels que

$$1 = \mu(P(\mathbf{t}; x) - 1) + \sum_{g\in G, 1\leq i\leq d} \lambda_i^g (P_i^g(x) - x_i)$$

Maintenant, par le théorème 3.1, G admet un point fixe $z_0 \in \mathbf{A}_d(\mathbf{C})$ et on a

$$\mu(P(\mathbf{t}; z_0) - 1) = 1$$

Or, $P(0, ..., 0; z_0) = 0$ par construction de P, donc $\mu = -1$ et $P(\mathbf{t}, z_0) = P(t_1, ..., t_d; z_0) \in \mathbf{Q}[t_1, ..., t_d]$ serait le polynôme nul. Mais ceci est impossible car on peut choisir $t_1, ..., t_d$ tous entiers positifs, et dans ce cas la forme quadratique associée à $A^{\mathbf{t}}_{z_0}$ est définie positive donc son discriminant est non nul et alors $\det(A^{\mathbf{t}}_{z_0})$ est non nul. On aboutit donc à une contradiction.

Ainsi, notre système $(\mathcal{P})$ a une solution $(\mathbf{t}, x)$ avec $\mathbf{t} = (t_1, ..., t_d) \in \mathbf{C}^d$ et $x = (x_1, ..., x_d) \in \mathbf{A}^d(\mathbf{C})$. On note A l'algèbre engendrée par les coefficients de tous les polynômes apparaissant dans $(\mathcal{P})$, par les t_i et par les x_i. C'est une $\mathbf{Z}$-algèbre finiment engendrée. Soit ℓ un nombre premier congru à $\pm 3 \mod 8$ assez grand pour ne diviser aucun des coefficients des polynômes apparaissant dans $(\mathcal{P})$ (un tel nombre ℓ existe par Dirichlet). Par la prop 2.8, il existe un idéal maximal $\mathfrak{m} \subset A$ contenant ℓ. Le corps $A/\mathfrak{m}$ est fini par la proposition 2.11 et on le note $\mathbf{F}_q$. Par notre choix de $\mathfrak{m}$, on a que q est une puissance de ℓ, i.e $q = \ell^t$.

Ainsi, G se plonge dans $\mathrm{Aut}_{\mathbf{F}_q}(\mathbf{A}^d)$ et on peut l'identifier avec son image dans ce groupe. En notant m l'image de x dans $\mathbf{A}^d(\mathbf{F}_q)$ et f la forme quadratique dont la matrice dans la base canonique est l'image de $A^{\mathbf{t}}_x$ par la réduction modulo $\mathfrak{m}$, on définit le morphisme de groupes injectif

$$\begin{array}{rccc} \varphi : & G & \hookrightarrow & O_d(\mathbf{F}_q, f) \\ & g & \mapsto & D_m g \end{array}$$

En effet, f est clairement stable par $\varphi(G)$ et comme m est un point fixe, φ est bien définie comme morphisme de groupes. L'injectivité de φ se montre de la même manière que pour la preuve de la borne de Minkoswki. De plus, par construction le discriminant de f vaut 1, donc f est non dégénérée.

Maintenant, si $q = \ell^t$ est une puissance impaire de ℓ, le résultat est démontré. Sinon, on remplace $\mathbf{F}_q$ par $\mathbf{F}_{\ell^{t+1}}$ grâce à l'injection $\mathbf{F}_{\ell^t} \hookrightarrow \mathbf{F}_{\ell^{t+1}}$. f reste une forme quadratique non dégénérée sur $\mathbf{F}_{\ell^{t+1}}$ et on a un plongement $G \hookrightarrow O_d(\mathbf{F}_{\ell^{t+1}}, f)$. On note alors $\mathbf{F}_q = \mathbf{F}_{\ell^{t+1}}$.

Dans tous les cas on obtient un plongement de G dans $O_d(\mathbf{F}_q, f)$ avec les propriétés désirées.

□

On obtient donc la même borne que pour les sous-groupes finis de $GL_d(\mathbf{Q})$ alors que $GL_d(\mathbf{Q}) \subset \mathrm{Aut}(\mathbf{A}^d_{\mathbf{Q}})$. Par la proposition 4.11, cette borne reste optimale dans le cas polynomial et on a donc le corollaire suivant :

Corollaire 5.4. *Il n'existe pas de plongement* $\mathrm{Aut}(\mathbf{A}^m_{\mathbf{Q}}) \hookrightarrow \mathrm{Aut}(\mathbf{A}^n_{\mathbf{Q}})$ *si* $m > n$.

Démonstration. On a $m > n$ et $v_2(m!) \geq v_2(n!)$, donc $M(2, m) > M(2, n)$. Ainsi, par la proposition 4.11, il existe un 2-sous-groupe dans $\mathrm{Aut}(\mathbf{A}^m_{\mathbf{Q}})$ de taille trop grande pour être un 2-sous-groupe de $\mathrm{Aut}(\mathbf{A}^n_{\mathbf{Q}})$. □

Troisième partie

Utilisation des nombres p-adiques

Maintenant que l'étude des groupes finis est terminée. On regarde les groupes nilpotents de type fini. Si pour les groupes finis, il fallait passer du corps des complexes aux corps finis pour appliquer des lemmes de comptage, ici nous allons passer de $\mathbf{C}$ à $\mathbf{Z}_p$ avec p un nombre premier car nous allons avoir besoin d'outils analytiques.

6 Résultats d'analyse p-adique

6.1 Le principe des Zéros Isolés

Dans cette partie K est un corps valué. C'est à dire un corps muni d'une valuation tel que K soit complet pour la valeur absolue $|\cdot|$ associée à cette valuation. C'est à dire une norme $|\cdot|$ telle que l'on ait l'inégalité triangulaire améliorée : $\forall a, b \in K, |a+b| \leq \max(|a|, |b|)$ et qu'on ait la multiplicativité : $|ab| = |a| \times |b|$. On note R l'anneau de valuation de K, c'est l'ensemble des éléments de valeur absolue inférieur ou égale à 1. En particulier, K est le corps des fractions de R.

Lemme 6.1. *Soit $a, b \in K$, alors si $|a| \neq |b|$, on a*

$$|a+b| = \max(|a|, |b|)$$

Démonstration. Si a ou b est nul c'est évident. Supposons que les deux sont non nuls. On peut supposer quitte à inverser a et b que $|a| < |b|$. On a $|a+b| = |b| \left|1 + \frac{a}{b}\right|$. Il suffit donc de montrer que $\forall x \in R, |x| < 1 \Rightarrow 1 + x \in R^*$. Prenons un tel x, on définit $y_n := \sum_{i=0}^{n} (-1)^i x^i$, alors la limite $y := \lim_n y_n$ est bien définie car $|x| < 1$. Et on a bien $(1+x)y_n = 1 - (-1)^{n+1} x^{n+1} \to 1$, y est donc l'inverse de $1+x$ ce qui donne le résultat. □

Ce lemme est très utile en pratique. Prenons une série entière à coefficients dans K, $f = \sum_{n \geq 0} a_n x^n$ de rayon de convergence $r_f > 0$. Alors pour tout $x \in K$ tel que $|x| < r_f$, on a

$$|f(x)| \leq \sup_{n \geq 0} |a_n| \, |x|^n .$$

Et s'il existe un entier m tel que pour tout $n \neq m$, $|a_n| \, |x|^n < |a_m| \, |x|^m$, alors

$$|f(x)| = |a_m| \, |x|^m .$$

En particulier, si x est non nul et f non plus, alors $f(x) \neq 0$. Ceci nous pousse à définir le module de croissance de f :

Définition 6.2 (Module de croissance)**.** Soit $f = \sum_{n \geq 0} a_n x^n$ une série entière à coefficients dans K. On note r_f le rayon de convergence de f. Soit $0 < r < r_f$.

1. Le *module de croissance* de f est défini par

$$M_r(f) = \sup_{n \in \mathbf{N}} |a_n| \, r^n = \max_{n \in \mathbf{N}} |a_n| \, r^n .$$

2. On dit que r est un rayon *régulier* s'il existe un unique entier $n = n(r)$ tel que $M_r(f) = |a_n| r^n$. Le monôme $a_n x^n$ est alors appelé le *monôme dominant pour ce rayon.*
3. S'il existe au moins 2 indices $i \neq j$, tel que $M_r(f) = |a_i| r^i = |a_j| r^j$, on dit que r est un *rayon critique.* Les tels monômes $a_i x^i$ sont alors appelés les *monômes résonnants.*

Remarque 6.3. On a bien un maximum dans la définition au lieu d'un supremum car $r < r_f$, donc $a_n r^n \to 0$.

Lemme 6.4. *Avec les mêmes notations que la définition précédente, soit $0 < r \leq r_f$ tel que $a_n r^n$ tende vers 0, alors l'ensemble des rayons critiques de f strictement inférieur à r est fini.*

Démonstration. Soit m tel que $M_r(f) = |a_m| r^m = \max_n |a_n| r^n$. Alors pour tout $N > m$, il vient $|a_N| r^N \leq |a_m| r^m \Rightarrow \frac{|a_N|}{|a_m|} r^{N-m} \leq 1$. Donc

$$\forall 0 < s < r, \quad \frac{|a_N|}{|a_m|} s^{N-m} < 1 \Rightarrow |a_N| s^N < |a_m| s^m.$$

Donc seulement les monômes d'indice plus petit que m peuvent résonner avec $a_m s^m$. Ainsi, les rayons critiques $s < r$ seront ceux qui vérifieront une équation de la forme

$$s^{i-j} = \frac{|a_j|}{|a_i|}, \quad (0 \leq i < j \leq m).$$

Il y en a donc bien un nombre fini. □

Ce lemme permet de démontrer le principe des zéros isolés pour une série entière à coefficients dans K.

Théorème 6.5 (Principe des zéros isolés)**.** *Soit $f : R \to K^d$ une fonction analytique, alors les zéros de f sont en nombre fini.*

Plus précisément, avec $d = 1$, en écrivant $f = \sum_i a_i x^i$ si $r_0 < r_1 < ... < r_s \leq 1$ sont les rayons critiques de f inférieur ou égaux à 1. On définit pour tout $i = 1, .., s$,

$$\nu_i := \min \left\{ n \in \mathbf{N} \;\middle|\; |a_n| = \sup_i |a_i| \right\} \text{ et } \mu_i := \max \left\{ n \in \mathbf{N} \;\middle|\; |a_n| = \sup_i |a_i| \right\}.$$

Alors f a au plus $\sum_{k=1}^{s} (\mu_k - \nu_k)$ zéros sur R.

Démonstration. Voir ([Rob13], chapitre 6 partie 2).

En projetant sur les coordonnées il suffit de montrer le résultat pour $d = 1$. On a alors

$$f(x) = \sum_{i \geq 0} a_i x^i$$

(le fait que f soit définie sur R impose que $a_i \to 0$, donc $r_f \geq 1$).

On va tout d'abord montrer que f a un nombre fini de zéros sur la sphère de rayon 1, c'est à dire sur R^*.

Pour cela, on définit $\nu = \min \{n \in \mathbf{N} \mid |a_n| = \sup_i |a_i|\}$ et $\mu = \max \{n \in \mathbf{N} \mid a_n = \sup_i |a_i|\}$. Si $\mu = \nu$, alors $\forall k \neq \mu, |a_k| < |a_\mu|$ et donc pour tout $x \in R^*$, on a $|f(x)| = |a_\mu| \neq 0$. Donc f n'a pas de zéros sur R^*.

Si $\mu < \nu$, on va montrer que f a au plus $\mu - \nu$ zéros comptés avec multiplicité sur R^*. Soit $a \in R^*$, un zéro de f, alors f se factorise $f(x) = (x - a)g(x)$. si on définit μ' et ν' pour g, on a alors si $g(x) =$

$\sum b_k x^k$ que $a_k = b_{k-1} - ab_k$, en particulier si $|b_{k-1}| \neq |b_k|$, alors $|a_k| = \max(|b_{k-1}|, |b_k|)$ par le lemme 6.1. Donc $\mu' = \mu - 1$ et $\nu' = \nu$. Donc $\mu' - \nu' = \mu - \nu - 1$. On voit donc que le procédé doit s'arrêter et lorsque $\mu - \nu = 0$ on a vu que la fonction n'avait plus de zéros.

Maintenant, soit a un zéro de f de norme $r < 1$. Il est clair que r est un rayon critique de f, sinon il ne pourrait pas y avoir de zéros de norme r. On regarde la fonction $h(x) := f(xa)$. h est analytique et $r_h = r_f / |a| > r_f \geq 1$. Donc h a un nombre fini de zéros sur R^* par ce qui précède. Ainsi, f a un nombre fini de zéros de norme r qui est un rayon critique. Et l'on conclut par le fait qu'il y a un nombre fini rayon critique inférieur à 1 par le lemme 6.4. □

Proposition 6.6 (Prolongement Analytique)**.** *Soit $f : R^d \to K^{d'}$ une fonction analytique. Si f est nulle sur un ouvert, alors f est nulle partout.*

Démonstration. Soit U un ouvert de R^d sur lequel f est nulle. Soit $x \in U$, on peut remplacer U par la boule ouverte de centre x et de rayon r pour un certain $r > 0$. Soit $y \in R^d$, on considère la fonction

$$\varphi : t \in R \mapsto f(x + t(y - x))$$

Soit k un entier tel que $\left|\left|p^k(y - x)\right|\right| < r$, alors pour tout $n \in \mathbf{N}^*$, on a $\varphi(p^{kn}) = 0$. Donc l'ensemble des zéros de φ est infini, φ étant analytique, par le théorème 6.5, elle est nulle et donc $f(y) = \varphi(1) = 0$. □

6.2 Flot et champs de vecteurs analytiques

Dans cette partie, K un corps valué et complet pour la norme associée à la valuation tel que $|p| = 1/p$. En particulier, pour tout $k \in \mathbf{Z}, |k| \leq 1$. Un telle norme est forcément ultramétrique, en effet, si $x, y \in K$, alors $(x + y)^N = \sum_{k=0}^{N} \binom{N}{k} x^k y^{n-k}$ et donc $|x + y|^N \leq (N + 1) \max(|x|, |y|)^N$ par l'inégalité triangulaire classique. Maintenant, en prenant la racine N-ième dans cette inégalité et en faisant $N \to \infty$, on a bien $|x + y| \leq \max(|x|, |y|)$.

On note R l'anneau de valuation de K. On définit la *norme de Gauss* sur $R[x_1, ..., x_d] =: R[\mathbf{x}]$ par

$$f = \sum_{I \subset \mathbf{N}^d} a_I \mathbf{x}^I, \quad ||f|| := \sup_{I \subset \mathbf{N}^d} |a_I|$$

On définit *l'algèbre de Tate* $R\langle \mathbf{x} \rangle$ comme le complété de $R[\mathbf{x}]$ pour cette norme. C'est l'anneau de séries entières à coefficients dans R définies sur R^d. Concrètement, tout élément de $R\langle \mathbf{x} \rangle$ est une série entière $f = \sum_{I \subset \mathbf{N}^d} f_I \mathbf{x}^I$ tel que $f_I \to 0$ lorsque $I \to \infty$.

Définition 6.7. Une fonction $f : \mathbf{R}^d \to \mathbf{R}$ est dite *Tate-analytique* si $f \in R\langle \mathbf{x} \rangle$.

Définition 6.8. Soient $c > 0$ et $f, g \in R\langle \mathbf{x} \rangle$, on note $f \equiv g \mod p^c$ si

$$||f - g|| \leq |p|^c$$

On note $\mathcal{U} = R^d$ le polydisque de dimension d, on définit une norme sur $\mathcal{U}$ de la façon suivante : si $x = (x_1, ..., x_d) \in \mathcal{U}$, alors $||x|| = \max |x_i|$. De sorte que pour tout $h \in R\langle \mathbf{x} \rangle$ et $y \in \mathcal{U}$, on a $||h(y)|| \leq 1$. Donc toute fonction g de $R\langle \mathbf{x} \rangle$ définit une fonction analytique $g : \mathcal{U} \to \mathcal{U}$.

si $g = (g_1, ..., g_d)$ est un élément de $R\langle \mathbf{x} \rangle$, on définit la norme de g comme $||g|| = \max_i ||g_i||$. On a

$$||g|| \leq 1 \text{ et } \forall x, y \in \mathcal{U}, \quad ||g(x) - g(y)|| \leq ||g|| \, ||x - y||$$

De sorte que g est 1-Lipschitzienne.

Si on a plusieurs indéterminées $\mathbf{x} = (\mathbf{x}_1, ..., \mathbf{x}_d)$ et $\mathbf{y} = (\mathbf{y}_1, ...\mathbf{y}_m)$, alors la composition

$$R\langle \mathbf{y} \rangle^n \times R\langle \mathbf{x} \rangle^m \to R\langle \mathbf{x} \rangle^n$$
$$(h_1, ..., h_n), (g_1, ..., g_m) \to (h_1(g_1, ..., g_n), ..., h_n(g_1, ..., g_m))$$

est bien définie et lorsque $n = m = d$, on obtient le monoïde $(R\langle \mathbf{x} \rangle^d, \circ)$ avec la loi de composition

$$R\langle \mathbf{x} \rangle^d \times R\langle \mathbf{x} \rangle^d \to R\langle \mathbf{x} \rangle^d$$

Définition 6.9. Les éléments inversibles du monoïde $R\langle \mathbf{x} \rangle$ muni de la composition sont les *difféomorphismes analytiques de Tate*. Ils forment un groupe que l'on notera $\mathrm{Diff}^{an}(\mathcal{U})$.

La distance entre deux difféomorphismes analytiques g,f est définie par $||g - f||$ ce qui permet de donner à $\mathrm{Diff}^{an}(\mathcal{U})$ une structure de groupe topologique.

Lemme 6.10. *Soient* $f, g, h \in R\langle \mathbf{x} \rangle^d$.

(1) $||g \circ f|| \leq ||g||$.

(2) si f *est dans* $\mathrm{Diff}^{an}(\mathcal{U})$, *alors* $||g \circ f|| = ||g||$.

(3) $||g \circ (\mathrm{id} + h) - g|| \leq ||h||$.

(4) Si f *est un difféomorphisme analytique, alors* $||f - \mathrm{id}|| = \left|\left|f^{-1} - \mathrm{id}\right|\right|$.

Démonstration. (1) Soit $s \in R$ et $c > 0$ tel que $|s| = |p|^c = ||g||$. Alors $(1/s)g$ est un élément de $R\langle \mathbf{x} \rangle^d$, donc $(1/s)g \circ f$ aussi, ainsi $||g \circ f|| \leq |p|^c = ||g||$.

(2) On a $||g|| = \left|\left|g \circ f \circ f^{-1}\right|\right| \leq ||g \circ f|| \leq ||g||$ par (1). Donc toutes les inégalités sont des égalités.

(3) On écrit $h = (h_1, ..., h_d)$ avec $||h||_i \leq 1$. Alors $g \circ (\mathrm{id} + h)$ s'écrit

$$g \circ (\mathrm{id} + h) = g + A_1(h) + \sum_{j \geq 2} A_2(h)$$

avec A_j un polynôme homogène de degré j, ce qui donne le résultat.

(4) On a $||f - \mathrm{id}|| = \left|\left|f \circ (\mathrm{id} + (f^{-1} - \mathrm{id})) - f\right|\right|$, donc par (3), $||f - \mathrm{id}|| \leq \left|\left|f^{-1} - \mathrm{id}\right|\right|$ et le résultat découle en appliquant ceci à f^{-1}. □

Ce lemme permet d'établir le résultat suivant :

Proposition 6.11. *Pour tout nombre réel* $c > 0$, *on note* $D_c = \{f \in \mathrm{Diff}^{an}(\mathcal{U} \mid ||f - \mathrm{id}|| \leq |p|^c\}$. *Alors* D_c *est un sous-groupe distingué de* $\mathrm{Diff}^{an}(\mathcal{U})$.

Démonstration. Si f, g appartiennent à D_c, alors par le lemme 6.10, on a que f^{-1} appartient à D_c et $g \circ f$ aussi. Donc D_c est un sous-groupe, car $\mathrm{id} \in D_c$.

Ensuite, si $f \in D_c$ et $h \in \mathrm{Diff}^{an}(\mathcal{U})$, alors

$$\left|\left|h^{-1} \circ f \circ h - \mathrm{id}\right|\right| = \left|\left|(h^{-1} \circ f - h^{-1}) \circ h\right|\right| = \left|\left|h^{-1} \circ f - h^{-1}\right|\right|.$$

Mais le lemme 6.10, donne que

$$\left|\left|h^{-1} \circ f - h^{-1}\right|\right| = \left|\left|h^{-1} \circ (\mathrm{id} + f - \mathrm{id}) - h^{-1}\right|\right| \leq ||f - \mathrm{id}|| \leq |p|^c.$$

Donc D_c est bien un sous-groupe distingué. □

Définition 6.12. Une fonction $\Phi \in R\langle \mathbf{x}, n\rangle^d$ telle que

$$\forall s,t \in \mathbf{R}, \forall x \in \mathcal{U}, \Phi(x, t+s) = \Phi(\Phi(s,x),t).$$

est appelé un *flot analytique*. On notera $\Phi_t = \Phi(\cdot, t)$.

Théorème 6.13 (Bell-Poonen)**.** *Soit f un élément de $R\langle \mathbf{x}\rangle^d$ tel que $f \equiv \mathrm{id} \mod p^c$ avec $c > \frac{1}{p-1}$, alors f est un difféomorphismes analytique et il existe un unique flot analytique $\Phi : \mathcal{U} \times R \to \mathcal{U}$ tel que $\Phi_1 = f$. On a en particulier*

$$\forall n \in \mathbf{Z}, \Phi_n = f^n.$$

Démonstration. L'unicité vient du fait que si Φ, Ψ sont deux flots qui vérifient les propriétés du théorème, en fixant $x \in R$, la fonction $t \in R \mapsto \Phi(x,t) - \Psi(x,t)$ est analytique et s'annule sur $\mathbf{Z}$ donc par le principe des zéros isolés (lemme 6.5) la fonction est nulle. Donc $\Phi = \Psi$.

Pour l'existence, comme $||f - \mathrm{id}|| \leq |p|^c$, on a pour tout $h \in R[\mathbf{x}]^d, h(f(\mathbf{x})) \equiv f(\mathbf{x}) \mod p^c$ et en prenant des limites $h(f(\mathbf{x})) \equiv h(\mathbf{x}) \mod p^c$ pour tout $h \in R\langle \mathbf{x}\rangle^d$. Donc l'opérateur Δ défini par $\Delta h(\mathbf{x}) = h(f(\mathbf{x})) - h(\mathbf{x})$ envoie $R\langle \mathbf{x}\rangle^d$ sur $p^c R\langle \mathbf{x}\rangle^d$. On va appliquer Δ à l'identité et on définit alors

$$\Phi(\mathbf{x}, n) = \sum_{m \geq 0} \binom{n}{m} \Delta^m \mathbf{x} = \sum_{m \geq 0} n(n-1)...(n-m+1)\frac{\Delta^m \mathbf{x}}{m!}$$

Φ est bien un élément de de $R\langle \mathbf{x}, n\rangle^d$ car il existe $\varepsilon > 0$ tel que $c = \frac{1}{p-1} + \varepsilon$ et donc $||\Delta^m \mathbf{x}|| \leq |p|^{mc} < p^{-\frac{m}{p-1} - m\varepsilon}$ et $|m!| = p^{-v_p(m!)} \geq p^{\frac{m}{p-1}}$. Donc $\left|\left|\frac{\Delta^m \mathbf{x}}{m!}\right|\right| \leq p^{-m\varepsilon} \to 0$.

Et si $n \in \mathbf{N}$, alors

$$\Phi(\mathbf{x}, n) = \sum_{m=0}^{n} \binom{n}{m} \Delta^m \mathbf{x} = (\Delta + \mathrm{id})^n \mathbf{x} = f^n(\mathbf{x})$$

Pour montrer les autres propriétés : On prend $t \in \mathbf{N}$ et on fixe $x \in R^d$. Prenons la fonction, $g : s \in R \mapsto \Phi(x, t+s) - \Phi(\Phi(x,s),t)$, alors g est analytique et s'annule sur tout $\mathbf{N}$ qui est infini, par le principe des zéros isolés (lemme 6.5), g est nulle. Donc pour tout $t \in \mathbf{N}, s \in R, \Phi(x, s+t) = \Phi(\Phi(x,s),t)$. En répétant cet argument à $s \in R$ fixé, on obtient que pour tout $t, s \in R, \Phi(x, t+s) = \Phi(\Phi(x,t),s)$.

Enfin, on a pour tout $t \in R, \Phi(x,t) = f \circ \Phi(x, t-1)$. Avec $t = 0$ on obtient que f est un difféomorphisme analytique et que $f^{-1} = \Phi(\cdot, -1)$. Ce qui donne bien pour tout $n \in \mathbf{Z}, \Phi(\mathbf{x}, n) = f^n(\mathbf{x})$. □

Remarque 6.14. Le théorème de Bell-Poonen nous donne que si $p \geq 3$, alors toute fonction analytique $f \in R\langle \mathbf{x}\rangle^d$ qui vérifie $f \equiv \mathrm{id} \mod p$ est inclus dans un flot analytique.

Définition 6.15. On considère la K-algèbre de Lie $\Theta(\mathcal{U})$ des champs de vecteurs analytiques sur $\mathcal{U}$. Un élément $\mathbf{X}$ de U s'écrit $\mathbf{X} = \sum_{j=1}^d u_j(\mathbf{x})\partial_j$, avec u_j des fonctions analytiques définies sur R^d à valeurs dans K^d (c'est à dire qu'il existe $s \in R$, tel que $\forall j, s u_j \in R\langle \mathbf{x}\rangle^d$).

Si $\mathbf{Y}$ est un autre champ de vecteurs on définit le crochet de Lie de $\mathbf{X}$ et $\mathbf{Y}$ par :

$$[\mathbf{X}, \mathbf{Y}] = \sum_{j=1}^d w_j(\mathbf{x})\partial_j \text{ avec } w_j = \sum_{i=1}^d \left(u_i \frac{\partial v_j}{\partial x_i} - v_i \frac{\partial u_j}{\partial x_i} \right).$$

Lemme 6.16. *Soit $\Phi : \mathcal{U} \times R \to \mathcal{U}$ un flot analytique. Alors $\mathbf{X} := \left(\frac{\partial \Phi_t}{\partial t}\right)_{t=0}$ est un champ de vecteurs analytique. Il est invariant par Φ_t : pour tout $t \in R$, $(\Phi_t)^* \mathbf{X} = \mathbf{X}$. De plus, en notant $f = \Phi_1$, on a $\mathbf{X}(x_0) = 0$ si et seulement si x_0 est un point fixe de f.*

Démonstration. Soit $x \in \mathcal{U}$, alors $\mathbf{X}(x) = \frac{\partial \Phi}{\partial t}_{|t=0}(x,t)$. Et

$$\begin{aligned}(\Phi_s)^*\mathbf{X}(x) = D_{\Phi_s(x)}\Phi_{-s}(\mathbf{X}(\Phi_s(x))) &= D_{\Phi_s(x)}\Phi_{-s}\left(\frac{\partial \Phi}{\partial t}_{|t=0}(x,t+s)\right) \\ &= \frac{\partial}{\partial t}_{|t=0}\Phi_{-s}(\Phi(x,t+s)) \\ &= \frac{\partial \Phi_t}{\partial t}_{|t=0}(x) = \mathbf{X}(x).\end{aligned}$$

Ensuite, si x_0 est un point tel que $\mathbf{X}(x_0) = 0$, alors $\mathbf{X}$ est nul le long de la courbe $t \mapsto \Phi(x_0, t)$ car $\mathbf{X}$ est invariant par Φ_t, donc $\partial_t \Phi(x_0, t) = 0$ pour tout t, comme $\Phi(x_0, 0) = x_0$, on a le résultat.

Réciproquement, si x_0 est un point fixe de f, alors c'est aussi un point fixe de $f^n \mod$ pour tout $n \in \mathbf{Z}$. Donc la fonction $t \in R \mapsto \Phi_t(x_0) - x_0$ est analytique et nulle sur $\mathbf{Z}$, il vient par le principe des zéros isolés (lemme 6.5) qu'elle est nulle. Ainsi, pour tout $t \in R, \Phi_t(x_0) = x_0$ et donc $\frac{\partial}{\partial t}_{|t=0}\Phi(x_0, t) = 0 = \mathbf{X}(x_0)$. □

Corollaire 6.17. *Si f est un élément de* $\mathrm{Diff}^{an}(\mathcal{U})$ *avec $f \equiv \mathrm{id} \mod p^c$ pour un certain $c > 1/(p-1)$, alors f est donné par le flot Φ_f au temps $t = 1$ d'un unique champ de vecteur analytique $\mathbf{X}_f$. Les zéros de $\mathbf{X}_f$ sont exactement les points fixes de f.*

Deux tels difféomorphismes f et g commutent si et seulement si $[\mathbf{X}_f, \mathbf{X}_g] = 0$.

Démonstration. Si $\mathbf{X}_f$ et $\mathbf{X}_g$ commutent, alors les flots commutent aussi dans le sens où

$$\Phi_f(\Phi_g(x,s),t) = \Phi_g(\Phi_f(x,t),s)).$$

En prenant $s = t = 1$, on a que f et g commutent. Réciproquement, si f et g commutent, on a pour tout $s, t \in \mathbf{N}$, $f^s \circ g^t = g^t \circ f^s$, donc

$$\Phi_f(\Phi_g(x,t),s) = \Phi_g(\Phi_f(x,s),t), \quad \forall s,t \in \mathbf{N}$$

Un argument d'analycité avec le principe des zéros isolés similaire à ceux fait précédemment donne que les flots Φ_f et Φ_g commutent et donc $[\mathbf{X}_f, \mathbf{X}_g] = 0$. □

7 Des complexes au p-adique

Pour étudier l'action de groupes nilpotents sur nos variétés complexes, nous allons nous ramener à l'étude d'un groupe nilpotent agissant de façon analytique sur une variété définie sur $\mathbf{Z}_p$. A la fin de cette partie, nous montrerons comment utiliser le passage vers $\mathbf{Z}_p$ pour démontrer un analogue du théorème de Skolem-Mahler-Lech en géométrie algébrique.

7.1 Un théorème de plongement

On énonce d'abord le leme de Hensel qui va servir dans la suite.

Théorème 7.1 (Hensel)**.** *Soit $f \in \mathbf{Z}[X]$ un polynôme à coefficient entiers. Soit $n \geq 1$ tel que f a une racine x modulo p^n, alors, si $f'(x) \neq 0 \mod p$, f admet une racine y dans $\mathbf{Z}_p$ tel que $y \equiv x \mod p^n$.*

Démonstration. On cherche à construire $y = (y_m)_{m \geq 1} \in \mathbf{Z}_p$ une racine de f, on va construire y_m par récurrence en démontrant le lemme suivant

Lemme 7.2. *Avec les mêmes hypothèses que l'énoncé, il existe* $y \in \mathbf{Z}/p^{n+1}\mathbf{Z}$ *tel que* $y \equiv x \mod p^n$ *et* $f(y) = 0 \mod p^{n+1}$.

Démonstration. soit $x_0 \in \mathbf{Z}$ un relèvement de x, prenons $h \in p^n\mathbf{Z}$, on a $f(x_0 + h) = f(x_0) + hf'(x_0) + h^2g(h)$ avec $g \in \mathbf{Z}[T]$. On a $f(x_0+h) \equiv f(x_0)+hf'(x_0) \mod p^{n+1}$. Comme $f'(x_0)$ est inversible modulo p, il l'est aussi modulo p^n et on choisit $h \in \mathbf{Z}$ tel que $h \equiv -\frac{f(x_0)}{f'(x_0)} \mod p^{n+1}$. En prenant $y = x_0+h \mod p^{n+1}$, comme $f(x) = 0 \mod p^n$, on a bien $y \equiv x \mod p^n$. □

On construit y de la façon suivante : on pose pour tout $i = 1, .., n$, $y_i = x \mod p^i$. Soit $m \geq n$, on suppose avoir construit $y_m \in \mathbf{Z}/p^m\mathbf{Z}$ tel que $f(y_m) = 0 \mod p^m$ et $y_m \equiv x \mod p^n$. On a $f'(y_m) \equiv f'(x)$ mod p, donc est inverisble modulo p et le lemme nous donne $y_{m+1} \in \mathbf{Z}/p^{m+1}\mathbf{Z}$ tel que $f(y_{m+1}) = 0$ mod p^{m+1} et $y_{m+1} \equiv y_m \mod p^m$.

En posant $y := (y_m)_{m\geq 1} \in \mathbf{Z}_p$, y est bien une racine de f dans $\mathbf{Z}_p$.

□

Tout est possible grâce au résultat suivant :

Proposition 7.3. *Soit* K *une extension de type finie sur* $\mathbf{Q}$ *et* $S \subset K$ *une partie finie. L'ensemble des nombres premiers* p *tel qu'il existe un plongement* $K \hookrightarrow \mathbf{Q}_p$ *de sorte que* S *soit envoyé dans* $\mathbf{Z}_p$ *est infini.*

Démonstration. Comme K est de type fini sur $\mathbf{Q}$, on peut trouver des éléments $t_1, ..., t_d, \theta \in K$ tels que $K = \mathbf{Q}(t_1, ..., t_d)(\theta)$, avec $t_1, ..., t_d$ algébriquement indépendants et θ algébrique sur $\mathbf{Q}(t_1, ..., t_d)$ par le théorème de l'élément primitif.

Soit $f \in \mathbf{Q}(t_1, .., t_d)[x]$ le polynôme minimal de θ sur $\mathbf{Q}(t_1, ..., t_d)$. En éliminant les dénominateurs on peut supposer que $f \in \mathbf{Z}[t_1, ..., t_d][x]$. On note $\Delta(t_1, ..., t_d) \in \mathbf{Z}[t_1, ..., t_d]$ le discriminant de f par rapport à x. Pour tout $s \in S$, il existe un polynôme $g_s \in \mathbf{Q}(t_1, ..., t_d)[x]$ tel que $g_s(\theta) = s$. On choisit un polynôme $B_s \in \mathbf{Z}[t_1, ..., t_d][x]$ tel que $B_sg_s \in \mathbf{Z}[t_1, ..., t_d][x]$. Enfin, on définit le polynôme $A_s \in \mathbf{Z}[t_1, ..., t_d]$ comme le résultat de $f(x)$ et $B_sg_s(x)$. Choisissons maintenant des entiers $a_1, ...a_d$ tels que

(i) $\Delta(a_1, ..., a_d) \neq 0$.

(ii) $f(a_1, ..., a_d; x)$ n'est pas un polynôme constant.

(iii) $B_s(a_1, ..., a_d) \neq 0$ pour tout $s \in S$.

(iv) $A_s(a_1, ..., a_d) \neq 0$ pour tout $s \in S$.

Un tel choix d'entiers est possible. En effet, si on note $P(t_1, ..., t_d)$ le coefficient dominant de f, alors le polynôme

$$P(t_1, ..., t_d)\Delta(t_1, ..., t_d)\left(\prod_{s\in S} A_s\right)\left(\prod_{s\in S} B_s\right)$$

est un polynôme non nul à coefficient entiers. Donc on peut trouver des entiers $a_1, ..., a_d$ qui n'annule pas ce polynôme (car $\mathbf{Z}^d$ est dense dans $\mathbf{Q}^d$ pour la topologie de Zariski) et ces entiers conviennent.

On regarde maintenant les nombres premiers p tels que

(i) $\Delta(a_1, ..., a_d) \neq 0 \mod p$.

(ii) $A_s(a_1, ..., a_d) \neq 0 \mod p$, pour tout $s \in S$.

(iii) $B_s(a_1, ..., a_d) \neq 0 \mod p$ pour tout $s \in S$.

(iv) $f(a_1, ..., a_d; x)$ a une racine modulo p.

Il existe une infinité de tels p premier. En effet, les trois premières condition sont vérifiées dès que p est assez grand et pour la dernière on a le lemme suivant :

Lemme 7.4. *Soit $f \in \mathbf{Z}[X]$, il existe une infinité de nombres premiers p tels que f a une racine modulo p.*

Démonstration. On suppose quitte à prendre $-f$ que le coefficient dominant de f est positif. Il existe alors un rang T à partir duquel $\forall n \geq T, f(n) \geq 0$.

Supposons que le lemme soit faux, il existe alors des nombres premiers $p_1, ..., p_r$ tels que

$$\forall n \in \mathbf{Z}, f(n) = p_1^{\alpha_n^1} \cdots p_r^{\alpha_n^r}$$

Mais alors, on a

$$\text{Card}\left(\{f(n) \mid n \in \mathbf{N}\} \cap [0, M]\right) = O((\log M)^r)$$

Car $f(n) \leq M \Rightarrow \forall i, \alpha_n^i \leq \frac{1}{p_i} \log M$.

Mais en $+\infty$, $f(n)$ est équivalent à cn^d avec d le degré de f et $c > 0$ le coefficient dominant de f. Ce qui donne que $\text{Card}\left(\{f(n) \mid n \in \mathbf{N}\} \cap [0, M]\right) \geq \beta M^{1/d}$ pour $\beta > 0$ une constante et M assez grand. Ceci est absurde. □

Fixons un tel p, on choisit $\mu_1, ..., \mu_d$ algébriquement indépendants dans $\mathbf{Z}_p$ (c'est possible car $\mathbf{Z}_p$ n'est pas dénombrable). Le polynôme $f(a_1 + p\mu_1, ..., a_d + p\mu_d)$ a une racine modulo p, et comme $\Delta(a_1, ..., a_d) \neq 0 \mod p$ le lemme de Hensel donne une racine $\theta' \in \mathbf{Z}_p$ de $f(a_1 + p\mu_1, ..., a_d + p\mu_d)$. On a donc un plongement $K \hookrightarrow \mathbf{Q}_p$ donné par

$$t_i \mapsto a_i + p\mu_i, \quad \theta \mapsto \theta'$$

De plus les conditions sur A_s et B_s nous assure que les éléments de S sont envoyés dans $\mathbf{Z}_p$. En effet, si on note s' l'image de $s \in S$ par ce morphisme, on a $s' = g_s(a_1 + p\mu_1, ..., a_d + p\mu_d)(\theta')$, ensuite $B_s(a_1 + p\mu_1, ..., a_d + p\mu_d)$ est dans $\mathbf{Z}_p^*$ car non nul modulo p. Donc $B_s(a_1 + p\mu_1, ..., a_d + p\mu_d)s' \in \mathbf{Z}_p$ et finalement, $s' \in \mathbf{Z}_p$. □

Définition 7.5. Soit X une variété irréductible complexe et Γ un sous-groupe finiment engendré de $\text{Aut}(X)$.

- Soit R un anneau intègre. On dit que (X, Γ) est défini sur R, s'il existe un schéma irréductible, séparé et réduit X_R sur R et un monomorphisme $\Gamma \hookrightarrow \text{Aut}(X_R)$ tel que X et Γ soit obtenu par le changement de base $X = X_R \times_{\text{Spec } R} \text{Spec } \mathbf{C}$.
- Soit p un nombre premier. Un *modèle* de (X, Γ) sur $\mathbf{Z}_p$ est est la donnée
  1. d'un anneau $R \subset \mathbf{C}$ sur lequel X et Γ sont définis et d'un plongement $R \hookrightarrow \mathbf{Z}_p$.
  2. D'une variété irréductible $\mathcal{X}$ sur $\mathbf{Z}_p$ et d'un monomorphisme $\rho : \Gamma \hookrightarrow \text{Aut}_{\mathbf{Z}_p}(\mathcal{X})$ tel que

$$\mathcal{X} \simeq X_R \times_{\text{Spec } R} \text{Spec } \mathbf{Z}_p$$

  est le changement de base de X_R et pour tout $f \in \Gamma$, $\rho(f)$ est le changement de base de f.
- Un *bon modèle* sur $\mathbf{Z}_p$ de (X, Γ) est la donné d'un modèle avec de plus la condition que la fibre spéciale $\mathcal{X}_{\mathbf{F}_p} = \mathcal{X} \times_{\text{Spec } \mathbf{Z}_p} \text{Spec } \mathbf{F}_p$ est géométriquement réduite et irréductible et que de plus sa dimension soit

$$\dim_{\mathbf{F}_p}(\mathcal{X}_{\mathbf{F}_p}) = \dim_{\mathbf{Q}_p}(\mathcal{X} \times_{\text{Spec } R} \text{Spec}(\mathbf{Q}_p))$$

Proposition 7.6. *Soit X une variété projective irréductible complexe et Γ un sous-groupe de $\mathrm{Aut}(X)$ de type fini. Alors il existe une infinité de nombres premiers $p \geq 3$ tels que (X, Γ) admet un bon modèle sur $\mathbf{Z}_p$.*

Démonstration. La preuve se décompose en deux parties, d'abord un lemme préparatoire puis la construction du bon modèle.

On choisit un plongement $X \hookrightarrow P^M(\mathbf{C})$ tel que $X = Z(\mathfrak{a})$ avec $\mathfrak{a}$ un idéal homogène de $\mathbf{C}[X_0, ..., X_M]$ et $Z(\mathfrak{a})$ le lieu d'annulation de $\mathfrak{a}$. Comme Γ est de type fini, il existe un anneau R de type fini sur $\mathbf{Z}$ sur lequel, X et Γ sont définis. C'est à dire qu'il existe une variété projective $X_R \to \operatorname{Spec} R$ telle que $X = X_R \times_{\operatorname{Spec} R} \operatorname{Spec} \mathbf{C}$. En effet, on peut prendre par exemple l'anneau engendré par les coefficients des générateurs de $\mathfrak{a}$ et de Γ. Soit $\pi : X_R \to \operatorname{Spec} R$ un tel modèle de fibre générique X_K où K est le corps des fractions de R.

Lemme 7.7. *Il existe un ouvert affine non vide U de $\operatorname{Spec} R$ tel que*

(1) *V est de type fini sur $\operatorname{Spec} \mathbf{Z}$.*

(2) *Pour tout point $y \in U$, la fibre X_y est géométriquement irréductible et $\dim_{k(y)} X_y = \dim_K X_K$, où $k(y)$ est le corps résiduel de y.*

Démonstration. On aura besoin du fait que pour tout schéma intègre affine $\operatorname{Spec} A$ de type fini sur $\operatorname{Spec} \mathbf{Z}$ et tout ouvert V_1 de $\operatorname{Spec} A$, il existe un ouvert affine $V_2 \subset V_1$ qui est de type fini sur $\operatorname{Spec} \mathbf{Z}$. En effet, si on note I l'idéal de A tel que $\operatorname{Spec} A \setminus V_1 = \operatorname{Spec} A/I$, alors en prenant n'importe quel $f \in I$ non nul, on a $\operatorname{Spec} A[1/f] \subset V_1$ qui est de type fini sur $\operatorname{Spec} Z$ car $\operatorname{Spec} A$ l'est.

Comme X est irréductible sur $\mathbf{C}$ et que $\overline{K} = \mathbf{C}$, on a que X_K est géométriquement réduite. Par ([DG66], Proposition 9.7.8), on a l'existence d'un ouvert V de $\operatorname{Spec} R$ tel que pour tout $y \in V$, X_y est géométriquement irréductible. par le lemme précédent, on peut supposer que V est affine, intègre, de type fini sur $\operatorname{Spec} \mathbf{Z}$. Ensuite, par le théorème de platitude générique ([DG66], Proposition 8.9.4) , on peut encore réduire V de sorte que $\pi : \pi^{-1}(V) \to V$ soit plat. Dans ce cas, pour tout $y \in V$, la fibre X_y est géométriquement irréductible et de dimension $\dim_{k(y)} X_y = \dim_K X_K$ par platitude.

□

Maintenant, on peut remplacer R par l'anneau R' tel que $V = \operatorname{Spec} R'$ en sachant que pour tout $y \in R', X_y$ est géométriquement irréductible de dimension $d = \dim X$. Comme R' est de type fini, il existe une infinité de nombre premiers $p \geq 3$ tels que $R' \hookrightarrow \mathbf{Z}_p$ par la proposition (7.3), ce qui donne un morphisme $\operatorname{Spec} \mathbf{Z}_p \to \operatorname{Spec} R'$. On pose $\mathcal{X} = X_R \times_{\operatorname{Spec} R'} \operatorname{Spec} \mathbf{Z}_p$. Par ce que l'on sait sur les fibres du morphismes $X_{R'} \to \operatorname{Spec} R'$, on a que la fibre spéciale $\mathcal{X}_{\mathbf{F}_p}$ est géométriquement réduite et de dimension d. $\mathcal{X}$ est donc un bon modèle de (X, Γ). □

Remarque 7.8. Ce théorème est aussi vrai pour les variétés quasi-projectives. En effet, soit X une telle variété, il suffit de reprendre la preuve en choisissant un plongement $X \hookrightarrow \mathbf{P}^M_{\mathbf{C}}$ tel que $X = Z(\mathfrak{a}) \setminus Z(\mathfrak{b})$ avec $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux homogènes, on prend alors pour R l'anneau engendré par les coefficients des générateurs de $\mathfrak{a}$ et $\mathfrak{b}$ et le reste de la preuve ne change pas.

7.2 D'automorphismes algébriques vers des difféomorphismes analytiques

Dans cette partie on considère $\mathcal{X}$ un schéma de dimension d sur $\mathbf{Z}_p$ tel que

- $\mathcal{X}$ est quasi-projectif sur $\mathbf{Z}_p$ et sa fibre générique et spéciale sont géométriquement irréductibles (sur $\mathbf{Q}_p$ et $\mathbf{F}_p$ respectivement).

- $\overline{\mathcal{X}} = \mathcal{X} \times_{\operatorname{Spec} \mathbf{Z}_p} \operatorname{Spec} \mathbf{F}_p$ est la fibre spéciale de $\mathcal{X}$.
- $\Phi : \mathcal{X} \to \mathcal{X}$ est un automorphisme de $\mathbf{Z}_p$-schémas.
- $\overline{\Phi} : \overline{\mathcal{X}} \to \overline{\mathcal{X}}$ est la restriction de Φ à la fibre spéciale.
- $r : \mathcal{X}(\mathbf{Z}_p) \to \overline{\mathcal{X}}(\mathbf{F}_p)$ est l'application de réduction.
- x est un $\mathbf{F}_p$-point.

Pour les deux propositions suivantes, on renvoie à [BGT10]

Proposition 7.9. *Soit $\mathcal{X}$ un schéma quasi-projectif sur $\mathbf{Z}_p$. Il existe une fonction $\iota : \mathcal{X}(\mathbf{Z}_p) \to \mathbf{Z}_p^d$ qui induit une bijection analytique entre $\mathbf{Z}_p^d$ et l'ouvert de $\mathcal{X}(\mathbf{Z}_p)$ des points β tels que $r(\beta) = x$.*

Proposition 7.10. *On suppose que $\overline{\Phi}(x) = x$, alors il existe des fonctions Tate-analytiques $F_1, ..., F_d \in \mathbf{Z}\langle T_1, ..., T_d\rangle$ telles que*

(i) Pour tout $\beta \in \mathcal{X}(\mathbf{Z}_p)$ tel que $r(\beta) = x$, en notant $\iota(\beta) = (\beta_1, ..., \beta_d)$ on a

$$\iota(\Phi(\beta)) = (F_1(\beta_1, ..., \beta_d), ..., F_d(\beta_1, ..., \beta_d))$$

(ii) Chaque F_i est congru à polynôme linéaire modulo p (c'est à dire que tous les coefficients de degré supérieur ou égal à 2 de F_i est divisible par p).

En notant $\mathcal{F} = (F_1, ..., F_d)$, on a que $\mathcal{F}$ est un difféomorphisme analytique de $\mathbf{Z}_p^d$ car Φ est un automorphisme.

Remarque 7.11. On a en fait unicité de $\mathcal{F}$ par prolongement analytique,de sorte que ce procédé est fonctoriel. En effet si Ψ est un autre automorphisme vérifiant les mêmes conditions que Φ, si on note $\mathcal{F}_\Psi$ le difféomorphisme analytique associé, on a par unicité que

$$\mathcal{F}_{\Phi\circ\Psi} = \mathcal{F}_\Phi \circ \mathcal{F}_\Psi$$

et $\mathcal{F}_{\mathrm{id}} = \mathrm{id}$.

Proposition 7.12. *Soit Γ un sous-groupe de $\operatorname{Aut}_{\mathbf{Z}_p}(\mathcal{X})$. Il existe un sous-groupe d'indice fini $\Gamma_0 \subset \Gamma$ tel que l'action de Γ_0 sur $\mathcal{X}$ est conjuguée à une action d'un sous-groupe de $\operatorname{Diff}_1^{an}(\mathcal{U})$ avec $\mathcal{U} = \mathbf{Z}_p^d$.*

Démonstration. La restriction à la fibre spéciale donne un morphisme de Γ vers $\operatorname{Perm}(\overline{\mathcal{X}}(\mathbf{F}_p))$ qui est un groupe fini. On peut donc trouver un sous-groupe $\Gamma' \subset \Gamma$ d'indice fini tel que Γ' agit trivialement sur $\overline{\mathcal{X}}(\mathbf{F}_p)$. Alors par la proposition 7.10 et la remarque 7.11, on a un monomorphisme $\Gamma' \hookrightarrow \operatorname{Diff}^{an}(\mathcal{U})$. On suppose maintenant que $\Gamma' \subset \operatorname{Diff}^{an}(\mathcal{U})$. Le (2) de la proposition 7.10 donne que la réduction modulo p fournit un morphisme de Γ' vers $\operatorname{Aff}(\mathbf{Z}/p\mathbf{Z})^d)$ le groupe des transformations affines de $(\mathbf{Z}/p\mathbf{Z})^d$ qui est fini. Donc le noyau $\Gamma_0 \subset \Gamma'$ du morphisme de réduction modulo p est d'indice fini et est un sous-groupe de $\operatorname{Diff}_1^{an}(\mathcal{U})$. Ainsi, Γ_0 est un sous-groupe d'indice fini de Γ dont l'action sur $\mathcal{X}$ est conjuguée à une action d'un sous-groupe de $\operatorname{Diff}_1^{an}(\mathcal{U})$. □

7.3 Le théorème de Skolem-Mahler-Lech en géométrie algébrique

Le théorème de Skolem-Mahler-Lech donne une information sur l'ensemble des zéros d'une suite récurrente linéaire.

Théorème 7.13 (Skolem-Mahler-Lech)**.** *Soit $u := (u_n)_{n\in\mathbf{N}}$ une suite récurrente linéaire à coefficients complexes, alors l'ensemble des zéros de u est une union d'un ensemble fini et d'une union finie de progression arithmétique. C'est à dire*

$$\{n \in N \mid u_n = 0\} = F \cup \bigcup_{i=1}^{r} (a_i\mathbf{N} + b_i)$$

avec F fini et a_i, b_i des entiers positifs.

La preuve utilise de l'analyse p-adique. On peut montrer un énoncé similaire en géométrie algébrique dont la preuve s'inspire du théorème pour les suites.

Théorème 7.14. *Soit X une variété affine sur $\mathbf{C}$, $\Phi : X \to X$ un automorphisme de X, $\alpha \in X(\mathbf{C})$ et V une sous-variété fermée de X, alors l'ensemble $\{n \in \mathbf{N} \mid \Phi^n(\alpha) \in V\}$ est une union d'un ensemble fini et d'une union finie de progression arithmétique.*

Remarque 7.15. On retrouve bien le théorème de Skolem-Mahler-Lech. En effet, si u est une suite récurrente linéaire d'ordre d, alors en notant $X_0 = (u_0, ..., u_{d-1})$, on sait qu'il existe une matrice A telle que

$$\begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix} = A^n X_0$$

et alors

$$\{n \in \mathbf{N} \mid u_n = 0\} = \{n \in \mathbf{N} \mid A^n X_0 \in \{x_0 = 0\}\}$$

On retrouve bien le théorème de Skolem-Mahler-Lech

Preuve du théorème. On traite d'abord le cas où $X = \mathbf{A}^n_{\mathbf{C}}$ est l'espace affine. $\Phi = (F_1, ..., F_n)$ est alors un automorphisme polynomial de $\mathbf{C}^n$ dans $\mathbf{C}^n$ et V est définie par des polynômes $G_1, .., G_s \in \mathbf{C}[X_1, ..., X_n]$. Soit R l'anneau engendré par les coefficients des F_i, des G_j et les coordonnées de α. Par la proposition 7.3, il existe un nombre premier p tel que $\Phi = (F_1, ..., F_n)$ soit alors un automorphisme de $\mathbf{A}^d_{\mathbf{Z}_p}$, V une sous-variété fermée définie par $G_1, ..., G_s \in \mathbf{Z}_p[X]$ et $\alpha \in \mathbf{A}^n_{\mathbf{Z}_p}(\mathbf{Z}_p)$.

Maintenant on veut utiliser le lemme de Bell-Poonen (6.13) pour plonger l'orbite de α dans un flot analytique. Cependant, on n'a pas forcément $\Phi \equiv \mathrm{id} \mod p$, pour remédier à cela, on va remplacer Φ par une certaine puissance. Avec la proposition 7.12, on a déjà qu'il existe une puissance de Φ qui appartient à $\mathrm{Diff}^{an}_1(\mathbf{Z}^d_p)$, mais dans le cas où l'on considère qu'un seul morphisme on peut voir directement comment utiliser le lemme de Bell-Poonen.

Par un changement de coordonnées affine, on peut supposer que $\alpha = 0$.

Comme $\mathbf{A}^n(\mathbf{Z}/p^2\mathbf{Z})$ est fini et que $GL_n(\mathbf{Z}/p\mathbf{Z})$ est fini aussi, il existe une puissance N de Φ telle que $\Phi^n \equiv \mathrm{id} \mod p^2$ et $D_m f \equiv \mathrm{id} \mod p$ pour tout point $m \in \mathbf{A}^n(\mathbf{Z}_p)$. Ainsi, on a

$$\Phi^N(\mathbf{x}) = p^2 A_0 + (\mathrm{id} + pB_1)(\mathbf{x}) + \sum_{k\geq 2} A_k(\mathbf{x})$$

avec $A_0 \in \mathbf{A}^n(\mathbf{Z}_p)$, B_1 une matrice $n \times n$ à coefficients dans $\mathbf{Z}_p$ et $\sum_{k\geq 2} A_k$ est une somme finie de polynômes homogènes de degré k à coefficients dans $\mathbf{Z}_p$.

On définit maintenant $\Psi(\mathbf{x}) := p^{-1}\Phi^N(p\mathbf{x}) = pA_0 + (\mathrm{id} + pB_1)(\mathbf{x}) + \sum_{k\geq 2} p^{k-1}A_k(\mathbf{x})$. On a $\Psi \equiv \mathrm{id}$ mod p et c'est un élément de $\mathbf{Z}_p\langle\mathbf{x}\rangle$. Par le lemme de Bell-Poonen (6.13), il existe un flot analytique $f(\mathbf{x}, t) \in \mathbf{Z}_p\langle\mathbf{x}, t\rangle$ tel que $\forall l \in \mathbf{Z}, f(\mathbf{x}, l) = \Psi^l(\mathbf{x}) = p^{-1}\Phi^{Nl}(p\mathbf{x})$. On voit que pour tout $l \in \mathbf{Z}$, $f(\cdot, l)$ est analytique définie sur la boule de fermée centre 0 et de rayon p, c'est donc le cas aussi pour $f(\cdot, t)$ pour tout $t \in \mathbf{Z}_p$.

On pose pour tout $j = 0, ..., n-1$:

$$f_j(t) = pf(p^{-1}\Phi^j(\alpha), t)$$

$f_j : \mathbf{Z}_p \to \mathbf{Q}_p^d$ est bien une fonction analytique et on a pour tout $b \in \mathbf{Z}$:

$$f_j(b) = \Phi^{Nb+j}(\alpha)$$

Maintenant, s'il existe une infinité d'entiers m tel que $\Phi^m(\alpha) \in V$, alors certaines des fonctions f_j ont une infinité de valeurs dans V. Ce qui veut dire que les fonctions analytiques $G_i(f_j(t))$ s'annule une infinité de fois, par le principe des zéros isolés (6.5), elles sont nulles. Donc pour tout $b \in \mathbf{N}$, $f_j(b) \in V$, c'est à dire

$$\left\{ \Phi^{Nb+j}(\alpha) \;\middle|\; b \in \mathbf{N} \right\} \subset V$$

Ce qui nous donne le résultat.

Pour le cas général, on utilise le théorème de Srinivas

Théorème 7.16 (Srinivas)**.** *Soit Y une variété affine sur un corps k, il existe un entier $n = n(Y) > 0$ tel que pour tout $N > n$, si $f, g : Y \hookrightarrow \mathbf{A}_k^N$ sont deux plongements dans un espace affine, alors il existe un automorphisme de k-schémas $\varphi : \mathbf{A}_k^N \to \mathbf{A}_k^N$ tel que $f = \varphi \circ g$.*

Démonstration. Voir [**?**], Théorème 2 , page 26]. □

Dans notre cas, on prend on a une variété affine X et un automorphisme de schémas $\Phi : X \to x$. on prend un entier N assez grand tel qu'il existe un plongement $\iota : X \hookrightarrow \mathbf{A}_{\mathbf{C}}^N$ et tel qu'on soit dans les conditions du théorème. Posons $g = \iota \circ \Phi$, on applique le théorème à g et ι, alors il existe un automorphisme $\Psi : \mathbf{A}_{\mathbf{C}}^N \to \mathbf{A}_{\mathbf{C}}^N$ tel que $g = \Psi \circ \iota$. C'est à dire

$$\iota \circ \Phi = \Psi \circ \iota$$

Donc Φ se prolonge en un automorphisme Ψ de $\mathbf{A}_{\mathbf{C}}^N$ et alors

$$\{n \in \mathbf{N} \mid \Phi^n(\alpha) \in V\} = \{n \in \mathbf{N} \mid \Psi^n(\alpha) \in V\}$$

V peut être vue comme une sous-variété fermée de $\mathbf{A}_{\mathbf{C}}^N$ et on s'est ramené au cas de l'espace affine.

□

Quatrième partie

Minoration de la dimension à l'aide de l'indice de Résolubilité

Dans cette partie, on va étudier l'action d'un groupe nilpotent sur une variété quasi-projective complexe. Le principal résultat de cette section et que l'on peut utiliser l'indice de résolubilité virtuel du groupe pour minorer la dimension sur laquelle le groupe agit, résultat qui est mentionné dans [CX14], théorème 6.6.

7.4 Résultat sur les groupes Nilpotents

Définition 7.17. Soit G un groupe, on définit la suite centrale descendante par $G^{(0)} := G$ et par induction $G^{(r)} = [G^{(r-1)}, G]$. On définit aussi $G_{(0)} = G$ et par induction $G_{(r)} = [G_{(r-1)}, G_{(r-1)}]$.

On dit que G est *nilpotent* s'il existe $s \geq 0$ tel que $G^{(s)} = 0$ et on note $\mathrm{nilp}(G)$ le plus petit s qui vérifie cette propriété. C'est l'*indice de nilpotence* de G.

On dit que G est résoluble, s'il existe $t \geq 0$ tel que $G_{(t)} = 0$. On note $\mathrm{dl}(G)$ le plus petit t qui vérifie cette propriété. C'est l'*indice de résolubilité* de G.

On définit les algèbres de Lie nilpotentes de la même manière.

Remarque 7.18. On a G nilpotent $\Rightarrow$, G résoluble.

Lemme 7.19. *Soit G un groupe et H un sous-groupe central de G. Alors G est nilpotent si et seulement si G/H est nilpotent.*

De même, si $\mathfrak{h}$ est une algèbre de Lie et $\mathfrak{z}$ une sous-algèbre de Lie centrale de $\mathfrak{h}$, alors $\mathfrak{h}$ est nilpotente si et seulement si $\mathfrak{h}/\mathfrak{z}$ l'est.

Démonstration. On a la suite exacte $0 \to H \to G \to G/H \to 0$. On note $G_1 := G/H$ Si G est nilpotent d'indice r, alors $G_1^{(r)} = 0$ car G se surjecte sur G_1. Réciproquement, si G_1 est nilpotent d'indice r, alors $G^{(r)} \subset H$ car il est nul dans G_1 et comme H est central, $G^{(r+1)} = 0$.

La preuve est analogue dans le cas des algèbres de Lie. □

Lemme 7.20. *Supposons que l'on a une suite exacte de groupe résolubles*

$$0 \to K \to G \to H \to 0$$

, alors $\mathrm{dl}(G) \leq \mathrm{dl}(H) + \mathrm{dl}(K)$.

Démonstration. Soient h, g, k les indices de résolubilités de H, G, K respectivement. On a $G_{(h)} \subset K$ car nul dans H. Comme $K_{(k)} = 0$, on a $(G_{(h)})_{(k)} = G_{(h+k)} = 0$. Donc $g \leq k + h$. □

7.5 Un premier résultat de minoration sur $\mathbf{Z}_p$.

Définition 7.21. Soit $H \subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ un groupe. On définit $\mathfrak{h}$ la $\mathbf{Q}_p$-algèbre de Lie engendrée par les champs de vecteurs analytiques X_f pour f dans H. On dit que $\mathfrak{h}$ est l'*algèbre de Lie associée à H*.

Théorème 7.22. *Si $H \subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p)$ est un groupe nilpotent, alors H est abélien et $\mathfrak{h}$ aussi.*

Démonstration. Si H est nilpotent, alors son centre n'est pas trivial. Soit $f \in Z(H)$ non trivial, alors X_f est dans le centre de $\mathfrak{h}$. On peut trouver un redressement de X_f sur un petit polydisque $\mathcal{V}$ tel que $X_f = \partial_x$. Mais alors, sur $\mathcal{V}$, tout élément X de $\mathfrak{h}$ s'écrit $X = \alpha\partial_x$ avec $\alpha \in \mathbf{Z}_p$ car X commute avec ∂_x. Donc $\mathfrak{h}_{|\mathcal{V}}$ est abélienne et par le corollaire 6.6, $\mathfrak{h}$ est abélienne, ce qui implique aussi que H est abélien. □

Théorème 7.23. *Soit $d \geq 1$ un entier et $H \subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ un groupe nilpotent. Soit $\mathfrak{h}$ l'algèbre de Lie associée à H, alors $\mathfrak{h}$ est nilpotente et on a*

$$\mathrm{dl}(H) \leq d.$$

Démonstration. Pour le cas $d = 1$, c'est le théorème 7.22. On suppose le théorème vrai en toute dimension inférieure à d et on prend $H \subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ nilpotent.

On note $\mathfrak{h}$ l'algèbre de Lie associée à H et $\mathfrak{z}$ son centre. Pour $x \in \mathbf{Z}_p^d$, on note $s(x)$ la dimension de $\mathfrak{z}(x) := \{X(x) \mid X \in \mathfrak{z}\}$ et on pose $s := \max_{x\in\mathbf{Z}_p^d} s(x)$. On peut trouver un certain polydisque $\mathcal{U} \subset \mathbf{Z}_p^d$ tel que $\mathfrak{z}(x)$ soit de dimension constante égale à s pour tout $x \in \mathcal{U}$, la restriction à $\mathcal{U}$ est un morphisme injectif par prolongement analytique (proposition 6.6), donc on travaille maintenant sur $\mathcal{U}$. Soit $X_1, ..., X_s$ une base de $\mathfrak{z}$ sur $\mathcal{U}$. Comme tous ces champs de vecteurs commutent entre eux, on peut trouver un redressement tel que $X_i = \partial_{d-i+1}$ quitte à prendre un plus petit polydisque inclus dans $\mathcal{U}$. Maintenant, comme $\mathfrak{z}$ est le centre de $\mathfrak{h}$, on a que tout $X \in \mathfrak{h}$ s'écrit sur $\mathcal{U}$:

$$X = \sum_{i=1}^{d} u_i(x_1, ..., x_{d-s})\partial_i \tag{2}$$

La projection sur les $d - s$ premières coordonnées donne une suite exacte d'algèbre de Lie

$$0 \to \mathfrak{z} \to \mathfrak{h} \to \mathfrak{h}_1 \to 0 \tag{3}$$

Nous allons maintenant étudier $\mathfrak{h}_1$. Soit $f \in H$, alors X_f est de la forme 2. Donc f s'écrit

$$f(x_1, ..., x_d) = (F(x_1, ..., x_{d-s}), x_{d-s+1} + F_{d-s+1}(x_1, ..., x_{d-s}), ..., x_d + F_d(x_1, ..., x_{d-s}))$$

où $F \in \mathrm{Diff}_1^{an}(\mathbf{Z}_p^{d-s})$.

La projection sur les $d - s$ premières coordonnées donnent un morphisme surjectif de H vers un groupe $H_1 \subset \mathrm{Diff}_1^{an}(\mathcal{V})$ où $\mathcal{V}$ est un polydisque inclus dans $\mathbf{Z}_p^{d-s}$, dont l'algèbre de Lie associée est exactement $\mathfrak{h}_1$. On note Z le noyau de ce morphisme. Z est abélien et on obtient la suite exacte,

$$0 \to Z \to H \to H_1 \to 0$$

Comme H est nilpotent, on a que H_1 l'est aussi par le lemme 7.19, donc par hypothèse de récurrence $\mathfrak{h}_1$ est nilpotente. Comme $\mathfrak{z}$ est central dans $\mathfrak{h}$ on a aussi par le lemme 7.19 que $\mathfrak{h}$ est nilpotente. Maintenant, par récurrence on a $\mathrm{dl}(H_1) \leq d-s \leq d-1$ et par le lemme 7.20, il vient $\mathrm{dl}(H) \leq 1+\mathrm{dl}(H_1) \leq d$. □

7.6 Le théorème

Définition 7.24. Soit H un groupe nilpotent, on définit l'indice de résolubilité virtuel de H par

$$\mathrm{vdl}(H) = \min\left\{\mathrm{dl}(H') \;\middle|\; H' \subset H \text{ d'indice fini}\right\}$$

Théorème 7.25. *Soit X une variété quasi-projective complexe de dimension d et H un groupe nilpotent de type fini qui agit fidèlement sur X par automorphisme algébrique, alors*

$$d \geq \mathrm{vdl}(H).$$

Démonstration. On va d'abord montrer que l'on peut supposer X irréductible pour pouvoir se ramener à un schéma sur $\mathbf{Z}_p$.

X a un nombre fini de composantes irréductibles et H les permute. Donc il existe un sous-groupe $H' \subset H$ d'indice fini qui stabilise les composantes irréductibles de X. On remplace X par sa composante irréductible de dimension maximale et H par H'.

X est alors une variété quasi-projective irréductible complexe de dimension d, par la proposition 7.6, il existe un nombre premier $p \geq 3$ tel que (X, H) admet un bon modèle $\mathcal{X}$ sur $\mathbf{Z}_p$. Maintenant, par la proposition 7.12, il existe un sous-groupe d'indice fini $H_0 \subset H$ qui est isomorphe à un sous-groupe de $\mathrm{Diff}_1^{an}(\mathcal{U})$. Comme H_0 est aussi nilpotent, le résultat découle du théorème 7.23 qui donne que $d \geq \mathrm{dl}(H_0)$. □

8 Exemple et Contre-Exemple

Dans cette partie, nous allons voir si la borne du théorème 7.25 est optimale. Étant donné que l'on regarde des groupes nilpotents, les groupes les plus généraux auxquels on pourrait penser sont les groupes F_n/D_r où F_n est le groupe libre et D_r le r-ième groupe de la suite centrale descendante $(D_0 = F_n, D_{i+1} = [D_i, F_n])$. En regardant des cas particuliers, nous allons voir que le théorème 7.25 ne peut pas être amélioré.

8.1 Indice de nilpotence

On pourrait se demander si l'on peut remplacer dans le théorème l'indice de résolubilité virtuel par l'indice de nilpotence virtuel. Il n'en est rien. En effet, l'exemple donnée par Epstein-Thurston dans [ET79] montre que l'on ne peut pas avoir une inégalité avec l'indice de nilpotence. On le traite en détail dans la suite.

Soit $n \in \mathbf{N}^*$ et A la matrice

$$A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}.$$

On a pour tout $t \in \mathbf{R}$,

$$\exp(tA) = \begin{pmatrix} 1 & t & \cdots & \frac{t^{n-1}}{(n-1)!} \\ & \ddots & \ddots & \vdots \\ & & \ddots & t \\ & & & 1 \end{pmatrix}.$$

On note G le sous-groupe des transformations affines

$$G = \{x \in \mathbf{R}^n \mapsto \exp(tA)x + b \mid t \in \mathbf{R}, b \in \mathbf{R}^n\}.$$

On notera $(t, b) := x \mapsto \exp(tA)x + b$. En fait, G est isomorphe au produit semi-direct $G \simeq \mathbf{R} \ltimes \mathbf{R}^n$ dont le produit est donné par

$$(t, b) \cdot (s, c) = (t + s, b + \exp(tA)c).$$

En particulier,

$$((t, b)^{-1} = (-t, -\exp(-tA)b).$$

Proposition 8.1. *G est nilpotent d'indice n et son indice de résolubilité est 2.*

Démonstration. Prenons $(t,b),(s,c) \in G$, alors

$$(t,b)(s,c)(t,b)^{-1}(s,c)^{-1} = (0,(I_n - \exp(sA))b + (\exp(tA) - I_n)c) =: (0,M_1)$$

Donc $D_1(G) = G_{(1)}$ est un sous-groupe de translations, il est donc abélien. Ainsi, G est résoluble d'indice 2.

Ensuite, prenons un autre élément $(u,d) \in G$,

$$(u,d)g(u,d)^{-1}g^{-1} = (0,(\exp(uA) - I_n)M) =: (0,M_2)$$

On a que M_1 est l'image combinaison linéaire d'image de vecteur par une matrice triangulaire supérieure à diagonale nulle. Comme $\exp(uA) - I_n$ est aussi à diagonale nulle, on a que M_2 est somme de l'image de deux vecteurs par une matrice triangulaire supérieure dont la diagonale et la première sur-diagonale est nulle. On peut donc montrer par récurrence que

Lemme 8.2. *Si g est un commutateur de longueur r, alors g est de la forme $g = (0,M_r)$ où M_r est une somme d'image de vecteurs par une matrice triangulaire supérieure dont la diagonale et les $(r-1)$ premières sur-diagonales sont nulles.*

En effet, il suffit juste de montrer le fait que si A est une matrice triangulaire supérieure à diagonale nulle et que B est telle que pour tout i,j, tels que $j - i \leq r$, on a $B_{ij} = 0$, alors pour tout i,j tels que $j - i \leq r+1, AB[i,j] = 0$ et c'est un calcul direct.

Ainsi, par le lemme 8.2, G est nilpotent d'indice au plus n et on a en fait égalité car

$$[(t,0),[,...,[(t,0),(0,c)]...] = (0,(\exp(tA) - I_n)^{n-1}c)$$

où on a pris $n-1$ commutateurs. Et $(\exp(tA) - I_n)^{n-1}$ n'est pas nul donc en prenant c qui n'est pas dans le noyau de cette matrice on a que ce commutateur n'est pas trivial. □

Maintenant, on peut montrer que G agit fidèlement en dimension 2. En effet, posons $\mathcal{S}$ l'espace vectoriel des translations engendrées par $T_{e_i}, 2 \leq i \leq n$, où $e_1,...,e_n$ est la base canonique de $\mathbf{R}^n$. G agit fidèlement sur $G/\mathcal{S}$ par translation à gauche.

En effet, si $g = (t,b)$ est un élément de G, on prend $h = (s,c)$. Alors $g\mathcal{S} \mapsto hg\mathcal{S}$ est bien définie. Si $(0,y_0)$ est un élément de $\mathcal{S}$, on a

$$hg(0,y_0) = (s+t, c + \exp(sA)b + \exp(s+t)Ay_0)$$

et si $(0,x_0)$ est un autre élément de $\mathcal{S}$, on a

$$hg(0,y_0) = hg(0,x_0)(0,y_0 - x_0)$$

L'action est donc bien définie.

Montrons qu'elle est fidèle. On note V l'espace vectoriel engendré par $e_2,...,e_n$. Supposons que $h = (s,c)$ agisse trivialement sur $G/\mathcal{S}$, alors pour tout $t \in \mathbf{R}$, $h(t,0)\mathcal{S} = (t,0)\mathcal{S}$. Donc il existe $x_t \in V$ tel que

$$(t+s,c) = (t,0)(0,x_t) = (t,\exp(tA)x_t)$$

Cela donne $s = 0$ et pour tout $t \in \mathbf{R}$, $\exp(-tA)c = x_t$. Donc $t \mapsto x_t$ est C^∞. On note $c = (c_1,...,c_n)$. En prenant $t = 0$, on a $c = x_0 \in V$ donc $c_1 = 0$. Ensuite, en dérivant à $t = 0$, $-Ac = \dot{x_0}$ qui appartient à V car V est un espace vectoriel, donc $c_2 = 0$. En généralisant, on a pour tout $k = 0,...,n-1$

$$\frac{1}{k!}(-A)^k c = \frac{\mathrm{d}^k}{\mathrm{d}t^k}_{|t=0} x_t \in V.$$

Ce qui donne que $d_k = 0$, en effet, A^k a tous ses coefficients nuls sauf la k-ième sur-diagonale qui contient des 1, donc la première coordonnée de $A^k c$ est c_k. Il vient $c = 0$ et h est l'identité. L'action est bien fidèle.

Enfin, $G/\mathcal{S}$ est difféomorphe à $\mathbf{R}^2$, donc on a bien une action fidèle de G par automorphisme polynomiaux sur un espace de dimension 2.

8.2 Une classe de groupe où le théorème est optimal

La partie précédente nous donne déjà un exemple de groupe où le théorème est optimal. Nous allons voir dans cette partie une classe d'exemple où l'inégalité ne peut être améliorée.

On travaille dans cette partie avec les groupe $F_n/D_2, (n \geq 2)$. Nous allons montrer que le théorème 7.25 est optimal pour ces groupes.

8.2.1 Une représentation de ce groupe

On va voir dans cette section que les groupes F_n/D_r peuvent être représenter comme des polynômes en des variables commutatives. Le fait d'être un commutateur se vérifie alors sur les degrés de ces polynômes et les calculs sont alors plus simples. On renvoie à [MKS04] pour une référence.

Dans la suite n est un entier naturel et $A = \mathbf{Z}[[X_1, ..., X_n]]$ est l'anneau des séries formelles en n variables non commutatives.

Soit $P, Q_1, ..., Q_n \in A$, alors la composition est bien définie $P(Q_1, ..., Q_n)$. On a le

Lemme 8.3. *Soit $Q_1, ..., Q_n \in A$ des séries formelles avec un terme constant nul. Alors l'application définie par*

$$x_i \mapsto Q_i$$

est un morphisme d'anneau de A dans A.

Remarque 8.4. On a besoin de supposer que les Q_i ont un coefficient constant nul, sinon on ne définit pas un élément de A. Par exemple, si $A = \mathbf{Z}[[X]]$ et $f = 1 + X + X^2 + ...$, alors $f(1 + X)$ n'est pas défini car son terme constant serait $1 + 1 + ... + 1 + ...$

Démonstration. Soit $f = f_0 + f_1(\mathbf{X}) + f_2(\mathbf{X}) + ... \in A$ et $g = g_0 + g_1(\mathbf{X}) + g_2(\mathbf{X}) + ...$, avec f_i, g_i la composante homogène de degré i de f et g respectivement. Alors fg s'écrit

$$fg = h_0 + h_1(\mathbf{X}) + ...$$

avec $h_i = \sum_{k=0}^{i} f_i(\mathbf{X}) g_{k-i}(\mathbf{X})$. On voit alors que la substitution $x_i \mapsto Q_i$ définit bien un morphisme d'anneau. □

Lemme 8.5. *L'ensemble H des éléments x de A de la forme*

$$x = 1 + h(X_1, ..., X_n)$$

où le coefficient constant de $h \in A$ est nul est un groupe.

Démonstration. On le vérifie d'abord avec $h = X_1$. L'inverse de X_1 est $g = 1 + \sum_{i \geq 1} (-1)^i X_1^i \in H$. Maintenant, soit $h \in A$ de coefficient constant nul, on sait d'après le lemme 8.3 que l'application qui envoie X_1 sur h est un morphisme d'anneau . Donc $1 + h$ est bien inversible et son inverse est bien dans H. □

Lemme 8.6. *Le sous-groupe de H engendré par les $a_i := 1 + X_i$ est libre de rang n.*

Démonstration. Soit $m = a_{i_1}^{\alpha_1} \cdots a_{i_p}^{\alpha_p}$ un mot avec $i_k \neq i_{k+1}$ et $\alpha_k \neq 0$. Alors on écrit

$$a_{i_k}^{\alpha_k} = 1 + \alpha_k X_{i_k} + \text{ termes de plus haut degré .}$$

En particulier, le terme devant $X_{i_1} X_{i_2} \cdots X_{i_p}$ est $\alpha_1 \cdots \alpha_p$, ce coefficient est non nul et $m \neq 1$. □

Définition 8.7. Dans F_n, on définit la suite de sous-groupe $D_0 = F_n, D_{i+1} = [D_i, F_n]$.

Proposition 8.8. *Si on note H_r le sous-groupe de H des éléments de la forme*

$$x = 1 + h_r(X_1, ..., X_n)$$

où h_r est une série formelle dont tous les monômes de degré inférieur ou égal à r sont nuls. Alors H_r est un sous-groupe distingué de H isomorphe à D_r.

Démonstration. Voir [MKS04]. □

On voit donc maintenant que pour travailler dans F_n/D_r, il suffit de prendre les séries formelles et de calculer les coefficients devant les monômes de degré inférieur ou égal à r.

Calculons l'indice de résolubilité virtuel du groupe F_n/D_2.

Proposition 8.9. *On a*

$$\mathrm{vdl}(F_n/D_2) = 2.$$

Démonstration. Supposons que F_n/D_2 contienne un sous-groupe d'indice fini H abélien. Soit $a_1 = 1 + X_1, a_2 = 1 + X_2$ deux des n générateurs canoniques de F_n/D_2, alors il existe $N > 0$ tel que $a_1^N, a_2^N \in H$. Donc il devrait commuter ce qui est absurde car

$$(1 + X_1)^N (1 + X_2)^N = 1 + NX_1 + NX_2 + \binom{N}{2} X_1 + \binom{N}{2} X_2 + N^2 X_1 X_2$$
$$\text{et } (1 + X_2)^N (1 + X_1)^N = 1 + NX_1 + NX_2 + \binom{N}{2} X_1 + \binom{N}{2} X_2 + N^2 X_2 X_1$$

□

8.2.2 Optimalité du théorème pour F_2/D_2

On va d'abord regarder le cas $n = 2$ qui va nous permettre de faire des calculs simples pour comprendre s'il est possible que notre groupe $G = F_2/D_2$ ait une action sur un espace de dimension 2.

On note a et b les générateurs de G et on suppose que G agit sur une variété complexe de dimension 2. Par la proposition 7.12, G admet un sous-groupe d'indice fini G' qui est isomorphe à un sous-groupe de $\mathrm{Diff}_1^{an}(\mathcal{U})$ avec $\mathcal{U} = \mathbf{Z}_p^2$ pour un certain nombre premier $p \geq 3$. Il existe alors un entier N tel que a^N et b^N appartiennent à G'.

Dans la suite, pour simplifier les notations on remplace a par a^N et b par b^N. On note $\mathbf{X}_a$, $\mathbf{X}_b$ $\mathbf{X}_{a,b}$ les champs de vecteurs analytiques associés respectivement à a, b et $[a, b]$ le commutateur de a et b. (voir le corollaire (6.17). D'après la définition de G, on a que $[a, b]$ commutent avec a et b donc $\mathbf{X}_{a,b}$ commute avec $\mathbf{X}_a$ et $\mathbf{X}_b$.

Proposition 8.10. *Il existe un polydisque $\mathcal{V} \subset \mathcal{U}$ tel que sur $\mathcal{V}$,* $\dim \mathrm{Vect}(\mathbf{X}_a, \mathbf{X}_b, \mathbf{X}_{a,b}) = 2$.

Démonstration. Supposons le contraire, alors sur tout $\mathcal{U}$, $\dim \mathrm{Vect}(\mathbf{X}_a, \mathbf{X}_b, \mathbf{X}_{a,b}) \geq 1$ et on peut écrire $X_a = fX_{a,b}$ et $X_b = g\mathbf{X}_{a,b}$ avec f, g analytique sur $\mathcal{U}$. Mais alors $[\mathbf{X}_a, \mathbf{X}_{a,b}] = 0$ donne $\mathbf{X}_{a,b}(f) = 0$ et de même $\mathbf{X}_{a,b}(g) = 0$. Donc $[X_a, X_b] = 0$ mais c'est absurde car a et b ne commutent pas d'après la preuve de la proposition 8.9. □

On remplace alors $\mathcal{U}$ par un tel polydisque $\mathcal{V}$. On peut réduire encore $\mathcal{V}$ de sorte que $(\mathbf{X}_a, \mathbf{X}_{a,b})$ ou $(\mathbf{X}_b, \mathbf{X}_{a,b})$ soit libre. Supposons par exemple que l'on ait un petit polydisque $\mathcal{V}$ tel que $(\mathbf{X}_a, \mathbf{X}_{a,b})$ soit libre. Comme les deux champs commutent, il existe un changement de coordonnées analytique tel que $\mathbf{X}_a = \partial_x$ et $\mathbf{X}_{a,b} = \partial_y$. Comme $\mathbf{X}_{a,b}$ commute avec $\mathbf{X}_b$, on a alors

$$\mathbf{X}_b = f(x)\partial_x + g(x)\partial_y$$

avec $f, g : \mathbf{Z}_p \to \mathbf{Z}_p$ analytique. Lorsque l'on intègre les champs de vecteurs pour récupérer a, b et $[a, b]$ on obtient dans ces coordonnées que

$$\begin{aligned} a(x, y) &= (x + 1, y) \\ [a, b](x, y) &= (x, y + 1) \\ b(x, y) &= (F(x), G(x) + y) \end{aligned}$$

avec F, G analytiques. Comme b est un difféomorphisme analytique, on a que F en est un aussi et alors $b^{-1}(x, y) = (F^{-1}(x), y - G(F^{-1}(x))$. En prenant le commutateur, on obtient :

$$[a, b](x, y) = (x, y + 1) = (F(F^{-1}(x) - 1) + 1, y - G(F^{-1}(x)) + G(F^{-1}(x) - 1))$$

Ce qui nous donne deux équations

$$\begin{cases} F(F^{-1}(x) - 1) = x - 1 \\ G(F^{-1}(x) - 1) = G(F^{-1}(x)) + 1 \end{cases}$$

En remplaçant x par $F(z)$ (ce que l'on peut faire car F est un difféomorphisme analytique). On a

$$\begin{cases} F(z - 1) = F(z) - 1 \\ G(z - 1) = G(z) + 1 \end{cases}$$

Ce qui nous donne qu F est affine et G aussi. En allant au bout du calcul, on voit qu'il existe des constantes $A, B \in \mathbf{Z}_p$ telles que $F(x) = x + A$ et $G(x) = -x + B$. Finalement, on a

$$\begin{aligned} a(x, y) &= (x + 1, y) \\ b(x, y) &= (x + A, y - x + B) \end{aligned}$$

Si on revient sur $\mathbf{C}$, cela définit bien des automorphismes algébriques. De plus, on obtient bien une action de G sur $\mathbf{C}^2$:

Proposition 8.11. *Si $A, B \in \mathbf{C}$ sont des nombres complexes alors le sous-groupe de* $\mathrm{Aut}(\mathbf{A}^2_{\mathbf{C}})$ *engendré par $a(x, y) = (x + 1, y)$ et $b(x, y) = (x + A, y - x + B)$ est isomorphe à G.*

De plus, tout action de G sur $\mathbf{A}^2_{\mathbf{C}}$ est localement conjuguée à cette action.

La seconde assertion de la proposition découle de l'étude que nous venons de mener.

La preuve de ce fait est assez calculatoire et se fait en plusieurs étapes. Prenons $A, B \in \mathbf{C}$. On note H le groupe engendré par a et b. On a un morphisme surjectif $F_2 \twoheadrightarrow H$ donné par si s et t sont les deux générateurs canoniques de F_2, $s \mapsto a$ et $t \mapsto b$. Ensuite, tout élément f de H est une transformation de la forme $f(x,y) = (x + \gamma_f, y - m_f x + \tau_f)$, si on prend une autre transformation $g \in H$, on a

$$[f,g] = (x, y + \gamma_g(m_f - m_g))$$

qui commute bien avec a et b. Donc tout commutateur de H est dans le centre de H et on a bien un morphisme $G \twoheadrightarrow H$.

Pour montrer l'injectivité de ce morphisme on aura besoin des lemmes calculatoires suivants.

Dans la suite f désigne la fonction $f : \mathbf{Z} \to \mathbf{N}$ définie par $\forall N \in \mathbf{Z}, f(N) = \frac{N^2-N}{2}$.

Lemme 8.12. *Soit $N \in \mathbf{Z}$, alors*

$$a^N(x,y) = \big((x+N, y) \quad et \quad b^N(x,y) = (x + NA, y - Nx + NB - f(N)A\big)$$

Démonstration. Ceci se fait par récurrence. □

Lemme 8.13. *Soit $x_1, ...x_p \in \mathbf{Z}$, si on note $M = \sum_{i=1}^p x_i$, on a*

$$f(M) = \sum_{i=1}^{p} f(x_i) + \sum_{1 \le i < j \le p} x_i x_j$$

Démonstration. On a

$$\sum_{1 \le i < j \le p} x_i x_j = \frac{1}{2} \sum_{1 \le i \ne j \le p} x_i x_j = \frac{1}{2} \sum_{i=1}^{p} x_i (M - x_i) = \frac{M^2}{2} - \frac{1}{2} \sum_{i=1}^{p} x_i^2$$

Comme $f(x_i) = \frac{x_i^2 - x_i}{2}$, on obtient l'égalité. □

Lemme 8.14. *Soient $\alpha_1, ...\alpha_p, \beta_1, ..., \beta_p \in \mathbf{Z}$ des entiers, alors*

$$a^{\alpha_1} \circ b^{\beta_1} \circ \cdots \circ a^{\alpha_p} b^{\beta_p}(x,y) = \left(x + \left(\sum_{i=1}^{p} \alpha_i \right) + A \left(\sum_{i=1}^{p} \beta_i \right) ; y - x \left(\sum_{i=1}^{p} \beta_i \right) + B \left(\sum_{i=1}^{p} \beta_i \right) - A \left(f \left(\sum_{i=1}^{p} \beta_i \right) \right) - \left(\sum_{j=1}^{p} \sum_{i<j} \beta_j \alpha_i \right) \right)$$

Démonstration. Pour $p = 1$, on a

$$a^\alpha \circ b^\beta = x + \alpha + A\beta, y - \beta + \beta B - f(\beta)A$$

Donc la formule est vraie pour $p = 1$.

Maintenant, soit $g \in H$, alors g s'écrit

$$g(x,y) = (x + \theta, y + \tau x + \eta)$$

avec $\theta, \tau, \eta \in \mathbf{C}$. Soit $\alpha, \beta \in \mathbf{Z}$, on a alors

$$a^\alpha \circ b^\beta \circ g = (x + \theta + \alpha + A\beta, y + x(\tau - \beta) + \beta B - f(\beta)A - \beta\theta + \eta) \tag{4}$$

Prenons maintenant $g = a^{\alpha_2} \circ b^{\beta_2} \circ \cdots \circ a^{\alpha_p} b^{\beta_p}$. Par récurrence, on a alors

$$\begin{cases} \theta = \displaystyle\sum_{i=2}^{p} \alpha_i + A \sum_{j=2}^{p} \beta_j \\ \tau = -\displaystyle\sum_{i=2}^{p} \beta_i \\ \eta = B \displaystyle\sum_{j=2}^{p} \beta_j - A \left(f \left(\sum_{j=2}^{p} \beta_j \right) \right) - \sum_{j=2}^{p} \sum_{2 \le i < j} \beta_i \alpha_j \end{cases}$$

Ensuite, si on regarde l'équation (4), on a que $\theta + \alpha_1 + \beta_1 = \sum_{i=1}^{p} \alpha_i + A \sum_{j=1}^{p} \beta_j$. Ce qui nous donne la forme voulue pour la première coordonnée. Ensuite, $\tau - \beta_i = -\sum_{i=1}^{p} \beta_i$.

Enfin, $\beta_1\theta = \sum_{i=2}^{p} \beta_1\alpha_i + A \sum_{j=2}^{p} \beta_1\beta_j$. Donc on obtient

$$\beta_1 B - f(\beta_1)A - \beta_1\theta + \eta = B \sum_{j=1}^{p} \beta_j - A \left(f \left(\sum_{j=2}^{p} \beta_j \right) + \sum_{j=2}^{p} \beta_1\beta_j + f(\beta_1) \right) - \sum_{j=2}^{p} \left(\beta_1\alpha_j + \sum_{2 \le i < j} \beta_i\alpha_j \right)$$

Par le lemme 8.13, le coefficient devant A vaut

$$\sum_{j=2}^{p} \beta_j^2 + \sum_{2 \le i < j \le p} \beta_i\beta_j + \sum_{j=2}^{p} \beta_1\beta_j + f(\beta_1) = \sum_{j=1}^{p} f(\beta_j) + \sum_{1 \le i < j \le p} \beta_i\beta_j$$

qui vaut bien $f(\sum_{j=1}^{p} \beta_j)$ par le lemme 8.13.

Enfin le coefficient constant en regroupant tous les termes vaut bien

$$\sum_{j=1}^{p} \sum_{i<j} \beta_i\alpha_j.$$

La formule est donc vraie par récurrence.

□

Lemme 8.15. *Si on note s et t les deux générateurs de G avec $s = 1+X$ et $t = 1+Y$. Si $\alpha_1, \beta_1, ..., \alpha_p, \beta_p \in \mathbf{Z}$, on a*

$$s^{\alpha_1} t^{\beta_1} \cdots s^{\alpha_p} t^{\beta_p} = 1 + X \left(\sum_{i=1}^{p} \alpha_i \right) + Y \left(\sum_{i=1}^{p} \beta_i \right) + X^2 \left(f \left(\sum_{i=1}^{p} \alpha_i \right) \right) + Y^2 \left(f \left(\sum_{i=1}^{p} \beta_i \right) \right) + XY \left(\sum_{j=1}^{p} \sum_{i \ge j} \alpha_j\beta_i \right) + YX \left(\sum_{j=1}^{p} \sum_{i<j} \alpha_j\beta_i \right)$$

Démonstration. On montre d'abord par récurrence que

$$\forall N \in \mathbf{Z}, \quad s^N = 1 + NX + f(N)X^2, \quad t^N = 1 + NY + f(N)Y^2$$

La preuve est analogue au lemme précédent, on remarque que si m est un élément de G, alors

$$m = 1 + aX + bY + cX^2 + dY^2 + eXY + hYX$$

Maintenant, si $\alpha, \beta \in \mathbf{Z}$, alors

$$s^\alpha t^\beta m = 1 + X(a+\alpha) + Y(b+\beta) + X^2(c + f(\alpha) + \alpha a) + Y^2(d + f(\beta) + \beta b) + XY(e + \alpha\beta) + YX(h + \beta a)$$

En prenant pour $m = s^{\alpha_2} t^{\beta_2} \cdots s^{\alpha_p} t^{\beta_p}$ et en appliquant l'hypothèse de récurrence, le résultat découle en regardant chaque coefficient, les calculs sont les mêmes que pour la preuve du lemme 4. □

On peut maintenant démontrer le résultat.

Soient $\alpha_1, \beta_1, ..., \alpha_p, \beta_p \in \mathbf{Z}$ tels que $a^{\alpha_1} \circ b^{\beta_1} \circ \cdots \circ a^{\alpha_p} b^{\beta_p} = \mathrm{id}$. Par le lemme 8.14, en regardant le coefficient devant x dans la deuxième coordonnée on a que

$$\sum_{i=1}^{p} \beta_i = 0$$

En revenant maintenant à la première coordonnée cela nous donne que

$$\sum_{i=1}^{p} \alpha_i = 0$$

Enfin, le coefficient constant de la deuxième coordonnée doit être nul donc

$$\sum_{j=1}^{p} \sum_{i<j} \alpha_j \beta_i = 0.$$

Mais en faisant la somme avec $\sum_{j=1}^{p} \sum_{i \geq j} \alpha_j \beta_i$, on obtient :

$$\left(\sum_{j=1}^{p} \sum_{i<j} \alpha_j \beta_i \right) + \left(\sum_{j=1}^{p} \sum_{i \geq j} \alpha_j \beta_i \right) = \sum_{i,j=1}^{p} \alpha_i \beta_j = 0.$$

Donc il vient que

$$\sum_{j=1}^{p} \sum_{i \geq j} \alpha_j \beta_i = 0$$

Ainsi, par le lemme 8.15, on a que

$$s^{\alpha_1} t^{\beta_1} \cdots s^{\alpha_p} t^{\beta_p} = 1$$

dans G. Le morphisme $G \to H$ est bien injectif. C'est donc un isomorphisme et ceci conclut la preuve.

Cette méthode peut se généraliser avec un nombre quelconque de générateurs, ce qui donne le théorème suivant qui montre l'optimalité du théorème 7.25 pour les groupes F_n/D_2.

8.2.3 Optimalité du théorème pour F_n/D_2

Définition 8.16. Soit Λ un anneau, on définit le groupe $\mathrm{Tri}(n,\Lambda)$ des matrices triangulaires supérieures avec des 1 sur la diagonale

$$\mathrm{Tri}(n,\Lambda) = \left\{ \begin{pmatrix} 1 & & (*) \\ & \ddots & \\ (0) & & 1 \end{pmatrix} \in GL_n(\Lambda) \right\}.$$

Théorème 8.17. *Soit $n \geq 2$ un entier et $A_1, B_1, C_1 ..., A_n, B_n, C_n \in \mathbf{C}$ des nombres complexes tels que la famille $(A_1, .., A_n, B_1, ..., B_n)$ soit algébriquement indépendante sur $\mathbf{Q}$. Alors le groupe engendré par*

$$b_i(x,y) = (x + A_i, y + B_i x + C_i) \quad , \forall i = 1, ..., n$$

est isomorphe à F_n/D_2.

Remarque 8.18. Les transformations b_i correspondent à la matrice

$$\begin{pmatrix} 1 & B_i & C_i \\ 0 & 1 & A_i \\ 0 & 0 & 1 \end{pmatrix}$$

Ceci donne en fait le

Théorème 8.19. *Pour tout $n \geq 2$, il existe un plongement*

$$F_n/D_2 \hookrightarrow \mathrm{Tri}(3, \mathbf{R})$$

La preuve est similaire que celle du cas $n = 2$, les calculs demandent simplement plus d'effort. On note H le groupe engendré par les b_i et $G = F_n/D_2$.

Lemme 8.20. *Soit $N \in \mathbf{Z}$ et $i = 1, ..., n$, alors*

$$b_i^N(x,y) = (x + NA_i, y + NB_i x + NC_i + f(N)A_iB_i)$$

Démonstration. C'est une récurrence directe. □

Lemme 8.21. *Soient $\beta_1^1, ..., \beta_1^p, ..., \beta_n^1, ..., \beta_n^p \in \mathbf{Z}$, alors*

$$\begin{aligned} & b_1^{\beta_1^1} \circ \cdots \circ b_n^{\beta_n^1} \circ \cdots \circ b_1^{\beta_1^p} \circ \cdots \circ b_n^{\beta_n^p} = \\ & \left(x + \sum_{i=1}^{n} A_i \left(\sum_{k=1}^{p} \beta_i^k \right), y + x \left[\sum_{i=1}^{n} B_i \left(\sum_{k=1}^{p} \beta_i^k \right) \right] + \sum_{i=1}^{n} C_i \left(\sum_{k=1}^{p} \beta_i^k \right) \right. \\ & \left. + \sum_{1 \leq i \neq j \leq n} A_i B_j \left(\sum_{l=1}^{p} \sum_{k \leq l} \beta_i^l \beta_j^k \right) + \sum_{i=1}^{n} A_i B_i \left[f \left(\sum_{k=1}^{p} \beta_i^k \right) \right] \right) \end{aligned}$$

Démonstration. La preuve suit le même schéma que celle du lemme 4. Si g est un élément de H, alors g s'écrit

$$g(x,y) = x + \theta, y + \tau x + \eta.$$

Si $\beta_1, ..., \beta_n \in \mathbf{Z}$, alors

$$\begin{aligned} b_1^{\beta_1} \circ \cdots \circ b_n^{\beta_n} \circ g(x,y) = \\ \left(x + \theta + \sum_{i=1}^{n} \beta_i A_i; y + x(\tau + \sum_{i=1}^{n} \beta_i B_i) + \theta \sum_{i=1}^{n} \beta_i B_i + \sum_{j=1}^{n} A_j \left(\sum_{i<j} \beta_i B_i \right) \right. \\ \left. + \sum_{i=1}^{n} \beta_i C_i + \sum_{i=1}^{n} A_i B_i f(\beta_i) + \eta \right) \end{aligned} \tag{5}$$

Ce qui nous donne le résultat pour $p = 1$ avec $g = \mathrm{id}$ i.e $\theta = \eta = \tau = 0$.

Prenons maintenant, $g = b_1^{\beta_1^2} \circ \cdots b_n^{\beta_n^2} \circ \cdots \circ b_1^{\beta_1^p} \circ \cdots \circ b_n^{\beta_n^p}$, alors θ, τ et η valent par récurrence

$$\begin{cases} \theta = \sum_{i=1}^{n} A_i \left(\sum_{k=2}^{p} \beta_i^k \right) \\ \tau = \sum_{i=1}^{n} B_i \left(\sum_{k=2}^{p} \beta_i^k \right) \\ \eta = \sum_{i=1}^{n} C_i \left(\sum_{k=2}^{p} \beta_i^k \right) + \sum_{1 \le i \ne j \le n} A_i B_j \left(\sum_{l=2}^{p} \sum_{2 \le k \le l} \beta_i^l \beta_j^k \right) + \sum_{i=1}^{n} A_i B_i \left[f \left(\sum_{k=2}^{p} \beta_i^k \right) \right] \end{cases}$$

On compose g avec $b_1^{\beta_1^1} \circ \cdots \circ b_n^{\beta_n^1}$ et on utilise l'équation (5). Sur la première coordonnée, on a

$$\theta + \sum_{i=1}^{n} \beta_i^1 A_i = \sum_{i=1}^{n} \sum_{k=1}^{p} A_i \beta_i^k.$$

Ensuite, $\tau + \sum_{i=1}^{n} B_i \beta_i^1$ donne bien

$$\sum_{i=1}^{n} \sum_{k=1}^{p} B_i \beta_i^k.$$

Enfin,

$$\theta \sum_{i=1}^{n} \beta_i^1 B_i = \sum_{i,j=1}^{n} \sum_{k=2}^{p} \beta_j^k \beta_i^1 A_j B_i = \left(\sum_{1 \le i \ne j \le n} \sum_{k=2}^{p} \beta_j^k \beta_i^1 A_j B_i \right) + \sum_{i=1}^{n} \sum_{k=2}^{p} \beta_i^k \beta_i^1 A_i B_i$$

En sommant les coefficients constants sur la dernière coordonnée on obtient

$$\sum_{i=1}^{n} C_i \left(\sum_{k=1}^{p} \beta_i^k \right) + \sum_{1 \le i \ne j \le n} A_i B_j \left[\sum_{l=2}^{p} \beta_i^l \beta_j^1 + \sum_{2 \le k \le l} \beta_i^l \beta_j^k \right] + \sum_{i=1}^{n} A_i B_i \left(f(\beta_i) + \sum_{k=2}^{p} \beta_i^k \beta_i^1 + f \left(\sum_{l=2}^{p} \beta_i^l \right) \right)$$

Donc on obtient bien (même calcul que dans la preuve du lemme 8.14) que le coefficient constant de la deuxième coordonnée est

$$\sum_{i=1}^{n} C_i \left(\sum_{k=1}^{p} \beta_i^k \right) + \sum_{1 \leq i \neq j \leq n} A_i B_j \left(\sum_{l=1}^{p} \sum_{k \leq l} \beta_i^l \beta_j^k \right) + \sum_{i=1}^{n} A_i B_i \left[f \left(\sum_{k=1}^{p} \beta_i^k \right) \right].$$

Le résultat est donc vrai par récurrence. □

Lemme 8.22. *Si on note $t_1, ..., t_n$ les générateurs de F_n/D_2 tels que $t_i = 1 + y_i$. Soient $\beta_1^1, ..., \beta_1^p$, $..., \beta_n^1, ..., \beta_n^p \in \mathbf{Z}$, alors*

$$\begin{aligned} & t_1^{\beta_1^1} t_n^{\beta_n^1} \cdots t_1^{\beta_1^p} \cdots t_n^{\beta_n^p} = \\ & 1 + \sum_{i=1}^{n} y_i \left(\sum_{k=1}^{p} \beta_i^k \right) + \sum_{i=1}^{n} y_i^2 \left(f \left(\sum_{k=1}^{p} \beta_i^k \right) \right) \\ & + \sum_{1 \leq i < j \leq n} \left[y_i y_j \left(\sum_{k=1}^{p} \sum_{l \leq k} \beta_j^k \beta_i^l \right) + y_j y_i \left(\sum_{k=1}^{p} \sum_{l > k} \beta_j^k \beta_i^l \right) \right] \end{aligned}$$

Démonstration. Là aussi, la preuve se fait par récurrence et suit le même schéma que la preuve du lemme 8.15. On remarque d'abord que si $m \in G$ s'écrit

$$m = 1 + \sum_{i=1}^{n} a_i y_i + \sum_{i=1}^{n} b_i y_i^2 + \sum_{1 \leq i < j \leq n} c_{ij} y_i y_j + d_{ij} y_j y_i$$

alors soit $\beta_1, ..., \beta_p \in \mathbf{Z}$, on a

$$\begin{aligned} & b_1^{\beta_1} \cdots b_n^{\beta_n} m = \\ & 1 + \sum_{i=1}^{n} y_i \left(a_i + \sum_{i=1}^{n} \beta_i \right) + \sum_{i=1}^{n} y_i^2 \left(b_i + f(\beta_i) + \beta_i a_i \right) \\ & + \sum_{1 \leq i < j \leq n} \left[y_i y_j \left(c_{ij} + \beta_i \beta_j + \beta_i a_j \right) + y_j y_i \left(d_{ij} + \beta_j a_i \right) \right] \end{aligned}$$

Ce qui permet d'initialiser la récurrence avec $a_i = b_i = c_{ij} = d_{ij} = 0$ et de faire l'hérédité en prenant $m = y_1^{\beta_1^2} \cdots y_n^{\beta_n^2} \cdots y_1^{\beta_1^p} \cdots y_n^{\beta_n^p}$. □

On conclut maintenant aisément la preuve, On note H le groupe engendré par $a, b_1, ..., b_n$. Comme dans le cas $n = 2$ (le calcul est exactement le même) tous les commutateurs sont dans le centre de H donc on a un morphisme surjectif $F_n/D_2 \twoheadrightarrow H$.

Maintenant, si un mot $m = t_1^{\beta_1^1} t_n^{\beta_n^1} \cdots t_1^{\beta_1^p} \cdots t_n^{\beta_n^p}$ est tel que

$$b_1^{\beta_1^1} \circ \cdots \circ b_n^{\beta_n^1} \circ \cdots \circ b_1^{\beta_1^p} \circ \cdots \circ b_n^{\beta_n^p} = \mathrm{id}$$

Alors en regardant la première coordonnée et par indépendance sur $\mathbf{Q}$ des A_i, on a

$$\sum_{k=1}^{p} \beta_i^k = 0, \quad \forall i = 1, ..., n$$

ce qui annule le coefficient devant y_i et y_i^2 de m.

Maintenant, en regardant la seconde coordonnée, on voit que le terme devant A_iB_j pour $i<j$ donne

$$\sum_{l=1}^{p}\sum_{k\leq l}\beta_i^l\beta_j^k=0$$

donc le coefficient de m devant y_iy_j est nul et en sommant le coefficient devant y_iy_j et celui devant y_jy_i on obtient

$$\sum_{k=1}^{p}\sum_{l=1}^{p}\beta_j^k\beta_i^l=0.$$

Donc le coefficient devant y_jy_i est lui aussi nul. On obtient donc que $m=0$ est le morphisme $F_n/D_2\to H$ est bien injectif.

Au vu de la preuve, on conjecture que ce fait est vrai pour tout $r\geq 2$.

Conjecture 8.23. *Soient $n\geq 1, r\geq 1$ des entiers, alors le groupe F_n/D_r se plonge dans le groupe* $\mathrm{Tri}(r+1,\mathbf{R})$.

Cette conjecture est démontrée en annexe pour $r=3$.

8.3 Un contre-exemple

Nous allons montrer qu'il existe des groupes H nilpotents, de type fini et sans torsion, avec $\mathrm{dl}(H)=\mathrm{vdl}(H)$ tel que la borne du théorème 7.25 ne soit pas optimale.

Considérons le groupe $T=\mathrm{Tri}(3,\mathbf{Z})=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\;\middle|\; a,b,c\in\mathbf{Z}\right\}$. On note

$$A_1=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\quad A_2=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\quad A_3=\begin{pmatrix}1&0&1\\0&0&0\\0&0&1\end{pmatrix}$$

les générateurs de T, en particulier $[A_1,A_2]=A_3$.

T est nilpotent et son indice de nilpotence est 2, tout comme son indice de résolubilité. On a en fait le

Lemme 8.24. *On a*

$$\mathrm{vdl}(T)=2.$$

Démonstration. Supposons que T admette un sous-groupe abélien d'indice fini K. Alors il existe $N>0$ tel que $A_1^N, A_2^N\in K$ mais alors A^N et B^N doivent commuter ce qui est absurde. □

Nous allons montrer que le groupe $H:=T\times T$ n'agit pas fidèlement en dimension 2. Il est aussi nilpotent d'indice 2 et son indice de nilpotence virtuel est aussi 2 par le lemme précédent. On note $T_1=T\times\{1\}$ et $T_2=\{1\}\times T_2$. On note $A_i^j(i=1,2,3)$ les trois générateurs de T_j. En particulier C_1 et C_2 engendrent le centre de H.

Supposons qu'il existe une variété quasi-projective X tel que H agisse fidèlement sur X. Alors par les propositions 7.6 et 7.12, il existe un nombre premier p et un sous-groupe d'indice fini $H'\subset H$ tel que $H'\subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p^2)$. Alors il existe $N>0$ tel que pour $i=1,2, j=1,2,3, (A_i^j)^N\in H'$. Dans la suite,

on remplace A_i^j par leur puissance et on note $\mathbf{X}_i^j$ le champ de vecteurs analytiques associé à A_i^j. On peut trouver un polydisque $\mathcal{U}$ tel que les 6 champs de vecteurs $\mathbf{X}_i^j, (i = 1, 2, j = 1, 2, 3)$ ne s'annulent pas sur $\mathcal{U}$. En particulier, le champ de vecteur $\mathbf{X}_1^3$ commute avec tous les autres. Maintenant, on a que sur $\mathcal{U}$ un des champs de vecteurs parmi $\mathbf{X}_1^1, \mathbf{X}_1^2, \mathbf{X}_2^1, \mathbf{X}_2^2$ n'appartient pas à la droite engendrée par $\mathbf{X}_1^3$, sinon ces 4 champs de vecteurs s'écriraient $\mathbf{X}_i^j = f_i^j \mathbf{X}_1^3$ avec $\mathbf{X}_1^3(f_i^j) = 0$ et donc commuteraient entre eux et les éléments A_1^i, A_2^i commuteraient aussi entre eux ce qui est absurde. Ainsi, on peut trouver un plus petit polydisque $\mathcal{V} \subset \mathcal{U}$ tel que sur $\mathcal{V}$, $\mathbf{X}_i^j$ et $\mathbf{X}_1^3$ forment une base de l'espace tangent pour un certain couple $(i, j) \in \{1, 2\}^2$. Comme ces deux champs de vecteurs commutent entre eux, il existe un redressement tel que $\mathbf{X}_i^j = \partial_x$ et $\mathbf{X}_1^3 = \partial_y$. Maintenant, si on note i' l'élément de $\{1, 2\}$ différent de i, on a alors, comme $A_{i'}^1$ et $A_{i'}^2$ commute avec A_i^j, que

$$\mathbf{X}_{i'}^1 = \alpha\partial_x + \beta\partial_y$$
$$\mathbf{X}_{i'}^2 = \gamma\partial_x + \delta\partial_y$$

avec $\alpha, \beta, \gamma, \delta \in \mathbf{Z}_p$ sur $\mathcal{V}$. Mais alors $\mathbf{X}_{i'}^1$ et $\mathbf{X}_{i'}^2$ commutent et donc par le corollaire 6.17, $A_{i'}^1$ et $A_{i'}^2$ commutent ce qui est absurde.

La preuve peut se faire en fait avec tous les groupes F_n/D_2. On a alors le

Théorème 8.25. *Pour tout $n \geq 2$, le groupe $F_n/D_2 \times F_n/D_2$ est un groupe nilpotent d'indice de résolubilité virtuel égal à 2 mais qui n'agit pas de manière fidèle sur une variété algébrique complexe de dimension 2.*

Démonstration. On note $H = F_n/D_2 \times F_n/D_2$, On note $H_1 = F_n/D_2 \times \{1\}$ et $H_2 = \{1\} \times F_n/D_2$. Supposons que H agisse sur une variété complexe de dimension 2. On note a_1, a_2 deux des n générateurs canoniques de F_n/D_2, le groupe engendré par a_1, a_2 est alors isomorphe à F_2/D_2. Par la remarque 8.18 et le théorème 8.17 il existe un plongement tel que a_1 s'envoie sur $A_1 \in \mathrm{Tri}(3)$ et a_2 sur $A_2 \in \mathrm{Tri}(3)$ (l'indépendance algébrique des coefficients n'est pas nécessaire pour le cas $n = 2$ d'après la proposition 8.11). Alors par ce plongement on aurait que $T \times T$ agit de manière fidèle sur une variété algébrique complexe de dimension 2 ce qui est absurde. □

Cinquième partie
Questions en suspens

9 Borne de Minkowski pour un corps de nombre

Dans [Ser07], Serre montre comment Schur généralise le théorème de Minkowski pour les sous-groupes finis de $GL_d(k)$ avec k un corps de nombre, i.e une extension finie de $\mathbf{Q}$. La question est de savoir si cette borne généralisée est aussi vraie pour les sous-groupes finis de $\mathrm{Aut}_k(\mathbf{A}^d)$.

Définition 9.1. Soit k un corps de nombre. On note z_a une racine primitive a-ième de l'unité ($a \geq 1$). On définit $t = [k(z_p) : k]$ et m l'entier maximal tel que $k(z_p)$ contient z_{p^m}. On définit alors

$$M_k(d, p) = m \times \left(\left\lfloor \frac{d}{t} \right\rfloor + \left\lfloor \frac{n}{pt} \right\rfloor + \left\lfloor \frac{d}{p^2 t} \right\rfloor + ... \right)$$

Théorème 9.2 (Schur, voir [Ser07], 2.2)**.** *Soit G un sous-groupe fini de $GL_d(\mathbf{C})$ tels que pour tout $g \in G, \mathrm{Tr}\, g \in k$, alors*

$$v_p(|G|) \leq M_k(d, p).$$

Remarque 9.3. Si $k = \mathbf{Q}$, alors $M_{\mathbf{Q}}(d,p) = M(d,p)$ et on retrouve le théorème de Minkowski.

Considérons G un sous-groupe fini de $\mathrm{Aut}_{\mathbf{C}}(\mathbf{A}^d)$, alors l'action de G est défini sur un corps de nombres k car G est fini. On a de plus par le théorème 3.1 que G admet un point fixe $x_0 \in \mathbf{A}^d(\overline{\mathbf{Q}})$. Maintenant, prenons $L := k(x_0)$, le corps engendré par les coordonnées de x_0 sur k. L est un corps de nombre et le morphisme de groupes $g \in G \mapsto D_{x_0}g$ est injectif par le même argument que celui de la preuve du théorème 5.2. Ainsi, G est isomorphe à un p-sous-groupe de $GL_d(L)$ et donc par le théorème de Schur

$$v_p(|G|) \leq M_L(d,p).$$

Mais ce n'est pas satisfaisant car on n'a pas de contrôle sur L étant donné que l'on n'a pas d'information sur le point fixe $x_0 \in \mathbf{A}^d(\overline{\mathbf{Q}})$.

10 Borne de Minkowski pour une variété autre que l'espace affine

Une question naturelle après avoir démontré le théorème 5.1 est de se demander si l'on peut avoir un énoncé similaire lorsque l'on ne considère plus le groupe d'automorphisme de l'espace affine mais celui d'une variété algébrique quelconque.

On ne peut pas espérer borner la taille des sous-groupes finis par une fonction de la dimension car on a le résultat suivant.

Théorème 10.1 (Hurwitz, voir [Hur92])**.** *Tout groupe fini agit fidèlement par isométrie sur une surface de Riemann de genre $g \geq 2$*

Mais on peut s'intéresser par exemple au cas de la quadrique

$$Q = \left\{ (x_1, ..., x_n) \in \mathbf{C}^n \;\middle|\; \sum_{i=1}^{n} |x_i|^2 = 1 \right\}$$

Si G est un p-sous-groupe de $\mathrm{Aut}_{\mathbf{Q}}(Q)$. On a évidemment $v_p(G) \leq M(n,p)$ et on voudrait voir si on peut améliorer cette inégalité. On aurait envie de passer dans un corps fini $\mathbf{F}_l$ avec l différent de p car on a le lemme :

Lemme 10.2. *On peut trouver un nombre premier $l \neq p$ tel que le cardinal de*

$$Q_l = \left\{ (x_1, ..., x_n) \in (\mathbf{F}_l)^n \;\middle|\; \sum x_i^2 = 1 \right\}$$

ne soit pas divisible par p.

Démonstration. Voir [Gro02], proposition 9.10. □

Si G stabilisait Q_l, on aurait l'existence d'un point fixe x_0 dans Q_l et alors on aurait un morphisme de groupe injectif $g \in G \mapsto D_{x_0}g \in GL(T_{x_0}(Q_l)) = GL_{n-1}(\mathbf{Q})$. De sorte que $v_p(G) \leq M(n-1,p)$. Mais il n'est pas clair à priori que G stabilise Q_l.

En revanche, si G est orthogonal, au sens où si B est le produit scalaire $B(x,y) = \sum_i x_i y_i$ tel que $B(gx, gy) = B(x,y)$, alors l'étude que nous venons de mener fonctionne, G stabilise bien Q_l et on a $v_p(|G|) \leq M(n-1,p)$.

11 Amélioration de la borne pour les groupes F_n/D_r

Dans la partie 8, l'étude du cas $n = r = 2$ montre que le théorème 7.25 est optimal. La conjecture 8.23 donnerait une action de F_n/D_r en dimension r. Et l'étude des cas $r = 2, r = 3$ nous pousse à conjecturer le fait suivant :

Conjecture 11.1. *Soient $n \geq 2, r \geq 1$, alors si F_n/D_r agit sur une variété quasi-projective de dimension d, on a*

$$d \geq r$$

On aurait donc une minoration de la dimension de l'action par l'indice de nilpotence virtuel et non pas l'indice de résolubilité virtuel pour ces groupes. Pour montrer ce résultat, il faudrait prendre une action de $G := F_n/D_r$ sur une variété X de dimension $r' < r$ et montrer en utilisant les champs de vecteurs associés aux éléments de G qu'une dimension trop petite force le groupe à avoir des relations que G n'admet pas comme on l'a fait dans le cas $r = 2$. Cependant même pour $r = 3$, les calculs deviennent assez complexes.

Remarque 11.2. Segal montre dans son livre *Polycyclic groups* ([Seg05], partie 5) que tout groupe nilpotent de type fini sans torsion se plonge dans un groupe $\mathrm{Tri}(n, \mathbf{Z})$ pour n assez grand. Donc tous les groupes F_n/D_r admettent une action fidèle sur une variété quasi-projective complexe et il fait sens de regarder la dimension minimale pour laquelle une telle action existe.

12 Le groupe modulaire

On peut appliquer la méthode p-adique au groupe modulaire de la surface de genre g. Dans [CX14], il est prouvé (théorème 6.3) que si $\mathrm{Mod}(S_g)$ agit de façon fidèle sur une variété quasi-projective complexe de dimension d, alors $d \geq 2g - 1$. Par manque de temps, je n'ai pas pu voir si l'on pouvait améliorer cette borne en reprenant la preuve de l'article.

Sixième partie
Annexe

13 Le Cas F_n/D_3

Nous allons montrer que l'étude que l'on a mené en dimension 2 peut se faire aussi en dimension 3. On veut tout d'abord montrer le résultat suivant :

Proposition 13.1. *Pour tout $n \geq 3$, F_n/D_3 se plonge dans* $\mathrm{Tri}(4, \mathbf{R})$.

Nous allons expliciter le plongement.

Proposition 13.2. *Soient $A_i, B_i, C_i, D_i, E_i, F_i (1 \leq i \leq n) \in \mathbf{R}$ des réels algébriquement indépendants. Alors le sous-groupe de* $\mathrm{Tri}(4, \mathbf{R})$ *engendré par les matrices*

$$M_i = \begin{pmatrix} 1 & D_i & E_i & F_i \\ 0 & 1 & B_i & C_i \\ 0 & 0 & 1 & A_i \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

est isomorphe à F_n/D_3.

La démonstration se fait en plusieurs étapes. On va calculer tout d'abord les puissances de M_i :

Lemme 13.3. *Soit $N \in \mathbf{Z}$, alors*

$$M_i^N = \begin{pmatrix} 1 & ND_i & NE_i + \binom{N}{2} D_iB_i & NF_i + \binom{N}{2} E_iA_i + \binom{N}{2} D_iC_i + \binom{N}{3} D_iB_iA_i \\ 0 & 1 & NB_i & NC_i + \binom{N}{2} B_iA_i \\ 0 & 0 & 1 & NA_i \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Démonstration. En notant M_i sous la forme

$$M_i = \begin{pmatrix} 1 & * \\ 0 & M_i' \end{pmatrix} = \begin{pmatrix} M_i'' & * \\ 0 & 1 \end{pmatrix}$$

Avec M_i', M_i'' de taille 3×3, on voit que l'on peut déduire tous les coefficients du cas $r = 2$ sauf pour le coefficient en position $(1, 4)$.

Pour ce dernier, une récurrence donne le résultat. □

Lemme 13.4. *Soient $\alpha_1, ..., \alpha_n \in \mathbf{Z}$, alors le coefficient en position $(1, 4)$ de $M_1^{\alpha_1} \cdots M_n^{\alpha_n}$ est*

$$\sum_{i=1}^{n} \alpha_i F_i + \sum_{i=1}^{n} \binom{\alpha_i}{2} (D_iC_i + E_iA_i) + \sum_{1 \le i < j \le n} \alpha_i\alpha_j (E_iA_j + D_iC_j) + \sum_{1 \le i < j < k \le n} \alpha_i\alpha_j\alpha_k D_iB_jA_k +$$
$$+ \sum_{1 \le i < j \le n} \binom{\alpha_i}{2} \alpha_j D_iB_iA_j + \sum_{1 \le i < j \le n} \alpha_i \binom{\alpha_j}{2} D_iB_jA_j + \sum_{i=1}^{n} \binom{\alpha_i}{3} D_iB_iA_i$$

Démonstration. On procède par récurrence n. Le cas $n = 1$ vient du lemme précédent. Les autres coefficients de la matrice sont calculables par le cas $r = 2$, en décomposant M_i sous la même forme que dans le lemme précédent. □

On procède maintenant au calcul général de notre matrice :

Lemme 13.5. *Soient $\alpha_1^1, ..., \alpha_n^p, ..., \alpha_1^p, ..., \alpha_n^p$ des entiers relatifs, alors le dernier coefficient de la matrice $M_1^{\alpha_1^1} \cdots M_n^{\alpha_n^1} \cdots M_1^{\alpha_1^p} \cdots M_n^{\alpha_n^p}$ est*

$$\text{terme de degré inférieur à 2} + \sum_{(1,1) \le (s,i) < (t,j) < (u,k) \le (p,n)} \alpha_i^s \alpha_j^t \alpha_k^u D_iB_jA_k$$
$$+ \sum_{(1,1) \le (s,i) < (t,j) \le (p,n)} \binom{\alpha_i^s}{2} \alpha_j^t D_iB_iA_j + \sum_{(1,1) \le (s,i) < (t,j) \le (p,n)} \alpha_i^s \binom{\alpha_j^t}{2} D_iB_jA_j + \sum_{i=1}^{n} D_iB_iA_i \left(\sum_{k=1}^{p} \binom{\alpha_i^k}{3} \right)$$

où $(a, b) < (c, d)$ correspond à l'ordre lexicographique.

Démonstration. La preuve se fait par récurrence sur p, sachant que le lemme précédent donne le résultat pour $p = 1$. Les autres coefficients de la matrice ont été calculés lors du cas $r = 2$. □

Il ne reste maintenant plus qu'à faire le même calcul dans F_n/D_3.

Lemme 13.6. *Si on note $a_i = 1 + X_i$ les générateurs canoniques de F_n/D_3, on a alors si $\alpha_i^k \in \mathbf{Z}(1 \leq i \leq n, 1 \leq k \leq p)$ que*

$$a_1^{\alpha_1^1} \cdots a_n^{\alpha_n^1} \cdots a_1^{\alpha_1^p} \cdots a_n^{\alpha_n^p} =$$

$$1 + h_2(X_1, ..., X_n) + \sum_{1 \leq i < j < k} \left\{ X_i X_j X_k \left(\sum_{1 \leq s \leq t \leq u} \alpha_i^s \alpha_j^t \alpha_k^u \right) + X_i X_k X_j \left(\sum_{1 \leq s \leq u < t \leq p} \alpha_i^s \alpha_k^u \alpha_j^t \right) \right.$$

$$+ X_j X_i X_k \left(\sum_{1 \leq t < s \leq u \leq p} \alpha_j^t \alpha_i^s \alpha_k^u \right) + X_k X_j X_i \left(\sum_{1 \leq u < t < s} \alpha_k^u \alpha_j^t \alpha_i^s \right) + X_j X_k X_i \left(\sum_{1 \leq t \leq u < i \leq n} \alpha_j^t \alpha_k^u \alpha_i^s \right) +$$

$$\left. + X_k X_i X_j \left(\sum_{1 \leq u < s \leq t \leq n} \alpha_k^u \alpha_i^s \alpha_j^t \right) \right\} + \sum_{1 \leq i < j \leq n} \left[X_i^2 X_j \left(\sum_{1 \leq s \leq t \leq p} \binom{\alpha_i^s}{2} \alpha_j^t \right) + X_j X_i^2 \left(\sum_{1 \leq t < s \leq p} \alpha_j^t \binom{\alpha_i^s}{2} \right) + \right.$$

$$\left. + X_i X_j^2 \left(\sum_{1 \leq i \leq j \leq t} \alpha_i^s \binom{\alpha_j^t}{2} \right) + X_j^2 X_i \left(\sum_{1 \leq t < s \leq p} \binom{\alpha_j^t}{2} \alpha_i^s \right) \right] + \sum_{i=1}^{n} X_i^3 \left(\sum_{k=1}^{p} \binom{\alpha_i^k}{3} \right)$$

où h_2 est un polynôme de degré inférieur ou égal à 2 à coefficient constant nul.

Démonstration. On prouve ce lemme par récurrence sur p. □

On peut maintenant montrer le résultat. On note H le groupe engendré par les matrices M_i. Comme H a n générateurs et a un indice de nilpotence égal à 3, il existe une unique morphisme de groupes surjectif $F_n/D_3 \twoheadrightarrow H$ qui envoie a_i sur M_i.

Soit $m = a_1^{\alpha_1^1} \cdots a_n^{\alpha_n^1} \cdots a_1^{\alpha_1^p} \cdots a_n^{\alpha_n^p}$ est dans le noyau de ce morphisme. En décomposant chaque matrice M_i sous la forme $\begin{pmatrix} 1 & * \\ 0 & N_i \end{pmatrix}$ avec N_i de taille 3×3. On a un morphisme de groupes injectif $H' \hookrightarrow H$ où H' est le sous-groupe de $\mathrm{Tri}(3, \mathbf{R})$ engendré par les N_i, donné par $N_i \mapsto M_i$. En considérant le morphisme injectif $F_n/D_3 \twoheadrightarrow F_n/D_2$ donné par $F_n/D_2 \simeq (F_n/D_3)/(D_3/D_2)$. Le morphisme $F_n/D_2 \to H'$ donné par $a_i \mapsto N_i$ est un isomorphisme par le cas $r = 2$ et on a le diagramme commutatif suivant :

$$F_n/D_3 \twoheadrightarrow F_n/D_2 \xrightarrow{\sim} H' \hookrightarrow H$$

Donc si m est dans le noyau du morphisme $\varphi : F_n/D_3 \to H$, alors m est nul modulo D_2, donc n'a pas de termes de degré inférieur ou égal à 2.

Il faut donc calculer les coefficients devant les monômes de degré 3 de m. Mais on voit par l'indépendance algébrique des coefficients et les calculs des lemmes 13.5 et 13.6 que ce sont les même coefficients qui apparaissent dans l'expression de m et dans celle de $\varphi(m)$. Donc m est nul et φ est bien injectif.

14 Esquisse du Cas général F_n/D_r

On écrit ici comment la preuve pour le cas r quelconque devrait se faire en s'inspirant de celle du cas $r = 3$. On veut montrer le résultat suivant :

Proposition 14.1. *Soient* $(M_{i,j}^t)_{\substack{2\leq i\leq r+1\\ 1\leq j<i}}^{1\leq t\leq n}$ *des nombres réels algébriquement indépendants. On note* M_t *la matrice*

$$M_t := \begin{pmatrix} 1 & & & (M_{i,j}^t) \\ & 1 & & \\ & & 1 & \\ (0) & & & 1 \end{pmatrix} \in \mathrm{Tri}(r+1, \mathbf{R})$$

Alors le groupe engendré par M_t *pour* $t = 1, ..., n$ *est isomorphe à* F_n/D_r.

Esquisse de preuve. On procède par récurrence sur r.

On procède par récurrence sur r. Pour $r = 2$, c'est le théorème 8.17 et la remarque 8.18. Notons H le groupe engendré par les matrices M_t. Chaque matrice M_t s'écrit sous la forme

$$M_t = \begin{pmatrix} 1 & * \\ 0 & N_t \end{pmatrix}$$

avec $N_t \in \mathrm{Tri}(r, \mathbf{R})$. On définit H' le sous-groupe de $\mathrm{Tri}(r, \mathbf{R})$ engendré par les N_i. Si on prend le morphisme de groupe F_n/D_{r-1} qui à chaque générateur canonique $b_i = 1 + X_i \in F_n/D_{r-1}$ associe N_i, sachant que F_n/D_{r-1} est isomorphe à $(F_n/D_r)/(D_{r-1}/D_r)$, on a alors un diagramme commutatif :

$$F_n/D_r \twoheadrightarrow F_n/D_{r-1} \xrightarrow{\sim} H' \hookrightarrow H$$

avec $H' \hookrightarrow H$ le morphisme injectif qui envoie N_t sur M_t.

Soit $x \in F_n/D_r$ qui a une image trivial dans H, l'image de x dans F_n/D_{r-1} est nulle par le diagramme précédent. Donc x n'a que des termes de degré r.

Il faut maintenant montrer que les termes d'ordre r sont aussi nuls. L'idée est de calculer les coefficients de x devant les monômes de degré r et les termes de degré r du coefficient $(1, r+1)$ de la matrice image de x dans H. En s'inspirant de la preuve des lemmes 13.6 et 13.5, montrer que ceux sont les mêmes coefficients qui apparaissent et conclure par indépendance algébrique des coefficients des matrices M_i.

□

.

La difficulté réside dans le fait qu'il faut compter toutes les manières de former des monômes de degré r avec n variables non commutatives. Pour cela, on va avoir besoin de la notion de partition.

Définition 14.2. Soit n un entier naturel, une *partition* de n est la donnée d'un uplet d'entiers naturels $(x_1, ..., x_u) \in (\mathbf{N}^*)^u$ tel que $x_1 + .. + x_u = n$.

On dit que u est la longueur de la partition. On note $\mathcal{P}(n)$ l'ensemble des partitions de n et $\mathcal{P}_u(n)$ l'ensemble des partitions de longueur égale à u.

On montre le lemme suivant :

Lemme 14.3. *Soient* $s_i = 1 + X_i, (i = 1, ..., r)$ *les générateurs de* F_n/D_r. *Alors soient* $\beta_1^1, ..., \beta_1^p$, $\beta_2^1, ..., \beta_2^p, ...,\ \beta_n^1, ..., \beta_n^p$ *des entiers. On a*

$$s_1^{\beta_1^1} \cdots s_n^{\beta_n^1} \cdots s_1^{\beta_1^p} \cdots s_n^{\beta_n^p} =$$
$$1 + \sum_{t=1}^{r} \sum_{u=1}^{t} \sum_{(v_1,...,v_u)\in\mathcal{P}_u(t)} \sum_{1\leq i_1,i_2,\cdots,i_u\leq n} X_{i_1}^{v_1} \cdots X_{i_u}^{v_u} \left(\sum_{1\leq k_1,...,k_u\leq p | (k_1,i_1)<\cdots<(k_u,i_u)} \binom{\beta_{i_1}^{k_1}}{v_1} \cdots \binom{\beta_{i_u}^{k_u}}{v_u} \right)$$

Démonstration. On prouve cette formule par récurrence sur p. L'idée est simple même si la formule peut paraître déplaisante.

Si $p = 1$, alors

$$s_1^{\beta_1} \cdots s_n^{\beta_n} = \sum_{t_1,\ldots,t_n=0}^{r} \binom{\beta_1}{t_1} \cdots \binom{\beta_n}{t_n} X_1^{t_1} \cdots X_n^{t_n}$$

En regroupant les termes, et en ne gardant que les monômes de degré $\leq r$, on obtient la forme voulue pour $p = 1$.

Supposons la formule vraie pour $p-1$. On a alors par récurrence et le cas $p = 1$:

$$\begin{aligned}
&s_1^{\beta_1^1} \cdots s_n^{\beta_n^1} \cdots s_1^{\beta_1^p} \cdots s_n^{\beta_n^p} = \\
&\left(1 + \sum_{\tau=1}^{r} \sum_{\mu=1}^{\tau} \sum_{w_1,\ldots,w_\mu \in \mathcal{P}_\mu(\tau)} \sum_{1 \leq j_1, j_2, \ldots, j_\mu \leq n} X_{j_1}^{w_1} \cdots X_{j_\mu}^{w_\mu} \binom{\beta_{j_1}^1}{w_1} \cdots \binom{\beta {j_\mu}^1}{w_\mu}\right) \\
&\times \left[1 + \sum_{t=1}^{r} \sum_{u=1}^{t} \sum_{(v_1,\ldots,v_u) \in \mathcal{P}_u(t)} \sum_{1 \leq i_1, i_2, \cdots, i_u \leq n} X_{i_1}^{v_1} \cdots X_{i_u}^{v_u} \left(\sum_{2 \leq k_1, \ldots, k_u \leq p | (k_1, i_1) < \cdots < (k_u, i_u)} \binom{\beta_{i_1}^{k_1}}{v_1} \cdots \binom{\beta_{i_u}^{k_u}}{v_u} \right)\right] \\
&= 1 + \sum_{t,\tau=1}^{r} \sum_{u,\mu=1}^{r} \sum_{\substack{(w_1,\ldots,w_\mu,v_1,\ldots,v_u) \\ \in \mathcal{P}_{u+\mu}(t+\tau)}} \sum_{\substack{1 \leq j_1,\ldots,j_\mu \leq n \\ 1 \leq i_1,\ldots,i_u \leq n}} X_{j_1}^{w_1} \cdots X_{j_\mu}^{w_\mu} X_{i_1}^{v_1} \cdots X_{i_u}^{v_u} \times \\
&\qquad \times \left(\sum_{\substack{2 \leq k_1,\ldots,k_u \leq p | \\ (1,j_1) < \ldots < (1,j_\mu) < \\ (k_1,i_1) < \ldots < (k_u,i_u)}} \binom{\beta_{j_1}^1}{w_1} \cdots \binom{\beta_{j_\mu}}{w_\mu} \binom{\beta_{i_1}^{k_1}}{v_1} \cdots \binom{\beta_{i_u}}{v_u} \right) \\
&+ \sum_{t=1}^{r} \sum_{u=1}^{t} \sum_{(v_1,\ldots,v_u) \in \mathcal{P}_u(t)} \sum_{1 \leq i_1, i_2, \cdots, i_u \leq n} X_{i_1}^{v_1} \cdots X_{i_u}^{v_u} \left(\sum_{\substack{2 \leq k_1,\ldots,k_u \leq p | \\ (k_1,i_1) < \cdots < (k_u,i_u)}} \binom{\beta_{i_1}^{k_1}}{v_1} \cdots \binom{\beta_{i_u}^{k_u}}{v_u} \right) \\
&+ \sum_{\tau=1}^{r} \sum_{\mu=1}^{\tau} \sum_{w_1,\ldots,w_\mu \in \mathcal{P}_\mu(\tau)} \sum_{1 \leq j_1, j_2, \ldots, j_\mu \leq n} X_{j_1}^{w_1} \cdots X_{j_\mu}^{w_\mu} \binom{\beta_{j_1}^1}{w_1} \cdots \binom{\beta {j_\mu}^1}{w_\mu}
\end{aligned}$$

Ce qui donne bien la forme voulue lorque l'on regroupe tous les termes. □

On peut obtenir une formule similaire avec le calcul matriciel faisant aussi intervenir les partitions d'entiers mais je n'ai pas encore trouvé de belle manière de l'écrire.

Références

[BGT10] Jason P Bell, Dragos Ghioca, and Thomas J Tucker. The dynamical mordell-lang problem for étale maps. *American journal of mathematics*, 132(6) :1655–1675, 2010.

[CX14] Serge Cantat and Junyi Xie. Algebraic actions of discrete groups : the p-adic method. 2014.

[DG66] J Dieudonné and A Grothendieck. Éléments de géométrie algébrique iv. troisieme partie. *Publications Mathématiques de l'IHÉS, Paris*, 1966.

[ET79] DBA Epstein and WP Thurston. Transformation groups and natural bundles. *Proceedings of the London Mathematical Society*, 3(2) :219–236, 1979.

[Gro02] Larry C Grove. *Classical groups and geometric algebra*, volume 39. American Mathematical Soc., 2002.

[Hur92] Adolf Hurwitz. Über algebraische gebilde mit eindeutigen transformationen in sich. *Mathematische Annalen*, 41(3) :403–442, 1892.

[MKS04] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory : Presentations of groups in terms of generators and relations*. Courier Corporation, 2004.

[PS16] Yuri Prokhorov and Constantin Shramov. Jordan property for cremona groups. *American Journal of Mathematics*, 138(2) :403–418, 2016.

[Rob13] Alain M Robert. *A course in p-adic analysis*, volume 198. Springer Science & Business Media, 2013.

[Seg05] Daniel Segal. *Polycyclic groups*. Number 82. Cambridge University Press, 2005.

[Ser07] Jean-Pierre Serre. Bounds for the orders of the finite subgroups of g (k). *Group representation theory*, pages 405–450, 2007.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. *Contemporary Mathematics*, 14 :183, 2009.