Serge CANTAT: Groups of polynomial transformations

0.1 Affine space and its automorphisms

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

$A^m_k$ is the affine space over $k$.

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

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

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

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

$\text{End}(A^m_k) = \text{polynomial transformations } f : A^m \rightarrow A^m$.

In coordinates, defined by $m$ polynomials: $f(x_1, \ldots, x_m) = (f_1, \ldots, f_m)$ where $f_i \in k[x_1, \ldots, x_m]$;

$\text{group law is just composition of maps } (f, g \in \text{End}(A^m_k)) : f \circ g = (f_1(g_1, \ldots, g_m), \ldots).$

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

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

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

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

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

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

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

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

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 $p \in k[x_2]$, $a, b, c \in k$, $ab \neq 0$.
The set of all such transformations is called the **elementary subgroup**

\[
E = \left\{ h \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) = \left( \begin{array}{c} ax_1 + p(x_2) \\ bx_2 + c \end{array} \right) \right\}
\]

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 \( f(x_1, \ldots, x_m) = (f_1, \ldots, f_m) \):

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

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

\[
\deg(f) = \max_{i=1, \ldots, m} \deg(f_i).
\]

**Geometric interpretation:** take a generic affine hyperplane \( H \subset K^n \), take a generic (affine) line \( L \subset K^n \), count number of points in \( f^{-1}(H) \cap L \) over \( K \) 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 \( \text{Aut}(A_2^2) \) is the free product of \( A = \text{Aff}_2(k) \) and \( E \) amalgamated along their intersection \( S = A \cap E \)

\[
S = \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) \mapsto L \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) + \left( \begin{array}{c} s \\ t \end{array} \right) \text{ where } L \in \text{GL}_2(k) \text{ is upper-triangular.}
\]

Note it is specific to dimension 2 (and hard; requires algebraic geometry) that \( A \) and \( E \) generate \( \text{Aut}(A_2^2) \).

**Proof of free product with amalgamation.** For every \( h \in \text{Aut}(A_2^2) \setminus S \), there exist \( g_1, \ldots, g_n \in (A \cup E) \setminus S \) 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 \( \text{id}_{A_2^2} \). 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 \( t \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) = \left( \begin{array}{c} x_2 \\ x_1 \end{array} \right) \).

\( S \circ t \circ S = A \setminus S \).

Hence we can write \( h = \cdots e'_4 \circ t \circ e'_2 \circ t \circ e'_1 \) where \( \deg(e'_i) = \deg(e_i) \) (since \( e'_i \) is the composition of \( e_i \) with one or two affine maps.)
Now \( e_1' \left( \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \right) = \left( \begin{array}{c} a_1 x_1 + p_1(x_2) \\ b_1 x_2 + c_1 \end{array} \right) \in E \setminus S \); \( \deg(e_1') = \deg(p_1) \)

\( t \circ e_1' = \left( \begin{array}{c} b_1 x_2 + c_1 \\ a_1 x_1 + p_1(x_2) \end{array} \right) = \left( \begin{array}{c} P_1 \\ Q_1 \end{array} \right) \): highest degree term is a monomial in \( x_2 \).

\( e_2'(t \circ e_1') = \left( \begin{array}{c} \text{linear} + p_2(Q_1) \\ \text{linear} + * \end{array} \right) \): the leading terms are in \( p_2(Q_1) = p_2(a_1 x_1 + p_1(x_2)) \), which has degree \( \deg(p_2) \cdot \deg(Q_1) = \deg(e_2') \cdot \deg(e_1') \).

\( t \circ e_2' \circ t \circ e_1' = \left( \begin{array}{c} P_2 \\ Q_2 \end{array} \right) \): now argue by recursion (induction?) \( \square \)

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

**Theorem 0.7 (S. Lamy).** The group \( \text{Aut}(\mathbb{A}_k^2) \) satisfies the Tits alternative: if \( \Gamma < \text{Aut}(\mathbb{A}_k^2) \) is finitely generated, then either \( \Gamma \) contains a finite-index solvable subgroup, or \( \Gamma \) 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 \( \text{Aut}(\mathbb{A}_k^m) \), \( m \geq 3 \)?

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

### 0.3 Degree growth

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

**Example 0.9.** \( \left( \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \right) \xrightarrow{h} \left( \begin{array}{c} x_2 \\ x_1 + x_2^2 \\ x_3 \end{array} \right) \)

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

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

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 \( f \in \text{End}(\mathbb{A}_k^m) \).

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

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

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

Consider the polynomial transformation

\[
\left( \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \right) \xrightarrow{\sigma_3} \left( \begin{array}{c} x_1 \\ x_2 \\ x_3^3 \end{array} \right) = \left( \begin{array}{c} x_1 \\ x_2 \\ x_1 x_2 - x_3 \end{array} \right).
\]

Affine space is foliated by such surfaces; \( \sigma_3 \) is a polynomial map which preserves these foliations.

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

3
Not known if we can find unbounded sequences with sublinear growth. Some evidence to suggest “no”:

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

\[
\max_{j=0,\ldots,n} \text{deg}(h^j) \geq C_m n^{1/m}
\]

where \( C_m > 0 \) is a constant depending only on dimension \( m \).

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

(2) Given \( h \in \text{End}(\mathbb{A}_m) \); assume linear relation among the iterates, e.g. \( h^5 = h^3 - 2h + \text{id} \). 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 \( \geq 5 \), get \( h = \sum_{j=0}^4 a_j h^j \) where \( a_j \in k \). The degree is hence uniformly bounded by \( \max_{j=0,\ldots,4} \text{deg}(h^j) \).

(3) Put step (1) and (2) together: \( D_h(n) = \text{deg}_{j=0,\ldots,n} \text{deg}(h^j) \). If \( n+1 \geq m \cdot (m+d)m \) (“too many iterates of small degree”), then have a linear relation among the iterates, and hence bounded degree growth. Otherwise have growth of \( \sim m \cdot (m+d) \sim d^m \).

\[ \square \]

**0.4 Finite subgroups**

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

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

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

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 \( \text{Aut}(\mathbb{A}_k^m) \) such that

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

(ii) char(\( k \)) \( \neq p \), \( k \) algebraically closed.

Then \( G \) has a fixed point.

**Consequences:** if \( G \) fixes the origin 0, consider

\[
\Phi = \sum_{g \in G} (Dg)_0^{-1} \circ g \in \text{End}(\mathbb{A}_k^m)
\]

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

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

**Corollary 0.14.** \( G \ni g \mapsto (Dg)_0 \in \text{GL}_m(k) \) is injective.
Theorem 0.15 (Minkowski, Abboud). Set \( \text{Mink}(m, \ell) = \left\lfloor \frac{m}{\ell-1} \right\rfloor + \left\lfloor \frac{m}{2(\ell-1)} \right\rfloor + \cdots + \left\lfloor \frac{m}{l(l-1)} \right\rfloor + \cdots \in \mathbb{Z} \) (a finite sum of integers.)

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

Aside: character variety

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

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

\( \chi(F_2, \text{SL}_2) = \text{rep} / \text{conjugacy in } \text{SL}_2 \)

Outer automorphisms of \( F_2 \) act on \( \chi \)

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

Finite subgroups, continued

Theorem 0.16. 1. \( \#G = p^r, G \subset \text{Aut}(\mathbb{A}^m_k), p \land \text{char}(k) = 1 \) (\( \text{char}(k) = 0 \) or \( q, q \neq p \)) if \( k \) 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. \( \text{Aut}(\mathbb{A}^m_k) \), 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 \( g(x) = x \) for all \( g \in G \).

Writing this out more fully, for \( g = (g_1, \ldots, g_m) \),

\[ g_1(x_1, \ldots, x_m) - x_1 = 0 \]
\[ \vdots \]
\[ g_m(x_1, \ldots, x_m) - x_m = 0 \]

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.

\[ \sum_{1 \leq i \leq m} (g_i - x_i)Q_{g,i}(x) = 1. \] (1)
Let $A \subset k$ be the algebra (over $\mathbb{Z}$) generated by the coefficients in $[\ ]$ 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 $m$, the quotient field $A/m$ is finite.

Reduce everything modulo a maximal ideal $m$.

Write $\bar{g} = g$ with coefficients in $A/m$, similarly $\bar{Q}_{g,i} = Q_{g,i}$ reduced modulo $m$.

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

But $\frac{1}{p} \in A$ so $p \neq \text{char}(A/m)$. 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 $P = ds$
- Introduce the difference operator $\Delta$ defined by
  \[(\Delta \mu)(n) = \mu(n + 1) - \mu(n)\]
  \[(\Delta^2 \mu)(0) = \mu(2) - 2\mu(1) + \mu(0); (\Delta^3 \mu)(0) = \mu(3) - 3\mu(2) + 3\mu(1) - \mu(0), \ldots, (\Delta^d \mu)(0) = \sum (-1)^{j-l} \binom{j}{l} \mu(l).\]

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

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

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

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

(2) $\Delta^j \binom{t}{j} = \binom{t+j}{j} - \binom{t}{j} = \binom{t}{j-1}$ (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 $p$ ($p \land a' = 1$)
  \[|a|_p := p^{-r}.\]
- 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 $(a' + p^{s-r} b') \land p = 1 \implies \ |a + b|_p = p^{-r}$.
  If $s = r$, $|a + b|_p \leq p^{-r}$ (with equality if $(a' + b') \land p = 1$.)
\[ |a + b|_p = \max(|a|_p, |b|_p), \text{ with equality if } |a|_p \neq |b|_p \text{ (the ultrametric property).} \]

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

Get \((\mathbb{Q}_p, | \cdot |_p)\) where \( | \cdot |_p : \mathbb{Q}_p \to \mathbb{R}_+^* \cup \{0\}. \)

**Example 0.20.** \( p = 5, a = 137. \)

\(|a|_5 = 1 \ldots \) but this is not so descriptive. Instead, write:

\[
\begin{align*}
a & = 2 + 135 = 2 \cdot 5 + 5^3. \\
|2|_5 & = 1, |2 \cdot 5|_5 = \frac{1}{5}, |5^3|_5 = \frac{1}{125}. \\
\mathbb{Z}_p & \subset \mathbb{Q}_p \text{ is the closure (for the } p\text{-adic topology) of } \mathbb{Z} \text{ in } \mathbb{Q}_p.
\end{align*}
\]

**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 \( |\mu(m) - \mu(n)|_p \leq p^{-r}. \)

**Theorem 0.21** (Mahler). The continuous extension \( \tilde{\mu} : \mathbb{Z}_p \to \mathbb{Z}_p \) of \( \mu \) (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.

- \( \mathbb{Z}_p[\underline{x}] = \mathbb{Z}_p(\underline{x}) \) is the completion of \( \mathbb{Z}_p[\underline{x}] \) for this norm.

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

If \( f \in \mathbb{Z}_p(\underline{x}) \) 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. \( f \in \mathbb{Z}_p(\underline{x}) \)
2. \( \|f_i - x_i\| \leq \frac{1}{p} \)

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

(a) \( \Phi \) is also given by Tate-analytic functions, in \( (m + 1) \) variables
(b) \( \Phi(n, x) = f^n(x) \) for all \( n \geq 1 \)

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

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

0.6 III