ALGEBRAIC ACTIONS OF DISCRETE GROUPS: THE p-ADIC METHOD

SERGE CANTAT AND JUNYI XIE

ABSTRACT. We study groups of automorphisms and birational transformations of quasi-projective varieties by p-adic methods. For instance, we show that if $\mathsf{SL}_n(\mathbf{Z})$ acts faithfully on a complex quasi-projective variety X by birational transformations, then $\dim(X) \geq n-1$ and X is rational if $\dim(X) = n-1$.

RÉSUMÉ. Nous employons des méthodes d'analyse p-adique pour étudier les groupes d'automorphismes et de transformations birationnelles des variétés quasi-projectives. Nous démontrons par exemple que si $\mathsf{SL}_n(\mathbf{Z})$ agit fidèlement par transformations birationnelles sur une variété complexe quasi-projective X, alors $\dim(X) \geq n-1$, et X est rationnelle en cas d'égalité.

CONTENTS

1. INTRODUCTION

1.1. **Automorphisms and birational transformations.** Let X be a quasi-projective variety of dimension d, defined over the field of complex numbers. Let $\mathsf{Aut}(X)$ denote its group of (regular) automorphisms and $\mathsf{Bir}(X)$ its group of birational transformations. A good example is provided by the affine space

---

Date: 2014/2015 (last version, Feb. 2015).

$\mathbb{A}^d_{\mathbf{C}}$ of dimension $d \geq 2$: Its group of automorphisms is "infinite dimensional" and contains elements with a rich dynamical behavior, such as the Hénon mapping (see [29, 2]); its group of birational transformations is the Cremona group $\mathsf{Cr}_d(\mathbf{C})$, and is known to be much larger that $\mathsf{Aut}(\mathbb{A}^d_{\mathbf{C}})$.

We present two new arguments that can be combined to study finitely generated groups acting by automorphims or birational transformations. The first argument is based on p-adic analysis and may be viewed as an extension of two classical strategies from a linear to a non-linear context. The first strategy appeared in the proof of Skolem, Mahler, and Lech theorem which says that the zeros of a linear recurrence sequence are obtained along a finite union of arithmetic progressions; it plays now a central role in arithmetic dynamics (see [4, 3]). The second strategy has been developed by Bass, Milnor, and Serre when they obtained rigidity results for finite dimensional linear representations of $\mathsf{SL}_n(\mathbf{Z})$ as a corollary of the congruence subgroup property (see [1, 45]). Our second argument combines isoperimetric inequalities from geometric group theory with Lang-Weil estimates from diophantine geometry. Altogether, they lead to *new constraints on groups of birational transformations in any dimension.*

1.2. **Actions of $\mathsf{SL}_n(\mathbf{Z})$.** Consider the group $\mathsf{SL}_n(\mathbf{Z})$ of $n \times n$ matrices with integer entries and determinant 1. Let Γ be a finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$; it acts by linear projective transformations on the projective space $\mathbb{P}^{n-1}_{\mathbf{C}}$, and the kernel of the morphism $\Gamma \to \mathsf{PGL}_n(\mathbf{C})$ contains at most 2 elements. The following result shows that Γ does not act faithfully on any smaller variety.

Theorem A. *Let Γ be a finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$. Let X be an irreducible, complex, quasi-projective variety. If Γ embeds into $\mathsf{Aut}(X)$, then*

$$\dim_{\mathbf{C}}(X) \geq n-1$$

and if $\dim_{\mathbf{C}}(X) = n-1$, then X is isomorphic to the projective space $\mathbb{P}^{n-1}_{\mathbf{C}}$.

Let $\mathbf{k}$ be a field of characteristic 0. Theorem A implies:

(1) *The group $\mathsf{SL}_n(\mathbf{Z})$ embeds into $\mathsf{Aut}(\mathbb{A}^d_{\mathbf{k}})$ if and only if $d \geq n$;*
(2) *if $\mathsf{Aut}(\mathbb{A}^d_{\mathbf{k}})$ is isomorphic to $\mathsf{Aut}(\mathbb{A}^{d'}_{\mathbf{k}})$ (as abstract groups) then $d = d'$.*

Previous proofs of Assertion (2) assumed $\mathbf{k}$ to be equal to $\mathbf{C}$ (see [23, 33]).

1.3. **Lattices in simple Lie groups.** One can extend Theorem A in two directions, replacing $\mathsf{SL}_n(\mathbf{Z})$ by more general lattices, and looking at actions by birational transformations instead of regular automorphisms.

Let S be an almost simple linear algebraic group which is defined over $\mathbf{Q}$. The $\mathbf{Q}$-rank of S is the maximal dimension of a Zariski-closed subgroup of S that is diagonalizable over $\mathbf{Q}$; the $\mathbf{R}$-rank of S is the maximal dimension of a Zariski-closed subgroup that is diagonalizable over $\mathbf{R}$. The subgroup $\mathsf{S}(\mathbf{Z})$ is a lattice in $\mathsf{S}(\mathbf{R})$, and it is co-compact if and only if the $\mathbf{Q}$-rank of S vanishes.

One says that S **splits** over $\mathbf{Q}$ if the $\mathbf{Q}$-rank $\mathsf{rank}_{\mathbf{Q}}(\mathsf{S})$ is equal to its $\mathbf{R}$-rank $\mathsf{rank}_{\mathbf{R}}(\mathsf{S})$. For example, the standard form of SL_n splits over $\mathbf{Q}$, and its rank is $n-1$. Similarly, the symplectic group Sp_{2n}, defined as the group of linear transformations of a vector space of dimension $2n$ preserving the standard symplectic form $dx_1 \wedge dy_1 + \ldots + dx_n \wedge dy_n$, has rank n and splits over $\mathbf{Q}$.

Theorem B. *Let X be an irreducible complex projective variety. Let S be an almost simple linear algebraic group over the field of rational numbers $\mathbf{Q}$. Assume that $\mathsf{S}(\mathbf{Z})$ is not co-compact. If a finite index subgroup of $\mathsf{S}(\mathbf{Z})$ embeds into $\mathsf{Bir}(X)$, then $\dim_{\mathbf{C}}(X) \geq \mathsf{rank}_{\mathbf{R}}(\mathsf{S})$ and $\mathsf{S}(\mathbf{R})$ is isogeneous to $\mathsf{SL}_{\dim(X)+1}(\mathbf{R})$ if $\dim(X) = \mathsf{rank}_{\mathbf{R}}(\mathsf{S})$.*

For instance, if G_2 denotes a split form of the exceptional Lie group of rank 2 (over $\mathbf{Q}$), then $\mathsf{G}_2(\mathbf{Z})$ does not act faithfully by birational transformations in dimension ≤ 4. Theorem B implies also that *the Cremona groups $\mathsf{Cr}_d(\mathbf{k})$ and $\mathsf{Cr}_{d'}(\mathbf{k}')$ are not isomorphic if $\mathbf{k}$ and $\mathbf{k}'$ have characteristic 0 and $d \neq d'$.*

Remark 1.1. Assume $\mathsf{rank}_{\mathbf{R}}(\mathsf{S}) \geq 2$. Then, every lattice Γ of $\mathsf{S}(\mathbf{R})$ is almost simple: Its normal subgroups are finite and central or co-finite (see [38], and [1, 45] for $\Gamma \leq \mathsf{SL}_n(\mathbf{Z})$). Thus, the assumption "*Γ embeds into $\mathsf{Bir}(X)$*" can be replaced by "*there is a morphism from Γ to $\mathsf{Bir}(X)$ with infinite image*".

Remark 1.2. The main theorems of [7, 14] extend Theorem B to all types of lattices (i.e., co-compact lattices) in simple real Lie groups but assume that the action is by regular automorphisms. When X is compact, $\mathsf{Aut}(X)$ is a Lie group, it may have infinitely many connected components, but its dimension is finite; the techniques of [7, 14] do not apply to arbitrary quasi-projective varieties (for instance to $X = \mathbb{A}^d_{\mathbf{C}}$) and to groups of birational transformations, but work for automorphisms of compact Kähler manifolds.

Remark 1.3. In dimension 2, *every faithful birational action of an infinite Kazhdan group on a complex projective surface Y is conjugate to a linear projective action on the plane by a birational transformation $Y \dashrightarrow \mathbb{P}^2_{\mathbf{C}}$.* (see [13, 9, 22], and § 6.1.2 below for a definition of Kazhdan groups).

Example 1.4. Consider an irreducible sextic plane curve with 10 double points; such a curve is rational. Blow-up the singular points to obtain a rational surface X with Picard number 11. The group of automorphisms of X acts by linear endomorphisms on the Néron-Severi group and preserves the canonical class k_X. The orthogonal complement of k_X with respect to the intersection form is a lattice of rank 10 and signature $(1,9)$. This provides a morphism from $\mathsf{Aut}(X)$ to the group $\mathsf{SO}_{1,9}(\mathbf{R})$. It turns out that, for a generic choice of the sextic curve, the image of $\mathsf{Aut}(X)$ is a lattice in $\mathsf{SO}_{1,9}(\mathbf{R})$ (see [12]). A similar phenomenon holds for generic Enriques surfaces (see [17]). This example shows that "large" lattices may act on small dimensional varieties if the size of the lattice is measured by the dimension of the Lie group $\mathsf{S}(\mathbf{R})$.

1.4. **Finite fields, Hrushovski's theorem and Mapping class groups.** To prove Theorems A and B, we first change the field of definition, replacing $\mathbf{C}$ by a p-adic field $\mathbf{Q}_p$. Then, we prove the existence of a p-adic polydisk in $X(\mathbf{Q}_p)$ (or $X(K)$ for some finite extension K of $\mathbf{Q}_p$) which is invariant under the action of a finite index subgroup Γ of the lattice $\mathsf{S}(\mathbf{Z})$, and on which Γ acts by p-adic analytic diffeomorphisms. Those polydisks correspond to periodic orbits in $X(\mathbb{F}_p)$ (or $X(F)$ for a finite extension F of $\mathbb{F}_p$), i.e. to fixed points m of finite index subgroups Γ' of Γ which are well defined at m (no element of Γ' has an indeterminacy at m). Therefore, an important step towards Theorem B is the existence of finite orbits that avoid all indeterminacy points. For cyclic groups of transformations, this can be obtained from Hrushovski theorem (see [32]). Here, we combine Lang-Weil estimates with isoperimetric inequalities from geometric group theory to construct such periodic orbits when the group satisfies Kazhdan property (T). Once such periodic orbits are constructed, several corollaries easily follows (see § 6.4.2):

Theorem C. *If a discrete group with Kazhdan property (T) acts faithfully by birational transformations on a complex projective variety X, the group is residually finite and contains a torsion free finite index subgroup.*

In particular, infinite, simple, discrete groups with Kazhdan property (T) do not act non-trivially by birational transformations.

Our strategy of proof applies to actions of other discrete groups, such as the mapping class group of a closed genus g surface, or the group of outer automorphisms of a free group. Here is a sample result:

Theorem D. *Let* $\mathsf{Mod}(g)$ *be the mapping class group of a closed orientable surface of genus g. Let* $\mathsf{ma}(g)$ *be the smallest dimension of a quasi-projective variety X on which a finite index subgroup of* $\mathsf{Mod}(g)$ *may act faithfully by automorphisms. Then* $\mathsf{ma}(1) = 1$ *and* $2g-1 \leq \mathsf{ma}(g) \leq 6g-6$ *for all* $g \geq 2$.

1.5. **Margulis super-rigidity and Zimmer program.** Let Γ be a lattice in a simple real Lie group S, with $\mathsf{rank}_{\mathbf{R}}(\mathsf{S}) \geq 2$. According to Margulis super-rigidity theorem, unbounded linear representations of the discrete group Γ "come from" linear algebraic representations of the group S itself. As a byproduct, the smallest dimension of a faithful linear representation of Γ coincides with the smallest dimension of a faithful linear representation of S (see [38]). Zimmer program asks for an extension of this type of rigidity results to non-linear actions of Γ, for instance to actions of Γ by diffeomorphisms on compact manifolds (see [49, 50], and the recent survey [27]). Theorems A and B are instances of Zimmer program in the context of algebraic geometry. In case $\Gamma = \mathsf{SL}_n(\mathbf{Z})$ or $\mathsf{Sp}_{2n}(\mathbf{Z})$, Bass, Milnor and Serre obtained a super-rigidity theorem from their solution of the congruence subgroup problem (see [1, 45]). Our proofs of Theorems A and B may be considered as extensions of their argument to the context of non-linear actions by algebraic transformations.

1.6. **Acknowledgement.** Thanks to Yves de Cornulier, Julie Déserti, Philippe Gille, Sébastien Gouezel, Vincent Guirardel, and Peter Sarnak for interesting discussions related to this article. This work was supported by the ANR project BirPol and the foundation Del Duca from the french academy of sciences. Part of this work was done during the visit of the first author as a member of the Institute for Advanced Studies, Princeton.

2. Analytic diffeomorphisms of the p-adic polydisk

In this section, we introduce the group of p-adic analytic (or Tate analytic) diffeomorphisms of the unit polydisk $\mathcal{U} = \mathbf{Z}_p^d$, describe its topology, and study its finite dimensional subgroups.

2.1. **Analytic diffeomorphisms.**

2.1.1. *Tate algebras.* Let p be a prime number. Let K be a field of characteristic 0 which is complete with respect to an absolute value $|\cdot|$ satisfying $|p| = 1/p$. Good examples to keep in mind are the fields of p-adic numbers $\mathbf{Q}_p$ and its finite extensions. Let R be the valuation ring of K, i.e. the subset of K defined by $R = \{x \in K;\ |x| \leq 1\}$; in the vector space K^d, the unit polydisk is the subset R^d.

Fix a positive integer d, and consider the ring $R[x] = R[x_1, ..., x_d]$ of polynomial functions in d variables with coefficients in R. For f in $R[x]$, define the norm $\parallel f \parallel$ to be the supremum of the absolute values of the coefficients of f:

$$\parallel f \parallel = \sup_I |a_I| \tag{2.1}$$

where $f = \sum_{I=(i_1,...,i_d)} a_I x^I$. By definition, the **Tate algebra** $R\langle x\rangle$ is the completion of $R[x]$ with respect to the norm $\parallel \cdot \parallel$. The Tate algebra coincides with the set of formal power series $f = \sum_I a_I x^I$, $I \in \mathbf{Z}_+^d$, converging on the closed unit polydisk R^d. Moreover, the convergence is equivalent to $|a_I| \to 0$ as $I \to \infty$.

For f and g in $R\langle x\rangle$ and c in $\mathbf{R}_+$, the notation $f \in p^c R\langle x\rangle$ means $\parallel f \parallel \leq |p|^c$ and the notation

$$f \equiv g \pmod{p^c}$$

means $\parallel f - g \parallel \leq |p|^c$; we then extend such notations component-wise to $(R\langle x\rangle)^m$ for all $m \geq 1$. For instance, the function $f(x) = p + x + px^2 + p^2x^2$ satisfies $f \equiv \mathrm{id} \pmod{p}$, where $\mathrm{id}(x) = x$ is the identity mapping.

2.1.2. *Tate diffeomorphisms.* Denote by $\mathcal{U}$ the unit polydisk of dimension d, that is $\mathcal{U} = R^d$. For x and y in $\mathcal{U}$, the distance $\mathsf{dist}(x, u)$ is defined by $\mathsf{dist}(x, y) = \max_i |x_i - y_i|$, where the x_i and y_i are the coordinates of x and y in R^d. The non-archimedean triangular inequality implies that $|h(y)| \leq 1$ for every h in $R\langle x\rangle$ and $y \in \mathcal{U}$. Consequently, every element g in $R\langle x\rangle^d$ determines an analytic map $g\colon \mathcal{U} \to \mathcal{U}$.

If $g = (g_1, \ldots, g_d)$ is an element of $R\langle x\rangle^d$, the norm $\parallel g \parallel$ is defined as the maximum of the norms $\parallel g_i \parallel$ (see Equation (2.1)); one has $\parallel g \parallel \leq 1$ and $\mathsf{dist}(g(x), g(y)) \leq \parallel g \parallel \mathsf{dist}(x, y)$, so that g is 1-Lipschitz.

Consider the group of transformations $f\colon \mathcal{U} \to \mathcal{U}$ given by

$$f(x) = (f_1, \ldots, f_d)(x)$$

where each f_i is in $R\langle x\rangle$ and f has an inverse $f^{-1}\colon \mathcal{U} \to \mathcal{U}$ that is also defined by power series in the Tate algebra. We denote this group by $\mathsf{Diff}^{an}(\mathcal{U})$ and call it the group of **analytic diffeomorphisms** (or **Tate diffeomorphisms**) of $\mathcal{U}$. The distance between two analytic diffeomorphisms f and g is then defined as $\| f-g \|$; by Lemma 2.2, this endows $\mathsf{Diff}^{an}(\mathcal{U})$ with the structure of a topological group.

Proposition 2.1. *For every $c>0$, the subgroup of all elements $f\in \mathsf{Diff}^{an}(\mathcal{U})$ with $f\equiv \mathrm{id} \pmod{p^c}$ is a normal subgroup of $\mathsf{Diff}^{an}(\mathcal{U})$.*

Lemma 2.2. *Let f, g, and h be elements of $R\langle x\rangle^d$.*

(1) $\| g\circ f \| \leq \| g \|$;
(2) *if f is an element of $\mathsf{Diff}^{an}(\mathcal{U})$ then* $\| g\circ f \| = \| g \|$
(3) $\| g\circ(\mathrm{id}+h)-g \| \leq \| h \|$
(4) $\| f^{-1}-\mathrm{id} \| \leq \| f-\mathrm{id} \|$ *if f is an analytic diffeomorphism.*

Proof. Let c satisfy $|p|^c = \| g \|$. Then $p^{-c}g$ is an element of $R\langle x\rangle^d$. It follows that $(p^{-c}g)\circ f$ is an element of $R\langle x\rangle^d$ too, and that $\| g\circ f \| \leq p^c$. This proves Assertion (1). The second assertion follows because $g=(g\circ f)\circ f^{-1}$. To prove Assertion (3), write $h=(h_1,h_2,\ldots,h_d)$ where each h_i satisfies $\| h_i \| \leq \| h \|$. Then $g\circ(\mathrm{id}+h)$ takes the form

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

where each A_i is a homogeneous polynomial in $(x_1,\ldots,x_d)$ of degree i with coefficients in R. Assertion (3) follows. To prove Assertion (4), assume that f is an analytic diffeomorphism and apply Assertion (2): $\| f^{-1}-\mathrm{id} \| = \| \mathrm{id}-f \| \leq |p|^c$ □

Proof of Proposition 2.1. Set $D_c=\{f\in \mathsf{Diff}^{an}(\mathcal{U});\quad \| f-\mathrm{id} \| \leq |p|^c\}$. If f is an element of D_c, so is f^{-1} (Lemma 2.2, Assertion (4)). Similarly, D_c is stable under composition because

$$\| g\circ f-\mathrm{id} \| = \| (g\circ f-f)+(f-\mathrm{id}) \| \leq \max\left(\| (g-\mathrm{id})\circ f \|, \| f-\mathrm{id} \|\right)$$

and Lemma 2.2 shows that both terms are bounded from above by $|p|^c$ if f and g are in D_c. Thus D_c is a subgroup of $\mathsf{Diff}^{an}(\mathcal{U})$. If g is an element of D_c and f is an element of $\mathsf{Diff}^{an}(\mathcal{U})$, one has

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

But Assertion (3) in Lemma 2.2 shows that

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

Thus, D_c is a normal subgroup. □

Lemma 2.3. *Let f be an element of $\mathsf{Diff}^{an}(\mathcal{U})$. If $f(x) \equiv x \pmod{p^c}$, with $c \geq 1$, and p^N divides l then $f^l(x) \equiv x \pmod{p^{c+N}}$. In particular, if $f \equiv \mathrm{id} \pmod{p}$, then $f^{p^\ell} \equiv \mathrm{id} \pmod{p^\ell}$.*

Proof. Write $f(x) = x + p^c r(x)$ where r is in $(R\langle x \rangle)^d$. Then

$$\begin{aligned} f \circ f(x) &= x + p^c r(x) + p^c r(x + p^c r(x)) \\ &= x + 2p^c r(x) \pmod{p^{2c}} \end{aligned}$$

and after p iterations one gets

$$\begin{aligned} f^p(x) &= x + p^{c+1} r(x) \pmod{p^{pc}} \\ &= x \pmod{p^{c+1}} \end{aligned}$$

if $c \geq 1$. Then, $f^{p^2}(x) \equiv x \pmod{p^{c+2}}$ and $f^{p^N}(x) \equiv x \pmod{p^{c+N}}$. $\square$

2.2. From cyclic groups to p-adic flows.

2.2.1. *From cyclic groups to R-flows.* The following theorem is due to Bell and to Poonen (see [40], and [4, 3] for former results).

Theorem 2.4. *Let $f\colon \mathcal{U} \to \mathcal{U}$ be an element of $R\langle x \rangle^d$. Assume that*

$$f(x) \equiv \mathrm{id} \pmod{p^c}$$

for some $c > 1/(p-1)$. Then there exists an element Φ in $R\langle x_1, \ldots, x_d, t \rangle^d$, i.e. a Tate analytic map $\Phi\colon \mathcal{U} \times R \to \mathcal{U}$, such that $\Phi(x,n) = f^n(x)$ for all n in $\mathbf{Z}_+$.

Remark 2.5. Let f and Φ be as in the Theorem 2.4.

(a) The relation $\Phi(x, n+1) = f \circ \Phi(x,n)$ holds for every integer $n \geq 0$. Thus, for every x in $\mathcal{U}$, the two Tate-analytic functions $t \mapsto \Phi(x, t+1)$ and $t \mapsto f \circ \Phi(x,t)$ coincide on $\mathbf{Z}_+$, hence on R by the isolated zero principle:

$$\Phi(x, t+1) = f \circ \Phi(x,t) \text{ in } R\langle x, t \rangle^d.$$

Apply this to $t = -1$ to deduce that f is indeed an analytic diffeomorphism of $\mathcal{U}$ and that $f^{-1} = \Phi(\cdot, -1)$. Then, by induction, one gets $\Phi(x,n) = f^n(x)$ for all $n \in \mathbf{Z}$.

(b) The relation $\Phi(x, n+m) = \Phi(\Phi(x,m), n)$ holds for all pairs of integers (n,m), because $f^{n+m} = f^n \circ f^m$. Thus,

$$\Phi(x, s+t) = \Phi(\Phi(x,t), s)$$

for all $(x,s,t) \in \mathcal{U} \times R \times R$. This means that Φ defines a group action of R on $\mathcal{U}$ that extends the action of $\mathbf{Z} \subset R$ determined by f. An analytic map

$\Phi\colon \mathcal{U}\times R\to\mathcal{U}$ which defines a group action of $(R,+)$ will be called **a R-flow**, or simply **a flow**. (see below, § 2.2.2, how it is viewed as the flow of an analytic vector field)

(c) Let $g\in R\langle x\rangle^d$ satisfy the assumptions of Theorem 2.4. Then, we get two flows $\Phi_f,\Phi_g\colon \mathcal{U}\times R\to\mathcal{U}$, and another flow $\Phi_{g\circ f}$ for the composition $g\circ f$. Moreover, $\Phi_{g\circ f}(x,1)=g\circ f(x)=\Phi_g(\Phi_f(x,1),1)$.

If f and g commute to each other, then $\Psi(x,s,t):=\Phi_g(\Phi_f(x,s),t)$ determines an action of the abelian group $R\times R$ on $\mathcal{U}$.

These remarks lead to the following strengthening of Theorem 2.4, in which Assertions (3) and (4) follow from Poonen's proof of Theorem 2.4.

Theorem 2.6. *Let f be an element of $R\langle x\rangle^d$ with $f\equiv \mathrm{id} \pmod{p^c}$ for $c>(p-1)^{-1}$. Then f is a Tate diffeomorphism of $\mathcal{U}=R^d$ and there exists a Tate-analytic map $\Phi\colon \mathcal{U}\times R\to\mathcal{U}$ such that*

1. *$\Phi(x,n)=f^n(x)$ for all $n\in\mathbf{Z}$ and $x\in\mathcal{U}$;*
2. *$\Phi(x,t+s)=\Phi(\Phi(x,s),t)$ for all t, s in R;*
3. *$\Phi\colon t\in R\mapsto\Phi(\cdot,t)$ is a continuous morphism from the abelian group $(R,+)$ to the group of Tate diffeomorphisms $\mathsf{Diff}^{an}(\mathcal{U})$;*
4. *$\Phi(x,t)\equiv x \pmod{p^{c-1/(p-1)}}$ for all $t\in R$.*

We shall refer to this theorem as "Bell-Poonen theorem", or "Bell-Poonen extension theorem". In this article, a flow Φ will be considered either as an analytic action $\Phi\colon \mathcal{U}\times R\to\mathcal{U}$ of the abelian group $(R,+)$, or as a morphism $\Phi\colon t\in R\mapsto\Phi_t\in\mathsf{Diff}^{an}(\mathcal{U})$; we use the same vocabulary (and the same letter Φ) for the two maps.

Corollary 2.7. *Let f be an element of $R\langle x\rangle^d$ with $f\equiv \mathrm{id} \pmod{p^c}$ for $c>(p-1)^{-1}$. Then f is a Tate diffeomorphism of $\mathcal{U}=R^d$, and if f is a finite order element of $\mathsf{Diff}^{an}(\mathcal{U})$, its order is a power of p.*

This follows from the Chinese Lemma, and from the fact that a continuous morphism from $(\mathbf{Z}_p,+)$ to $\mathbf{Z}/q\mathbf{Z}$ is automatically trivial if q is prime to p.

2.2.2. *Flows and analytic vector fields.* Consider the Lie algebra $\Theta(\mathcal{U})$ of vector fields

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

where each u_i is an element of the Tate algebra $R\langle x\rangle$. The Lie bracket with a vector field $\mathbf{Y} = \sum_i v_i(x)\partial_i$ is given by

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

Lemma 2.8. *Let $\Phi\colon\ \mathcal{U}\times R \to \mathcal{U}$ be an element of $R\langle x,t\rangle^d$ that defines an analytic flow. Then*

$$\mathbf{X} = \left(\frac{\partial\Phi}{\partial t}\right)_{|t=0}$$

is an analytic vector field. It is preserved by Φ_t: For all $t\in R$, $(\Phi_t)_*\mathbf{X} = \mathbf{X}$. Moreover, $\mathbf{X}(x_0) = \mathbf{0}$ if and only if $\Phi_t(x_0) = x_0$ for all $t \in R$.

The analyticity and Φ_t-invariance are easily obtained. Let us show that $\mathbf{X}(x_0) = 0$ if and only if x_0 is a fixed point of Φ_t for all t. Indeed, if $\mathbf{X}$ vanishes at x_0, then $\mathbf{X}$ vanishes along the curve $\Phi(x_0,t)$, $t\in R$, because $\mathbf{X}$ is Φ_t-invariant. Thus, $\partial_t\Phi(x_0,t) = 0$ for all t, and the result follows.

Corollary 2.9. *If f is an element of $\mathsf{Diff}^{an}(\mathcal{U})$ with $f\equiv \mathrm{id} \pmod{p^c}$ for some $c > (p-1)^{-1}$, then f is given by the flow Φ_f, at time $t = 1$, of a unique analytic vector field $\mathbf{X}_f$. The zeros of $\mathbf{X}$ are the fixed points of f. If two such diffeomorphisms f and g commute to each other, then $[\mathbf{X}_f,\mathbf{X}_g] = \mathbf{0}$.*

2.3. **A pro-p structure.** Recall that a **pro-p group** is a topological group G which is a compact Hausdorff space, with a basis of neighborhoods of the neutral element 1_G generated by subgroups of index a (finite) power of p. In such a group, the index of every open normal subgroup is a power of p. See [24] for a good introduction to pro-p groups.

In this subsection, we assume that the residue field, i.e. the quotient of R by its maximal ideal $\mathbf{m}_K = \{x\in K;\ |x|<1\}$, is a finite field (of characteristic p). In particular, the residue field has q elements, with q a power of p; similarly, the number of elements of $R/\mathbf{m}_K^k$ is a power of p for every k. We also fix an element π that generates the ideal $\mathbf{m}_K$.

2.3.1. *Action modulo $\mathbf{m}_K^k$.* Recall that $\mathcal{U}$ denotes the polydisk R^d. If f is an element of $\mathsf{Diff}^{an}(\mathcal{U})$, its reduction modulo $\mathbf{m}_K^k$ is a polynomial transformation with coefficients $\overline{a_I}$ in the finite ring $R/\mathbf{m}_K^k$; it determines a bijection of the finite set $(R/\mathbf{m}_K^k)^d$. Each element of $\mathsf{Diff}^{an}(\mathcal{U})$ acts isometrically on $\mathcal{U}$ with respect to the distance $\mathsf{dist}(x,y)$ (see § 2.1.2). Since balls of radius $|\pi|^{-k}$ are in one to one correspondence with points in $(R/\mathbf{m}_K^k)^d$, this action of $\mathsf{Diff}^{an}(\mathcal{U})$

on the set of balls may be identified to its action modulo $\mathbf{m}_K^k$. Thus, for each $k \geq 1$, one gets a morphism of $\mathsf{Diff}^{an}(\mathcal{U})$ into the group of permutations of the finite set $(R/\mathbf{m}_K^k)^d$, and an element f of $\mathsf{Diff}^{an}(\mathcal{U})$ is the identity if and only if its image in each of these finite groups is trivial (i.e. if and only if $\mathsf{dist}(f(x),x) \leq |\pi|^k$ for all x and all k).

2.3.2. *A pro-p completion.* Given a positive integer ℓ, define $\mathsf{Diff}^{an}(\mathcal{U})_\ell$ as the subgroup of $\mathsf{Diff}^{an}(\mathcal{U})$ whose elements are equal to the identity modulo p^ℓ. Let $D = \mathsf{Diff}^{an}(\mathcal{U})_1$. By definition, every element f of D can be written $f = \mathrm{id} + ph$ where h is in $R\langle x\rangle^d$. Thus, D acts trivially on $(R/pR)^d$ (here, $pR = \mathbf{m}_K^l$ with $|\pi^l| = 1/p$).

Consider an element f of D that acts trivially modulo p^m for some $m \geq 1$.

Writing $f(z)$ as a sum of homogeneous terms $A_0 + A_1(z) + \sum_{k\geq 2} A_k(z)$, one easily checks the following property: There are two maps $\alpha_f \colon (R/p^mR)^d \to \mathrm{Mat}_d(R/pR)$ and $\beta_f \colon (R/p^mR)^d \to (R/pR)^d$ such that, for every point $x_0 \in \mathcal{U}$ and every point $x_0 + p^m b$ in the ball of radius p^{-m} around x_0, we have

$$f(x_0 + p^m b) = x_0 + p^m(\alpha_f(x_0)(b) + \beta_f(x_0)) \ (\mathrm{mod}\, p^{m+1}). \qquad (2.2)$$

Moreover, given any pair of maps $\alpha(\cdot)$ and $\beta(\cdot)$ as above, one can find a polynomial transformation f of the affine space $\mathbb{A}_R^d$, with coefficients in R, which acts trivially modulo p^m and for which $\alpha_f = \alpha$ and $\beta_f = \beta$. By Bell-Poonen theorem, f determines an analytic diffeomorphism of $\mathcal{U}$. The group of all bijections of $(R/p^{m+1}R)^d$ given by formulas of type (2.2) is a p-group. As a consequence, a recursion on m shows that the image of D into the group of permutations of $(R/p^mR)^d$ is a p-group for every $m \geq 1$.

Thus, D may be endowed with a pro-p topology, for which the kernels of the action on $(R/p^mR)^d$, $m \geq 1$, form a basis of neighborhoods of the identity. Since the action on $(R/p^mR)^d$ is the action on the set of balls of radius p^{-m} in $\mathcal{U}$, the Tate topology is finer than the pro-p topology: The identity map $f \mapsto f$ is a continuous morphism with respect to the Tate topology on the source, and the pro-p topology on the target. Therefore, if $\hat{D}$ is the completion of D with respect to this pro-p topology, the map

$$D \to \hat{D}$$

defines an injective continuous morphism.

Remark 2.10. Fix a prime p and consider the field $K = \mathbf{Q}_p$, with valuation ring $R = \mathbf{Z}_p$. The sequence of polynomial automorphisms of the affine plane defined by $h_n(x,y) = (x, y + p(x + x^2 + x^3 + \cdots + x^n))$ determines a sequence of elements of D for $d = 2$. There is no subsequence of $(h_n)_n$ that converges in the Tate topology. Being a pro-p group, $\hat{D}$ is compact, and one can extract a subsequence of (h_n) that converges in $\hat{D}$.

2.4. Extension theorem.

2.4.1. *Analytic groups (see* [24, 44] *and* [6] *Chapter III).* One says that a pro-p group is **finitely generated** if it contains a dense, finitely generated subgroup. For such groups, the pro-p topology is uniquely determined by the algebraic structure: A subgroup is open if and only if it has finite index, and finite index subgroups form a basis of neighborhoods of the neutral element (see [24], Theorem 1.17). Let G be a finitely generated pro-p group. Given a positive integer m, one denotes by G^m the subgroup of G which is generated by all x^m, $x \in G$. One says that G is **powerful** if p is odd and the closure of G^p contains the derived subgroup of G, or if $p = 2$ and the closure of G^4 contains the derived subgroup of G. Then, for a pro-p group, the following properties are equivalent:

(a) G is finitely generated and virtually powerful,
(b) G embeds continuously in $\mathsf{GL}_d(\mathbf{Z}_p)$ for some d,
(c) G is a **p-adic analytic group**.

We refer to [24] for the definition of p-adic analytic groups and a proof of the equivalence of these three properties.

In what follows, we fix a pair (G, Γ) where G is a p-adic analytic group and Γ is a finitely generated, dense subgroup of G. A good example to keep in mind is $\Gamma = \mathsf{SL}_n(\mathbf{Z})$ in $G = \mathsf{SL}_n(\mathbf{Z}_p)$ (see §3.4 below).

2.4.2. *One parameter subgroups.* Let g be an element of the pro-p group G. The morphism $\varphi\colon m \in \mathbf{Z} \mapsto g^m \in G$ extends automatically to the pro-p completion of $\mathbf{Z}$, i.e. to a continuous morphism of pro-p groups

$$\overline{\varphi}\colon \mathbf{Z}_p \to G.$$

For simplicity, we denote $\overline{\varphi}(t)$ by g^t for all t in $\mathbf{Z}_p$ (see [24], Proposition 1.28, for embeddings of $\mathbf{Z}_p$ into pro-p groups).

Lemma 2.11. *Let Γ be a dense subgroup of a p-adic analytic group G. There exist γ_1, ..., γ_r in Γ (for some $r \geq 1$) such that the map $\pi\colon (\mathbf{Z}_p)^r \to G$*

$$\pi(t_1, \ldots, t_r) \quad = \quad \gamma_1^{t_1} \cdots \gamma_r^{t_r}$$

is a surjective, p-adic analytic map. Moreover, as l runs over the set of positive integers, the sets $\pi(p^l\mathbf{Z}_p)^r$ *form a basis of neighborhoods of the neutral element in G.*

Proof. Let $\mathfrak{g}$ be the Lie algebra of G; as a finite dimensional $\mathbf{Q}_p$-vector space, $\mathfrak{g}$ coincides with the tangent space of G at the neutral element 1_G. There are finite index open subgroups H of G for which the exponential map defines a p-adic analytic diffeomorphism from a neighborhood of the origin in $\mathfrak{g}(\mathbf{Z}_p)$ onto the group H itself. Let H be such a subgroup (see the notion of standard subgroups in [6, 24]).

Since Γ is dense in G its intersection with H is dense in H. Each $\alpha_i \in \Gamma \cap H$ corresponds to a tangent vector $\nu_i \in \mathfrak{g}$ such that $\exp(t\nu_i) = \alpha_i^t$ for $t \in \mathbf{Z}_p$. Since Γ is dense in H, the subspace of $\mathfrak{g}$ generated by all the ν_i is equal to $\mathfrak{g}$. Thus, one can find elements α_1, ..., α_s of Γ, with $s = \dim(G)$, such that the ν_i generate $\mathfrak{g}$. Then, the map $\pi\colon (\mathbf{Z}_p)^s \to H$ defined by

$$\pi(t_1, \dots, t_s) = \exp(t_1\nu_1)\cdots\exp(t_s\nu_s) = \alpha_1^{t_1}\cdots\alpha_s^{t_s}$$

is analytic and determines a local analytic diffeomorphism from a neighborhood of 0 in $\mathfrak{g}$ to a neighborhood V of 1_G. The group G can then be covered by a finite number of translates h_jV, $j = 1, \dots, s'$. Since Γ is dense, one can find elements β_j in Γ with $\beta_j^{-1}h_j \in V$. The lemma follows if one sets $r = s + s'$, $\gamma_i = \alpha_i$ for $1 \le i \le s$, and $\gamma_i = \beta_{i-s}$, $s \le i \le r$. $\square$

2.4.3. *Actions by analytic diffeomorphisms.* We now study morphisms from Γ to the group $\mathsf{Diff}^{an}(\mathcal{U})$, where $\mathcal{U} = R^d$ for some d. Thus, in this paragraph, the same prime number p plays two roles since it appears in the definition of the pro-p structure of G, and of the Tate topology on $\mathsf{Diff}^{an}(\mathcal{U})$.

Theorem 2.12. *Let G be a p-adic analytic group and let* Γ *be a finitely generated, dense subgroup of G. Let* $\Phi\colon \Gamma \to \mathsf{Diff}^{an}(\mathcal{U})_1$ *be a morphism into the group of analytic diffeomorphisms of* $\mathcal{U}$ *which are equal to the identity modulo p. Then,* Φ *extends to a continuous morphism*

$$\overline{\Phi}\colon G \to \mathsf{Diff}^{an}(\mathcal{U})_1$$

such that the action $G \times \mathcal{U} \to \mathcal{U}$ *given by* $(g,x) \mapsto \Phi(g)(x)$ *is analytic.*

For simplicity, denote $\mathsf{Diff}^{an}(\mathcal{U})_1$ by D. Recall that D embeds continuously into the pro-p group $\hat{D}$ (see §2.3.2). The following properties will be used to prove the lemma.

(1) The morphism $\Gamma \to \hat{D}$ extends uniquely into a continuous morphism $\hat{\Phi}$ from G to $\hat{D}$ because G is the pro-p completion of Γ.
(2) Let f be an element of D. By Bell-Poonen extension theorem, the morphism $t \in \mathbf{Z} \mapsto f^t$ extends to a continuous morphism $\mathbf{Z}_p \to D$. If $\hat{f}$ denotes the image of f in $\hat{D}$, then $t \mapsto (\hat{f})^t$ is a morphism from $\mathbf{Z}$ to the pro-p group $\hat{D}$; as such, it extends canocially to the pro-p completion $\mathbf{Z}_p$, giving rise to a morphism $t \in \mathbf{Z}_p \mapsto (\hat{f})^t \in \hat{D}$. These two extensions are compatible: $\widehat{(f^t)} = (\hat{f})^t$ for all t in $\mathbf{Z}_p$.

Thus, given any one-parameter subgroup $\mathbf{Z}$ of Γ, we already know how to extend $\Phi\colon \mathbf{Z} \subset \Gamma \to D$ into $\Phi\colon \mathbf{Z}_p \subset G \to D$, in a way that is compatible with the extension $\hat{\Phi}\colon G \to \hat{D}$.

Lemma 2.13. *Let (α_n) be a sequence of elements of Γ that converges towards 1_G in G. Then $\Phi(\alpha_n)$ converges towards the identity in $\mathsf{Diff}^{an}(\mathcal{U})$.*

Proof. Write $\alpha_n = \pi(t_1(n), \ldots, t_r(n)) = \gamma_1^{t_1(n)} \cdots \gamma_r^{t_r(n)}$, where π and the γ_i are given by Lemma 2.11. Since α_n converges towards 1_G, we may assume that each $(t_i(n))$ converges towards 0 in $\mathbf{Z}_p$ as n goes to $+\infty$. By Bell-Poonen theorem, each $f_i := \Phi(\gamma_i)$ gives rise to a flow $t \mapsto f_i^t$, t in $\mathbf{Z}_p$; moreover, $\parallel f_i^t - \mathsf{id} \parallel \leq p^m$ if $|t| < p^m$ (apply Lemma 2.3 and the last assertion in Bell-Poonen theorem). Thus, the lemma follows from Lemma 2.2 and the following equality

$$\Phi(\alpha_n) = f_1^{t_1(n)} \cdots f_r^{t_r(n)}. \tag{2.3}$$

To prove this equality, one only needs to check it in the group $\hat{D}$ because D embeds into $\hat{D}$. But in $\hat{D}$, the equality holds trivially because the morphism $\Gamma \to \hat{D}$ extends to G continuously (apply Properties (1) and (2) above). □

Lemma 2.14. *If $(g_m)_{m\geq 1}$ is a sequence of elements of Γ that converges towards an element g_∞ of G, then $\Phi(g_m)$ converges to an element of $\mathsf{Diff}^{an}(\mathcal{U})$ which depends only on g_∞.*

Proof. Since (g_m) converges, $g_m \circ g_{m'}^{-1}$ converges towards the neutral element 1_G as m and m' go to $+\infty$. Consequently, the previous lemma shows that the sequence $(\Phi(g_m))$ is a Cauchy sequence, hence a convergent sequence, in $\mathsf{Diff}^{an}(\mathcal{U})$.[1] The limit depends only on g_∞, not on the choice of the sequence

[1]Write $\Phi(g_m \circ g_{m'}^{-1}) = \mathrm{id} + \varepsilon_{m,m'}$ where $\varepsilon_{m,m'}$ is equivalent to the constant map 0 in $R\langle x\rangle^d$ modulo $|p|^{k(m,m')}$, with $k(m,m')$ that goes to $+\infty$ as m and m' do. Then, apply Lemma 2.2.

(g_m) (if another sequence (g'_m) converges toward g_∞, consider the sequence $g_1, g'_1, g_2, g'_2, \ldots$). $\square$

We can now prove Theorem 2.12. Lemmas 2.13 and 2.14 show that Φ extends, in a unique way, to a continuous morphism $\overline{\Phi}\colon G \to D$ (with $D = \mathsf{Diff}^{an}(\mathcal{U})_1$). Moreover, this extension coincides with Bell-Poonen extensions $\mathbf{Z}_p \to D$ along one parameter subgroups of G generated by elements of Γ. According to Lemma 2.11 (and its proof), one can find s elements $\gamma_1, \ldots, \gamma_s$ of Γ, with $s = \dim(G)$, such that the map

$$(t_1, \ldots, t_s) \mapsto \pi(t_1, \ldots, t_s) = \gamma_1^{t_1} \cdots \gamma_s^{t_s}$$

determines an analytic diffeomorphism from a neighborhood of 0 in $\mathbf{Z}_p^s$ to a neighborhood of the identity in G. By Bell-Poonen theorem, the map

$$(t_1, \ldots, t_s, x) \in (\mathbf{Z}_p)^s \times \mathcal{U} \mapsto \Phi(\gamma_1)^{t_1} \circ \cdots \Phi(\gamma_s)^{t_s}(x)$$

is analytic. Thus, the action of G on $\mathcal{U}$ determined by $\overline{\Phi}$ is analytic. This concludes the proof od Theorem 2.12.

3. Regular actions of $\mathsf{SL}_n(\mathbf{Z})$ on quasi-projective varieties

In this section, we prove the first assertion of Theorem A together with one of its corollaries.

Theorem 3.1. *Let n be a positive integer. Let Γ be a finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$. If Γ embeds into the group of automorphisms of a complex quasi-projective variety X, then $\dim(X) \geq n-1$; if X is a complex affine space, then $\dim(X) \geq n$.*

3.1. **Dimension 1.** When $\dim_{\mathbf{C}}(X) = 1$, the group of automorphisms of X is isomorphic to $\mathsf{PGL}_2(\mathbf{C})$ if X is the projective line and virtually solvable otherwise. On the other hand, every finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$ contains a free group if $n \geq 2$ (see [19], Chapter 1). Theorems A and 3.1 follow from these remarks when $n = 2$. There is nothing to prove when $n = 1$. Thus, in what follows, we assume $\dim_{\mathbf{C}}(X) \geq 2$ and $n \geq 3$.

3.2. **From complex to p-adics coefficients.** Let X be a complex quasi-projective variety. Fix an embedding of X into a projective space $\mathbb{P}^N_{\mathbf{C}}$ and write

$$X = \mathcal{Z}(\mathfrak{a}) \setminus \mathcal{Z}(\mathfrak{b})$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are two homogeneous ideals in $\mathbf{C}[x_0,\ldots,x_N]$ and $\mathcal{Z}(\mathfrak{a})$ denotes the zeros of the ideal $\mathfrak{a}$. Choose generators $(F_i)_{1\leq i\leq a}$ and $(G_j)_{1\leq j\leq b}$ for $\mathfrak{a}$ and $\mathfrak{b}$ respectively.

Let Γ be a subgroup of $\mathsf{Bir}(X_{\mathbf{C}})$ with a finite, symmetric set of generators $S=\{\gamma_1,\ldots,\gamma_s\}$. Let C be a finitely generated $\mathbf{Q}$-algebra containing the set B of all coefficients of the F_i, the G_j, and the polynomials defining the γ_k; more precisely, each γ_k is defined by explicit formulas on affine open subsets $\mathcal{U}_l = X\setminus W_l$ and one includes the coefficients of these formulas and of the defining equations of the Zariski closed subsets W_l. One can view X and Γ as defined over $\mathrm{Spec}(C)$.

Lemma 3.2 (see Lech [35], and Bell [4])**.** *Let F be a finitely generated extension of $\mathbf{Q}$ and B be a finite subset of F. There exist infinitely many primes p such that F embeds in $\mathbf{Q}_p$; moreover, one can choose this embedding so that B embeds into $\mathbf{Z}_p$.*

Apply this lemma to the fraction field F of C and the set B of coefficients. This provides a model of X over $\mathbf{Z}_p$ such that Γ embeds into $\mathsf{Bir}(X_{\mathbf{Z}_p})$ – or in $\mathsf{Aut}(X_{\mathbf{Z}_p})$ if Γ is initially a subgroup of $\mathsf{Aut}(X_{\mathbf{C}})$. More generally, given any finite extension K of $\mathbf{Q}_p$ (for some prime p) and any embedding of the field $F=\mathsf{Frac}(C)$ into K that maps B into the valuation ring R of K, one obtains what will be called a **model of the pair** (X,Γ) **over** R. We refer to [4, 3] for the details regarding this construction and to Section 8.1 for the notion of good models, in the case of groups of birational transformations.

3.3. **From automorphisms to local analytic diffeomorphisms.** Let p be a prime number. Let Γ be a subgroup of $\mathsf{Aut}(X_{\mathbf{Z}_p})$ for some algebraic variety of dimension d. If X is the affine space, this just means that all elements of Γ are polynomial automorphisms of X defined by formulas with coefficients in $\mathbf{Z}_p$.

3.3.1. Let us first assume, for simplicity, that X is the affine space $\mathbb{A}^d$. Reduction modulo p provides a morphism from Γ to the group $\mathsf{Aut}(\mathbb{A}^d_{\mathbb{F}_p})$: Every automorphism $f\in\Gamma$ determines an automorphism $\overline{f}$ of the affine space with coefficients in $\mathbb{F}_p$. One can also reduce modulo p^2, p^3, ...

If R_0 is a finite ring, then $\mathbb{A}^d(R_0)$ and $\mathsf{GL}_d(R_0)$ are both finite. Therefore, the automorphisms $f\in\Gamma$ with $f(m)=m \pmod{p^2}$ and $df_m=\mathrm{Id} \pmod{p}$ for all points m in $\mathbb{A}^d(\mathbf{Z}_p)$ form a finite index subgroup Γ_0 of Γ. Every element of

Γ_0 can be written

$$f(x) = p^2x_0 + (\mathrm{Id} + pB)(x) + \sum_{k\geq 2} A_k(x)$$

where x_0 is a point with coordinates in $\mathbf{Z}_p$, B is a $d\times d$ matrix with coefficients in $\mathbf{Z}_p$, and $\sum_k r_k(x)$ is a finite sum of higher degree homogeneous terms with coefficients in $\mathbf{Z}_p$. Rescaling, one gets

$$p^{-1}f(px) = px_0 + (\mathrm{Id} + pB)(x) + \sum_{k\geq 2} p^{k-1}A_k(x).$$

This proves the following lemma.

Lemma 3.3. *Let Γ be a group of automorphisms of $\mathsf{Aut}(\mathbb{A}^d_{\mathbf{Z}_p})$. Changing Γ into a finite index subgroup, and conjugating by the scalar multiplication $x\mapsto px$, one can assume that Γ is a subgroup of $\mathsf{Aut}(\mathbb{A}^d_{\mathbf{Z}_p})$ with $f(x)\equiv x \pmod p$ for all f in Γ.*

A similar argument applies to every quasi-projective variety X of dimension d. One first needs to replace $\mathbf{Q}_p$ into a finite extension K to assure the existence of at least one point m in $X(R/\mathbf{m}_K)$. Then, the stabilizer of m is a finite index subgroup, because $X(R/\mathbf{m}_K)$ is a finite set; this group fixes a polydisk in $X(K)$ and Bell-Poonen theorem can be applied to a smaller, finite index subgroup. This provides the following statement, the proof of which is given in [3] (see also Section 8 for groups of birational transformations).

Proposition 3.4 (see [3])**.** *Let $X_{\mathbf{Z}_p}$ be a quasi-projective variety defined over $\mathbf{Z}_p$ and let Γ be a finitely generated subgroup of $\mathsf{Aut}(X_{\mathbf{Z}_p})$. Then, changing $\mathbf{Q}_p$ into a finite extension K, and Γ in a finite index subgroup, one can find a local analytic diffeomorphism φ from the unit polydisk $\mathcal{U} = R^d \subset K^d$ to an open subset $\mathcal{V}$ of $X(K)$ such that $\mathcal{V}$ is Γ-invariant and the action of Γ on $\mathcal{V}$ is conjugate, via φ, to a subgroup of $\mathsf{Diff}^{an}(\mathcal{U})_1$.*

From now on, we assume that Γ has been replaced by an appropriate finite index subgroup, so as to satisfy the conclusion of Proposition 3.4. Apply Bell-Poonen theorem: Every element f of Γ determines both an analytic diffeomorphism of the polydisk $\mathcal{U} = R^d$ and a flow $\Phi_f\colon \mathcal{U}\times R\to\mathcal{U}$ parametrized by R with $\Phi(\cdot,1) = f(\cdot)$. In other words, the morphism

$$\Phi\colon \Gamma\to \mathsf{Diff}^{an}(\mathcal{U})$$

extends as a R-flow along each cyclic subgroup of Γ.

3.4. **Congruence subgroups of $\mathsf{SL}_n(\mathbf{Z})$; see** [1, 45]**.**

3.4.1. *Normal subgroups.* For $n \geq 3$, the group $\mathsf{SL}_n(\mathbf{Z})$ is a lattice in the higher rank simple Lie group $\mathsf{SL}_n(\mathbf{R})$. For such a lattice, every normal subgroup is either finite and central, or co-finite; in particular, if Γ is a finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$, the derived subgroup of Γ has finite index in Γ.

3.4.2. *Strong approximation.* For any $n \geq 2$ and $q \geq 1$, denote by Γ_q and Γ_q^* the following subgroups of $\mathsf{SL}_n(\mathbf{Z})$:

$$\begin{aligned} \Gamma_q &= \{B \in \mathsf{SL}_n(\mathbf{Z}) \mid B \equiv \mathrm{Id} \pmod{q}\}, \\ \Gamma_q^* &= \{B \in \mathsf{SL}_n(\mathbf{Z}) \mid \exists a \in \mathbf{Z},\, B \equiv a\mathrm{Id} \pmod{q}\}. \end{aligned}$$

Let p be a prime number. The closure of Γ_q in $\mathsf{SL}_n(\mathbf{Z}_p)$ is the finite index open subgroup of matrices which are equal to Id modulo q; thus, if $q = p^m r$ with $r \wedge p = 1$, the closure of Γ_q in $\mathsf{SL}_n(\mathbf{Q}_p)$ coincides with the open subgroup of matrices $M \in \mathsf{SL}_n(\mathbf{Z}_p)$ which are equal to Id modulo p^m. This result is an instance of the strong approximation theorem.

3.4.3. *Congruence subgroup property.* Another deep property that we shall use is the congruence subgroup property, which holds for $n \geq 3$. It asserts that, given any finite index subgroup Γ of $\mathsf{SL}_n(\mathbf{Z})$, there exists a unique integer q with $\Gamma_q \subset \Gamma \subset \Gamma_q^*$. We shall come back to this property in Section 7.1 for more general algebraic groups (note that the congruence subgroup property is not known for co-compact lattices).

3.5. **Extension, algebraic groups, and Lie algebras.** Given an analytic diffeomorphism f of the unit polydisk $\mathcal{U}$, its jacobian determinant is an analytic function which is defined by $\mathsf{Jac}(f)(x) = \det(df_x)$, where df_x is the differential of f at x. One says that the jacobian determinant of f is identically equal to 1, if $\mathsf{Jac}(f)$ is the constant function 1.

In the following theorem, p is an odd prime, and K and R are as in Section 2.1.1.

Theorem 3.5. *Let $n \geq 3$ be an integer. Let Γ be a finite index subgroup in $\mathsf{SL}_n(\mathbf{Z})$. Let $\mathcal{U}$ be the unit polydisk $\mathbf{Z}_p^d$, for some $d \geq 1$. Let $\Phi\colon \Gamma \to \mathsf{Diff}^{an}(\mathcal{U})$ be a morphism such that $f(x) \equiv x \pmod{p}$ for all f in $\Phi(\Gamma)$. If the image of Φ is infinite, then $n - 1 \leq d$. If, moreover, the jacobian determinant is identically equal to 1 for all f in $\Phi(\Gamma)$, then $n \leq d$.*

Remark 3.6. All proper algebraic subgroups of minimal co-dimension in $\mathsf{SL}_n(\mathbf{Q}_p)$ are conjugate to the stabilizer of a point in $\mathbb{P}^{n-1}(\mathbf{Q}_p)$; their co-dimension is equal to $n-1$. Similarly, all proper sub-algebras of $\mathfrak{sl}_n(\mathbf{Q}_p)$ have co-dimension $\geq n-1$. (see § 7.2).

Proof. Let G be the closure of Γ in $\mathsf{SL}_n(\mathbf{Q}_p)$. By Theorem 2.12, Φ extends to an analytic morphism $\overline{\Phi}$ of the group G to $\mathsf{Diff}^{an}(\mathcal{U})$. The differential $d\overline{\Phi}_{\mathrm{Id}}$ provides a morphism of Lie algebras

$$d\overline{\Phi}_{\mathrm{Id}} \colon \mathfrak{sl}_n(\mathbf{Q}_p) \to \Theta(\mathcal{U}),$$

where $\Theta(\mathcal{U})$ is the algebra of analytic vector fields on $\mathcal{U}$. If the image of Φ is infinite, its kernel is a finite central subgroup of Γ (see § 3.4); hence, there are infinite order elements in $\Phi(\Gamma)$. The vector field corresponding to such an element does not vanish identically, so that $d\overline{\Phi}_{\mathrm{Id}}$ is a non-trivial morphism. Since $\mathfrak{sl}_n(\mathbf{Q}_p)$ is a simple Lie algebra, $d\overline{\Phi}_{\mathrm{Id}}$ is an embedding. Pick w in $\mathfrak{sl}_n(\mathbf{Q}_p)\setminus\{0\}$. Since $d\overline{\Phi}_{\mathrm{Id}}$ is an embedding, there is a point o in $\mathcal{U}$ such that $d\overline{\Phi}_{\mathrm{Id}}(w)(o)\neq 0$. The subset of $\mathfrak{sl}_n(\mathbf{Q}_p)$ whose elements satisfy $d\overline{\Phi}_{\mathrm{Id}}(v)(o)=0$ is a proper subalgebra of $\mathfrak{sl}_n(\mathbf{Q}_p)$ of co-dimension at most d. Thus, $d\geq n-1$ by Remark 3.6.

Let us now assume $d=n-1$. There is a unique subgroup of SL_n of co-dimension $n-1$ up to conjugacy, and this group is the parabolic subgroup P_0 that stabilizes the point $m_0=[1:0:0\ldots:0]$ in the projective space $\mathbb{P}^{n-1}$. The quotient of $\mathfrak{sl}_n$ by the Lie algebra $\mathfrak{p}_0$ of P_0 can be identified to the tangent space $T_{m_0}\mathbb{P}^{n-1}$ of $\mathbb{P}^{n-1}$ at m_0, and to the tangent space of $\mathcal{U}$ at the fixed point o. The group P_0 contains the diagonal matrices with diagonal coefficients $a_{11}=a$ and $a_{ii}=b$ for $2\leq i\leq n$, where a and b satisfy the relation $ab^{n-1}=1$, and those diagonal matrices act by multiplication by a/b on $T_{m_0}\mathbb{P}^{n-1}$. Thus there are elements g in G fixing the point o in $\mathcal{U}$ and acting by non-trivial scalar multiplication on the tangent space $T_0\mathcal{U}$; such elements have jacobian determinant $\neq 1$. Since Γ is dense in G, and bot Φ and Jac are continuous, there are elements f in Γ with $\mathsf{Jac}(f)\neq 1$. □

3.6. **Embeddings of $\mathsf{SL}_n(\mathbf{Z})$ in $\mathsf{Aut}(X)$ or $\mathsf{Aut}(\mathbb{A}^d_{\mathbf{C}})$.** We may now prove Theorem 3.1. According to Section 3.1 we assume $n\geq 3$. Let d be the dimension of X and $\Phi\colon \Gamma\to\mathsf{Aut}(X)$ be a morphism with infinite image. Changing Γ in a finite index subgroup, we assume that Γ is a congruence subgroup and that Φ is an embedding.

According to Section 3.2 and Proposition 3.4, one can find a prime $p \geq 3$, a model of (X,Γ) over a finite extension K of $\mathbf{Q}_p$, and a polydisk $\mathcal{U} = R^d$ in $X(K)$ which is invariant by a finite index subgroup of Γ; this provides an embedding of a finite index subgroup of Γ in $\mathsf{Diff}^{an}(\mathcal{U})_1$. Theorem 3.5 implies $\dim(X) \geq n-1$.

Assume now that X is the affine space $\mathbb{A}^d_{\mathbf{C}}$. If f is an automorphism of $\mathbb{A}^d_{\mathbf{C}}$, its jacobian determinant $\mathsf{Jac}(f)$ is constant because $\mathsf{Jac}(f)$ is a polynomial function on $\mathbb{A}^d(\mathbf{C})$ that does not vanish. This provides a morphism from Γ to $(\mathbf{C}^*,\cdot)$; since congruence subgroups are almost perfect ($[\Gamma,\Gamma]$ has finite index in Γ), one can change Γ in a smaller congruence subgroup and assume that $\mathsf{Jac}(\Phi(\gamma)) = 1$ for all $\gamma \in \Gamma$. Then, Theorem 3.5 implies $d \geq n$.

4. Actions of $\mathsf{SL}_n(\mathbf{Z})$ in dimension $n-1$

In this paragraph, we pursue the study of algebraic actions of finite index subgroups of $\mathsf{SL}_n(\mathbf{Z})$ on quasi-projective varieties X of dimension d, and complete the proof of Theorem A. The notation and main properties are the same as in Section 3, but with a constraint on the dimension of X; thus

- Γ is a finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$,
- $X_{\mathbf{C}}$ is a complex quasi-projective variety of dimension $d = n-1$,
- Γ embeds into $\mathsf{Aut}(X_{\mathbf{C}})$,
- there is a finite extension K of $\mathbf{Q}_p$, and a model of (X,Γ) over the valuation ring R of K, together with a polydisk $\mathcal{U}$ in $X(K)$ which is Γ invariant, and on which Γ acts by analytic diffeomorphisms (as in Proposition 3.4).

To conclude the proof of Theorem A, our goal is to show that X is isomorphic to the projective space of dimension $d = n-1$.

Remark 4.1. We shall simultaneously deal with a closely related situation, in which X is a projective variety of dimension $n-1$, Γ acts by birational transformations on X, and there is a Γ-invariant polydisk $\mathcal{U}$ in $X(K)$ on which Γ acts by analytic diffeomorphisms (in particular, $\mathcal{U}$ does not contain any indeterminacy point of Γ). Our goal is to prove that X is rational. Each time the proof requires a modification, we add a comment or state a separate lemma.

4.1. **Stabilizer of the origin in $\mathcal{U}$.** Let P_0 be the subgroup of $\mathsf{SL}_n(\mathbf{Q}_p)$ which fixes the point $m_0 = [1\colon 0\colon \cdots\colon 0]$ in the projective space $\mathbb{P}^{n-1}(\mathbf{Q}_p)$; it is a maximal parabolic subgroup of $\mathsf{SL}_n(\mathbf{Q}_p)$. Let $\mathfrak{p}_0$ denote its Lie algebra.

We may assume that Γ is a congruence subgroup Γ_q of $\mathsf{SL}_n(\mathbf{Z})$ and the morphism Φ from Γ to $\mathsf{Diff}^{an}(\mathcal{U})$ extends to an analytic morphism from the p-adic Lie group $G = \overline{\Gamma}$ to $\mathsf{Diff}^{an}(\mathcal{U})$. Since $d = n-1$, we may assume that the stabilizer $P \subset G$ of the origin $o \in \mathcal{U}$ is a maximal parabolic subgroup of G. Hence, in $\mathfrak{g} = \mathfrak{sl}_n(\mathbf{Q}_p)$, the Lie algebra $\mathfrak{p}$ of P is conjugate to the standard maximal parabolic algebra $\mathfrak{p}_0$ over the field $\mathbf{Q}_p$ (see [5], chapter 5). Let $\tilde{P}$ be the Zariski closure of P in $\mathsf{SL}_n(\mathbf{Q}_p)$, so that $\tilde{P} \cap G$ coïncides with P. Since $\tilde{P}$ is a parabolic subgroup of $\mathsf{SL}_n(\mathbf{Q}_p)$ of co-dimension $n-1$, it is conjugate to P_0 in $\mathsf{SL}_n(\mathbf{Q}_p)$ (it fixes a point in $\mathbb{P}^{n-1}(\mathbf{Q}_p)$).

Lemma 4.2. *There is an element A in $\mathsf{SL}_n(\mathbf{Z})$ and a point o' in $\mathcal{U}$ with the following properties. Changing Φ into $\Phi \circ c_A$, where c_A is the conjugacy $c_A(M) = AMA^{-1}$, the stabilizer $P' \subset G$ of the point o' coincides with $P_0 \cap G$.*

The proof follows from the following remarks.

(1) There is a point $[a]$ in $\mathbb{P}^{n-1}(\mathbf{Q}_p)$ such that $\tilde{P}$ is the stabilizer of $[a]$ in $\mathsf{SL}_n(\mathbf{Q}_p)$. One can write $[a] = [a_1 : \ldots : a_n]$ with a_i in $\mathbf{Z}_p$ and at least one $|a_i|$ equal to 1.
(2) There is a matrix B in G such that $B[a]$ is in $\mathbb{P}^{n-1}(\mathbf{Z})$. Indeed, G is the congruence subgroup of $\mathsf{SL}_n(\mathbf{Z}_p)$ defined as the group of matrices M with $M \equiv \mathsf{Id} \pmod{q}$ for some integer q; if one picks an element $[a'] = [a'_1 : \ldots : a'_n]$ of $\mathbb{P}^{n-1}(\mathbf{Z})$ with entries $a'_i \equiv a_i$ modulo a large power of q, then there is an element B of G that maps $[a]$ to $[a']$. The stabilizer of the point $o' := \Phi(B)(0)$ in the group G is equal to BPB^{-1} and coincides with the stabilizer of a point $[a'] \in \mathbb{P}^{n-1}(\mathbf{Z})$.
(3) Then, there exists A in $\mathsf{SL}_n(\mathbf{Z})$ such that $A[a'] = [1 : 0 : \cdots : 0]$. Composing Φ with the conjugation c_A, the stabilizer of o' is now equal to $P_0 \cap G$.
(4) Being a congruence subgroup, Γ is normal in $\mathsf{SL}_n(\mathbf{Z})$; it is therefore invariant under the conjugacy $c_A \colon M \mapsto AMA^{-1}$. Thus, the morphism $\Phi \circ c_A$ determines a new morphism from Γ to $\mathsf{Aut}(X_K)$ which preserves the polydisk $\mathcal{U}$ and for which the stabilizer of o' coïncides with $P_0 \cap G$.

We can then conjugate the action of Γ on $\mathcal{U}$ by the translation $x \mapsto x + o'$ to assume that *the stabilizer of the origin in G is the intersection of G with the parabolic subgroup P_0*. (note that the embedding of Γ in $\mathsf{Aut}(X)$ has been twisted by the automorphism c_A of Γ, for some matrix A in $\mathsf{SL}_n(\mathbf{Z})$; it may happen that this automorphism is not an interior automorphism of Γ.

4.2. **Local normal form.** Consider the abelian subgroup T of G made of all matrices

$$\begin{pmatrix} 1 & 0 \\ \mathbf{t} & \mathsf{Id} \end{pmatrix}$$

where Id is the identity matrix of size $(n-1)\times(n-1)$ and $\mathbf{t}$ is a “vertical" vector of size $(n-1)$ with entries $t_2,\ldots,t_n$ in $\mathbf{Z}_p$; the entries t_i are equal to 0 modulo q if Γ is the congruence subgroup Γ_q. The intersection $T\cap P_0$ is the trivial subgroup $\{\mathsf{Id}\}$.

The group T is an abelian subgroup of G that acts locally freely near the origin of $\mathcal{U}$ (if not, this would contradict the maximality of P). Thus, the t_i may be used as local coordinates around 0 in $\mathcal{U}$. In these coordinates, the action of the group G is locally conjugate to the linear projective action of G around the point $m_0 = [1:0\cdots:0]$ in $\mathbb{P}^{n-1}(K)$.

Note that the local coordinate t_i may be transcendental; it is not obvious, a priori, that t_i extends as an algebraic (rational) function on the quasi-projective variety X. We shall prove that this is indeed the case in the next subsection (see Lemma 4.3)

4.3. **Invariant (algebraic) functions.** Consider the one-parameter unipotent subgroup E_{12} of P whose elements have the form

$$\begin{pmatrix} 1 & \mathbf{s} \\ 0 & \mathsf{Id} \end{pmatrix}$$

with $\mathbf{s} = (s,0,\ldots,0)$, s in $\mathbf{Z}_p$, and $s\equiv 0$ modulo q. Let α_{12} be a non-trivial element of $E_{12}\cap\Gamma$. By construction, the automorphism α_{12} of $\mathcal{U}$ transforms the local coordinate t_2 into $\frac{t_2}{1+mt_2}$ for some integer $m\neq 0$, and the set $\{t_2=0\}$ is, locally, the set of fixed points of α_{12}. Thus, the hypersurface $\{t_2=0\}$ is the intersection of an algebraic hypersurface of X with a neighborhood of 0 in $\mathcal{U}$.

Let α_{21} be a non-trivial element of $T\cap\Gamma$ corresponding to a vector $\mathbf{t}$ of type $(t,0,\ldots,0)$ (with $t\neq 0$ and $t\equiv 0$ modulo q). Then α_{21}^{ℓ} acts on $\mathcal{U}$ and transports the hypersurface $\{t_2=0\}$ to the hypersurface $\{t_2=t\ell\}$. Since $\{t_2=0\}$ is algebraic and α_{21} is in $\mathsf{Aut}(X)$ (resp. in $\mathsf{Bir}(X)$ in the situation of Remark 4.1), the hypersurfaces $\{t_2=t\ell\}$ are all algebraic.

Denote by T_2 the subgroup of T whose elements are defined by vectors of type $\mathbf{t}=(0,t_3,\ldots,t_n)$. The action of this subgroup on $\mathcal{U}$ preserves the local coordinate t_2 and is locally transitive on each level set $\{t_2=c^{st}\}$. Thus, each non-trivial element of $T_2\cap\Gamma$ fixes infinitely many algebraic hypersurfaces in X, whose local equations are $t_2=\ell t$, $\ell\in\mathbf{Z}$; moreover, the orbits of $T_2\cap\Gamma$ are

Zariski dense on these hypersurfaces. Let us now apply Theorem B of [8], or more precisely its proof, to the group T_2 (Theorem B is stated for a single transformation g but applies to a finitely generated group with infinitely many invariant hypersurfaces). Together with Stein factorization, we deduce that there is a curve $Y_{\overline{K}}$ and a rational function $\tau_2\colon X_{\overline{K}} \dashrightarrow Y_{\overline{K}}$, both defined over the algebraic closure of K, such that

- τ_2 is invariant under the action of $T_2 \cap \Gamma$, meaning that $\tau_2 \circ \beta = \tau_2$ for every β in $T_2 \cap \Gamma$.
- the generic hypersurface $\{\tau_2 = c^{st}\}$ is irreducible.

Since the orbits of T_2 along the invariant hypersurfaces $\{t_2 = \ell t\}$ are Zariski dense and the action of T_2 on $Y_{\overline{K}}$ is trivial, the projection τ_2 is constant along each of these hypersurfaces. As a consequence, the local analytic coordinate t_2 is, locally, a function of τ_2: There is an analytic one-variable function ϕ_2 such that $t_2 = \phi_2 \circ \tau_2$.

The transformation α_{12} transforms t_2 into $\frac{t_2}{1+mt_2}$ for some $m \neq 0$. Thus, it permutes the level sets of the algebraic function τ_2, and induces an infinite order automorphism of $Y_{\overline{K}}$ fixing the point $\tau_2(\{t_2 = 0\})$. This implies that $Y_{\overline{K}}$ is a projective line $\mathbb{P}^1_{\overline{K}}$: There is an isomorphism from $Y_{\overline{K}}$ to $\mathbb{P}^1_{\overline{K}}$ that maps the point $\tau_2(\{t_2 = 0\})$ to the point $[0:1]$. We now fix an affine coordinate z on $\mathbb{P}^1_{\overline{K}}$ for which this point is $z = 0$.

The iterates α_{12}^{ℓ} of α_{12} transform the coordinate t_2 into

$$\frac{t_2}{1+\ell m t_2}.$$

Thus, if $\ell = p^n$, one sees that the sequences of hypersurfaces $\alpha_{12}^{+\ell}(\{t_2 = c^{st}\})$ and $\alpha_{12}^{-\ell}(\{t_2 = c^{st}\})$ converge both to the fixed hypersurface $\{t_2 = 0\}$. This implies that the automorphism of $\mathbb{P}^1_{\overline{K}}$ induced by α_{12} is a parabolic transformation, acting by

$$z \mapsto \frac{z}{1+m'z}$$

for some m'. Changing the affine coordinate z of $\mathbb{P}^1_{\overline{K}}$ into εz with $\varepsilon = m'/m$ (hence the function τ_2 into $\varepsilon\tau_2$ and $\phi_2(x)$ into $\phi_2(x/\varepsilon)$), one may assume that $m' = m$. Then, both τ_2 and t_2 satisfy the same transformation rule under α_{12}:

$$\tau_2 \circ \alpha_{12} = \frac{\tau_2}{1+m\tau_2}, \quad t_2 \circ \alpha_{12} = \frac{t_2}{1+mt_2}.$$

We deduce that the function ϕ_2 commutes with the linear projective transformation $z \mapsto z/(1+mz)$:

$$\forall \ell \in \mathbf{Z}, \quad \phi_2\left(\frac{z}{1+\ell mz}\right) = \frac{\phi_2(z)}{1+\ell m \phi_2(z)}. \tag{4.1}$$

By construction ϕ_2 is analytic (in a neighborhood of 0) and maps 0 to 0. Changing $\phi_2(z)$ into $\phi_2(z/(1+uz))$ for some non-zero u, one may assume that $\phi_2(x_0) = x_0$ for some $x_0 \neq 0$. If one applies the functional equation (4.1) with $\ell \equiv 0$ modulo sufficiently large powers of p, then the sequence $x_\ell = x_0/(1+\ell m x_0)$ stays in the domain of definition of ϕ_2 and $\phi_2(x_\ell) = x_\ell$ for all ℓ; thus, ϕ_2 is the identity: $\phi_2(z) = z$.

This concludes the proof of the following lemma, because the local coordinates t_i coincide with the rational functions τ_i and provide a local conjugacy with the linear projective action of Γ on $\mathbb{P}^{n-1}_{\overline{K}}$.

Lemma 4.3. *Each local analytic function t_i, $i = 2, \ldots, n$, extends to a global rational function $\tau_i \dashrightarrow X_{\overline{K}} \to \overline{K}$. Altogether, they define a rational map*

$$\tau \colon X_{\overline{K}} \dashrightarrow \mathbb{P}^{n-1}_{\overline{K}},$$

defined by $\tau(x) = [1 : \tau_2(x) : \ldots : \tau_n(x)]$. This rational map τ is dominant, and is equivariant with respect to the action of Γ on X and the action of $\Gamma \subset \mathsf{SL}_n(\mathbf{Z})$ on $\mathbb{P}^{n-1}_{\overline{K}}$ by linear projective transformations.

4.4. **Conclusion.** We now assume that Γ acts by automorphisms on the quasi-projective variety X (the case of birational transformations, as in Remark 4.1, is dealt with below).

Lemma 4.4. *The variety $X_{\overline{K}}$ is complete, and the equivariant rational map $\tau \colon X_{\overline{K}} \to \mathbb{P}^{n-1}_{\overline{K}}$ is an isomorphism.*

Proof. Fix a compactification $\overline{X}_{\overline{K}}$ of $X_{\overline{K}}$. Via the morphism Φ, the group Γ acts by automorphisms on $X_{\overline{K}}$ and by birational transformations on $\overline{X}_{\overline{K}}$. The image of Γ in $\mathsf{PGL}_n(\overline{K}) = \mathsf{Aut}(\mathbb{P}^{n-1}_{\overline{K}})$ is a Zariski-dense subgroup Γ'. Let $\mathrm{Ind}(\tau)$ be the indeterminacy set of τ. Its intersection with $X_{\overline{K}}$ is a Γ-invariant algebraic subset, because Γ acts by automorphisms on both X and $\mathbb{P}^{n-1}_{\overline{K}}$. Its total transform under τ is a Γ'-invariant locally closed subset of $\mathbb{P}^{n-1}_{\overline{K}}$. But all such subsets are either empty or equal to $\mathbb{P}^{n-1}_{\overline{K}}$ because Γ' is a Zariski-dense subgroup of $\mathsf{PGL}_n(\overline{K})$. Thus, $\mathrm{Ind}(\tau)$ does not intersect $X_{\overline{K}}$.

In particular, the image of $X_{\overline{K}}$ by τ is a constructible Γ'-invariant subset of $\mathbb{P}^{n-1}_{\overline{K}}$; as such, it must be equal to $\mathbb{P}^{n-1}_{\overline{K}}$. Similarly, the total transform of the boundary $\overline{X}_{\overline{K}} \setminus X_{\overline{K}}$ is empty. Thus, $X_{\overline{K}}$ is complete, and τ determines a morphism from $X_{\overline{K}}$ to $\mathbb{P}^{n-1}_{\overline{K}}$. The critical locus of τ is a Γ'-invariant subset of $\mathbb{P}^{n-1}_{\overline{K}}$ of positive co-dimension: It is therefore empty, and τ is an isomorphism because $\mathbb{P}^{n-1}_{\overline{K}}$ is simply connected. $\square$

Since the model $X_{\overline{K}}$ is isomorphic to the projective space $\mathbb{P}^{n-1}_{\overline{K}}$, the complex variety $X_{\mathbf{C}}$ is isomorphic to $\mathbb{P}^{n-1}_{\mathbf{C}}$. This concludes the proof of Theorem A.

Let us now assume, as in Remark 4.1, that X is projective and Γ acts by birational transformations on X.

Lemma 4.5. *The equivariant rational mapping* $\tau\colon X_{\overline{K}} \dashrightarrow \mathbb{P}^{n-1}_{\overline{K}}$ *is birational.*

Proof. By construction, τ is rational and dominant; changing X in a birationally equivalent variety, we assume that τ is a regular morphism. The elements of Γ satisfy

$$\tau \circ f_X = f_{\mathbb{P}^{n-1}} \circ \tau$$

where f_X corresponds to the birational action on X and $f_{\mathbb{P}^{n-1}}$ corresponds to the linear projective action on $\mathbb{P}^{n-1}$. Embed X in some projective space $\mathbb{P}^N$, and consider the linear system of hyperplane sections H of X. Fix an element f of Γ, and intersect X with $n-1$ hyperplanes to get an irreducible curve $C \subset X$ that does not intersect the indeterminacy set of f. The image of C by f_X is an irreducible curve $(f_X)_*C$, which satisfies $\pi_*((f_X)_*(C)) = (f_{P^{n-1}})_*\tau_*(C)$. The degree of the curve $\tau_*(C)$ does not depend on f and is equal to the degree of $f_{\mathbb{P}^{n-1}})_*\tau_*(C)$ because $f_{\mathbb{P}^{n-1}}$ is a regular automorphism of the projective space. This implies that the degree of the curve $(f_X)_*C$ in $X \subset \mathbb{P}^N$ is bounded by an integer $D(\tau)$ that does not depend on f. As a consequence, the degrees of the formulas defining the elements f_X of Γ in $\mathsf{Bir}(X)$ are uniformly bounded. The following result shows that the group Γ is “regularizable" (see [48] and the references in [11]).

Theorem 4.6 (Weil regularization theorem)**.** *Let M be a projective variety, defined over an algebraically closed field. Let Γ be a subgroup of* $\mathsf{Bir}(M)$. *If there is a uniform upper bound on the degrees of the elements of Γ, then there exists a birational transformation $\varepsilon\colon M \dashrightarrow M'$ and a finite index subgroup Γ' of Γ such that $\varepsilon \circ \Gamma' \circ \varepsilon^{-1}$ is a subgroup of the connected component of the identity* $\mathsf{Aut}(M)^0$ *in* $\mathsf{Aut}(M)$.

In our context, this shows that, after conjugacy by a birational map $\varepsilon\colon X \dashrightarrow X'$, the group Γ becomes a group of automorphisms, up to finite index. The previous lemma then shows that $\varepsilon \circ \tau \circ \varepsilon^{-1}$ is birational (the proof of the lemma shows that X' is isomorphic to the projective space $\mathbb{P}^{n-1}$). □

Thus, under the assumption of Remark 4.1, one can change Γ in a finite index subgroup Γ' and find a birational conjugacy between the action of Γ' on X and the action of Γ' by linear projective transformation on the projective space.

5. Algebraic actions of mapping class groups and nilpotent groups

5.1. **Mapping class groups.** To show how the p-adic method may be applied to certain non-linear countable groups, we study the following problem: Given a positive integer g, what is the minimal dimension $\mathsf{ma}(g)$ of a quasi-projective variety X such that a finite index subgroup of the mapping class group $\mathsf{Mod}(g)$ embeds into $\mathsf{Aut}(X)$.

Theorem 5.1. *The minimal dimension* $\mathsf{ma}(g)$ *is equal to* 1 *for* $g = 1$*, and satisfies* $2g-1 \leq \mathsf{ma}(g) \leq 6g-6$ *for all* $g \geq 2$*.*

Proof. The upper bound is well known: Consider the variety of representations of the fundamental group $\pi_1(\Sigma_g)$ into SL_2, where Σ_g denotes the closed orientable surface of genus g. This variety is defined by the equation

$$\Pi_{i=1}^{g}[A_i, B_i] = \mathsf{Id}$$

with $(A_1, B_1, A_2, \ldots, B_g)$ in $(\mathsf{SL}_2)^{2g}$. The algebraic group SL_2 acts by conjugacy on this affine algebraic variety, and one denotes by $\chi(g, \mathsf{SL}_2)$ the quotient in the sense of geometric invariant theory. It is an affine variety on which the mapping class group $\mathsf{Mod}(g)$ acts almost faithfully (see [36, 37]). Its dimension is $6g-6$, as desired.

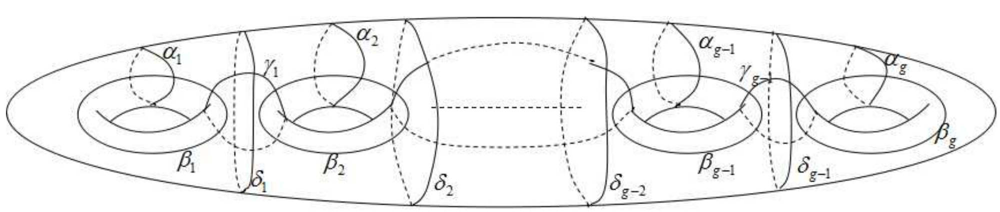

FIGURE 1. Simple closed loops on the surface of genus g.

The lower bound is obtained as follows. Let X be a quasi-projective variety of dimension d. Let Γ be a finite index subgroup of the mapping class group

$\mathsf{Mod}(g)$ acting faithfully on X, and identify Γ with its image in $\mathsf{Aut}(X)$. Denote by d the dimension of X. We need to show that $d \geq g$. From Sections 3.2 and 3.3, we know that there is a p-adic field $\mathbf{Q}_p$, a finite extension K of $\mathbf{Q}_p$, and a model of (X,Γ) over K; moreover, changing Γ in a finite index subgroup, one can find an analytic polydisk $\mathcal{U} \subset X(K)$ which is Γ-invariant. Then we have an embedding $\Gamma \to \mathsf{Diff}^{an}(\mathcal{U})$.

Denote by T_{α_i} and T_{β_i}, $i = 1,\dots,g$, and T_{γ_j}, $j = 1,\dots,g-1$, the Dehn twists along the simple closed loops which are depicted on Figure 1. There exists an integer $m \geq 1$ such that the twists $T_{\alpha_i}^m$, $T_{\beta_i}^m$, and $T_{\gamma_j}^m$ are all in Γ.

Observe that the g twists $T_{\alpha_i}^m$ commute to each other. From Bell-Poonen theorem, each of them determines a p-adic analytic flow on $\mathcal{U}$, hence an analytic vector field $\mathbf{X}_{T_{\alpha_i}^m}$; these vector fields commute. For $q \in \mathcal{U}$, denote by $s(q)$ the dimension of the K-linear space spanned by the tangent vectors $\mathbf{X}_{T_{\alpha_i}^m}(q)$, $1 \leq i \leq g$; let s be the maximum of $s(q)$, for q in $\mathcal{U}$.

Changing $\mathcal{U}$ in a smaller polydisk, there exists a subset S of $\{1,\dots,g\}$ such that $|S| = s$ and the $\mathbf{X}_{T_{\alpha_j}^m}(x)$, $j \in S$, are linearly independent at every point x of $\mathcal{U}$. Denote by $\mathbf{X}_j$ the vector field $\mathbf{X}_{T_{\alpha_j}^m}$ for j in S. Each $\mathbf{X}_{T_{\alpha_i}^m}$,$1 \leq i \leq g$, can be written in a unique way as a sum

$$\mathbf{X}_{T_{\alpha_i}^m} = \sum_{j\in S} F_{i,j}\mathbf{X}_j \tag{5.1}$$

where the $F_{i,j}$'s are analytic functions on $\mathcal{U}$. Since $[\mathbf{X}_{T_{\alpha_l}^m}, \mathbf{X}_{T_{\alpha_j}^m}] = 0$ for every pair of indices $l \in \{1,\dots g\}$ and $j \in S$, we obtain

$$\mathbf{X}_k F_{i,j} = 0 \tag{5.2}$$

for all $i \in \{1,\dots,g\}$ and j, $k \in S$.

Suppose that $S \neq \{1,\dots,g\}$, and pick an index k in $\{1,\dots,g\} \setminus S$. Observe that $T_{\beta_k}^m$ does not commute to $T_{\alpha_k}^m$ but commutes to the other $T_{\alpha_i}^m$; hence $[\mathbf{X}_{T_{\beta_k}^m}, \mathbf{X}_j] = 0$ for every $j \in S$. Assume that, for every x in $\mathcal{U}$, $\mathbf{X}_{T_{\beta_k}^m}(x)$ is a linear combination of the $\mathbf{X}_j(x)$, $j \in S$, and write

$$\mathbf{X}_{T_{\beta_k}^m} = \sum_{j\in S} G_{k,j}\mathbf{X}_j$$

where the $G_{k,j}$'s are analytic functions on $\mathcal{U}$. The commutation rules imply $\mathbf{X}_i G_{k,j} = 0$ for all indices i and j in S; thus, Equations (5.1) and (5.2) lead to

$$\mathbf{X}_{T_{\alpha_l}^m} G_{k,j} = 0$$

for all indices $l \in \{1, \dots g\}$. In particular, $[\mathbf{X}_{T^m_{\alpha_k}}, \mathbf{X}_{T^m_{\beta_k}}] = 0$, so that $T^m_{\beta_k}$ commutes to $T^m_{\alpha_k}$, a contradiction. So, replacing $\mathcal{U}$ by a smaller polydisk, we may assume that the vector fields $\{\mathbf{X}_{T^m_{\beta_k}}\} \cup \{\mathbf{X}_j, j \in S\}$ are linearly independent at every point x of $\mathcal{U}$. Now we add k to S and set $\mathbf{X}_k := \mathbf{X}_{T^m_{\beta_k}}$.

Repeat this argument to end up with a set $\mathbf{X}_i$, $i \in S = \{1, \dots, g\}$, of vector fields which are linearly independent at the generic point; these vector fields correspond to elements of type $T^m_{\alpha_i}$ or $T^m_{\beta_i}$, for a disjoint set of curves α_i and β_i. In what follows, we apply a conjugacy by an element of the mapping class group which maps this set of disjoint non-separating curves to α_1, …, α_g, and assume that each $\mathbf{X}_i$ is given by the twist $T^m_{\alpha_i}$.

Now, consider the curves γ_1 and δ_1. The Dehn twists $T^m_{\gamma_1}$ and $T^m_{\delta_1}$ generate a free subgroup of the mapping class group (see Theorem 3.14 in [26]), and they commute to the $T^m_{\alpha_i}$. If the vector field $\mathbf{Y}_1$ and $\mathbf{Z}_1$ corresponding to $T^m_{\gamma_1}$ and $T^m_{\delta_1}$ are combinations $\mathbf{Y}_1 = \sum H_{1,j}\mathbf{X}_i$, $\mathbf{Z}_1 = \sum H'_{1,j}\mathbf{X}_i$, then $T^m_{\gamma_1}$ and $T^m_{\delta_1}$ commute, a contradiction. Thus, one can add a vector field $\mathbf{Y}_1$ (or $\mathbf{Z}_1$) to our list of generically independant vector fields. Playing the same game with the curves γ_k and δ_k for $2 \leq k \leq g-1$, we end up with $2g-1$ vectors fields, and deduce that $\dim(X) \geq 2g-1$. □

5.2. **Nilpotent groups.** Let H be a group. Define $H^{(1)} = [H, H]$, the derived subgroup of H, generated by all commutators $aba^{-1}b^{-1}$ with a and b in H, and then inductively $H^{(r)} = [H^{(r-1)}, H^{(r-1)}]$. The first integer $r \geq 1$ such that $H^{(r)}$ is trivial is called the **derived length** of H; such an r exists if and only if H is solvable. This integer is denoted by $\mathsf{dl}(H)$, and similar notations are used for Lie algebras. Then, define the stable derived length of H by

$$\mathsf{sdl}(H) = \min\{\mathsf{dl}(H') \mid H' \text{ is a finite index subgroup of } H\}.$$

Theorem 5.2. *Let N be a finitely generated nilpotent group. If N acts faithfully by automorphisms on a complex quasi-projective variety X, then* $\mathsf{sdl}(H) \leq \dim(X)$.

The proof is a direct combination of the p-adic method, as used for finite index subgroups of $\mathsf{SL}_n(\mathbf{Z})$ and $\mathsf{Mod}(g)$, and the arguments of [11], §3.4.

6. Periodic orbits and invariant polydisks

In this section, our goal is to produce invariant p-adic polydisks for groups of birational transformations of a projective variety defined over $\mathbf{Q}_p$ (or a finite extension K of $\mathbf{Q}_p$). As explained in Sections 3.3 and 8, this is closely related to the existence of "good" periodic orbits for groups of birational transformations defined over a finite field F. Thus, we focus first on the construction of such orbits.

In what follows, Γ is a group with a finite symmetric set of generators S. Let $\mathcal{G} = \mathcal{G}(\Gamma, S)$ be its Cayley graph: Vertices are elements of the group, and two vertices g_1 and g_2 are joined by an edge if $g_1 = sg_2$ for some element $s \in S$.

6.1. **Kazhdan property (T) and linear isoperimetric inequalities.** In this section, we describe a consequence of Kazhdan property (T) which is well known to specialists of expander graphs and isoperimetric inequalities (see [20]).

6.1.1. *The graph of cosets.* Given a subgroup R of Γ, consider the set V_R of cosets $f \cdot R$, $f \in \Gamma$. Define a graph $\mathcal{G}_R$ as follows:

- the set of vertices of $\mathcal{G}_R$ is V_R;
- two vertices g_1R and $g_2R \in V_R$ are joined by an edge if and only if there exists $s \in S$ satisfying $g_2 = sg_1$.

When $R = \{e\}$, $\mathcal{G}_R$ is the Cayley graph of Γ. The group Γ acts by left translations on the set of vertices V_R; given h in Γ, we denote by L_h the translation $gR \mapsto hgR$. When R is a normal subgroup of Γ, then Γ also acts on the right, $gR \to gRh = ghR$, and this is an action by isometries.

Denote by $\mathbb{L}^2(\mathcal{G}_R)$ the space of $\mathbb{L}^2$-functions on V_R, i.e. functions $\varphi \colon V_R \to \mathbf{C}$ which are square integrable:

$$\| \varphi \|^2_{\mathbb{L}^2(\mathcal{G}_R)} := \sum_{\omega \in \mathcal{G}_R} |\varphi(\omega)|^2 < \infty.$$

The action of Γ on V_R by left translations determines a unitary representation $g \mapsto L^*_{g^{-1}}$ of Γ on $\mathbb{L}^2(\mathcal{G}_R)$, where $L^*_{g^{-1}}\varphi := \varphi \circ L_g^{-1}$.

Let Ω be a finite subset of V_R. Denote by $\chi_\Omega : V_R \to \{0,1\}$ the characteristic function of Ω, i.e. $\chi_\Omega(x) = 1$ if and only if $x \in \Omega$. Since Ω is finite, χ_Ω is square integrable. An element $x \in \Omega$ is in the **boundary** $\partial\Omega$ of Ω if and only if there exists an element y of $V_R \setminus \Omega$ which is connected to x by an edge of $\mathcal{G}_R$. In other words, $x \in \partial\Omega$ if and only if $x \in \Omega$ and there exists $s \in S$ such that $L_s(x) \notin \Omega$, if and only if $\chi_\Omega(x) = 1$ and there exists $s \in S$ such that $(L_s^*\chi_\Omega)(x) = 0$. Thus, we have

$$\begin{aligned}\|\chi_\Omega - L_s^*\chi_\Omega)\|^2_{\mathbb{L}^2(\mathcal{G}_R)} &= \sum_{x\in V_R}(\chi_\Omega(x)-\chi_\Omega(L_s x))^2 \\ &\leq \sum_{x\in\cup_{s\in S}(\Omega\Delta s^{-1}(\Omega))} 1^2\end{aligned}$$

and

$$\|\chi_\Omega - L_s^*\chi_\Omega)\|^2_{\mathbb{L}^2(\mathcal{G}_R)} \leq 2|S||\partial\Omega|. \tag{6.1}$$

6.1.2. *Kazhdan property (T) and isoperimetric inequality (see* [20]*).* A finitely generated group Γ has **Kazhdan property (T)** if for any finite symmetric set of generators S, there exists an $\varepsilon > 0$, which depends only on Γ and S, with the following property: Given any unitary representation ρ of Γ on a Hilbert space $\mathcal{H}$, either there exists $v \in \mathcal{H}$ with $\|v\| = 1$ and $\rho(\Gamma)\cdot v = v$, or, for every $v \in \mathcal{H}$, there exists $s \in S$ such that

$$\|\rho(s)\cdot v - v\| \geq \varepsilon\|v\|.$$

Such a positive number ε is called a **Kazhdan constant** for the pair (Γ, S).

Proposition 6.1. *Let Γ be a discrete group with Kazhdan property (T), let S be a finite symmetric set of generators of Γ, and let ε be a Kazhdan constant for the pair (Γ, S). Let R be a subgroup of Γ. Either $\mathcal{G}_R$ is finite, which means that R is a finite index subgroup of Γ, or $\mathcal{G}_R$ satisfies the following linear isoperimetric inequality:*

$$|\partial\Omega| \geq \frac{\varepsilon^2}{2|S|}|\Omega|$$

for every finite subset $\Omega \subseteq V_R$.

Proof. Consider the unitary action of Γ on $\mathbb{L}^2(\mathrm{X}_R)$ by left translations.

First case.– There exists a function $\varphi \in \mathbb{L}^2(\mathcal{G}_R)$ with $\mathbb{L}^2$-norm equal to 1 which is invariant under left translation. Such a function is constant because Γ acts transitively on V_R. Since $\varphi \not\equiv 0$, this implies $|\mathcal{G}_R| < \infty$.

Second case.– There is no invariant function in $\mathbb{L}^2(\mathcal{G}_R)\setminus\{0\}$. For every finite set $\Omega \subseteq \mathcal{G}_R$, the characteristic function χ_Ω is an element of $\mathbb{L}^2(\mathcal{G}_R)$ and property (T) implies the existence of an element $s \in S$ such that

$$\|\chi_\Omega - L_s^*\chi_\Omega\|_{\mathbb{L}^2(\mathcal{G}_R)} \geq \varepsilon\|\chi_\Omega\|_{\mathbb{L}^2(\mathcal{G}_R)} = \varepsilon|\Omega|^{1/2}.$$

From Inequality (6.1), we deduce $(2|S||\Omega|)^{1/2} \geq \varepsilon|\Omega|^{1/2}$. $\square$

6.2. **Finite orbits and finite index subgroups.** Let X be a geometrically irreducible projective variety of dimension d defined over a finite field F. Assume that the group Γ embeds into the group $\mathsf{Bir}(X)$ of birational transformations of X (defined over F) and identify Γ to its image in $\mathsf{Bir}(X)$.

6.2.1. *The escaping set E.* Let U be a Zariski open subset of X defined over F such that for every $s \in S$, the map $s_{|U} : U \to X$ is a morphism and a regular embedding; in other words, $s_{|U}$ has no indeterminacy point and does not contract any curve. Such a set exists because S is finite: One can take U to be the complement of the union of all indeterminacy sets and critical loci of all elements of S.

Remark 6.2. One may want to reduce U in certain situations. For instance, given an element f of the group Γ, with $f \neq \mathrm{Id}$, one may remove the set of fixed points of f from X, and take $U \subset X \setminus \{f(x) = x\}$.

By construction, the co-dimension of the Zariski closed set $X \setminus U$ is at least one. Let $E \subseteq U$ be the subset of points that may escape U when one applies one of the generators:

$$E \;:=\; \bigcup_{s \in S} s^{-1}(X \setminus U)$$

where $s^{-1}(X \setminus U)$ is the total transform of the Zariski closed set $X \setminus U$. This **escaping set** E is a proper, Zariski closed subset of U.

6.2.2. *Lang-Weil estimates (see* [34]*).* By Lang-Weil estimates, there exists a positive constant c_U such that, given any finite field extension F' of F, the number of points in $U(F')$ satisfies:

$$|F'|^d - c_U|F'|^{d-1/2} \leq |U(F')| \leq |F'|^d + c_U|F'|^{d-1/2} \tag{6.2}$$

where $d = \dim U = \dim X$. (the constant c_U does not depend on F)

Similarly,

$$|E(F')| \leq b_E|F|^{d-1} + c_E|F|^{d-3/2} \tag{6.3}$$

where b_E is the number of geometrically irreducible $(d-1)$-dimensional components of E; the constants b_E and c_E depend on E but not on F'.

Remark 6.3. Assume that Γ is a group of pseudo-automorphisms of X, meaning that each element of Γ is an isomorphism in co-dimension 1; one can then choose U such that $X \setminus U$ and E have co-dimension ≥ 2. In that case, the Lang-Weil estimates can be strengthen: For instance, $|E(F')| \leq b_E|F|^{d-2} + c_E|F|^{d-5/2}$.

6.2.3. *Regular stabilizers.* Fix a finite extension F' of the field F. Given a point $x \in U(F')$, one associates a subgroup R_x of Γ which will be called the **regular stabilizer** of x. To define it, we proceed as follows. Let $(e, g_1, \cdots, g_l)$ be a path in the Cayley graph $\mathcal{G}$, and denote by s_{i+1} the element of S such that $g_{i+1} = s_{i+1} g_i$, $1 \leq i \leq l-1$. One says that the path $(e, g_1, \cdots, g_l)$ is a **regular path** if

(i) s_1 is well defined at $x_0 := x$ and maps x_0 to a point $x_1 \in U$;
(ii) for all $i \leq l-1$, s_{i+1} maps x_i to a point $x_{i+1} \in U$. (since x_i is in U, s_{i+1} is well defined at x_i)

Thus the notion of regular path depends on the starting point x. By definition, the **regular orbit** of x is the set of all points $g_l(x)$ for all regular paths $(e, g_1, \cdots, g_l)$. The regular orbit of x may intersect the escaping set E; when it does, we simply do not apply an element of S that would make it leave U.

Definition 6.4. *An element $g \in \Gamma$ is* **a regular stabilizer** *of $x \in U(F')$ if there exists a regular path $(e, g_1, \cdots, g_l)$ in G such that (i) $g_l = g$ and (ii) $g_l(x) = x$. The set of all regular stabilizers is called the* **regular stabilizer** *of x, and is denoted by R_x.*

Lemma 6.5. *The regular stabilizer R_x is a subgroup of Γ.*

Proof. Given g and h in R_x, and regular paths $(e, g_1, \cdots, g_l)$ and $(e, h_1, \cdots, h_{l'})$ in Γ satisfying properties (i) and (ii) of Definition 6.5 for g and h respectively, one can define a new regular path $(e, h_1, \cdots, h_{l'}, g_1 h_{l'}, \cdots, g_l h_{l'})$ which fixes x; thus, $g \circ h$ is an element of R_x. Similarly, write $g_{i+1} = s_{i+1} g_i$, $s_{i+1} \in S$, $x_0 = x$, and $x_{i+1} = s_{i+1}(x_i)$ for $0 \leq i \leq l-1$. By construction of U (and symmetry of S), s_{i+1} is a regular automorphism from a neighborhood of x_i to a neighborhood of x_{i+1}; hence s_{i+1}^{-1} is well defined at x_{i+1}. One can therefore reverse the regular path and get a path $(e, s_l^{-1}, s_{l-1}^{-1} \circ s_l^{-1}, \cdots, g^{-1})$ which starts at x_l and ends at x_0. In our case, $x_l = x = x_0$, and we conclude that g^{-1} is an element of R_x. □

This proof shows that we can concatenate and reverse regular paths. The **evaluation map** ev_x takes a regular path $(e, g_1, \cdots, g_l)$ and gives a point

$$\mathrm{ev}_x(e, g_1, \cdots, g_l) = g_l(x).$$

We shall say that an element $g \in \Gamma$ is **very well defined** at $x \in U(F')$ if there is a regular path from e to $g_l = g$. For such an element, the image $\mathrm{ev}_x(e, g_1, \cdots, g_l) = g_l(x) = g(x)$ does not depend on the choice of the regular path joining e to g. As a consequence, the evaluation map is defined on the set of elements of Γ which are very well defined at x and maps it into the set $U(F')$. The preimage of x is the regular stabilizer. The image is the regular orbit of x.

6.2.4. *The subset $\Omega_x \subseteq \mathcal{G}_{R_x}$.* Fix a point $x \in U(F')$. Given an element $g \in \Gamma$ which is very well defined at x, one gets a point $g(x) \in U$, as well as a vertex $[g] := gR_x$ in the graph of cosets $\mathcal{G}_{R_x}$ for the regular stabilizer R_x of x. We define $\Omega_x \subseteq \mathcal{G}_{R_x}$ to be the set of all such vertices $[g]$.

Proposition 6.6. *The subset $\Omega_x \subseteq \mathcal{G}_{R_x}$ satisfies the following properties:*

1. Ω_x *contains* $[e]$*;*
2. Ω_x *is connected: For every $[g] \in \Omega_x$ there is a path in $\mathcal{G}_{R_x}$, corresponding to a regular path $(e, g_1, \cdots, g_l)$ in Γ, which connects $[e]$ to $[g]$ in Ω_x;*
3. *the evaluation map* $\mathrm{ev}_x : [g] \mapsto g(x)$ *is well defined (because R_x stabilizes x) and is an injective map* $\mathrm{ev}_x : \Omega \to U(F')$*, the image of which is the regular obit of x.*

Proof. All we have to prove is that ev_x is injective. If $g(x) = h(x)$ with two regular paths $(e, g_1, \cdots, g_l = g)$ and $(e, h_1, \cdots, h_{l'} = h)$, one can reverse the path from e to $h_{l'} = h$ and get a regular path that maps x to $h^{-1} \circ g(x) = x$; this means $h^{-1} \circ g \in R_x$. □

Thus one gets a parametrization of the regular orbit of x by the set Ω_x. An element $[g] \in \Omega_x$ is a boundary point of Ω_x in the graph $\mathcal{G}_{R_x}$ if and only if there is a generator $s \in S$ such that $[sg] \notin \Omega_x$; this means that s is not a regular automorphism from a neighborhood of $g(x)$ to its image $s(x)$: $g(x)$ escapes from U when one applies s, and therefore $g(x) \in E(F')$. Since the evaluation map is injective, one gets

$$|\partial\Omega_x| = |\mathrm{ev}_x(\partial\Omega_x)| = |E_x(F')|$$

where $E_x(F')$ is the subset of $E(F')$ which is equal to $\mathrm{ev}_x(\partial\Omega_x)$.

Since regular orbits are disjoint, the sets $E_x(F')$ and $E_y(F')$ are disjoint as soon as x and y are not in the same regular orbit. Being finite, $U(F')$ is a union of finitely many disjoint regular orbits. Fixing a set $\{x_1, \cdots, x_m\}$ of representatives of these regular orbits, we obtain

$$U(F') = \bigsqcup_{i=1}^{m} \mathrm{ev}_{x_i}(\Omega_{x_i}).$$

Suppose that R_x has infinite index in Γ for every $x \in U(F')$. Proposition 6.1 implies

$$|U(F')| = \sum_{i=1}^{m} |\mathrm{ev}_{x_i}(\Omega_{x_i})| = \sum_{i=1}^{m} |\Omega_{x_i}|$$
$$\leq \sum_{i=1}^{m} \frac{2|S|}{\varepsilon^2} |\partial\Omega_{x_i}| = \sum_{i=1}^{m} \frac{2|S|}{\varepsilon^2} |E_{x_i}(F')| \leq \frac{2|S|}{\varepsilon^2} |E(F')|.$$

Then the Lang-Weil estimates stated in Equations (6.2) and (6.3) imply that

$$|F'|^d \leq c_U |F'|^{d-1/2} + \frac{2|S|}{\varepsilon^2} \left(b_E |F'|^{d-1} + c_E |F'|^{d-3/2} \right).$$

Thus, if the degree of the extension is large enough (for instance if $|F'|^{1/2} \geq c_U + 2|S|(b_E + c_E)/\varepsilon^2$), one gets a contradiction. This provides a proof of the following theorem.

Theorem 6.7. *Let X be a projective variety defined over a finite field F. Let Γ be a subgroup of $\mathsf{Bir}(X)$ with Kazhdan property (T) and S be a finite symmetric set of generators of Γ. Let U be a Zariski open subset of X such that for every $s \in S$, the map $s_{|U} : U \to X$ is a regular embedding defined over F. If F' is a finite extension of F and $|F'|$ is large enough, there exists a point x in $U(F')$ such that the regular stabilizer R_x of x is a finite index subgroup of Γ.*

6.2.5. *Abelian groups.* Say that a graph $\mathcal{G}$ satisfies an isoperimetric inequality of type α if there is a constant $c > 0$ such that

$$|\partial\Omega|^{\alpha} \geq c|\Omega| \tag{6.4}$$

for every finite subset Ω of $\mathcal{G}$. For instance, the Cayley graph of the group $\mathbf{Z}^d$, for any finite symmetric set of generators, satisfies an isoperimetric inequality of type $d/(d-1)$, and the isoperimetric inequality satisfied in Proposition 6.1 is of linear type ($\alpha = 1$). If $\mathcal{G}$ satisfies an isoperimetric inequality of type α, for some constant $c > 0$, it satisfies the isoperimetric inequality of type β for every $\beta \geq \alpha$ with the same constant c.

Given a group Γ, with a finite symmetric set of generators S, denote by $B(r)$ the ball of radius r in the Cayley graph $\mathcal{G} = \mathcal{G}(\Gamma, S)$.The number of vertices in $B(r)$ is denoted by $|B(r)|$, and the isoperimetric profile Φ_S is defined by

$$\Phi_S(t) = \min\{r \mid |B(r)| \geq t\}.$$

For instance, if Γ is a free abelian group of rank d, and S is any finite symmetric set of generators, one can find a subset S' of S such that S' forms a basis of the vector space $\Gamma \otimes_{\mathbf{Z}} \mathbf{Q}$. The set S' has d elements; thus, the ball of radius r in

$\mathcal{G}(\Gamma, S)$ contains at least $(1+2r)^d$ elements. This implies that $\Phi_S(t) \leq t^{1/d}$. Coulhon and Saloff-Coste proved in [18], that

$$\frac{|\partial\Omega|}{|\Omega|} \geq \frac{1}{8|S|\Phi_S(2|\Omega|)}$$

for every finite subset of the Cayley graph $\mathcal{G}$ of a group Γ. We shall use this inequality to give a short proof of the following lemma, which provides a uniform constant c_S for the isoperimetric inequality in quotients of abelian groups.

Lemma 6.8. *Let A be a free abelian group of rank $k > 1$, and let S be a finite symmetric set of generators of A. Fix an integer $l < k$, and set $q = k - l$ and $c_S(l) = (16|S|)^{-(q-1)/q}$. Then, given any subgroup R of A of rank at most l, and any finite subset Ω of the Cayley graph $\mathcal{G}(A/R, S)$, we have*

$$|\partial\Omega|^{q/q-1} \geq c_S(l)|\Omega|.$$

Proof. The group R is contained in a subgroup T of A such that A/T is a free abelian group of rank at least q. In the group A/T, with the set of generators given by S, the isoperimetric profile Φ satisfies $\Phi(t) \leq t^{1/q}$. The projection $A/R \to A/T$ maps the ball of radius r in the Cayley graph $\mathcal{G}(A/R, S)$ onto the ball of the same radius in $\mathcal{G}(A/T, S)$. Thus, the isoperimetric profile of A/R satisfies the same inequality $\Phi(t) \leq t^{1/q}$. This implies

$$|\partial\Omega| \geq (8|S|)^{-1} 2^{-1/q} |\Omega|^{(q-1)/q}.$$

and the result follows. □

Theorem 6.9. *Let X be a projective variety, defined over a finite field F. Let A be a free abelian group of birational transformations of X (defined over F). Let k be the rank of A and d be the dimension of X. Then, there exists a finite extension F' of F and a point x in $X(F')$ such that the rank of the regular stabilizer R_x of x in A is at least $k - d$.*

Proof. Changing F in a finite extension and X in one of its irreducible components, we may assume that X is geometrically irreducible. We may assume that d is positive, since otherwise X is just one point. Assume that the regular stabilizer of every point has rank at most l, with $l < k - d$. Denote by α the ratio $q/(q-1)$ with $q = k - l > d$; we have $1 < \alpha < d/(d-1)$. Following the proof of Theorem 6.7, Lemma 6.8 implies

$$\begin{aligned} |U(F')| &\leq c^{st}\sum_i |E_{x_i}(F')|^{\alpha} \\ &\leq c^{st}\left(\sum_i |E_{x_i}(F')|\right)^{\alpha}. \end{aligned}$$

From Lang-Weil estimates, one derives

$$|F'|^d \leq c_U|F'|^{d-1/2} + c^{st}\left(b_E|F'|^{d-1}+c_E|F'|^{d-3/2}\right)^{\alpha}.$$

This provides a contradiction if $|F'|$ is large because $(d-1)\alpha < d$. □

6.3. **Invariant polydisks for Kazhdan groups.** Let $\mathcal{X}_{Z_p}$ be a projective variety defined over $\mathbf{Z}_p$ and let Γ be a finitely generated subgroup of $\mathsf{Bir}(\mathcal{X}_{\mathbf{Z}_p})$ with a finite symmetric set of generators S. Let X be the special fiber of $\mathcal{X}_{Z_p}$, defined over $\mathbb{F}_p$. For $g \in \mathsf{Bir}(\mathcal{X}_{\mathbf{Z}_p})$, denote by $B_{\mathbf{Z}_p,g}$ the union of the indeterminacy loci and the critical loci of g in $\mathcal{X}_{\mathbf{Z}_p}$. Assume that the special fiber X is not contained in $B_{\mathbf{Z}_p,s}$, for any $s \in S$. This implies that X is not contained in $B_{\mathbf{Z}_p,g}$ for any $g \in \Gamma$; in particular, the restriction of g to X is birational. In other words, we assume that the action of Γ on $\mathcal{X}_{\mathbf{Z}_p}$ is a good model in the sense of Section 8.1.

When K is an extension of $\mathbf{Q}_p$, denote by O_K its valuation ring.

Theorem 6.10. *Assume that Γ satisfies Kazdan property (T). Then, changing $\mathbf{Q}_p$ in a finite extension K, and Γ in a finite index subgroup, one can find a local analytic diffeomorphism φ from the unit polydisk $\mathcal{U} = (O_K)^d \subset K^d$ to an open subset $\mathcal{V}$ of $X(K)$ such that $\mathcal{V}$ is Γ-invariant and the action of Γ on $\mathcal{V}$ is conjugate, via φ, to a subgroup of $\mathsf{Diff}^{an}(\mathcal{U})$. Moreover, one can choose this polydisk in the complement of any given proper Zariski closed subset of the generic fiber.*

Proof. Denote by $\mathsf{Sing}(\mathcal{X}_{\mathbf{Z}_p})$ the singular locus of $\mathcal{X}_{\mathbf{Z}_p}$ and set

$$U_{\mathbf{Z}_p} := \mathcal{X}_{\mathbf{Z}_p} \setminus \left(\mathsf{Sing}(\mathcal{X}_{\mathbf{Z}_p})\bigcup(\cup_{s\in S}B_{\mathbf{Z}_p,s})\right).$$

By assumption, $U_{\mathbf{Z}_p}\cap X$ is a non-empty Zariski open set of X defined over F; let U be an open subset of $U_{\mathbf{Z}_p}\cap X$ (for instance, take for U the complement of a given divisor). Observe that for any $s \in S$, the map $s_{|U_{\mathbf{Z}_p}} : U_{\mathbf{Z}_p} \to \mathcal{X}_{\mathbf{Z}_p}$ is a regular open embedding; hence, $s_{|U} : U \to X$ is also a regular open embedding. By Theorem 6.7, there exists a finite field extension F of $\mathbb{F}_q$ and a point x in $U(F)$ such that the regular stabilizer R_x of x is a finite index subgroup of Γ.

Let K be a finite extension of $\mathbf{Q}_p$ whose residue field is F.

Every element g of R_x is a regular morphism on a neighborhood of x and fixes x. Denote by $\mathcal{W}$ the set of K-points $y \in X_K$ whose specialization in the special fiber X coincides with x. By Proposition 8.6, one can find a local analytic diffeomorphism φ from the unit polydisk $\mathcal{U} = (O_K)^d \subset K^d$ to an open subset $\mathcal{V} \subset \mathcal{W}$ such that $\mathcal{V}$ is R_x-invariant and the action of R_x on $\mathcal{V}$ is conjugate, via φ, to a subgroup of $\mathsf{Diff}^{an}(\mathcal{U})$. □

Similarly, Theorem 6.9 provides invariant polydisks for subgroups of rank $l \geq k - \dim(X)$ when Γ is a free abelian group of birational transformations of rank k.

6.4. **Groups of birational transformations and finite index subgroups.**

6.4.1. *Groups of birational transformations.* One says that a group Γ is linear if there is a field $\mathbf{k}$, a positive integer n, and an embedding of Γ into $\mathsf{GL}_n(\mathbf{k})$. Similarly, we shall say that Γ is a **group of birational transformations** if there is a field $\mathbf{k}$, a projective variety $X_{\mathbf{k}}$, and an embedding of Γ into $\mathsf{Bir}(X_{\mathbf{k}})$. The following properties are obvious.

(1) Linear groups are groups of birational transformations.
(2) The product of two groups of birational transformations is a group of birational transformations.
(3) Any subgroup of a group of birational transformations is also a group of birational transformations.

In certain cases, one may want to specify further properties: If Γ acts faithfully by birational transformations on a variety of dimension d over a field of characteristic p, we shall say that Γ is a group of birational transformations in dimension at most d in characteristic p. For instance,

(4) Every finite group is a group of birational transformations in dimension 1 and characteristic 0. (see [30], Theorem 6')
(5) The modular group $\mathsf{Mod}(g)$ of a closed, orientable surface of genus $g \geq 3$ and the group $\mathsf{Out}(\mathbf{F}_g)$ are groups of birational transformations in dimension $\leq 6g$, but $\mathsf{Out}(\mathbf{F}_g)$ is not linear if $g \geq 4$ (see Section 5 and [36, 28]).

6.4.2. *Malcev and Selberg properties.* Linear groups satisfy Malcev and Selberg properties: Every finitely generated linear group is residually finite and contains a torsion free, finite index subgroup. One doesn't know whether groups of birational transformations share the same properties (see [10, 16] for an introduction to this problem). We can now prove the following result, which is stated as Theorem C in the introduction.

Theorem 6.11. *Let Γ be a discrete group with Kazhdan property (T). If Γ is a group of birational transformations in characteristic 0, then Γ is residually finite and contains a torsion free, finite index subgroup.*

Proof. Since Γ has property (T), it is finitely generated (see [20]); fix a finite symmetric set of generators S for Γ, and an embedding of Γ in the group of birational transformations of a smooth projective variety X (over a field $\mathbf{k}$ of characteristic 0). Pick an element f in $\Gamma\setminus\{\mathrm{Id}\}$ and denote by $\mathrm{Fix}(f)$ the proper Zariski closed set of fixed points of f; more precisely, $\mathrm{Fix}(f)$ is defined as the Zariski closure of the subset of the domain of definition of f defined by the equation $f(z)=z$.

By Section 8.1, one can find a prime number p, and a good model for $\Gamma\subset \mathsf{Bir}(\mathcal{X}_{\mathbf{Z}_p})$ for (X,Γ), such that the special fiber X_p of $\mathcal{X}_{\mathbf{Z}_p}$ is not contained in $\mathrm{Fix}(f)$. Choose a Zariski open subset U of X_p which is contained in the complement of $\mathrm{Fix}(f)$. We now copy the proof of Theorem 6.10. Since Γ has property (T), one can find an extension F' of the residue field $\mathbb{F}_p$, and a point x in $U(F')$, for which the regular stabilizer R_x has finite index in Γ. By construction, R_x does not contain f. Changing R_x in the intersection of its conjugates gR_xg^{-1} for g in the finite set Γ/R_x, one obtains a finite index, normal subgroup R'_x such that f reduces to a non-trivial element in the finite group Γ/R'_x. This shows that Γ is residually finite.

To prove the second assertion, we keep the same notation. Let $\mathcal{V}=(O_K)^d$ denote an R_x-invariant polydisk, on which R_x acts by analytic diffeomorphisms. Changing R_x into a finite index subgroup R''_x, one may assume that every element g in R''_x corresponds to a power series

$$g(z)=A_0+A_1(x)+\sum_{k\geq 2}A_k(z)$$

where each A_i is a homogeneous polynomial of degree i, A_0 is equal to 0 modulo p^2 and A_1 is the identity modulo p. After a conjugation by multiplication by p, Bell-Poonen theorem can be applied to g. Thus, Corollary 2.7 implies that the order of every torsion element of R''_x is a power of p.

Now, take another prime p' for which one can find a good model of the pair (X,Γ) and apply the same strategy to construct a finite index subgroup R''_y

such that every torsion element of R''_y has order a power of p'. The intersection $R''_x \cap R''_y$ is a torsion free, finite index subgroup of Γ. $\square$

6.4.3. *Central extensions and simple groups.* Fix two positive integers q and n with $q \geq 5$ and $n \geq 2$. Consider the group $\mathsf{Sp}_{2n}(\mathbf{Z})$, and the central extension

$$0 \to \mathbf{Z}/q\mathbf{Z} \to \Gamma \to \mathsf{Sp}_{2n}(\mathbf{Z}) \to 1$$

which is obtained from the universal cover

$$0 \to \mathbf{Z} \to \tilde{\mathsf{Sp}}_{2n}(\mathbf{R}) \to \mathsf{Sp}_{2n}(\mathbf{R}) \to 1$$

by taking the quotient with respect to the subgroup $q\mathbf{Z}$ of the center $\mathbf{Z}$. Since $n \geq 2$, $\mathsf{Sp}_{2n}(\mathbf{Z})$ has property (T) (see [20]). Since $q \geq 5$, every finite index subgroup of Γ contains the non-trivial finite subgroup $4\mathbf{Z}/q\mathbf{Z}$ of $\mathbf{Z}/q\mathbf{Z}$ (see [21]); hence, Γ does not contain any torsion free finite index subgroup.

Corollary 6.12. *The group $\mathsf{Sp}_{2n}(\mathbf{Z})$ is a group of birational transformations, but there is a finite cyclic central extension Γ of $\mathsf{Sp}_{2n}(\mathbf{Z})$ that does not act faithfully by birational transformations.*

In particular, the property "Γ *is a group of birational transformations*" is not stable under finite central extensions. Similar examples can be derived from [39] and [41].

Corollary 6.13. *If Γ is an infinite, simple, discrete group with Kazhdan property (T), and X is a complex projective variety, every morphism $\Gamma \to \mathsf{Bir}(X)$ is trivial.*

In particular, the simple groups constructed in [25, 15] do not act non trivially by birational transformations.

Proof. If there exists a non-trivial morphism $\Gamma \to \mathsf{Bir}(X)$, this morphism is an embedding because Γ is simple; thus, Γ contains a non-trivial, finite index subgroup, contradicting the fact that Γ is infinite and simple. $\square$

7. Actions of lattices on quasi-projective varieties

In this section, we prove Theorem B, and a corollary which concerns birational actions of the lattice $\mathsf{SL}_n(\mathbf{Z})$.

7.1. **Lattices in higher rank Lie groups (see** [5]**).** Let $\mathsf{S} \subset \mathsf{GL}_m$ be an algebraic subgroup of GL_m defined over the field of rational numbers $\mathbf{Q}$. We shall assume that

(i) S is almost simple (this means that the Lie algebra $\mathfrak{g}_{\mathbf{R}}$ of $\mathsf{S}(\mathbf{R})$ is simple);
(ii) as an algebraic group, S is connected and simply connected (equivalently $\mathsf{S}(\mathbf{C})$ is a simply connected manifold);
(iii) the real rank of S is greater than 1 (see § 1.3);
(iv) the lattice $\Gamma = \mathsf{S}(\mathbf{Z})$ of $\mathsf{S}(\mathbf{R})$ is not co-compact (i.e. $\mathsf{rank}_{\mathbf{Q}}(\mathsf{S}) > 0$).

Theorem 7.1. *Let* S *be an algebraic subgroup of* GL_m *defined over the field of rational numbers* $\mathbf{Q}$*. Assume that* S *is almost simple and simply connected, and that its real rank is greater than* 1*. Assume, moreover, that the lattice* $\Gamma = \mathsf{S}(\mathbf{Z})$ *is not co-compact. Then, given any prime number p,* Γ *is dense in* $\mathsf{S}(\mathbf{Z}_p)$ *and the pro-p complection of* Γ *is a finite central extension of* $\mathsf{S}(\mathbf{Z}_p)$*.*

This theorem encapsulates two types of results, known as the strong approximation and the congruence subgroup properties. It summarizes a long sequence of efforts; see [43] and [42] for two good survey articles.

Example 7.2. Let $r > 0$ be a square-free integer. Let $L = \mathbf{Q}(\sqrt{r})$, a real quadratic extension of $\mathbf{Q}$, and σ be its unique non-trivial Galois automorphism: $\sigma(\sqrt{r}) = -\sqrt{r}$. Let $\tilde{\sigma}$ be the automorphism of the vector space of 3×3 matrices with coefficients in L which is defined by applying σ to all coefficients of each matrix. Let J_3 be the 3×3 symmetric matrix

$$J_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Consider the group

$$\Gamma = \mathsf{SU}(J_3; \mathbf{Z}[\sqrt{r}], \sigma) = \left\{ g \in \mathsf{SL}_3(\mathbf{Z}[\sqrt{r}]) \mid \tilde{\sigma}({}^t g) J_3 g = J_3 \right\}.$$

Then Γ is lattice in $\mathsf{SL}_3(\mathbf{R})$. If one embeds L^3 in $V = \mathbf{R}^3 \oplus \mathbf{R}^3$ by the $\mathbf{Q}$-linear map $\Delta(v) = (v, J_3 \sigma(v))$ then $\Delta(L^3)$ spans V and $\Delta((\mathbf{Z}[\sqrt{r}])^3)$ is a lattice in V. This defines a structure of $\mathbf{Q}$-vector space $V_{\mathbf{Q}}$ on V. Now, define $\rho \colon \mathsf{SL}_3(\mathbf{R}) \to \mathsf{SL}(V)$ by

$$\rho(A)(v, w) = (A(v), {}^t A^{-1}(w)) \quad \forall (v, w) \in V = \mathbf{R}^3 \oplus \mathbf{R}^3.$$

Then, one can verify that the Lie group $\rho(\mathsf{SL}_3(\mathbf{R})) \subset \mathsf{GL}(V)$ is defined over $\mathbf{Q}$ (with respect to the $\mathbf{Q}$-structure $V_{\mathbf{Q}}$), and that Γ is the subgroup preserving the lattice $V_{\mathbf{Q}}(\mathbf{Z}) \subset V$. This provides an example of an $\mathbf{Q}$-algebraic group $\mathsf{S} \subset \mathsf{GL}_6$ with $\mathsf{S}(\mathbf{R})$ isomorphic to $\mathsf{SL}_3(\mathbf{R})$ and $\mathsf{S}(\mathbf{Z})$ not co-compact. The $\mathbf{Q}$-rank of S is equal to 1, and Γ is not commensurable to $\mathsf{SL}_3(\mathbf{Z})$.

Example 7.3. For every $0 \leq \ell \leq n-1$, there is a linear algebraic group G_ℓ which is defined over $\mathbf{Q}$ such that (i) $G_\ell(\mathbf{R})$ is isomorphic to $\mathsf{SL}_n(\mathbf{R})$ and (ii) the $\mathbf{Q}$-rank of G_ℓ is equal to ℓ. For $n = 3$, there are only three type of lattices Γ in $\mathsf{SL}_3(\mathbf{R})$: Either Γ is co-compact, or Γ has rank 1 is commensurable to $\mathsf{SU}(J_3; \mathbf{Z}[\sqrt{r}], \sigma)$ for some $r > 0$, or Γ has rank 2 and is commensurable to $\mathsf{SL}_3(\mathbf{Z})$.

7.2. **Minimal homogeneous spaces (see** [47]**, p. 187, and** [46]**).** Given a simple complex Lie algebra $\mathfrak{s}$, one denotes by $\delta(\mathfrak{s})$ the minimal co-dimension of its proper Lie subalgebras $\mathfrak{p} < \mathfrak{s}$. If S is a complex Lie group with Lie algebra equal to $\mathfrak{s}$, then $\delta(\mathfrak{s})$ is equal to the minimal dimension $\delta(\mathsf{S})$ of a homogeneous variety $V = \mathsf{S}/P$ with $\dim(V) > 0$. Such a maximal group P is the stabilizer of a point $m \in V$; it is a parabolic subgroup of S (see [47], page 187). If $\mathfrak{s}$ (resp. S) is defined over a subfield of $\mathbf{C}$, we use the same notation $\delta(\mathfrak{s})$ (resp. $\delta(\mathsf{S})$) to denote $\delta(\mathfrak{s} \otimes \mathbf{C})$.

TABLE 1. Minimal dimensions of faithful representations and minimal homogeneous spaces

the Lie algebra	its dimension	the dimension of its minimal representation	smallest homogeneous space
$\mathfrak{sl}_k(\mathbf{C})$, $k \geq 2$	k^2-1	k	$k-1$
$\mathfrak{so}_k(\mathbf{C})$, $k \geq 7$	$k(k-1)/2$	k	$k-2$
$\mathfrak{sp}_{2k}(\mathbf{C})$, $k \geq 2$	$2k^2+k$	$2k$	$2k-1$
$\mathfrak{e}_6(\mathbf{C})$	78	27	14
$\mathfrak{e}_7(\mathbf{C})$	133	56	27
$\mathfrak{e}_8(\mathbf{C})$	248	248	57
$\mathfrak{f}_4(\mathbf{C})$	52	26	15
$\mathfrak{g}_2(\mathbf{C})$	14	7	5

This dimension $\delta(\mathsf{S})$ has been computed for all simple complex Lie groups (see [46] for instance). The results are summarized in Table 1, from which one sees that $\delta(\mathfrak{s}) \geq \mathrm{rank}_{\mathbf{C}}(\mathfrak{s})$ with equality if and only if $\mathfrak{s}$ is $\mathfrak{sl}_{\delta(\mathfrak{s})+1}(\mathbf{C})$.

Remark 7.4. Note that $\mathsf{SO}_5(\mathbf{C})$ is isogenous to $\mathsf{SL}_4(\mathbf{C})$ and acts on $\mathbb{P}^3$ (the space of lines in the smooth quadric $Q \subset \mathbb{P}^4$ is isomorphic to $\mathbb{P}^3$). Similarly, $\mathsf{SO}_6(\mathbf{C})$ is isogenous to $\mathsf{Sp}_4(\mathbf{C})$ and acts on $\mathbb{P}^3$ too.

7.3. **Proof of Theorem *B*.** Changing S in a finite cover, and Γ into its preimage under the covering morphism, we may assume that S is simply connected. Identify Γ with its image in $\mathsf{Bir}(X)$, and choose a good p-adic model for (X,Γ), as in Section 8.

Changing Γ in a finite index subgroup and the field $\mathbf{Q}_p$ in a finite extension K, one can find an analytic polydisk $\mathcal{U} \subset X(K)$ which is Γ-invariant, and on which the action of Γ extends as an analytic action of its closure, an open subgroup $G = \overline{\Gamma}$ of the p-adic group $\mathsf{S}(\mathbf{Z}_p)$. This follows from Theorem 7.1 and Theorem 2.12

Let o be a point of $\mathcal{U}$ which is not fixed by G; the stabilizer of o is a closed subgroup P of G: Its Lie algebra determines a subalgebra of $\mathfrak{s}$ of co-dimension at most $\dim(X)$. If $\dim(X) < \delta(\mathsf{S})$, then P is a finite index subgroup of G, and the action of Γ on X factors through a finite group. Thus,

$$\dim(X) \geq \delta(\mathsf{S}) \geq \mathsf{rank}_{\mathbf{R}}(\mathsf{S})$$

(which is better than the inequality in Theorem B). If $\dim(X) = \mathsf{rank}_{\mathbf{R}}(\mathsf{S})$, then $\delta(\mathsf{S}) = \mathsf{rank}_{\mathbf{R}}(\mathsf{S})$ and $(s) = \mathfrak{sl}_n$ with $n = \dim(X) + 1$.

7.4. **Birational actions of $\mathsf{SL}_n(\mathbf{Z})$.** Theorem B and Section 4 (in the case of birational transformations) lead to the following corollary.

Corollary 7.5. *Let Γ be a finite index subgroup of $\mathsf{SL}_n(\mathbf{Z})$, with $n \geq 3$. If Γ acts by birational transformations on an irreducible complex projective variety X, then either the image of Γ in $\mathsf{Bir}(X)$ is finite, or $\dim(X) \geq n-1$. Moreover, if the image is infinite and $\dim(X) = n-1$, then X is rational, and the action of Γ on X is birationally conjugate to a linear projective action of Γ on $\mathbb{P}^{n-1}$.*

Proof. Since $n \geq 3$, Γ is almost simple: Its normal subgroups are finite and central, or co-finite. Changing Γ in a finite index subgroup, we may assume that Γ is torsion free. Then, if the image of Γ in $\mathsf{Bir}(X)$ is infinite, the morphism $\Gamma \to \mathsf{Bir}(X)$ is in fact injective. Theorem B implies that $\dim(X) \geq n-1$, and its proof shows that there is a good, p-adic model of (X,Γ) for which a finite index subgroup of Γ preserves a p-adic polydisk, acting by analytic diffeomorphisms on it. Then, Section 4 shows that there is a birational, Γ-equivariant mapping

$\tau\colon X \dashrightarrow \mathbb{P}^{n-1}$ if $\dim(X) = n-1$ (the action of Γ on $\mathbb{P}^{n-1}$ is by linear projective automorphisms). $\square$

8. Appendix: good models and Invariant polydisks

8.1. **Good models.** Denote by $\mathbf{k}$ an algebraically closed field of characteristic zero. Let X be a projective variety, which is defined over $\mathbf{k}$ and is geometrically irreducible. Let Γ be a finitely generated subgroup of $\mathsf{Bir}(X_{\mathbf{k}})$, with a finite symmetric set of generators $S \subset \Gamma$.

As explained in Section 3.2, there exists a subring R of $\mathbf{k}$, which is finitely generated over $\mathbf{Z}$, such that X is defined over the fraction field K of R and every birational transformation $s \in S$ is defined over K. This means that there exists a projective variety $X_K \to \mathrm{Spec}(K)$ such that $X = X_K \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\mathbf{k})$.

Pick a model $\pi : \mathcal{X}_R \to \mathrm{Spec}(R)$ which is projective over $\mathrm{Spec}(R)$ and whose generic fiber is X_K. Every birational transformation f of X_K extends to a birational transformation of $\mathcal{X}_R$ over $\mathrm{Spec}(R)$. For every point $y \in \mathrm{Spec}(R)$, denote by X_y the fiber of $\mathcal{X}_R$ above y and by f_y the restriction of f to X_y. For any $g \in \mathsf{Bir}_R(\mathcal{X}_R)$, denote by $B_{R,g}$ the union of the indeterminacy loci and the critical loci of g in $\mathcal{X}_R$.

Lemma 8.1. *There exists a nonempty, affine, open subset U of* $\mathrm{Spec}(R)$ *such that*

(1) *U is of finite type over* $\mathrm{Spec}(\mathbf{Z})$*;*
(2) *for every point $y \in U$, the fiber X_y is geometrically irreducible and* $\dim_{K(y)} X_y = \dim_K X_K$*, where $K(y)$ is the residue field at y;*
(3) *for every $s \in S$ and every $y \in U$, the fiber X_y is not contained in $B_{R,s}$.*

Proof. To prove the lemma, we shall use the following fact, which is proved below.

Lemma 8.2. *For any integral affine scheme* $\mathrm{Spec}(A)$ *of finite type over* $\mathrm{Spec}(\mathbf{Z})$ *and any nonempty open subset V_1 of* $\mathrm{Spec}(A)$*, there exists an affine open subset V_2 of V_1 which is of finite type over* $\mathrm{Spec}(\mathbf{Z})$.

Since X_K is geometrically irreducible, by ([31], Prop. 9.7.8) there exists an affine open subset V of $\mathrm{Spec}(R)$ such that X_y is geometrically irreducible for every $y \in V$. By Lemma 8.2, we may suppose that V is of finite type over $\mathrm{Spec}(\mathbf{Z})$.

By generic flatness ([31], Thm. 6.9.1) and Lemma 8.2, we may change V in a smaller subset and suppose that the restriction of π to $\pi^{-1}(V)$ is flat. Then, the fiber X_y is geometrically irreducible and of dimension $\dim_{K(y)} X_y = \dim_K X_K$ for every point $y \in V$.

For $s \in S$, denote by $B_{K,s}$ the union of the indeterminacy locus and the critical locus of s in X_K; thus, the complement of $B_{K,s}$ is the open subset on which s is a local isomorphism. Then $B_{K,s}$ is a proper closed subset of X_K. Observe that $B_{K,s}$ is exactly the generic fiber of $\pi_{|B_{R,s}} : B_{R,s} \to \mathrm{Spec}(R)$.

By generic flatness, there exists a nonempty, affine, open subset U_s of V such that the restriction of π to every irreducible component of $\pi^{-1}_{|B_{R,s}}(U_s)$ is flat. Set

$$U := \bigcap_{s \in S} U_s;$$

if $s \in S$ and $y \in U$, the fiber X_y is not contained in $B_{R,s}$. By Lemma 8.2, we may change U to suppose that U is of finite type over $\mathrm{Spec}(Z)$. Then

$$\dim_{K(y)}(B_{R,s} \cap X_y) = \dim_K(B_{K,s}) < \dim_K X_K = \dim_{K(y)} X_y$$

for every $s \in S$ and $y \in V$; consequently, X_y is not contained in $B_{R,s}$. $\square$

Proof of Lemma 8.2. Denote by I the ideal of A that defines the closed subset $\mathrm{Spec}(A) \setminus V$. Pick any non-zero element $f \in I$; the open set $U := \mathrm{Spec}(A) \setminus \{f = 0\}$ is an open subset of V. Moreover since $U = \mathrm{Spec}(A[1/f])$, it is of finite type over $\mathrm{Spec}(\mathbf{Z})$. $\square$

By Lemma 8.1, we may replace $\mathrm{Spec}(R)$ by U and assume that

- for every $y \in \mathrm{Spec}(R)$, the fiber X_y is geometrically irreducible;
- for every $s \in S$ and $y \in \mathrm{Spec}(R)$, the fiber X_y is not contained in $B_{R,s}$.

Proposition 8.3. *There exists a prime $p \geq 3$, an embedding of R into $\mathbf{Z}_p$ and a projective scheme $\mathcal{X}_{\mathbf{Z}_p} \to \mathrm{Spec}(\mathbf{Z}_p)$ such that*

(1) *the special fiber X_p of $\mathcal{X}_{\mathbf{Z}_p} \to \mathrm{Spec}(\mathbf{Z}_p)$ is geometrically irreducible and $\dim_{\mathbb{F}_p} X_p = \dim_{\mathbf{Q}_p} \mathcal{X}_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(\mathbf{Q}_p)$;*
(2) *for every $s \in S$, the fiber X_p is not contained in $B_{\mathbf{Z}_p,s}$, where $B_{\mathbf{Z}_p,s}$ denotes the union of the indeterminacy loci and the critical loci of s in $\mathcal{X}_{\mathbf{Z}_p}$.*

We shall say that such an embedding provides a **good model** for the pair (X, Γ) over $\mathbf{Z}_p$. There are, indeed, infinitely many primes p for which the conclusions of this proposition are satisfied (because there are infinitely many possible choices for the prime p in Lemma 3.2).

Proof. Set $d = \dim_{\mathbf{Q}_p} \mathcal{X}_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(\mathbf{Q}_p)$.

Since R is integral and finitely generated over $\mathbf{Z}$, by Lemma 3.2 (i.e. Lemma 3.1 of [4]) there exists a prime $p \geq 3$ such that R can be embedded into $\mathbf{Z}_p$. This induces an embedding $\mathrm{Spec}(\mathbf{Z}_p) \to \mathrm{Spec}(R)$.

Set $\mathcal{X}_{\mathbf{Z}_p} := \mathcal{X}_R \times_{\mathrm{Spec}(R)} \mathrm{Spec}(\mathbf{Z}_p)$. All fibers X_y, for $y \in \mathrm{Spec}(R)$, are geometrically irreducible and of dimension d; hence, the special fiber X_p of $\mathcal{X}_{\mathbf{Z}_p} \to \mathrm{Spec}(\mathbf{Z}_p)$ is geometrically irreducible and of dimension d. Since $B_{\mathbf{Z}_p,s} \subset B_{R,s} \cap X_p$ for every $s \in S$, the fiber X_p is not contained in $B_{\mathbf{Z}_p,s}$. $\square$

8.2. **From fixed points to invariant polydisks.** Let $\mathcal{X}_{\mathbf{Z}_p}$ be a projective variety defined over $\mathbf{Z}_p$ and let Γ be a finitely generated subgroup of $\mathsf{Bir}(\mathcal{X}_{\mathbf{Z}_p})$ with a finite symmetric set of generators S. Let X be the special fiber of $\mathcal{X}_{\mathbf{Z}_p}$; it is defined over $\mathbb{F}_p$.

For $g \in \mathsf{Bir}(\mathcal{X}_{\mathbf{Z}_p})$, denote by $B_{\mathbf{Z}_p,g}$ the union of the indeterminacy locus and the critical locus of g in $\mathcal{X}_{\mathbf{Z}_p}$. Assume that the special fiber X is not contained in $B_{\mathbf{Z}_p,s}$ for any $s \in S$; this implies that X is not contained in $B_{\mathbf{Z}_p,g}$ for any $g \in \Gamma$. In particular, the restriction of g to X is birational for every $g \in \Gamma$. These assumptions are satisfied when the pair $(\mathcal{X}_{\mathbf{Z}_p}, \Gamma)$ is a good model (as in Section 8.1).

Let K be a finite extension of $\mathbf{Q}_p$, O_K be the valuation ring of K, and F the residue field of O_K; by definition, $F = O_K/\mathbf{m}_K$ where $\mathbf{m}_K$ is the maximal ideal of O_K. Denote by $|\cdot|_p$ the p-adic norm on K, normalized by $|p|_p = 1/p$. Set

$$\mathcal{X}_{O_K} = \mathcal{X}_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(O_K).$$

The generic fiber $\mathcal{X}_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(K)$ is denoted by X_K, and the special fiber is $X_F = \mathcal{X}_{\mathbf{Z}_p} \times_{\mathrm{Spec}(\mathbf{Z}_p)} \mathrm{Spec}(F)$. Denote by $r\colon X_K(K) \to X_F(F) = X(F)$ the reduction map.

Since $\mathcal{X}_{O_K}$ is projective, there exists an embedding $\iota\colon \mathcal{X}_{O_K} \to \mathbb{P}^N_{O_K}$ defined over O_K. On the projective space $\mathbb{P}^N(K)$, there is a metric dist_p, defined by

$$\mathsf{dist}_p([x_0 : \cdots : x_N], [y_0 : \cdots : y_N]) = \frac{\max_{i\neq j}(|x_i y_j - x_j y_i|_p)}{\max_i(|x_i||_p)\max_j(|y_j|_p)}$$

for every pair of points $[x_0 : \cdots : x_N]$, $[y_0 : \cdots : y_N] \in \mathbb{P}^N(K)$. Via the embedding $\iota_{|X(K)}\colon X_K(K) \to \mathbb{P}^N_K$, dist_p restricts to a metric $\mathsf{dist}_{p,\iota}$ on $X_K(K)$. This metric does not depend on the choice of the embedding ι; thus, we simply write dist_p instead of $\mathsf{dist}_{p,\iota}$.

Proposition 8.4. *For any pair of points w, $z \in X_K(K)$, we have $r(w) = r(z)$ if and only if $\mathsf{dist}_p(w,z) < 1$.*

Proof. Set $\iota(w) = [x_0 : \cdots : x_N]$ and $\iota(z) = [y_0 : \cdots : y_N]$ where the coordinates x_i, y_i are in O_K and satisfy $\max_i |x_i|_p = \max_i |y_i|_p = 1$. Then $\iota(r(w)) = [\overline{x_0} : \cdots : \overline{x_N}]$ and $\iota(r(z)) = [\overline{y_0} : \cdots : \overline{y_N}]$ where $\overline{x_i}$ and $\overline{y_i}$ denote the images of x_i and y_i in the residue field $F = O_K/\mathbf{m}_K$. By definition,

$$\mathsf{dist}_p([x_0 : \cdots : x_N], [y_0 : \cdots : y_N]) = \max_{i\neq j}(|x_i y_j - x_j y_i|_p).$$

If $r(w) = r(z)$, we have $\overline{x_i} = \overline{y_i}$ for all indices i; thus

$$|x_i y_j - x_j y_i|_p = |x_i(y_j - y_i) + (x_i - x_j)y_i|_p < 1$$

and $\mathsf{dist}_p(w,z) < 1$. Now, suppose that $r(w) \neq r(z)$. Assume, first, that there exists an index i, say $i = 0$, with $\overline{x_i y_i} \neq 0$. Replacing x_i by x_i/x_0 and y_i by y_i/y_0, we get $x_0 = y_0 = 1$. Since $r(w) \neq r(z)$, there exists $i \geq 1$ with $\overline{x_i} \neq \overline{y_i}$. It follows that

$$\mathsf{dist}_p(w,z) \geq |x_i y_0 - x_0 y_i|_p = |x_i - y_i|_p = 1.$$

To conclude, suppose that $\overline{x_i y_i} = 0$ for all indices $i \in \{0,\ldots,N\}$. Pick two indices i and j such that $\overline{x_i} \neq 0$ and $\overline{y_j} \neq 0$; thus, $\overline{y_i} = 0$ and $\overline{x_j} = 0$, and we obtain $\mathsf{dist}_p(w,z) \geq |x_i y_j - x_i y_j|_p = 1$. □

Let x be a smooth point in $X(F)$ and $\mathcal{V}$ be the open subset of $X_K(K)$ consisting of points $z \in X_K(K)$ satisfying $r(z) = x$. Choosing suitable homogeneous coordinates, we may suppose that x is the point $[1 : 0 : \cdots : 0] \in \mathbb{P}^N_F$. Then $\mathcal{V}$ is contained in the unit polydisk.

$$B := \{[1 : z_1 : \cdots : z_N] \mid z_i \in O_K \text{ for all } i = 1,,N\}.$$

Recall from Section 2.1.1 that a map φ from the unit polydisk $\mathcal{U} = O_K^d \subset K^d$ to B is analytic if we can find elements φ_i, $1 \leq i \leq N$, of the Tate algebra $O_K\langle x_1,\ldots,x_d\rangle$, such that

$$\varphi(x_1,\ldots,x_d) = [1 : \varphi_1(x_1,,x_d) : \cdots : \varphi_N(x_1,\ldots,x_d)].$$

Proposition 8.5. *There exists a one to one analytic diffeomorphism φ from the unit polydisk $\mathcal{U} = (O_K)^d \subset K^d$ to $\mathcal{V}$.*

Proof. Consider the affine chart $\mathbb{A}^N_{O_K} \to \mathbb{P}^N_{O_K}$ defined by $z_0 \neq 0$. Both x and B are contained in $\mathbb{A}^N_{O_K}$. Since $\mathcal{X}_{O_K}$ is smooth at x, we know that there are equations $G_j \in O_K[z_1, \ldots, z_N]$, $1 \leq j \leq N-d$, such that

- X is locally defined by equations $G_1 = \cdots = G_{N-d} = 0$; in particular,
$$\mathcal{V} = X_K(K) \cap B = \{z \in B \mid G_i(z) = 0,\ \forall i = 1, \ldots, N-d\}.$$
- The rank of the matrix $(\partial_{z_j}\overline{G_i}(0))_{i \leq N-d, j \leq N}$ is $N-d$, where $\overline{G_i} = G_i$ modulo $\mathbf{m}_K O_K[z_1, \ldots, z_N]$.

Permuting the coordinates $x_1, \ldots, x_N$ we may suppose that the determinant of the matrix $(\partial_{z_j}\overline{G_i}(0))_{i,j \leq N-d}$ is different from 0 in F. Denote by $\pi \colon B \to (O_K)^d$ the projection $[1 : z_1 : \cdots : z_N] \mapsto (z_1, \ldots, z_d)$. By Hensel's lemma, there exists a unique analytic diffeomorphism $\varphi \colon (O_K)^d \to \mathcal{V}$ such that $\varphi(x)$ is the unique point in B satisfying $G_i((x, \varphi(x))) = 0$ for all $i \leq N-d$. $\square$

Let f be a birational map in $\mathsf{Bir}_{O_K}(\mathcal{X}_{O_K})$ such that $x \notin B_{O_K,f}$ and $f(x) = x$. Then f fixes the set $\mathcal{V}$ of points z in $X_K(K)$ such that $r(z) = x$, and the action f on $\mathcal{V}$ is conjugate, via φ, to an analytic diffeomorphism on the polydisk $\mathcal{U}$. This concludes the proof of the following proposition.

Proposition 8.6. *There exists an analytic diffeomorphism φ from the unit polydisk $\mathcal{U} = (O_K)^d$ to an open subset $\mathcal{V}$ of $X_K(K)$ such that for any birational map f in $\mathsf{Bir}_{O_K}(\mathcal{X}_{O_K})$ with $x \notin B_{O_K,f}$ and $f(x) = x$, the set $\mathcal{V}$ is f-invariant and the action of f on $\mathcal{V}$ is conjugate, via φ, to an analytic diffeomorphism on $\mathcal{U}$.*

When one applies this proposition to groups of birational transformations, one gets the following. If $\Gamma < \mathsf{Bir}(\mathcal{X}_{\mathbf{Z}_p})$ satisfies both

(i) x is not contained in any of the sets $B_{O_K,f}$ (for $f \in \Gamma$),
(ii) $f(x) = x$ for every f in Γ,

then $\mathcal{V}$ is Γ-invariant and φ conjugates the action of Γ on $\mathcal{V}$ to a group of analytic diffeormorphisms of the polydisk $\mathcal{U}$.

Thus, once a good model has been constructed (as in Section 8.1), the existence of an invariant polydisk on which the action is analytic is equivalent to the existence of a fixed point $x \in X_F(F)$ in the complement of the bad loci $B_{O_K,f}$, f in Γ. Periodic orbits correspond to polydisks which are invariant by finite index subgroups.

References

[1] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geq 3)$ and $\mathrm{Sp}_{2n}\,(n \geq 2)$. *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[2] Eric Bedford, Mikhail Lyubich, and John Smillie. Polynomial diffeomorphisms of $\mathbf{C}^2$. IV. The measure of maximal entropy and laminar currents. *Invent. Math.*, 112(1):77–125, 1993.

[3] 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.

[4] Jason P. Bell. A generalised Skolem-Mahler-Lech theorem for affine varieties. *J. London Math. Soc. (2)*, 73(2):367–379, 2006.

[5] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[6] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[7] Serge Cantat. Version kählérienne d'une conjecture de Robert J. Zimmer. *Ann. Sci. École Norm. Sup. (4)*, 37(5):759–768, 2004.

[8] Serge Cantat. Invariant hypersurfaces in holomorphic dynamics. *Math. Res. Lett.*, 17(5):833–841, 2010.

[9] Serge Cantat. Sur les groupes de transformations birationnelles des surfaces. *Ann. of Math. (2)*, 174(1):299–340, 2011.

[10] Serge Cantat. The Cremona group in two variables. *European Congress of Mathematics*, VI(5):211–225, 2012.

[11] Serge Cantat. Morphisms between Cremona groups, and characterization of rational varieties. *Compos. Math.*, 150(7):1107–1124, 2014.

[12] Serge Cantat and Igor Dolgachev. Rational surfaces with a large group of automorphisms. *J. Amer. Math. Soc.*, 25(3):863–905, 2012.

[13] Serge Cantat and Stéphane Lamy. Groupes d'automorphismes polynomiaux du plan. *Geom. Dedicata*, 123:201–221, 2006.

[14] Serge Cantat and Abdelghani Zeghib. Holomorphic actions, Kummer examples, and Zimmer program. *Ann. Sci. Éc. Norm. Supér. (4)*, 45(3):447–489, 2012.

[15] Pierre-Emmanuel Caprace and Bertrand Rémy. Simplicity and superrigidity of twin building lattices. *Invent. Math.*, 176(1):169–221, 2009.

[16] Yves Cornulier. Sofic profile and computability of Cremona groups. *Michigan Math. J.*, 62(4):823–841, 2013.

[17] François R. Cossec and Igor V. Dolgachev. *Enriques surfaces. I*, volume 76 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1989.

[18] Thierry Coulhon and Laurent Saloff-Coste. Isopérimétrie pour les groupes et les variétés. *Rev. Mat. Iberoamericana*, 9(2):293–314, 1993.

[19] Pierre de la Harpe. *Topics in geometric group theory*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2000.

[20] Pierre de la Harpe and Alain Valette. La propriété (T) de Kazhdan pour les groupes localement compacts (avec un appendice de Marc Burger). *Astérisque*, (175):158, 1989. With an appendix by M. Burger.

[21] Pierre Deligne. Extensions centrales non résiduellement finies de groupes arithmétiques. *C. R. Acad. Sci. Paris Sér. A-B*, 287(4):A203–A208, 1978.

[22] Julie Déserti. Groupe de Cremona et dynamique complexe: une approche de la conjecture de Zimmer. *Int. Math. Res. Not.*, pages Art. ID 71701, 27, 2006.

[23] Julie Déserti. Sur le groupe des automorphismes polynomiaux du plan affine. *J. Algebra*, 297(2):584–599, 2006.

[24] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[25] Mikhail Ershov. Golod-Shafarevich groups with property (T) and Kac-Moody groups. *Duke Math. J.*, 145(2):309–339, 2008.

[26] Benson Farb and Dan Margalit. *A primer on mapping class groups*, volume 49 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 2012.

[27] David Fisher. Groups acting on manifolds: around the Zimmer program. In *Geometry, rigidity, and group actions*, Chicago Lectures in Math., pages 72–157. Univ. Chicago Press, Chicago, IL, 2011.

[28] Edward Formanek and Claudio Procesi. The automorphism group of a free group is not linear. *J. Algebra*, 149(2):494–499, 1992.

[29] Shmuel Friedland and John Milnor. Dynamical properties of plane polynomial automorphisms. *Ergodic Theory Dynam. Systems*, 9(1):67–99, 1989.

[30] Leon Greenberg. Maximal groups and signatures. In *Discontinuous groups and Riemann surfaces (Proc. Conf., Univ. Maryland, College Park, Md., 1973)*, pages 207–226. Ann. of Math. Studies, No. 79. Princeton Univ. Press, Princeton, N.J., 1974.

[31] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[32] Ehud Hrushovski. The elementary theory of the frobenius automorphism. *http://arxiv.org/pdf/math/0406514v1*, pages 1–135, 2004.

[33] Hanspeter Kraft and Immanuel Stampfli. On automorphisms of the affine Cremona group. *Ann. Inst. Fourier (Grenoble)*, 63(3):1137–1148, 2013.

[34] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

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

[36] A. M. Macbeath and D. Singerman. Spaces of subgroups and Teichmüller space. *Proc. London Math. Soc. (3)*, 31(2):211–256, 1975.

[37] Wilhelm Magnus. Rings of Fricke characters and automorphism groups of free groups. *Math. Z.*, 170(1):91–103, 1980.

[38] G. A. Margulis. *Discrete subgroups of semisimple Lie groups*, volume 17 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1991.

[39] John J. Millson. Real vector bundles with discrete structure group. *Topology*, 18(1):83–89, 1979.

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

[41] M. S. Raghunathan. Torsion in cocompact lattices in coverings of $\mathrm{Spin}(2,n)$. *Math. Ann.*, 266 (see also 303 for a correction)(4):403–419, 1984.

[42] M. S. Raghunathan. The congruence subgroup problem. In *Proceedings of the Hyderabad Conference on Algebraic Groups (Hyderabad, 1989)*, pages 465–494. Manoj Prakashan, Madras, 1991.

[43] Andrei S. Rapinchuk. Strong approximation for algebraic groups. In *Thin groups and superstrong approximation*, volume 61 of *Math. Sci. Res. Inst. Publ.*, pages 269–298. Cambridge Univ. Press, Cambridge, 2014.

[44] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition.

[45] Robert Steinberg. Some consequences of the elementary relations in SL_n. In *Finite groups—coming of age (Montreal, Que., 1982)*, volume 45 of *Contemp. Math.*, pages 335–350. Amer. Math. Soc., Providence, RI, 1985.

[46] Garrett Stuck. Low-dimensional actions of semisimple groups. *Israel J. Math.*, 76(1-2):27–71, 1991.

[47] È. B. Vinberg, editor. *Lie groups and Lie algebras, III*, volume 41 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1994. Structure of Lie groups and

Lie algebras, A translation of ıt Current problems in mathematics. Fundamental directions. Vol. 41 (Russian), Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1990 [MR1056485 (91b:22001)], Translation by V. Minachin [V. V. Minakhin], Translation edited by A. L. Onishchik and È. B. Vinberg.

[48] André Weil. On algebraic groups of transformations. *Amer. J. Math.*, 77:355–391, 1955.

[49] R. J. Zimmer. Actions of semisimple groups and discrete subgroups. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 1247–1258, Providence, RI, 1987. Amer. Math. Soc.

[50] R. J. Zimmer. Lattices in semisimple groups and invariant geometric structures on compact manifolds. In *Discrete groups in geometry and analysis (New Haven, Conn., 1984)*, volume 67 of *Progr. Math.*, pages 152–210. Birkhäuser Boston, Boston, MA, 1987.

IRMAR (UMR 6625 DU CNRS), UNIVERSITÉ DE RENNES 1, FRANCE
E-mail address: serge.cantat@univ-rennes1.fr
E-mail address: junyi.xie@univ-rennes1.fr