Peer Seminar
'24. 3. 11.
Younghun Jo

The local-Global Principle for periodic orbits of polynomial maps.

「local-Global Principle」

: "To solve a problem, it suffices to solve it p-adically. (i.e., in mod p.)"

e.g. Hasse-Minkowski theorem.

: let $q(\underline{x})$ be a quadratic form over $\mathbb{Q}$.

Then, $q(\underline{x}) = 0$ has a solution in $\mathbb{Q}$ iff it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ $\forall p$: prime.

[Note $(\Rightarrow)$ is trivial, but $(\Leftarrow)$ is highly nontrivial.]

Problem Setting

- R : comm. ring w/ unity. $\quad N \geq 1$.
- $f \in \mathrm{End}(R^N)$ i.e., $f = (f^{(1)}, \cdots, f^{(N)})$ $\quad f^{(r)} \in R[X_1, \cdots, X_N]$.
- $x \in R^N$ is periodic w.r.t. f if
  its orbit $\mathcal{O}_f(x) = \{ f^i(x) : i \geq 0 \}$ is finite and f permutes $\mathcal{O}_f(x)$.
  i.e., $f^n(x) = x$ for some $n \geq 0$.

  Denote $n = \# \mathcal{O}_f(x)$.
- $\mathrm{Cycl}(R, N) := \{ n : \exists x \in R^N, f \in \mathrm{End}(R^N) \text{ s.t. } x \text{ is } n\text{-periodic w.r.t. } f \}$.

Q. Is $\mathrm{Cycl}(R,N)$ finite? $\quad$ [cf. $\mathrm{Cycl}(\mathbb{Z}, 1) = \{1, 2\}$.]

$\boxed{\text{Thm}}$ (local – Global Principle).
let R : Dedekind domain. [e.g. $R = \mathbb{Z}$, or $\mathcal{O}_K$. K : #field.]
Then for $N \geq 2$,

$$\mathrm{Cycl}(R, N) = \bigcap_{\mathfrak{p} (\neq 0) \in \mathrm{Spec}\, R} \mathrm{Cycl}(R_{\mathfrak{p}}, N) = \bigcap_{\mathfrak{p} (\neq 0) \in \mathrm{Spec}\, R} \mathrm{Cycl}(\hat{R}_{\mathfrak{p}}, N).$$

[Note ($\subseteq$) is trivial, but ($\supseteq$) is not.]

$\boxed{\text{Thm}}$ let R : discrete valuation domain of char 0. w/ unique maximal ideal $\mathfrak{p}$.
$\mathcal{K} = R/\mathfrak{p}$. $\quad \# \mathcal{K} = p^t$. $\quad p$: prime #.
$n \in \mathrm{Cycl}(R, N)$ be a min. period of $x \in R^N$ w.r.t. $f \in \mathrm{End}(R^N)$.
Then, $n = m \cdot d \cdot p^e$
where $m = (\text{min. period of } (x \bmod \mathfrak{p}) \text{ w.r.t. } (f \bmod \mathfrak{p})) \leq \# \mathcal{K}^N = p^{tN}$
$d \leq p^{tN} - 1$.

$\boxed{\text{Cor}}$ let $R = \mathcal{O}_K$. $\quad K$: # field. $\quad N \geq 2$.
Then, $\# \mathrm{Cycl}(R, N) < \infty$.

$\boxed{\text{lemma}}$. let R: comm. ring w/ unity of char 0., $N \geq 1$.

$\mathcal{O} = (x_1, \cdots, x_n)$ periodic orbit on R^N.

(a) let $\sigma \in AGL_N R$ be an invertible affine transformation,

i.e., $\sigma(x) = Ax + b$ for some $A \in GL_N R$. $b \in R^N$.

Then, $\sigma(\mathcal{O})$ is also a periodic orbit on R^N.

(b) There exists a periodic orbit of length n on R^N ~~...~~ whose coordinates of the pts are pairwise distinct.

pf (a) Suppose that $\mathcal{O}$ is an orbit w.r.t. $f \in \mathrm{End}(R^N)$.

Then, $\sigma(\mathcal{O})$ is an orbit w.r.t. $f^\sigma = \sigma \circ f \circ \sigma^{-1}$.

(b) Apply a suitable $\sigma \in AGL_N R$. ▨

We will focus on the case when $R = \mathbb{Z}$. [The proof is essentially the same for general cases.]

Suppose that $n \in \mathrm{Cycl}(\mathbb{Z}_p, N)$ $\forall p$: prime.

For each $p < n$,

let $\mathcal{O}_p = (x_{p,1}, \cdots, x_{p,n})$ be a periodic orbit in $\mathbb{Z}_p^N$ w.r.t. $f_p \in \mathrm{End}(\mathbb{Z}_p^N)$.

WMA $x_{p,i_1}^{(r_1)} \neq x_{p,i_2}^{(r_2)}$ $\forall (i_1, r_1) \neq (i_2, r_2)$.

For each p, let $\mathrm{ord}_p : \mathbb{Z}_p \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on $\mathbb{Z}_p$ w/ $\mathrm{ord}_p(p) = 1$.

Pick $M \in \mathbb{Z}$ s.t.

(i) For each $p < n$, $\quad \mathrm{ord}_p(M) > \mathrm{ord}_p\left(\prod_{(i_1,r_1)\neq(i_2,r_2)} (x_{p,i_1}^{(r_1)} - x_{p,i_2}^{(r_2)})\right)$.

(ii) For each $p \geq n$, $\quad \mathrm{ord}_p(M) = 0$.

Idea

- Pick $x_1, \cdots, x_n \in \mathbb{Z}^N$ which are "nice" approximations of $x_{p,1}, \cdots, x_{p,n}$.
- Pick $\tilde{f} \in \mathrm{End}(\mathbb{Z}^N)$ that approximates f_p well.
- To construct $f \in \mathrm{End}(\mathbb{Z}^N)$ from $\tilde{f}$, we add a few terms inductively so that f satisfies $f(x_i) = x_{i+1}$.

$\boxed{\text{lemma}}$ There exists $x_1, \cdots, x_n \in \mathbb{Z}^N$ s.t.

(i) For each $p < n$, $\quad \mathrm{ord}_p\left(x_{p,i}^{(r)} - x_i^{(r)} \right) \geq \mathrm{ord}_p(M)$. $\quad \forall i,\ \forall r$.

(ii) For each $p \geq n$, $\quad \min\left\{ \mathrm{ord}_p\left(\prod_{i_1 \neq i_2} (x_{i_1}^{(1)} - x_{i_2}^{(1)}) \right), \mathrm{ord}_p\left(\prod_{i_1 \neq i_2} (x_{i_1}^{(2)} - x_{i_2}^{(2)}) \right) \right\} = 0$.

pf. Pick $\tilde{x}_1, \cdots, \tilde{x}_n \in \mathbb{Z}^N$ satisfying (i).

We will pick $a_1, a_2, \cdots, a_n \in \mathbb{Z}$,

and put $x_i = \left(\tilde{x}_i^{(1)} + a_i \cdot M, \tilde{x}_i^{(2)}, \cdots, \tilde{x}_i^{(N)} \right)$ so that (ii) holds.

There are only finitely many primes $p \geq n$ s.t. $\mathrm{ord}_p\left(\prod_{i_1 \neq i_2} (x_{i_1}^{(2)} - x_{i_2}^{(2)}) \right) > 0$.

Denote the set of such primes by ϕ.

For each $p \in \phi$, since $p \geq n$,

we may pick $a_1, \cdots, a_n \pmod{p}$ so that $x_1^{(1)}, \cdots, x_n^{(1)} \pmod{p}$ are pairwise distinct.

Use CRT to choose such $a_1, \cdots, a_n \in \mathbb{Z}$. ▨

let $\tilde{f} \in \mathrm{End}(\mathbb{Z}^N)$ be s.t. $\tilde{f}^{(r)} \equiv f_p^{(r)} \pmod{M^n \cdot \mathbb{Z}[X_1, \cdots, X_N]}$ $\forall r, \forall p < n$

We will put

$$f^{(r)}(X_1, \cdots, X_N) = \tilde{f}^{(r)}(X_1, \cdots, X_N)$$
$$+ \sum_{k=0}^{n-1} M^{n-k} \cdot \left[b_k \cdot \prod_{v=1}^{k} (X_1 - x_v^{(1)}) + B_k \prod_{v=1}^{k} (X_2 - x_v^{(2)}) \right]$$

for suitable $b_k, B_k \in \mathbb{Z}$ s.t. that

$$x_{i+1}^{(r)} = \tilde{f}^{(r)}(x_i^{(1)}, \cdots, x_i^{(N)})$$
$$+ \sum_{k=0}^{n-1} M^{n-k} \cdot \left[b_k \cdot \prod_{v=1}^{k} (x_i^{(1)} - x_v^{(1)}) + B_k \cdot \prod_{v=1}^{k} (x_i^{(2)} - x_v^{(2)}) \right] \quad \cdots (*)$$

for all $i = 1, \cdots, n$. $(x_{n+1} = x_1)$.

We inductively choose coeff.s $b_k, B_k \in \mathbb{Z}$.

Note that given i, $(*)$ only depends on b_k, B_k w/ $k \leq i$.

Assume that for some ℓ, b_k, B_k, $k < \ell$ are chosen so that $(*)$ holds for $i < \ell$

Eqn. $(*)$ for $i = \ell$ reduces to

$$A_1 \cdot b_\ell + A_2 \cdot B_\ell = A.$$

where $A_t = M^{n-\ell} \cdot \prod_{v=1}^{\ell-1} (x_\ell^{(t)} - x_v^{(t)})$. $t = 1, 2$.

$$A = x_{\ell+1}^{(r)} - \tilde{f}^{(r)}(x_\ell^{(1)}, \cdots, x_\ell^{(N)})$$
$$- \sum_{k=1}^{\ell-1} M^{n-k} \left[b_k \cdot \prod_{v=1}^{k-1} (x_\ell^{(1)} - x_v^{(1)}) + B_k \cdot \prod_{v=1}^{k-1} (x_\ell^{(2)} - x_v^{(2)}) \right].$$

Hence, it suffices to show that

$$\gcd(A_1, A_2) \mid A.$$

In other words, we will show that

$$\min\{\operatorname{ord}_p(A_1),\ \operatorname{ord}_p(A_2)\} \leq \operatorname{ord}_p(A) \qquad \forall p.$$

- For each $p < n$, $\quad \operatorname{ord}_p(A) \geqslant (n-\ell+1)\cdot \operatorname{ord}_p(M)$.

  so we will show that $\quad \operatorname{ord}_p(A_t) \leqslant (n-\ell+1)\cdot \operatorname{ord}_p(M)$.

  that is, $\quad \operatorname{ord}_p\left(\prod_{v=1}^{\ell-1} (x_\ell^{(t)} - x_v^{(t)})\right) \leqslant \operatorname{ord}_p(M)$.

  This holds since

  $$x_\ell^{(t)} - x_v^{(t)} \equiv x_{p,\ell}^{(t)} - x_{p,v}^{(t)} \pmod{p^{\operatorname{ord}_p(M)}},$$

  $$\operatorname{ord}_p\left(\prod_{v=1}^{\ell-1} (x_{p,\ell}^{(t)} - x_{p,v}^{(t)})\right) \leqslant \operatorname{ord}_p(M).$$

For each $p \geqslant n$,

$$\min\{\operatorname{ord}_p(A_1),\ \operatorname{ord}_p(A_2)\} = \operatorname{ord}_p(M^{n-\ell}) \cdot \min\left\{\operatorname{ord}_p\left(\prod_{v=1}^{\ell-1}(x_\ell^{(1)} - x_v^{(1)})\right),\ \operatorname{ord}_p\left(\prod_{v=1}^{\ell-1}(x_\ell^{(2)} - x_v^{(2)})\right)\right\}$$

$$= 0.$$

$\blacksquare$