

Algebraic actions of discrete groups: the p -adic method

by

SERGE CANTAT

*Université de Rennes 1
Rennes, France*

JUNYI XIE

*Université de Rennes 1
Rennes, France*

Contents

1. Introduction	239
2. Tate analytic diffeomorphisms of the p -adic polydisk	244
3. Good models, p -adic integers, and invariant polydisks	253
4. Regular actions of $\mathrm{SL}_n(\mathbf{Z})$ on quasi-projective varieties	258
5. Actions of $\mathrm{SL}_n(\mathbf{Z})$ in dimension $n-1$	262
6. Mapping class groups and nilpotent groups	269
7. Periodic orbits and invariant polydisks	273
8. Birational actions of lattices on quasi-projective varieties	285
9. Appendix	289
References	292

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 $\mathrm{Aut}(X)$ denote its group of (regular) automorphisms and $\mathrm{Bir}(X)$ its group of birational transformations. A good example is provided by the affine space $\mathbb{A}_{\mathbf{C}}^d$ of dimension $d \geq 2$: Its group of automorphisms is “infinite-dimensional” and contains elements with a rich dynamical behavior (see [34], [3]); its group of birational transformations is the Cremona group $\mathrm{Cr}_d(\mathbf{C})$, and is known to be much larger than $\mathrm{Aut}(\mathbb{A}_{\mathbf{C}}^d)$.

We present two new arguments that can be combined to study finitely generated groups acting by automorphisms or birational transformations. They lead to new constraints on groups of birational transformations, *in any dimension*.

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 the theorem of Skolem, Mahler, and Lech, which says that the zeros of a linear recurrence sequence occur along a finite union of arithmetic progressions. This method plays now a central role in arithmetic dynamics (see [6], [7], [55]). The second strategy has been developed by Bass, Milnor, and Serre when they obtained rigidity results for finite-dimensional linear representations of $\mathrm{SL}_n(\mathbf{Z})$ as a corollary of the congruence subgroup property (see [2], [62]). Here, we combine these strategies for non-linear actions of finitely generated groups of birational transformations.

Our second argument makes use of isoperimetric inequalities from geometric group theory and of the Lang–Weil estimates from diophantine geometry. We now list the main results that follow from the combination of those arguments.

1.2. Actions of $\mathrm{SL}_n(\mathbf{Z})$

Consider the group $\mathrm{SL}_n(\mathbf{Z})$ of $n \times n$ matrices with integer entries and determinant 1. Let Γ be a finite-index subgroup of $\mathrm{SL}_n(\mathbf{Z})$; it acts by linear projective transformations on the projective space $\mathbb{P}_{\mathbf{C}}^{n-1}$, and the kernel of the homomorphism $\Gamma \rightarrow \mathrm{PGL}_n(\mathbf{C})$ contains at most two 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 $\mathrm{SL}_n(\mathbf{Z})$. Let X be an irreducible, complex, quasi-projective variety. If Γ embeds into $\mathrm{Aut}(X)$, then $\dim_{\mathbf{C}}(X) \geq n-1$. If $\dim_{\mathbf{C}}(X) = n-1$, then there is an isomorphism $\tau: X \rightarrow \mathbb{P}_{\mathbf{C}}^{n-1}$ which conjugates the action of Γ on X to a linear projective action on $\mathbb{P}_{\mathbf{C}}^{n-1}$.*

Let \mathbf{k} and \mathbf{k}' be fields of characteristic zero. Every field of characteristic zero which is generated by finitely many elements embeds into \mathbf{C} . Since finite-index subgroups of $\mathrm{SL}_n(\mathbf{Z})$ are finitely generated, Theorem A implies: (1) *the group $\mathrm{SL}_n(\mathbf{Z})$ embeds into $\mathrm{Aut}(\mathbb{A}_{\mathbf{k}}^d)$ if and only if $d \geq n$* ; (2) *if $\mathrm{Aut}(\mathbb{A}_{\mathbf{k}}^d)$ embeds into $\mathrm{Aut}(\mathbb{A}_{\mathbf{k}'}^{d'})$ (as abstract groups), then $d \leq d'$* . Previous proofs of assertion (2) assumed \mathbf{k} to be equal to \mathbf{C} (see [27], [45]).

1.3. Lattices in simple Lie groups

Theorem A may be extended in two directions, replacing $\mathrm{SL}_n(\mathbf{Z})$ by more general lattices, and looking at actions by birational transformations instead of automorphisms. Let S be an absolutely almost simple linear algebraic group which is defined over \mathbf{Q} ; fix an embedding of S in GL_n (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 $S(\mathbf{Z})$ is a lattice in $S(\mathbf{R})$; it is cocompact if and only if the \mathbf{Q} -rank of S vanishes (see [8]).

THEOREM B. *Let X be an irreducible complex projective variety. Let $S \subset \mathrm{GL}_n$ be a linear algebraic group, over the field of rational numbers \mathbf{Q} . Assume that S is absolutely almost simple, and that the lattice $S(\mathbf{Z})$ is not cocompact in $S(\mathbf{R})$. If a finite-index subgroup of $S(\mathbf{Z})$ embeds into $\mathrm{Bir}(X)$, then*

$$\dim_{\mathbf{C}}(X) \geq \mathrm{rank}_{\mathbf{R}}(S).$$

If $\dim(X) = \mathrm{rank}_{\mathbf{R}}(S) \geq 2$, then $S_{\mathbf{R}}$ is \mathbf{R} -isogeneous to $\mathrm{SL}_{\dim(X)+1, \mathbf{R}}$.

As a corollary, the Cremona group $\mathrm{Cr}_d(\mathbf{k})$ does not embed into $\mathrm{Cr}_{d'}(\mathbf{k}')$ if \mathbf{k} and \mathbf{k}' have characteristic zero and $d > d'$.

Remark 1.1. If $\mathrm{rank}_{\mathbf{R}}(S) \geq 2$, every lattice Γ of $S(\mathbf{R})$ is almost simple: Its normal subgroups are finite and central, or cofinite (see §4.2 and 8.1). Thus, the assumption “ Γ embeds into $\mathrm{Bir}(X)$ ” can be replaced by “there is a homomorphism from Γ to $\mathrm{Bir}(X)$ with infinite image”. Using the Margulis arithmeticity theorem, one can replace S by any simple real Lie group H with $\mathrm{rank}_{\mathbf{R}}(H) \geq 2$, and $S(\mathbf{Z})$ by any non-uniform lattice of H in the statement of Theorem B.

Remark 1.2. The statement of Theorem B concerns non-uniform lattices, because the proof makes use of the congruence subgroup property, and the congruence kernel is known to be finite for all those lattices. There are also uniform lattices for which this property is known and the same proof applies (for instance for all lattices in \mathbf{Q} -anisotropic spin groups for quadratic forms in $m \geq 5$ variables with real rank ≥ 2 ; see [43], [64]).

Remark 1.3. The main theorems of [11], [19] extend Theorem B to all types of lattices (including cocompact lattices) in simple real Lie groups, but assume that the action is by regular automorphisms on a compact Kähler manifold. When X is compact, $\mathrm{Aut}(X)$ is a complex Lie group: It may have infinitely many connected components, but its dimension is finite. The techniques of [11], [19] do not apply to arbitrary quasi-projective varieties (for instance to $X = \mathbb{A}_{\mathbf{C}}^d$) and to groups of birational transformations. See [17], [13], [26] for groups of birational transformations of surfaces.

Example 1.4. There is a lattice in $\mathrm{SO}_{1,9}(\mathbf{R})$ which acts faithfully on a rational surface by regular automorphisms: This is due to Coble (see [16, §3.4]). A similar phenomenon holds for general Enriques surfaces (see [23]). Thus, lattices in simple Lie groups of large dimension may act faithfully on small-dimensional varieties.

1.4. Finite fields and Hrushovski's theorem

Let Γ be a finite-index subgroup of $S(\mathbf{Z})$, where S is as in Theorem B. To prove Theorems A and B, we first change the field of definition, replacing \mathbf{C} by the field of p -adic numbers \mathbf{Q}_p for some large prime number p ; indeed, since the ring generated by the coefficients of the formulae defining the variety X and the generators of the group $\Gamma \subset \text{Bir}(X)$ is finitely generated, we may embed this ring in \mathbf{Z}_p for some large prime p .

Then, we prove that there exists a finite extension K of \mathbf{Q}_p and a p -adic polydisk in $X(K)$ which is invariant under the action of a finite-index subgroup Γ' of Γ , and on which Γ' acts by Tate analytic diffeomorphisms. Those polydisks correspond to periodic orbits for the action of Γ on $X(\mathbf{F})$, where \mathbf{F} is the residue field of the non-archimedean field K . Thus, an important step toward Theorem B is the existence of pairs (m, Γ') , where m is in $X(\mathbf{F})$, Γ' is a finite-index subgroup of Γ , and all elements of Γ' are well defined at m and fix m (no element of Γ' has an indeterminacy at m). For cyclic groups of transformations, this follows from a theorem of Hrushovski (see [41]). Here, we combine the Lang–Weil estimates with isoperimetric inequalities from geometric group theory: The existence of the pair (m, Γ') is obtained for groups with Kazhdan property (T) in Theorems 7.10 and 7.13; the argument applies also to other types of groups (see §7.2.5).

Once such invariant polydisks are constructed, several corollaries easily follow (see §7.4.2). For instance, we get the following result.

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

1.5. The p -adic method

When an invariant p -adic polydisk is constructed, a theorem of Bell and Poonen provides a tool to extend the action of every element γ in our group into a Tate analytic action of the additive group \mathbf{Z}_p . When Γ has finite index in $S(\mathbf{Z})$, as in Theorem B, and $\text{rank}_{\mathbf{R}}(S) \geq 2$, this may be combined with the congruence subgroup property: We prove that the action of the lattice extends to an action of a finite-index subgroup of the p -adic group $S(\mathbf{Z}_p)$ by Tate analytic transformations (Theorem 2.11). Thus, starting with a countable group of birational transformations, we end up with an analytic action of a p -adic Lie group to which Lie theory may be applied. This is how Theorems A and B are proven; our strategy applies also to actions of other discrete groups, such as the mapping class group of a closed surface of genus g , or the group of outer automorphisms of a free group (see §6 and §[1]). Let us state a sample result.

Given a group Γ , let $\text{ma}(\Gamma)$ be the smallest dimension of a complex irreducible variety on which some finite-index subgroup of Γ acts faithfully by automorphisms. Let $\text{Mod}(g)$ be the mapping class group of a closed orientable surface of genus g . It is known that $\text{ma}(\text{Mod}(g)) \leq 6g - 6$ for all $g \geq 2$ (see §6.1), and that $\text{ma}(\text{Mod}(1)) = 1$ (because a finite-index subgroup of $\text{GL}_2(\mathbf{Z})$ embeds into $\text{PGL}_2(\mathbf{C})$).

THEOREM D. *If $\text{Mod}(g)$ acts faithfully on a complex variety X by automorphisms, then $\dim(X) \geq 2g - 1$. Thus, $2g - 1 \leq \text{ma}(\text{Mod}(g)) \leq 6g - 6$ for every $g \geq 2$.*

1.6. Margulis super-rigidity and Zimmer program

Let Γ be a lattice in a simple real Lie group S , with $\text{rank}_{\mathbf{R}}(S) \geq 2$. According to the 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 [51]).

The 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 [67], [68], and the recent survey [32]). Theorems A and B are instances of Zimmer program in the context of algebraic geometry.

When $\Gamma = \text{SL}_n(\mathbf{Z})$ or $\Gamma = \text{Sp}_{2n}(\mathbf{Z})$, Bass, Milnor, and Serre obtained a super-rigidity theorem from their solution of the congruence subgroup problem (see [2, §16] and [62]). 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.

1.7. Notation

To specify the field (or ring) of definition K of an algebraic variety (or scheme) X , we use the notation X_K . If K' is an extension of K , $X(K')$ is the set of K' -points of X . The group of automorphisms (resp. birational transformations) of X which are defined over K' is denoted $\text{Aut}(X_{K'})$ (resp. $\text{Bir}(X_{K'})$).

1.8. Acknowledgement

Thanks to Yves de Cornulier, Julie Déserti, Philippe Gille, Sébastien Gouezel, Vincent Guirardel, and Peter Sarnak for interesting discussions related to this article. We thank the referees for numerous insightful remarks, and in particular for their suggestions regarding §2.4, §6 and §7. This work was supported by the ANR project BirPol and

the foundation Del Duca from the French Academy of Sciences, and the Institute for Advanced Study, Princeton.

2. Tate analytic diffeomorphisms of the p -adic polydisk

In this section, we introduce the group of Tate analytic diffeomorphisms of the unit polydisk $\mathcal{U}=\mathbf{Z}_p^d$, describe its topology, and study its finite-dimensional subgroups. The main result of this section is Theorem 2.11.

2.1. Tate analytic diffeomorphisms

2.1.1. The Tate algebra (see [59, §6])

Let p be a prime number. Let K be a field of characteristic zero which is complete with respect to an absolute value $|\cdot|$ satisfying $|p|=1/p$; such an absolute value is automatically ultrametric (see [44, Examples 2 and 3 in §I.2]). 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 $R[\mathbf{x}]=R[\mathbf{x}_1, \dots, \mathbf{x}_d]$ of polynomial functions in d variables with coefficients in R . For f in $R[\mathbf{x}]$, define the norm $\|f\|$ to be the supremum of the absolute values of the coefficients of f :

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

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

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

$$f \equiv g \pmod{p^c} \tag{2.2}$$

means $\|f - g\| \leq |p|^c$; we then extend such notation componentwise to $(R\langle \mathbf{x} \rangle)^m$ for all $m \geq 1$. For instance, with $d=2$, the polynomial mapping $f(\mathbf{x}) = (\mathbf{x}_1 + p, \mathbf{x}_2 + p\mathbf{x}_1\mathbf{x}_2)$ satisfies $f \equiv \text{id} \pmod{p}$, where $\text{id}(\mathbf{x}) = \mathbf{x}$ is the identity.

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 $\text{dist}(x, y)$ is defined by $\text{dist}(x, y)=\max_i |x_i - y_i|$, where the x_i 's and y_i 's are the coordinates of x and y in R^d . The non-archimedean triangle inequality implies that $|h(y)| \leq 1$ for every h in $R\langle \mathbf{x} \rangle$ and $y \in \mathcal{U}$. Consequently, every element g in $R\langle \mathbf{x} \rangle^d$ determines a Tate analytic map $g: \mathcal{U} \rightarrow \mathcal{U}$.

If $g=(g_1, \dots, g_d)$ is an element of $R\langle \mathbf{x} \rangle^d$, the norm $\|g\|$ is defined as the maximum of the norms $\|g_i\|$ (see equation (2.1)); one has

$$\|g\| \leq 1 \quad \text{and} \quad \text{dist}(g(x), g(y)) \leq \|g\| \text{dist}(x, y), \tag{2.3}$$

so that g is 1-Lipschitz.

For indeterminates $\mathbf{x}=(\mathbf{x}_1, \dots, \mathbf{x}_d)$ and $\mathbf{y}=(\mathbf{y}_1, \dots, \mathbf{y}_m)$, the composition

$$R\langle \mathbf{y} \rangle \times R\langle \mathbf{x} \rangle^m \longrightarrow R\langle \mathbf{x} \rangle$$

is well defined, and hence coordinatewise we obtain

$$R\langle \mathbf{y} \rangle^n \times R\langle \mathbf{x} \rangle^m \longrightarrow R\langle \mathbf{x} \rangle^n.$$

In particular, with $m=n=d$, we get a semigroup $R\langle \mathbf{x} \rangle^d$. The group of (Tate) *analytic diffeomorphisms* of \mathcal{U} is the group of invertible elements in this semigroup; we denote it by $\text{Diff}^{\text{an}}(\mathcal{U})$. Elements of $\text{Diff}^{\text{an}}(\mathcal{U})$ are transformations $f: \mathcal{U} \rightarrow \mathcal{U}$ given by

$$f(\mathbf{x}) = (f_1, \dots, f_d)(\mathbf{x}),$$

where each f_i is in $R\langle \mathbf{x} \rangle$ and f has an inverse $f^{-1}: \mathcal{U} \rightarrow \mathcal{U}$ that is also defined by power series in the Tate algebra. The distance between two Tate analytic diffeomorphisms f and g is defined as $\|f - g\|$; by the following lemma, this endows $\text{Diff}^{\text{an}}(\mathcal{U})$ with the structure of a topological group.

LEMMA 2.1. *Let f, g , and h be elements of $R\langle \mathbf{x} \rangle^d$. Then,*

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

Proof. Let $s \in R$ and $c > 0$ satisfy $|p|^c = |s| = \|g\|$. Then $(1/s)g$ is an element of $R\langle \mathbf{x} \rangle^d$. It follows that $(1/s)g \circ f$ is an element of $R\langle \mathbf{x} \rangle^d$ 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 $h=(h_1, h_2, \dots, h_d)$, where each h_i satisfies $\|h_i\| \leq \|h\|$. Then $g \circ (\text{id} + h)$ takes the form

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

where each A_i is a homogeneous polynomial in $(\mathbf{x}_1, \dots, \mathbf{x}_d)$ of degree i with coefficients in R . Assertion (3) follows. For assertion (4), assume that f is an analytic diffeomorphism and apply assertion (2): $\|f^{-1} - \text{id}\| = \|\text{id} - f\|$. □

This lemma easily implies the following proposition (see [18] for details).

PROPOSITION 2.2. *For every real number $c > 0$, the subgroup of all elements $f \in \text{Diff}^{\text{an}}(\mathcal{U})$ with $f \equiv \text{id} \pmod{p^c}$ is a normal subgroup of $\text{Diff}^{\text{an}}(\mathcal{U})$.*

LEMMA 2.3. *Let f be an element of $\text{Diff}^{\text{an}}(\mathcal{U})$. If $f(\mathbf{x}) \equiv \text{id} \pmod{p^c}$, with $c \geq 1$, and p^N divides l , then the l -th iterate of f satisfies $f^l(\mathbf{x}) \equiv \text{id} \pmod{p^{c+N}}$. In particular, if $f \equiv \text{id} \pmod{p}$, then $f^{p^\ell} \equiv \text{id} \pmod{p^\ell}$.*

Proof. Write $f(\mathbf{x}) = \mathbf{x} + sr(\mathbf{x})$, where r is in $R\langle \mathbf{x} \rangle^d$ and $s \in R$ satisfies $|s| \leq |p|^c$. Then,

$$f \circ f(\mathbf{x}) = \mathbf{x} + sr(\mathbf{x}) + sr(\mathbf{x} + sr(\mathbf{x})) = \mathbf{x} + 2sr(\mathbf{x}) + s^2u_2(\mathbf{x})$$

for some $u_2 \in R\langle \mathbf{x} \rangle^d$. After k iterations, one gets

$$f^k(\mathbf{x}) = \mathbf{x} + ksr(\mathbf{x}) + s^2u_k(\mathbf{x}),$$

with $u_k \in R\langle \mathbf{x} \rangle^d$. Taking $k=p$, we obtain

$$f^p(\mathbf{x}) = \mathbf{x} + psr(\mathbf{x}) + s^2u_p(\mathbf{x}) \equiv \mathbf{x} \pmod{p^{c+1}},$$

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

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 [55], as well as [6, Lemma 4.2] and [7, Theorem 3.3]).

THEOREM 2.4. *Let f be an element of $R\langle \mathbf{x} \rangle^d$ with $f \equiv \text{id} \pmod{p^c}$ for some real number $c > 1/(p-1)$. Then, f is a Tate diffeomorphism of $\mathcal{U} = R^d$ and there exists a unique Tate analytic map $\Phi: \mathcal{U} \times R \rightarrow \mathcal{U}$ such that*

- (1) $\Phi(\mathbf{x}, n) = f^n(\mathbf{x})$ for all $n \in \mathbf{Z}$;

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

We shall refer to this theorem as the “Bell–Poonen theorem”, or “Bell–Poonen extension theorem”. An analytic map $\Phi: \mathcal{U} \times R \rightarrow \mathcal{U}$ which defines an action of the group $(R, +)$ will be called an R -flow, or simply a flow. See below, in §2.2.2, how it is viewed as the flow of an analytic vector field. A flow Φ will be considered either as an analytic action $\Phi: \mathcal{U} \times R \rightarrow \mathcal{U}$ of the abelian group $(R, +)$, or as a morphism

$$\Phi: t \in R \mapsto \Phi_t = \Phi(\cdot, t) \in \text{Diff}^{\text{an}}(\mathcal{U});$$

we use the same vocabulary (and the same letter Φ) for the two maps. The Bell–Poonen theorem implies that every element f of $R\langle \mathbf{x} \rangle^d$ with $f \equiv \text{id} \pmod{p^2}$ is included in an analytic R -flow.

COROLLARY 2.5. *Let f be an element of $R\langle \mathbf{x} \rangle^d$ with $f \equiv \text{id} \pmod{p^c}$ for some real number $c > 1/(p-1)$. Then, f is a Tate diffeomorphism of $\mathcal{U} = R^d$ and, if f has finite order in $\text{Diff}^{\text{an}}(\mathcal{U})$, then $f = \text{id}$.*

To prove it, assume that f has order $k \geq 1$ and apply the Bell–Poonen theorem. For every $x \in \mathcal{U}$, the analytic curve $t \mapsto \Phi(x, t) - x$ vanishes on the infinite set $\mathbf{Z}k$; hence, it vanishes identically, $f(x) = \Phi(x, 1) = x$ for all $x \in \mathcal{U}$, and $f = \text{id}$.

Remark 2.6. Theorem 2.4 is not stated as such in [55]. Poonen constructs a Tate analytic map $\Phi: \mathcal{U} \times R \rightarrow \mathcal{U}$ which satisfies property (1) for $n \geq 0$; his proof implies also Properties (3) and (4). We now deduce property (1) for $n \in \mathbf{Z}$. We already know that the relation $\Phi(\mathbf{x}, n+1) = f \circ \Phi(\mathbf{x}, n)$ 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}_+ , and hence on R , by the isolated zero principle. This implies $\Phi(\mathbf{x}, t+1) = f \circ \Phi(\mathbf{x}, t)$ in $R\langle \mathbf{x}, t \rangle^d$. Take $t = -1$ to deduce that f is an analytic diffeomorphism of \mathcal{U} and $f^{-1} = \Phi(\cdot, -1)$. Then, by induction, one gets $\Phi(\mathbf{x}, n) = f^n(\mathbf{x})$ for all $n \in \mathbf{Z}$. Property (2) follows from (1) for s and t in \mathbf{Z} , and then for all values of s and t in R by the isolated zero principle.

2.2.2. Flows and Tate analytic vector fields

Consider the Lie algebra $\Theta(\mathcal{U})$ of vector fields $\mathbf{X} = \sum_{i=1}^d u_i(\mathbf{x})\partial_i$, where each u_i is an element of the Tate algebra $R\langle \mathbf{x} \rangle$. The Lie bracket with a vector field $\mathbf{Y} = \sum_i v_i(\mathbf{x})\partial_i$ is given by

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

LEMMA 2.7. *Let $\Phi: \mathcal{U} \times R \rightarrow \mathcal{U}$ be an element of $R\langle \mathbf{x}, t \rangle^d$ that defines an analytic flow. Then, $\mathbf{X} = (\partial\Phi/\partial t)|_{t=0}$ 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 $\mathbf{X}(x_0) = \mathbf{0}$ 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 2.8. *If f is an element of $\text{Diff}^{\text{an}}(\mathcal{U})$ with $f \equiv \text{id} \pmod{p^c}$ for some $c > 1/(p-1)$, 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}_f are the fixed points of f .*

Two such diffeomorphisms f and g commute if and only if $[\mathbf{X}_f, \mathbf{X}_g] = \mathbf{0}$.

Proof. The first assertion follows directly from Lemma 2.7 and the Bell–Poonen theorem (Theorem 2.4). Let us prove the second assertion. If \mathbf{X}_f commute with \mathbf{X}_g , then Φ_f and Φ_g commute too, meaning that $\Phi_f(\Phi_g(x, t), s) = \Phi_g(\Phi_f(x, s), t)$ for every pair $(s, t) \in R \times R$. Taking $(s, t) = (1, 1)$, we obtain $f \circ g = g \circ f$. If f and g commute, then $\Phi_f(\Phi_g(x, n), m) = f^m \circ g^n = \Phi_g(\Phi_f(x, m), n)$ for every pair (m, n) of integers, and the principle of isolated zeros implies that the flows Φ_f and Φ_g commute; hence, $[\mathbf{X}_f, \mathbf{X}_g] = \mathbf{0}$. \square

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 having a (finite) power of p as index. In such a group, the index of every open normal subgroup is a power of p . We refer to [28] for a good introduction to pro- p groups.

In this subsection, we assume that K is a finite extension of \mathbf{Q}_p . The residue field, i.e. the quotient of R by its maximal ideal $\mathfrak{m}_K = \{x \in K : |x| < 1\}$, is a finite field of characteristic p . It has q elements, with q being a power of p , and the number of elements of the ring R/\mathfrak{m}_K^k is a power of p for every k . We also fix an element π that generates the ideal \mathfrak{m}_K .

2.3.1. Action modulo \mathfrak{m}_K^k

Recall that \mathcal{U} denotes the polydisk R^d . Let f be an element of $\text{Diff}^{\text{an}}(\mathcal{U})$. Its reduction modulo \mathfrak{m}_K^k is a polynomial transformation with coefficients \bar{a}_I in the finite ring R/\mathfrak{m}_K^k ; it determines a permutation of the finite set $(R/\mathfrak{m}_K^k)^d$. Thus, for each $k \geq 1$, reduction

modulo \mathfrak{m}_K^k provides a homomorphism $\theta_k: \text{Diff}^{\text{an}}(\mathcal{U}) \rightarrow \text{Perm}((R/\mathfrak{m}_K^k)^d)$ into the group of permutations of the finite set $(R/\mathfrak{m}_K^k)^d$.

Another way to look at the same action is as follows. Each element of $\text{Diff}^{\text{an}}(\mathcal{U})$ acts isometrically on \mathcal{U} with respect to the distance $\text{dist}(x, y)$ (see §2.1.2); in particular, for every radius r , $\text{Diff}^{\text{an}}(\mathcal{U})$ acts by permutations on the set of balls of \mathcal{U} of radius r . Since the set of balls of radius $|\pi|^{-k}$ is in bijection with the set $(R/\mathfrak{m}_K^k)^d$, the action of $\text{Diff}^{\text{an}}(\mathcal{U})$ on this set of balls may be identified with its action on $(R/\mathfrak{m}_K^k)^d$ after reduction modulo \mathfrak{m}_K^k .

As a consequence, we have that an element f of $\text{Diff}^{\text{an}}(\mathcal{U})$ is the identity if and only if $\text{dist}(f(x), x) \leq |\pi|^k$ for all x and all k , and this is true if and only if its image in the group of permutations of $(R/\mathfrak{m}_K^k)^d$ is trivial for all k .

2.3.2. A pro- p completion

Given a positive integer r , define $\text{Diff}^{\text{an}}(\mathcal{U})_r$ as the subgroup of $\text{Diff}^{\text{an}}(\mathcal{U})$ whose elements are equal to the identity modulo p^r . For $r=1$, we set

$$D = \text{Diff}^{\text{an}}(\mathcal{U})_1 = \{f \in \text{Diff}^{\text{an}}(\mathcal{U}) : f \equiv \text{id} \pmod{p}\}. \tag{2.4}$$

By definition, f is an element of D if it can be written $f = \text{id} + ph$, where h is in $R\langle \mathbf{x} \rangle^d$. Thus, D acts trivially on $(R/pR)^d$ (here, $pR = \mathfrak{m}_K^\ell$ with $|\pi^\ell| = 1/p$ for some ℓ).

Now we show that the image $\theta_{\ell m}(D)$ in $\text{Perm}((R/p^m R)^d)$ is a finite p -group. Indeed, by Lemma 2.3, for any $f \in D$, we have $f^{p^{m-1}} \equiv \text{id} \pmod{p^m}$. Thus, $f^{p^{m-1}}$ acts trivially on $(R/p^m R)^d$. It follows that the order of every element in $\theta_{\ell m}(D)$ is a power of p . Since $\theta_{\ell m}(D)$ is a finite group, Sylow’s theorem implies that $\theta_{\ell m}(D)$ is a p -group.

We endow the finite groups $\text{Perm}((R/p^m R)^d)$ with the discrete topology, and we denote by \widehat{D} the inverse limit of the p -groups $\theta_{\ell m}(D) \subset \text{Perm}((R/p^m R)^d)$; \widehat{D} is a pro- p group: It is the closure of the image of D in $\prod_m \text{Perm}((R/p^m R)^d)$ by the diagonal embedding $(\theta_{\ell m})_{m \geq 1}$. We denote by \mathcal{T} the topology of \widehat{D} (resp. the induced topology on D); the kernels of the homomorphisms $\theta_{\ell m}$ form a basis of neighborhoods of the identity for this topology.

Since the action on $(R/p^m R)^d$ is the action on the set of balls of radius p^{-m} in \mathcal{U} , the Tate topology is finer than the topology \mathcal{T} : The identity map $f \mapsto f$ is a continuous homomorphism with respect to the Tate topology on the source, and the topology \mathcal{T} on the target; we shall denote this continuous injective homomorphism by

$$D \ni f \mapsto \hat{f} \in \widehat{D}.$$

Remark 2.9. Fix a prime p and consider the field $K = \mathbf{Q}_p$, with valuation ring $R = \mathbf{Z}_p$. Assume that the dimension d is 2. The sequence of polynomial automorphisms of the affine plane defined by $h_n(x, y) = (x, y + p(x + x^2 + x^3 + \dots + x^n))$ determines a sequence of elements of D . No subsequence of $\{h_n\}_n$ converges in the Tate topology, but in the compact group \widehat{D} one can extract a converging subsequence. A better example is provided by the sequence $g_n(x, y) = (x, y + s_n(x))$ with $s_n(x) = x^n(x^{p^n - p^{n-1}} - 1)$. This sequence converges towards the identity in \widehat{D} , because s_n vanishes on $\mathbf{Z}/p^n\mathbf{Z}$, but does not converge in D for the Tate topology.

2.4. Extension theorem

2.4.1. Analytic groups (see [47, §IV], or [28], [60] and [10, Chapter III])

Let G be a topological group. We say that G is a p -adic analytic group if there is a structure of p -adic analytic manifold on G which is compatible with the topology of G and the group structure. The group law $G \times G \ni (x, y) \mapsto xy^{-1}$ is p -adic analytic (see [28, Chapter 8]). If such a structure exists, it is unique (see [28, Chapter 9]). The dimension $\dim(G)$ is the dimension of G as a p -adic manifold.

If G is a compact, p -adic analytic group, then G contains a finite-index, open, normal subgroup G_0 which is a (uniform) pro- p group. Moreover, G_0 embeds continuously in $\mathrm{GL}_d(\mathbf{Z}_p)$ for some d (see [28, Chapters 7 and 8]).

Let g be an element of the pro- p group G . The homomorphism $\varphi: m \in \mathbf{Z} \mapsto g^m \in G$ extends automatically to the pro- p completion of \mathbf{Z} , i.e. to a continuous homomorphism of pro- p groups

$$\bar{\varphi}: \mathbf{Z}_p \longrightarrow G.$$

For simplicity, we denote $\bar{\varphi}(t)$ by g^t for t in \mathbf{Z}_p (see [28, Proposition 1.28], for embeddings of \mathbf{Z}_p into pro- p groups).

LEMMA 2.10. *Let G be a p -adic analytic pro- p group of dimension $s = \dim(G)$. Let Γ be a dense subgroup of G . There exist an integer $r \geq s$ and elements $\gamma_1, \dots, \gamma_r$ in Γ such that the map $\pi: \mathbf{Z}_p^r \rightarrow G$, $\pi(t_1, \dots, t_r) = (\gamma_1)^{t_1} \dots (\gamma_r)^{t_r}$, satisfies the following properties:*

- (1) π is a surjective, p -adic analytic map;
- (2) the restriction of π to $\{(t_i)_i: t_j = 0 \text{ if } j > s\}$ is a local diffeomorphism onto its image;
- (3) 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 (see the notion of standard subgroups in [10], [28]). Let H be such a subgroup.

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 $\alpha_1, \dots, \alpha_s$ of Γ , with $s = \dim(G)$, such that the ν_i generate \mathfrak{g} . Then, the map $\pi: \mathbf{Z}_p^d \rightarrow H$ defined by

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

is analytic and, by the p -adic inverse function theorem, it determines a local analytic diffeomorphism from a neighborhood of zero in \mathfrak{g} to a neighborhood V of 1_G . The group G can then be covered by a finite number of translates $h_j V$, $j = 1, \dots, s'$. 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 $1 \leq i \leq s$, and $\gamma_i = \beta_{i-s}$ for $s + 1 \leq i \leq r$. □

2.4.2. Actions by Tate analytic diffeomorphisms.

Let G be a compact p -adic analytic group. Let Γ be a finitely generated subgroup of G . We say that G is a *virtual pro- p completion* of Γ if there exists a finite-index subgroup Γ_0 of Γ such that (1) the closure of Γ_0 in G is an open pro- p subgroup G_0 of G , and (2) G_0 coincides with the pro- p completion of Γ_0 . Note that, by compactness of G , the group G_0 has finite index in G . A good example to keep in mind is $\Gamma = \mathrm{SL}_n(\mathbf{Z})$ in $G = \mathrm{SL}_n(\mathbf{Z}_p)$ (see §4.2.3 below).

We now study homomorphisms from Γ to the group $\mathrm{Diff}^{\mathrm{an}}(\mathcal{U})$. 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 $\mathrm{Diff}^{\mathrm{an}}(\mathcal{U})$.

THEOREM 2.11. *Let p be an odd prime, and let G be a compact, p -adic analytic group. Let Γ be a finitely generated subgroup of G . Assume that G is a virtual pro- p completion of Γ .*

Let $\Phi: \Gamma \rightarrow \mathrm{Diff}^{\mathrm{an}}(\mathcal{U})_1$ be a homomorphism into the group of Tate analytic diffeomorphisms of \mathcal{U} which are equal to the identity modulo p . Then, there exists a finite-index subgroup Γ_0 of Γ for which $\Phi|_{\Gamma_0}$ extends to the closure $G_0 = \bar{\Gamma}_0 \subset G$ as a continuous homomorphism

$$\bar{\Phi}: G_0 \longrightarrow \mathrm{Diff}^{\mathrm{an}}(\mathcal{U})_1$$

such that the action $G_0 \times \mathcal{U} \rightarrow \mathcal{U}$ given by $(g, x) \mapsto \bar{\Phi}(g)(x)$ is analytic.

Denote $\text{Diff}^{\text{an}}(\mathcal{U})_1$ by D , as in equation (2.4). Recall from §2.3.2 that D embeds continuously into the pro- p group \widehat{D} . Let Γ_0 be a finite-index subgroup of Γ whose closure G_0 in G is the pro- p completion of Γ_0 . We obtain:

(1) The homomorphism $\Gamma_0 \rightarrow \widehat{D}$ extends uniquely into a continuous homomorphism $\hat{\Phi}$ from $G_0 = \bar{\Gamma}_0$ to \widehat{D} .

Then, the following property is automatically satisfied:

(2) Let f be an element of D . By the Bell–Poonen extension theorem (Theorem 2.4), the homomorphism $t \in \mathbf{Z} \mapsto f^t$ extends to a continuous morphism $\mathbf{Z}_p \rightarrow D$ via a Tate analytic flow. If \hat{f} denotes the image of f in \widehat{D} , then $n \mapsto (\hat{f})^n$ is a homomorphism from \mathbf{Z} to the pro- p group \widehat{D} ; as such, it extends canonically to the pro- p completion \mathbf{Z}_p , giving rise to a homomorphism $t \in \mathbf{Z}_p \mapsto (\hat{f})^t \in \widehat{D}$. These two extensions are compatible: $(\widehat{f^t}) = (\hat{f})^t$ for all t in \mathbf{Z}_p .

Thus, given any 1-parameter subgroup \mathbf{Z} of Γ , we already know how to extend $\Phi: \mathbf{Z} \subset \Gamma \rightarrow D$ into $\bar{\Phi}: \mathbf{Z}_p \subset G_0 \rightarrow D$ in a way that is compatible with the extension $\hat{\Phi}: G_0 \rightarrow \widehat{D}$.

For simplicity, we now denote Γ_0 by Γ and G_0 and G .

LEMMA 2.12. *Let $(\alpha_n)_n$ be a sequence of elements of Γ that converges towards 1_G in G . Then $(\Phi(\alpha_n))_n$ converges towards the identity in $\text{Diff}^{\text{an}}(\mathcal{U})$.*

Proof. Write $\alpha_n = \pi(t_1(n), \dots, t_r(n)) = (\gamma_1)^{t_1(n)} \dots (\gamma_r)^{t_r(n)}$, where π and the γ_i are given by Lemma 2.10 and the $t_i(n)$ are in \mathbf{Z}_p . Since α_n converges towards 1_G , we may assume, by Lemma 2.10, that each $(t_i(n))$ converges towards zero in \mathbf{Z}_p as n goes to ∞ . By the Bell–Poonen theorem (Theorem 2.4), each $f_i := \Phi(\gamma_i)$ gives rise to a flow $t \mapsto f_i^t$, $t \in \mathbf{Z}_p$; moreover, $\|f_i^t - \text{id}\| \leq p^m$ if $|t| < p^m$ (apply Lemma 2.3 and the last assertion in the Bell–Poonen theorem). Thus, the lemma follows from Lemma 2.1 and the equality

$$\Phi(\alpha_n) = f_1^{t_1(n)} \dots f_r^{t_r(n)}. \tag{2.5}$$

To prove this equality, one only needs to check it in the group \widehat{D} , because D embeds into \widehat{D} . But, in \widehat{D} , the equality holds trivially because the homomorphism $\Gamma_0 \rightarrow \widehat{D}$ extends to G_0 continuously (apply properties (1) and (2) above). □

LEMMA 2.13. *If $(\alpha_m)_{m \geq 1}$ is a sequence of elements of Γ that converges towards an element α_∞ of G , then $(\Phi(\alpha_m))_m$ converges to an element of $\text{Diff}^{\text{an}}(\mathcal{U})$ which depends only on α_∞ .*

Proof. Since $(\alpha_m)_m$ converges, $\alpha_m \circ \alpha_{m'}^{-1}$ converges towards the neutral element 1_G as m and m' go to ∞ . Consequently, Lemma 2.12 shows that the sequence $(\Phi(\alpha_m))_m$ is a Cauchy sequence in $\text{Diff}^{\text{an}}(\mathcal{U})$, and hence a convergent sequence.⁽¹⁾ The limit depends

⁽¹⁾ Write $\Phi(\alpha_m \circ \alpha_{m'}^{-1}) = \text{id} + \varepsilon_{m,m'}$, where $\varepsilon_{m,m'}$ is equivalent to the constant map zero in $R(\mathbf{x})^d$ modulo $|p|^{k(m,m')}$, with $k(m,m')$ that goes to ∞ as m and m' do. Then, apply Lemma 2.1.

only on α_∞ , not on the sequence $(\alpha_m)_m$ (if another sequence $(\alpha'_m)_m$ converges toward α_∞ , consider the sequence $\alpha_1, \alpha'_1, \alpha_2, \alpha'_2, \dots$). \square

We can now prove Theorem 2.11. Lemmas 2.12 and 2.13 show that Φ extends, in a unique way, to a continuous homomorphism $\bar{\Phi}: G \rightarrow D$. Moreover, this extension coincides with Bell–Poonen extensions $\mathbf{Z}_p \rightarrow D$ along 1-parameter subgroups of G generated by elements of Γ . According to Lemma 2.10, one can find s elements $\gamma_1, \dots, \gamma_s$ of Γ , with $s = \dim(G)$, such that the map

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

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

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

is analytic. Thus, the action of G on \mathcal{U} determined by $\bar{\Phi}$ is analytic. This concludes the proof of Theorem 2.11.

3. Good models, p -adic integers, and invariant polydisks

Start with an irreducible complex variety X of dimension d , a finitely generated group Γ , and a homomorphism $\varrho: \Gamma \rightarrow \text{Bir}(X)$. First, we explain how to replace the field \mathbf{C} , or any algebraically closed field \mathbf{k} of characteristic zero, by the ring of p -adic integers \mathbf{Z}_p , for some prime p , the variety X by a variety $X_{\mathbf{Z}_p}$ which is defined over \mathbf{Z}_p , and the homomorphism ϱ by a homomorphism into $\text{Bir}(X_{\mathbf{Z}_p})$.

In a second step, we look for a polydisk $\mathcal{U} \simeq \mathbf{Z}_p^d$ in $X_{\mathbf{Z}_p}(\mathbf{Q}_p)$ which is invariant under the action of Γ in order to apply the Bell–Poonen extension theorem (Theorem 2.4) on \mathcal{U} . This is easy when $\varrho(\Gamma)$ is contained in $\text{Aut}(X)$, but much harder when Γ acts by birational transformations; §7 addresses this problem.

3.1. From complex to p -adic coefficients: good models

Let \mathbf{k} be an algebraically closed field of characteristic zero. Let $X = X_{\mathbf{k}}$ be a quasi-projective variety defined over \mathbf{k} , for instance $X = \mathbb{A}^d$, the affine space. Let Γ be a subgroup of $\text{Bir}(X_{\mathbf{k}})$ with a finite, symmetric set of generators $S = \{\gamma_1, \dots, \gamma_s\}$.

3.1.1. From complex to p -adic coefficients

Fix an embedding of X into a projective space $\mathbb{P}_{\mathbf{k}}^N$ and write

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

where \mathfrak{a} and \mathfrak{b} are two homogeneous ideals in $\mathbf{k}[\mathbf{x}_0, \dots, \mathbf{x}_N]$ and $\mathcal{Z}(\mathfrak{a})$ denotes the zero-set of the ideal \mathfrak{a} . Choose generators $(F_i)_{i=1}^a$ and $(G_j)_{j=1}^b$ for \mathfrak{a} and \mathfrak{b} , respectively.

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 polynomial formulas defining the generators $\gamma_k \in S$; more precisely, each γ_k is defined by ratios of regular functions on affine open subsets $\mathcal{V}_l = X \setminus W_l$, and one includes the coefficients of the formulas for these regular functions and for the defining equations of the Zariski closed subsets W_l . One can view X and Γ as defined over $\text{Spec}(C)$.

LEMMA 3.1. (See [48, §4 and §5] and [6, Lemma 3.1]) *Let L be a finitely generated extension of \mathbf{Q} and B be a finite subset of L . The set of primes p for which there exists an embedding of L into \mathbf{Q}_p that maps B into \mathbf{Z}_p has positive density among the set of all primes.*

By *positive density*, we mean that there exist $\varepsilon > 0$ and $N_0 > 0$ such that, among the first N primes, the proportion of primes p that satisfy the statement is bounded from below by ε if $N \geq N_0$.

Apply this lemma to the fraction field $L = \text{Frac}(C)$ and the set B of coefficients. This provides an odd prime p and an embedding $\iota: L \rightarrow \mathbf{Q}_p$ with $\iota(B) \subset \mathbf{Z}_p$. Applying ι to the coefficients of the formulas that define X and the elements of Γ , we obtain what will be called a “model of the pair (X, Γ) over \mathbf{Z}_p ”; in particular, Γ embeds into $\text{Bir}(X_{\mathbf{Z}_p})$, or in $\text{Aut}(X_{\mathbf{Z}_p})$ if Γ is initially a subgroup of $\text{Aut}(X_{\mathbf{k}})$. The following paragraphs clarify this idea.

3.1.2. Good models

Let R be an integral domain. Let X_R and Y_R be separated and reduced schemes of finite type defined over R . Assume, moreover, that the morphism $X_R \rightarrow \text{Spec}(R)$ is dominant on every irreducible component of X_R . Let \mathcal{U} and \mathcal{V} be two dense open subsets of X_R . Two morphisms of R -schemes $f: \mathcal{U} \rightarrow Y_R$ and $g: \mathcal{V} \rightarrow Y_R$ are equivalent if they coincide on some dense open subset W of $\mathcal{U} \cap \mathcal{V}$; rational maps $f: X_R \dashrightarrow Y_R$ are equivalence classes for this relation ([38, §7.1]). For any rational map f , there is a maximal open subset $\text{Dom}(f) \subset X_R$ on which f induces a morphism: if a morphism $\mathcal{V} \rightarrow Y_R$ is in the equivalence

class of f , then \mathcal{V} is contained in $\text{Dom}(f)$. This open subset $\text{Dom}(f)$ is the domain of definition of f ([38, §7.2]); its complement is the indeterminacy locus $\text{Ind}(f)$.

A rational map f is birational if there is a rational map $g: Y_R \dashrightarrow X_R$ such that $g \circ f = \text{Id}$ and $f \circ g = \text{Id}$. The group of birational transformations $f: X_R \dashrightarrow X_R$ is denoted $\text{Bir}(X_R)$; the group of regular automorphisms is denoted $\text{Aut}(X_R)$. Consider a birational map $f: X \dashrightarrow Y$ and denote by g the inverse map f^{-1} . The domains of definition $\text{Dom}(f)$ and $\text{Dom}(g)$ are dense open subsets of X and Y , respectively, for the Zariski topology. Then, set $U_{R,f} = (f|_{\text{Dom}(f)})^{-1}(\text{Dom}(g))$. As f is birational, $U_{R,f}$ is open and dense in X . The restriction of f to this open subset is an open immersion of $U_{R,f}$ into Y ; indeed, $f(U_{R,f})$ is the open set $(g|_{\text{Dom}(g)})^{-1}(U_{R,f})$ and g is a morphism on $f(U_{R,f})$ such that $g \circ f = \text{Id}$. Moreover, $U_{R,f}$ is the largest open subset of X on which f is locally, for the Zariski topology, an open immersion. In what follows, we denote by $B_{R,f}$ the complement of $U_{R,f}$ in X_R : this nowhere dense Zariski closed subset is the set of *bad* points; on its complement, f is an open immersion.

For $y \in \text{Spec}(R)$, denote by X_y the reduced fiber of X_R above y . If $X_y \cap B_{R,f}$ is nowhere dense in X_y , then f induces a birational transformation $f_y: X_y \dashrightarrow X_y$; we have $\text{Ind}(f_y) \subset X_y \cap B_{R,f}$, and this inclusion may be strict.

If η is the generic point of $\text{Spec}(R)$, we can always restrict f to X_η . This map $f \mapsto f_\eta$ determines an isomorphism of groups $i: \text{Bir}(X_R) \rightarrow \text{Bir}(X_\eta)$. More precisely, the following holds: *let K be the fraction field of the integral domain R ; let X_R be a separated and reduced scheme over R ; assume that X_R is of finite type over R , and that the morphism $X_R \rightarrow \text{Spec}(R)$ is dominant on every irreducible component of X_R ; then, the map $i: \text{Bir}(X_R) \rightarrow \text{Bir}(X_K)$ is bijective.* Indeed, i is injective because X_R is of finite type over R and the map $X_R \rightarrow \text{Spec}(R)$ is dominant on every irreducible component of X_R . It is surjective, because f_η can be defined on a dense affine open subset

$$U = \text{Spec}(R[x_1, \dots, x_m]/I)$$

of X_R by polynomial functions G_i with coefficients in K . There is an element d of R such that the functions dG_i have coefficients in R ; then, f_η extends as a morphism on $\text{Spec}(R[1/d, x_1, \dots, x_m]/I)$. (See [18, §9.1] for details.)

Let \mathbf{k} be an algebraically closed field of characteristic zero. Let $X_{\mathbf{k}}$ be an irreducible variety which is defined over \mathbf{k} . Let Γ be a subgroup of $\text{Bir}(X_{\mathbf{k}})$ (resp. $\text{Aut}(X_{\mathbf{k}})$). Let R be a subring of \mathbf{k} . We say that the pair (X, Γ) is defined over R if there is a separated, reduced, irreducible scheme X_R over R for which the structure morphism $X_R \rightarrow \text{Spec}(R)$ is dominant, and an embedding $\Gamma \rightarrow \text{Bir}(X_R)$ (resp. in $\text{Aut}(X_R)$) such that both $X_{\mathbf{k}}$ and Γ are obtained from X_R by base change: $X_{\mathbf{k}} = X_R \times_{\text{Spec}(R)} \text{Spec}(\mathbf{k})$ and similarly for all elements $f \in \Gamma$.

Let p be a prime number. A *model* for the pair (X, Γ) over the ring \mathbf{Z}_p is given by the following data. First, a ring $R \subset \mathbf{k}$ on which X and Γ are defined, and an embedding $\iota: R \rightarrow \mathbf{Z}_p$. Then, an irreducible scheme $X_{\mathbf{Z}_p}$ over \mathbf{Z}_p and an embedding $\varrho: \Gamma \rightarrow \text{Bir}(X_{\mathbf{Z}_p})$ (resp. in $\text{Aut}(X_{\mathbf{Z}_p})$) such that

(i) $X_{\mathbf{Z}_p} \simeq X_R \times_{\text{Spec}(R)} \text{Spec}(\mathbf{Z}_p)$ is the base change of X_R and $\varrho(f)$ is the base change of $f \in \text{Bir}(X_R)$ for every f in Γ .

A *good model* for the pair (X, Γ) over the ring \mathbf{Z}_p is a model such that

(ii) the special fiber $X_{\mathbf{F}_p}$ of $X_{\mathbf{Z}_p} \rightarrow \text{Spec}(\mathbf{Z}_p)$ is absolutely reduced and irreducible and its dimension is

$$\dim_{\mathbf{F}_p}(X_{\mathbf{F}_p}) = \dim_{\mathbf{Q}_p}(X_{\mathbf{Z}_p} \times_{\text{Spec}(R)} \text{Spec}(\mathbf{Q}_p));$$

(iii) for all $f \in \Gamma$, the special fiber $X_{\mathbf{F}_p}$ is not contained in $B_{\mathbf{Z}_p, \varrho(f)}$.

If K is a finite extension of \mathbf{Q}_p and \mathcal{O}_K is its valuation ring, one can also introduce the notion of good models over \mathcal{O}_K . The following is proven in the appendix.

PROPOSITION 3.2. *Let X be an irreducible complex projective variety, and Γ be a finitely generated subgroup of $\text{Bir}(X)$ (resp. of $\text{Aut}(X)$). Then, there exist infinitely many primes $p \geq 3$ such that the pair (X, Γ) has a good model over \mathbf{Z}_p .*

3.2. From birational transformations to local analytic diffeomorphisms

3.2.1. Automorphisms and invariant polydisks

Now, for simplicity, assume that X is the affine space \mathbb{A}^d . Let p be an odd prime number, and let Γ be a subgroup of $\text{Aut}(\mathbb{A}_{\mathbf{Z}_p}^d)$; all elements of Γ are polynomial automorphisms of the affine space defined by formulas with coefficients in \mathbf{Z}_p . Reduction modulo p provides a homomorphism from Γ to the group $\text{Aut}(\mathbb{A}_{\mathbf{F}_p}^d)$: every automorphism $f \in \Gamma$ determines an automorphism \bar{f} of the affine space with coefficients in \mathbf{F}_p . One can also reduce modulo p^2, p^3, \dots

If R_0 is a finite ring, then $\mathbb{A}^d(R_0)$ and $\text{GL}_d(R_0)$ are both finite. Therefore, the automorphisms $f \in \Gamma$ with $f(m) \equiv m \pmod{p^2}$ and $df_m \equiv \text{Id} \pmod{p}$ 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

$$f(\mathbf{x}) = p^2 A_0 + (\text{Id} + p B_1)(\mathbf{x}) + \sum_{k \geq 2} A_k(\mathbf{x}),$$

where A_0 is a point with coordinates in \mathbf{Z}_p , B_1 is a $d \times d$ matrix with coefficients in \mathbf{Z}_p , and $\sum_{k \geq 2} A_k(\mathbf{x})$ is a finite sum of higher-degree homogeneous terms with coefficients in \mathbf{Z}_p . Rescaling, one gets

$$p^{-1} f(p\mathbf{x}) = p A_0 + (\text{Id} + p B_1)(\mathbf{x}) + \sum_{k \geq 2} p^{k-1} A_k(\mathbf{x}).$$

Thus, the Bell–Poonen extension theorem (Theorem 2.4) applies to $p^{-1}f(p\mathbf{x})$, because $p \geq 3$.

A similar argument applies to automorphism groups Γ of any quasi-projective variety X of dimension d . One first replaces \mathbf{Q}_p by a finite extension K to assure the existence of at least one point m in $X(R/\mathbf{m}_K)$ (with R the valuation ring of K). Then, the stabilizer of m modulo \mathbf{m}_K is a finite-index subgroup, because $X(R/\mathbf{m}_K)$ is a finite set; this group fixes a polydisk in $X(K)$ and the Bell–Poonen theorem can be applied to a smaller, finite-index subgroup. This provides the following statement, the proof of which is given in [7] (Propositions 4.4 and 2.2), when the group Γ is cyclic. Propositions 3.2 and 3.4 are inspired by [7] and also imply this statement.

PROPOSITION 3.3. (see [7]) *Let $X_{\mathbf{Z}_p}$ be a quasi-projective variety defined over \mathbf{Z}_p , and let Γ be a subgroup of $\text{Aut}(X_{\mathbf{Z}_p})$. Then, there exist a finite extension K of \mathbf{Q}_p , a finite-index subgroup Γ_0 of Γ , and an 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_0 -invariant and the action of Γ_0 on \mathcal{V} is conjugate, via φ , to a subgroup of $\text{Diff}^{\text{an}}(\mathcal{U})_1$.*

Combining this result with Proposition 3.2, we get: If a finitely generated group Γ admits a faithful action by automorphisms on some irreducible d -dimensional complex variety, there are a finite-index subgroup Γ_0 in Γ , a prime p , and a finite extension K of \mathbf{Q}_p such that Γ_0 admits a faithful action by Tate analytic diffeomorphisms on a polydisk $\mathcal{U} \subset K^d$. This will be used as a first step in the proofs of Theorems A and D.

3.2.2. Birational transformations and invariant polydisks

Let us now deal with invariant polydisks for groups of birational transformations. Let $X_{\mathbf{Z}_p}$ be a projective variety defined over \mathbf{Z}_p and let Γ be a subgroup of $\text{Bir}(X_{\mathbf{Z}_p})$ with a finite symmetric set of generators S . Let $X_{\mathbf{F}_p}$ be the special fiber of $X_{\mathbf{Z}_p}$. We assume that the special fiber is not contained in $B_{\mathbf{Z}_p, s}$ for any $s \in S$; this implies that $X_{\mathbf{F}_p}$ is not contained in $B_{\mathbf{Z}_p, g}$ for every $g \in \Gamma$. By restriction, we obtain a homomorphism $\Gamma \rightarrow \text{Bir}(X_{\mathbf{F}_p})$. These assumptions are satisfied by good models.

Let K be a finite extension of \mathbf{Q}_p , O_K be the valuation ring of K , and \mathbf{F} be the residue field of O_K ; by definition, $\mathbf{F} = O_K/\mathbf{m}_K$, 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

$$X_{O_K} = X_{\mathbf{Z}_p} \times_{\text{Spec}(\mathbf{Z}_p)} \text{Spec}(O_K).$$

The generic fiber

$$X_{\mathbf{Z}_p} \times_{\text{Spec}(\mathbf{Z}_p)} \text{Spec}(K)$$

is denoted by X_K , and the special fiber is

$$X_{\mathbf{F}} = X_{\mathbf{Z}_p} \times_{\text{Spec}(\mathbf{Z}_p)} \text{Spec}(\mathbf{F}).$$

Denote by $r: X_K(K) \rightarrow X_{\mathbf{F}}(\mathbf{F}) = X(\mathbf{F})$ the reduction map. Let x be a smooth point in $X(\mathbf{F})$ and \mathcal{V} be the open subset of $X_K(K)$ consisting of points z satisfying $r(z) = x$.

PROPOSITION 3.4. (See also [7, Proposition 2.2]) *There exists an analytic diffeomorphism φ from the unit polydisk $\mathcal{U} = O_K^d$ to the open subset \mathcal{V} of $X_K(K)$ such that, for every $f \in \text{Bir}(X_{O_K})$ 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 a Tate analytic diffeomorphism on \mathcal{U} . Thus, if $\Gamma \subset \text{Bir}(X_{\mathbf{Z}_p})$ satisfies*

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

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

Thus, once a good model has been constructed, the existence of an invariant polydisk on which the action is analytic is equivalent to the existence of a smooth fixed point $x \in X_{\mathbf{F}}(\mathbf{F})$ 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. This will be used to prove Theorems B and C.

We shall prove this proposition in the appendix. Note that Propositions 3.4 and 3.2, together with rescaling argument of §3.2.1, provide a proof of Proposition 3.3.

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

In this section, we prove the first assertion of Theorem A together with one of its corollaries. Thus, our goal is the following statement.

THEOREM 4.1. *Let $n \geq 2$ be an integer. Let Γ be a finite-index subgroup of $\text{SL}_n(\mathbf{Z})$. 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 $\dim(X) \geq n$.*

4.1. Dimension 1

When $\dim_{\mathbf{C}}(X) = 1$, the group of automorphisms of X is isomorphic to $\text{PGL}_2(\mathbf{C})$, if X is the projective line, and is virtually solvable, otherwise. On the other hand, every finite-index subgroup of $\text{SL}_n(\mathbf{Z})$ contains a non-abelian free group if $n \geq 2$ (see [39, Chapter 1]). Theorems A and 4.1 follow from these remarks when $n = 2$ or $\dim(X) = 1$. In what follows, we assume $\dim_{\mathbf{C}}(X) \geq 2$ and $n \geq 3$.

4.2. Congruence subgroups of $\mathbf{SL}_n(\mathbf{Z})$; see [2], [62]

4.2.1. Normal subgroups

Let Γ be a finite-index subgroup of $\mathbf{SL}_n(\mathbf{Z})$. For $n \geq 3$, the group Γ is a lattice in the higher-rank almost simple Lie group $\mathbf{SL}_n(\mathbf{R})$. For such a lattice, every normal subgroup is either finite and central, or cofinite. In particular, the derived subgroup $[\Gamma, \Gamma]$ has finite index in Γ .

4.2.2. Strong approximation

For any $n \geq 2$ and $m \geq 1$, denote by Γ_m and Γ_m^* the following subgroups of $\mathbf{SL}_n(\mathbf{Z})$:

$$\Gamma_m = \{B \in \mathbf{SL}_n(\mathbf{Z}) : B \equiv \text{Id} \pmod{m}\},$$

$$\Gamma_m^* = \{B \in \mathbf{SL}_n(\mathbf{Z}) : \text{there exists } a \in \mathbf{Z} \text{ such that } B \equiv a \text{Id} \pmod{m}\}.$$

By definition, Γ_m is the *principal congruence subgroup of level m* .

Let p be a prime number. The closure of Γ_m in $\mathbf{SL}_n(\mathbf{Z}_p)$ is the finite-index, open subgroup of matrices which are equal to Id modulo m ; thus, if $m = p^u r$ with $r \wedge p = 1$, the closure of Γ_m in $\mathbf{SL}_n(\mathbf{Q}_p)$ coincides with the open subgroup of matrices $M \in \mathbf{SL}_n(\mathbf{Z}_p)$ which are equal to Id modulo p^u .

The strong approximation theorem states that the image of $\mathbf{SL}_n(\mathbf{Z})$ is dense in the product $\prod_p \mathbf{SL}_n(\mathbf{Z}_p)$ (product over all prime numbers). If Γ has finite index in $\mathbf{SL}_n(\mathbf{Z})$, its closure in $\prod_p \mathbf{SL}_n(\mathbf{Z}_p)$ is a finite-index subgroup; it contains almost all $\mathbf{SL}_n(\mathbf{Z}_p)$.

4.2.3. Congruence subgroup property

A deep property that we shall use is the congruence subgroup property, which holds for $n \geq 3$. It asserts that every finite-index subgroup Γ of $\mathbf{SL}_n(\mathbf{Z})$ contains a principal congruence subgroup Γ_m ; if Γ is normal, there exists a unique integer m with $\Gamma_m \subset \Gamma \subset \Gamma_m^*$. We shall come back to this property in §8.1 for more general algebraic groups (the congruence subgroup property is not known in full generality for cocompact lattices).

Another way to state the congruence subgroup and strong approximation properties is to say that the profinite completion of $\mathbf{SL}_n(\mathbf{Z})$ coincides with the product $\prod_p \mathbf{SL}_n(\mathbf{Z}_p)$. If Γ has finite index in $\mathbf{SL}_n(\mathbf{Z})$, its profinite completion is a product $\prod_q G_q \subset \prod_q \mathbf{SL}_n(\mathbf{Z}_q)$, where each G_q has finite index in $\mathbf{SL}_n(\mathbf{Z}_q)$, and $G_q = \mathbf{SL}_n(\mathbf{Z}_q)$ for almost all primes q .

Remark 4.2. Fix $n \geq 3$. For every prime number q , the group $\mathbf{SL}_n(\mathbf{Z}_q)$ is a perfect group, because it is generated by the elementary matrices $e_{ij}(r)$, $r \in \mathbf{Z}_q$, and every elementary matrix is a commutator. Thus, every homomorphism from $\mathbf{SL}_n(\mathbf{Z}_q)$ to a p -group

is trivial, because every p -group is nilpotent. Thus, the pro- p completion of $\mathrm{SL}_n(\mathbf{Z}_q)$ is trivial.

Before stating the following lemma, recall that the concept of virtual pro- p completion is introduced in §2.4.2.

LEMMA 4.3. *Let n be an integer ≥ 3 . Let Γ be a finite-index subgroup of $\mathrm{SL}_n(\mathbf{Z})$. Let Γ_m be a principal congruence subgroup contained in Γ . If p divides the integer m , the pro- p completion of Γ_m coincides with its closure in $\mathrm{SL}_n(\mathbf{Z}_p)$. Therefore, $\mathrm{SL}_n(\mathbf{Z}_p)$ is a virtual pro- p completion of its subgroup Γ .*

Proof. Fix a positive integer m such that Γ contains Γ_m and p divides m . The profinite completion of Γ_m coincides with the product $\prod_q G_q$, where G_q is the closure of Γ_m in $\mathrm{SL}_n(\mathbf{Z}_q)$. If $m=p^u r$ with $p \wedge r=1$, then G_p is the open, pro- p subgroup of $\mathrm{SL}_n(\mathbf{Z}_p)$ defined by $G_p=\{B \in \mathrm{SL}_n(\mathbf{Z}_p) : B \equiv \mathrm{Id} \pmod{p^u}\}$. If q does not divide m , G_q is equal to $\mathrm{SL}_n(\mathbf{Z}_q)$. If $q \neq p$ and q divides m , then the group G_q is an open subgroup of the pro- q group $\{B \in \mathrm{SL}_n(\mathbf{Z}_q) : B \equiv \mathrm{Id} \pmod{q}\}$. Thus, if $q \neq p$, then the pro- p completion of G_q is trivial; and the pro- p completion of Γ_m coincides with its closure G_p in $\mathrm{SL}_n(\mathbf{Z}_p)$. \square

4.3. 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 $\mathrm{Jac}(f)(\mathbf{x})=\det(df_{\mathbf{x}})$, where $df_{\mathbf{x}}$ denotes the differential of f at \mathbf{x} . One says that the jacobian determinant of f is identically equal to 1 if $\mathrm{Jac}(f)$ is the constant function 1. In the following theorem, p is an odd prime, and K and R are as in §2.1.1.

THEOREM 4.4. *Let $n \geq 3$ be an integer. Let Γ be a finite-index subgroup of $\mathrm{SL}_n(\mathbf{Z})$. Let \mathcal{U} be the unit polydisk R^d , for some $d \geq 1$. Let $\Phi: \Gamma \rightarrow \mathrm{Diff}^{\mathrm{an}}(\mathcal{U})$ be a homomorphism such that $f(\mathbf{x}) \equiv \mathbf{x} \pmod{p}$ 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 4.5. All proper subalgebras of $\mathfrak{sl}_n(\mathbf{Q}_p)$ have codimension $\geq n-1$, and there are two conjugacy classes of algebraic subgroups of codimension $n-1$ in $\mathrm{SL}_{n, \mathbf{Q}_p}$ for $n \geq 3$. The stabilizer of a point in the projective space $\mathbb{P}^{n-1}(\mathbf{Q}_p)$, and the stabilizer of a hyperplane in that space (see [9, Chapter 5] and §8.2 below). These conjugacy classes are exchanged by the outer automorphism $\theta: A \mapsto {}^t A^{-1}$. When $n=2$, θ is an inner automorphism and there is only one conjugacy class.

Proof. According to Lemma 4.3 and Theorem 2.11, $\mathrm{SL}_n(\mathbf{Z}_p)$ is a virtual pro- p completion of Γ , and there is a principal congruence subgroup $\Gamma_m \subset \Gamma$ such that Φ extends as an analytic homomorphism $\bar{\Phi}: G \rightarrow \mathrm{Diff}^{\mathrm{an}}(\mathcal{U})_1$ from the group Γ_m to its pro- p completion $G = \bar{\Gamma}_m \subset \mathrm{SL}_n(\mathbf{Z}_p)$. The differential $d\bar{\Phi}_{\mathrm{Id}}$ provides a homomorphism of Lie algebras

$$d\bar{\Phi}_{\mathrm{Id}}: \mathfrak{sl}_n(\mathbf{Q}_p) \longrightarrow \Theta(\mathcal{U}),$$

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 §4.2); hence, there are infinite-order elements in $\Phi(\Gamma)$. The vector field corresponding to such an element does not vanish identically; thus, $d\bar{\Phi}_{\mathrm{Id}}$ is a non-trivial homomorphism. Since $\mathfrak{sl}_n(\mathbf{Q}_p)$ is a simple Lie algebra, $d\bar{\Phi}_{\mathrm{Id}}$ is an embedding. Pick w in $\mathfrak{sl}_n(\mathbf{Q}_p) \setminus \{0\}$. Since $d\bar{\Phi}_{\mathrm{Id}}$ is an embedding, there is a point o in \mathcal{U} such that $d\bar{\Phi}_{\mathrm{Id}}(w)(o) \neq 0$. The subset of elements $v \in \mathfrak{sl}_n(\mathbf{Q}_p)$ such that $d\bar{\Phi}_{\mathrm{Id}}(v)(o) = 0$ constitutes a proper subalgebra \mathfrak{p}_Φ of $\mathfrak{sl}_n(\mathbf{Q}_p)$ of codimension at most d . Thus, $d \geq n - 1$ by Remark 4.5.

Let us now assume that $d = n - 1$. Consider the parabolic subgroup P_0 of SL_n which is defined as the stabilizer of the point $m_0 = [1:0:0 \dots :0]$ in the projective space \mathbb{P}^{n-1} . Assume, first, that \mathfrak{p}_Φ coincides with the Lie algebra \mathfrak{p}_0 of P_0 . The quotient of \mathfrak{sl}_n by \mathfrak{p}_0 can be identified with 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 b/a 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 multiplications on the tangent space $T_o\mathcal{U}$; such elements have jacobian determinant $\neq 1$. Since Γ is dense in G , and both Φ and Jac are continuous, there are elements f in Γ with $\mathrm{Jac}(f) \neq 1$. This concludes the proof of the theorem when $\mathfrak{p}_\Phi = \mathfrak{p}_0$, or more generally when \mathfrak{p}_Φ is conjugate to \mathfrak{p}_0 . If \mathfrak{p}_Φ is not conjugate to \mathfrak{p}_0 , we replace Φ by $\Phi \circ \theta$ and apply Remark 4.5 to conclude (note that the outer automorphism θ preserves Γ_m and induces an analytic automorphism of G). □

4.4. Embeddings of $\mathrm{SL}_n(\mathbf{Z})$ in $\mathrm{Aut}(X)$ or $\mathrm{Aut}(\mathbb{A}_C^d)$

We may now prove Theorem 4.1. According to §4.1, we assume $n \geq 3$. Let d be the dimension of X and $\Psi: \Gamma \rightarrow \mathrm{Aut}(X)$ be a homomorphism with infinite image.

According to §3.1 and Proposition 3.3, one can find a prime $p \geq 3$, a model of (X, Γ) over a finite extension K of \mathbf{Q}_p , a finite-index subgroup Γ' of Γ , and a polydisk $\mathcal{U} \simeq R^d$ in $X(K)$ such that \mathcal{U} is invariant under the action of Γ' and the action of Γ' on \mathcal{U} is given by a homomorphism $\Phi: \Gamma' \rightarrow \mathrm{Diff}^{\mathrm{an}}(\mathcal{U})_1$. Theorem 4.4 implies $\dim(X) \geq n - 1$.

Assume now that X is the affine space $\mathbb{A}_{\mathbb{C}}^d$. If f is an automorphism of $\mathbb{A}_{\mathbb{C}}^d$, its jacobian determinant $\text{Jac}(f)$ is constant because $\text{Jac}(f)$ is a polynomial function on $\mathbb{A}^d(\mathbb{C})$ that does not vanish. Thus, $\text{Jac}(\cdot)$ provides a homomorphism from Γ to (\mathbb{C}^*, \cdot) ; since the derived group $[\Gamma, \Gamma]$ has finite index in Γ (see §4.2.1), one may assume that $\text{Jac}(\Phi(\gamma))=1$ for all $\gamma \in \Gamma'$. Then, Theorem 4.4 implies that $d \geq n$.

5. Actions of $\text{SL}_n(\mathbb{Z})$ in dimension $n-1$

In this paragraph, we pursue the study of algebraic actions of finite-index subgroups of $\text{SL}_n(\mathbb{Z})$ 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 §4, but with two differences: we study both regular and birational actions, and we add a constraint on the dimension of X , which corresponds to the limit case in the inequality $d \geq n-1$ of Theorem 4.1. Thus,

- (i) Γ is a finite-index subgroup of $\text{SL}_n(\mathbb{Z})$;
- (ii) $X_{\mathbb{C}}$ is a complex, irreducible, quasi-projective variety of dimension $d=n-1$;
- (iii) Γ embeds into $\text{Aut}(X_{\mathbb{C}})$ (resp. in $\text{Bir}(X_{\mathbb{C}})$);
- (iv) there is a finite extension K of \mathbb{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 3.3: this gives a homomorphism $\Phi: \Gamma \rightarrow \text{Diff}^{\text{an}}(\mathcal{U})_1$.

THEOREM 5.1. *Under the above four hypotheses (i)–(iv), there exists an isomorphism $\tau: X \rightarrow \mathbb{P}_{\mathbb{C}}^d$ (resp. a birational map $\tau: X \dashrightarrow \mathbb{P}_{\mathbb{C}}^d$), from X to the projective space of dimension $d=n-1$ and a homomorphism $\varrho: \Gamma \rightarrow \text{PGL}_n(\mathbb{C})$ such that $\tau \circ \gamma = \varrho(\gamma) \circ \tau$ for every γ in Γ .*

Theorem A follows from Theorem 4.1, Proposition 3.3, and Theorem 5.1.

Remark 5.2. When Γ acts by birational transformations on X , the existence of 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) may look as a strong hypothesis. We shall obtain such polydisks in §7.3

5.1. Extension

We apply Lemma 4.3 and Theorem 2.11 to the analytic action of Γ on \mathcal{U} . Thus, there exists a principal congruence subgroup $\Gamma_m \subset \Gamma$ such that the homomorphism Φ from Γ_m

to $\text{Diff}^{\text{an}}(\mathcal{U})_1$ extends as an analytic homomorphism $\bar{\Phi}$ from the p -adic analytic group $G = \bar{\Gamma}_m \subset \text{SL}_n(\mathbf{Z}_p)$ to $\text{Diff}^{\text{an}}(\mathcal{U})_1$.

5.2. Stabilizer of the origin in \mathcal{U}

Let P_0 be the subgroup of $\text{SL}_n(\mathbf{Q}_p)$ which fixes the point $m_0 = [1:0:\dots:0]$ in the projective space $\mathbb{P}^{n-1}(\mathbf{Q}_p)$; it is a maximal parabolic subgroup of $\text{SL}_n(\mathbf{Q}_p)$. We denote by \mathfrak{p}_0 its Lie algebra, as in the proof of Theorem 4.4.

LEMMA 5.3. *There are an element A in $\text{SL}_n(\mathbf{Z})$ and a point o' in \mathcal{U} with the following property. For the homomorphism $\bar{\Phi} \circ c_A: G \rightarrow \text{Diff}^{\text{an}}(\mathcal{U})_1$, where c_A is either the conjugacy $c_A(M) = AMA^{-1}$, or its composition with the outer automorphism $\theta: M \mapsto {}^tM^{-1}$, the stabilizer $P' \subset G$ of the point o' coincides with $P_0 \cap G$.*

Let $P \subset G$ be the stabilizer of the origin $o \in \mathcal{U}$. Since $d = n - 1$, the Lie algebra \mathfrak{p} of P has codimension $n - 1$ in $\mathfrak{g} = \mathfrak{sl}_n(\mathbf{Q}_p)$, and is therefore maximal. Let \tilde{P} be the Zariski closure of P in $\text{SL}_n(\mathbf{Q}_p)$. Then, $\tilde{P} \cap G$ coincides with P , and \tilde{P} is conjugate to P_0 or to $\theta(P_0)$ in $\text{SL}_n(\mathbf{Q}_p)$ (see Remark 4.5). For simplicity, we assume that \tilde{P} is conjugate to P_0 ; if \tilde{P} is conjugate to $\theta(P_0)$, one only needs to replace the action of $\text{SL}_n(\mathbf{Q}_p)$ on the projective space by the dual action on the space of hyperplanes in $\mathbb{P}^{n-1}(\mathbf{Q}_p)$, or to compose $\bar{\Phi}$ with θ .

To prove the lemma, we make 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 $\text{SL}_n(\mathbf{Q}_p)$. One can write $[a] = [a_1 : \dots : a_n]$ with a_i in \mathbf{Z}_p for all $1 \leq i \leq n$ 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 $\text{SL}_n(\mathbf{Z}_p)$ defined as the group of matrices M with $M \equiv \text{Id} \pmod{m}$; if one picks an element $[a'] = [a'_1 : \dots : a'_n]$ of $\mathbb{P}^{n-1}(\mathbf{Z})$ with entries $a'_i \equiv a_i$ modulo a large power of m , 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 $\text{SL}_n(\mathbf{Z})$ such that $A[a'] = [1:0:\dots:0]$. Composing Φ with the conjugation c_A , the stabilizer of o' is now equal to $P_0 \cap G$.

(4) Being a principal congruence subgroup, Γ_m is normal in $\text{SL}_n(\mathbf{Z})$; it is therefore invariant under the conjugacy $c_A: M \mapsto AMA^{-1}$ (and under the automorphism θ). Thus, the homomorphism $\Phi \circ c_A$ (resp. $\bar{\Phi} \circ c_A$) determines a new homomorphism from Γ_m

(resp. G) to $\text{Diff}^{\text{an}}(\mathcal{U})_1$ which preserves the polydisk \mathcal{U} and for which the stabilizer of o' coincides with $P_0 \cap \Gamma_m$ (resp. with $P_0 \cap G$).

Let us now apply Lemma 5.3 to rigidify slightly the situation. We conjugate the action of Γ_m on \mathcal{U} by the translation $x \mapsto x + o'$; then we compose the embedding of Γ_m in $\text{Aut}(X)$ by the automorphism c_A of Γ_m given by Lemma 5.3 to assume that *the stabilizer of the origin in G is the intersection of G with the parabolic subgroup P_0* . Thus, the embedding $\Gamma_m \rightarrow \text{Aut}(X)$ and the coordinates of \mathcal{U} have been modified.

5.3. Local normal form

Consider the subgroup T of G consisting of all matrices

$$\begin{pmatrix} 1 & 0 \\ \mathbf{t} & \text{Id}_{n-1} \end{pmatrix},$$

where Id_{n-1} 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, \dots, t_n in \mathbf{Z}_p that are equal to zero modulo m . By construction, T is contained in $G = \bar{\Gamma}_m$. The intersection $T \cap P_0$ is the trivial subgroup $\{\text{Id}_n\}$.

The group T is an abelian subgroup of G of dimension $d = n - 1$ that acts locally freely near the origin of \mathcal{U} (if not, this would contradict the maximality of P_0). There are local coordinates $\mathbf{z} = (z_2, \dots, z_n)$ on \mathcal{U} near the origin o such that T acts by

$$\Phi(\mathbf{t})(\mathbf{z}) = (z_2 + t_2, \dots, z_n + t_n);$$

in these coordinates, the action of the group G is locally conjugate to the linear projective action of G around the point $m_0 = [1:0:\dots:0]$ in $\mathbb{P}^{n-1}(K)$ (see the proof of Theorem 4.4). Note that the local coordinate z_i may be transcendental; it is not obvious, a priori, that z_i extends as an algebraic (or rational) function on the quasi-projective variety X . We shall prove that this is indeed the case in the next subsection (see Lemma 5.5).

5.4. Invariant (algebraic) functions

Our goal, in this subsection, is to prove Lemma 5.5. Consider the 1-parameter unipotent subgroup E_{12} of P whose elements have the form

$$e_{12}(s) = \begin{pmatrix} 1 & \mathbf{s} \\ 0 & \text{Id}_{n-1} \end{pmatrix},$$

with $\mathbf{s} = (s, 0, \dots, 0)$, s in \mathbf{Z}_p , and $s \equiv 0$ modulo m . Let $\alpha_{12} = e_{12}(s)$, $s \in \mathbf{Z} \setminus \{0\}$, be a non-trivial element of $E_{12} \cap \Gamma_m$. By construction, the analytic diffeomorphism $\Phi(\alpha_{12})$ of \mathcal{U}

transforms the local coordinate z_2 into $z_2/(1+sz_2)$, and the set $\{z_2=0\}$ is, locally, the set of fixed points of $\Phi(\alpha_{12})$. Since $\Phi(\alpha_{12})$ is the restriction to \mathcal{U} of a birational transformation of X , the hypersurface $\{z_2=0\}$ is the intersection of an algebraic hypersurface of X with a neighborhood of zero in \mathcal{U} .

Let $\alpha_{21}=e_{21}(t)$ be a non-trivial element of $T \cap \Gamma_m$ corresponding to the vector $\mathbf{t}=(t, 0, \dots, 0)$ (with $t \neq 0$ and $t \equiv 0$ modulo m). Then $\Phi(\alpha_{21})^\ell$ acts on \mathcal{U} and transports the hypersurface $\{z_2=0\}$ to the hypersurface $\{z_2=t\ell\}$. Since $\{z_2=0\}$ is algebraic and $\Phi(\alpha_{21})$ is in $\text{Aut}(X)$ (resp. in $\text{Bir}(X)$ when the action is by birational transformations), the hypersurfaces $\{z_2=t\ell\}$ are all algebraic.

Denote by T_2 the subgroup of T whose elements are defined by vectors of type $\mathbf{t}=(0, t_3, \dots, t_n)$. The action of $\bar{\Phi}(T_2)$ on \mathcal{U} preserves the local coordinate z_2 and is locally free on each level set $\{z_2=c^{st}\}$. Thus, every non-trivial element of $T_2 \cap \Gamma_m$ fixes infinitely many algebraic hypersurfaces in X , whose local equations are $z_2=\ell t$, $\ell \in \mathbf{Z}$; moreover, the orbits of $T_2 \cap \Gamma$ are Zariski dense in these hypersurfaces.

LEMMA 5.4. *Let X be an irreducible quasi-projective variety, defined over an algebraically closed field \bar{K} of characteristic zero. Let A be a group of birational transformations of X . If A preserves infinitely many hypersurfaces of X , then A preserves a non-constant rational function $\varphi \in \bar{K}(X)$, meaning that $\varphi \circ a = \varphi$ for every $a \in A$.*

This lemma corresponds to Theorem B of [12]: Theorem B is stated for a single transformation g but applies to groups of birational transformations, as one easily checks. Let us apply it to the group T_2 . From the Stein factorization theorem, we may assume that the general fibers of the function $\tau_2 := \varphi$ are irreducible hypersurfaces of X . Since the action of T_2 on the hypersurfaces $\{z_2=t\ell\}$ is locally free, these hypersurfaces coincide locally with the fibers of τ_2 . Thus, there is a complete curve $Y_{\bar{K}}$ and a rational function $\tau_2: X_{\bar{K}} \dashrightarrow Y_{\bar{K}}$, 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 $\beta \in T_2 \cap \Gamma$;
- the general hypersurface $\{\tau_2=c^{st}\}$ is irreducible;
- the local analytic coordinate z_2 is, locally, a function of τ_2 : there is an analytic 1-variable function ϕ_2 such that $z_2 = \phi_2 \circ \tau_2$ on \mathcal{U} .

The transformation $\Phi(\alpha_{12})$ transforms z_2 into $z_2/(1+sz_2)$ for some $s \neq 0$. Thus, it permutes the level sets of the algebraic function τ_2 . We deduce that the birational transformation α_{12} of X induces an infinite order automorphism of $Y_{\bar{K}}$ fixing the point $\tau_2(\{z_2=0\})$. This implies that $Y_{\bar{K}}$ is a projective line: there is an isomorphism from $Y_{\bar{K}}$ to $\mathbb{P}_{\bar{K}}^1$ that maps the point $\tau_2(\{z_2=0\})$ to the point $[0:1]$. We now fix an affine coordinate z on $\mathbb{P}_{\bar{K}}^1$ for which this point is $z=0$.

The iterates $\Phi(\alpha_{12})^\ell$ of $\Phi(\alpha_{12})$ transform the coordinate z_2 into $z_2/(1+\ell s z_2)$. Thus, if

$\ell=p^n$, one sees that the sequences of hypersurfaces $\Phi(\alpha_{12}^{+\ell})(\{z_2=c\})$ and $\Phi(\alpha_{12}^{-\ell})(\{z_2=c\})$ converge to the fixed hypersurface $\{z_2=0\}$ as n goes to ∞ , for every $c \in K$ with small absolute value. This implies that the automorphism of $\mathbb{P}_{\overline{K}}^1$ induced by α_{12} is a parabolic transformation, acting by

$$z \mapsto \frac{z}{1+s'z} \tag{5.1}$$

for some s' . Changing the affine coordinate z of $\mathbb{P}_{\overline{K}}^1$ into εz with $\varepsilon=s'/s$ (hence the function τ_2 into $\varepsilon\tau_2$ and $\phi_2(x)$ into $\phi_2(x/\varepsilon)$), one may assume that $s'=s$. Then, both τ_2 and z_2 satisfy the same transformation rule under $\Phi(\alpha_{12})$:

$$\tau_2 \circ \Phi(\alpha_{12}) = \frac{\tau_2}{1+s\tau_2} \quad \text{and} \quad z_2 \circ \Phi(\alpha_{12}) = \frac{z_2}{1+sz_2}. \tag{5.2}$$

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

$$\phi_2\left(\frac{z}{1+\ell sz}\right) = \frac{\phi_2(z)}{1+\ell s\phi_2(z)} \quad \text{for all } \ell \in \mathbf{Z}. \tag{5.3}$$

By construction, ϕ_2 is analytic (in a neighborhood of zero) and maps zero to zero. Changing $\phi_2(z)$ into $\phi_2(z/(1+uz))$ for a well-chosen $u \neq 0$, one may assume that $\phi_2(x_0)=x_0$ for some $x_0 \neq 0$. If one applies the functional equation (5.3) with $\ell \equiv 0$ modulo sufficiently large powers of p , then the sequence $x_\ell = x_0/(1+\ell s x_0)$ 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: $\phi_2(z) = z$. In particular, the local coordinate z_2 extends to a global rational function τ_2 on X .

If one applies the same strategy for $i=2, 3, \dots, n$, one gets $d=n-1$ rational functions τ_i on X . These functions are local coordinates near the origin of \mathcal{U} . And, from §5.3, we know that these coordinates provide a local conjugacy from the action of G on \mathcal{U} to the linear projective action of G near $[1:0:\dots:0]$ in $\mathbb{P}_{\overline{K}}^{n-1}$. This concludes the proof of the following lemma.

LEMMA 5.5. *Each local analytic function $z_i, i=2, \dots, n$, extends to a global rational function $\tau_i \dashrightarrow X_{\overline{K}} \rightarrow \overline{K}$. Altogether, they define a rational map*

$$\begin{aligned} \tau: X_{\overline{K}} &\dashrightarrow \mathbb{P}_{\overline{K}}^{n-1}, \\ x &\mapsto [1 : \tau_2(x) : \dots : \tau_n(x)]. \end{aligned}$$

This rational map τ is dominant. It is equivariant with respect to the action of Γ_m on X and the action of $\Gamma_m \subset \text{SL}_n(\mathbf{Z})$ on $\mathbb{P}_{\overline{K}}^{n-1}$ by linear projective transformations.

5.5. Conclusion, in the case of regular actions

We now assume that Γ acts by automorphisms on the quasi-projective variety X ; the case of birational transformations is dealt with in the next subsection.

LEMMA 5.6. *Let $\tau: X_{\bar{K}} \dashrightarrow \mathbb{P}_{\bar{K}}^{n-1}$ be a rational map which is equivariant with respect to an action of Γ_m on $X_{\bar{K}}$ by automorphisms and the linear projective action of $\Gamma_m \subset \mathrm{SL}_n(K)$ on $\mathbb{P}_{\bar{K}}^{n-1}$. Then, $X_{\bar{K}}$ is a projective variety, and the Γ_m -equivariant rational map τ is an isomorphism.*

Proof. Assume that $X_{\bar{K}}$ is normal and fix a compactification $\bar{X}_{\bar{K}}$ of $X_{\bar{K}}$. Via its embedding into $\mathrm{Aut}(X_K)$, the group Γ_m acts by automorphisms on $X_{\bar{K}}$ and by birational transformations on $\bar{X}_{\bar{K}}$.

The image of Γ_m in $\mathrm{PGL}_n(\bar{K}) = \mathrm{Aut}(\mathbb{P}_{\bar{K}}^{n-1})$ is a Zariski-dense subgroup Γ'_m (this is a simple instance of the Borel density theorem).

Let $\mathrm{Ind}(\tau)$ be the indeterminacy set of τ . Its intersection with $X_{\bar{K}}$ is a Γ_m -invariant algebraic subset, because Γ_m acts by automorphisms on both X and $\mathbb{P}_{\bar{K}}^{n-1}$. Its total transform under τ is a Γ'_m -invariant locally closed subset of $\mathbb{P}_{\bar{K}}^{n-1}$. But all such subsets are either empty or equal to $\mathbb{P}_{\bar{K}}^{n-1}$, because Γ'_m is Zariski-dense in $\mathrm{PGL}_n(\bar{K})$. Thus, $\mathrm{Ind}(\tau)$ does not intersect $X_{\bar{K}}$.

The image of $X_{\bar{K}}$ by τ is a constructible Γ'_m -invariant subset of $\mathbb{P}_{\bar{K}}^{n-1}$; as such, it must be equal to $\mathbb{P}_{\bar{K}}^{n-1}$, because Γ'_m is Zariski-dense in $\mathrm{PGL}_n(\bar{K})$. Similarly, the total transform of the boundary $\bar{X}_{\bar{K}} \setminus X_{\bar{K}}$ is empty. Thus, $X_{\bar{K}}$ is complete, and τ determines a morphism from $X_{\bar{K}}$ to $\mathbb{P}_{\bar{K}}^{n-1}$. The critical locus of τ is a Γ'_m -invariant subset of $\mathbb{P}_{\bar{K}}^{n-1}$ of positive codimension: it is therefore empty, and τ is an isomorphism because $\mathbb{P}_{\bar{K}}^{n-1}$ is simply connected.

If $X_{\bar{K}}$ is not normal, replace it by its normalization $\tilde{X}_{\bar{K}}$, and lift the action of Γ_m on $X_{\bar{K}}$ to an action by automorphisms on $\tilde{X}_{\bar{K}}$. We deduce that $\tilde{X}_{\bar{K}}$ is isomorphic to the projective space and the action of Γ_m on $\tilde{X}_{\bar{K}}$ does not preserve any non-empty Zariski closed subset; thus, the normalization $\tilde{X}_{\bar{K}} \rightarrow X_{\bar{K}}$ is an isomorphism. This proves the lemma. □

Apply this lemma to the rational map τ given by Lemma 5.5. Since $X_{\bar{K}}$ is isomorphic to the projective space $\mathbb{P}_{\bar{K}}^{n-1}$, the complex variety $X_{\mathbf{C}}$ is also isomorphic to $\mathbb{P}_{\mathbf{C}}^{n-1}$. Since the action of Γ on X is an action by automorphisms, it is given by an embedding of Γ into $\mathrm{PGL}_n(\mathbf{C})$. This concludes the proof of Theorem 5.1, and of Theorem A.

5.6. Conclusion, in the case of birational actions

Let us now assume that X is projective and Γ acts by birational transformations on X .

LEMMA 5.7. *The equivariant rational mapping $\tau: X_{\bar{K}} \dashrightarrow \mathbb{P}_{\bar{K}}^{n-1}$ is birational.*

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

elements γ of Γ_m satisfy

$$\tau \circ \gamma_X = \gamma_{\mathbb{P}^{n-1}} \circ \tau$$

where γ_X denotes the birational action of γ on $X_{\bar{K}}$ and $\gamma_{\mathbb{P}^{n-1}}$ corresponds to the linear projective action on $\mathbb{P}_{\bar{K}}^{n-1}$.

We may assume that X is normal. Embed X in some projective space \mathbb{P}^N , and consider the linear system of hyperplane sections H of X . Fix an element γ of Γ_m , and intersect X with $n-1$ hyperplanes to get an irreducible curve $C \subset X$ that does not intersect the indeterminacy set of γ . The image of C by γ_X is an irreducible curve $(\gamma_X)_*C$, which satisfies $\tau_*((\gamma_X)_*(C)) = (\gamma_{\mathbb{P}^{n-1}})_*\tau_*(C)$. The degree of the curve $(\gamma_{\mathbb{P}^{n-1}})_*\tau_*(C)$ is equal to the degree of $\tau_*(C)$, because $\gamma_{\mathbb{P}^{n-1}}$ is a regular automorphism of the projective space; in particular, it does not depend on γ . This implies that the degree of the curve $(\gamma_X)_*C$ in $X \subset \mathbb{P}^N$ is bounded by an integer $D(\tau)$ that does not depend on γ . As a consequence, the degrees of the formulas defining the elements γ_X of Γ_m in $\text{Bir}(X_{\bar{K}})$ are uniformly bounded. The following result shows that Γ_m is “regularizable” (see [66] and the references in [15]).

THEOREM 5.8. (Weil regularization theorem) *Let M be a projective variety, defined over an algebraically closed field. Let Λ be a subgroup of $\text{Bir}(M)$. If there is a uniform upper bound on the degrees of the elements of Λ , then there exist a birational map $\varepsilon: M \dashrightarrow M'$ and a finite-index subgroup Λ' of Λ such that $\varepsilon \circ \Lambda \circ \varepsilon^{-1}$ is a subgroup of $\text{Aut}(M)$ and $\varepsilon \circ \Lambda' \circ \varepsilon^{-1}$ is a subgroup of the connected component of the identity $\text{Aut}(M)^0$ in $\text{Aut}(M)$.*

In our context, this result shows that, after conjugacy by a birational map $\varepsilon: X \dashrightarrow X'$, Γ_m becomes a group of automorphisms of X' . Lemma 5.6 shows that the rational map $\tau \circ \varepsilon^{-1}: X'_{\bar{K}} \dashrightarrow \mathbb{P}_{\bar{K}}^{n-1}$ is an isomorphism which conjugates the action of Γ_m on $X'_{\bar{K}}$ to the linear projective action on $\mathbb{P}_{\bar{K}}^{n-1}$. In particular, τ is a birational map. \square

Thus, τ is a birational conjugacy between the action of Γ_m on X and the action of Γ_m by linear projective transformations on the projective space.

LEMMA 5.9. *The action of $\tau \circ \Gamma \circ \tau^{-1}$ on $\mathbb{P}_{\bar{K}}^{n-1}$ is an action by automorphisms.*

Proof. The group Γ_m is a normal, finite-index subgroup of Γ . Its image Γ'_m in $\text{PGL}_n(\bar{K})$ is Zariski dense. Let γ be an element of Γ , and let $\gamma_{\mathbb{P}^{n-1}}$ denote the birational transformation $\tau \circ \gamma_X \circ \tau^{-1}$; we have $\gamma_{\mathbb{P}^{n-1}} \Gamma'_m = \Gamma'_m \gamma_{\mathbb{P}^{n-1}}$. Since Γ'_m acts by automorphisms on $\mathbb{P}_{\bar{K}}^{n-1}$, it fixes the indeterminacy set of $\gamma_{\mathbb{P}^{n-1}}$, and this indeterminacy set must be empty, because Γ'_m is Zariski dense in $\text{PGL}_n(\bar{K})$. This shows that $\gamma_{\mathbb{P}^{n-1}}$ has no indeterminacy point and that $\tau \circ \Gamma \circ \tau^{-1} \subset \text{PGL}_n(\bar{K})$. \square

The existence of such a conjugacy $\tau: X_{\bar{K}} \dashrightarrow \mathbb{P}_{\bar{K}}^{n-1}$ implies also the existence of a

conjugacy $X_{\mathbf{C}} \dashrightarrow \mathbb{P}_{\mathbf{C}}^{n-1}$ over the field of complex numbers. This concludes the proof of Theorem 5.1.

6. Mapping class groups and nilpotent groups

To describe another application of the p -adic method, we study the actions by automorphisms of the mapping class groups $\text{Mod}(g)$ and of nilpotent groups.

6.1. Mapping class groups

Recall from §1.5 that $\text{ma}(\Gamma)$ is the smallest dimension of a complex irreducible variety X on which some finite-index subgroup of Γ acts faithfully by automorphisms.

Remark 6.1. Assume that Γ_0 is a finite-index subgroup of Γ , and that Γ_0 acts faithfully on a complex irreducible variety X . Let us show that Γ acts faithfully on the disjoint union of n copies of X . Indeed, Γ acts faithfully on the quotient $\Gamma \times_{\Gamma_0} X$ of $\Gamma \times X$ by the action of Γ_0 defined by $h \cdot (g, x) = (gh^{-1}, hx)$; and $\Gamma \times_{\Gamma_0} X$ is a disjoint union of $[\Gamma : \Gamma_0]$ copies of X .

Thus, $\text{ma}(\Gamma)$ is bounded from below by the smallest dimension of a complex variety X on which Γ acts faithfully by regular automorphisms (the dimension of X is the largest dimension of its irreducible components). The following example shows that this inequality may be strict.

Example 6.2. Consider the direct product H of two non-abelian free groups \mathbb{F}_ℓ and $\mathbb{F}_{\ell'}$. Since $\text{PGL}_2(\mathbf{C})$ contains a free group, H acts faithfully on the disjoint union of two projective lines. But H does not act faithfully by automorphisms on an irreducible curve.

THEOREM 6.3. (Theorem D) *If $\text{Mod}(g)$ acts faithfully on a (not necessarily irreducible) complex variety X by automorphisms, then $\dim(X) \geq 2g - 1$. The minimal dimension $\text{ma}(\text{Mod}(g))$ satisfies $2g - 1 \leq \text{ma}(\text{Mod}(g)) \leq 6g - 6$ for all $g \geq 2$.*

Remark 6.4. We shall need the following fact because X is not assumed to be irreducible: *In $\text{Mod}(g)$, the intersection of two infinite normal subgroups is infinite.* Indeed, if N is an infinite normal subgroup of $\text{Mod}(g)$, then N contains two pseudo-Anosov elements a and b that generate a free group (see [42, Theorem 2]). If M is another normal subgroup containing a pseudo-Anosov element h , then $[w, h] = whw^{-1}h^{-1}$ is an element of $N \cap M$ for every $w \in N$. By a theorem of McCarthy [52], the centralizer of a pseudo-Anosov element is virtually cyclic. Thus, $N \cap M$ is infinite.

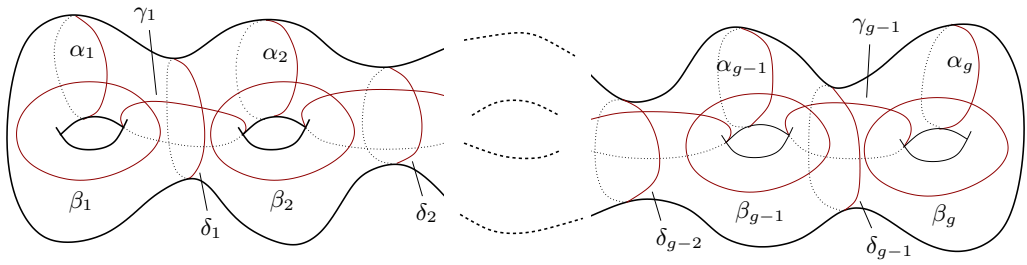


Figure 1. Simple closed loops on the surface of genus g .

Proof. The upper bound $\text{ma}(\text{Mod}(g)) \leq 6g - 6$ is well known; it comes from the action of $\text{Mod}(g)$ on the character variety parameterizing conjugacy classes of representations of the fundamental group of the surface of genus g in SL_2 , an affine variety of dimension $6g - 6$. This action is faithful for $g \geq 3$ (see [50, Theorem 9.15] and [1, Theorem 4.2]). For $g = 2$, the kernel of the action of $\text{Mod}(2)$ on the character variety is the order-2 subgroup generated by the hyperelliptic involution. From [1, Theorem 4.3], or [31, Theorem 6.8], $\text{Mod}(g)$ is virtually torsion-free. Consequently, $\text{Mod}(2)$ contains a finite-index torsion-free subgroup; this subgroup acts faithfully on the character variety.

We now fix a finite-index subgroup Γ of $\text{Mod}(g)$, and we assume that Γ acts faithfully on a complex quasi-projective variety X of dimension d (note that X is not assumed to be irreducible). Our goal is to obtain the lower bound $d \geq 2g - 1$. We identify Γ with its image in $\text{Aut}(X)$. Since $\text{Mod}(g)$ is virtually torsion-free, there is a finite-index, torsion-free subgroup in Γ ; we now replace Γ by such a group.

The group Γ permutes the irreducible components of X ; let Γ' be the kernel of this action by permutations. Denote by X_i the irreducible components of X , and by Γ'_i the kernel of the action of Γ' on X_i . The intersection of the Γ'_i is trivial. As Γ is torsion-free, either Γ'_i is trivial, or Γ'_i is infinite. Since the intersection of two infinite normal subgroups of $\text{Mod}(g)$ is infinite (Remark 6.4), at least one of the Γ'_i is trivial, and the action of Γ' on X_i is faithful. We replace Γ by its finite-index subgroup Γ' and the variety X by such a component X_i . Thus, in what follows, Γ acts faithfully on the irreducible variety X .

We need to show that $d = \dim(X) \geq 2g - 1$. Apply Proposition 3.2 to obtain a prime number $p \geq 3$ and a good model of the pair (X, Γ) over \mathbf{Z}_p . Then, apply Proposition 3.3. We obtain a finite extension K of \mathbf{Q}_p , an analytic polydisk $\mathcal{U} \subset X(K)$, and a finite-index subgroup Γ'' of Γ that preserves \mathcal{U} : The action of Γ'' on \mathcal{U} is given by an embedding Γ'' into $\text{Diff}^{\text{an}}(\mathcal{U})_1$, the group of Tate analytic diffeomorphisms which are equal to Id modulo p (see §2.3.2). Again, we replace Γ by this finite-index subgroup Γ'' . Then, the conclusion is a consequence of the following lemma. \square

LEMMA 6.5. *Let p be an odd prime and K be a finite extension of \mathbf{Q}_p . If a finite-index subgroup Γ of $\text{Mod}(g)$ embeds in $\text{Diff}^{\text{an}}(\mathcal{U})_1$, where $\mathcal{U} \simeq \mathcal{O}_K^d$ is an analytic polydisk of dimension d , then $d \geq 2g - 1$.*

Proof. Elements of Γ give Tate analytic diffeomorphisms of \mathcal{U} which are equal to the identity modulo p . Since $p \geq 3$, we can apply the Bell–Poonen theorem to every element of Γ (take $c=1$ in Theorem 2.4). In particular, each element $\gamma \in \Gamma$ determines a Tate analytic vector field \mathbf{X}_γ on \mathcal{U} ; and, if γ and γ' commute, then so do the corresponding vector fields (Corollary 2.8).

Denote by T_{α_i} and T_{β_i} , $i=1, \dots, g$, the Dehn twists along the simple closed loops which are depicted in Figure 1. There exists an integer $m \geq 1$ such that the twists $T_{\alpha_i}^m$ and $T_{\beta_i}^m$ are all in Γ . Observe that the g twists $T_{\alpha_i}^m$ commute. For $x \in \mathcal{U}$, denote by $s(x)$ the dimension of the K -vector space spanned by the tangent vectors $\mathbf{X}_{T_{\alpha_i}^m}(x)$, $1 \leq i \leq g$; let s be the maximum of $s(x)$, for x in \mathcal{U} .

There exists a smaller polydisk $\mathcal{V} \subset \mathcal{U}$ and 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{V} . 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

$$\mathbf{X}_{T_{\alpha_i}^m} = \sum_{j \in S} F_{i,j} \mathbf{X}_j \tag{6.1}$$

where the $F_{i,j}$'s are analytic functions on \mathcal{V} . 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

$$\mathbf{X}_k F_{i,j} = 0 \tag{6.2}$$

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

Suppose that $S \neq \{1, \dots, g\}$, and pick an index r in $\{1, \dots, g\} \setminus S$. Observe that $T_{\beta_r}^m$ does not commute with $T_{\alpha_r}^m$ but commutes with the other $T_{\alpha_i}^m$; hence $[\mathbf{X}_{T_{\beta_r}^m}, \mathbf{X}_j] = 0$ for every $j \in S$. Assume by contradiction that, for every x in \mathcal{V} , $\mathbf{X}_{T_{\beta_r}^m}(x)$ is a linear combination of the $\mathbf{X}_j(x)$, $j \in S$, and write $\mathbf{X}_{T_{\beta_r}^m} = \sum_{j \in S} G_j \mathbf{X}_j$, where the G_j 's are analytic functions on \mathcal{U} . The commutation rules imply $\mathbf{X}_i G_j = 0$ for all indices i and j in S ; thus, equations (6.1) and (6.2) lead to

- $\mathbf{X}_{T_{\alpha_l}^m} G_j = 0$ for all indices $l \in \{1, \dots, g\}$;
- $[\mathbf{X}_{T_{\alpha_r}^m}, \mathbf{X}_{T_{\beta_r}^m}] = 0$.

Thus, by Corollary 2.8, $T_{\beta_r}^m$ commutes with $T_{\alpha_r}^m$, a contradiction. This means that there exists a smaller polydisk $\mathcal{W} \subset \mathcal{V} \subset \mathcal{U}$ on which the vector fields $\{\mathbf{X}_{T_{\beta_r}^m}\} \cup \{\mathbf{X}_j : j \in S\}$ are everywhere linearly independent. Now, we add r to S and set $\mathbf{X}_r := \mathbf{X}_{T_{\beta_r}^m}$.

Use that the $T_{\beta_i}^m$ commute, and commute with the $T_{\alpha_j}^m$ for $i \neq j$, and 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 on a smaller polydisk; these vector fields correspond to elements of type $T_{\alpha_j}^m$ or $T_{\beta_i}^m$, for a disjoint set of curves α_j and β_i ; we denote by Λ this set of curves. Each index $s \in S = \{1, \dots, g\}$ corresponds to a unique curve α_s or β_s in Λ ; the vector field \mathbf{X}_s is determined by $T_{\alpha_s}^m$ or $T_{\beta_s}^m$.

In what follows, we fix an element Φ of the mapping class group which maps this non-separating set of disjoint curves Λ to $\alpha_1, \alpha_2, \dots, \alpha_g$. Then, denote by γ'_i and δ'_i the images of the curves γ_i and δ_i , respectively, by Φ^{-1} (see Figure 1); these curves are disjoint from the g curves of Λ .

Consider the curves γ'_1 and δ'_1 , and fix an integer $m > 0$ such that the Dehn twists $T_{\gamma'_1}^m$ and $T_{\delta'_1}^m$ generate a free subgroup of Γ (see [31, Theorem 3.14]). These twists commute with the T_ν^m for all curves $\nu \in \Lambda$. If, on some polydisk $\mathcal{P} \subset \mathcal{U}$, the vector fields \mathbf{Y}_1 and \mathbf{Z}_1 corresponding to $T_{\gamma'_1}^m$ and $T_{\delta'_1}^m$, respectively, are combinations $\mathbf{Y}_1 = \sum_j H_j \mathbf{X}_j$ and $\mathbf{Z}_1 = \sum_j H'_j \mathbf{X}_j$, then $T_{\gamma'_1}^m$ and $T_{\delta'_1}^m$ commute on that polydisk, and then they commute everywhere, a contradiction. Thus, one can add a vector field \mathbf{Y}_1 (or \mathbf{Z}_1) to our list of generically independent 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 $\dim(\mathcal{U}) \geq 2g-1$. \square

The group $\text{Out}(\mathbb{F}_{2n+s-1})$ contains a copy of $\text{Mod}(n, s)$, the mapping class group of the surface of genus n with $s \geq 1$ punctures. The proof of Theorem D also shows that

$$2n-1 \leq \text{ma}(\text{Mod}(n, 1)) \leq \text{ma}(\text{Out}(\mathbb{F}_{2n}))$$

(with $s=1$) and that

$$2n-1 \leq \text{ma}(\text{Mod}(n, 2)) \leq \text{ma}(\text{Out}(\mathbb{F}_{2n+1}))$$

(with $s=2$). Thus, we obtain $m-2 \leq \text{ma}(\text{Out}(\mathbb{F}_m))$ for all $m \geq 2$.

6.2. 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 $\text{dl}(H)$, and a similar notation is used for Lie algebras. Then, define the *virtual derived length* of H by

$$\text{vdl}(H) = \min\{\text{dl}(H') : H' \text{ is a finite-index subgroup of } H\}.$$

THEOREM 6.6. *Let H be a finitely generated nilpotent group. If H acts faithfully by automorphisms on an irreducible complex quasi-projective variety X , then we have $\text{vdl}(H) \leq \dim(X)$. Thus, $\text{ma}(H) \geq \text{vdl}(H)$.*

Let us sketch the proof. Let d be the dimension of X . Apply Propositions 3.2 and 3.3: there is a finite-index subgroup H_0 of H and a polydisk $\mathcal{U} \simeq \mathbf{Z}_p^d \subset X(\mathbf{Z}_p)$ such that the action of H_0 on $X(\mathbf{Z}_p)$ preserves the polydisk \mathcal{U} and determines an embedding of H_0 in $\text{Diff}^{\text{an}}(\mathcal{U})_1$. Consider the Lie algebra \mathfrak{h} which is generated by the vector fields X_f , for f in $H_0 \subset \text{Diff}^{\text{an}}(\mathcal{U})_1$. Corollary 2.8 shows that the derived length of \mathfrak{h} is equal to the derived length of H_0 . To conclude, apply the following lemma, the proof of which is the same as in [15, Proposition 3.9], or [29, Theorem 1.1].

LEMMA 6.7. *Let \mathfrak{h} be a nilpotent Lie algebra of Tate analytic vector fields on a polydisk \mathcal{U} . Then, $\text{dl}(\mathfrak{h}) \leq \dim(\mathcal{U})$.*

7. Periodic orbits and invariant polydisks

Our goal is to produce invariant p -adic polydisks for some groups of birational transformations of a projective variety defined over a finite extension K of \mathbf{Q}_p . This is closely related to the existence of “good” periodic orbits for groups of birational transformations defined over finite fields; in a first time, we focus on the construction of such orbits.

7.1. Property (τ^∞) and linear isoperimetric inequalities

In this section, we introduce property (τ^∞) , which may be viewed as a weak form of Kazhdan property (T) (see [40]), and we relate this property to linear isoperimetric inequalities. Then, we prove that property (τ^∞) is equivalent to property (FM), introduced in [35] and [22].

In what follows, Γ will be a group with a finite symmetric set of generators S (the symmetry means that $s \in S$ if and only if $s^{-1} \in S$). If h is an element of Γ , $|h|_S$ denotes the length of h with respect to S ; by definition, $|h|_S$ is the minimum of the integers $m \geq 0$ such that h is a product of m elements of S .

7.1.1. Quotients and Schreier graphs

Given a subgroup R of Γ , consider the quotient space Γ/R . The group Γ acts on Γ/R by left translations: given h in Γ , we denote by L_h the translation $gR \mapsto hgR$. Denote by $\ell^2(\Gamma/R)$ the space of ℓ^2 -functions on Γ/R , i.e. functions $\varphi: \Gamma/R \rightarrow \mathbf{C}$ which are square integrable:

$$\|\varphi\|_{\ell^2(\Gamma/R)}^2 := \sum_{\omega \in \Gamma/R} |\varphi(\omega)|^2 < \infty.$$

The action of Γ on Γ/R by left translations determines a unitary representation $g \mapsto L_{g^{-1}}^*$ of Γ on $\ell^2(\Gamma/R)$, where $L_{g^{-1}}^* \varphi := \varphi \circ L_{g^{-1}}$.

The Schreier graph \mathcal{G}_R is defined as follows: The set of vertices of \mathcal{G}_R is $\mathcal{G}_R^0 = \Gamma/R$; two vertices g_1R and $g_2R \in \Gamma/R$ are joined by an edge if and only if there exists $s \in S$ satisfying $g_2R = sg_1R$. When $R = \{e\}$, \mathcal{G}_R is the Cayley graph $\mathcal{G} := \mathcal{G}_{\{e\}}$ of Γ . Those graphs depend on the choice of the generating set S .

Remark 7.1. If the distance between gR and $g'R$ in the graph \mathcal{G}_R is δ , then

$$\text{dist}(L_h(gR), L_h(g'R))$$

is at most $\delta + 2|h|_S$. When R is a normal subgroup of Γ , then Γ also acts on the right, $gR \mapsto gRh = ghR$, and this right action is by isometries.

Let Ω be a finite subset of Γ/R . Denote by $\chi_\Omega: \Gamma/R \rightarrow \{0, 1\}$ 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 $(\Gamma/R) \setminus \Omega$ 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 $L_s(x) \notin \Omega$, that is, 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

$$\|\chi_\Omega - L_s^*(\chi_\Omega)\|_{\ell^2(\Gamma/R)}^2 = \sum_{x \in \Gamma/R} (\chi_\Omega(x) - \chi_\Omega(L_s x))^2 \leq \sum_{x \in \bigcup_{s \in S} \Omega \Delta s^{-1}(\Omega)} 1^2,$$

and hence

$$\|\chi_\Omega - L_s^*(\chi_\Omega)\|_{\ell^2(\Gamma/R)}^2 \leq 2|S| |\partial\Omega|. \tag{7.1}$$

The *Cheeger constant* of the Schreier graph \mathcal{G}_R is the infimum

$$h(\mathcal{G}_R) = \inf_{\Omega} \frac{|\partial\Omega|}{|\Omega|},$$

where Ω describes the non-empty finite subsets of Γ/R with $|\Omega| \leq \frac{1}{2}|\Gamma/R|$ (this constraint is void when Γ/R is infinite).

7.1.2. Uniform, linear isoperimetric inequalities and property (τ^∞)

Let Γ be a group with a finite, symmetric set of generators S . The group Γ has *property (τ^∞)* if there exists a constant $\varepsilon = \varepsilon(\Gamma, S) > 0$ such that, for every subgroup $R \subset \Gamma$ of infinite index and every function $\xi \in \ell^2(\Gamma/R)$, there exists an element $s \in S$ such that $\|\xi - L_s^* \xi\| \geq \varepsilon \|\xi\|$. Property (τ^∞) does not depend on S , even if the constant ε does (this follows from Proposition 7.3 below); thus, we refer to property (τ^∞) as a property of the (finitely generated) group Γ , and not of the pair (Γ, S) .

PROPOSITION 7.2. *Let Γ be a group with a finite, symmetric set of generators S . Then, Γ has property (τ^∞) if and only if there is a positive constant h_∞ such that $h(\mathcal{G}_R) \geq h_\infty > 0$ for every subgroup R of Γ of infinite index.*

In fact, $h(\mathcal{G}_R) \geq \varepsilon^2/2|S|$ if Γ satisfies property (τ^∞) with constant ε for S .

Proof. Assume that Γ/R is infinite. Consider the unitary action of Γ on $\ell^2(\Gamma/R)$ by left translations. For every finite set $\Omega \subseteq \Gamma/R$, the characteristic function χ_Ω is an element of $\ell^2(\Gamma/R)$ and property (τ^∞) implies the existence of an element $s \in S$ such that

$$\|\chi_\Omega - L_s^* \chi_\Omega\|_{\ell^2(\Gamma/R)} \geq \varepsilon \|\chi_\Omega\|_{\ell^2(\Gamma/R)} = \varepsilon |\Omega|^{1/2}.$$

From inequality (7.1), we deduce that $(2|S| |\partial\Omega|)^{1/2} \geq \varepsilon |\Omega|^{1/2}$. Hence, $h(\mathcal{G}_R) \geq h_\infty$ for $h_\infty = \varepsilon^2/2|S|$.

The other implication may be obtained as in Hulanicki’s characterization of amenability (see [49, Theorems 3.1.5 and 4.3.2]). We do not prove it because it is not used in this article. □

7.1.3. Other classical properties and examples

We now compare property (τ^∞) to other classical properties.

- A group Γ has property (τ) if there exists a constant $\varepsilon > 0$ such that, for every finite-index normal subgroup $R \subset \Gamma$, and for every function $\xi: \Gamma/R \rightarrow \mathbf{C}$ which is ℓ^2 -orthogonal to the constant functions, there exists a generator $s \in S$ such that $\|\xi - L_s^* \xi\| \geq \varepsilon \|\xi\|$ (see [49]). In [5], Bekka and Olivier study property (T_{ℓ^p}) , for $p \neq 2$, and show that this property is equivalent to the conjunction of properties (τ) and (τ^∞) . In particular, property (T_{ℓ^p}) implies property (τ^∞) .

- In [22], Cornulier introduces property (FM). Let us describe this property in the case of a discrete group Γ . A discrete Γ -set is, by definition, an action of Γ on a discrete set X . A mean on X (or more precisely on $\ell^\infty(X)$), is a linear functional $m: \ell^\infty(X) \rightarrow \mathbf{R}$ that satisfies $m(\mathbb{1}) = 1$ and $m(\xi) \geq 0$ for every bounded function $\xi: X \rightarrow \mathbf{R}_+$. A mean is Γ -invariant if its values on ξ and $\xi \circ \gamma^{-1}$ are equal for all $\xi \in \ell^\infty(X)$ and $\gamma \in \Gamma$. One says that Γ has property (FM) if every discrete Γ -set with a Γ -invariant mean contains a finite Γ -orbit. From [22], we get the following result.

PROPOSITION 7.3. *Discrete groups with property (FM) are finitely generated. Property (FM) is equivalent to property (τ^∞) .*

Thus, we could have started with property (FM), without assuming Γ to be finitely generated, and then deduce property (τ^∞) , which is really the definition that we use in the sequel.

Proof. The first assertion is contained in [22, Proposition 5.6]. [22, Remark 5.16] shows that property (FM) implies property (τ^∞) . The argument is the following. Assume that there is a sequence of infinite quotient spaces $Y_n = \Gamma/R_n$ and functions $\xi_n \in \ell^2(Y_n)$ of norm 1 such that $\|\xi_n - L_s^* \xi_n\| \leq 1/n$. Consider the discrete Γ -set X which is obtained as the disjoint union of the Y_n , and extend each ξ_n as a function on X by $\xi_n(y) = 0$ if $y \in X \setminus Y_n$. The linear maps $m_n(\xi) = \sum_x \xi_n(x)^2 \xi(x)$ define a sequence of means on X . By compactness of the set of means, a subsequence $\{m_{n_i}\}_i$ converges towards a mean m_∞ ; by construction, m_∞ is Γ -invariant. But X does not contain any finite orbit. Thus, (FM) implies (τ^∞) .

In the opposite direction, assume that Γ has property (τ^∞) but does not have property (FM). Then, there exists a discrete Γ -set X , which is a disjoint union of infinite orbits $Y_i = \Gamma/R_i$ and which supports an invariant mean m . The existence of m implies that $\ell^2(X)$ contains a sequence of almost invariant vectors ξ_n (see [22, Lemma 5.9] and [4, Appendix G.3]): ξ_n has norm 1 and $\|\xi_n - L_s^* \xi_n\| \leq 1/n$ for all s in the generating set S . To obtain a contradiction, decompose ξ_n as an orthogonal sum $\xi_n = \sum_i \xi_{n,i}$, where each $\xi_{n,i}$ is the restriction of ξ_n to the orbit Y_i . Since Γ/R_i is infinite, there exists a generator $s_{n,i}$ such that $\|\xi_{n,i} - L_{s_{n,i}}^* \xi_{n,i}\|^2 \geq \varepsilon^2$ (with ε the constant provided by property (τ^∞)). Hence, there is a generator s_n such that $\|\xi_n - L_{s_n}^* \xi_n\|^2 \geq \varepsilon^2/|S|$. We get a contradiction when $n^2 > |S|/\varepsilon^2$. □

- A discrete group Γ has Kazhdan property (T) if every action of Γ on a Hilbert space \mathcal{H} by affine isometries has a fixed point (see [40, Chapters 1 and 4]). Such a group is automatically finitely generated and, given a finite system of generators, the following equivalent definition of Kazhdan property (T) will be more useful to us. A finitely generated group Γ has *Kazhdan property (T)* if, for any finite symmetric set of generators S , there exists an $\varepsilon > 0$, with the following property: given any unitary representation ϱ of Γ on a Hilbert space \mathcal{H} , either there exists $v \in \mathcal{H} \setminus \{0\}$ such that $\varrho(\Gamma) \cdot v = v$, or, for every $v \in \mathcal{H}$, there exists $s \in S$ such that

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

Such a positive number ε is called a *Kazhdan constant* for the pair (Γ, S) . Thus, property (τ^∞) turns out to be a weak form of property (T), in which one only considers the unitary representations $\ell^2(Y)$, where Y is a set on which Γ acts transitively. We obtain the following result.

PROPOSITION 7.4. *If Γ satisfies Kazhdan property (T) with constant ε for the generating set S , then it satisfies the uniform linear isoperimetric inequality $|\partial\Omega| \geq (\varepsilon^2/2|S|)|\Omega|$ in all its infinite quotients Γ/R .*

Example 7.5. Let Γ be a non-amenable group with no infinite proper subgroup. Then Γ has property (τ^∞) (see [5, Proposition 15 and Example 17], or [35, §4.C]). Let Γ be an irreducible lattice in $\mathrm{SO}(n, 2) \times \mathrm{SO}(n+1, 1)$, for some $n \geq 3$. Then Γ does not have property (T), but has property (τ^∞) (see [5, Example 14] and [22, Example 1.14] for a related construction).

7.2. Finite orbits and finite-index subgroups

Let X be an absolutely irreducible projective variety of dimension d defined over a finite field \mathbf{F} . Let Γ be a group with a finite symmetric set of generators S . Assume that the group Γ embeds into the group $\mathrm{Bir}(X_{\mathbf{F}})$ and identify Γ with its image in $\mathrm{Bir}(X_{\mathbf{F}})$.

7.2.1. The escaping set E

Let U be a Zariski open subset of X defined over \mathbf{F} such that, for every $s \in S$, the map $s|_U: U \rightarrow X$ is a morphism and an open immersion. Such a set exists because S is finite: for U , take the complement of all the proper subsets B_s , for s in S , where B_s is defined as in §3.1.2.

Remark 7.6. One may want to shrink 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 $U \subset X \setminus \{x: f(x) = x\}$. Or one can remove the singular locus of X from U .

By construction, the codimension of the Zariski closed set $X \setminus U$ is at least 1. 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 .

7.2.2. Lang–Weil estimates (see [46])

By Lang–Weil estimates, there exists a positive constant c_U such that, given any finite field extension \mathbf{F}' of \mathbf{F} , the number of points in $U(\mathbf{F}')$ satisfies

$$|\mathbf{F}'|^d - c_U |\mathbf{F}'|^{d-1/2} \leq |U(\mathbf{F}')| \leq |\mathbf{F}'|^d + c_U |\mathbf{F}'|^{d-1/2}, \tag{7.2}$$

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

Similarly,

$$|E(\mathbf{F}')| \leq b_E |\mathbf{F}'|^{d-1} + c_E |\mathbf{F}'|^{d-3/2}, \tag{7.3}$$

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

7.2.3. Regular stabilizers

Fix a finite extension \mathbf{F}' of the field \mathbf{F} . Given a point $x \in U(\mathbf{F}')$, 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, \dots, g_l) be a path in the Cayley graph \mathcal{G} , and denote by s_{i+1} the element of S such that $g_{i+1} = s_{i+1}g_i$, $1 \leq i \leq l-1$. The path (e, g_1, \dots, 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, \dots, 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 7.7. An element $g \in \Gamma$ is a *regular stabilizer* of $x \in U(\mathbf{F}')$ if there exists a regular path (e, g_1, \dots, g_l) in \mathcal{G} such that (i) $g_l = g$ and (ii) $g_l(x) = x$. The set of all regular stabilizers is the *regular stabilizer* of x , and is denoted by R_x .

LEMMA 7.8. *The regular stabilizer R_x is a subgroup of Γ .*

Proof. Given g and h in R_x , and regular paths (e, g_1, \dots, g_l) and $(e, h_1, \dots, h_{l'})$ in Γ satisfying properties (i) and (ii) of Definition 7.7 for g and h , respectively, one can define a new regular path $(e, h_1, \dots, h_{l'}, g_l h_{l'}, \dots, g_l h_{l'})$ 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 $(e, s_l^{-1}, s_{l-1}^{-1} \circ s_l^{-1}, \dots, g^{-1})$ 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, \dots, g_l) and gives a point

$$ev_x(e, g_1, \dots, g_l) = g_l(x).$$

We shall say that an element $g \in \Gamma$ is *very well defined* at $x \in U(\mathbf{F}')$ if there is a regular path from e to $g_l = g$. For such an element, the image $\text{ev}_x(e, g_1, \dots, g_l) = g_l(x) = g(x)$ 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 $U(\mathbf{F}')$. The preimage of x is the regular stabilizer. The image is the regular orbit of x .

7.2.4. The subsets $\Omega_x \subseteq \Gamma/R_x$

Fix a point $x \in U(\mathbf{F}')$. 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 $\Omega_x \subseteq \Gamma/R_x$ to be the set of all such vertices $[g]$. The evaluation map determines a map $\text{ev}_x: \Omega_x \rightarrow U(\mathbf{F}')$ (we make use of the same notation for simplicity).

PROPOSITION 7.9. *Let \mathbf{F}' be a finite extension of \mathbf{F} . Let x be a point of $U(\mathbf{F}')$. The subset $\Omega_x \subseteq \Gamma/R_x$ 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, \dots, g_l) in Γ , which connects $[e]$ to $[g]$ in Ω_x ;
- (3) the evaluation map $\text{ev}_x: [g] \mapsto g(x)$ is well defined (because R_x stabilizes x) and is an injective map $\text{ev}_x: \Omega_x \rightarrow U(\mathbf{F}')$, the image of which is the regular orbit of x ;
- (4) Ω_x is a finite set, with $|\Omega_x| \leq |U(\mathbf{F}')|$.

Proof. All we have to prove is that ev_x is injective. If $g(x) = h(x)$ with two regular paths $(e, g_1, \dots, g_l = g)$ and $(e, h_1, \dots, h_{l'} = h)$, 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 that $h^{-1} \circ g \in R_x$. □

Thus, one gets a parametrization of the regular orbit of $x \in U(\mathbf{F}')$ 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 $g(x) \in E(\mathbf{F}')$. Since the evaluation map is injective, one gets

$$|\partial\Omega_x| = |\text{ev}_x(\partial\Omega_x)| = |E_x(\mathbf{F}')|,$$

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

Since regular orbits are disjoint, the sets $E_x(\mathbf{F}')$ and $E_y(\mathbf{F}')$ are disjoint as soon as x and y are not in the same regular orbit. Being finite, $U(\mathbf{F}')$ is a union of finitely many

disjoint regular orbits. Fixing a set $\{x_1, \dots, x_m\}$ of representatives of these regular orbits, we obtain

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

Let us now assume that Γ has property (τ^∞) ; thus, by Proposition 7.2, Γ satisfies a uniform linear isoperimetric inequality

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

in all its infinite Schreier graphs \mathcal{G}_R . Suppose that R_x has infinite index in Γ for every $x \in U(\mathbf{F}')$. Then,

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

Then, the Lang–Weil estimates stated in equations (7.2) and (7.3) imply that

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

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

THEOREM 7.10. *Let X be an absolutely irreducible projective variety defined over a finite field \mathbf{F} . Let Γ be a subgroup of $\text{Bir}(X_{\mathbf{F}})$ with property (τ^∞) and S be a finite symmetric set of generators of Γ . Let U be a non-trivial, Zariski open subset of X such that, for every $s \in S$, the map $s|_U: U \rightarrow X$ is an open immersion. If \mathbf{F}' is a finite extension of \mathbf{F} and $|\mathbf{F}'|$ is large enough, there exists a point x in $U(\mathbf{F}')$ such that the regular stabilizer R_x of x is a finite-index subgroup of Γ .*

7.2.5. Abelian groups

Let $\alpha \geq 1$ be a real number. Say that a graph \mathcal{G} satisfies an isoperimetric inequality of type α if there is a constant $c > 0$ such that

$$|\partial\Omega|^\alpha \geq c|\Omega| \tag{7.4}$$

for every finite subset Ω of \mathcal{G} . Let $d \geq 2$ be an integer. The Cayley graph of the group \mathbf{Z}^d satisfies an isoperimetric inequality of type $d/(d-1)$ for any finite symmetric set of

generators; the isoperimetric inequality satisfied in Proposition 7.2 is of linear type (i.e. $\alpha=1$). 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 $|B(r)|$. Then, define the function Φ_S by

$$\Phi_S(t) = \min\{r : t \leq |B(r)|\}$$

(as in [24, §1, p. 295]). 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 [24] that

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

for every non-empty finite subset 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 7.11. *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 $l<k$; set $q=k-l$ and $c_S=(16|S|)^{-(q-1)/q}$. 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*

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

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 the projection of S , the function Φ_S satisfies $\Phi_S(t) \leq t^{1/q}$. The projection $A/R \rightarrow A/T$ 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 function Φ_S for A/R satisfies the same inequality $\Phi_S(t) \leq t^{1/q}$. This implies that

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

and the result follows. \square

THEOREM 7.12. *Let X be a projective variety, defined over a finite field \mathbf{F} , and let d be its dimension. Let A be a free abelian group of rank $k<\infty$, acting by birational transformations on X (defined over \mathbf{F}). Then, there exist a finite extension \mathbf{F}' of \mathbf{F} , a point x in $X(\mathbf{F}')$, and a subgroup R of A such that the rank of R is $\geq k-d$ and every element of R is defined at the point x and fixes it.*

Proof. Changing \mathbf{F} in a finite extension, X in one of its irreducible components, and A in a finite-index subgroup, we may assume that X is absolutely irreducible. Fix an algebraic closure $\bar{\mathbf{F}}$ of \mathbf{F} . We may assume that d is positive, since otherwise X is just one point. We fix a system of generators for A and an open subset U of X such that, on U , every generator restricts to an open immersion $s|_U: U \rightarrow X$ (see §7.2.1). Assume by contradiction that the regular stabilizer R_x of every point of $X(\bar{\mathbf{F}})$ has rank at most l , with $l < k - d$. Denote by α the ratio $q/(q-1)$ with $q = k - l > d$; we have $1 < \alpha < d/(d-1)$. Let \mathbf{F}' be a finite extension of \mathbf{F} and $\{x_i\}_i$ be a set of representatives of the regular orbits of $U(\mathbf{F}')$. From assertion (3) of Proposition 7.9, we obtain

$$|\partial\Omega_{x_i}| = |\text{ev}_{x_i}(\partial\Omega_{x_i})| = |E_{x_i}(\mathbf{F}')|,$$

and Lemma 7.11 provides a constant $c > 0$ such that

$$|U(\mathbf{F}')| = \sum_i |\Omega_{x_i}| \leq c \sum_i |\partial\Omega_{x_i}|^\alpha = c \sum_i |E_{x_i}(\mathbf{F}')|^\alpha \leq c \left(\sum_i |E_{x_i}(\mathbf{F}')| \right)^\alpha.$$

From Lang–Weil estimates, one derives

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

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

7.3. Invariant polydisks for groups with property (τ^∞)

Let $X_{\mathbf{Q}_p}$ be an absolutely irreducible projective variety. Assume that X is defined over \mathbf{Z}_p , that Γ is a finitely generated subgroup of $\text{Bir}(X_{\mathbf{Z}_p})$ with a finite symmetric set of generators S , and that $(X_{\mathbf{Z}_p}, \Gamma)$ is a good model over \mathbf{Z}_p .

THEOREM 7.13. *Assume that Γ has property (τ^∞) . There exist a finite extension K of \mathbf{Q}_p , a finite-index subgroup Γ_0 of Γ , and a Tate 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_0 -invariant and the action of Γ_0 on \mathcal{V} is conjugate, via φ , to a subgroup of $\text{Diff}^{\text{an}}(\mathcal{U})$. Moreover, one can choose this polydisk in the complement of any given proper Zariski closed subset of the generic fiber.*

The following proof constructs Γ_0 as a regular stabilizer R_x .

Proof. Given $g \in \text{Bir}(X_{\mathbf{Z}_p})$, recall that $B_{\mathbf{Z}_p, g}$ denotes the complement of the points of $X_{\mathbf{Z}_p}$ around which g is an open immersion (see §3.1.2). Since $(X_{\mathbf{Z}_p}, \Gamma)$ is a good model over \mathbf{Z}_p , the singular locus of the scheme $X_{\mathbf{Z}_p}$ and the sets $B_{\mathbf{Z}_p, g}$, for g in S , have

codimension ≥ 1 in $X_{\mathbf{Z}_p}$ and in the special fiber too (see (ii) and (iii) in §3.1.2). Denote by $\text{Sing}(X_{\mathbf{Z}_p})$ the singular locus of $X_{\mathbf{Z}_p}$, and set

$$U_{\mathbf{Z}_p} := X_{\mathbf{Z}_p} \setminus \left(\text{Sing}(X_{\mathbf{Z}_p}) \cup \left(\bigcup_{s \in S} B_{\mathbf{Z}_p, s} \right) \right).$$

Let $X_{\mathbf{F}_p}$ be the special fiber. By assumption, $U_{\mathbf{Z}_p} \cap X_{\mathbf{F}_p}$ is a non-empty Zariski open subset of $X_{\mathbf{F}_p}$; let U be any open subset of $U_{\mathbf{Z}_p} \cap X_{\mathbf{F}_p}$ (for instance, take for U the complement of a given divisor). Observe that, for any $s \in S$, the map $s|_{U_{\mathbf{Z}_p}} : U_{\mathbf{Z}_p} \rightarrow X_{\mathbf{Z}_p}$ is an open immersion; hence, $s|_U : U \rightarrow X_{\mathbf{F}_p}$ is also an open immersion.

By Theorem 7.10, there exist a finite field extension \mathbf{F}' of \mathbf{F}_p and a point $x \in U(\mathbf{F}')$ 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 \mathbf{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 $X_{\mathbf{F}'}$ coincides with x . By Proposition 3.4, one can find an 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 $\text{Diff}^{\text{an}}(\mathcal{U})$. □

Similarly, Theorem 7.12 provides invariant polydisks for subgroups of rank $l \geq k - \dim(X)$ when Γ is a free abelian group of rank k .

7.4. Groups of birational transformations and finite-index subgroups

7.4.1. Groups of birational transformations

A group Γ is linear over the field \mathbf{k} if Γ is isomorphic to a subgroup of $\text{GL}_n(\mathbf{k})$ for some $n \geq 1$ (see [39]). Similarly, a group Γ is a *group of birational transformations over the field \mathbf{k}* if Γ is isomorphic to a subgroup of $\text{Bir}(X_{\mathbf{k}})$ for some algebraic variety defined over \mathbf{k} .

Example 7.14. Linear groups over \mathbf{k} are groups of birational transformations over \mathbf{k} . Every finite group is a group of automorphisms of some complex irreducible curve (see [36, Theorem 6']). The modular group $\text{Mod}(g)$ of a closed, orientable surface of genus $g \geq 3$ and the group $\text{Out}(\mathbb{F}_g)$ are groups of birational transformations in dimension $\leq 6g$ over \mathbf{C} , but $\text{Out}(\mathbb{F}_g)$ is not a linear group if $g \geq 4$ (see §6 and [50], [33]).

7.4.2. Malcev and Selberg properties

In characteristic zero, linear groups satisfy Malcev and Selberg properties: every finitely generated linear group is residually finite and contains a torsion-free, finite-index sub-

group. One does not know whether groups of birational transformations share the same properties (see [14] and [21]). The following result implies Theorem C of the introduction.

THEOREM 7.15. *Let Γ be a discrete group with property (τ^∞) . If Γ is a group of birational transformations over a field \mathbf{k} of characteristic zero, then Γ is residually finite and contains a torsion-free, finite-index subgroup.*

Proof. Since Γ has property (τ^∞) , it is finitely generated (see §7.1 and Proposition 7.3); 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 an algebraically closed field \mathbf{k} of characteristic zero). Pick an element f in $\Gamma \setminus \{\text{Id}\}$ and denote by $\text{Fix}(f)$ the proper Zariski closed set of fixed points of f ; more precisely, $\text{Fix}(f) \subset X$ is defined as the Zariski closure of the subset of the domain of definition of f defined by the equation $f(z)=z$. By Proposition 3.2, one can find a prime number $p \geq 3$, and a good model $\Gamma \subset \text{Bir}(X_{\mathbf{Z}_p})$ for (X, Γ) , such that the special fiber $X_{\mathbf{F}_p}$ of $X_{\mathbf{Z}_p}$ is not contained in $\text{Fix}(f)$.

Choose a Zariski open subset U of $X_{\mathbf{F}_p}$ which is contained in the complement of $\text{Fix}(f)$ and of the sets $B_{\mathbf{Z}_p, s}$, for $s \in S$. We now apply Theorem 7.10. Since Γ has property (τ^∞) , one can find an extension \mathbf{F}' of the residue field \mathbf{F}_p , and a point $x \in U(\mathbf{F}')$, for which the regular stabilizer R_x has finite index in Γ . By construction, R_x does not contain f . This shows that Γ is residually finite.

Let \mathcal{U} be the polydisk $(O_K)^d$. To prove the second assertion, keep the same notation and apply Theorem 7.13. This provides an R_x -invariant subset \mathcal{V} and an analytic diffeomorphism $\varphi: \mathcal{U} \rightarrow \mathcal{V}$ such that, after conjugacy by φ , R_x acts by Tate analytic diffeomorphisms on \mathcal{U} . Then, there exists a finite-index subgroup R'_x of R_x such that every element $g \in R'_x$ corresponds to a power series

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

where each A_i is homogeneous of degree i , A_0 is zero modulo p^2 and A_1 is the identity modulo p . After conjugation by $z \mapsto pz$, the Bell–Poonen theorem (Theorem 2.4) can be applied to g . Thus, Corollary 2.5 shows that R'_x is torsion-free. □

7.4.3. Central extensions and simple groups

Fix two positive integers q and n , with $q \neq 1, 2, 4$ and $n \geq 2$. Consider the group $\text{Sp}_{2n}(\mathbf{Z})$, and the central extension

$$0 \longrightarrow \mathbf{Z}/q\mathbf{Z} \longrightarrow \Gamma \longrightarrow \text{Sp}_{2n}(\mathbf{Z}) \longrightarrow 1,$$

which is obtained from the universal cover

$$0 \longrightarrow \mathbf{Z}/q\mathbf{Z} \longrightarrow \widetilde{\mathrm{Sp}}_{2n}(\mathbf{R})/q\mathbf{Z} \longrightarrow \mathrm{Sp}_{2n}(\mathbf{R}) \longrightarrow 1$$

by taking the quotient with respect to the subgroup $q\mathbf{Z}$ of the center $\mathbf{Z} \subset \widetilde{\mathrm{Sp}}_{2n}(\mathbf{R})$. Since $n \geq 2$, $\mathrm{Sp}_{2n}(\mathbf{Z})$ has Kazhdan property (T) (see [40]). Since q does not divide 4, the image of $4\mathbf{Z}$ in the center $\mathbf{Z}/q\mathbf{Z}$ of Γ is non-trivial and is contained in every finite-index subgroup of Γ (see [25]); consequently, Γ does not contain any torsion-free finite-index subgroup.

COROLLARY 7.16. *The group $\mathrm{Sp}_{2n}(\mathbf{Z})$ is a group of birational transformations over the field \mathbf{Q} but, if $n \geq 2$, there is a finite cyclic central extension Γ of $\mathrm{Sp}_{2n}(\mathbf{Z})$ that does not act faithfully by birational transformations in characteristic zero.*

In particular, the property “ Γ is a group of birational transformations” is not stable under finite central extensions. Similar examples can be derived from [53] and [56]. The following corollary shows that the simple groups constructed in [30] and [20] do not act non-trivially by birational transformations.

COROLLARY 7.17. *If Γ is an infinite, simple, discrete group with property (τ^∞) , and X is a complex projective variety, every homomorphism $\Gamma \rightarrow \mathrm{Bir}(X)$ is trivial.*

Proof. A non-trivial homomorphism $\Gamma \rightarrow \mathrm{Bir}(X)$ is an embedding, as Γ is simple. If such an embedding exists, Γ contains non-trivial finite-index subgroups, contradicting the simplicity of Γ . □

8. Birational actions of lattices on quasi-projective varieties

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

8.1. Lattices in higher-rank Lie groups

Let $S \subset \mathrm{GL}_m$ be an algebraic subgroup of GL_m defined over the field of rational numbers \mathbf{Q} (see [9]). We make the following assumptions:

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

We refer to [58], [54, §7.4], and [57] for a good introduction to the following result, and for references to the literature and original contributions.

THEOREM 8.1. *Let S be an algebraic subgroup of GL_m , defined over the field \mathbf{Q} , with the above four properties. Then $S(\mathbf{Z})$ satisfies the strong approximation and congruence subgroup properties.*

This means that the closure of $S(\mathbf{Z})$ has finite index in $\prod_q S(\mathbf{Z}_q)$, and that every finite-index subgroup of $S(\mathbf{Z})$ contains a congruence subgroup $\{B \in S(\mathbf{Z}) : B \equiv \text{Id} \pmod{m}\}$ for some integer m . In other words, the profinite completion of $S(\mathbf{Z})$ coincides with a finite-index subgroup of $\prod_q S(\mathbf{Z}_q)$.

LEMMA 8.2. *Let S be an algebraic subgroup of GL_m defined over \mathbf{Q} , that satisfies the above four properties. If Γ is a finite-index subgroup of $S(\mathbf{Z})$, then $S(\mathbf{Z}_p)$ is a virtual pro- p completion of Γ .*

Proof. (See also §4.2.3.) According to [61] (Theorems 5 and 34, and the corollary to Lemma 64) and to the above Theorem 8.1, there is a prime q_0 such that $S(\mathbf{F}_q)$ is a perfect group and $S(\mathbf{Z})$ is dense in $S(\mathbf{Z}_q)$ for every prime $q \geq q_0$.

Let Γ be a finite-index subgroup of $S(\mathbf{Z})$. Let m be a positive integer such that p divides m , every prime $q < q_0$ divides m , and the congruence subgroup

$$\Gamma_m := \{B \in S(\mathbf{Z}) : B \equiv \text{Id} \pmod{m}\}$$

is contained in Γ . Let F be the set of prime divisors of m .

Denote by G_q the closure of Γ_m in $S(\mathbf{Z}_q)$; the profinite completion of Γ_m is $\prod_q G_q$. The first congruence subgroup of $S(\mathbf{Z}_q)$ is an analytic pro- q group, thus, if $q \in F \setminus \{p\}$, G_q is a pro- q group and every morphism to a p -group is trivial. Similarly, if $q \notin F$, every morphism from $G_q = S(\mathbf{Z}_q)$ to a p -group factors through the quotient $S(\mathbf{F}_q)$, and is trivial because $S(\mathbf{F}_q)$ is perfect. This shows that the pro- p completion of Γ_m is G_p , and that $S(\mathbf{Z}_p)$ is a virtual pro- p completion of Γ . □

8.2. Minimal homogeneous spaces (see [65, p. 187] and [63])

Given a simple complex Lie algebra \mathfrak{s} , one denotes by $\delta(\mathfrak{s})$ the minimal codimension of its proper Lie subalgebras $\mathfrak{p} < \mathfrak{s}$. If S is a complex connected algebraic group with Lie algebra equal to \mathfrak{s} , then $\delta(\mathfrak{s})$ is equal to the minimal dimension $\delta(S)$ of a homogeneous variety $V = S/P$ 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 [65, p. 187]). If \mathfrak{s} (resp. S) is defined over a subfield of \mathbf{C} , we use the same notation $\delta(\mathfrak{s})$ (resp. $\delta(S)$) to denote $\delta(\mathfrak{s} \otimes \mathbf{C})$.

This dimension $\delta(S)$ has been computed for all complex, simple and connected algebraic groups (see [63] for instance). The results are summarized in Table 1, from which one sees that $\delta(\mathfrak{s}) \geq \text{rank}_{\mathbf{C}}(\mathfrak{s})$ with equality if and only if \mathfrak{s} is $\mathfrak{sl}_{\delta(\mathfrak{s})+1}(\mathbf{C})$.

Lie algebra	dimension	dimension of the minimal representation	dimension of the smallest homogeneous space
$\mathfrak{sl}_k(\mathbf{C}), k \geq 2$	$k^2 - 1$	k	$k - 1$
$\mathfrak{so}_k(\mathbf{C}), k \geq 7$	$\frac{1}{2}k(k - 1)$	k	$k - 2$
$\mathfrak{sp}_{2k}(\mathbf{C}), k \geq 2$	$k(2k + 1)$	$2k$	$2k - 1$
$\mathfrak{e}_6(\mathbf{C})$	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

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

Remark 8.3. Here are a few comments on Table 1. The inequality $\delta(\mathfrak{g}) \geq \text{rank}_{\mathbf{C}}(\mathfrak{g})$ may be obtained with the following argument. Choose a maximal torus T in S . Since S is almost simple, T acts on $V = S/P$ with a finite kernel, and hence the isotropy group in T of a general point of V is finite; thus, $\dim(V) \geq \dim(T)$.

The algebra $\mathfrak{sl}_k(\mathbf{C})$ has two representations of minimal dimension (the standard representation on \mathbf{C}^k and its dual); likewise, $\text{SL}_k(\mathbf{C})$ has two minimal homogeneous spaces. (The other simple complex Lie algebras have a unique minimal representation, up to isomorphism).

The group $\text{SO}_5(\mathbf{C})$ is isogenous to $\text{Sp}_4(\mathbf{C})$ 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, $\text{SO}_6(\mathbf{C})$ is isogenous to $\text{SL}_4(\mathbf{C})$ and acts on \mathbb{P}^3 too.

8.3. Proof of Theorem B

Changing S into a finite cover, and Γ into its pre-image under the covering homomorphism, we may assume that the semisimple algebraic group S is simply connected. Identify Γ with its image in $\text{Bir}(X)$, and choose a good p -adic model for (X, Γ) , as in Proposition 3.2.

The group Γ is a lattice in the higher rank, almost simple Lie group $S(\mathbf{R})$. As such, Γ has Kazhdan property (T) (see [40, Chapters 2 and 3]); hence, it has property (τ^∞) .

According to Theorem 7.13, there is a finite-index subgroup Γ_0 in Γ , a field extension K of \mathbf{Q}_p and an analytic polydisk $\mathcal{U} \subset X(K)$ which is Γ_0 -invariant, and on which Γ_0 acts by Tate analytic diffeomorphisms.

We also know from Lemma 8.2 that $\mathbf{S}(\mathbf{Z}_p)$ is a virtual pro- p completion of Γ_0 . By Theorem 2.11, there exists a finite-index subgroup Γ_1 of Γ_0 such that the analytic action of Γ_1 on the polydisk \mathcal{U} extends to an analytic action of its closure $G_1 = \bar{\Gamma}_1$, an open subgroup of the p -adic group $\mathbf{S}(\mathbf{Z}_p)$.

Let o be a point of \mathcal{U} which is not fixed by G_1 ; the stabilizer of o is a closed subgroup P of G_1 : its Lie algebra determines a subalgebra of \mathfrak{s} of codimension at most $\dim(X)$. If $\dim(X) < \delta(\mathbf{S})$, then P is a finite-index subgroup of G_1 , and the action of Γ_1 on X factors through a finite group. Thus,

$$\dim(X) \geq \delta(\mathbf{S}) \geq \text{rank}_{\mathbf{R}}(\mathbf{S}). \tag{8.1}$$

If $\dim(X) = \text{rank}_{\mathbf{R}}(\mathbf{S})$, then $\delta(\mathbf{S}) = \text{rank}_{\mathbf{R}}(\mathbf{S})$ and $\mathfrak{s} = \mathfrak{sl}_n$ with $n = \dim(X) + 1$.

Remark 8.4. The inequality (8.1) is stronger than $\dim(X) \geq \text{rank}_{\mathbf{R}}(\mathbf{S})$. For instance, if Γ is a non-uniform lattice in \mathbf{F}_4 , then Γ does not act faithfully by birational transformations in dimension ≤ 14 .

COROLLARY 8.5. *Let Γ be a finite-index subgroup of $\text{SL}_n(\mathbf{Z})$, with $n \geq 3$. If Γ acts by birational transformations on an irreducible complex projective variety X , then either the image of Γ in $\text{Bir}(X)$ 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. Let Γ_m be a principal congruence subgroup which is contained in Γ , with $m \equiv 0 \pmod{3}$; then Γ_m is torsion-free. The kernel of the action of Γ_m on X is either trivial, or a finite-index subgroup, because every infinite normal subgroup of Γ_m has finite index. Thus, we may now assume that Γ_m acts faithfully on X by birational transformations. Theorem B implies that $\dim(X) \geq n - 1$. In case of equality, there is a good, p -adic model of (X, Γ) such that a finite-index subgroup of Γ preserves a p -adic polydisk and acts by analytic diffeomorphisms on it. Then, Theorem 5.1 shows that there is a birational, Γ -equivariant mapping $\tau: X \dashrightarrow \mathbb{P}^{n-1}$, where the action of Γ on \mathbb{P}^{n-1} is by linear projective automorphisms. □

9. Appendix

9.1. Proof of Proposition 3.2

As explained in §3.1, there exists a subring R of \mathbf{k} , which is finitely generated over \mathbf{Z} , such that X and the birational transformations $s \in S$ are defined over R . This means that there exists a projective scheme $X_R \rightarrow \text{Spec}(R)$ such that $X = X_R \times_{\text{Spec}(R)} \text{Spec}(\mathbf{k})$. Let $\pi: X_R \rightarrow \text{Spec}(R)$ be such a model, with generic fiber X_K (K is the fraction field of R).

LEMMA 9.1. *There exists a non-empty, affine, open subset U of $\text{Spec}(R)$ such that the following conditions are satisfied:*

- (i) U is of finite type over $\text{Spec}(\mathbf{Z})$;
- (ii) for every point $y \in U$, the fiber X_y is absolutely irreducible and

$$\dim_{K(y)} X_y = \dim_K X_K,$$

where $K(y)$ is the residue field at y ;

- (iii) for every $s \in S$ and every $y \in U$, the fiber X_y is not contained in $B_{R,s}$.

Proof. (See [7, Proposition 4.3].) To prove the lemma, we shall use the following fact: For any integral affine scheme $\text{Spec}(A)$ of finite type over $\text{Spec}(\mathbf{Z})$ and any non-empty open subset V_1 of $\text{Spec}(A)$, there exists an affine open subset V_2 of V_1 which is of finite type over $\text{Spec}(\mathbf{Z})$. Indeed, we may pick any non-zero element $f \in I$, where I is the ideal of A that defines the closed subset $\text{Spec}(A) \setminus V$ and set $U := \text{Spec}(A) \setminus \{f=0\}$. Then $U = \text{Spec}(A[1/f])$ is of finite type over $\text{Spec}(\mathbf{Z})$.

Since X_K is absolutely irreducible, [37, Proposition 9.7.8] gives an affine open subset V of $\text{Spec}(R)$ such that X_y is absolutely irreducible for every $y \in V$. We may suppose that V is of finite type over $\text{Spec}(\mathbf{Z})$. By generic flatness (see [37, Theorem 6.9.1]), 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 absolutely 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 complement of the points in X_K around which s is an open immersion. Observe that $B_{K,s}$ is exactly the generic fiber of $\pi|_{B_{R,s}}: B_{R,s} \rightarrow \text{Spec}(R)$. By generic flatness, there exists a non-empty, affine, open subset U_s of V such that the restriction of π to every irreducible component of $(\pi|_{B_{R,s}})^{-1}(U_s)$ is flat. Let U be the intersection of the open subsets U_s , for s in S ; then, shrink U to suppose that U is of finite type over $\text{Spec}(\mathbf{Z})$. Since

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

for every $s \in S$ and $y \in U$, the fiber X_y is not contained in $B_{R,s}$. □

By Lemma 9.1, we may replace $\text{Spec}(R)$ by U and assume that

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

Since R is integral and finitely generated over \mathbf{Z} , by Lemma 3.1 there exist infinitely many primes $p \geq 3$ such that R can be embedded into \mathbf{Z}_p . This induces an embedding $\text{Spec}(\mathbf{Z}_p) \rightarrow \text{Spec}(R)$. Set $X_{\mathbf{Z}_p} := X_R \times_{\text{Spec}(R)} \text{Spec}(\mathbf{Z}_p)$. All fibers X_y , for $y \in \text{Spec}(R)$, are absolutely irreducible and of dimension d ; hence, the special fiber $X_{\mathbf{F}_p}$ of $X_{\mathbf{Z}_p} \rightarrow \text{Spec}(\mathbf{Z}_p)$ is absolutely irreducible and of dimension $d = \dim(X)$. Since $B_{\mathbf{Z}_p,s} \cap X_{\mathbf{F}_p} \subset B_{R,s} \cap X_{\mathbf{F}_p}$ for every $s \in S$, the fiber $X_{\mathbf{F}_p}$ is not contained in $B_{\mathbf{Z}_p,s}$. Thus, $X_{\mathbf{Z}_p}$ provides a good model for (X, Γ) .

9.2. From fixed points to invariant polydisks

We now prove Proposition 3.4; the notation is from §3.2.2. Since X_{O_K} is projective, there exists an embedding $\psi: X_{O_K} \rightarrow \mathbb{P}_{O_K}^N$ defined over O_K . On the projective space $\mathbb{P}^N(K)$, there is a metric dist_p defined by

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

for all points $[x_0 : \dots : x_N], [y_0 : \dots : y_N] \in \mathbb{P}^N(K)$. Via the embedding $\psi|_{X(K)}: X_K(K) \rightarrow \mathbb{P}_K^N$, dist_p restricts to a metric $\text{dist}_{p,\psi}$ on $X_K(K)$. This metric does not depend on the choice of the embedding ψ ; thus, we simply write dist_p instead of $\text{dist}_{p,\psi}$.

LEMMA 9.2. *For $w, z \in X_K(K)$, $\text{dist}_p(w, z) < 1$ if and only if the reductions $r(w)$ and $r(z)$ coincide.*

Proof. Set $\psi(w) = [x_0 : \dots : x_N]$ and $\psi(z) = [y_0 : \dots : y_N]$, where the coordinates x_i and y_i are in O_K and satisfy $\max_i |x_i|_p = \max_i |y_i|_p = 1$. Then,

$$\psi(r(w)) = [\bar{x}_0 : \dots : \bar{x}_N] \quad \text{and} \quad \psi(r(z)) = [\bar{y}_0 : \dots : \bar{y}_N],$$

where \bar{x}_i and \bar{y}_i denote the images of x_i and y_i in the residue field $\mathbf{F} = O_K/\mathfrak{m}_K$. By definition,

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

If $r(w) = r(z)$, we have $\bar{x}_i = \bar{y}_i$ for all indices i ; thus,

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

and $\text{dist}_p(w, z) < 1$. Now, suppose that $r(w) \neq r(z)$. Assume, first, that there exists an index i , say $i=0$, with $\bar{x}_i \bar{y}_i \neq 0$. Replacing each x_j by x_j/x_0 and each y_j by y_j/y_0 , we get $x_0=y_0=1$. Since $r(w) \neq r(z)$, there exists $j \geq 1$ with $\bar{x}_j \neq \bar{y}_j$. It follows that

$$\text{dist}_p(w, z) \geq |x_j y_0 - x_0 y_j|_p = |x_j - y_j|_p = 1.$$

To conclude, suppose that $\bar{x}_i \bar{y}_i = 0$ for all $i \in \{0, \dots, N\}$. Pick two indices i and j such that $\bar{x}_i \neq 0$ and $\bar{y}_j \neq 0$; thus, $\bar{y}_i = 0$ and $\bar{x}_j = 0$, and $\text{dist}_p(w, z) \geq |x_i y_j - x_j y_i|_p = 1$. \square

Recall that x is a smooth point in $X(\mathbf{F})$ and \mathcal{V} is the open subset of $X_K(K)$ consisting of points $z \in X_K(K)$ satisfying $r(z) = x$. With suitable homogeneous coordinates, x is the point $[1:0:\dots:0] \in \mathbb{P}_{\mathbf{F}}^N$. Then, the open set \mathcal{V} is contained in the unit polydisk

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

Recall from §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 $O_K\langle \mathbf{x}_1, \dots, \mathbf{x}_d \rangle$, such that

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

PROPOSITION 9.3. *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 $\mathbb{A}_{O_K}^N \rightarrow \mathbb{P}_{O_K}^N$ defined by $z_0 \neq 0$. Both x and B are contained in $\mathbb{A}_{O_K}^N$. Since X_{O_K} is smooth at x , we know that there are polynomial functions $G_j \in O_K[z_1, \dots, z_N]$, $1 \leq j \leq N-d$, such that

- X is locally defined by the equations $G_1 = \dots = G_{N-d} = 0$; in particular,

$$\mathcal{V} = X_K(K) \cap B = \{z \in B : G_i(z) = 0 \text{ for all } i = 1, \dots, N-d\};$$

- the rank of the matrix $(\partial_{z_j} \bar{G}_i(0))_{i \leq N-d, j \leq N}$ is $N-d$, where $\bar{G}_i = G_i$ modulo $\mathfrak{m}_K O_K[z_1, \dots, z_N]$.

Permuting the coordinates z_1, \dots, z_N , we may suppose that the determinant of the matrix $(\partial_{z_j} \bar{G}_i(0))_{i, j \leq N-d}$ is different from zero in \mathbf{F} . Denote by $\pi: B \rightarrow (O_K)^d$ the projection $[1:z_1:\dots:z_N] \mapsto (z_1, \dots, z_d)$. By Hensel's lemma, there exists a unique analytic diffeomorphism $\varphi: (O_K)^d \rightarrow \mathcal{V}$ such that $G_i((z, \varphi(z))) = 0$ for all $i \leq N-d$. \square

Let f be a birational map in $\text{Bir}(X_{O_K})$ 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 of f on \mathcal{V} is conjugate, via φ , to an analytic diffeomorphism on the polydisk \mathcal{U} . This concludes the proof of Proposition 3.4.

References

- [1] BASS, H. & LUBOTZKY, A., Automorphisms of groups and of schemes of finite type. *Israel J. Math.*, 44 (1983), 1–22.
- [2] BASS, H., MILNOR, J. & SERRE, J. P., Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$). *Inst. Hautes Études Sci. Publ. Math.*, 33 (1967), 59–137.
- [3] BEDFORD, E., LYUBICH, M. & SMILLIE, J., Polynomial diffeomorphisms of \mathbf{C}^2 . IV. The measure of maximal entropy and laminar currents. *Invent. Math.*, 112 (1993), 77–125.
- [4] BEKKA, B., DE LA HARPE, P. & VALETTE, A., *Kazhdan's property (T)*. New Mathematical Monographs, 11. Cambridge Univ. Press, Cambridge, 2008.
- [5] BEKKA, B. & OLIVIER, B., On groups with property (T_{ℓ_p}) . *J. Funct. Anal.*, 267 (2014), 643–659.
- [6] BELL, J. P., A generalised Skolem–Mahler–Lech theorem for affine varieties. *J. London Math. Soc.*, 73 (2006), 367–379.
- [7] BELL, J. P., GHIOCA, D. & TUCKER, T. J., The dynamical Mordell–Lang problem for étale maps. *Amer. J. Math.*, 132 (2010), 1655–1675.
- [8] BOREL, A., *Introduction aux Groupes Arithmétiques*. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris, 1969.
- [9] — *Linear Algebraic Groups*. Graduate Texts in Mathematics, 126. Springer, New York, 1991.
- [10] BOURBAKI, N., *Lie Groups and Lie Algebras*. Chapters 1–3. Elements of Mathematics (Berlin). Springer, Berlin–Heidelberg, 1998.
- [11] CANTAT, S., Version kählérienne d'une conjecture de Robert J. Zimmer. *Ann. Sci. École Norm. Sup.*, 37 (2004), 759–768.
- [12] — Invariant hypersurfaces in holomorphic dynamics. *Math. Res. Lett.*, 17 (2010), 833–841.
- [13] — Sur les groupes de transformations birationnelles des surfaces. *Ann. of Math.*, 174 (2011), 299–340.
- [14] — The Cremona group in two variables. *European Congress of Mathematics*, VI (2012), 211–225.
- [15] — Morphisms between Cremona groups, and characterization of rational varieties. *Compos. Math.*, 150 (2014), 1107–1124.
- [16] CANTAT, S. & DOLGACHEV, I., Rational surfaces with a large group of automorphisms. *J. Amer. Math. Soc.*, 25 (2012), 863–905.
- [17] CANTAT, S. & LAMY, S., Groupes d'automorphismes polynomiaux du plan. *Geom. Dedicata*, 123 (2006), 201–221.
- [18] CANTAT, S. & XIE, J., Algebraic actions of discrete groups: the p -adic method (expanded version). Preprint, 2018. Available at <http://perso.univ-rennes1.fr/serge.cantat/publications.html>.
- [19] CANTAT, S. & ZEGHIB, A., Holomorphic actions, Kummer examples, and Zimmer program. *Ann. Sci. Éc. Norm. Supér.*, 45 (2012), 447–489.
- [20] CAPRACE, P. E. & RÉMY, B., Simplicity and superrigidity of twin building lattices. *Invent. Math.*, 176 (2009), 169–221.
- [21] CORNULIER, Y., Sofic profile and computability of Cremona groups. *Michigan Math. J.*, 62 (2013), 823–841.
- [22] — Irreducible lattices, invariant means, and commensurating actions. *Math. Z.*, 279 (2015), 1–26.
- [23] COSSEC, F. R. & DOLGACHEV, I. V., *Enriques Surfaces*. I. Progress in Mathematics, 76. Birkhäuser, Boston, MA, 1989.

- [24] COULHON, T. & SALOFF-COSTE, L., Isopérimétrie pour les groupes et les variétés. *Rev. Mat. Iberoamericana*, 9 (1993), 293–314.
- [25] DELIGNE, P., Extensions centrales non résiduellement finies de groupes arithmétiques. *C. R. Acad. Sci. Paris Sér. A-B*, 287 (1978), A203–A208.
- [26] DÉSERTE, J., Groupe de Cremona et dynamique complexe: une approche de la conjecture de Zimmer. *Int. Math. Res. Not.*, 2006 (2006), Art. ID 71701, 27 pp.
- [27] — Sur le groupe des automorphismes polynomiaux du plan affine. *J. Algebra*, 297 (2006), 584–599.
- [28] DIXON, J. D., DU SAUTOY, M. P. F., MANN, A. & SEGAL, D., *Analytic Pro- p Groups*. Cambridge Studies in Advanced Mathematics, 61. Cambridge Univ. Press, Cambridge, 1999.
- [29] EPSTEIN, D. B. A. & THURSTON, W. P., Transformation groups and natural bundles. *Proc. London Math. Soc.*, 38 (1979), 219–236.
- [30] ERSHOV, M., Golod–Shafarevich groups with property (T) and Kac–Moody groups. *Duke Math. J.*, 145 (2008), 309–339.
- [31] FARB, B. & MARGALIT, D., *A Primer on Mapping Class Groups*. Princeton Mathematical Series, 49. Princeton Univ. Press, Princeton, NJ, 2012.
- [32] FISHER, D., Groups acting on manifolds: around the Zimmer program, in *Geometry, Rigidity, and Group Actions*, Chicago Lectures in Math., pp. 72–157. Univ. Chicago Press, Chicago, IL, 2011.
- [33] FORMANEK, E. & PROCESI, C., The automorphism group of a free group is not linear. *J. Algebra*, 149 (1992), 494–499.
- [34] FRIEDLAND, S. & MILNOR, J., Dynamical properties of plane polynomial automorphisms. *Ergodic Theory Dynam. Systems*, 9 (1989), 67–99.
- [35] GLASNER, Y. & MONOD, N., Amenable actions, free products and a fixed point property. *Bull. Lond. Math. Soc.*, 39 (2007), 138–150.
- [36] GREENBERG, L., Maximal groups and signatures, in *Discontinuous Groups and Riemann Surfaces* (Univ. Maryland, College Park, MD, 1973), Ann. of Math. Studies, 79, pp. 207–226. Princeton Univ. Press, Princeton, NJ, 1974.
- [37] GROTHENDIECK, A., Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, 32 (1967), 361.
- [38] GROTHENDIECK, A. & DIEUDONNÉ, J. A., *Éléments de Géométrie Algébrique*. I. Grundlehren der Mathematischen Wissenschaften, 166. Springer, Berlin–Heidelberg, 1971.
- [39] DE LA HARPE, P., *Topics in Geometric Group Theory*. Chicago Lectures in Mathematics. Univ. of Chicago Press, Chicago, IL, 2000.
- [40] DE LA HARPE, P. & VALETTE, A., La propriété (T) de Kazhdan pour les groupes localement compacts. *Astérisque*, 175 (1989), 158 pp.
- [41] HRUSHOVSKI, E., The elementary theory of the Frobenius automorphism. Preprint, 2004. [arXiv:math/0406514](https://arxiv.org/abs/math/0406514) [[math.LO](https://arxiv.org/abs/math/0406514)].
- [42] IVANOV, N. V., *Subgroups of Teichmüller Modular Groups*. Translations of Mathematical Monographs, 115. Amer. Math. Soc., Providence, RI, 1992.
- [43] KNESER, M., Normalteiler ganzzahliger Spingruppen. *J. Reine Angew. Math.*, 311/312 (1979), 191–214.
- [44] KOBLITZ, N., *p -adic Numbers, p -adic Analysis, and Zeta-Functions*. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984.
- [45] KRAFT, H. & STAMPFLI, I., On automorphisms of the affine Cremona group. *Ann. Inst. Fourier (Grenoble)*, 63 (2013), 1137–1148.

- [46] LANG, S. & WEIL, A., Number of points of varieties in finite fields. *Amer. J. Math.*, 76 (1954), 819–827.
- [47] LAZARD, M., Groupes analytiques p -adiques. *Inst. Hautes Études Sci. Publ. Math.*, (1965), 389–603.
- [48] LECH, C., A note on recurring series. *Ark. Mat.*, 2 (1953), 417–421.
- [49] LUBOTZKY, A., *Discrete Groups, Expanding Graphs and Invariant Measures*. Progress in Mathematics, 125. Birkhäuser, Basel, 1994.
- [50] MACBEATH, A. M. & SINGERMAN, D., Spaces of subgroups and Teichmüller space. *Proc. London Math. Soc.*, 31 (1975), 211–256.
- [51] MARGULIS, G. A., *Discrete Subgroups of Semisimple Lie Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete, 17. Springer-Verlag, Berlin, 1991.
- [52] MCCARTHY, J., Normalizers and centralizers of pseudo-Anosov mapping classes. Preprint, 1982. Revised version, 1994. Available at <http://users.math.msu.edu/users/mccarthy/publications/normcent.pdf>.
- [53] MILLSON, J. J., Real vector bundles with discrete structure group. *Topology*, 18 (1979), 83–89.
- [54] PLATONOV, V. & RAPINCHUK, A., *Algebraic Groups and Number Theory*. Pure and Applied Mathematics, 139. Academic Press, Boston, MA, 1994.
- [55] POONEN, B., p -adic interpolation of iterates. *Bull. Lond. Math. Soc.*, 46 (2014), 525–527.
- [56] RAGHUNATHAN, M. S., Torsion in cocompact lattices in coverings of $\text{Spin}(2, n)$. *Math. Ann.*, 266 (1984), 403–419. Correction in *Math. Ann.*, 303 (1995), 575–578.
- [57] — The congruence subgroup problem, in *Proceedings of the Hyderabad Conference on Algebraic Groups* (Hyderabad, 1989), pp. 465–494. Manoj Prakashan, Madras, 1991.
- [58] RAPINCHUK, A. S., Strong approximation for algebraic groups, in *Thin Groups and Superstrong Approximation*, Math. Sci. Res. Inst. Publ., 61, pp. 269–298. Cambridge Univ. Press, Cambridge, 2014.
- [59] ROBERT, A. M., *A Course in p -adic Analysis*. Graduate Texts in Mathematics, 198. Springer-Verlag, New York, 2000.
- [60] SERRE, J. P., *Lie Algebras and Lie Groups*. Lecture Notes in Mathematics, 1500. Springer-Verlag, Berlin, 2006.
- [61] STEINBERG, R., *Lectures on Chevalley Groups*. Yale Univ., New Haven, CT, 1968.
- [62] — Some consequences of the elementary relations in SL_n , in *Finite Groups—Coming of Age* (Montreal, QC, 1982), *Contemp. Math.*, 45, pp. 335–350. Amer. Math. Soc., Providence, RI, 1985.
- [63] STUCK, G., Low-dimensional actions of semisimple groups. *Israel J. Math.*, 76 (1991), 27–71.
- [64] TOMANOV, G., On the congruence-subgroup problem for some anisotropic algebraic groups over number fields. *J. Reine Angew. Math.*, 402 (1989), 138–152.
- [65] VINBERG, È. B. (ED.), *Lie Groups and Lie Algebras*, III. Encyclopaedia of Mathematical Sciences, 41. Springer, Berlin–Heidelberg, 1994.
- [66] WEIL, A., On algebraic groups of transformations. *Amer. J. Math.*, 77 (1955), 355–391.
- [67] ZIMMER, R. J., Actions of semisimple groups and discrete subgroups, in *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Berkeley, CA, 1986), pp. 1247–1258. Amer. Math. Soc., Providence, RI, 1987.
- [68] — Lattices in semisimple groups and invariant geometric structures on compact manifolds, in *Discrete Groups in Geometry and Analysis* (New Haven, CT, 1984), *Progr. Math.*, 67, pp. 152–210. Birkhäuser, Boston, MA, 1987.

SERGE CANTAT

Institut de recherche mathématique de Rennes

Université de Rennes 1

Beaulieu – Bâtiment 22–23

263, avenue du Général Leclerc

FR-35042 Rennes Cedex

France

serge.cantat@univ-rennes1.fr

JUNYI XIE

Institut de recherche mathématique de Rennes

Université de Rennes 1

Beaulieu – Bâtiment 22–23

263, avenue du Général Leclerc

FR-35042 Rennes Cedex

France

junyi.xie@univ-rennes1.fr

Received July 7, 2015

Received in revised form February 3, 2018