Actions of nilpotent groups on complex algebraic varieties

Marc Abboud

January 26, 2022

Abstract

We study nilpotent groups acting faithfully on complex algebraic varieties. We use a method of base change. For finite p-groups, we go from $\mathbf{k}$, a number field, to a finite field in order to use counting lemmas. We show that a finite p-group of polynomial automorphisms of $\mathbf{k}^d$ is isomorphic to a subgroup of $\mathrm{GL}_d(\mathbf{k})$. For infinite groups, we go from $\mathbf{C}$ to $\mathbf{Z}_p$ and use p-adic analytic tools and the theory of p-adic Lie groups. We show that a finitely generated nilpotent group H acting faithfully on a complex quasiprojective variety X of dimension d can be embedded into a p-adic Lie group acting faithfully and analytically on $\mathbf{Z}_p^d$; we deduce that d is larger than the virtual derived length of H.

Contents

1 Introduction

1.1 Minkowski's bound for polynomial automorphisms.

Rational numbers.– Let p be a prime. A finite *p-group* is a group of size p^α for some integer $\alpha \geq 0$. For $d \in \mathbf{Z}_+$, define $M_{\mathbf{Q}}(d,p)$ to be the integer

$$M_{\mathbf{Q}}(d,p) = \left\lfloor \frac{d}{p-1} \right\rfloor + \left\lfloor \frac{d}{p(p-1)} \right\rfloor + \left\lfloor \frac{d}{p^2(p-1)} \right\rfloor + \cdots$$

(Here M stands for Minkowski). Let v_p be the p-adic valuation; then $M_{\mathbf{Q}}(d,p) = \left\lfloor \frac{d}{p-1} \right\rfloor + v_p\left(\left\lfloor \frac{d}{p-1} \right\rfloor !\right)$.

Theorem 1.1 (Minkowski 1887, see [Ser07])**.** *Let d be a natural number and let p be a prime. If G is a finite p-subgroup of $\mathrm{GL}_d(\mathbf{Q})$, then $v_p(|G|) \leq M_{\mathbf{Q}}(d,p)$, and this upper bound is optimal: there are groups of order $p^{M_{\mathbf{Q}}(d,p)}$ in $\mathrm{GL}_d(\mathbf{Q})$.*

Number fields.– Schur extended Minkowski's result to the case of number fields. To state Schur's result, let us introduce some notation for cyclotomic extensions. Consider a number field $\mathbf{k}$ and fix an algebraic closure $\overline{\mathbf{k}}$ of $\mathbf{k}$. Denote by $z_a \in \overline{\mathbf{k}}$ any primitive a-th root of unity, for a any positive integer; for instance $z_4 = \mathsf{i}$, a square root of -1.

- If $p \geq 3$, set $t(\mathbf{k};p) = [\mathbf{k}(z_p) : \mathbf{k}]$ and let $m(\mathbf{k};p)$ be the maximal integer a such that $\mathbf{k}(z_p)$ contains z_{p^a}; note that $m(\mathbf{k};p)$ is finite because $\mathbf{k}$ is a finite extension of $\mathbf{Q}$. Then, define

$$M_{\mathbf{k}}(d,p) := m(\mathbf{k};p) \cdot \left\lfloor \frac{d}{t(\mathbf{k};p)} \right\rfloor + \left\lfloor \frac{d}{p \cdot t(\mathbf{k};p)} \right\rfloor + \left\lfloor \frac{d}{p^2 t(\mathbf{k};p)} \right\rfloor + \cdots .$$

- If $p = 2$, set $t(\mathbf{k};2) = [\mathbf{k}(z_4) : \mathbf{k}]$ and let $m(\mathbf{k};2)$ be the largest integer a such that $z_{2^a} \in \mathbf{k}(z_4)$. Define

$$M_{\mathbf{k}}(d,2) = d + (m(\mathbf{k};2) - 1)\left\lfloor \frac{d}{t(\mathbf{k};2)} \right\rfloor + \left\lfloor \frac{d}{2t(\mathbf{k};2)} \right\rfloor + \left\lfloor \frac{d}{4t(\mathbf{k};2)} \right\rfloor + \cdots .$$

This definition is consistent with the definition of $M_{\mathbf{Q}}(d,p)$ given above.

Theorem 1.2 ([Sch05], [Ser07]). *Let d be a natural number, and let p be a prime. If G is a finite p-subgroup of $\mathrm{GL}_d(\mathbf{k})$ then $v_p(|G|) \leq M_{\mathbf{k}}(d,p)$ and this bound is optimal.*

It is not difficult to find a subgroup $G \subset \mathrm{GL}_d(\mathbf{k})$ such that $|G| = p^{M(d,p)}$. We recall how to do so in Proposition 2.17.

Polynomial automorphisms.– Our first goal is to extend the theorem of Minkowski and Schur to an algebraic, but nonlinear context. Let $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$ be the group of polynomial automorphisms of the affine space $\mathbf{A}^d$, over some number field $\mathbf{k}$. This group contains $\mathrm{GL}_d(\mathbf{k})$ but it is much more complicated. Surprisingly, we are able to show that the Minkowski-Schur bound still holds for subgroups of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$ and in fact the same finite subgroups appear.

Theorem A. *Let $\mathbf{k}$ be a number field, let d a natural number, and let $p \geq 3$ be a prime. If G is a finite p-subgroup of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$, then there exists a group embedding $G \hookrightarrow \mathrm{GL}_d(\mathbf{k})$. In particular, Schur's bound still holds:*

$$v_p(|G|) \leq M_{\mathbf{k}}(d,p),$$

and this bound is optimal.

The proof first shows the bound on the cardinal of the group G and we then find the group embedding $G \hookrightarrow \mathrm{GL}_d(\mathbf{k})$ using a Sylow argument.

Remark 1.3. The case $p = 2$ is also dealt with in Section 2. But we don't get an optimal bound. For example for $p = 2$ and $\mathbf{k} = \mathbf{Q}$, we show that any 2-subgroup G of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{Q}})$ can be embedded into $\mathrm{GL}_d(\mathbf{Q}(z_4))$ and therefore satisfies $v_2(|G|) \leq M_{\mathbf{Q}}(d,2) + \lfloor \frac{d}{2} \rfloor$. More precisely, Proposition 2.10 defines three cases $(a), (b)$ and (c) when $p = 2$. We get an embedding into $\mathrm{GL}_d(\mathbf{k})$ in case (a) and (b) (this is the case for example if $\mathbf{k}$ contains z_4), but in case (c) we can only get an embedding of G into $\mathrm{GL}_d(\mathbf{k}(z_4))$ and therefore we get the bound $v_2(|G|) \leq M_{\mathbf{k}}(d,2) + \lfloor \frac{d}{2} \rfloor = M_{\mathbf{k}(z_4)}(d,2)$. See Theorem C page 8 for the general statement.

In fact, Theorem A still holds when $\mathbf{k}$ is a finitely generated field over $\mathbf{Q}$ but the proof is less intuitive so we will show the proof for $\mathbf{k}$ a number field and explain how to extend it to finitely generated field over $\mathbf{Q}$ in Remark 2.16. We then state the complete theorem for finitely generated fields over $\mathbf{Q}$ in Theorem D page 9.

Our method of proof follows [Ser07], in which Serre bounds the order of the finite subgroups of $\mathrm{H}(\mathbf{k})$, for H a semi-simple algebraic group; the phenomenon mentioned in Remark 1.3 also appears for such groups H. The general idea is to embed G into a group of linear automorphisms over a finite field, study the finite field case, and use cyclotomic characters to find the optimal bound yield by this method.

Birational transformations.– The problem of the existence of uniform bounds on the size of finite p-groups or finite simple groups in infinite dimensional groups such as $\mathrm{Aut}(\mathbf{A}^d)$ or $\mathrm{Bir}(\mathbf{A}^d)$ has been studied extensively during the last decade (see [Ser09]). For an arbitrary complex projective variety X, one cannot expect uniform bounds that would only depend on the dimension of X, since every finite group is the group of automorphisms of a complex projective curve (see [Gre60]). But precise results have been obtained when X is rationally connected. Recently, Jinsong Xu showed the following optimal result: *Let d be a natural number and let p be a prime $> d+1$. If X is a rationally connected variety of dimension d over an algebraically closed field of characteristic 0, and G is a finite p-subgroup of $\mathrm{Bir}(X)$, then G is abelian and its rank is at most d* (see [Xu20]). Results of this type were first shown by Prokhorov, Shramov and Birkar in [PS14] for birational transformations of any varieties and improvements were made for rationally connected varieties in [PS16].

These results are deeper than our Theorem A, but our contribution has a few advantages: it may serve as an introduction to the work of Prokhorov and Shramov, the techniques are more elementary, the precise bound we obtain illustrates the interplay between the arithmetic of the field $\mathbf{k}$ and the size of the group, and the proof shows why the upper bound of Minkowski and Schur is still valid in $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$.

Remark 1.4. The results of Prokhorov and Shramov rely on the BAB conjecture, which was proved by Birkar in [Bir21]. The result of J. Xu relies on the work of Haution on equivariant cohomology and fixed points of finite groups (see [Hau19]).

1.2 A bound for the action of finitely generated nilpotent groups

1.2.1 Nilpotent and solvable groups

Let H be a group. If $a, b \in H$, we denote by $[a,b] := aba^{-1}b^{-1}$ their commutator. If H_1, H_2 are two subgroups of H, then we denote by H_1H_2 the subgroup generated by the set $\{h_1h_2 : h_1 \in H_1, h_2 \in H_2\}$ and by $[H_1, H_2]$ the subgroup generated by the set $\{[h_1,h_2] : h_1 \in H_1, h_2 \in H_2\}$. The lower central (resp. derived) series is defined by $D^0(H) = H$ (resp. $D_0(H) = H$) and $D^{i+1}(H) = [H, D^i(H)]$ (resp. $D_{i+1}(H) = [D_i(H), D_i(H)]$). A group H is *nilpotent* (resp. *solvable*) when there exists an integer k such that $D^k(H) = 1$ (resp. $D_k(H) = 1$).

If H is nilpotent, its *nilpotency class* $\mathrm{nilp}(H)$ is the lowest integer such that $D^k(H) = 1$. For a solvable group H, denote by $\mathrm{dl}(H)$ its derived length, that is the least integer k such that $D_k(H) = 1$. The *virtual derived length* is the minimum of $\mathrm{dl}(H_0)$ over finite index subgroups H_0 of H. Similar definitions and notation will be used for Lie algebras.

1.2.2 Upper bounds on the virtual derived length

Finite p-groups are nilpotent. We now look at infinite, finitely generated nilpotent groups, and their actions by automorphisms and birational transformations. In [CX18], Cantat and Xie used p-adic analysis to give information on group actions on complex algebraic varieties by birational transformations, and sketched the proof of the following result.

Theorem B. *Let H be a finitely generated nilpotent group acting faithfully on a quasi-projective variety X by algebraic automorphisms over a field of characteristic zero. Then,*

$$\mathrm{vdl}(H) \leq \dim X$$

where $\mathrm{vdl}(H)$ *is the* virtual derived length *of H. Furthermore, this bound is optimal.*

Another goal of this paper is to give a complete proof of this result. Again, the main idea is to replace the initial field of definition by another one, here $\mathbf{Q}_p$, and in fact by $\mathbf{Z}_p$, for a suitable prime p. Then, the initial action of the discrete group H will be extended to an analytic action of a p-adic Lie group over $\mathbf{Z}_p^{\dim X}$, so that tools from p-adic analysis will be available, in particular p-adic analytic vector fields and p-adic Lie algebras. Thus, Theorem B will follow from a similar theorem we prove over $\mathbf{Z}_p$. Section 3 is dedicated to the construction of p-adic analytic tools needed for the proof of Theorem B such as infinite dimensional p-adic Lie groups or Tate-analytic diffeomorphisms and Section 4 is dedicated to the proof of Theorem B.

2 Finite p-groups

2.1 Preliminaries

Primes and p-adic numbers In the rest of the article, p is a prime unless mentioned otherwise, $\mathbf{Z}_p$ denote the ring of p-adic integers and $\mathbf{Q}_p$ is the fraction field of $\mathbf{Z}_p$. Recall that Dirichlet's theorem states for any integers a, n such that $gcd(a, n) = 1$, there is an infinite amount of prime numbers ℓ such that $\ell = a \mod n$.

Maximal ideals and reduction If q is a power of a prime, we denote by $\mathbf{F}_q$ the field with q elements. Let A be a finitely generated $\mathbf{Z}$-algebra. Then for every maximal ideal $\mathfrak{m} \subset A$, $A/\mathfrak{m}$ is a finite field. This comes from the Nullstellensatz for Jacobson rings which is proven in [Bou07a], chapter 5, §3, theorem 3 of section 4.

2.2 Groups of linear transformations over Q

To warm up, let us prove the theorem of Minkowski. For a ring A, we denote by $A^\times$ its subgroup of invertible elements; for any prime p the group $(\mathbf{Z}/p^2\mathbf{Z})^\times$ is cyclic.

Proposition 2.1. *Let G be a finite subgroup of $\mathrm{GL}_d(\mathbf{Q})$. For any prime ℓ large enough there exists an injective homomorphism $G \hookrightarrow \mathrm{GL}_d(\mathbf{F}_\ell)$.*

Proof. Since G is finite, there exists an integer N such that $G \subset \mathrm{GL}_d(\mathbf{Z}[1/N])$. Now, for each $g \in G \setminus \{\mathrm{id}\}$ denote by $l(g)$ the largest prime factor that appears in the prime decomposition of the rational numbers given by the coefficients of the matrix $g - \mathrm{id}$; denote by L the maximum of the primes $l(g)$. If $\ell > \max(N, L)$, the homomorphism of reduction modulo l is defined on G and is injective. □

Thus, if $G \subset \mathrm{GL}_d(\mathbf{Q})$ is a finite subgroup, $v_p(|G|) \leq v_p(|\mathrm{GL}_d(\mathbf{F}_\ell)|)$ for any ℓ given by Proposition 2.1. We know that

$$|\mathrm{GL}_d(\mathbf{F}_\ell)| = \ell^{d(d-1)/2} \prod_{i=1}^{d-1} \left(\ell^i - 1\right). \tag{1}$$

for any prime ℓ. Let us compute the p-adic valuation of such a product.

Lemma 2.2. *Suppose $p \neq 2$ and let ℓ be a generator of $(\mathbf{Z}/p^2\mathbf{Z})^\times$.*

1. *If p divides $\ell^i - 1$ then $p - 1$ divides i;*
2. *If $p - 1$ divides i then $v_p(\ell^i - 1) = 1 + v_p(i)$.*

Proof. Suppose p divides $\ell^i - 1$. Note that $\ell^{ip} - 1 = (\ell^i - 1)\sum_{j=0}^{p-1} \ell^{ij}$; since $\ell^i \equiv 1 \mod p$, we have $\sum_{j=0}^{p-1} \ell^{ij} \equiv 0 \mod p$, and then $\ell^{ip} \equiv 1 \mod p^2$. Since ℓ is of order $p(p-1)$ in $(\mathbf{Z}/p^2\mathbf{Z})^\times$, we have that $p(p-1)$ divides ip therefore, $p-1$ divides i, which proves the first assertion.

We prove assertion 2 by induction on $v_p(i)$. To initialize the induction assume $v_p(i) = 0$. Then p and therefore $p(p-1)$ do not divide i; thus $\ell^i \not\equiv 1 \mod p^2$ because ℓ is of order $p(p-1)$. Thus, $v_p(\ell^i - 1) = 1$. Now suppose the assertion true for $v_p(i) = k$ with $k \geq 0$ and suppose $v_p(i) = k+1$. Write $i = (p-1)p^{k+1}m$ with m not divisible by p and suppose the result true for $v_p(i) = k$. Let $s := \ell^{(p-1)m}$, then

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

By induction, s^{p^k} is of the form $s^{p^k} = 1 + up^{k+1}$ where u is an integer not divisible by p. Therefore, for all $1 \leq j \leq p-1$, $s^{jp^k} = 1 + jp^{k+1}u + v_j p^2$ where v_j is some integer. , therefore we can write

$$\sum_{j=0}^{p-1} s^{jp^k} = p + p^{k+1}\frac{p(p-1)}{2}u + p^2 V = p\left(1 + p^{k+1}\frac{p-1}{2}u + pV\right)$$

where $V = \sum v_j$. Since p is odd, $\frac{p-1}{2}$ is an integer and this sum has p-adic valuation 1 since $k+1 \geq 1$.

$$s^{p^{k+1}} - 1 = (s^{p^k} - 1)\cdot p\left(1 + p^k\sum_{j=0}^{p-1} u_j\right)$$

since $k \geq 1$, we get $v_p(s^{p^{k+1}} - 1) = 1 + v_p(s^k - 1) = 1 + (k+1)$. □

Equation (1) and Lemma 2.2 provide the following corollary.

Corollary 2.3. *Let d be an integer, let p be an odd prime, and let ℓ be a prime whose image in $(\mathbf{Z}/p^2\mathbf{Z})^\times$ is a generator. Then*

$$v_p(\mathrm{GL}_d(\mathbf{F}_\ell)) = M_{\mathbf{Q}}(d,p).$$

This proves also the fact that Theorem 1.1 "is optimal for $\mathrm{GL}_d(\mathbf{F}_\ell)$" by Sylow.

To prove Theorem 1.1, consider a finite group $G \subset \mathrm{GL}_d(\mathbf{Q})$, then apply Dirichlet's theorem and Proposition 2.1 to embed G in $\mathrm{GL}_d(\mathbf{F}_\ell)$ for some prime generator ℓ of $(\mathbf{Z}/p^2\mathbf{Z})^*$. The corollary gives the desired upper bound.

Remark 2.4. The case $p = 2$ is also treated by Minkowski and in fact the same bound applies. However the proof is slightly different as it is required to embed G into an orthogonal group over a finite field. Indeed, If ℓ is an odd prime then the best bound one can get is $v_2(\mathrm{GL}_d(\mathbf{F}_l)) \leq M(d,2) + \lfloor d/2 \rfloor$ with equality with the right choice of ℓ (see Proposition 2.13). To embed a finite group H of matrices over $\mathbf{Q}$ into an orthogonal group over a finite field, one just need to look at the positive definite bilinear form $\psi := \sum_{h\in H} {}^tHH$. For any prime ℓ large enough such that ℓ does not divide $\det\psi$, the group homomorphism of reduction mod ℓ induces an embedding of H into an orthogonal group over $\mathbf{F}_l$, however this process does not generalize well when looking at polynomial automorphisms (See Remark 2.18).

2.3 The Minkowski's bound for finite groups of polynomial automorphisms with rational coefficients

To prove Theorem A, we adapt the proof of the Minkowski bound for linear automorphisms. Actually, to conclude it suffices to show that Proposition 2.1 also holds for finite p-subgroups of polynomial automorphisms.

Proposition 2.5. *Let d be an integer. Let G be a finite p-subgroup of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{Q}})$. Then, there exists a prime ℓ such that*

1. *ℓ is a generator of $(\mathbf{Z}/p^2\mathbf{Z})^\times$*
2. *There is an injective homomorphism $G \hookrightarrow \mathrm{GL}_d(\mathbf{F}_\ell)$*

Lemma 2.6. *Let d be an integer and p a prime. Let F be a finite field with $\mathrm{char}(F) \neq p$. Let G be a finite subgroup of $\mathrm{Aut}(\mathbf{A}^d_F)$ of order p^α. Then G has a fixed point $x_0 \in \mathbf{A}^d(F) = F^d$ and the homomorphism*

$$\begin{array}{rccc} \Phi: & G & \longrightarrow & \mathrm{GL}_d(F) \\ & g & \longmapsto & D_{x_0}g \end{array}$$

is injective.

Proof. The group G acts on F^d which is of size $|F|^d$. Since $|G| = p^\alpha$ and p does not divide $|F|$, the class equations gives the existence of at least one trivial G-orbit in F^d; hence, the existence of a fixed point $x_0 \in F^d$.

Up to a translation we can suppose that $x_0 = 0$. Now to show the injectivity of Φ. Take g in G such that $D_0 g = \mathrm{id}$, then

$$g(x_1, \cdots, x_d) = g(\mathbf{x}) = \mathrm{id} + \sum_{j \geq 2} A_j(\mathbf{x})$$

where A_j is the homogeneous part of g of degree j. Suppose that $g \neq \mathrm{id}$, let j_0 be the lowest index $j \geq 2$ such that $A_j \neq 0$. We rewrite g as $g = \mathrm{id} + A_{j_0} + B$ where $B = \sum_{j > j_0} A_j$ and compute the second iterate

$$\begin{aligned} g^2(\mathbf{x}) &= g(\mathbf{x}) + A_{j_0}(g(\mathbf{x})) + B(g(\mathbf{x})) \\ &= \mathrm{id} + A_{j_0}(\mathbf{x}) + B(\mathbf{x}) + A_{j_0}(\mathbf{x} + A_{j_0}(\mathbf{x}) + B(\mathbf{x})) + B(g(\mathbf{x})) \\ &= \mathrm{id} + 2A_{j_0}(\mathbf{x}) + (\text{terms of higher degree}). \end{aligned}$$

And for every $k \geq 1$ we obtain

$$g^k(\mathbf{x}) = \mathrm{id} + kA_{j_0}(\mathbf{x}) + (\text{terms of higher degree}).$$

Since, g is of order p^t for a certain $t > 0$, replacing k by p^t in this formula we get $p^t A_{j_0}(\mathbf{x}) = 0$, a contradiction since $\mathrm{char}\, F \neq p$. □

Remark 2.7. If F is of characteristic 0 and x_0 is fixed by G, then the proof shows also that $\Phi : g \mapsto D_{x_0} g$ is injective.

Proof of Theorem A when $\mathbf{k} = \mathbf{Q}$. As in the linear case, we can find an integer N such that $G \subset \mathrm{Aut}(\mathbf{A}^d_{\mathbf{Z}[1/N]})$. So, for $\ell > N$ prime , reduction modulo ℓ is well defined on G. Now, for ℓ large enough such that ℓ does not divide any coefficient of $g - \mathrm{id}$ for all $g \in G \subset \mathrm{Aut}(\mathbf{A}^d_{\mathbf{Z}[1/N]})$, this homomorphism is injective and we can use Dirichlet's theorem to ensure that ℓ is a generator of $(\mathbf{Z}/p^2\mathbf{Z})^\times$. G is now embedded in $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{F}_\ell})$ and we replace it by its image in $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{F}_\ell})$. By Lemma 2.6, there is a point $x_0 \in \mathbf{F}_\ell^d$ fixed by G and we have an injective homomorphism $\Phi : G \hookrightarrow \mathrm{GL}_d(\mathbf{F}_\ell)$. This concludes the proof when $p \neq 2$.

□

2.4 Extension of Minkoswski's bound to number fields

Strategy.– This part is dedicated to the proof of Schur's bound for finite p-groups of polynomial automorphisms over arbitrary number fields. We will then prove Theorem A using a Sylow argument. As in the previous section, we want to show the

Theorem 2.8. *Let* $\mathbf{k}$ *be a number field,* d *an integer and* p *be an odd prime. Let* G *be a finite* p*-subgroup of* $\mathrm{Aut}_{\mathbf{k}}(\mathbf{A}^d)$*, then there exists a finite field* $\mathbf{F}$ *with* $\mathrm{char}\, \mathbf{F} \neq p$ *and an injective group homomorphism* $G \hookrightarrow \mathrm{GL}_d(\mathbf{F})$ *such that* $v_p(|\mathrm{GL}_d(\mathbf{F})|) \leq M_{\mathbf{k}}(d, p)$.

Indeed, this would prove that $v_p(|G|) \leq v_p(|\mathrm{GL}_d(\mathbf{F})|) \leq M_{\mathbf{k}}(d, p)$. The natural idea is to do an analog of the proof for $\mathbf{k} = \mathbf{Q}$. Replace $\mathbf{Z}$ by the ring of integers $L := \mathcal{O}_{\mathbf{k}}$ of $\mathbf{k}$, then for any maximal ideal $\mathfrak{m}$ of L lying over a sufficiently large prime, there is an injective homomorphism $G \hookrightarrow \mathrm{Aut}(\mathbf{A}^d_{L/\mathfrak{m}})$. By taking differentials at a fixed point over $L/\mathfrak{m}$ we would see G as a subgroup of $\mathrm{GL}_d(L/\mathfrak{m})$ and the order of $\mathrm{GL}_d(L/\mathfrak{m})$ would give a bound $v_p(|G|) \leq \sum_{i=1}^d v_p(|L/\mathfrak{m}|^i - 1)$. The remaining part is to choose $\mathfrak{m}$ wisely so that we get the lowest bound possible. To do this, we use cyclotomic characters.

Cyclotomic characters.– In this part, $\mathbf{k}$ is a finitely generated field over $\mathbf{Q}$. We denote by μ_n the group of n-th roots of unity in $\overline{\mathbf{k}}$. Recall that $\mathrm{Aut}(\mu_n) = (\mathbf{Z}/n\mathbf{Z})^\times$ because every automorphism ϕ is of the form $\phi(\omega) = \omega^a$ where $a \in (\mathbf{Z}/n\mathbf{Z})^\times$.

Definition 2.9 (Cyclotomic character)**.** Denote by $\Gamma_{\mathbf{k}} = \mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})$ the absolute Galois group of $\mathbf{k}$. For every $n \geq 1, \Gamma_{\mathbf{k}}$ preserves the group $\mu_n \subset \overline{\mathbf{k}}^\times$ of n-th roots of unity, this induces a group homomorphism

$$\chi_n : \Gamma_{\mathbf{k}} \to \mathrm{Aut}(\mu_n) = (\mathbf{Z}/n\mathbf{Z})^\times$$

called the *n-th cyclotomic character of* $\mathbf{k}$. In particular, if p is a prime number, since the inclusion $\mu_{p^n} \subset \mu_{p^{n+1}}$ induces a group homomorphism $\mathrm{Aut}(\mu_{p^{n+1}}) = (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times \to \mathrm{Aut}(\mu_{p^n}) = (\mathbf{Z}/p^n\mathbf{Z})^\times$, we have a compatible family of homomorphisms

$$\chi_{p^n} : \Gamma_{\mathbf{k}} \to \mathrm{Aut}(\mu_{p^n}).$$

This family of homomorphisms induces the *p^∞-cyclotomic character*

$$\chi_{p^\infty} : \Gamma_{\mathbf{k}} \to \mathbf{Z}_p^\times = \varprojlim (\mathbf{Z}/p^n\mathbf{Z})^\times$$

where $\mathbf{Z}_p$ is the ring of p-adic integers. This homomorphism is continuous with respect to the profinite topologies on $\Gamma_{\mathbf{k}}$ and $\mathbf{Z}_p^\times$.

We are interested in the image of χ_{p^∞} which is a closed subgroup of $\mathbf{Z}_p^\times$. Define $t(\mathbf{k};p)$ and $m(\mathbf{k};p)$ as in Section 1.1. The number $m(\mathbf{k};p)$ is always finite if $\mathbf{k}$ is finitely generated over $\mathbf{Q}$ (see [Ser07], §4.3). If s is an integer, we denote by C_s the cyclic group of order s.

Proposition 2.10 ([Ser07], §4)**.**

1. *If p is an odd prime, one has*
$$\mathbf{Z}_p^\times \simeq C_{p-1} \times (1 + p \cdot \mathbf{Z}_p).$$
The group $1 + p \cdot \mathbf{Z}_p$ is a procyclic subgroup generated by $1 + p$ as a topological group and isomorphic to the additive group $\mathbf{Z}_p$. Its closed subgroups are the groups $1 + p^j\mathbf{Z}_p$ with $j \geq 1$.
Furthermore, one has
$$\operatorname{Im}\chi_{p^\infty} = C_{t(\mathbf{k};p)} \times \left\{1 + p^{m(\mathbf{k};p)} \cdot \mathbf{Z}_p\right\}.$$
2. *If $p = 2$, then $\mathbf{Z}_2^\times = C_2 \times \{1 + 4 \cdot \mathbf{Z}_2\}$. There are 3 possibilities for $\operatorname{Im}\chi_{2^\infty}$:*
   (a) $\operatorname{Im}\chi_{2^\infty} = 1 + 2^{m(\mathbf{k};p)} \cdot \mathbf{Z}_2$ and then $t(\mathbf{k};p) = 1$.
   (b) $\operatorname{Im}\chi_{2^\infty} = \langle -1 + 2^{m(\mathbf{k};p)-1}\rangle$ (the closure of the group generated by $-1 + 2^{m(\mathbf{k};p)-1}$) and then $t(\mathbf{k};p) = 2$.
   (c) $\operatorname{Im}\chi_{2^\infty} = C_2 \times \left\{1 + 2^{m(\mathbf{k};p)}\mathbf{Z}_2\right\}$ and then $t(\mathbf{k};p) = 2$.

Remark 2.11. Those 3 cases are distinct when $m(\mathbf{k}, p) \neq \infty$. We will refer as $\mathbf{k}$ being in case (a), (b), or (c) when $\operatorname{Im}\chi_{2^\infty}$ is of the form (a),(b) or (c) of Proposition 2.10.

Recall that an integral domain L is *normal* if every localisation at a prime ideal of L is integrally closed. Let L be a normal domain that is finitely generated over $\mathbf{Z}$ such that the fraction field of L is $\mathbf{k}$. For any maximal ideal $\mathfrak{m} \subset L$, the quotient $L/\mathfrak{m}$ is finite by the Nullstellensatz for Jacobson rings and $N(\mathfrak{m}) := |L/\mathfrak{m}|$ is the *norm* of $\mathfrak{m}$. Recall that for a ring R, $\operatorname{Spec} R$ denotes the set of prime ideals of R and $\operatorname{Specmax} R$ the set of its maximal ideals both with the Zariski topology. The following theorem is proven in [Ser07, §6 Theorem 7].

Theorem 2.12. *Let L be a normal domain finitely generated over $\mathbf{Z}$ such that the fraction field of L is $\mathbf{k}$. Let n be an integer and c an element of $(\mathbf{Z}/n\mathbf{Z})^\times$. Denote by X_c the set of elements $x \in \operatorname{Specmax}(L)$ such that $N(x) \equiv c \mod n$. Then:*

1. *If $c \notin \operatorname{Im}\chi_n$, $X_c = \emptyset$.*
2. *If $c \in \operatorname{Im}\chi_n$, then X_c is Zariski-dense in $\operatorname{Specmax}(L)$. In particular, X_c is infinite.*

In particular, the ring of integers of a number field is normal because it is integrally closed and this property is stable under localisation. So Theorem 2.12 holds for L the ring of integers of a number field.

Valuations.– We define the constant
$$M'_{\mathbf{k}}(d,p) = \inf_{u \in \operatorname{Im}\chi_{p^\infty}} \sum_{i=1}^{d} v_p(u^i - 1).$$

The next proposition is adapted from Proposition 4, §6 of [Ser07] to our context.

Proposition 2.13. *One has*

(a) If $p \neq 2$ or if $p = 2$ and $t(\mathbf{k};p) = 1$ ($\mathbf{k}$ is in case (a)), then
$$M'_{\mathbf{k}}(d,p) = \sum_{\substack{i=1 \\ t(\mathbf{k};p)|i}}^{d} (m(\mathbf{k};p) + v_p(i)) = M_{\mathbf{k}}(d,p).$$

(b) If $p = 2$, $t(\mathbf{k};p) = 2$ and $\mathbf{k}$ is in case (b), one has
$$M'_{\mathbf{k}}(d,2) = r_1 + (m(\mathbf{k};p) - 1)r_0 + \sum_{i=1}^{d} v_2(i) = M_{\mathbf{k}}(d,2)$$
where r_1 is the number of odd integers between 1 and d and r_0 the number of even integers in this range.

(c) If $p = 2$, $t(\mathbf{k};p) = 2$ and $\mathbf{k}$ is in case(c), one has
$$M'_{\mathbf{k}}(d,2) = r_1 + m(\mathbf{k};p)r_0 + \sum_{i=1}^{d} v_2(i) = \left\lfloor \frac{d}{2} \right\rfloor + M_{\mathbf{k}}(d,2)$$
with the same definition for r_1 and r_0.

Proof. Set $t = t(\mathbf{k}; p), m = m(\mathbf{k}; p)$. We start with the case $p \neq 2$. First if t divides i, then $v_p(u^i - 1) \geq m + v_p(i)$. This is because u can be written as zv with $z^t = 1$ and $v_p(v - 1) \geq m$, so $v_p(u^i - 1) = v_p(v^i - 1)$. So we have an inequality $M'_{\mathbf{k}}(d, p) \geq \sum_{\substack{i=1 \\ t|i}}^{d} (m + v_p(i))$. To have the opposite one, choose $u \in \operatorname{Im} \chi_{p^\infty}$ such that $u = zx$ with z of order t and $v_p(x - 1) = m$. This also works for $p = 2$ and $t = 1$.

Suppose now that $p = 2$ and $t = 2$, Define $m' = m - 1$ in case (b) and $m' = m$ in case (c). Then for every $x \in \operatorname{Im} \chi_{2^\infty}$,

$$v_2(x^i - 1) \geq m' + v_2(i) \text{ if } i \text{ is even.}$$
$$v_2(x^i - 1) \geq 1 \text{ if } i \text{ is odd.}$$

This gives

$$M'_{\mathbf{k}}(d, 2) \geq \sum_{i \text{ odd}} 1 + \sum_{i \text{ even}} (m' + v_2(i)) = r_1 + m' r_0 + \sum_{i \text{ even}} v_2(i).$$

To show the opposite inequality, we use the fact that $x = -1 + 2^{m'} \in \operatorname{Im} \chi_{2^\infty}$ and we check that $\sum_{i=1}^{d} v_2(x^i - 1) = r_1 + m' r_0 + \sum_{i=1}^{d} v_2(i)$.

Now, to show the different equalities, notice that for (a):

$$M'_{\mathbf{k}}(d, p) = m \cdot \left\lfloor \frac{d}{t} \right\rfloor + \sum_{i=1}^{\left\lfloor \frac{d}{t} \right\rfloor} v_p(ti).$$

Now, since t divides $p - 1$, one has $v_p(ti) = v_p(i)$ and the rest of the computation is similar as in the case $\mathbf{k} = \mathbf{Q}$.

For (b) and (c), we have $r_0 = \left\lfloor \frac{d}{2} \right\rfloor$ and $r_1 = d - r_0$.

$$\begin{aligned} M'_{\mathbf{k}}(d, 2) &\leq d - \left\lfloor \frac{d}{2} \right\rfloor + m' \left\lfloor \frac{d}{2} \right\rfloor + \sum_{i=1}^{d} v_2(i) \\ &= d + (m' - 1) \left\lfloor \frac{d}{2} \right\rfloor + \sum_{i=1}^{d} v_2(i) \\ &= d + (m' - 1) \left\lfloor \frac{d}{t} \right\rfloor + \sum_{k \geq 1} \left\lfloor \frac{d}{2^k} \right\rfloor \\ &= d + m' \left\lfloor \frac{d}{t} \right\rfloor + \sum_{k \geq 1} \left\lfloor \frac{d}{2^k t} \right\rfloor. \end{aligned}$$

□

We can now state Theorem 2.8 without assuming p odd.

Theorem 2.14. *Let $\mathbf{k}$ be a number field, d an integer and p be prime. Let G be a finite p-subgroup of $\operatorname{Aut}_{\mathbf{k}}(\mathbf{A}^d)$, then there exists a finite field $\mathbf{F}$ with $\operatorname{char} \mathbf{F} \neq p$ and an injective group homomorphism $G \hookrightarrow \mathrm{GL}_d(\mathbf{F})$ such that $v_p(|\mathrm{GL}_d(\mathbf{F})|) \leq M'_{\mathbf{k}}(d, p)$.*

Proof of Theorem 2.14.– Take G a finite p-subgroup of $\operatorname{Aut}(\mathbf{A}^d_{\mathbf{k}})$ with p prime.

Step 1. Reduction modulo $\mathfrak{l}$.– Set $L = \mathcal{O}_{\mathbf{k}}$. For every element $a \in \mathbf{k}^\times$ the fractional ideal generated by a is of the form (see [Neu99], §3)

$$a \cdot \mathcal{O}_{\mathbf{k}} = (a) = \prod_{\mathfrak{l} \in \operatorname{Spec} L} \mathfrak{l}^{v_{\mathfrak{l}}(a)}$$

and the prime ideals $\mathfrak{l}$ such that $v_{\mathfrak{l}}(a) \neq 0$ are in finite number. For such an $\mathfrak{l}$ there exists a unique prime $\ell \in \mathbf{Z}_+$ such that $(\ell) \subset \mathfrak{l}$. We define for $g \in \operatorname{Aut}(\mathbf{A}^d_{\mathbf{k}})$

$$\ell_g := \max_{a \in \operatorname{coeff}(g - \mathrm{id})} \{\text{prime } \ell \in \mathbf{Z}_+ : \exists \mathfrak{l} \in \operatorname{Spec} L, (\ell) \subset \mathfrak{l}, v_{\mathfrak{l}}(a) \neq 0\}$$

where $\operatorname{coeff}(g - \mathrm{id})$ is the set of coefficients of the polynomial transformation $g - \mathrm{id}$. Set $M_1 = \max_{g \in G} \ell_g$ ($M_1 < +\infty$ since G is finite) and $M = \max(M_1, p)$, then for every prime $\ell > M$ and for every $\mathfrak{m} \in \operatorname{Specmax}(L)$ such that $(\ell) \subset \mathfrak{m}$, we have a well-defined injective homomorphism

$$\Psi : G \hookrightarrow \operatorname{Aut}(\mathbf{A}^d_{\mathbf{F}}),$$

where $\mathbf{F} = L/\mathfrak{m}$. Indeed, the homomorphism of rings $\phi : L \twoheadrightarrow L/\mathfrak{m}$ induces the homomorphism $\phi : L_{\mathfrak{m}} := (L \setminus \mathfrak{m})^{-1} L \to L/\mathfrak{m}$. By construction, G is a subgroup of $\operatorname{Aut}(\mathbf{A}^d_{L_{\mathfrak{m}}})$, so $\phi : G \to \operatorname{Aut}(\mathbf{A}^d_{L/\mathfrak{m}})$ is well-defined and it is injective by our definition of M.

Step 2. The group $\Psi(G)$.– Now, $\Psi(G)$ is a p-subgroup of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{F}})$. Since $p \notin \mathfrak{m}$, we get $\mathrm{char}(\mathbf{F}) \neq p$. By Proposition 2.6, there is a point x_0 in $\mathbf{A}^d(\mathbf{F})$ fixed by $\Psi(G)$ and by taking the differentials at x_0, we obtain an injective homomorphism $G \hookrightarrow \Psi(G) \hookrightarrow \mathrm{GL}_d(\mathbf{F})$. So, we get

$$v_p(|G|) \leq v_p\left(N(\mathfrak{m})^{\frac{d(d+1)}{2}} \prod_{i=1}^{d} (N(\mathfrak{m})^i - 1)\right) = \sum_{i=1}^{d} v_p(N(\mathfrak{m})^i - 1). \tag{2}$$

Set $X := \{\mathfrak{m} \in \mathrm{Specmax}(L) : \mathfrak{m}|(s), \text{for some } s > M \text{ prime}\}$, then (2) holds for all $\mathfrak{m} \in X$ and we obtain $v_p(|G|) \leq \inf_{\mathfrak{m}\in X} \sum_{i=1}^{d} v_p(N(\mathfrak{m})^i - 1)$. So, to conclude, all we have to prove is

$$\inf_{\mathfrak{m}\in X} \sum_{i=1}^{d} v_p(N(\mathfrak{m})^i - 1) \leq M'_{\mathbf{k}}(d,p). \tag{3}$$

Step 3. Proof of (3).– The set X is open in $\mathrm{Specmax}\, L$. For, $X = \left(\bigcup_{l\leq M, l \text{ prime}} V(l)\right)^c$ with $V(l) = \{\mathfrak{m} \in \mathrm{Specmax}(L) : (l) \subset \mathfrak{m}\}$ and $V(l)$ is closed. Take $u \in \mathrm{Im}\, \chi_{p^\infty}$. For $j \geq 1$, let u_j be the projection of u in $(\mathbf{Z}/p^j\mathbf{Z})^\times$. By Theorem 2.12 the set of maximal ideals $\mathfrak{m}$ such that $N(\mathfrak{m}) \equiv u_j \mod p^j$ is dense, therefore it intersects the open subset X, so for every $j \geq 1$, we can find $\mathfrak{m}_j \in X$ such that $N(\mathfrak{m}_j) \equiv u_j \mod p^j$. Then, one has $\lim_{j\to\infty} N(\mathfrak{m}_j) = u$ in $\mathbf{Z}_p^\times$, therefore $v_p(u^i - 1) = \lim_{j\to\infty} v_p(N(\mathfrak{m}_j)^i - 1)$ so

$$\inf_{\mathfrak{m}\in X} \sum_{i=1}^{d} v_p(N(\mathfrak{m})^i - 1) \leq \sum_{i=1}^{d} v_p(u^i - 1);$$

and this holds for every $u \in \mathrm{Im}\, \chi_{p^\infty}$. Using Proposition 2.13, we get

$$\inf_{\mathfrak{m}\in X} \sum_{i=1}^{d} v_p(N(\mathfrak{m})^i - 1) \leq \inf_{u\in \mathrm{Im}_{\chi_{p^\infty}}} \sum_{i=1}^{d} v_p(u^i - 1) = M'_{\mathbf{k}}(d,p).$$

Proof of Theorem A and comments.–

Theorem C. *Let $\mathbf{k}$ be a number field, let d be a natural number, and let p be a prime. Let G be a finite p-subgroup of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$, then*

1. *If $p \geq 3$ or $p = 2$ and $\mathbf{k}$ is in case (a) or (b), there exists a group embedding*
$$G \hookrightarrow \mathrm{GL}_d(\mathbf{k}).$$
2. *If $p = 2$ and $\mathbf{k}$ is in case (c), there exists a group embedding*
$$G \hookrightarrow \mathrm{GL}_d(\mathbf{k}(z_4)).$$

Remark 2.15. We do not state a Sylow-like property, saying that G is conjugated to a subgroup of $\mathrm{GL}_d(\mathbf{k})$, we only state that we can find an isomorphism of abstract groups from G to a subgroup of $\mathrm{GL}_d(\mathbf{k})$.

Proof. For 1, we know that $v_p(|G|) \leq M_{\mathbf{k}}(d,p)$ and that there exists a subgroup $H \subset \mathrm{GL}_d(\mathbf{k})$ such that $|H| = p^{M_{\mathbf{k}}(d,p)}$ by Theorem 1.2. Let $L = \mathcal{O}_{\mathbf{k}}$ be the ring of integers of $\mathbf{k}$. The proof of Theorem 2.14 shows that there exists an infinite number of maximal ideals $\mathfrak{m}$ of L such that $v_p(\mathrm{GL}_d(\mathbf{F})) \leq M_{\mathbf{k}}(d,p)$ where $\mathbf{F} = L/\mathfrak{m}$. So for any such maximal ideal $\mathfrak{m} \subset L$ lying over a sufficiently large prime, there are embeddings $\Psi_H : H \hookrightarrow \mathrm{GL}_d(\mathbf{F})$ and $\Psi_G : G \hookrightarrow \mathrm{GL}_d(\mathbf{F})$. Looking at the size of H, we deduce that $v_p(\mathrm{GL}_d(\mathbf{F})) = M_{\mathbf{k}}(d,p)$ and $\Psi_H(H)$ is a p-Sylow of $\mathrm{GL}_d(\mathbf{F})$. By Sylow's theorems, $\Psi_G(G)$ is conjugated to a subgroup of $\Psi_H(H)$ in $\mathrm{GL}_d(\mathbf{F})$. This implies that G is isomorphic to a subgroup of H.

For 2, if $\mathbf{k}$ is in case (c) then one can check that $\mathbf{k}(z_4)$ is in case (a) and that $m(\mathbf{k}(z_4);2) = m(\mathbf{k};2)$, therefore $M_{\mathbf{k}(z_4)}(d,2) = M_{\mathbf{k}}(d,2) + \left\lfloor \frac{d}{2} \right\rfloor$ and the same proof as 1 shows the result. □

Remark 2.16. Theorem A and C still hold for $\mathbf{k}$ finitely generated over $\mathbf{Q}$. We just need to explain how the proof of Theorem 2.14 works in that case.

We need to find a normal domain L finitely generated over $\mathbf{Z}$ such that G is defined over L and to define the open subset $X \subset \mathrm{Specmax}\, L$ used for equation (3). Here is how to proceed: since G is finite, there exists a finitely generated $\mathbf{Z}$-algebra R such that the elements of G are defined over R, we can suppose that R contains $1/p$. By Noether Normalization's Lemma and more precisely by generic freeness (see [Eis95], Theorem 14.4), there exists $t_1, \ldots, t_s \in R$ and an integer N such that R is a finite free module over $\mathbf{Z}[1/N][t_1, \ldots, t_s]$. We can then take for L the integral closure of $\mathbf{Z}[1/N][t_1, \ldots, t_s]$ in $\mathbf{k}$, L is a normal domain over which G is defined since $R \subset L$. We also have that L is finitely generated over $\mathbf{Z}$ because by [Eis95, Theorem 4.14] it is a finite module over $\mathbf{Z}[1/N][t_1, \ldots, t_s]$.

Now, let A be the set of coefficients of $g - \mathrm{id}$ for $g \in G$. Set $X = \{\mathfrak{m} \in \mathrm{Specmax}\, L : A \cap \mathfrak{m} = \emptyset\}$. This is an open subset of $\mathrm{Specmax}\, L$ as A is finite and $X = \bigcap_{a\in A} V(a)^c$. For any $\mathfrak{m} \in X$ we have an injective group homomorphism $G \hookrightarrow \mathrm{Aut}(\mathbf{A}^d_{L/\mathfrak{m}})$ and Equation (2) holds. The proof of Equation (3) is the same as in the case of number fields. This proves Theorem 2.14 for finitely generated fields over $\mathbf{Q}$.

To prove Theorem C, the key ingredient is that there exists subgroups of $\mathrm{GL}_d(\mathbf{k})$ of size $p^{M_{\mathbf{k}}(d,p)}$, as Theorem A is stated only for number fields we show for completeness how to construct finite p-groups of $\mathrm{GL}_d(\mathbf{k})$ of size $p^{M_{\mathbf{k}}(d,p)}$ when $\mathbf{k}$ is finitely generated over $\mathbf{Q}$. The proof of Theorem C for finitely generated fields over $\mathbf{Q}$ is then similar as in the case of number fields using Noether Normalization Lemma, we leave the details to the reader.

Proposition 2.17. *Let $\mathbf{k}$ be a finitely generated field over $\mathbf{Q}$ and let p be a prime, there exists a finite p-subgroup of $\mathrm{GL}_d(\mathbf{k})$ of size $p^{M_{\mathbf{k}}(d,p)}$.*

Proof. Set $t = t(\mathbf{k}; p), m = m(\mathbf{k}; p)$ and $r = \lfloor d/t \rfloor$.

The case $p \geq 3$.– Let $\rho = z_{p^m} \in \mathbf{k}(z_p)$. Then, the group $(\mathbf{Z}/p^m\mathbf{Z})$ acts on $\mathbf{k}(z_p)$ via multiplication by ρ^k for all $k \in \mathbf{Z}/p^m\mathbf{Z}$. Now take r copies of $\mathbf{k}(z_p)$; this is a $\mathbf{k}$-vector space V of dimension $t \cdot r \leq d$ and let S_r be the r-th symmetric group, S_r acts on V by permuting the r copies of $\mathbf{k}(z_p)$ and therefore the group

$$G := S_r \ltimes (\mathbf{Z}/p^m\mathbf{Z})^r$$

acts faithfully by linear automorphisms on V and has the desired size. Indeed, $v_p(|G|) = m \cdot \lfloor \frac{d}{t} \rfloor + v_p(\lfloor \frac{d}{t} \rfloor !)$.

The case $p = 2$ and $t = 1$.– In that case, $\mathbf{k} = \mathbf{k}(z_4)$, then $M_{\mathbf{k}}(d, 2) = m \cdot \lfloor \frac{d}{t} \rfloor + v_2(\lfloor \frac{d}{t} \rfloor !)$. Therefore, the proof above works as well, with $\rho = z_{2^m}$ acting on $\mathbf{k}(z_4) = \mathbf{k}$.

The case $p = 2$ and $t = 2$.– The construction above yields that $(\mathbf{Z}/2^m\mathbf{Z})$ acts linearly on $\mathbf{k}(z_4)$. We twist this action by the Galois automorphism σ that sends z_4 to $-z_4$; σ is an involution that sends $\rho = z_{2^m}$ to another primitive 2^m-th root of unity. So we get that the group $H := \mathbf{Z}/2\mathbf{Z} \ltimes \mathbf{Z}/2^m\mathbf{Z}$ acts faithfully on $\mathbf{k}(z_4)$. Now set $r = \lfloor d/2 \rfloor$, we have that $G := S_r \ltimes H$ acts faithfully and linearly on a $\mathbf{k}$ vector space V consisting of r copies of $\mathbf{k}(z_4)$. The vector space V has dimension $2 \cdot \lfloor d/2 \rfloor \leq d$. Now, we have

$$v_2(|G|) = (m + 1) \cdot \lfloor d/2 \rfloor + v_2(\lfloor d/2 \rfloor !).$$

If d is even this is equal to $M_{\mathbf{k}}(d, 2)$ and we are done. If d is odd then $v_2(|G|) = M_{\mathbf{k}}(d, 2) - 1$ but then V is of dimension $d - 1$ so the group $G \times \{\pm 1\}$ acts faithfully on $V \oplus \mathbf{k}$ that is of dimension d and this group has the desired size.

□

We can therefore state:

Theorem D. *Let $\mathbf{k}$ be a finitely generated field over $\mathbf{Q}$, let d be a natural number, and let p be a prime. Let G be a finite p-subgroup of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$, then*

1. *If $p \geq 3$ or $p = 2$ and $\mathbf{k}$ is in case (a) or (b), there exists a group embedding $G \hookrightarrow \mathrm{GL}_d(\mathbf{k})$ and $v_p(|G|) \leq M_{\mathbf{k}}(d; p)$.*
2. *If $p = 2$ and $\mathbf{k}$ is in case (c), there exists a group embedding $G \hookrightarrow \mathrm{GL}_d(\mathbf{k}(z_4))$ and $v_2(|G|) \leq M_{\mathbf{k}}(d, 2) + \lfloor \frac{d}{2} \rfloor$.*

Remark 2.18. We get the optimal bounds except when $p = 2$ and $\mathbf{k}$ is in case (c) (this includes $\mathbf{k} = \mathbf{Q}$). For that case, following Remark 2.4, to get the optimal bound one would need a result of the following type: *Let $\mathbf{k}$ be a number field in case (c) and G a finite subgroup of $\mathrm{Aut}(\mathbf{A}^d_{\mathbf{k}})$ of order 2^α, then for $\mathfrak{m}$ in the complement of a finite set of $\mathrm{Specmax}\, \mathcal{O}_{\mathbf{k}}$ the group G embeds into an orthogonal group over $\mathcal{O}_{\mathbf{k}}/\mathfrak{m}$.*

We know that for any maximal ideal $\mathfrak{m}$ lying over a large enough prime, there exists an embedding $G \hookrightarrow \mathrm{GL}_d(\mathbf{F})$ and a fixed point $\bar{x} \in (\mathbf{F})^d$ of G where $\mathbf{F} = \mathcal{O}_{\mathbf{k}}/\mathfrak{m}$. The problem is to find a symmetric matrix A such that

$$A_G := \sum_{g \in G} {}^t D_{\bar{x}} g \cdot A \cdot D_{\bar{x}} g$$

is non-degenerate. Such an A does not exist for every subgroup of $\mathrm{GL}_d(\mathbf{F})$ precisely because $v_2(|\mathrm{GL}_d(\mathbf{F})|)$ is larger than the 2-adic valuation of the order of any orthogonal group over $\mathbf{F}$. So we have to use that G comes from a group over $\mathbf{k}$ and adapt $\mathfrak{m}$ wisely.

Here is one way to attack this problem. Pick a fixed point $\overline{x}$ of G with coordinates in $\overline{\mathbf{Q}}$; such a point exist because otherwise let (P_n) be the system of polynomial equations stating that G has a fixed point. If this system has no solution over $\overline{\mathbf{Q}}$ then by Hilbert's Nullstellensatz, there is a relation of the form $1 = \sum Q_i P_i$ for some polynomials Q_i. Now take a number field $\mathbf{k}'$ where this relation is defined. By the previous paragraph we can reduce modulo a large enough maximal ideal $\mathfrak{m}$ of $\mathcal{O}_{\mathbf{k}'}$ (i.e lying over a large enough prime) and this would yield an injective group homomorphism $G \hookrightarrow \mathrm{Aut}(\mathbf{A}^d)$ where F is a finite field with $\mathrm{char}\, F \neq p$. The relation $1 = \sum Q_i P_i$ still holds in $\mathbf{F}$ but this is absurd since we know that G admits a fixed point over $\mathbf{F}$. Let $\mathbf{k}'$ be the number field generated by the coordinates of $\overline{x}$ and $\mathbf{k}$. We would like to find A such that A_G is non-degenerate. If $\mathbf{k}' \subset \mathbf{R}$ we can use argument of positive definiteness to do so, but otherwise a first difficulty occurs. Now, even if such an A could be found, the arithmetic of $\mathbf{k}'$ leads to another difficulty: For any maximal ideal $\mathfrak{m}' \subset \mathcal{O}_{\mathbf{k}'}$ lying over a large enough maximal ideal $\mathfrak{m} \subset \mathcal{O}_{\mathbf{k}}$, the image x' of $\overline{x}$ in $\mathbf{F}' = \mathcal{O}_{\mathbf{k}'}/\mathfrak{m}'$ is a fixed point of G, and the reduction modulo $\mathfrak{m}'$ of A_G is an invertible symmetric matrix over $\mathbf{F}'$. But if the degree $[\mathbf{F}', \mathbf{F}]$ is even, then the 2-adic valuation of any orthogonal group over $\mathbf{F}'$ will be too large to get the optimal bound.

3 p-adic analysis

To prove Theorem B, we will show that any finitely generated nilpotent group acting on a complex quasiprojective variety of dimension d can be embedded in a finite dimensional p-adic Lie group acting analytically on a p-adic manifold of dimension d. The theorem will follow from a version of Theorem 1.1 of [ET79] in a p-adic context. In this section, we introduce all the tools from p-adic analysis and p-adic Lie groups needed for the proof.

3.1 Tate-Analytic Diffeomorphisms

3.1.1 Definitions and topology

Let p be a prime. We denote by $\mathbf{Z}_p$ the completed ring of $\mathbf{Z}$ with respect to the p-adic norm defined such that $|p| = 1/p$. Denote by $\mathbf{Q}_p$ the completion of $\mathbf{Q}$ with respect to this norm. Then $\mathbf{Q}_p = \mathrm{Frac}(\mathbf{Z}_p)$ and $\mathbf{Z}_p$ is the set of elements of $\mathbf{Q}_p$ of absolute value ≤ 1. We extend this norm to $\mathbf{Q}_p^d$ by taking the maximum of the absolute values of the coordinates. We will use explicitly the ring $\mathbf{Z}_p$ and the field $\mathbf{Q}_p$ but what follows can be done with any complete valued ring or field of characteristic 0. The right setup would be to consider $\mathbf{C}_p$ the completion of the algebraic closure of $\mathbf{Q}_p$ and $\mathbf{D}_p$ the unit ball of $\mathbf{C}_p$.

For reference, check [CX18]. We denote by $B(x,r) = \left\{y \in \mathbf{Q}_p^d : ||x-y|| \leq r\right\}$ the closed ball of radius r and center x. It is both open and closed. Such sets will be called *clopen*.

Tate analytic maps.– Classically, a function $\mathbf{Z}_p^d \to \mathbf{Q}_p$ is analytic if it can be written locally as a converging power series, we work with *Tate-analytic* functions which are converging power series of radius ≥ 1 over $\mathbf{Z}_p^d$.

Take $\mathbf{Z}_p^d$ with its standard coordinates $\mathbf{x} = x_1, \cdots, x_d$. On $\mathbf{Q}_p[x_1, \cdots, x_d] =: \mathbf{Q}_p[\mathbf{x}]$ the Gauss norm is defined by

$$\forall g \in \mathbf{Q}_p[\mathbf{x}], \quad g = \sum_{I \subset \mathbf{Z}_+^d} a_I \mathbf{x}^I, \quad ||g|| := \max_I |a_I|$$

where $I = (I_1, \cdots, I_d)$ and $\mathbf{x}^I := x_1^{I_1} \cdots x_d^{I_d}$; we denote by $\mathbf{Q}_p\langle x_1, \cdots, x_d\rangle =: \mathbf{Q}_p\langle \mathbf{x}\rangle$ the completion of $\mathbf{Q}_p[x_1, \cdots, x_d]$ with respect to the Gauss norm $\mathbf{Q}_p\langle \mathbf{x}\rangle$ is the set of formal power series with coefficients in $\mathbf{Q}_p$ such that $a_I \to 0$ when $I \to \infty$ (i.e when $\max(I) \to \infty$). It is also the set of formal power series with coefficients in $\mathbf{Q}_p$ converging over $\mathbf{Z}_p^d$. This shows that $\mathbf{Q}_p\langle \mathbf{x}\rangle$ equipped with the Gauss norm is an infinite-dimensional Banach space over $\mathbf{Q}_p$. For all polynomials $f, g \in \mathbf{Q}_p[\mathbf{x}]$, then $||f \cdot g|| \leq ||f|| \cdot ||g||$ and this is also true in $\mathbf{Q}_p\langle \mathbf{x}\rangle$, therefore $\mathbf{Q}_p\langle \mathbf{x}\rangle$ is a Banach algebra over $\mathbf{Q}_p$, it is the *Tate algebra* over $\mathbf{Q}_p$ in d variables (see [Rob00]). We also define $\mathbf{Z}_p\langle \mathbf{x}\rangle$ which is the completion of $\mathbf{Z}_p[\mathbf{x}]$ for the gauss norm; it is in fact the set of elements of $\mathbf{Q}_p\langle \mathbf{x}\rangle$ of norm ≤ 1.

Remark 3.1. For each $f \in \mathbf{Q}_p\langle \mathbf{x}\rangle$ there exists an element $s \in \mathbf{Z}_p$ such that $s \cdot f \in \mathbf{Z}_p\langle \mathbf{x}\rangle$ and if $g \in \mathbf{Q}_p\langle \mathbf{x}\rangle$ is such that $g(0) \in \mathbf{Z}_p$, then there exist an integer $N > 0$ such that $g(p^N \mathbf{x}) \in \mathbf{Z}_p\langle \mathbf{x}\rangle$. Moreover, if $g \in \mathbf{Q}_p[[\mathbf{x}]]$ is a formal power series with coefficients in $\mathbf{Q}_p$ with a strictly positive radius of convergence, then there exists an integer N such that $g(p^N \mathbf{x})$ belongs to $\mathbf{Q}_p\langle \mathbf{x}\rangle$.

Remark 3.2. There exist Tate-analytic maps with non-integer coefficients such that $f(\mathbf{Z}_p^d) \subset \mathbf{Z}_p$. For example, take

$$f(x) = \frac{x^p - x}{p}.$$

Since for all $x \in \mathbf{Z}_p, x^p \equiv x \mod p$, f induces a map $f : \mathbf{Z}_p \to \mathbf{Z}_p$. However every element $f \in \mathbf{Q}_p\langle \mathbf{x}\rangle^d$ induces a map $f : \mathbf{D}_p^d \to \mathbf{C}_p$ and we have $f(\mathbf{D}_p^d) \subset \mathbf{D}_p \Leftrightarrow f \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$. This has to do with the residue field of $\mathbf{Z}_p$ being finite but not the residue field of $\mathbf{D}_p$ (see [Rob00], Proposition of page 240).

For any $m \geq 0$, elements of $\mathbf{Q}_p\langle \mathbf{x}\rangle^m$ are called *Tate-analytic functions*. If $g \in \mathbf{Q}_p\langle \mathbf{x}\rangle^d$, then

$$\forall x, y \in \mathbf{Z}_p^d, ||g(x) - g(y)|| \leq ||g||\,||x - y||\,. \tag{4}$$

In particular, g is $||g||$-Lipschitz.

Proposition 3.3 (Strassman's Theorem, see [Rob00], chapter 6, section 2.1)**.** *Let $f \in \mathbf{Q}_p\langle t\rangle$ be a Tate-analytic function in one variable, if f is not the zero function, then f has a finite number of zeros over $\mathbf{Z}_p$.*

Corollary 3.4. *Let $f \in \mathbf{Q}_p\langle \mathbf{x}\rangle$, if there exists a non-empty open subset $\mathcal{U} \subset \mathbf{Z}_p^d$ such that $f_{|\mathcal{U}} \equiv 0$ then f is the zero function.*

Remark 3.5. This is not true for analytic functions over $\mathbf{Z}_p^d$. For example define g by $g(y) = 1$ if $||y|| \leq |p|$ and $g(y) = 0$ otherwise. Then, g is analytic at every point of $\mathbf{Z}_p^d$ because it is locally constant, it vanishes on the open subset $\left\{x \in \mathbf{Z}_p^d : ||x|| = 1\right\}$ but g is not the zero function.

Proof of Corollary 3.4. Take $y \in \mathcal{U}$ and $x \in \mathbf{Z}_p^d$. Let φ be the function $\varphi : t \in \mathbf{Z}_p \mapsto f(tx + (1-t)y)$. Then φ belongs to $\mathbf{Q}_p\langle t\rangle$ and it vanishes for any sufficiently small t. By Proposition 3.3, we have that φ is the zero function, therefore $f(x) = 0$. □

Let $f, g \in \mathbf{Q}_p\langle \mathbf{x}\rangle$ and $c > 0$, we write $f \equiv g \mod p^c$ if $||f-g|| \leq |p|^c$ and we extend such notation componentwise for $\mathbf{Q}_p\langle \mathbf{x}\rangle^m$ for every $m \geq 1$.

Example 3.6. If $c = 1$ and $f, g \in \mathbf{Z}_p\langle \mathbf{x}\rangle$, then $f = \sum_I a_I \mathbf{x}^I \equiv \mathrm{id}(\mathbf{x}) \mod p$ means that $\overline{f} := \sum_I \overline{a_I}\mathbf{x}^I = \mathrm{id}(\mathbf{x})$ where $\overline{a_I} = a_I \mod p$ is the reduction of $a_i \bmod p\mathbf{Z}_p$.

Tate analytic diffeomorphisms.– The composition determines a natural map

$$\begin{array}{ccccc} \mathbf{Z}_p\langle X_1, \cdots, X_n\rangle^m & \times & \mathbf{Z}_p\langle Y_1, \cdots, Y_s\rangle^n & \longrightarrow & \mathbf{Z}_p\langle Y_1, \cdots, Y_s\rangle^m \\ (g_1, \cdots ., g_m) & & (h_1, \cdots, h_n) & \longmapsto & (g_1(h_1, \cdots, h_n), \cdots, g_m(h_1, \cdots, h_n)) \end{array}$$

If the three integers n, m, s are equal to the same integer d, $(\mathbf{Z}_p\langle \mathbf{x}\rangle^d, \circ)$ becomes a semigroup. The invertible elements of this semigroup are called *Tate-analytic diffeomorphisms* and form a group denoted by $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$. Using Equation (4), we have that $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ acts by isometries on $\mathbf{Z}_p^d$.

Remark 3.7. Following Remark 3.2, we see that $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ consists exactly of the elements of $f \in \mathbf{Q}_p\langle \mathbf{x}\rangle$ that induces a Tate-analytic diffeomorphisms $f : \mathbf{D}_p^d \to \mathbf{D}_p^d$.

The next proposition shows an easy way to construct Tate-analytic diffeomorphisms of small polydisks.

Proposition 3.8 (Local inversion theorem, see [Ser92])**.** *Let $\Phi \in \mathbf{Z}_p[[X_1, \cdots ., X_d]]^d$ be a power series with a strictly positive radius of convergence. Suppose that $\Phi(0) = 0$ and $\det(D_0\Phi) \neq 0$, then there exists a unique $\Psi \in \mathbf{Q}_p[[X_1, \cdots ., X_d]]^d$, with a strictly positive radius of convergence, such that $\Psi(0) = 0$ and*

$$\Phi \circ \Psi(\mathbf{x}) = \Psi \circ \Phi(\mathbf{x}) = \mathbf{x}.$$

Furthermore, $||\Psi_n|| \leq \max(1, \left|\left|D_0\Phi^{-1}\right|\right|^n)$, where $\Psi_n \in \mathbf{Q}_p[X_1, \cdots, X_n]^d$ is the homogeneous part of degree n of Ψ and $||\cdot||$ is the Gauss norm over polynomials. Therefore, if Φ belongs to $\mathbf{Z}_p\langle \mathbf{x}\rangle^d$, then for any k such that $|p|^k < \left|\left|D_0\Phi^{-1}\right|\right|$, we have that $\frac{1}{p^k}\Phi(p^k\mathbf{x})$ and $\frac{1}{p^k}\Psi(p^k\mathbf{x})$ are Tate-analytic diffeomorphisms and are inverse of each other.

Group topology.– The following proposition shows that $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ is a topological group with respect to the topology induced by the Gauss norm.

Proposition 3.9. *Let $f, g, h \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$, then*

1. $||g \circ f|| \leq ||g||$.
2. *If f is an element of $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ then $||g \circ f|| = ||g||$.*
3. $||g \circ (\mathrm{id} + h) - g|| \leq ||h||$.
4. $\left|\left|f^{-1} - \mathrm{id}\right|\right| = ||f - \mathrm{id}||$ *if f is a Tate-analytic diffeomorphism.*

Lemma 3.10. *Let f be an element of $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$, if $f \equiv \mathrm{id} \mod p$ then $f^{p^c} \equiv \mathrm{id} \mod p^c$.*

Corollary 3.11. *Let $c > 0$ be a real number, then the subgroup $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ of $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ consisting of all elements $f \in \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ such that $f \equiv \mathrm{id} \mod p^c$ is a normal subgroup of $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$.*

Proposition 3.9, Lemma 3.10 and Corollary 3.11 are proven in [CX18], section 2.1.

3.1.2 Analytic flow and Bell-Poonen theorem

Flows and vector fields.– As in real or complex geometry, we define vector fields and flows. Let d be an integer:

A *Tate-analytic vector field* $\mathbf{X}$ over $\mathbf{Z}_p^d$ is a vector field of the form

$$\mathbf{X}(\mathbf{x}) = \sum_{i=1}^{d} u_i(\mathbf{x})\partial_i$$

where each u_i belongs to $\mathbf{Q}_p\langle \mathbf{x}\rangle$. The Lie bracket of two vector fields $\mathbf{X}$ and $\mathbf{Y} = \sum_{i=1}^d v_i\partial_i$ is the vector field defined by

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

The $\mathbf{Q}_p$-Lie algebra of Tate-analytic vector fields over $\mathbf{Z}_p^d$ is denoted by $\Theta(\mathbf{Z}_p^d)$ it is a strict subalgebra of the Lie Algebra of analytic vector fields over $\mathbf{Z}_p^d$. The Gauss norm of a Tate-analytic vector field $\mathbf{X} = \sum u_i(\mathbf{x})\partial_i$ is defined as $||\mathbf{X}|| = \max_i ||u_i||$ and makes $\Theta(\mathbf{Z}_p^d)$ a complete Lie Algebra over $\mathbf{Q}_p$ isomorphic as a Banach space to $\mathbf{Q}_p\langle \mathbf{x}\rangle^d$.

A *Tate-analytic flow* Φ over $\mathbf{Z}_p^d$ is an element of $\mathbf{Z}_p\langle X_1, \cdots, X_d, t\rangle^d = \mathbf{Z}_p\langle \mathbf{x}, t\rangle^d$ which satisfies the following properties

(i) $\forall \mathbf{x} \in \mathbf{Z}_p^d,\ \forall s,t \in \mathbf{Z}_p, \quad \Phi(\mathbf{x}, s+t) = \Phi(\Phi(\mathbf{x}, s), t).$

(ii) $\forall \mathbf{x} \in \mathbf{Z}_p^d, \quad \Phi(\mathbf{x}, 0) = \mathrm{id}(\mathbf{x}).$

Set $\Phi_t := \Phi(\cdot, t) \in \mathbf{Z}_p\langle \mathbf{x} \rangle$. Then, $\Phi_0 = \mathrm{id}$ and $\Phi_t \in \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ since $\Phi_t^{-1} = \Phi_{-t}$. Then, $t \in \mathbf{Z}_p \mapsto \Phi_t \in \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ is a continuous homomorphism of topological groups with respect to the Gauss norm. The main point here is that flows are parametrized by the compact group $(\mathbf{Z}_p, +)$.

Example 3.12. If Φ is a Tate-analytic flow, then we can define its associated Tate-analytic vector field $\mathbf{X}_\Phi := \frac{\partial \Phi_t}{\partial t}_{|t=0}$. In particular, $\mathbf{X}_\Phi$ is Φ_t-invariant, for all $t \in \mathbf{Z}_p$.

From vector fields to Tate-analytic flows.– Since a Tate-analytic vector field $\mathbf{X}$ is analytic, it is a general fact that it admits local analytic flows over $\mathbf{Z}_p^d$ (see [Bou07b] for example), the next proposition shows that if the norm of $\mathbf{X}$ is sufficiently small, then it admits a global Tate-analytic flow.

Proposition 3.13. *If $\mathbf{X}$ is a Tate-analytic flow over $\mathbf{Z}_p^d$, then for any sufficiently small $\lambda \in \mathbf{Z}_p$, there exists a unique Tate-analytic flow $\Phi^\lambda \in \mathbf{Z}_p\langle \mathbf{x}, t \rangle^d$ such that*

$$\frac{\partial \Phi_t^\lambda(\mathbf{x})}{\partial t} = \lambda \mathbf{X}(\Phi_t^\lambda(\mathbf{x})).$$

In particular, let $c > 0$ be such that $c > \frac{1}{p-1}$, then every Tate-analytic vector fields $\mathbf{X}$ such that $||\mathbf{X}|| \leq |p|^c$ admits a global Tate-analytic flow.

Proof. The strategy is to solve this differential equation in the space of power series $\mathbf{Q}_p\left[[\mathbf{x}, t]\right]^d$ and then to show some properties on the radius of convergence of the solution. We first replace $\mathbf{X}$ by $\mu\mathbf{X}$ for some $\mu \in \mathbf{Z}_p$ such that $||\mathbf{X}|| \leq 1$. Write $\mathbf{X}(\mathbf{x}) = \sum_i u_i(\mathbf{x})\partial_i$ with $u_i \in \mathbf{Z}_p\langle \mathbf{x} \rangle$. We look at the differential equations

$$\frac{\partial}{\partial t} f_i(\mathbf{x}, t) = u_i(f(\mathbf{x}, t)) \tag{5}$$

with $f_i \in \mathbf{Q}_p\left[[\mathbf{x}, t]\right]$ and $f = (f_1, \cdots, f_d)$ such that $f(\mathbf{x}, 0) = \mathbf{x}$. Write

$$f_i(\mathbf{x}, t) = \sum_{k \geq 0} a_k^{(i)}(\mathbf{x}) t^k, \quad a_k^{(i)} \in \mathbf{Q}_p\left[[\mathbf{x}]\right]$$

then, the unique solution of this equation is formally given by the formulas $a_k^{(i)}(\mathbf{x}) = \frac{1}{k!}\frac{\partial^k f_i}{\partial t^k}(\mathbf{x}, 0)$. We show that for all integer $k \geq 0$, $\frac{\partial^k f_i}{\partial t^k}(\mathbf{x}, 0)$ belongs to $\mathbf{Z}_p\langle \mathbf{x} \rangle$ by induction on k. We get $a_0^{(i)} = x_i$ since $f(\mathbf{x}, 0) = \mathrm{id}(\mathbf{x})$ and $a_1^{(i)}(\mathbf{x}) = u_i(\mathbf{x})$ by Equation (5). Take $k \geq 2$ and suppose the result to be true for all $l < k$. By differentiating both sides of Equation (5) $k-1$ times with respect to t and taking $t = 0$, we see that $\frac{\partial^k f_i}{\partial t^k}(\mathbf{x}, 0)$ is obtained by sum and compositions of differentials of orders $\leq k-1$ of the Tate-analytic function $u_i \in \mathbf{Z}_p\langle \mathbf{x} \rangle$ and the Tate-analytic functions $\frac{\partial^l}{\partial t^l} f_i(\mathbf{x}, 0) \in \mathbf{Z}_p\langle \mathbf{x} \rangle$ with $l < k$. So $\frac{\partial^k f_i}{\partial t^k}(\mathbf{x}, 0)$ belongs to $\mathbf{Z}_p\langle \mathbf{x} \rangle$ by induction.

The solution f is then of the form

$$f(\mathbf{x}, t) = \mathrm{id}(\mathbf{x}) + \sum_{k \geq 1} \frac{\partial^k f}{\partial t^k}(\mathbf{x}, 0)\frac{t^k}{k!}.$$

Now take $\lambda \in \mathbf{Z}_p$, such that $|\lambda| \leq |p|^c$. We have that for all $k \geq 0$, $\frac{\lambda^k}{k!} \in \mathbf{Z}_p$ and $\lambda^k/k! \to 0$ in $\mathbf{Z}_p$ when $k \to \infty$. Then, $\Phi_t^\lambda := f(\cdot, \lambda t)$ is a Tate-analytic flow such that $\frac{\partial \Phi_t^\lambda}{\partial t}(\mathbf{x}) = \lambda \mathbf{X}(\Phi_t^\lambda(\mathbf{x}))$.

For the final statement, take $\mathbf{X}$ a Tate-analytic vector field such that $||\mathbf{X}|| \leq |p|^c$ and let $s \in \mathbf{Z}_p$ be such that $|s| = ||\mathbf{X}||$, then $\mathbf{Y} := \frac{1}{s}\mathbf{X}$ has norm ≤ 1. The proof shows that there exists a unique Tate-analytic flow Φ such that $\frac{\partial \Phi_t}{\partial t}_{|t=0} = s\mathbf{Y} = \mathbf{X}$.

□

Theorem 3.14 (local linearisation of vector fields)**.** *Let $\mathbf{X}_1, \cdots, \mathbf{X}_k$ be Tate-analytic vector fields over $\mathbf{Z}_p^d$ such that $[\mathbf{X}_i, \mathbf{X}_j] = 0$ for all $1 \leq i, j \leq k$. Suppose that there exists a point $m \in \mathbf{Z}_p^d$ such that the vectors $\mathbf{X}_i(m)$ are linearly independent. Then, there exists a clopen subset $\mathcal{V} \subset \mathbf{Z}_p^d$ containing m and an analytic diffeomorphism φ from $\mathbf{Z}_p^d$ onto $\mathcal{V}$ such that $\varphi^*(X_{i|\mathcal{V}}) = \partial_i$ and such that φ^* yields an injective Lie Algebra homomorphism $\Theta(\mathbf{Z}_p^d)_{|\mathcal{V}} \hookrightarrow \Theta(\mathcal{V})$.*

Remark 3.15. This theorem is well known in p-adic differential geometry with analytic regularity (see [Bou07b]), what is important here is that when changing coordinates we keep the Tate-analytic regularity for vector fields.

Proof. By translation, we can suppose that $m = 0$. We pick $Y_0 \subset T_0\mathbf{Z}_p^d$ such that we have the decomposition $T_0\mathbf{Z}_p^d = \mathrm{Vect}(X_1(0), \cdots, X_k(0)) \oplus Y_0$. Let $e_1, \cdots, e_{d-k}$ be a basis of Y_0. Pick local (analytic) coordinates $(x_1, \cdots, x_k, y_1, \cdots, y_{d-k})$ such that for all $1 \leq j \leq d-k$, $\frac{\partial}{\partial y_j}(0) = e_j$.

Define : $f : \mathbf{Z}_p^{d-k} \to \mathbf{Z}_p^d$ by

$$f(y_1, \cdots, y_{d-k}) = (0, \cdots, 0, y_1, \cdots, y_{d-k}).$$

Take the local analytic flows $\varphi^1, \cdots, \varphi^k$ associated to $\mathbf{X}_1, \cdots, \mathbf{X}_k$ at 0 (here we do not suppose these flows to be Tate-analytic) and consider

$$\begin{array}{rccc} g & : \mathbf{Z}_p^k \times \mathbf{Z}_p^{d-k} & \longrightarrow & \mathbf{Z}_p^d \\ & (t_1, \cdots, t_k; y) & \longmapsto & \varphi_{t_1}^1 \circ \cdots \circ \varphi_{t_k}^k(f(y)). \end{array}$$

The function g belongs to $\mathbf{Z}_p\left[[t_1, \cdots, t_k, \mathbf{y}]\right]^d$ with a radius of convergence $r_g > 0$, satisfies $g(0) = 0$ and its differential at the point $(0, 0)$ is

$$(x_1, \cdots, x_k; z) \mapsto x_1\mathbf{X}_1(0) + \cdots + x_k\mathbf{X}_k(0) + \sum_j z_j \frac{\partial}{\partial y_j}(0).$$

Therefore it is invertible. By Proposition 3.8 g admits a formal inverse $h \in \mathbf{Q}_p\left[[t_1, \cdots, t_k, \mathbf{y}]\right]^d$ with a radius of convergence $r_h > 0$. Denote by $\mathbf{z}$ the set of coordinates $(t_1, \cdots, t_k, y_1, \cdots, y_{d-k})$. Pick integers K, L such that $|p|^K < r_g$ and $|p|^L < r_h$ such that $g(B(0, |p|^K)) \subset B(0, |p|^L)$. Let $\mathcal{V}$ denote $g(B(0, |p|^K))$; it is a clopen subset of $\mathbf{Z}_p^d$ because $B(0, |p|^K)$ is clopen. Set $\varphi := \frac{1}{p^L} g(p^K \mathbf{z})$ and $\psi := \frac{1}{p^K} h(p^L \mathbf{z})$, they both belong to $\mathbf{Q}_p\langle \mathbf{z} \rangle^d$ and are inverse of each other and we have $\varphi^* \mathbf{X}_i = \partial_i$. Finally, since $\varphi \in \mathbf{Q}_p\langle \mathbf{z} \rangle^d$, the map φ^* preserves Tate-analytic vector fields. □

Theorem 3.16 (p-adic version of [ET79] Theorem 1.1)**.** *Let $\mathfrak{h}$ be a nilpotent Lie algebra of Tate-analytic vector fields of $\mathbf{Z}_p^d$, then $d \geq \mathrm{dl}(\mathfrak{h})$.*

Proof. We follow the proof of [Can14] Proposition 3.10 and proceed by induction on the dimension d. If $d = 0$, there is nothing to prove. Suppose $d \geq 1$ and that the result is true in dimension $d-1$. Since $\mathfrak{h}$ is nilpotent, its center is not trivial. Let $\mathbf{X}$ be a nonzero central element of $\mathfrak{h}$. Let m be a point where $\mathbf{X}(m) \neq 0$, then by Theorem 3.14, there exists a small clopen subset $\mathcal{V} \subset \mathbf{Z}_p^d$ and an analytic diffeomorphism $\varphi : \mathcal{V} \to \mathbf{Z}_p^d$ that yields coordinates $x_1, \cdots, x_d$ over $\mathcal{V}$ such that $\varphi_* \mathbf{X} = \partial_d$ and such that φ_* maps Tate-analytic vector fields to Tate-analytic vector fields. By Proposition 3.4 the morphism of restriction $\mathfrak{h} \to \mathfrak{h}_{|\mathcal{V}}$ is an isomorphism of Lie algebras. We replace $\mathfrak{h}$ by $\mathfrak{h}_{|\mathcal{V}}$ and work with the coordinates $x_1, \cdots, x_d$ over $\mathcal{V}$. Every vector field $\mathbf{Y}$ of $\mathfrak{h}$ must commute with $\mathbf{X} = \partial_d$ so it is of the form

$$\mathbf{Y} = \sum_{i=1}^{d} u_i(x_1, \cdots, x_{d-1}) \partial_i.$$

Let $\pi : \mathcal{V} \simeq \mathbf{Z}_p^d \to \mathbf{Z}_p^{d-1}$ be the projection over the first $d-1$ coordinates. This yields a Lie algebra homomorphism $\pi_* : \mathfrak{h} \to \Theta(\mathbf{Z}_p^{d-1})$. Denote by $\mathfrak{h}_1$ the image of $\mathfrak{h}$ under π_* and $\mathfrak{h}_0$ its kernel. We have the exact sequence

$$0 \to \mathfrak{h}_0 \to \mathfrak{h} \to \mathfrak{h}_1 \to 0.$$

Now, $\mathfrak{h}_0$ consists of Tate-analytic vector fields of $\mathfrak{h}$ of the form $u(x_1, \ldots, x_{d-1})\partial_d$ so it is abelian and $\mathfrak{h}_1$ is nilpotent because $\mathfrak{h}$ is. So we get $\mathrm{dl}(\mathfrak{h}) \leq \mathrm{dl}(\mathfrak{h}_1) + 1$ by the exact sequence and $\mathrm{dl}(\mathfrak{h}_1) \leq d-1$ by induction. □

We discuss the optimality of Theorem 3.16 in Section 4.4.

The theorem of Bell and Poonen.– The following theorem first proven by Bell in [Bel05] then by Poonen in [Poo14] gives us an easy way to construct flows from analytic transformations. This is a very strong theorem as it shows that, contrary to $\mathbf{R}$, over $\mathbf{Q}_p$ a lot of analytic diffeomorphisms are in a flow. See [Can18] for a more precise discussion on Bell-Poonen theorem.

Theorem 3.17 (Bell-Poonen)**.** *Let $d \geq 1$ be an integer, and $f \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$. Take $c > \frac{1}{p-1}$ and suppose that $f \equiv \mathrm{id} \mod p^c$, then*

1. *f is a Tate-analytic diffeomorphism.*
2. *There exists a unique Tate-analytic flow $\Phi \in \mathbf{Z}_p\langle \mathbf{x}, t \rangle^d$ such that*

$$\forall n \in \mathbf{Z}, \quad \Phi(\mathbf{x}, n) = f^n(\mathbf{x}).$$

In particular, $\Phi_1 = f$.

In fact, Poonen showed this theorem for the valuation ring of any ultrametric field $\mathbf{K}$. So, Bell-Poonen Theorem also holds over $\mathbf{D}_p$ or over any finite extension of $\mathbf{Q}_p$ for example.

Corollary 3.18. *Let H be a subgroup of $\mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ with $p \geq 3$, then H is torsion-free.*

Proof. Let $h \in H$, suppose that h has order $N < \infty$. By Theorem 3.17, there exists an Tate-analytic flow Φ such that $\Phi_1 = h$. Then for all $\mathbf{x} \in \mathbf{Z}_p^d$ the function $t \in \mathbf{Z}_p \mapsto \Phi_t(\mathbf{x}) - \mathbf{x} \in \mathbf{Z}_p^d$ is analytic and has an infinite number of zeros, so it is zero everywhere by Proposition 3.4. Therefore $\Phi_1(\mathbf{x}) = h(\mathbf{x}) = \mathbf{x}$ and $h = \mathrm{id}$. □

The next proposition won't be used in the proof of Theorem B but it gives useful information on the dynamics of Tate-analytic flows.

Proposition 3.19. *Let $\Phi \in \mathbf{Z}_p\langle \mathbf{x}, t\rangle$ be a Tate-analytic flow over $\mathbf{Z}_p^d$. If $\mathcal{U} \subset \mathbf{Z}_p^d$ is a clopen set, then there exists an $\varepsilon > 0$ such that*

$$\forall t \in \mathbf{Z}_p, \quad |t| \leq \varepsilon \Rightarrow \Phi_t(\mathcal{U}) = \mathcal{U}.$$

Proof. Fix $x \in \mathbf{Z}_p^d$ and $0 < r \leq 1$. Since $\Phi_t \to \mathrm{id}$ as $t \to 0$ in $\mathrm{Diff}^{an}(\mathbf{Z}_p)$, there exists $\varepsilon > 0$ such that for all $t \in \mathbf{Z}_p$, $|t| \leq \varepsilon \Rightarrow ||\Phi_t - \mathrm{id}|| \leq r$. Now for all $z \in \mathbf{Z}_p^d$, $||\Phi_t(z) - z|| \leq ||\Phi_t - \mathrm{id}|| \leq r$. Then, for all y such that $||y - x|| \leq r$,

$$\begin{aligned} ||\Phi_t(y) - x|| &= ||\Phi_t(y) - y + y - x|| \\ &\leq \max(||\Phi_t(y) - y||, ||y - x||) \leq r. \end{aligned}$$

So if $|t| \leq \varepsilon$, we have $\Phi_t(B(x,r)) \subset B(x,r)$ and $\Phi_{-t}(B(x,r)) \subset B(x,r)$, so we get the equality.

Since $\mathcal{U}$ is clopen, by compactness, $\mathcal{U} = \bigcup_{i=1}^{T} B(x_i, r_i)$ for some finite set $\{x_1, \cdots, x_T\} \subset \mathcal{U}$ and radii $r_i \in (0, 1]$. Thus, the results follows from the case of one ball. □

3.2 Infinite-dimensional analytic manifold over $\mathbf{Q}_p$

The main goal of the next two sections is to show that the topological group $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ is in fact an infinite dimensional Lie group over $\mathbf{Q}_p$.

We refer to [Bou07b] for reference on analytic functions and analytic manifolds over a Banach space. In this section $\mathbf{k}$ is an ultrametric complete field and E, F are Banach spaces over $\mathbf{k}$ (potentially of infinite dimension). As we shall see, taking $\mathbf{k} = \mathbf{Q}_p$ and $E, F = \mathbf{Q}_p^d$ allows one to recover the definition of converging power series and analytic functions over $\mathbf{Q}_p^d$.

Basically, if A is a Banach algebra over $\mathbf{Q}_p$, then any map of the form $f : A^d \to A$ such that locally at any point $x \in A^d$, there is a expression of f as a converging power series

$$f(x + h) = \sum_{I \subset \mathbf{Z}_+^d} a_I h^I$$

with $a_I \in A, a_I \to 0$ is an analytic map from A^d to A. The problem is that if A is not finite dimensional, this definition is not enough, as for example a continuous linear map is not necessarily described by an expression of this form but still should be analytic.

Multi-indices, multi-linear maps.– If $\alpha = (\alpha_1, \cdots, \alpha_d) \in \mathbf{Z}_+^d$ is a multi-index, then $|\alpha| := \sum_i \alpha_i$. For $1 \leq j \leq |\alpha|$, we define

$$\alpha(j) = \max\{k + 1 \in \mathbf{Z}_+ : \alpha_1 + \cdots + \alpha_k < j\}.$$

The sequence $(\alpha(j))_{1 \leq j \leq |\alpha|}$ is the increasing sequence consisting of α_1 times the number 1, α_2 times the number 2, …, α_d times the number d. For example, if $\alpha = (1, 5, 7)$, then $d = 3, |\alpha| = 13$ and

$$(\alpha(j))_{1 \leq j \leq 13} = (1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3).$$

For $1 \leq i \leq d$, we denote by $p_i : E^d \to E$ the projection to the i-th coordinate. For a multi-index $\alpha \in \mathbf{Z}_+^d$, we define

$$p_\alpha := (p_{\alpha(j)})_{1 \leq j \leq |\alpha|} : E^d \to E^{|\alpha|}.$$

If $\beta \in \mathbf{Z}_+^d$ is another multi-index, then we write $\alpha + \beta$ for the multi-index $(\alpha_i + \beta_i)_{1 \leq i \leq d}$. We write $\alpha \geq \beta$ if $\alpha_i \geq \beta_i$ for all $1 \leq i \leq d$; in that case there is a unique multi-index γ such that $\alpha = \beta + \gamma$, and we set $\alpha - \beta := \gamma$. We also define the binomial coefficient $\binom{\alpha}{\beta} := \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_d}{\beta_d}$. Finally, if $\mathbf{x} = (x_1, \cdots, x_d)$,

then $\mathbf{x}^\alpha := x_1^{\alpha_1} \cdots x_d^{\alpha_d}$ and if $\mathbf{y} = (y_1, \cdots, y_d)$, one has the identity

$$\begin{aligned}(\mathbf{x}+\mathbf{y})^\alpha &= (x_1+y_1)^{\alpha_1} \cdots (x_d+y_d)^{\alpha_d} \\ &= \left(\sum_{\beta_1=0}^{\alpha_1} \binom{\alpha_1}{\beta_1} x_1^{\beta_1} y_1^{\alpha_1-\beta_1}\right) \cdots \left(\sum_{\beta_d=0}^{\alpha_d} \binom{\alpha_d}{\beta_d} x_d^{\beta_d} y_d^{\alpha_d-\beta_d}\right) \\ &= \sum_{0\le\beta_1\le\alpha_1} \cdots \sum_{0\le\beta_d\le\alpha_d} \binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_d}{\beta_d} x_1^{\beta_1} \cdots x_d^{\beta_d} y_1^{\alpha_1-\beta_1} \cdots y_d^{\alpha_d-\beta_d} \\ &= \sum_{\beta\le\alpha} \binom{\alpha}{\beta} \mathbf{x}^\beta \mathbf{y}^{\alpha-\beta}.\end{aligned}$$

For an integer k, let $\mathcal{L}_k(E,F)$ be the set of continuous multilinear maps from E^k to F equipped with the topology of uniform convergence over bounded subsets. The norm of an element $\phi \in \mathcal{L}_k(E,F)$ is defined by

$$||\phi|| = \inf\left\{a > 0 : \forall x_1, \cdots, x_k \in E^k, ||\phi(x_1, \cdots, x_k)||_F \le a\, ||x_1||_E \cdots ||x_k||_E\right\}.$$

Continuous polynomial maps and power series.– ([Bou07b] Appendix of §1-7) A *continuous homogeneous polynomial map of multi degree* α, is a map $f : E^d \to F$ such that there exists $u \in \mathcal{L}_{|\alpha|}(E,F)$ for which $f = u \circ p_\alpha$. We denote by $P_\alpha(E,F)$ the vector space of continuous homogeneous polynomial maps of multi-degree α equipped with the quotient topology from $\mathcal{L}_{|\alpha|}(E,F)$. The norm of a continuous homogeneous polynomial map $P \in P_\alpha(E,F)$ is defined by

$$||P|| := \inf_{u\in\mathcal{L}_{|\alpha|}(E,F), P=u\circ p_\alpha} ||u||_{\mathcal{L}_{|\alpha|}(E,F)}.$$

Example 3.20. Set $E, F = \mathbf{Q}_p\langle\mathbf{x}\rangle$. Let P be the monomial $\mathbf{x}^\alpha$, then the map $P : g \in \mathbf{Q}_p\langle\mathbf{x}\rangle^d \mapsto P(g) \in \mathbf{Q}_p\langle\mathbf{x}\rangle$ is a continuous homogeneous polynomial map of multi-degree α. Indeed, let $k = |\alpha|$ and consider the multilinear map

$$\begin{array}{rccc} T_k : & E^k & \longrightarrow & F \\ & (f_1, \cdots, f_k) & \longmapsto & f_1 \cdots f_k; \end{array}$$

it is continuous as $||T_k(f_1, \cdots, f_k)|| \le ||f_1|| \cdots ||f_k||$ and $P = T_k \circ p_\alpha$.

Furthermore, for a multi-index β, define $\phi_\beta : \mathbf{Q}_p\langle\mathbf{x}\rangle \to \mathbf{Q}_p\langle\mathbf{x}\rangle$ such that $\phi_\beta(g)$ is the homogeneous part of multi-degree β of g. Then, ϕ_β is linear and continuous, therefore if $P(\mathbf{x}) = \mathbf{x}^\alpha$, the map $g \in \mathbf{Q}_p\langle\mathbf{x}\rangle^d \mapsto P(\phi_{\beta_1}(g_1), \cdots, \phi_{\beta_d}(g_d))$ is a continuous homogeneous polynomial map of multi-degree α for any multi-index $(\beta_i)_{1\le i\le d}$.

For an integer k, $P_k(E^d, F)$ is the direct sum of the $P_\alpha(E,F)$ for α such that $|\alpha| = k$, the elements of $P_k(E^d,F)$ are the *continuous homogeneous polynomial maps of total degree* k.

Example 3.21. If $P \in \mathbf{Q}_p[\mathbf{x}]$ is a homogeneous polynomial of degree k in d variables, then the map $P : g \in \mathbf{Q}_p\langle\mathbf{x}\rangle^d \mapsto P(g)$ is a continuous homogeneous polynomial map of total degree k and for any sequence of multi-index $(\beta_i)_{1\le i\le d}$, the map $g \in \mathbf{Q}_p\langle\mathbf{x}\rangle^d \mapsto P(\phi_{\beta_1}(g), \cdots, \phi_{\beta_d}(g))$ also is.

We denote by $P(E^d,F)$ the direct sum of the spaces $P(E^d,F)$, its elements are the *continuous polynomial maps in* d *variables*.

Proposition 3.22. *Set* $E, F = \mathbf{Q}_p\langle\mathbf{x}\rangle$. *Take a polynomial* $P \in \mathbf{Q}_p[\mathbf{x}]$. *Then,* P *induces a continuous polynomial map* $E^d \to F$ *and the linear embedding* $\mathbf{Q}_p[\mathbf{x}] \hookrightarrow P(E^d,F)$ *is an isometry.*

Finally, the set $\widehat{P}(E^d,F)$ of *power series* in d variables over E is the (infinite) product of the $P_\alpha(E,F)$ (or of the $P_k(E^d,F)$) for $\alpha \in \mathbf{Z}_+^d$ (for $k \in \mathbf{Z}_+$) equipped with the product topology of the discrete topology over each factor; equivalently if $f = \sum_\alpha f_\alpha \in \widehat{P}(E^d,F)$, then the order of vanishing at 0 of f is $\mathrm{ord}(f) = \min\{|\alpha| : f_\alpha \neq 0\}$ and this is the topology induced by the norm $||f|| := 2^{-\mathrm{ord}(f)}$. The space $\widehat{P}(E^d,F)$ is complete Hausdorff for this topology. A *converging power series* is an element $f = \sum_\alpha f_\alpha$ of $\widehat{P}(E^d,F)$ such that there exists $R \in (\mathbf{R}_{>0})^d$ satisfying $\sup_\alpha R^\alpha ||f_\alpha||_{P_\alpha(E,F)} < +\infty$. If $f = \sum_\alpha f_\alpha$, then the *polyradius of convergence of* f is

$$r(f) := \sup\left\{R \in (\mathbf{R}_{>0})^d : R^\alpha ||f_\alpha|| \to 0 \text{ when } |\alpha| \to \infty\right\}.$$

Definition 3.23. Let $\mathcal{U}$ be an open subset of E^d, a map $f : \mathcal{U} \to F$ is *analytic* at a point $a \in \mathcal{U}$ if there exists a converging power series f_a such that for all x in a small neighbourhood of a in $\mathcal{U}$, $f(a+x) = f_a(x)$. The function f is analytic if it is analytic at every point of $\mathcal{U}$.

For any integer $m \ge 1$, a map $f : \mathcal{U} \to F^m$ is analytic if each of its coordinates is analytic.

Example 3.24. Every continuous linear map $\mathbf{Q}_p\langle\mathbf{x}\rangle^d \to \mathbf{Q}_p\langle\mathbf{x}\rangle^d$ is analytic.

Proposition 3.25. *The map* $\mathrm{Comp} : (h,f) \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d \times \mathbf{Z}_p\langle \mathbf{x}\rangle^d \mapsto h \circ f \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$ *is analytic. In particular, it is linear in* h.

Proof. It is enough to show that the map $\Phi : (h,f) \in \mathbf{Z}_p\langle \mathbf{x}\rangle \times \mathbf{Z}_p\langle \mathbf{x}\rangle^d \mapsto h \circ f \in \mathbf{Z}_p\langle \mathbf{x}\rangle$ is analytic. Let $(h,f) \in \mathbf{Z}_p\langle \mathbf{x}\rangle \times \mathbf{Z}_p\langle \mathbf{x}\rangle^d$, we show that Φ is analytic at (h,f). Let $g \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$ and write $h(\mathbf{x}) = \sum_\alpha a_\alpha \mathbf{x}^\alpha$, then

$$\begin{aligned} h \circ (f + g(\mathbf{x})) &= \sum_\alpha a_\alpha (f(\mathbf{x}) + g(\mathbf{x}))^\alpha \\ &= \sum_\alpha \sum_{\gamma \leq \alpha} a_\alpha \binom{\alpha}{\gamma} f(\mathbf{x})^{\alpha-\gamma} g(\mathbf{x})^\gamma \\ &= \sum_\beta \left(\sum_{\alpha \geq \beta} a_\alpha \binom{\alpha}{\beta} f(\mathbf{x})^{\alpha-\beta} \right) g(\mathbf{x})^\beta \\ &= \sum_\beta Q_{\beta,f}(h)(\mathbf{x}) \cdot g(\mathbf{x})^\beta \end{aligned}$$

where $Q_{\beta,f} : \mathbf{Q}_p\langle \mathbf{x}\rangle \to \mathbf{Q}_p\langle \mathbf{x}\rangle$ is a continuous linear map and $||Q_\beta|| \to 0$ when $\beta \to \infty$, this is a converging power series in the variables (h,g) of polyradius of convergence $(+\infty, 1)$. Therefore Φ is analytic at any point $(0,f)$ and by linearity in h, Φ is analytic at any point (h,f). □

Analytic manifolds.– Let $\mathbf{K}$ be an ultrametric field and let X be a topological space. A $\mathbf{K}$-*chart* of X is a homeomorphism $\phi : U \to \phi(U) \subset E$ where U in an open subset of X and E a Banach space over $\mathbf{K}$. We say that two $\mathbf{K}$-charts $\phi : U \to E, \psi : V \to F$ are *compatible* if

1. $\phi(U \cap V)$ is open in E and $\psi(U \cap V)$ is open in F.
2. $\psi \circ \phi^{-1} : \phi(U \cap V) \to F$ is analytic.
3. $\phi \circ \psi^{-1} : \psi(U \cap V) \to E$ is analytic.

An analytic manifold X over $\mathbf{K}$ is defined classically as a topological space equipped with an atlas of compatible $\mathbf{K}$-charts. For a point $x \in X$, the tangent space at x is denoted by $T_x X$. A function $f : X \to Y$ between two analytic manifolds is analytic if for every chart $\phi : U \subset X \to E, \psi : V \subset Y \to F$, the map $\psi \circ f \circ \phi^{-1} : \phi^{-1}(U) \to F$ is analytic. The differential of f at a point x will be denoted $D_x f$.

Proposition 3.26. *The topological space* $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ *is an analytic manifold over* $\mathbf{Q}_p$*, it is in fact an open subset of the Banach space* $\mathbf{Q}_p\langle \mathbf{x}\rangle^d$*. The subgroups* $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ *for* $c > \frac{1}{p-1}$ *are diffeomorphic to* $\mathbf{Z}_p\langle \mathbf{x}\rangle^d$ *and they form a basis of neighbourhood of* id *in* $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$.

Proof. Theorem 3.17 shows that $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ is the ball of center id and radius $|p|^c$ in $\mathbf{Z}_p\langle \mathbf{x}\rangle^d$, using Proposition 3.9 we see that for every $f \in \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$, the ball of center f and radius $|p|^c$ is included in $f \circ \mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ therefore it is an open set of $\mathbf{Q}_p\langle \mathbf{x}\rangle^d$, so $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ is an infinite dimensional analytic manifold over $\mathbf{Q}_p$. □

The implicit function theorem.– Let X, Y, Z be manifolds over $\mathbf{K}$ and let $f : X \times Y \to Z$ be an analytic map. Let $(a,b) \in X \times Y$, we write $D_{(a,b)} f$ the differential map of f at (a,b) and let $D^{(1)}_{(a,b)} f$ be the differential of the partial map $x \in X \mapsto f(x,b)$ at a and $D^{(2)}_{(a,b)} f$ the differential of the partial map $y \in Y \mapsto f(a,y)$ at b. Then, one has $T_{(a,b)} X \times Y = T_a X \times T_b Y$ and $D_{(a,b)} f(u,v) = D^{(1)}_{(a,b)} f \cdot u + D^{(2)}_{(a,b)} f \cdot v$.

Theorem 3.27 (Implicit function theorem, 5.6.1 of [Bou07b])**.** *Suppose that* $D^{(2)}_{(a,b)} f$ *is bijective, then there exists an open neighbourhood* U *of* a *in* X *and an open neighbourhood* V *of* b *in* Y *and a unique analytic map* $g : U \to V$ *such that*

$$\forall x \in U, \quad f(x, g(x)) = f(a,b)$$

and the differential of g *at any* $x \in \mathcal{U}$ *is given by*

$$D_x g = -\left(D^{(2)}_{(x,g(x))} f \right)^{-1} \circ D^{(1)}_{(x,g(x))} f$$

Proposition 3.28. *The inversion map* $\mathrm{Inv} : f \in \mathrm{Diff}^{an}(\mathbf{Z}_p^d) \mapsto f^{-1}$ *is analytic.*

Proof. We write $\mathcal{U} = \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$, we know that $\mathcal{U}$ is an analytic manifold over $\mathbf{Q}_p$ by Proposition 3.26. By Proposition 3.25, the composition operation is analytic over $\mathbf{Z}_p\langle \mathbf{x}\rangle^d \times \mathbf{Z}_p\langle \mathbf{x}\rangle^d$, therefore it is over $\mathcal{U} \times \mathcal{U}$.

To show that Inv is analytic we only need to show that it is analytic at id. Indeed, take $f \in \mathcal{U}$, then $\mathrm{Inv} = L_{f^{-1}} \circ \mathrm{Inv} \circ R_{f^{-1}}$ where $R_{f^{-1}}$ is composition on the right by f^{-1} and $L_{f^{-1}}$ composition on the left. Since $L_{f^{-1}}$ and $R_{f^{-1}}$ are analytic, Inv is analytic at f if and only if it is analytic at id. To show that Inv is analytic at id, we use the implicit function theorem, since the map $M : (f,g) \in \mathcal{U} \times \mathcal{U} \to f \circ g \in \mathcal{U}$ is analytic and the partial differential $D^{(2)}_{\mathrm{id},\mathrm{id}} M = \mathrm{id}$, one has the existence of a unique function $G : \mathcal{V} \to \mathcal{U}$ with $\mathcal{V}$ an open neighbourhood of id such that G is analytic at id and $M(f, G(f)) = \mathrm{id}$ for all $f \in \mathcal{V}$. Therefore $\mathrm{Inv}_{|\mathcal{V}} = G$ and inversion is analytic at id. □

3.3 p-adic Lie groups

We refer to [Bou06] for more details on the results provided in this section.

A p-adic Lie group G is a topological group with a structure of a p-adic analytic manifold such that the multiplication map and the inverse map are analytic. The dimension of G is its dimension as an analytic manifold. It can be infinite. Its *Lie algebra* $\mathfrak{g}$ is the tangent space of G at the neutral element, it is equipped with a Lie bracket $[\cdot,\cdot]$ defined as follows. Let $g \in G$ and $\iota_g : h \in G \mapsto ghg^{-1}$, then $\mathrm{Ad}(g) := D_e\iota_g \in \mathrm{GL}(\mathfrak{g})$ is the adjoint representation of G. Define $\mathrm{ad} := D_e \mathrm{Ad}$, then

$$\forall \mathbf{X}, \mathbf{Y} \in \mathfrak{g}, [\mathbf{X}, \mathbf{Y}] := \mathrm{ad}(\mathbf{X})(\mathbf{Y}).$$

Theorem 3.29. *The topological group* $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ *is an infinite-dimensional Lie group over* $\mathbf{Q}_p$*. Its Lie Algebra is* $\Theta(\mathbf{Z}_p^d)$*.*

Moreover, the subgroups $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ *are also Lie groups for* $c > \frac{1}{p-1}$ *and they form a basis of neighbourhood of* id *in* $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$*.*

Proof. The fact that $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ is a Lie group over $\mathbf{Q}_p$ follows from Propositions 3.25, 3.26 and 3.28 where it was shown that it was an analytic manifold and that composition and inversion are analytic maps. The statement for $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ follows from the same propositions.

The tangent space at id is $\mathbf{Q}_p\langle \mathbf{x}\rangle^d$ that we identify with $\Theta(\mathbf{Z}_p^d)$ and under this identification the Lie bracket between two Tate-analytic vector fields corresponds to the Lie bracket of the Lie algebra of the Lie group $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ because if $\mathbf{X}, \mathbf{Y}$ are of norm $\leq |p|^c$ with $c > \frac{1}{p-1}$, then they admit global Tate-analytic flows $\Phi^{\mathbf{X}}$ and $\Phi^{\mathbf{Y}}$ by Proposition 3.13 and

$$\begin{aligned}[\mathbf{X}, \mathbf{Y}] &= \tfrac{\partial}{\partial s}_{|s=0} \tfrac{\partial}{\partial t}_{|t=0} \Phi^{\mathbf{X}}_{-s} \circ \Phi^{\mathbf{Y}}_t \circ \Phi^{\mathbf{X}}_s \\ &= \tfrac{\partial}{\partial s}_{|s=0} \tfrac{\partial}{\partial t}_{|t=0} \iota_{\Phi^{\mathbf{X}}_s}(\Phi^{\mathbf{Y}}_t) \\ &= D_{\mathrm{id}} \mathrm{Ad}(\mathbf{X})(\mathbf{Y}) = \mathrm{ad}(\mathbf{X})(\mathbf{Y}).\end{aligned}$$

On the other hand, if $f, g \in \mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ with $c > \frac{1}{p-1}$, then $\frac{\partial}{\partial s}_{|s=0} \frac{\partial}{\partial t}_{|t=0} \Phi^f_{-s} \circ \Phi^g_t \circ \Phi^f_s = [\mathbf{X}_f, \mathbf{X}_g] = \mathrm{ad}\, \mathbf{X}_f(\mathbf{X}_g)$. □

Remark 3.30. Since Bell-Poonen theorem holds for any ultrametric field, the same proof shows that $\mathrm{Diff}^{an}(\mathbf{D}_p^d)$ is a Lie group over $\mathbf{C}_p$. In fact, for any complete extension $\mathbf{K}$ of $\mathbf{Q}_p$ with unit ball $\mathbf{A}$, the group $\mathrm{Diff}^{an}(\mathbf{A}^d)$ is a Lie group over $\mathbf{K}$.

Theorem 3.31 ([Bou06], §8, Theorem 1)**.** *Let* G, H *be Lie groups over* $\mathbf{Q}_p$ *and* $\phi : G \to H$ *be a continuous homomorphism of topological groups. Then,* ϕ *is analytic and therefore a homomorphism of Lie groups.*

Remark 3.32. The proof relies heavily on $\mathbf{Q}$ being dense in $\mathbf{Q}_p$ and the theorem is false if we replace $\mathbf{Q}_p$ by any finite extension of $\mathbf{Q}_p$. Indeed, suppose for example that $K = \mathbf{Q}_p(\sqrt{\alpha})$ is a quadratic extension. Any element z of $\mathbf{K}$ is of the form $z = x + \sqrt{\alpha}y$. Then, the function

$$f : z = x + \sqrt{\alpha}y \mapsto x - \sqrt{\alpha}y$$

is a continuous group homomorphism, it is $\mathbf{Q}_p$-analytic but not $\mathbf{K}$-analytic as $f_{|1\cdot\mathbf{Q}_p} = \mathrm{id}$ and $f_{|\sqrt{\alpha}\cdot\mathbf{Q}_p} = -\mathrm{id}$.

Let Γ be a finitely generated group, the pro-p completion Γ_p of Γ is the projective limit of the quotient of Γ that are finite p-groups, it is a topological group with respect to the profinite topology. In particular, for any $\gamma \in \Gamma$, the group homomorphism $n \in \mathbf{Z} \mapsto \gamma^n \in \Gamma$ extends uniquely to a continuous group homomorphism $t \in \mathbf{Z}_p \mapsto \gamma^t \in \Gamma_p$. In the context of Tate-analytic diffeomorphisms, if $p \geq 3$ and $f \equiv \mathrm{id} \mod p$, then the extension $n \in \mathbf{Z} \mapsto f^n \in \mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ is the Tate-analytic flow $t \in \mathbf{Z}_p \mapsto \Phi_t^f \in \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ associated to f given by Bell-Poonen theorem.

Proposition 3.33. *Let* p *be a prime, let* $c > 0$ *be such that* $c > \frac{1}{p-1}$ *and let* G *be a compact Lie group over* $\mathbf{Q}_p$*. Let* Γ *be a finitely generated subgroup of* G *such that* G *is the pro-*p*-completion of* Γ *and let* $\iota : \Gamma \to \mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ *be a group homomorphism, then* ι *extends uniquely to a Lie group homomorphism* $\iota : G \to \mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ *such that for all* $t \in \mathbf{Z}_p$*, all* $g \in \Gamma$*,* $\iota(g^t) = \iota(g)^t$ *and the map* $(t, \mathbf{x}) \in \mathbf{Z}_p \times \mathbf{Z}_p^d \mapsto \iota(g)^t(\mathbf{x})$ *is analytic.*

Proof. Theorem 2.11 of [CX18] shows that ι extends uniquely to a continuous map. In [CX18] this is only shown when $p \geq 3$ and $c = 1$ but the proof is identical with $p \geq 2$ and $c > \frac{1}{p-1}$ at it is only required that the image of the elements of Γ admits a Tate-analytic flow. Since G and $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ are both Lie groups over $\mathbf{Q}_p$, ι is automatically a Lie group homomorphism by Theorem 3.31. □

Theorem 3.34 ([Bou06], §8, Theorem 2)**.** *Let* G *be a finite-dimensional Lie group over* $\mathbf{Q}_p$*, then every closed subgroup of* G *is a Lie subgroup of* G*.*

Proposition 3.35 ([Bou06], §9, Corollary of Proposition 6)**.** *Let* G *be a finite-dimensional Lie group over* $\mathbf{Q}_p$ *and* $\mathfrak{g}$ *its Lie algebra, there exists an open subgroup* G_0 *of* G *such that for all* $i \geq 0$*, the subgroups* $D^i(G_0)$ *and* $D_i(G_0)$ *are Lie subgroups with Lie algebra* $\mathcal{D}^i(\mathfrak{h})$ *and* $\mathcal{D}_i(\mathfrak{h})$ *respectively.*

3.4 Nilpotent groups and embedding into p-adic Lie groups.

3.4.1 Nilpotent groups

The main goal of this section is to show that if H is a finitely generated nilpotent group with generators $h_1, \dots, h_s$, then for any $m \geq 1$ the subgroup H_m of H generated by $h_1^m, \dots, h_s^m$ is a finite index subgroup of H. This will be useful in the proof of Theorem B because if $H \subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ we will need to consider such a subgroup H_m to get the desired result.

Recall the notation introduced in § 1.2.1 for nilpotent and solvable groups and Lie algebras. We shall say that an expression that involves k commutator brackets is a commutator of length k; for instance $[[a,[b,c]],d]$ is a commutator of length 3 and a single element can be viewed as a commutator of length 0. For $k \geq 1$, we denote by $[a_1; \cdots ; a_k]$ the commutator $[a_1, [a_2, \cdots, [a_{k-1}, a_k] \cdots]$; its length is k.

Let G, G', G'' be groups, a map $\phi : G \times G' \to G''$ is *bilinear* if for every $g \in G, g' \in G'$, the maps $\phi(g, \cdot)$ and $\phi(\cdot, g')$ are group homomorphisms. More generally, a map $G_1 \times \cdots \times G_m \to G$ is m-linear if fixing $m-1$ coordinates yields a group homomorphism. For any triple of elements x, y, z in G, we have

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

The image of the map $(a,b) \mapsto [a,b]$ from $G \times D^{k-1}(G)$ to $D^k(G)$ generates $D^k(G)$. It follows from the last three formulas that, for every $k \geq 1$, this map induces a bilinear map

$$\mathrm{co}_k : G \times D^{k-1}(G) \mapsto D^k(G)/D^{k+1}(G)$$

and the image $\mathrm{Im}\,\mathrm{co}_k$ generates $D^k(G)/D^{k+1}(G)$.

Proposition 3.36. *Let G be a group and S a set of generators of G.*

1. *for every integer $k \geq 0$, the subgroup $D^k(G)/D^{k+1}(G)$ is generated by the commutators of length k consisting of elements of S.*
2. *if G is finitely generated, then $D^k(G)/D^{k+1}(G)$ is finitely generated for every $k \geq 0$.*
3. *If G is nilpotent, then $D^{\mathrm{nilp}(G)-1}(G)$ is generated by the commutators of length $\mathrm{nilp}(G)-1$ in elements of S.*

Proof. Let us prove the first assertion by induction on k. Let X_k be the set of commutators of length k in elements of S. The initialization $k=0$ follows from $X_0 = S$ and the fact that S generates G. Now, suppose $k \geq 1$ and that X_{k-1} generates $D^{k-1}(G)/D^k(G)$. The image of the map co_k generates $D^k(G)/D^{k+1}(G)$; by induction and since $\mathrm{co}_k(a,b)$ is a homomorphism with respect to a and with respect to b, the elements $[s, x_{k-1}]$ for s in S and $x_{k-1} \in X_{k-1}$ generate $D^k(G)/D^{k+1}(G)$, and these elements are exactly the commutators of length k in the elements of S. The second and third assertions follow from the first one. □

Proposition 3.37. *Let H be a finitely generated nilpotent group, then every subgroup H_0 of H is finitely generated.*

For a proof see [Seg83] where this is actually shown for polycyclic groups, the result follows since finitely generated nilpotent groups are polycyclic.

Proposition 3.38. *Let H be a nilpotent group of nilpotency class t.*

1. *the map $\mathrm{Br}_t : H^t \to D^{t-1}, (h_1, \cdots, h_t) \mapsto [h_1; h_2; \cdots ; h_t]$ is multilinear.*
2. *If $\{h_1, \cdots, h_s\}$ generates H, then for every $m \geq 1$, the subgroup generated by $\{h_1^m, \cdots, h_s^m\}$ is of finite index in H.*

Proof of the first assertion. Let us do an induction on t. The case $t=1$ being trivial, suppose the result true for a nilpotent group of class $t-1$ and consider H a nilpotent group of class t. Since $D^t(H) = 0$, one has that the map $\mathrm{co}_{t-1} : (h_1, h) \in H \times D^{t-2}(H)/D^{t-1}(H) \mapsto [h;x] \in D^{t-1}(H)$ is bilinear; thus, Br_t is a homomorphism with respect to the first factor $h_1 \in H$. Let us show that Br_t is a homomorphism in the second coordinates h_2, the other coordinates are dealt with in the same way. By induction, the map

$$\mathrm{Br}_{t-1}^{H/D^{t-1}(H)} : (H/D^{t-1}(H))^{t-1} \to D^{t-2}(H)/D^{t-1}(H)$$

is multilinear. Take $h_1, h_2, h_2', h_3, \cdots, h_{t-1} \in H$, the multilinearity of $\mathrm{Br}_{t-1}^{H/D^{t-1}(H)}$ provides an element $g \in D^{t-1}(H)$ such that

$$[h_1; h_2 h_2'; \cdots ; h_{t-1}] = [h_1, [h_2; \cdots ; h_{t-1}] \cdot [h_2'; \cdots ; h_{t-1}] \cdot g]$$

and the bilinearity of co_{t-1} gives the result since $[h_1, g] = 0$.

□

Proof of the second assertion. We set $S = \{h_1, \cdots, h_s\}$ and we denote by $H_{S,m}$ the subgroup of H generated by the set $\{s^m : s \in S\}$. We show by induction on $t = \mathrm{nilp}(H)$ that $H_{S,m}$ is of finite index in H.

If $t = 1$ then H is abelian and there is a unique surjective group homomorphism $\mathbf{Z}^s \to H$ sending the canonical basis to $S = (h_1, \cdots, h_s)$. The subgroup $H_{S,m}$ is the image of $m\mathbf{Z}^s$. Therefore, there is a surjective group homomorphism $\mathbf{Z}^s/m\mathbf{Z}^s \twoheadrightarrow H/H_{S,m}$ and we get that $H/H_{S,m}$ has at most m^s elements.

Now suppose the result true for a group of nilpotency class $t-1$ and assume $\mathrm{nilp}(H) = t$, with $t \geq 2$. Set $T := D^{t-1}(H)$, T is central in H. One has the exact sequence

$$1 \to T \to H \to H/T \to 1.$$

By induction, the image of $H_{S,m}$ in H/T is of finite index; thus, one can fix a finite set $A \subset H$ such that $H = \bigsqcup_{h \in A} hH_{S,m}T$. To conclude, we only need to show that the index of $T \cap H_{S,m}$ in T is finite. Since, $T \cap H_{S,m}$ contains the subgroup of $t-1$ commutators $D^{t-1}(H_{S,m})$ it suffices to show that the index of $D^{t-1}(H_{S,m})$ in T is finite.

By Proposition 3.36, T is generated by the set $S' = \{[x_1; \cdots; x_{t-1}] : x_i \in S\}$ and $D^{t-1}(H_{S,m})$ is generated by the set $S'' = \{[x_1^m; \cdots; x_{t-1}^m] : x_i \in S\}$ furthermore, the first assertion shows that S'' consists exactly of the elements of S' raised to the power m^{t-1}. So by the abelian case, $D^{t-1}(H_{S,m})$ is of finite index in T.

□

3.4.2 Malcev's completion of nilpotent torsion-free finitely generated group

Denote by $\widehat{\mathbf{Z}} = \prod_{p \text{ prime}} \mathbf{Z}_p$ equipped with the product topology (the adelic topology). It is the profinite completion of $\mathbf{Z}$. Let H be a nilpotent torsion-free finitely generated group. It is known that H embeds into $\mathrm{Tri}_1(n, \mathbf{Z})$ the group of upper triangular matrices with integer coefficients and 1's on the diagonal for some integer n (see for example [Seg83] Theorem 2 of Chapter 5). For the rest of this section, we fix an embedding $\iota : H \hookrightarrow \mathrm{Tri}_1(n, \mathbf{Z})$. There are two topologies that one can consider on $\iota(H)$. First the adelic topology induced by the inclusion $\mathrm{Tri}_1(n, \mathbf{Z}) \subset \mathrm{Tri}_1(n, \widehat{\mathbf{Z}})$, and second, the profinite topology where a basis of neighbourhood for the neutral element are the subgroups of finite index in $\iota(H)$.

Proposition 3.39. *Let $G \subset \mathrm{Tri}_1(n, \mathbf{Z})$ be a subgroup of matrices with integer coefficients and 1's on the diagonal, then the profinite topology and the adelic topology on G are the same. In particular, the profinite completion of G coincides with the closure of G in $\mathrm{Tri}_1(n, \widehat{\mathbf{Z}})$.*

Proof. First, let K be a subgroup of $\mathrm{GL}_n(\mathbf{Z})$ of the form $K = \{A \in \mathrm{GL}_n(\mathbf{Z}) : A \equiv \mathrm{id} \mod m\}$ for some integer m, such groups K form a basis of open neighbourhood of id for the adelic topology. It is a normal subgroup of $\mathrm{GL}_n(\mathbf{Z})$ with finite quotient, therefore $G \cap K$ is a finite index subgroup of G. Therefore the adelic topology is finer than the profinite topology.

Conversely, G is a unipotent group of matrices over $\mathbf{Q}$, therefore it is arithmetic (see [Seg83] Exercise 13 of Chapter 6). By the affirmative solution to the congruence subgroup problem for arithmetic soluble groups (see [Cha80]), we get that G is a congruence subgroup. This means that every finite index subgroup of G contains a subgroup of the form $G \cap \{A \in \mathrm{GL}_n(\mathbf{Z}) : A \equiv \mathrm{id} \mod m\}$ for some integer m. Therefore, the profinite topology is finer than the adelic topology; thus, they are the same. □

A consequence of this proposition is that the profinite completion of $\iota(H)$ is exactly the closure of $\iota(H)$ in $\mathrm{Tri}_1(n, \widehat{\mathbf{Z}})$.

Proposition 3.40. *Let G be a nilpotent subgroup of $\mathrm{Tri}_1(n, \mathbf{Z})$. The closure of G in $\mathrm{Tri}_1(n, \mathbf{Z}_p)$ is the pro-p-completion of G, in particular it is a p-adic Lie group.*

Proof. Denote by $\widehat{G}$ the profinite completion of G and for a prime ℓ, G_ℓ the pro-ℓ-completion of G. Since G is nilpotent and a finite nilpotent group is a product of ℓ-groups for some primes ℓ (see [Bou70] chapter 1, §7, Theorem 4) we have that $\widehat{G} = \prod_\ell G_\ell$. By Proposition 3.39, we have a continuous injective homomorphism of topological groups

$$\widehat{G} = \prod_\ell G_\ell \hookrightarrow \mathrm{Tri}_1(n, \widehat{\mathbf{Z}}) = \prod_\ell \mathrm{Tri}_1(n, \mathbf{Z}_\ell).$$

For a prime p, this induces a continuous group homomorphism $G_p \hookrightarrow \prod_\ell \mathrm{Tri}_1(n, \mathbf{Z}_\ell)$. But, G_p is a pro-p-group and for every prime ℓ, $\mathrm{Tri}_1(n, \mathbf{Z}_\ell) = \varprojlim \mathrm{Tri}_1(n, \mathbf{Z}/\ell^k\mathbf{Z})$ is a pro-ℓ-group. Therefore, G_p can be identified with the image of $\widehat{G}$ in $\mathrm{Tri}_1(n, \mathbf{Z}_p)$; this is exactly the completion of G in $\mathrm{Tri}_1(n, \mathbf{Z}_p)$, meaning that G_p is a closed subgroup of the p-adic Lie group $\mathrm{Tri}_1(n, \mathbf{Z}_p)$, so it is a Lie group by Theorem 3.34. □

Theorem 3.41. *Let $c > 0$ be such that $c > \frac{1}{p-1}$ and let H be a finitely generated nilpotent subgroup of $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$, then the closure $\bar{H}$ of H in $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ is a finite-dimensional nilpotent Lie group.*

Furthermore, denote by $\mathfrak{h}$ the Lie algebra of $\bar{H}$, then $\mathfrak{h}$ is a finite-dimensional nilpotent Lie algebra and $\mathrm{dl}(\mathfrak{h}) \geq \mathrm{vdl}(H)$.

Proof. Set $G = \iota(H)$ and $\psi := \iota^{-1} : G \to \mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$. By Proposition 3.40 and Proposition 3.33, ψ extends to a Lie group homomorphism $\psi : G_p \to \mathrm{Diff}_c^{an}(\mathbf{Z}_p^d)$ where G_p is the closure of G in $\mathrm{Tri}_1(n, \mathbf{Z}_p)$; we show that the image of ψ is the closure of H in $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$.

Let K be the image of ψ. Since $\mathrm{Tri}_1(n, \mathbf{Z}_p)$ is compact and G_p is closed, G_p is also compact and so is K. This implies that the closure $\overline{H}$ of H is included in K. And K is included in $\overline{H}$ because of the continuity of ψ. This shows that $\overline{H}$ is a finite dimensional Lie group isomorphic to $G_p/\ker\psi$.

Now, we show the statement for $\mathfrak{h}$. By Proposition 3.35, there exists an open subgroup H_1 of $\overline{H}$, such that $D^i(H_1)$ is a Lie subgroup of $\overline{H}$ with Lie algebra $\mathcal{D}^i(\mathfrak{h})$. Since H_1 is open, by Theorem 3.29 there exists an integer $c > 0$ such that $\mathrm{Diff}_c^{an}(\mathbf{Z}_p^d) \cap H \subset H_1$. Take $f_1, \cdots, f_s$ generators of H. Then by Proposition 3.38 the subgroup H' generated by the $f_i^{p^c}$'s is a finite index subgroup of H and it is included in H_1 by Lemma 3.10, therefore $\mathrm{dl}(\mathfrak{h}) = \mathrm{dl}(H_1) \geq \mathrm{dl}(H') \geq \mathrm{vdl}(H)$. □

4 Finitely generated nilpotent groups

4.1 Base change from C to $\mathbf{Z}_p$: Good models

To prove Theorem B, we shall ultimately apply Theorem 3.41. Thus, we need a method to transfer problems regarding groups of automorphisms defined over $\mathbf{C}$ to similar problems on groups of Tate analytic diffeomorphisms over $\mathbf{Z}_p$, for certain primes p.

Theorem 4.1 (Lech, see [Lec53])**.** *Let $\mathbf{K}$ be a finitely generated field over $\mathbf{Q}$ and let S be a finite subset of $\mathbf{K}$. Then there exists an infinite number of prime numbers p with an embedding $\mathbf{K} \hookrightarrow \mathbf{Q}_p$ such that all elements of S are mapped to $\mathbf{Z}_p$.*

Let X be an irreducible quasiprojective variety over $\mathbf{C}$ and Γ a finitely generated subgroup of $\mathrm{Aut}(X_{\mathbf{C}})$.

- Let R be an integral domain. We say that (X, Γ) is *defined over* R, if there exists an irreducible separated reduced scheme X_R over R and an injective homomorphism $\Gamma \hookrightarrow \mathrm{Aut}_{\mathbf{R}}(X_{\mathbf{R}})$ such that X and Γ are obtained by the base change $X = X_R \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \mathbf{C}$.
- Let p be a prime number. A *model* of (X, Γ) over $\mathbf{Z}_p$ is the data of
  - (i) A ring $R \subset \mathbf{C}$ over which (X, Γ) is defined and an embedding $R \hookrightarrow \mathbf{Z}_p$.
  - (ii) An irreducible variety $\mathcal{X}$ over $\mathbf{Z}_p$ and an injective homomorphism $\rho : \Gamma \hookrightarrow \mathrm{Aut}_{\mathbf{Z}_p}(\mathcal{X})$ such that
$$\mathcal{X} \simeq X_R \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \mathbf{Z}_p.$$
  is the base change of X_R and for all $f \in \Gamma$, $\rho(f)$ is the base change of f.
- A *good model* over $\mathbf{Z}_p$ of (X, Γ) is the data of a model of (X, Γ) with the additional condition that the special fiber $\mathcal{X}_{\mathbf{F}_p} = \mathcal{X} \times_{\mathrm{Spec}\, \mathbf{Z}_p} \mathrm{Spec}\, \mathbf{F}_p$ is geometrically reduced and irreducible and of dimension
$$\dim_{\mathbf{F}_p}(\mathcal{X}_{\mathbf{F}_p}) = \dim_{\mathbf{Q}_p}(\mathcal{X} \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \mathbf{Q}_p).$$

Proposition 4.2 (Proposition 4.4 of [BGT10], Proposition 3.2 of [CX18])**.** *Let X be an irreducible complex quasi-projective variety, $\alpha \in X(\mathbf{C})$ and Γ be a finitely generated subgroup of $\mathrm{Aut}_{\mathbf{C}}(X)$. Then, there exists an infinite number of primes $p \geq 3$ such that (X, Γ) has a good model $\mathcal{X}$ over $\mathbf{Z}_p$ and such that α extends to a section $\alpha : \mathrm{Spec}\, \mathbf{Z}_p \to \mathcal{X}$.*

Example 4.3. For simplicity, suppose X is the affine space $\mathbf{A}_{\mathbf{C}}^d$ with its standard coordinates $x_1, \cdots, x_d$ and $\Gamma \subset \mathrm{Aut}(\mathbf{A}_{\mathbf{C}}^d)$ is a finitely generated group of polynomial automorphisms. This is already an interesting example. Let S be a finite symmetrical ($S^{-1} = S$) set of generators of Γ. Let R be the ring generated by all the coefficients of the elements of S and the coordinates of α. Then, (X, Γ) is defined over R. Plus, by Theorem 4.1 there exists a prime p and an embedding $\iota : R \hookrightarrow \mathbf{Z}_p$. Using this embedding, the base change $\mathcal{X} = \mathbf{A}_{\mathbf{Z}_p}^d$ and $\rho : \Gamma \hookrightarrow \mathrm{Aut}(\mathbf{A}_{\mathbf{Z}_p}^d)$ show that $(\mathbf{A}^d, \Gamma)$ is a good model over $\mathbf{Z}_p$ and α extends to a $\mathbf{Z}_p$-point of $\mathcal{X}$.

4.2 From algebraic automorphisms to analytic diffeomorphisms over $\mathbf{Z}_p$

In this section, we consider a scheme $\mathcal{X}$ of dimension d over $\mathbf{Z}_p$, where $p \geq 3$ is a prime number, such that

- $\mathcal{X}$ is a quasi-projective variety over $\mathbf{Z}_p$, and its generic fiber is geometrically irreducible over $\mathbf{Q}_p$.
- $\overline{\mathcal{X}} = \mathcal{X} \times_{\mathrm{Spec}\, \mathbf{Z}_p} \mathrm{Spec}\, \mathbf{F}_p$ is the special fiber of $\mathcal{X}$ and is geometrically irreducible over $\mathbf{F}_p$.
- $f : \mathcal{X} \to \mathcal{X}$ is an automorphism of $\mathbf{Z}_p$-schemes.
- $\overline{f} : \overline{\mathcal{X}} \to \overline{\mathcal{X}}$ is the restriction of $\mathcal{X}$ to the special fiber.
- $r : \mathcal{X}(\mathbf{Z}_p) \to \overline{\mathcal{X}}(\mathbf{F}_p)$ is the reduction map.

- x is a smooth $\mathbf{F}_p$-point and there exists $\alpha \in \mathcal{X}(\mathbf{Z}_p)$ such that $r(\alpha) = x$.

For the two next propositions, we refer to [BGT10]. They will enable us to go from algebraic automorphisms to analytic diffeomorphisms.

Proposition 4.4. *Let $\mathcal{X}$ be a quasi-projective scheme over $\mathbf{Z}_p$. There exists a function $\iota : \mathbf{Z}_p^d \to \mathcal{X}(\mathbf{Z}_p)$ which induces an analytic bijection between $\mathbf{Z}_p^d$ and the open subset of $\mathcal{X}(\mathbf{Z}_p)$ consisting of the points β such that $r(\beta) = x$.*

Proposition 4.5. *Suppose that $\bar{f}(x) = x$. Let $\iota : \mathbf{Z}_p^d \to \mathcal{X}(\mathbf{Z}_p)$ be the function defined in Proposition 4.4. Then there exist analytic functions $F_1, \cdots, F_d \in \mathbf{Z}_p\langle T_1, \cdots, T_d\rangle$ such that*

(i) One has

$$\iota^{-1} \circ f \circ \iota = (F_1, \cdots, F_d) =: \mathcal{F} \in \mathbf{Z}_p\langle T_1, \cdots, T_d\rangle^d.$$

(ii) if $\bar{\mathcal{F}}$ is the reduction mod p of $\mathcal{F}$, then $\bar{\mathcal{F}} = \mathcal{F}_0 + \mathcal{F}_1$ with $\mathcal{F}_0 \in (\mathbf{Z}/p\mathbf{Z})^d$ and $\mathcal{F}_1 \in \mathrm{GL}_d(\mathbf{Z}/p\mathbf{Z})$.

Furthermore $\mathcal{F}$ is a Tate-analytic diffeomorphism because f is an automorphism.

Example 4.6. Propositions 4.4 and 4.5 are proven in [BGT10]. We only do the proof in the case $\mathcal{X} = \mathbf{A}^d_{\mathbf{Z}_p}$. Take standard coordinates $\mathbf{x} = x_1, \cdots, x_d$ over $\mathcal{X}$. Then, $\mathcal{X} = \operatorname{Spec} \mathbf{Z}_p[\mathbf{x}]$ and $\overline{\mathcal{X}} = \operatorname{Spec} \mathbf{F}_p[\mathbf{x}]$. The reduction map $r : \mathcal{X}(\mathbf{Z}_p) = \mathbf{Z}_p^d \to \overline{\mathcal{X}}(\mathbf{F}_p) = \mathbf{F}_p^d$ is the reduction mod p coordinates by coordinates.

Take $x \in \mathbf{F}_p^d$ and $z \in \mathbf{Z}_p^d$ such that $r(z) = x$, then the open subset of $\mathcal{X}(\mathbf{Z}_p)$ of elements β such that $r(\beta) = x$ is the ball of center z and radius $1/p$. The analytic bijection ι is given by $\iota : m \in \mathbf{Z}_p^d \mapsto z + p \cdot m \in \mathcal{X}(\mathbf{Z}_p) = \mathbf{Z}_p^d$. This proves Proposition 4.4.

Now, take a polynomial automorphism f, the map $\overline{f}$ is the polynomial automorphism over $\mathbf{F}_p^d$ obtained when taking the coefficients of $f \mod p$. Take a point $x \in \mathbf{F}_p^d$ such that $\bar{f}(x) = x$, up to a conjugation by a translation (which does not change the result), we can suppose that $x = 0 \in \mathbf{F}_p^d$. This means that f preserves the ball of center 0 and radius $1/p$ in $\mathbf{Z}_p^d$. Writing f in coordinates, we have

$$f(\mathbf{x}) = pa_0 + A_1(\mathbf{x}) + A_2(\mathbf{x}) + \cdots$$

where $a_0 \in \mathbf{Z}_p^d$ and A_i is the homogeneous part of degree i of f. Then,

$$\iota^{-1} \circ f \circ \iota(\mathbf{x}) = \frac{1}{p} f(p\mathbf{x}) = a_0 + A_1(\mathbf{x}) + \sum_{k \geq 2} p^{k-1} A_k(\mathbf{x}).$$

This is indeed an element of $\mathbf{Z}_p\langle \mathbf{x}\rangle^d$ and $\overline{\frac{1}{p} f(p\mathbf{x})}$ is an invertible affine transformation of $\mathbf{F}_p^d$, this proves Proposition 4.5.

Proposition 4.7. *[Proposition 3.3 of [CX18]] Let Γ be a finitely generated subgroup of $\mathrm{Aut}_{\mathbf{Z}_p}(\mathcal{X})$. There exists a finite index subgroup $\Gamma_0 \subset \Gamma$ and an open subset $\mathcal{U} \subset \mathcal{X}(\mathbf{Z}_p)$ analytically diffeomorphic to $\mathbf{Z}_p^d$ such that $\mathcal{U}$ is stable by the action of Γ_0 on $\mathcal{X}$ and this action over $\mathcal{U}$ is conjugated to the action of a subgroup of $\mathrm{Diff}_1^{an}(\mathcal{U})$.*

Proof. Since $r(\alpha) = x \in \overline{\mathcal{X}}(\mathbf{F}_p)$, the set $\overline{\mathcal{X}}(\mathbf{F}_p)$ is not empty and since $\overline{\mathcal{X}}$ has finitely many $\mathbf{F}_p$-points, there exists a finite index subgroup $\Gamma_1 \subset \Gamma$ that acts trivially on $\overline{\mathcal{X}}(\mathbf{F}_p)$. The point x is fixed by Γ_1, let ι be as in Proposition 4.4 and $\mathcal{U}$ the open subset of $\mathcal{X}(\mathbf{Z}_p)$ consisting of the points β such that $r(\beta) = x$. Therefore, Γ_1 preserves $\mathcal{U}$ and by applying Proposition 4.5 to the elements of Γ_1, we get that conjugation by ι induces a group homomorphism $\Gamma_1 \hookrightarrow \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$. Composing this embedding with the homomorphism of reduction mod p induces a group homomorphism from Γ_1 to the finite group of affine transformations of $(\mathbf{Z}/p\mathbf{Z})^d$. Denote by Γ_0 the kernel of this homomorphism and the theorem is proven. □

4.3 Proof of Theorem B

Take H a finitely generated nilpotent group acting by algebraic automorphisms on a quasi-projective variety X over a field of characteristic zero.

We are first going to show that we can suppose X to be irreducible in order to work on a $\mathbf{Z}_p$-scheme: X has a finite number of irreducible components and H permutes them. So there exists a finite index subgroup $H' \subset H$ that stabilizes every irreducible component X_i of X. Call H_i the restriction of H' to X_i, then $H' = \prod H_i$ and $\mathrm{vdl}(H') = \min \mathrm{vdl}(H_i)$. We replace X by one of its irreducible component of maximal dimension and H by H' restricted to this component, H' is also finitely generated by Proposition 3.37.

Let $\alpha \in X(\mathbf{C})$, X is then an irreducible complex quasi-projective variety of dimension d, by proposition 4.2, there exists a prime number $p \geq 3$ such that (X, H) admits a good model $\mathcal{X}$ over $\mathbf{Z}_p$ and such that α extends to a $\mathbf{Z}_p$-point of $\mathcal{X}$. Now, by Proposition 4.7, there exists a finite index subgroup $H_0 \subset H$ which is isomorphic to a subgroup of $\mathrm{Diff}_1^{an}(\mathcal{U})$, for $\mathcal{U}$ an open subset of $\mathcal{X}(\mathbf{Z}_p)$ analytically diffeomorphic to $\mathbf{Z}_p^d$. By Proposition 3.37, H_0 is a finitely generated nilpotent subgroup of $\mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$. Using Theorem 3.41, we get that the Lie algebra $\mathfrak{h}$ associated to H_0 is nilpotent and $\mathrm{dl}(\mathfrak{h}) \geq \mathrm{vdl}(H_0) \geq \mathrm{vdl}(H)$. Applying Theorem 3.16, we get $d \geq \mathrm{vdl}(H)$.

4.4 Optimality of Theorem B

An example from [ET79].– We will use the construction from [ET79] to find groups where Theorem B is optimal.

Let n be an integer and let A be the matrix such that $A(e_i) = e_{i+1}, 1 < i \leq n$ where e_i is the canonical basis. Consider the subgroup of affine transformations $G = \{x \in \mathbf{R}^n \mapsto \exp(tA)x + b : t \in \mathbf{R}, b \in \mathbf{R}^n\}$, we will write $(t; b)$ for the element $(x \mapsto \exp(tA)x + b)$. This is a real Lie group of dimension $n + 1$ of nilpotency class n and derived length 2, diffeomorphic to $\mathbf{R}^{n+1}$. The group law is given by

$$(t; b)(s; c) = (t + s; b + e^{tA}c).$$

Notice that the group law is given by polynomials with rational coefficients in s, t and the coordinates of b and c; thus G is in fact an algebraic group.

Lemma 4.8. *Recall the notation of 3.4.1. Let $k < n$ be an integer. The map*

$$((t_0; b_0), \cdots, (t_k; b_k)) \in G^{k+1} = \mathbf{R}^{(n+1)(k+1)} \mapsto \mathrm{Br}_{k+1}((t_0; b_0), \cdots, (t_k; b_k)) \in G = \mathbf{R}^{n+1}$$

is a nonconstant polynomial map with rational coefficients from $\mathbf{R}^{(n+1)(k+1)}$ to $\mathbf{R}^{n+1}$.

Proof. The map is polynomial with rational coefficients because the group law is, and this map is not constant because $\mathrm{nilp}(H) = n > k$. □

Consider the vector space generated by the translations $T_{e_i}, 2 \leq i \leq n$. The Lie group S acts on the variety G on the left and G/S is a variety diffeomorphic to $\mathbf{R}^2$. The diffeomorphisms are given by

$$[(t; b)] \in G/S \mapsto (t, b_1) \in \mathbf{R}^2$$

and

$$(x, y) \in \mathbf{R}^2 \mapsto [(x; ye_1)] \in G/S$$

where the brackets mean that we take the orbit under the action of S.

The group G acts by right composition on G/S and this action is faithful. The formulas are given by

$$\forall (t; b) \in G, \forall (x, y) \in \mathbf{R}^2 = G/S, \quad (x, y) \cdot (t; b) = \left(x + t, y + \sum_{k=1}^{n} \frac{t^{k-1}}{(k-1)!} b_k \right).$$

We see that the action is therefore by polynomial automorphisms. We will write $(t; b)$ on the left even though the action is on the right because we view it as a polynomial automorphism of $\mathbf{A}^2_{\mathbf{C}}$.

A group where theorem B is optimal.– Now, take H a finitely generated subgroup of G such that $\mathrm{nilp}(H) = n$ and H contains two elements $(t; b), (s; c)$ such that t, s and all the coordinates of b, c are algebraically independent over $\mathbf{Q}$. The group H satisfies the condition of Theorem B, it acts faithfully on the quasiprojective variety $\mathbf{A}^2_{\mathbf{C}}$ and we have $\mathrm{vdl}(H) = 2$. Indeed, if H admits an abelian finite index subgroup, then there exists an integer N such that $(t; b)^N$ and $(s; c)^N$ commute. But this would give a non-trivial polynomial relation over $\mathbf{Q}$ between s, t and the coordinates of b, c by Lemma 4.8, this is absurd. Thus, the bound in Theorem B is optimal for H.

Derived length versus nilpotency class.– In Theorem B we suppose that H is nilpotent. One might wonder if the bound can be improved using the virtual nilpotency class, i.e the minimum of $\mathrm{nilp}(H')$ for H' of finite index in H. We show that this is not possible with a similar counterexample as above. Take H a finitely generated subgroup of G such that H contains $(t_0; b_0), \cdots, (t_{n-1}; b_{n-1}) \in G^n$ such that all the t_i's and the coordinates of the b_i's are algebraically independent over $\mathbf{Q}$. We show that every finite index subgroup H' of H has a nilpotency class equal to n. Indeed, there exists an integer N such that for all $0 \leq i \leq n-1, h_i := (t_i; b_i)^N \in H'$. The coordinates of the h_i's are still algebraically independent over $\mathbf{Q}$ because the group law is given by polynomials with rational coefficients and by Lemma 4.8, the bracket $[h_0; \cdots; h_{n-1}]$ of length n is not the identity, because that would give a nontrivial polynomial relation between the coordinates of the h_i's.

Optimality of Theorem 3.16.– We show that in Theorem 3.16 we can't replace the derived length with the nilpotency class and that the theorem is optimal. In fact, the counterexample of [ET79] can be adapted over $\mathbf{Z}_p$ as follows. Consider the group G given by

$$G := \left\{ \mathbf{x} \in \mathbf{Z}_p^n \mapsto \exp(p \cdot tA)\mathbf{x} + b : t \in \mathbf{Z}_p, b \in \mathbf{Z}_p^n \right\}.$$

The group law is now given by polynomials with coefficients in $\mathbf{Z}_p$ and Lemma 4.8 still holds but the polynomials are with coefficients in $\mathbf{Z}_p$.

Then, G/S is analytically diffeomorphic to $\mathbf{Z}_p^2$ and we have an embedding of Lie groups $G \hookrightarrow \mathrm{Diff}^{an}(\mathbf{Z}_p^2)$ given by

$$\forall (t;b) \in G, \quad (t;b)(x,y) = \left(x + t, y + \sum_{k=1}^{n} \frac{p^{k-1}t^{k-1}}{(k-1)!} b_k \right).$$

Let $\mathfrak{g} \subset \Theta(\mathbf{Z}_p^2)$ be the Lie algebra of G, $\mathfrak{g}$ is nilpotent and we show that $\mathrm{nilp}(\mathfrak{g}) = n$. Let $k = \mathrm{nilp}(\mathfrak{g})$, then by Proposition 3.35, there exists a small subgroup G' of G which is a neighbourhood of id such that $\mathrm{nilp}(G') = k$. Therefore $k \leq n$, suppose $k < n$. By Lemma 4.8 the map

$$(t_0;b_0), \cdots, (t_k;b_k), (x,y) \in \mathbf{Z}_p^{(n+1)(k+1)} \times \mathbf{Z}_p^2 \mapsto \mathrm{Br}_{k+1}((t_0;b_0), \cdots, (t_k;b_k))(x,y) \in \mathbf{Z}_p^2$$

is polynomial. Let $P_1(\mathbf{w}), P_2(\mathbf{w})$ be the first and second coordinate of this map where $\mathbf{w}$ is a multivariate variable representing all the variables t_i, b_i, x, y. Since, $\mathrm{nilp}(G) > k$, the polynomials $Q_1(\mathbf{w}) = P_1(\mathbf{w}) - x$, $Q_2(\mathbf{w}) = P_2(\mathbf{w}) - y$ are not zero. Notice that if $(t;b) \in G$, then the Gauss norm of $(t;b) - \mathrm{id} \in \mathbf{Z}_p\langle x,y \rangle^2$ is bounded by the norm of $(t;b) \in \mathbf{Z}_p^{n+1}$, therefore there exists an integer $N > 0$ such that for all $(t;b) \in G$, $(p^N t; p^N b) \in G'$; thus

$$Q_1(p^N \mathbf{w}) \equiv 0, \quad Q_2(p^N \mathbf{w}) \equiv 0$$

and this implies that $Q_1 = 0, Q_2 = 0$, this is a contradiction.

By a similar argument, we can show there are no small abelian subgroups $G' \subset G$ neighbourhood of the identity therefore $\mathrm{dl}(\mathfrak{g}) = 2$ by Proposition 3.35 and Theorem 3.16 is also optimal.

Acknowledgements.– I would like to thank my advisor Serge Cantat for his help. He gave me helpful advice whenever I needed them. I would also like to thank Junyi Xie for his suggestions. Finally, I would like to thank the reviewer for his/her very useful observations and detailed advice.

References

[Bel05] Jason Bell. A generalised skolem-mahler-lech theorem for affine varieties. *Journal of the London Mathematical Society*, 73, 2005.

[BGT10] J. P. Bell, D. Ghioca, and T. J. Tucker. The dynamical Mordell-Lang problem for étale maps. *Amer. J. Math.*, 132(6):1655–1675, 2010.

[Bir21] Caucher Birkar. Singularities of linear systems and boundedness of fano varieties. *Annals of Mathematics*, 193(2):347–405, 2021.

[Bou70] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris, 1970.

[Bou06] N. Bourbaki. *Eléments de Mathématique. Groupes et algèbres de Lie: Chapitres 2 et 3.* 01 2006.

[Bou07a] N. Bourbaki. *Algèbre commutative: Chapitres 5 à 7.* Bourbaki, Nicolas. Springer Berlin Heidelberg, 2007.

[Bou07b] N. Bourbaki. *Variétés différentielles et analytiques: Fascicule de résultats.* Bourbaki, Nicolas. Springer Berlin Heidelberg, 2007.

[Can14] Serge Cantat. Morphisms between cremona groups and characterization of rational varieties. *Compositio Mathematica*, 150, 2014.

[Can18] Serge Cantat. Un lemme d'interpolation. *Congrès SMF 2018, Séminaire et Congrès*, 33:219–236, 2018.

[Cha80] Jasbir Singh Chahal. Solution of the congruence subgroup problem for solvable algebraic groups. *Nagoya Math. J.*, 79:141–144, 1980.

[CX18] Serge Cantat and Junyi Xie. Algebraic actions of discrete groups: the p-adic method. *Acta Math.*, 220(2):239–295, 2018.

[Eis95] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer, 1995.

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

[Gre60] Leon Greenberg. Conformal transformations of riemann surfaces. *American Journal of Mathematics*, 82(4):749–760, 1960.

[Hau19] Olivier Hantion. Fixed point theorems involving numerical invariants. *Compositio Mathematica*, 155(2):260–288, 2019.

[Lec53] Christer Lech. A note on recurring series. *Ark. Mat.*, 2:417–421, 1953.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Poo14] Bjorn Poonen. p-adic interpolation of iterates. *Bull. Lond. Math. Soc.*, 46(3):525–527, 2014.

[PS14] Yuri Prokhorov and Constantin Shramov. Jordan property for groups of birational selfmaps. *Compositio Mathematica*, 150(12):2054–2072, 2014.

[PS16] Yuri Prokhorov and Constantin Shramov. Jordan property for Cremona groups. *Amer. J. Math.*, 138(2):403–418, 2016.

[Rob00] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Sch05] I Schur. Über eine klasse von endlichen gruppen linearer substitutionen, nr. 6 der ges. abh, 1905.

[Seg83] Daniel Segal. *Polycyclic groups*, volume 82 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1983.

[Ser92] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, second edition, 1992. 1964 lectures given at Harvard University.

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

[Ser09] Jean-Pierre Serre. A minkowski-style bound for the orders of the finite subgroups of the cremona group of rank 2 over an arbitrary field. *Moscow Mathematical Journal*, 9, 01 2009.

[Xu20] Jinsong Xu. A remark on the rank of finite p-groups of birational automorphisms. *Comptes Rendus. Mathématique*, 358(7):827–829, 2020.