yGGT IX Notes

February 28, 2020

Serge CANTAT: Groups of polynomial transformations

0.1 Affine space and its automorphisms

k is a field (any field, not neccessarily algebraically closed or of characteristic 0.)

$\mathbb{A}^m_k$ is the affine space over k

$(x_1, x_2, \ldots, x_m)$ = the standard affine coordinates

From time to time, may distinguish between affine space and points in it:

$\mathbb{A}^m(S)$ = points with coordinates in S, where S is e.g. a subset of k, or sometimes e.g. an extension of k

e.g. given $\mathbb{A}^m_{\mathbb{Q}}$, can look at $\mathbb{A}^m(\mathbb{Z}) \cong \mathbb{Z}^m$, or $\mathbb{A}^m(\mathbb{C}) \cong \mathbb{C}^m$.

$\mathrm{End}(\mathbb{A}^m_k)$ = polynomial transformations $f : \mathbb{A}^m \to \mathbb{A}^m$

In coordinates, defined by m polynomials: $f(x_1, \ldots, _m) = (f_1, \ldots, f_m)$ where $f_i \in k[x_1, \ldots, x_m]$; group law is just composition of maps ($f, g \in \mathrm{End}(AA^m_k)$: $f \circ g = (f_1(g_1, \ldots, g_m), \ldots)$.)

$\mathrm{Aut}(\mathbb{A}^m_k)$ = invertible elements in $\mathrm{End}(\mathbb{A}^m_k)$= group of **automorphisms** of $\mathbb{A}^m$ defined over k

"Leitmotif": take properties of linear group $\mathrm{GL}_n\, k$, decide if they are satisfied by $\mathrm{Aut}(\mathbb{A}^m_k)$.

Example 0.1. For all m, $\mathrm{Aff}_m(k)$ = affine transformations = $\mathrm{GL}_m(k) \ltimes k^m$ where $k^m = \mathbb{A}^m_k$ acts by transformations.

$((x_1, \ldots, x_m) \mapsto L(x_1, \ldots, x_m) + t) \subset \mathrm{Aut}(\mathbb{A}^m_k)$.

Exercise. $\mathrm{Aut}(\mathbb{A}^1_k) = \mathrm{Aff}_1(k)$.

Proof. Given $f \in \mathrm{Aut}(\mathbb{A}^1_k)$, $f(x_1) \in k[x_1]$; $f^{-1}(x_1) \in k[x_1]$.

$f \circ f^{-1}(x_1) = x_1$.

$\deg(f) \cdot \deg(f^{-1}) = 1$, so $\deg(f) = 1$, i.e. $x = ax_1 + b \in \mathrm{Aff}_1(k)$ □

0.2 Dimension 2

Example 0.2. $h \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + p(x_2) \\ bx_2 + c \end{pmatrix}$

where $p \in k[x_2]$, $a, b, c \in k$, $ab \neq 0$

$h^{-1} = \begin{pmatrix} *x_1 - p(x_2) \\ *x_2 + * \end{pmatrix}$

The set of all such transformations is called the **elementary subgroup**

$$E = \left\{ h \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + p(x_2) \\ bx_2 + c \end{pmatrix} \right\}$$

This is an infinite-dimensional group (we need as many parameters as are needed to describe polynomials in one variable ...)

The **degree** of an endomorphism $f(x_1, \dots, x_m) = (f_1, \dots, f_m)$:

Given $\varphi \in k[x_1, \dots, x_m]$, write $\varphi(\underline{x}) = \sum_{j=0}^{+\infty} \varphi_j(\underline{x})$ where φ_j is a homogeneous polynomial function of degree j. Then $\deg(\varphi) = \max\{j : \varphi_j \neq 0\}$.

Example 0.3. For $\varphi(x_1, x_2, x_3) = x_1 + 2x_2x_3^4 + x_2^2 + x_1x_3$, $\varphi_1 = x_1$, $\varphi_2 = x_2^2 + x_1x_3$, and $\varphi_5 = 2x_2x_3^4$, so $\deg \varphi = 5$

$\deg(f) = \max_{i=1,\dots,m} \deg(f_i)$.

Geometric interpretation: take a generic affine hyperplane $H \subset \mathbb{A}_k^m$, take a generic (affine) line $L \subset \mathbb{A}_k^m$, count number of points in $f^{-1}(H) \cap L$ over $\bar{k}$ the algebraic closure of k

Exercise. If $h_1, h_2 \in E$, then $\deg(h_1 \circ h_2) \leq \max(\deg h_1, \deg h_2)$.

Two new phenomenon starting from dimension 2: group is now infinite-dimensional; degree is now only sub-multiplicative, not multiplicative.

Theorem 0.4 (Jung, van der Kulk 1942)**.** *The group* $\mathrm{Aut}(\mathbb{A}_k^2)$ *is the free product of* $A = \mathrm{Aff}_2(k)$ *and* E *amalgamated along their intersection* $S = A \cap E$

$S = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto L \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} s \\ t \end{pmatrix}$ *where* $L \in \mathrm{GL}_2(k)$ *is upper-triangular.*

Note it is specific to dimension 2 (and hard; requires algebraic geometry) that A and E generate $\mathrm{Aut}(\mathbb{A}_k^2)$.

Proof of free product with amalgamation. For every $h \in \mathrm{Aut}(\mathbb{A}_k^2) \setminus S$, there exist $g_1, \dots, g_n \in (A \cup E) \setminus S$ such that $h = g_n \circ \cdots \circ g_1$ and two consecutive g_i, g_{i+1} are in distinct subgroups A, E. Call this a reduced word (or composition)

To show that we have a free product with amalgamation, it suffices to show that any such reduced word / composition is not $\mathrm{id}_{\mathbb{A}^2}$. In fact, we will show

Proposition 0.5. *The degree of a reduced word* $h = g_n \circ \cdots \circ g_1$ *is* $\deg(h) = \prod_{i=1}^n \deg(g_i)$.

To prove this formula: write e.g $h = a_n \cdots e_3 \circ a_2 \circ e_2 \circ a_1 \circ e_1$ where $a_i \in A \setminus S$ and $e_i \in E \setminus S$.

$\deg a_i = 1$, so it suffices to show $\deg(h) = \prod \deg(e_i)$.

Remark 0.6. Every element of $A \setminus S$ can be written as $s_1 \circ t \circ s_2$ where $s_i \in S$ and $t \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$. $S \circ t \circ S = A \setminus S$.

Hence we can write $h = \cdots e_3' \circ t \circ e_2' \circ t \circ e_1'$ where $\deg(e_i') = \deg(e_i)$ (since e_i' is the composition of e_i with one or two affine maps.)

Now $e_1' \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1x_1 + p_1(x_2) \\ b_1x_2 + c_1 \end{pmatrix} \in E \setminus S$; $\deg(e_1') = \deg(p_1)$

$t \circ e_1' = \begin{pmatrix} b_1x_2 + c_1 \\ a_1x_1 + p_1(x_2) \end{pmatrix} = \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}$; highest degree term is a monomial in x_2.

$e_2'(t \circ e_1') = \begin{pmatrix} \text{linear} + p_2(Q_1) \\ \text{linear} + * \end{pmatrix}$; the leading terms are in $p_2(Q_1) = p_2(a_1x_1 + p_1(x_2))$, which has degree $\deg(p_2) \cdot \deg(Q_1) = \deg(e_2') \cdot \deg(e_1')$.

$t \circ e_2' \circ t \circ e_1' = \begin{pmatrix} P_2 \\ Q_2 \end{pmatrix}$; now argue by recursion (induction?) □

"When you study these things you have to do these [computations] every day."

Theorem 0.7 (S. Lamy)**.** *The group* $\mathrm{Aut}(\mathbb{A}^2_{\mathbb{C}})$ *satisfies the Tits alternative: if* $\Gamma < \mathrm{Aut}(\mathbb{A}^2_{\mathbb{C}})$ *is finitely generated, then either* Γ *contains a finite-index solvable subgroup, or* Γ *contains a non-abelian free group*

(Proof uses ping-pong by considering action on tree coming from Bass–Serre theory, since we do have a free product with amalgamation)

Question: What about the Tits alternative for $\mathrm{Aut}(\mathbb{A}^m_k)$, $m \geq 3$?

Note that such a result will have, as corollaries, the Tits alternative for $\mathrm{Out}(\mathbb{F}_n)$ (still an open question) and for $MCG(\Sigma_g)$ (known to be true.)

0.3 Degree growth

Proposition 0.8 (Exercise)**.** *If* $h \in \mathrm{Aut}(\mathbb{A}^2_k)$*, then either* $n \mapsto \deg(h^n)$ *is bounded, or* $n \mapsto \deg(h^n)$ *grows like* λ^n *for some integer* $\lambda > 1$.

Example 0.9. $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \overset{h}{\mapsto} \begin{pmatrix} x_2 \\ x_1 + x_2^2 \end{pmatrix}$

$\deg(h^n) = 2^n$.

Question: what kinds of sequences can we get by looking at $n \mapsto \deg(f^n)$ for $f \in \mathrm{Aut}(\mathbb{A}^m_k)$?

Can we get intermediate growth? Polynomial growth (of arbitrarily large degree)?

Have examples of exponential, bounded, linear growth; in general more mysterious.

Can ask same question for $f \in \mathrm{End}(\mathbb{A}^m_k)$.

Example 0.10. $m = 3$: consider the surface x_D defined by $x_1^2 + x_2^2 + x_3^2 = x_1x_2x_3 + D$ where $D \in k$

(A representation variety of $\mathbb{F}_2$ in $\mathrm{SL}_2\,\mathbb{C}$, D is related to the trace of [a distinguished element / the commutator of the generators].)

The equation is cubic; in any fixed variable, it is quadratic.

Consider the polynomial transformation

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \overset{\sigma_3}{\mapsto} \begin{pmatrix} x_1 \\ x_2 \\ x_3' \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_1x_2 - x_3 \end{pmatrix}.$$

Affine space is foliated by such surfaces; σ_3 is a polynomial map which preserves these foliations.

Can analogously define σ_1, σ_2; $\deg\left((\sigma_2 \circ \sigma_3)^n\right) \sigma n$; $\deg\left((\sigma_1 \circ \sigma_2 \circ \sigma_3)^n\right) \sim \lambda^n$ where $\lambda = \frac{1+\sqrt{5}}{2}$.

Not known if we can find unbounded sequences with sublinear growth. Some evidence to suggest "no":

Theorem 0.11 (C. Urech)**.** *Let $h \in \mathrm{Aut}(\mathbb{A}^m_k)$. If $n \mapsto \deg(h^n)$ is not bounded then*

$$\max_{j=0,\dots,n} \deg(h^j) \geq C_m n^{1/m}$$

where $C_m > 0$ is a constant depending only on dimension m.

Proof. (1) Look at $\mathrm{End}_{\leq d}(\mathbb{A}^m_k)$, i.e. endomorphisms defined by formulas of degree d. This is a k-vector space, of dimension $m \times \dim(k_{\leq d}[x_1, \cdots x_m]) = m \cdot \binom{m+d}{m} \sim m^{m+1}$ (have a basis formed by monomials of the form $x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m}$ where $i_0 + \dots i_m = d$.)

(2) Given $h \in \mathrm{End}(\mathbb{A}^m)$; assume linear relation among the iterates, e.g. $h^5 = h^3 - 2h + \mathrm{id}$. Compose on the right with h^n: get (in our example) $h^{5+n} = h^{3+n} - 2h^{1+n} + h^n$; replacing any terms with degree ≥ 5, get $h = \sum_{j=0}^4 a_j h^j$ where $a_j \in k$. The degree is hence uniformly bounded by $\max_{j=0,\dots,4} \deg h^j$.

(3) Put step (1) and (2) together: $D_h(n) = \deg_{j=0,\dots,n} \deg(h^j)$. If $n+1 \geq m \cdot \binom{m+D_h(n)}{m}$ ("too many iterates of small degree"), then have a linear relation among the iterates, and hence bounded degree growth. Otherwise have growth of $\sim m \cdot \binom{m+d}{m} \leq \frac{(m+d)^m}{(m-1)!} \sim d^m$. □

0.4 Finite subgroups

Proposition 0.12. *If G is a finite subgroup of $\mathrm{Aut}(\mathbb{A}^2_k)$, then*

(1) G is conjugate to a subgroup of $\mathrm{Aff}_2(k)$ or E

(2) If k has characteristic 0, then G is conjugate to a subgroup of $\mathrm{GL}_2(k)$.

Can prove by looking at action on a tree, using Bass–Serre theory.

Now for the main content of lectures: to prove results about polynomial transformation groups by changing field of definition. Start with finite fields or p-adics ...

0.4.1 Fixed-point theorem

Theorem 0.13. *Let G be a subgroup of $\mathrm{Aut}(\mathbb{A}^m_k)$ such that*

(i) G is a p-group, i.e. $\#G = p^r$ for some $r \geq 1$, p prime

(ii) $\mathrm{char}(k) \neq p$, k algebraically closed.

Then G has a fixed point.

Consequences: if G fixes the origin 0, consider

$$\Phi = \sum_{g \in G} (Dg)_0^{-1} \circ g \in \mathrm{End}(\mathbb{A}^m_k)$$

where the differential $Dg \in \mathrm{GL}_m(k)$; $(D\Phi)_0 = (\#G)\,\mathrm{id} \in \mathrm{GL}_m(k)$.

$\Phi \circ h = (Dh)_0 \circ \Phi$ for all $h \in G$.

Corollary 0.14. *$G \ni g \mapsto (Dg)_0 \in \mathrm{GL}_m(k)$ is injective.*

Theorem 0.15 (Minkowski, Abboud)**.** *Set* $\mathrm{Mink}(m,\ell) = \lfloor \frac{m}{l-1} \rfloor + \lfloor \frac{m}{l(l-1)} \rfloor + \cdots + \lfloor ml^j(l-1) \rfloor + \cdots \in \mathbb{Z}$ *(a finite sum of integers.)*

If G is a p-group in $\mathrm{GL}_m(\mathbb{Q})$ (Minkowski) or $\mathrm{Aut}(\mathbb{A}^M_{\mathbb{Q}})$ (Abboud—combining ideas in proof of fixed-point theorem above and of Minkowski), $\#G = p^r$ where $r \leq \mathrm{Mink}(m,p)$; this upper bound is optimal.

Aside: character variety

$Rep(F_2, \mathrm{SL}_2\, k) = \mathrm{SL}_2\, k \times \mathrm{SL}_2\, k$

$\mathrm{Aut}(F_2)$ acts on this representation space by $\varphi \cdot \rho = \rho \circ (\varphi^{-1})$.

$\chi(F_2, \mathrm{SL}_2)$ = rep / conjugacy in SL_2

Outer automorphisms of F_2 act on χ

$\chi = \mathbb{A}^3_k$: $(x_1, x_2, x_3) = (\mathrm{tr}A, \mathrm{tr}B, \mathrm{tr}AB)$.

Finite subgroups, continued

Theorem 0.16. *1. $\#G = p^r$, $G \subset \mathrm{Aut}(\mathbb{A}^m_k)$, $p \wedge \mathrm{char}(k) = 1$ ($\mathrm{char}(k) = 0$ or q, $q \neq p$)*

k is algebraically closed, or k is finite.

$\implies$ G has a fixed point in $\mathbb{A}^m_k$

Proof. Assume k is finite: $k = \mathbb{F}_{q^s}$ for some prime $q \neq p$ and some $s \geq 1$.

Every orbit of G in $\mathbb{A}^m_k$ has either 1 element (a fixed point) or a number of elements divisible by p (by the orbit-stabilizer theorem) ... and p does not divide q.

Remark 0.17. $\mathrm{Aut}(A^m_k)$, when $m \geq 2$, is infinite-dimensional even if $\mathbb{A}^m(k)$ may be finite (!)

e.g. always have $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_2^d \\ x_2 \end{pmatrix}$—some of these coincide as permutations of $\mathbb{A}^m_k$ for k finite, but they are still different transformations (and stop coinciding when we change the field of definition.)

2. k algebraically closed (e.g. $k = \mathbb{C}$.) Equations for fixed points given by $g(\underline{x}) = \underline{x}$ for all $g \in G$. Writing this out more fully, for $g = (g_1, \ldots, g_m)$,

$$\begin{aligned} g_1(x_1, \ldots, x_m) - x_1 &= 0 \\ &\vdots \\ g_m(x_1, \ldots, x_m) - x_m &= 0 \end{aligned}$$

If there is no fixed point, this system of equations has no solution.

Hilbert Nullstellensatz ("if there is no solution, there is a good reason why there is no solution"): $\exists$ polynomial functions $Q_{g,i} \in k[x_1, \ldots, x_m]$ for $g \in G$, $1 \leq i \leq m$ s.t.

$$\sum_{\substack{g \in G \\ 1 \leq i \leq m}} (g_i - x_i) Q_{g,i}(\underline{x}) = 1. \tag{1}$$

Let $A \subset k$ be the algebra (over $\mathbb{Z}$) generated by the coefficients in (1) and $\frac{1}{p}$.

Theorem 0.18. *Let A be a finitely-generated algebra over $\mathbb{Z}$. Then A has a maximal ideal, and for every maximal ideal $\mathfrak{m}$, the quotient field $A/\mathfrak{m}$ is finite.*

Reduce everything modulo a maximal ideal $\mathfrak{m}$.

Write $\bar{g} = g$ with coefficients in $A/\mathfrak{m}$,

similarly $\bar{Q}_{g,i} = Q_{g,i}$ reduced modulo $\mathfrak{m}$.

(1) continues to hold modulo $\mathfrak{m}$, so $\bar{G}$ has no fixed point in $\mathbb{A}^m(A/\mathfrak{m})$, where $A/\mathfrak{m}$ is a finite field.

But $\frac{1}{p} \in A$ so $p \neq \mathrm{char}(A/\mathfrak{m})$. Here we get a contradiction with step 1. □

0.5 Bell's Theorem

0.5.1 Newton's algorithm for interpolation

- $\mu(n)$ a sequence of (complex) numbers
- Look for $P \in \mathbb{C}[t]$ s.t. $P(j) = \mu(j)$ for $0 \leq j \leq d$, $\deg P = d$s
- Introduce the difference operator Δ defined by

$$(\Delta\mu)(n) = \mu(n+1) - \mu(n)$$

$(\Delta\mu) = (\mu(1) - \mu(0), \mu(2) - \mu(1), \dots)$; $(\Delta^2\mu)(0) = \mu(2) - 2\mu(1) + \mu(0)$; $(\Delta^3\mu)(0) = \mu(3) - 3\mu(2) + 3\mu(1) - \mu(0)$, .., $(\Delta^j\mu)(0) = \sum_l (-1)^{j-l}\binom{j}{l}\mu(l)$.

Theorem 0.19. *The polynomial function P is equal to*

$$P(t) = \sum_{j=0}^{d} (\Delta^j\mu)\binom{t}{j}$$

where $\binom{t}{j} = \frac{t(t-1)\cdots(t-j+1)}{j!}$

Sketch of proof. (1) The functions $\binom{t}{j}$ (for $0 \leq j \leq d$) form a basis of $\mathbb{C}[t]$ ($\mathbb{C}[t]_{\leq d}$, resp.)

(2) $\Delta\binom{t}{j} = \binom{t+1}{j} - \binom{t}{j} = \binom{t}{j-1}$ (Pascal)

(3) Write P as a linear combination $\sum_j A_j\binom{t}{j}$. It remains to show $A_j = (\Delta^j\mu)(0)$. Observe that $P(0) = A_0 = \mu(0) = (\Delta^0\mu)(0)$; by (2) $A_1 = (\Delta\mu)(0)$, and so on. □

0.5.2 p-adic numbers

- $\mathbb{Z}^\times \ni a = p^r \times a'$ where a' is not divisible by p ($p \wedge a' = 1$)

  $|a|_p := p^{-r}$.
- Suppose $a = p^r a'$, $b = p^s b'$, $s \geq r$.

  $a + b = p^r(a' + p^{s-r}b')$.

  If $s > r$, then $(a' + p^{s-r}b') \wedge p = 1$, $\implies$ $|a+b|_p = p^{-r}$.

  If $s = r$, $|a+b|_p \leq p^{-r}$ (with equality if $(a' + b') \wedge p = 1$.)

$|a+b|_p \leq \max(|a|_p, |b|_p)$, with equality if $|a|_p \neq |b|_p$ (the ultrametric property).

- Extend $|\cdot|_p$ to $\mathbb{Q}$ by $|0|_p = 0$, $\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p}$
- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for this absolute value.

  Get $(\mathbb{Q}_p, |\cdot|_p)$ where $|\cdot|_p : \mathbb{Q}_p \to p^{\mathbb{Z}} \cup \{0\}$.

Example 0.20. $p = 5$, $a = 137$.

$|a|_5 = 1$ ... but this is not so descriptive. Instead, write:

$a = 2 + 135 = 2 + 2 \cdot 5 + 5^3$.

$|2|_5 = 1$, $|2 \cdot 5|_5 = \frac{1}{5}$, $|5^3|_5 = \frac{1}{125}$.

$\mathbb{Z}_p \subset \mathbb{Q}_p$ is the closure (for the p-adic topology) of $\mathbb{Z}$ in $\mathbb{Q}_p$.

Exercise.

- Every $x \in \mathbb{Z}_p$ can be written in a unique way $x = \sum_{k=0}^{+\infty} a_k p^k$ with $a_k \in \{0, 1, \ldots, p-1\}$
- $\mathbb{Z}_p$ is the unit disk in $\mathbb{Q}_p$, i.e. it is $\{x \in \mathbb{Q}_p : |x|_p = 1\}$.

  It is the valuation ring (in particular, it is a ring—this is related to the ultrametric property.)

  It contains a unique maximal ideal $p\mathbb{Z}_p$ = disk of radius $\frac{1}{p}$, and $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Let $\mu : \mathbb{Z} \to \mathbb{Z}_p$ be uniformly continuous (w.r.t. p-adic topology on both sides), i.e $\forall r > 0$, $\exists s > 0$ s.t if p^s divides $m - n$, then $|\mu(m) - \mu(n)|_p \leq p^{-r}$.

spacer

Theorem 0.21 (Mahler)**.** *The continuous extension $\tilde{\mu} : \mathbb{Z}_p \to \mathbb{Z}_p$ of μ (i.e. $\tilde{\mu}(n) = \mu(n)$ for all $n \in \mathbb{Z}$) is given by the Newton algorithm:*

$$\tilde{\mu}(t) = \sum_{j=0}^{+\infty} (\Delta^j \mu)(0) \binom{t}{j}.$$

0.5.3 The Tate algebra

- $\mathbb{Z}_p[x_1, \ldots, x_m] =: \mathbb{Z}_p[\underline{x}]$ = polynomial functions with coefficients in $\mathbb{Z}_p$.

  Given $P = \sum a_I \underline{x}^I \in \mathbb{Z}_p[\underline{x}]$, define $\|P\| = \max(|a_I|)_p)$. This is a (multiplicative) norm.
- $\mathbb{Z}_p\langle x_1, \ldots, x_m\rangle = \mathbb{Z}_p\langle \underline{x}\rangle$ is the completion of $\mathbb{Z}_p[\underline{x}]$ for this norm.

  An element $f \in \mathbb{Z}_p\langle \underline{x}\rangle$ can be written as $f = \sum a_I \underline{x}^I$ where $|a_I|_p \to 0$ as $|I| \to +\infty$.

  If $f \in \mathbb{Z}_p\langle \underline{x}\rangle$ then $f : (\mathbb{Z}_p)^m \to \mathbb{Z}_p$.

0.5.4 Bell–Poonen

Theorem 0.22 (Bell)**.** *Assume $p \geq 3$. Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ be given by $\underline{x} \mapsto (f_1(\underline{x}), \ldots, f_m(\underline{x}))$ such that*

(1) $f \in \mathbb{Z}_p\langle \underline{x}\rangle$

(2) $\|f_i - x_i\| \leq \frac{1}{p}$

Then $\exists \Phi : \mathbb{Z}_p \times \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ $((t, \underline{x}) \mapsto \Phi(t, \underline{x}))$ such that

(a) Φ *is also given by Tate-analytic functions, in* $(m+1)$ *variables*

(b) $\Phi(n, \underline{x})) = f^n(\underline{x})$ *for all* $n \geq 1$

(c) Φ *defines an action of* $(\mathbb{Z}_p, +)$ *on* $\mathbb{Z}_p^m$*, i.e* $\Phi(t+s, \underline{x}) = \Phi(t, \Phi(s, \underline{x}))$.

(i.e. any such f [analytic, close to identity] is contained in an analytic "flow", but with time measured by p-adics.)

Proof. Write $f(\underline{x}) = A_0 + A_1(\underline{x}) + A_2(\underline{x}) + \dots$ where $A_0 = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix}$, $A_1(\underline{x})$ is the linear term, $A_2(\underline{x})$ the degree-2 term, and so on.

e.g. if $f \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 + x_2^3 + x_2 - 3 \end{pmatrix} = \begin{pmatrix} 0 \\ -3 \end{pmatrix} + \begin{pmatrix} x_2 \\ x_1 + x_2 \end{pmatrix} + 0 + \begin{pmatrix} 0 \\ x_2^3 \end{pmatrix}$.

For $m = 1$, $f = \sum a_k x^k$ where $|a_k|_p \leq 1$ and $|a_k|_p \to 0$.

Fixing z we have a sequence $\mu(n) = f^n(z)$.

To interpolate a sequence (Newton, Mahler), $(\Delta\mu)(n) = f^{n+1}(z) - f^n(z) = f^n \circ f(z) - f^n(z)$

Want to do this simultaneously for all z in polydisk.

Introduce a new difference operator Δ_f: for $h : \mathbb{Z}_p^m \to \mathbb{Z}_p$ or $\mathbb{Z}_p^m$, define $\Delta_f h := h \circ f - h$. Define

$$\Phi(t, \underline{x}) = \sum_{j=0}^{+\infty} (\Delta_f^j \,\mathrm{id})(\underline{x}) \binom{t}{j} = \mathrm{id} + (f - \mathrm{id})t + (f^2 - 2f + \mathrm{id})\frac{t(t-1)}{2} + \dots$$

where $\mathrm{id}(x_1, \dots, x_m) = (x_1, \dots, x_m)$.

It suffices to show that this series converges, i.e. we want to prove that the formal power series defines an element in $(\mathbb{Z}_p\langle t, \underline{x}\rangle)^m$.

Recall $\|h\| = \max_I |a_I|_p$ where $h = \sum a_I x^I$.

$f = \mathrm{id} + R$ where all coefficients in R have $|\cdot|_p \leq \frac{1}{p}$.

If $M(x_1, \dots, x_m) = \underline{x}^I = x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$, then $M \circ f$ is M + something of norm $< \frac{1}{p}$.

$\Delta_f M$ is something of norm $\leq \frac{1}{p}$

...

$\|\Delta_f^j M\| \leq p^{-j}$.

Using the ultrametric inequality, $\|\,|\Delta_f^j h\| \leq p^{-j}$

By density of polynomials in $\mathbb{Z}_p\langle \underline{x}\rangle$, $\|\Delta_f^j h\| \leq p^{-j}$ for all $h \in \mathbb{Z}_p\langle \underline{x}\rangle$.

Consequence: $\|\Delta_f^j \,\mathrm{id}\,\| \leq p^{-j}$.

Next need to control $\binom{t}{j} = \frac{t(t-1)\cdots(t-j+1)}{j!} = \frac{\in \mathbb{Z}[t]}{j!}$

For all $P \in \mathbb{Z}[t]$, $\|P\| \leq 1$. Need to control the p-adic absolute value of $j!$

$\nu_p(j!) = \nu_p(1 \times 2 \times \times \cdots \times j) = \lfloor \frac{j}{p} \rfloor + \lfloor \frac{j}{p^2} \rfloor + \cdots = \sum_{k=1}^{+\infty} \lfloor \frac{j}{p^k} \rfloor \leq \sum_{k=1}^{+\infty} \frac{j}{p^k} = \frac{j}{p} \frac{1}{1-1/p} = \frac{j}{p-1}$.

Hence $|j!|_p \geq p^{-j/p-1} = \left(p^{-\frac{1}{p-1}}\right)^j$.

If $p \geq 3$, win! (If $p = 2$, result still true if e.g. have reduction mod p^2.)

Φ is a well-defined map in $\mathbb{Z}_p\langle t, \underline{x}\rangle$; by construction, if $n \in \mathbb{Z}_{\geq 0}$, then $\Phi(n, \underline{x}) = f^n(\underline{x})$, since

$$\Phi(n, \underline{x}) = (\mathrm{id} + \Delta f)^n(\mathrm{id}) = \sum \Delta_f^j \binom{n}{j}.$$

Last step: want to show

$$\Phi(s + t, \underline{x}) = \Phi(s, \Phi(t, \underline{x}))$$

for all $s, t \in \mathbb{Z}_p$.

If $(s, t) \in (n, m) \in \mathbb{Z}_+ \times \mathbb{Z}_+$, this is just $f^{n+m} = f^n \circ f^m$. Now use that Φ is continuous, and $\overline{\mathbb{Z}_{\geq 0}} = \mathbb{Z}_p$. □

Remarks:

(1) $\Phi : (\mathbb{Z}_p, +) \curvearrowright \mathbb{Z}_p^m$; inverse of $\Phi(1, \underline{x}) = f(\underline{x})$ is $\Phi(-1, \underline{x})$, so $f(\underline{x})$ is invertible

$\implies$ f is in fact a (Tate-)analytic diffeomorphism of $\mathbb{Z}_p^m$.

(2) Given $g : \mathbb{Z}_p^m \to \mathbb{Z}_p^m \in (\mathbb{Z}_p\langle \underline{x}\rangle)^m$, consider the distance on $\mathbb{Z}_p^m$ given by $d(\underline{x}, \underline{y}) = \max_{i=1,\dots,m} |x_i - y_i|_p$.

The ultrametric property implies that g is 1-Lipschitz wrt this distance.

$\implies$ f is in fact an analytic isometry (1-Lipschitz with 1-Lipschitz inverse) of $\mathbb{Z}_p^m$.

$\implies$ $f^{\mathbb{Z}} \subset \Phi(\mathbb{Z}_p, \dots) \subset \mathrm{Isom}(\mathbb{Z}_p^m)$.

(3) (say $m = 1$): (recall $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$; say $p = 5$)

[[picture placeholder]]

... $\mathbb{Z}_p$ is a Cantor set; disks of radius $\frac{1}{p^j}$ correspond to points in $\mathbb{Z}/p^j\mathbb{Z}$.

Action of f on polydisks of radius p^{-j} $\leftrightarrow$ action of f on $(\mathbb{Z}/p^j\mathbb{Z})^m$ after reduction of coefficients.

Remark 0.23. Write $f = A_0 + A_1(\underline{x}) + A_2(\underline{x}) + \cdots + A_j(\underline{x}) + \dots$

Assumption was $\|A_0\| \leq \frac{1}{p}$, $\|A_j\| \frac{1}{p}$ for $j \geq 2$, $\|A_1 - \mathrm{id}\,\|_p \leq \frac{1}{p}$. These is not a strong assumption, by the following reduction/s:

Start with $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ analytic which is invertible.

Iterate f and reduce mod $p\mathbb{Z}_p$.

We get a transformation of $(\mathbb{Z}/p\mathbb{Z})^m$, which is a finite set. $\implies$ $\exists \ell \geq 1$ s.t $.f^\ell(0) = 0 \mod p\mathbb{Z}_p$, i.e. up to iteration [and ℓ is uniform given p and m / independent of f], first constraint is always satisfied ($A_0(f^\ell) = 0 \mod p$)

Assume $A_0 = 0 \mod p$; look at $A_1 = (Df)_0 \mod (p)$, $\in \mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$.

$\implies$ $\exists \ell'$ s.t. $f^{\ell'}(0) = 0$ and $\left(Df^{\ell'}\right)_0 = \mathrm{id} \mod p$ (again, last constraint always satisfied up to uniform iteration.)

Now assume that $f(x) = A_0 + A_1(\underline{x}) + \sum_{j\geq 2} A_j(\underline{x})$ s.t. $A_0 = 0 \mod p$, $A_1 - \mathrm{id} = 0 \mod p$, $A_j \in \mathbb{Z}_p[\underline{x}]$ homogeneous of degree j.

Change f into $h \circ f \circ h^{-1}$ where $h(\underline{x}) = \frac{1}{p}(x_1, \ldots, x_m)$.

$h^{-1}(\underline{x}) = (px_1, \ldots, px_m)$.

$h \circ f \circ h^{-1}(x) = \frac{1}{p}A_0 + A_1(\underline{x}) + pA_2(\underline{x}) + p^2A_3(\underline{x}) + \ldots$, so all coefficients in quadratic and higher terms are in $p\mathbb{Z}_p$ (up to conjugation.)

Remaining problem is in conjugated constant term $\frac{1}{p}A_0$, but this is okay as long as $A_0 = 0(\mod p^2)$ (which, again, we can assume by passing to a uniform iterate.)

0.6 Skolem–Mahler–Lech, Bell–Ghioca–Tucker

Consider any linear recurrence, e.g.

$$u_{n+2} = u_{n+1} - \pi u_n + u_{n-1}$$

with starting point (u_0, u_1, u_2).

Consider $Z(u) = \{n : u_n = 0\}$.

Theorem 0.24 (Skolem–Mahler–Lech)**.** *This set is a finite union of arithmetic progressions, i.e.* $\exists k\ \exists r_i, s_i$ *for* $1 \leq i \leq k$ *s.t.*

$$Z(u) = \bigcup_{i=1}^{k} \{r_i n + s_i : n \in \mathbb{Z}_+\}$$

(r_i may be zero, in which case that arithmetic progression reduces to a single point.)

In fact, using the Bell–Poonen theorem, there is a non-linear (polynomial) version of this:
Theorem 0.25 (Bell–Ghioca–Tucker)**.** *Given* $f \in \mathrm{Aut}(\mathbb{A}^m_{\mathbb{C}})$, $\underline{x} \in \mathbb{A}^m_{\mathbb{C}}$, $W \subset \mathbb{A}^m$ *an algebraic subvariety.*

Let $Z = \{n \in \mathbb{Z} : f^n(\underline{z}) \in W\}$. *Then* Z *is a finite union of arithmetic progressions.*

Proof. **Step 1.** Assume [instead] f is defined by polynomial functions in $\mathbb{Z}_p[\underline{x}]$, $\underline{z} \in \mathbb{A}^m(\mathbb{Z}_p)$, W defined by equations $F_i(\underline{x}) = 0$ with $F_i \in \mathbb{Z}_p[\underline{x}]$. Conjugating by translation $0 \mapsto \underline{z}$, we may assume $\underline{z} = 0$.

F maps points in polydisk to points in polydisk, so orbit of 0 remains in polydisk. Look at when orbit is contained in $W \cap$ polydisk.

Change f into $h \circ f^\ell \circ h^{-1}$ (where h is multiplication by $\frac{1}{p}$ as above) to assume that $f = \mathrm{id} \mod p$.

$W' = W \cup f(W) \cup \cdots \cup f^{\ell-1}(W)$.

Let $Z' = \{n : g^n(0) \in W'\}$ where $g = f^\ell$.

Bell–Poonen: $g(\underline{x}) = \Phi(1, \underline{x})$.

Case 1: Z' finite: done.

Case 2: Z' infinite: let G_i be an equation defining W'.

$t \mapsto G_i(\Phi(t, 0))$ has infinitely many zeros in $\mathbb{Z}_p$. Principle of isolated zeroes $\implies G_i \circ \Phi(t, 0) \equiv 0$.

True for each G_i; $\implies$ for all $t \in \mathbb{Z}_p$: $\Phi(t, 0) \subset W'$

$\implies$ for all n: $g^n(0) \subset W'$.

Step 2. From $\mathbb{C}$ to $\mathbb{Z}_p$.

Recall $f^{-1}, f \in \mathrm{Aut}(\mathbb{A}^m_{\mathbb{C}})$, $z \in \mathbb{A}^m(\mathbb{C})$; $W = \{F_1 = 0, \dots, F_k = 0\}$.

Get finite set of coefficients $S \subset \mathbb{C}$; problem is defined over field $\mathbb{Q}(S)$, S.

Lemma 0.26. *Let K be a finitely-generated extension of $\mathbb{Q}$, e.g. $\mathbb{Q}(\sqrt{2}, \pi)$, S be a finite subset of K.*

Then $\exists$ an embedding $\iota : K \hookrightarrow \mathbb{Q}_p$ for some p s.t. $|\iota(s)|_p = 1$ for every $s \in S \setminus \{0\}$.

Idea of proof. Two main ingredients: say $K = \mathbb{Q}(\pi)(\sqrt{2})$.

1. $\mathbb{Q}(t) \hookrightarrow \mathbb{Q}_p$ (map t to some transcendental; this is okay because $\mathbb{Q}_p$ is not countable.)

2. for algebraic extensions: say $P[t] \in \mathbb{Z}[t]$ irreducible, e.g. $t^2 - 2$. 1st step: find p s.t. $P(t)$ has a root in $\mathbb{Z}/p\mathbb{Z}$. There are infinitely many such p; if not $\exists p_1, \dots, p_k$ s.t. $P(n) = p_1^{\alpha_1(n)} \cdots p_k^{\alpha_k(n)} \sim n^{\deg P}$ for all $n \in \mathbb{Z}$. 2nd step: Hensel lemma $\implies$ $\exists p$ s.t. P has a root in $\mathbb{Z}_p$. □

... and now we have reduced the problem to one in $\mathbb{Z}_p$ (i.e. see Step 1.) □

0.7 Malcev and Selberg

Theorem 0.27. *Let Γ be a finitely-generated subgroup of $\mathrm{GL}_m(\mathbb{C})$ or (Bass–Lubotzsky) $\mathrm{Aut}(\mathbb{A}^m_{\mathbb{C}})$. Then*

(1) (Malcev) Γ is residually finite, i.e. $\forall \gamma \in \Gamma \setminus \{\mathrm{id}\}$, $\exists$ a homomorphism from Γ to a finite group such that γ is sent to a non-identity element.

(2) (Selberg) Γ contains a finite-index torsion-free subgroup.

Statement is more general—can change field, and replace $\mathbb{A}^m_k$ with an algebraic variety.

Example 0.28. $\Gamma = \mathrm{SL}_m \mathbb{Z}$.

Pick $\gamma \in \Gamma \setminus \{\mathrm{id}\}$.

$\exists a_{ij}$ a coefficient of the matrix $[a_{ij}]$ such that $a_{ij} \neq \delta_{ij}$ (the Kronecker delta.)

Choose $p \gg 1$ such that $a_{ij} - \delta_{ij} \neq 0 \bmod [p]$

Reduce mod $[p]$: get morphism

$$\mathrm{SL}_m(\mathbb{Z}) \to \mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$$

to a finite group with $\gamma \mapsto \bar{\gamma} \neq \mathrm{id}$.

... will do similar proof in general, in non-linear context.

Proof of Bass–Lubotzky theorem. Let $\Gamma < \mathrm{Aut}(\mathbb{A}^m_{\mathbb{C}})$, S be a finite set of generators.

Let C_S be the set of coefficients in $\mathbb{C}$ in the formulas defining the elements of S.

$\exists$ an embedding of $\mathbb{Q}(C_S) \overset{\iota}{\hookrightarrow} \mathbb{Q}_p$ for some $p \geq 3$ such that $\iota(C_S) \subset \mathbb{Z}_p$ and $|\iota(s)|_p = 1$ for all $s \in C_S \setminus \{0\}$.

Now $\Gamma \subset \mathrm{Aut}(\mathbb{A}^m_{\mathbb{Z}_p})$.

(1) [Malcev] The action of Γ on balls of $(\mathbb{Z}_p)^m$ of radius p^{-j} is the same as looking at $\Gamma \curvearrowright (\mathbb{Z}/p^j\mathbb{Z})^m$.

Take $\gamma \in \Gamma \setminus \{\mathrm{id}\}$. γ must map some ball of small radius to a different ball, hence acts non-trivially on $(\mathbb{Z}/p^j\mathbb{Z})^m$ for some $j \gg 1$ (related to the radius of the ball.)

(i.e. if $\gamma = (f_1, \ldots, f_m)$ with $f_\ell \in \mathbb{Z}_p[\underline{x}]$ is not the identity, there is some coefficient which explains this; this remains true under reduction mod some p^j, and sowe get $\gamma \mapsto \bar{\gamma} \in \mathrm{Aut}(\mathbb{A}^m_{\mathbb{Z}/p^j\mathbb{Z}}) \setminus \{\mathrm{id}\}$.)

Note $\mathrm{Aut}(\mathbb{A}^m_{\mathbb{Z}/p^j\mathbb{Z}})$ is not finite. But we can look at these as permutations on the finite set $\mathbb{A}^m_{\mathbb{Z}/p^j\mathbb{Z}}$, and that is a finite group.

(2) [Selberg] Recall we now have $\Gamma < \mathrm{Aut}(\mathbb{A}^m_{\mathbb{Z}_p})$; recall from above that

Fact 1. *$\exists$ a finite-index subgroup Γ_0 of Γ (with index depending only on m and p) s.t. for every $f \in \Gamma_0$, $p^{-1} \circ f \circ (p\underline{x})$ is contained in a p-adic analytic flow $\Phi(t, \underline{x})$, i.e. $\forall n \in \mathbb{Z}$, $\Phi(n, \underline{x}) = p^{-1} f^n (p\underline{x})$.*

Want to show that Γ_0 is torsion-free. Assume $f \in \Gamma_0$ is a torsion element; wewill show that $f = \mathrm{id}$.

f torsion $\implies$ $f^k = \mathrm{id}$ for some $k \geq 1$, and so $p^{-1} f^{kn}(p\underline{x}) = \mathrm{id}$ for all m, $\implies$ $\Phi(t, \underline{x})$ satisfies $\Phi(kn, \underline{x}) - \mathrm{id} = 0$ for all $n \in \mathbb{Z}$. By the principle of isolated zeros, $\Phi(t, \underline{x}) = \mathrm{id}$ for every $t \in \mathbb{Z}_p$. In particular, with $t = 0$, $f = \mathrm{id}$. □

Exercise (Minkowski)**.** $\Gamma_0 = \ker(\mathrm{SL}_m \mathbb{Z} \to \mathrm{SL}_m \mathbb{Z}/3\mathbb{Z})$ is torsion-free.

(Prove this directly, and see how it fits into the framework / proof above.)

0.8 Zimmer problem

Say $\Gamma = \mathrm{SL}_n \mathbb{R}$ with $n \geq 3$, Γ a lattice in G, finite index in $\mathrm{SL}_n(\mathbb{Z})$.

$\Gamma \curvearrowright \mathbf{P}^{n-1}(\mathbb{R})$. Does Γ act faithfully by diffeomorphisms or homeomorphisms on some compact manifold of dimension $< n - 1$?

... we can ask the same question for groups of polynomial automorphisms.

Theorem 0.29 (Cantat, Junyi Xie)**.** *Assume Γ not cocompact. If Γ embeds into $\mathrm{Aut}(\mathbb{A}^m_{\mathbb{C}})$, then $m \geq n$.*

Strategy of proof. Γ, being a lattice, is finitely-generated. Consider embedding of field in a p-adic field as above. For each group element, can apply Bell–Poonen theorem, sothat it is contained in an analytic flow of maps on the $\mathbb{Z}_p$-polydisk.

(New ingredient) Can put all of these flows together to get an action of a p-adic Lie group which is locally like the Lie group G (a non-local version of Bell–Poonen); then do (p-adic) differential geometry. (This is specific to Γ being a lattice in a simple Lie group, and Γ being not co-compact; uses congruence subgroups; for $\mathrm{SL}_n \mathbb{Z}$ subgroups, consider unipotents.) □

0.9 Birational transformations in dimension 2 and hyperbolic space of infinite dimension

$\mathbb{H}^\infty$ = hyperbolic space of infinite dimension.

Consider $\mathbb{A}^2_{\mathbb{C}}$, group of birational transformations $\mathrm{Bir}(\mathbb{A}^2_{\mathbb{C}})$.

An element $f \in \mathrm{Bir}(\mathbb{A}^2_{\mathbb{C}})$is given by formulas $f = (f_1(x_1, x_2), f_2(x_1, x_2))$ where $f_i = \frac{P_i(x_1,x_2)}{Q_i(x_1,x_2)} \in k(x_1, x_2)$.

Example 0.30. Given $\mathrm{GL}_2(\mathbb{Z}) \ni B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $(x_1, x_2) \mapsto (x_1^a x_2^b, x_1^c x_2^d)$ is in $\mathrm{Bir}(\mathbb{A}^2_{\mathbb{C}})$.

If $B = -\mathrm{id}$, $(x_1, x_2) \mapsto \left(\frac{1}{x_1}, \frac{1}{x_2}\right)$ is its own inverse.

Note e.g. $(x_1, x_2) \mapsto \left(\frac{x_1}{x_2}, x_2\right)$ is not well-defined everywhere.

$\sigma(x_1, x_2) = \left(\frac{1}{x_1}, \frac{1}{x_2}\right)$ maps $x_1 = 0$ and $x_2 = 0$ points to line at infinity; better to compactify affine space by adding a line at infinity, get $\mathbf{P}^2_{\mathbb{C}} = \{[x_1 : x_2 : x_3]\}$. When $x_3 = 1$, get $\mathbb{A}^2_{\mathbb{C}}$; when $x_3 = 0$ get line at infinity.

$\sigma[x_1 : x_2 : 1] = \left[\frac{1}{x_1}, \frac{1}{x_2} : 1\right]$;

$\sigma[x_1 : x_2 : x_3] = [x_3 x_2 : x_1 x_3 : x_1 x_2]$.

... better to look at transformations of $\mathbf{P}^2_{\mathbb{C}}$ given by $f[x_1 : x_2 : x_3] = [f_1 : f_2 : f_3]$ where f_1, f_2, f_3 are homogeneous polynomials of the same degree without common factors, with inverse of the same form.

... to find an inverse?

$$\sigma \circ \sigma = [x_1^2 x_2 x_3 : x_1 x_2^2 x_3 : x_1 x_2 x_3^2] = [x_1 : x_2 : x_3]$$

(when $x_1 x_2 x_3 \neq 0$.)

Geometrically: x_2-axis mapped to infinity, similarly with x_1-axis

When $x_1 = 0$: $\sigma = [x_2 x_3 : 0 : 0]$; $x_1 = 0$ line blown down to a point $[1 : 0 : 0]$; similarly with other axes; σ is an involution, those points are blown up to lines.

Blowing up points: take a point $x$of a smooth surface X; construct a new surface X' in which x is replaced by a curve $\mathbf{P}^1 = \mathbf{P}(T_x X)$ (the set of tangent directions to X at the point x.)

Doing this for σ: we replace each of the three vertices $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]$: on this blow-up surface, with a hexagon, σ is well-defined.

Main difference between polynomial automorphisms, birational maps: have points of indeterminacy; can resolve this by doing blow-ups.

...

A mapping class group acts on curves on surfaces, hence on curve complex, get interesting results.

Want to do analogous thing for $\mathrm{Bir}(\mathbb{A}^2_{\mathbb{C}})$ acting on curves in $\mathbf{P}^2_{\mathbb{C}}$. Problem: action not well-defined, curves can be mapped to points.

Note: here we are $\mathbb{C}$ world, so "curve" = Riemann surface ($\dim_{\mathbb{C}} = 2, \dim_{\mathbb{R}} = 1$.)

$\mathbf{P}^2(\mathbb{C}) \supset C$ a complex (algebraic) curve. It suffices to look at a homology class of C.

$[C] \in H_2(\mathbf{P}^2(\mathbb{C})) = \mathbb{Z} e_0$ where e_0 is the homology class of a(ny) projective line.

Line at infinity is a $\mathbf{P}^1(\mathbb{C}) = \hat{\mathbb{C}} = \bar{\mathbb{C}} = S^2$.

$[C] = d\, e_0$ where d is the degree of the equation defining C, = number of intersection points between C and a generic line.

$\mathrm{Bir}(\mathbf{P}^2(\mathbb{C})) \curvearrowright H_2(\mathbf{P}^2(\mathbb{C}); \mathbb{Z})$?

Algebraic geometry viewpoint: given a line $\ell = \{ax_1+bx_2+cx_3 = 0\}$, $\mathrm{Bir}(\mathbf{P}^2(\mathbb{C})) \ni f = [f_1 : f_2 : f_3]$, $f^{-1}(\ell) = \{af_1 + bf_2 + cf_3 = 0\}$, so action should be multplication by d ... but this is not an automorphism of $\mathbb{Z}$.

In our example σ, preimage of a generic line is a conic going through $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]$.

Instead: blow things up so that our maps are regular ... this gives new surfaces, and increases H_2. Now do this everywhere at once.

Trick: blowup all (possible) points and take the limit of $H^2(X_m;\mathbb{Z})$ (iven $\pi_1 : X_1 \to X_0 = \mathbf{P}^2$, get $H^2(X_1) \supset \pi_1^* H^2(\mathbf{P}^2)$.

$H^2(X_1;\mathbb{Z}) = \mathbb{Z}e_0 \oplus \mathbb{Z}e_1$ where e_1 is (co)homology class of the blow-up curve. $e_0^2 = 1$, $e_0\, e_1 = 0$, $e_1^2 = -1$.

$H^2(X_2;\mathbb{Z}) = \mathbb{Z}e_0 \oplus \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ with e_2 orthogonal to previous e_i, $e_2^2 = -1$.

In the limit, get $\mathbb{Z}e_0 \oplus \bigoplus_j \mathbb{Z}e_j$ with e_i pairwise orthogonal, $e_0^2 = 1$, $e_j^2 = -1$ for $j > 0$

... a (discrete) Minkowski space of infinite dimension!

$$\mathbb{H}_\infty^{\mathbb{Z}} = \{u \in \mathbb{Z}e_0 \oplus \bigoplus \mathbb{Z}e_j : u \cdot u = +1, u \cdot e_0 \geq 0\}.$$

Tensoring with $\mathbb{R}$,

$$\mathbb{H}_\infty = \{u \in \mathbb{R}e_0 \oplus \bigoplus \mathbb{R}e_j : u \cdot u = +1, u \cdot e_0 \geq 0\}.$$

Metric: for $u, v \in \mathbb{H}_\infty$, $\cosh d(u,v) = u\dot{v}$.

Lemma 0.31. $\mathrm{Bir}(\mathbf{P}^2_{\mathbb{C}})$ *embeds as a group of isometries of* $\mathbb{H}_\infty$.

(Action is natural action on classes of curves with self-intersection 1.)

Theorem 0.32 (Gizatullin)**.** *Let f be an element of* $\mathrm{Bir}(\mathbf{P}^2_{\mathbb{C}})$. *Denote by f_* the corresponding isometry of* $\mathbb{H}_\infty$. *There are only three possibilities:*

1. *f_* is elliptic, iff $\exists$ a birational change-of-coordinates $\varphi : \mathbf{P}^2_{\mathbb{C}} \dashrightarrow X$ s.t. $\varphi \circ f \circ \varphi^{-1}$ is contained in a Lie group acting algebraically on X;* $\deg(f^m)$ *bounded.*
2. *f_* is parabolic:*

   either $\deg(f^n) \sim n$ *and f preserves a pencil of* $\mathbf{P}^1$*'s*

   or $\deg(f^n) \sim n^2$ *and f preserves a pencil of elliptic curves*
3. *f_* is loxodromic, iff* $\deg(f^n) \sim \lambda^n$ *with* $\log\lambda$ *the translation length of f_*.*

+ ping-pong, + more structure theory $\implies$ Tits alternative

... any subgroup of $\mathrm{Bir}(\mathbf{P}^2_{\mathbb{C}})$ with (T) is conjugate to a subgroup of PGL_2.

... not known if subgroups of $\mathrm{Bir}(\mathbf{P}^2_{\mathbb{C}})$ are residually finite (second step of Malcev argument breaks down—do not have actions on finite sets due to indeterminacy points, although we do almost—get that these groups are sofic.)