4.

- $|G| = p^r \subset \mathrm{Aut}(/\mathbb{A}^m_k)$
- $\mathrm{char}(k) \neq p$

  0 or $q \neq p$
- k is alg. closed, or k is finite

$\Rightarrow$ G has a fixed pt $\mathbb{A}^m(k)$

(1) 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 or a number of elmts divisible by p, but $p \nmid |\mathbb{A}^m_k|$

$\Rightarrow$ 1 element orbit

$\square$

⚠ **Note**: Aut$(\mathbb{A}^m_k)$ when $m \geq 2$ is ∞-dim even if $\mathbb{A}^m(k)$ may be finite.

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \longmapsto \begin{pmatrix} x_1 + x_2^d \\ x_2 \end{pmatrix}$$

action may not be faithful.

② k alg. closed ($k = \mathbb{C}$)

Equations for fixed pts

$$g(\vec{x}) = \vec{x} \quad \forall g \in G, \; g = (g_1, \dots, g_m)$$

$$\forall g \in G, \begin{cases} g_1(x_1, \dots, x_m) - x_1 = 0 \\ \vdots \\ g_m(x_1, \dots, x_m) - x_m = 0 \end{cases}$$

Hilbert Nullstellenzatz

alg closed

$\exists$ polynomial fns $Q_{g,i} \in K[x_1, \dots, x_m]$
for $g \in G$ and $1 \le i \le m$

$$\sum_{\substack{g \in G \\ 1 \le i \le m}} (g_i - x_i)\, Q_{g,i}(\vec{x}) = 1 \;. \quad \bigstar$$

Let $A \subset K$ be an algebra generated by the coeffs you see in the formula $(\star)$ and $1/p$.

Thm: Let A be a fg algebra over $\mathbb{Z}$. Then A has a max ideal, and for every max ideal m, the quotient field A/m is finite.

Reduce everything mod m,

$\bar{g} := g \mod m$

Then:

$$\sum_{\substack{g \in G \\ 1 \le i \le m}} (\bar{g}_i - \bar{x}_i)\, \bar{Q}_{g,i}(\vec{x}) = 1$$

is true mod m

$\Rightarrow \bar{G}$ has no fixed pt in $\mathbb{A}^m(A/m) \leftarrow$ finite field.

But $\frac{1}{p} \in A$ so $p \neq$ char A/m.

contradicts assumption.

$\Rightarrow$ Contradiction $\square$

5. Bell Thm

Newton's algorithm for interpolation

- $u(n)$ a seq of numbers in $\mathbb{C}$
- look for $P \in \mathbb{C}[t]$ st

  $P(j) = u(j)$

  $\deg(P) = d$

· Δ difference op.

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

$(\Delta u) = (u(1) - u(0), u(2) - u(1), \dots)$

$(\Delta^2 u)(0) = u(2) - 2u(1) + u(0)$

$(\Delta^3 u)(0) = u(3) - 3u(2) + 3u(1) - u(0)$

$(\Delta^j u)(0) = \sum (-1)^\ell \binom{j}{\ell} u(\ell)$

Thm: The polynomial fn P is equal to

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

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

Pf: (1) The fns $\binom{t}{j}$ form a basis $\mathbb{C}[t]_{\le d}$ (for $0 \le j \le d$)

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

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

(3) Write $P(t) = \sum A_j \binom{t}{j}$

$$P(0) = A_0 = u(0) = (\Delta^0 u)(0).$$

5.B p-adic numbers

- $\mathbb{Z} \ni a = p^r \times a'$

  where a' is not divisible by p.

  (p, a') rel prime.

$$|a|_p := p^{-r} \quad \text{where}$$

- $a = p^r a'$, $b = p^s b'$, $s \geq r$.

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

if $s > r \Rightarrow \underbrace{(a' + p^{s-r} b') \wedge p}_{\text{gcd}} = 1$

$$\Rightarrow |a+b|_p = p^{-r}.$$

if $s=r$, $\Rightarrow |a+b|_p \leq p^{-r}$.

$$\Rightarrow \quad |a+b|_p \le \max(|a|_p, |b|_p)$$

w/ equality $|a|_p \neq |b|_p$.

Extend it to $\mathbb{Q}$:

$$|0|_p = 0$$

$$\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p}$$

- $\mathbb{Q}_p$ = completion of $\mathbb{Q}$ for this $|\cdot|_p$.

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

<u>ex</u>: $p = 5$

$a = 137$

$|a|_5 = 1$.

$$a = 2 + 135$$

$$= \underset{1}{2} + \underset{1/5}{2 \cdot 5} + \underset{1/125}{5^3}$$

Exc: • $\mathbb{Z}_p \subset \mathbb{Q}_p$
= closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

• Every $x \in \mathbb{Z}_p$ can be written in a unique way

$$x = \sum_{k=0}^{\infty} a_k p^k$$

w/ $a_k \in \{0, 1, 2, \ldots, p-1\}$.

• $\mathbb{Z}_p$ = unit disk in $\mathbb{Q}_p$
$= \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$
= valuation ring

it contains a unique maximal ideal, namely
$p\mathbb{Z}_p$ = disk of radius $1/p$

b/c these all rel. prime to p.

and $\mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{F}_p$.

why?

· Let $u : \mathbb{Z} \to \mathbb{Z}_p$ be uniformely continuous :

$\forall r > 0, \exists s > 0$ st
if $p^s \mid n-m$,
divides
then $|u(n) - u(m)|_p \leq p^{-r}$

Thm (Mahler)
The continuous extension, $\tilde{u} : \mathbb{Z}_p \to \mathbb{Z}_p$ of u, ie $\tilde{u}(n) = u(n) \ \forall n \in \mathbb{Z}$ is given by the Newton algorithm:

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

5.C Tate algebra

· $\mathbb{Z}_p[x_1, \ldots, x_m]$ = poly fn w/ coeff in $\mathbb{Z}_p$

not same p's.

$\vec{p} = \sum a_I x^I$, $\|\vec{p}\| = \max(|a_I|_p)$

- $\mathbb{Z}_p\langle x_1, \dots, x_m\rangle = \mathbb{Z}_p\langle \vec{x}\rangle$
$= \text{completion } \mathbb{Z}_p[\vec{x}] \text{ for this norm.}$

$\rightsquigarrow f = \sum a_I x^I$ st $a_I \in \mathbb{Z}_p$
and $|a_I|_p \to 0$, $|I| \to \infty$

if $f \in \mathbb{Z}_p\langle\vec{x}\rangle$ then
$f : (\mathbb{Z}_p)^m \longrightarrow \mathbb{Z}_p$.

<u>5.D : Bell - Poonen</u>

<u>**Thm (Bell)**</u> $\qquad p \geq 3$

Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$
$\vec{x} \mapsto (f_1(\vec{x}), \dots, f_m(\vec{x}))$

st (1) $f_i \in \mathbb{Z}_p\langle\vec{x}\rangle$
(2) $\|f_i - x_i\| \leq \frac{1}{p}$

Then $\exists\, \Phi : \mathbb{Z}_p \times \mathbb{Z}_p^m \longrightarrow \mathbb{Z}_p^m$
$(t, \vec{x}) \longmapsto \Phi(t, \vec{x})$

st:

(a) Φ is also given by Tate-analytic fns in $(m+1)$-variables.

(b) $\Phi(n,\vec{x}) = f^n(\vec{x})$, $\forall n \geq 1$

(c) Φ defines an action of $(\mathbb{Z}_p, +)$ on $\mathbb{Z}_p^m$

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