$$f : \mathbb{Z}_p \to \mathbb{Z}_p^m \qquad , p \geq 3.$$
$$\vec{x} \mapsto (f_1(\vec{x}), \dots, f_m(\vec{x}))$$

$$f_i \in \mathbb{Z}_p \langle \vec{x} \rangle$$

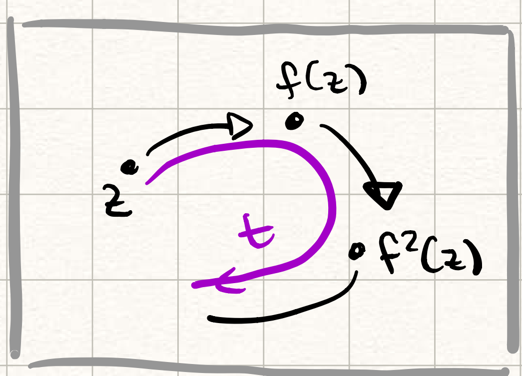
$$f(\vec{x}) = \underbrace{A_0}_{\uparrow ct} + A_1(\vec{x}) + A_2(\vec{x}) + \dots$$

$$\| $$

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix} + \text{linear term} + \text{degree } 2 + \dots$$

$$f\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 + x_2^3 + x_2 - 3 \end{pmatrix}$$

$$= \underbrace{\begin{pmatrix} 0 \\ -3 \end{pmatrix}}_{A_0} + \underbrace{\begin{pmatrix} x_2 \\ x_1 + x_2 \end{pmatrix}}_{A_1} + \underbrace{0}_{A_2} + \underbrace{\begin{pmatrix} 0 \\ x_2^3 \end{pmatrix}}_{A_3}$$



$$\Phi : \mathbb{Z}_p \times \mathbb{Z}_p^m \to \mathbb{Z}_p^m$$
$$\Phi(j, \vec{x}) = f^j(\vec{x})$$
$$\Phi(t, \vec{x})$$
$$t \in \mathbb{Z}_p$$

analytic flow interpolating f.

Fixing z, we have a sequence

$$u(n) = f^n(z).$$

To interpolate a sequence, (Newton, Mahler)

$$\Delta u(n) = f^{n+1}(z) - f^n(z)$$
$$= f^n \circ f(z) - f^n(z)$$

New difference op:

$$\Delta_f h = h \circ f - h.$$

For $h : \mathbb{Z}_p^m \to \mathbb{Z}_p$ or $\mathbb{Z}_p^m$, set $\Delta_f h = h \circ f - h$.

Define:

$$\Phi(t, \vec{x}) := \sum_{j=0}^{\infty} \overbrace{\left(\Delta_f^j \, \mathrm{Id}\right)}^{\mathrm{Id}(x_1, \dots, x_m) = (x_1, \dots, x_m)}(\vec{x}) \binom{t}{j}$$

$$= \mathrm{Id} + (f - \mathrm{Id})t + (f^2 - 2f + \mathrm{Id}) \frac{t(t-1)}{2} + \dots$$

NTS: series converge $\underset{\text{(yesterday)}}{\Leftrightarrow}$ interpolates orbit

We want to prove that it defines an element in $(\mathbb{Z}_p\langle t, \vec{x} \rangle)^m$.

$$\|h\| = \max_I |a_I|_p$$

$$h = \sum a_I x^I$$

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

$$\underline{M}(x_1, \dots, x_m) = \vec{x}^I = x_1^{i_1} x_2^{i_2} \dots x_m^{i_m}$$

monomial

$\Rightarrow M \circ f = M +$ something of norm $< 1/p$.

$$\Delta_f M = 0 + \text{something of norm} \leq 1/p.$$

$$\Delta_f^j M = 0 + \underbrace{\qquad\qquad}_{} \leq 1/p^j$$

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

ultrametric inequality

$$\| \Delta_f^j h \| \leq p^{-j}, \ \forall h \in \mathbb{Z}_p \langle \vec{x} \rangle.$$

Consequence: $\|\Delta_f^j \mathrm{Id}\| \le p^{-j}$ *

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

$$\forall\, \vec{p} \in \mathbb{Z}[t], \quad \|\vec{p}\| \le 1.$$

Control the p-adic abs. val. of $j!$

$$v_p(j!) = v_p(1 \times 2 \times \cdots \times j)$$

p-adic value

$$= \left\lfloor \frac{j}{p} \right\rfloor + \left\lfloor \frac{j}{p^2} \right\rfloor + \cdots$$

terms divisible by p.

$$= \sum_{k=1}^{\infty} \left\lfloor \frac{j}{p^k} \right\rfloor$$

$$\le \sum_{k=1}^{\infty} \frac{j}{p^k}$$

$$\le j\left(\frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

$$\le \frac{j}{p} \frac{1}{1-1/p}$$

$$\le j \frac{1}{p-1}$$

$$|j!|_p \geq p^{-j/p-1}$$
$$\geq (p^{-1/p-1})^j$$

if $p \geq 3$, WIN ie series converges.

<u>What happened</u>:

- Φ is well-defined $\in \mathbb{Z}_p\langle t, \vec{x}\rangle$.

By construction, if $n \geq 0 \in \mathbb{Z}$, then

$$\Phi(n, \vec{x}) = f^n(x),$$
$$\Phi(n, \vec{x}) = (Id + \Delta f)^n \longleftarrow \text{we showed this by interpol.}$$
$$= \sum \Delta_f^j \binom{n}{j}$$

<u>Last step</u>

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

$(\forall s, t \in \mathbb{Z}_p)$

if $(s,t) = (n,m) \in \mathbb{Z}_+ \times \mathbb{Z}_+$

$$f^{n+m} = f^n \circ f^m$$

Now we use that $\Phi(t, \vec{x})$ is $\mathcal{C}^0$ and $\overline{\mathbb{Z}_{\geq 0}} = \mathbb{Z}_p$

Note: we can approx
$$-1 = \sum_{k \geq 0} a_k p^k .$$

Rmk:

(1) $\Phi : (\mathbb{Z}_p, +) \curvearrowright \mathbb{Z}_p^m$

$\Rightarrow$ inverse of $\Phi(1, \vec{x}) = f(\vec{x})$ is $\Phi(-1, \vec{x})$ so $f(\vec{x})$ is invertible.

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

(2) $g : \mathbb{Z}_p^m \longrightarrow \mathbb{Z}_p^m \in (\mathbb{Z}_p\langle\vec{x}\rangle)^m$

Consider the distance on $\mathbb{Z}_p^m$ given by

$$d(\vec{x},\vec{y}) = \max_{i=1}^{m} (|x_i - y_i|_p)$$

ultrametric prop $\Rightarrow$ g is 1-Lipschitz.
(b/c take max).

$\Rightarrow$ f is in fact an analytic isom. of $\mathbb{Z}_p^m$

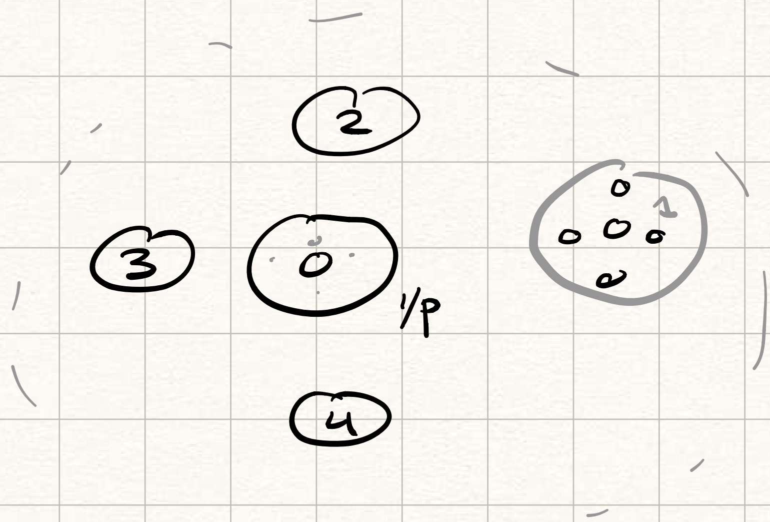
$\Rightarrow f^{\mathbb{Z}} \subset \Phi(\mathbb{Z}_p, \cdot) \subset \mathrm{Isom}(\mathbb{Z}_p^m)$

(3) $\boxed{m=1}$ $\quad p=5$

$1 + a_1 p + \cdots$, $x \in \mathbb{Q}_p$, $|x|_p \leq 1$.

$a_0 + a_1 p + \cdots$

$\mathbb{Z}_p^{\{0,1,2,3,4\}}$



$\Rightarrow$ $\mathbb{Z}_p$ is a Cantor set,
disks of radius $\frac{1}{p^j}$ corresponds
to pts in $\mathbb{Z}/p^j\mathbb{Z}$

Action of f in polydisks
of radius p^{-j}

$\Leftrightarrow$ Action of f on $(\mathbb{Z}/p^j\mathbb{Z})^m$
after reduction of coeff.

New goal: Relax assumpt.

Summary: $f = A_0 + A_1(\vec{x}) + A_2(\vec{x}) + \cdots$

Assumption was $\|A_0\| \leq 1/p$
$\|A_j\| \leq 1/p$, $j \geq 2$
$\|A_1 - Id\|_p \leq \frac{1}{p}$

$=$ take suf large pow of f.

= conjugate.

Start w/ $f: \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ analytic.
which is invertible, then
iterate f and reduce mod $p\mathbb{Z}_p$

↳ transformations of $(\mathbb{Z}/p\mathbb{Z})^m$
= finite set

max ideal
gen by p in $\mathbb{Z}_p$.

$\Rightarrow \exists\, \ell \geqslant 1,\ f^\ell(0) = 0 \mod (p\mathbb{Z}_p)$
$\Rightarrow A_0(f^\ell) = 0 \mod p.$

Assume $A_0 = 0 \mod p$.
Look at $A_1 \mod p$,

$$A_1 = (Df)_0 \mod (p)$$
$$\in GL_m(\mathbb{Z}/p\mathbb{Z})$$

$\Rightarrow \exists\, \ell',\ f^{\ell'}(0) = 0$ and $(Df^{\ell'})_0 = Id$
mod (p)

Now assume that

$$f(x) = A_0 + A_1(\vec{x}) + \sum_{j \geq 2} A_j(\vec{x}) \quad w/$$

$$A_0 = 0 \mod (p)^2,$$ ← so don't change norm.

$$A_1 - Id = 0 \mod (p)$$

$A_j \in \mathbb{Z}_p[\vec{x}]$ homogeneous j.

Change f into

$$h \circ f \circ h^{-1}$$

where

$$h(\vec{x}) = \frac{1}{p}(x_1, \dots, x_m)$$

$$h^{-1}(\vec{x}) = (px_1, \dots, px_m)$$

$$h \circ f \circ h^{-1}(x) = \frac{1}{p} A_0 + A_1(\vec{x}) + \underline{p A_2(x) + p^2 A_3(\vec{x})} + \dots$$

$\in p\mathbb{Z}_p$

§ 6. Skolem, Mahler, Lech. . .

6.A Linear case

$$u_{n+2} = 3u_{n+1} - \pi u_n + u_{n-1}$$

some linear sequence

(u_0, u_1, u_2) = starting pt.

$$Z(u) = \{n \geq 0 \,;\, u_n = 0\}$$

Thm: This set is a finite union of arithmetic progressions:

$$\exists k, \exists r_i, s_i, 1 \leq i \leq k$$

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

6.B

Thm:
- $f \in Aut(\mathbb{A}^m_{\mathbb{C}})$
- $\vec{x} \in \mathbb{A}^m(\mathbb{C})$
- $W \subset \mathbb{A}^m$ is an algebraic subvariety

$$Z = \{n \in \mathbb{Z} \,;\, f^n(x) \in W\}.$$

Then Z is a finite union of arithmetic progression.

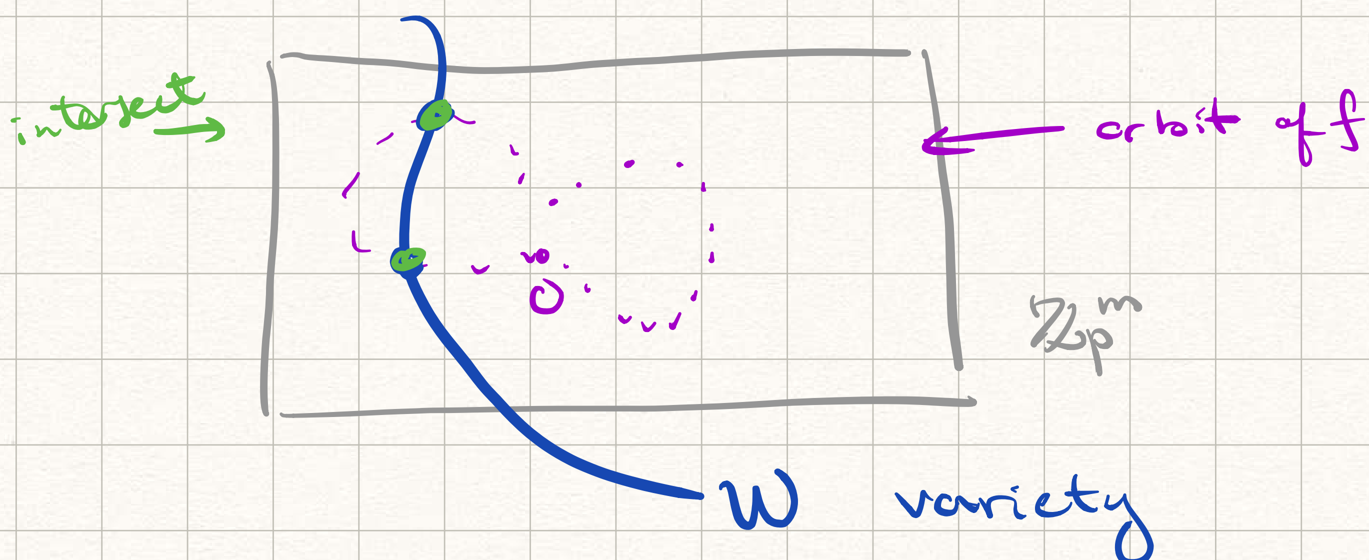
Pf:

$\boxed{\text{Step 1}}$ - Assume f is defined by poly in $\mathbb{Z}_p[\vec{x}]$

- $z \in \mathbb{A}^m(\mathbb{Z}_p)$

- W is defined by eqs $F_i(x) = 0$ w/ $F_i \in \mathbb{Z}_p[\vec{x}]$.

Conjugate by translation st $0 \mapsto z$



Change f into $h \circ f^{\ell} \circ h^{-1}$ to assume that $f = \mathrm{Id} \bmod (p)$

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

look $Z' = \{n ; \underline{(f^{\ell})^n}(0) \in W'\}$

↑ pow of sub.

↑ $g = f^{\ell}$.

$g(\vec{x}) = \Phi(1, \vec{x})$

<u>Case 1</u> : Z' is finite

<u>Case 2</u> : Z' is infinite

G_i = some equation of W'

$t \mapsto G_i(\Phi(t, 0))$

∞-many zeroes in $\mathbb{Z}_p$.

By principle of isolated 0s (complex analysis)

$\Rightarrow G_i \circ \Phi(t, 0) \equiv 0$

$\Rightarrow \forall t \in \mathbb{Z}_p, \ \Phi(t, 0) \subset W'$

$\Rightarrow \forall n \,,\; g^n(o) \subset W'.$

$\square$

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

- $f \in \mathrm{Aut}(\mathbb{A}^m_{\mathbb{C}})$; $z \in \mathbb{A}^m(\mathbb{C})$;

$$W = \begin{pmatrix} F_1 = 0 \\ \vdots \\ F_R = 0 \end{pmatrix}$$

- finite set of coefficients $S \subset \mathbb{C}$.

$\rightarrow$ defined over $\mathbb{Q}(S)$, S

Lemma: Let K be a finitely generated extension of $\mathbb{Q}$ (for instance, $\mathbb{Q}(\sqrt{2}, \pi)$ and S a finite subset of K).

Then, there is an embedding

$$\tau : K \hookrightarrow \mathbb{Q}_p$$

for some p, st

$$|\tau(s)|_p = 1 \;,\; \forall s \in S \setminus \{0\}.$$

<u>Main ingredients</u> ; $\sum a_k p^k$

$\mathbb{Q}(\pi)(\sqrt{2})$

$\mathbb{Q}(t) \xrightarrow{\mathbb{Z}_p} \mathbb{Q}_p$

$\vec{P}(t) \in \mathbb{Z}[t]$

$\overset{\shortparallel}{\text{irred}}$ t^2-2

<u>1st - step</u> : Find p st $\vec{P}(t)$ has a root in $\mathbb{Z}/p\mathbb{Z}$

$\exists\ \infty$ - many p st $\vec{P}(t)$ has a root mod p.

If not, $\exists\, p_1, \ldots, p_k$ st

$$\vec{P}(n) = p_1^{\alpha_1(n)} \cdots p_k^{\alpha_k(n)}$$

$$\sim n^{\deg P} \quad \forall n \in \mathbb{Z}$$

<u>2nd step</u>: Hensel lemma

$\Rightarrow \exists p /\ \vec{P}$ has a root in $\mathbb{Z}_p$.