Cours 4

lunedì 8 marzo 2021 13:54

3) Canonical heights for endomorphisms of $\mathbb{P}^k$.

1) Introduction

Goal. $\mathbb{K}$ number field, $f \in \mathbb{K}(T)$, $\deg(f) = d \geq 2$

We want to show that $\mathrm{Preper}(f, \mathbb{K}) = \{x \in \mathbb{P}^1(\mathbb{K}),\ \mathcal{O}_f(x) \text{ is finite}\}$ is finite.

We will discuss higher dimensional dynamical systems.

↳ dynamical heights.

· What is a height? tool introduced by Weil (when working on the Mordell conjecture: bound torsion points of abelian varieties over a number field).

It is a function $h : \mathbb{Q}^{alg} \to \mathbb{R}_+$ (or more generally $h : X(\mathbb{Q}^{alg}) \to \mathbb{R}_+$)

that measures the "complexity" of a point $x \in \mathbb{Q}^{alg}$.

· Canonical height: "height function" such that $h_f \circ f(x) = d \cdot h_f(x)$

Observation: suppose that you know that $\{x \in \mathbb{P}^1(\mathbb{K}),\ h_f(x) = 0\}$ is finite.

Then $\mathrm{Preper}(f, \mathbb{K}) \subseteq \{h \circ f = 0\} \cap \mathbb{P}^1(\mathbb{K})$ is also finite.

NORTHCOTT PROPERTY.

Hence to prove our result, it suffices to construct a height associated to f, and with the Northcott property.

Standard height (a.k.a naive)

$x \in \mathbb{Q}$, $x = \frac{a}{b}$ $a \wedge b = 1$ $\qquad h(x) = \log \max\{|a|, |b|\}$.

$h(x) = \#\{\text{digits necessary to define } x\}_{\sim}$ (if $\log_b$, in base b).

Goal: extend h to $\mathbb{Q}^{alg}$.

Idea 1: $x \in \mathbb{Q}^{alg}$, take its minimal polynomial $/\mathbb{Q}$:

$P(T) = a_0 T^d + \dots + a_d \qquad a_0 \in \mathbb{Z},\ \gcd(a_i) = 1,\ a_0 \neq 0$.

We can set $\bar{h}(x) = \frac{1}{d} \log \max\{|a_i|\}$

We can set $\bar{h}(x) = \frac{1}{d} \log \max \{|a_i|\}$

Lemma: $\cdot\ \bar{h}(x) = h(x)$ if $x \in \mathbb{Q}$.

$\cdot\ \bar{h}(\sigma(x)) = \bar{h}(x) \quad \forall \sigma \in Gal(\mathbb{Q}^{alg}/\mathbb{Q})$

$\cdot$ Northcott $N < +\infty$, $H < +\infty$.

$\mathcal{E}(N,H) := \{x \in \mathbb{Q}^{alg}, \deg(x) \leq N, \bar{h}(x) \leq H\}$ is finite

Proof. $x \in \mathcal{E}(N,H)$. P, a_i as above then $|a_0| \leq \exp(NH)$

$\leadsto \mathrm{Card}\, \mathcal{E}(N,H) \leq (2e^{NH}+1)^{d+1} < +\infty$ $\square$

Problem: $\bar{h}$ is hard to handle, and to relate $\bar{h}$ to arithmetic properties of x.

Idea 2: interpretation of $h(x)$ with $x \in \mathbb{Q}$ in terms of p-adic norms.

Recall: $x = \frac{a'}{b'} p^n$, $a' \wedge p = b' \wedge p = 1 \leadsto |x|_p := p^{-n}$.

Lemma: $x \in \mathbb{Q}$. Then

$$\underbrace{h(x) =}_{H(x) :=} \log^+ |x|_\infty + \sum_{p \in \mathcal{P}} \log^+ |x|_p \qquad \log^+ t = \max\{0, \log t\}$$

$|x|_\infty$ = euclidean norm. $\mathcal{P} = \{\text{primes}\}$

Proof: $x = \prod_{p \in \mathcal{P}} p^{v_p(x)} \qquad v_p(x) \in \mathbb{Z} \quad$ (for all but finitely many p, $v_p(x) = 0$).

$$\log^+ |x|_\infty + \sum_{p \in \mathcal{P}} \log^+ |x|_p = \log^+ |x|_\infty - \sum_{v_p(x) < 0} v_p(x) \log p$$

since $\left| p^{v_p(x)} \right| = p^{-v_p(x)} \qquad \log^+ |x|_p = \begin{cases} 0 & v_p(x) \geq 0 \\ -v_p(x) \log p & v_p(x) < 0 \end{cases}$

Hence $$H(x) = \begin{cases} \log |x|_\infty - \sum_{v_p(x)<0} v_p(x) \log p & |x|_\infty \geq 1 \quad \overset{?}{=} \log |a| \\ - \sum_{v_p(x)<0} v_p(x) \log p & |x|_\infty < 1 \quad \overset{?}{=} \log |b| \end{cases}$$

We conclude by observing that $b = \prod_{v_p(x)<0} p^{-v_p(x)}$. $\square$

Aim: extend this formula to any number field $\mathbb{K}/\mathbb{Q}$.

I'd like to have, $\forall x \in \mathbb{K}$, "$h(x) = \sum_{v \in M_{\mathbb{K}}} \log^+ |x|_v$." $M_K \overset{"}{=}{}^{"} \{\text{set of norms on } \mathbb{K}\}$.

($\nwarrow$ not exactly)

2) Metrised fields.

Def: A metrised (normed) field is a pair $(\mathbb{K}, |\cdot|)$, with $\mathbb{K}$ a field, and $|\cdot| : \mathbb{K} \to \mathbb{R}_+$, s.t.

$$\begin{cases} |x| = 0 \iff x = 0 \\ |xy| = |x| \cdot |y| \\ |x+y| \leq |x| + |y| \end{cases}$$

Example: trivial norm $|x|_0 = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$

Def: A metrised field is archimedean if for all $x \neq 0$ $\exists n > 0$ s.t. $|nx| > 1$.

Examples: $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, $|\cdot|_\infty =$ euclidean norm

(or any subfield of $(\mathbb{C}, |\cdot|_\infty)$)

Thm (Gelfand - Mazur) $(\mathbb{K}, |\cdot|)$ complete archimedean metrised field.

Then $(\mathbb{K}, |\cdot|) \simeq (\mathbb{R}, |\cdot|_\infty^\varepsilon)$ or $\simeq (\mathbb{C}, |\cdot|_\infty^\varepsilon)$, $\varepsilon \in (0,1]$

Sketch of proof: $|nx| > 1 \Rightarrow \operatorname{char}(\mathbb{K}) = 0$. $\Rightarrow \mathbb{K} \supseteq \mathbb{Q}$. Ostrowski $\Rightarrow$

$|\cdot|\big|_{\mathbb{Q}} = |\cdot|_\infty^\varepsilon$. $\Rightarrow \mathbb{K}$ is an extension of $(\mathbb{R}, |\cdot|_\infty^\varepsilon)$ $\quad$ $M_{\mathbb{Q}} = \left\{ \begin{matrix} |\cdot|_\infty \\ |\cdot|_p, p \in \mathcal{P} \end{matrix} \right\}$.

Gelfand - Mazur $\Rightarrow \mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. $\square$

Lemma $(\mathbb{K}, |\cdot|)$ metrised field. TFAE:

(i) $(\mathbb{K}, |\cdot|)$ is not archimedean

(ii) $(\mathbb{K}, |\cdot|)$ is non-archimedean: $|x+y| \leq \max\{|x|, |y|\}$.

Proof: (ii $\Rightarrow$ i) $|nx| \leq |x|$ by induction on n.

(i $\Rightarrow$ ii) Take $x, y \in \mathbb{K}$.

$$|x+y| = |(x+y)^n|^{\frac{1}{n}} = \Big| \sum_{j=0}^{n} \underbrace{\binom{n}{j}}_{\in \mathbb{N}} x^j y^{n-j} \Big|^{\frac{1}{n}} \qquad \left|\binom{n}{j}\right| \leq C \text{ (bounded)}$$

(by not archimedean assumption)

[illegible]

$\in \mathbb{N}$ (by not archimedean assumption)

$$\leq \left(\sum_{j=0}^{n} |x|^j |y|^{n-j} \right)^{\frac{1}{n}} C^{\frac{1}{n}}$$

$\exists x, |nx| \leq 1 \Rightarrow |n| \leq \frac{1}{|x|}$.

$$\leq \left((n+1) \max\{|x|, |y|\}^n \right)^{\frac{1}{n}} C^{\frac{1}{n}} \to \max\{|x|, |y|\} \quad \square$$

Remark: $(\mathbb{K}, |\cdot|)$ is non-archimedean (NA), then $|x| < |y| \Rightarrow |x+y| = |y|$

Example: $p \in \mathcal{P}$ (prime). $|\cdot|_p =$ p-adic norm on $\mathbb{Q}$ is N.A
(easy to check, consequence of the fact that v_p is a valuation: $v_p(0) = \infty$,
$v_p(xy) = v_p(x) + v_p(y)$, $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$).
Set $\mathbb{Q}_p$ = completion of $(\mathbb{Q}, |\cdot|_p)$.
$(\mathbb{Q}_p, |\cdot|_p)$ is a NA complete metrized field.

Lemma $(\mathbb{K}, |\cdot|)$ NA complete metrized field.
$\mathbb{K}^\circ := \{x \in \mathbb{K}, |x| \leq 1\}$ is a ring (the ring of integers of $\mathbb{K}$)
$\mathbb{K}^{\circ\circ} := \{x \in \mathbb{K}, |x| < 1\}$ is the unique maximal ideal of $\mathbb{K}^\circ$
(in particular, $\mathbb{K}^\circ$ is a local ring).
One may consider: $\tilde{\mathbb{K}} = \mathbb{K}^\circ / \mathbb{K}^{\circ\circ}$, it is a field, called the residue field of $\mathbb{K}$.
$\pi : \mathbb{K}^\circ \to \tilde{\mathbb{K}}$ the projection map is called the residue map.
For $x \in \mathbb{K}^\circ$, we denote $\pi(x) =: \tilde{x}$ its class.

Proof of lemma:
$\mathbb{K}^\circ$ is a ring: $0 \in \mathbb{K}^\circ$, $x, y \in \mathbb{K}^\circ \Rightarrow xy \in \mathbb{K}^\circ$ (this holds $\forall |\cdot|$)
· $x + y \in \mathbb{K}^\circ$ by $|x+y| \leq \max\{|x|, |y|\}$ (N.A).
$\mathbb{K}^{\circ\circ}$ is an ideal of $\mathbb{K}^\circ$ and it is the unique maximal ideal, because $\mathbb{K}^\circ \setminus \mathbb{K}^{\circ\circ} = \{x \in \mathbb{K} \mid |x| = 1\}$ consists of units in $\mathbb{K}^\circ$. $\square$

Example: $\mathbb{K} = \mathbb{Q}_p$, $|\cdot|_p$

$|\mathbb{K}^\times|$ = value group of $(\mathbb{K}, |\cdot|) = \{|x| : x \in \mathbb{K}^\times\}$.

$|\mathbb{Q}^\times|_p = p^{\mathbb{Z}}$, $|\mathbb{Q}_p^\times|_p = p^{\mathbb{Z}}$. In fact $x \in \mathbb{Q}_p^\times$, $\exists x_n \in \mathbb{Q}$,

$|x_n - x|_p \to 0$. $\Rightarrow \forall n >> 1$, $|x_n - x|_p < |x|_p \Rightarrow |x_n|_p = |x_n - x + x|_p = |x|_p$.

- $\mathbb{Z}_p \overset{\text{def}}{=} \mathbb{Q}_p^\circ = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$

Claim: $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $(\mathbb{Q}_p, |\cdot|_p)$.

Proof: $x \in \mathbb{Z}$, $|x| \leq 1$, $|x|_p < 1 \iff p \mid x$. $\Rightarrow \overline{\mathbb{Z}} \subseteq \mathbb{Z}_p$.

$x \in \mathbb{Z}_p$, $|x|_p \leq 1$, $x = \lim_n x_n$, $x_n \in \mathbb{Q}$ (want to pick $x_n \in \mathbb{Z}$)

$x_n = \frac{a_n}{b_n}$, $|x_n| \leq 1 \Rightarrow p \wedge b_n = 1$ find β_n, $\beta_n b_n \equiv 1 \pmod{p^{n^2}}$

$$|x - a_n\beta_n|_p \leq \max\{\underbrace{|x - x_n|}_{\to 0}, \left|\frac{a_n}{b_n}\right| \underbrace{|1 - \beta_n b_n|}_{\to 0}\} \qquad \square$$

$\mathbb{Q}_p^{\circ\circ} = \{|x|_p < 1\} = \{|x|_p \leq \frac{1}{p}\} = p\mathbb{Z}_p$.

$$\widetilde{\mathbb{Q}}_p = \mathbb{Q}_p^\circ / \mathbb{Q}_p^{\circ\circ} \simeq \frac{\mathbb{Q} \cap \mathbb{Z}_p}{\mathbb{Q} \cap p\mathbb{Z}_p} = \{\tfrac{a}{b} : b \wedge p = 1\} \big/ \{\tfrac{a}{b} : b \wedge p = 1,\ p \nmid a\}$$

$$\begin{array}{ccc} \frac{a}{b} & & \\ \downarrow & & \downarrow \text{ isomorphism} \\ \frac{a}{b} & & \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \end{array}$$

Lemma: $(\mathbb{Z}_p, |\cdot|_p)$ is compact.

Proof: reasons: $|\mathbb{Q}_p^\times|$ is discrete, $\widetilde{\mathbb{Q}}_p$ is finite

We will check that it is sequentially compact ($\overset{\text{metric spaces}}{\iff}$ compact)

$x_n \in \mathbb{Z}_p$, $\tilde{x}_n \in \mathbb{F}_p$. For all $n \geq 2$, may assume that $\tilde{x}_n = \tilde{a}_0 \in \{0, \ldots, p-1\}$.

(up to subsequences). But then $|x_n - a_0|_p < 1$ $\forall n \geq 2$ and $|x_n - a_0|_p \leq \frac{1}{p}$.

[illegible]

(up to subsequences). But then $|x_n - a_0|_p < 1 \ \forall n \geq 2$, and $|x_n - a_0|_p \leq \frac{1}{p}$.

Proceed by recursion & diagonal extraction:

Here $\frac{x_n - a_0}{p} \in \mathbb{Z}_p$, may assume $\widetilde{\frac{x_n - a_0}{p}} = \tilde{a}_1 \ \ldots$

By induction we get $x_n \to a_0 + p a_1 + \ldots = \underbrace{\sum_{i \in \mathbb{N}} a_i p^i}_{\in \mathbb{Z}_p}$, $a_i \in \{0, \ldots, p-1\}$. $\square$

Def: A p-adic field is a complete metrised field of char 0 $(\mathbb{K}, |\cdot|)$ such that $|\cdot||_{\mathbb{Q}} = |\cdot|_p$.

Ex: $\mathbb{K} = \mathbb{Q}_p$.

Thm: Let $\mathbb{K}$ be a finite field extension of $\mathbb{Q}_p$.
Then there exist a unique extension of the p-adic norm $|\cdot|_p$ to $\mathbb{K}$.
Moreover, $(\mathbb{K}, |\cdot|_p)$ is complete.

Proof: (!) Let $|\cdot|_1$ and $|\cdot|_2$ be two norms on $\mathbb{K}$ whose restriction to $\mathbb{Q}_p$ are equal to $|\cdot|_p$. We first show that they are equivalent.

Write $\mathbb{K} = e_1 \mathbb{Q}_p + \ldots + e_n \mathbb{Q}_p$ (being $\mathbb{K}$ a finite extension of $\mathbb{Q}_p$).

Consider the product norm $\underset{\mathbb{K}}{\|x\|} = \|\sum_{i=1}^n \underset{\mathbb{Q}_p}{x_i} e_i\| := \max |x_i|_p$.

$|x|_1 = |\sum x_i e_i|_1 \leq \max |e_i|_1 \cdot |x_i|_p \leq C_1 \cdot \|x\|$.

$\Rightarrow x \mapsto |x|_1$ is continuous for $\|\cdot\|$.

Set $\alpha := \inf_{\|x\|=1} |x|_1$. We show that $\alpha > 0$. In fact, $\{\|x\| = 1\}$ is compact, being a closed subset of $\mathbb{Z}_p^n$, which is compact.

Then $|x|_1 \geq \alpha \|x\|$. and $|\cdot|_1$ and $\|\cdot\|$ are equivalent.

Repeating the argument for $|\cdot|_2$, we get that $|\cdot|_1$ and $|\cdot|_2$ are equivalent. In particular $|x|_1 \leq C |x|_2$ (C constant).

$\Rightarrow |x|_1 = |x^n|_1^{\frac{1}{n}} \leq (C |x^n|)^{\frac{1}{n}} \to |x|_2$. $\Rightarrow |\cdot|_1 \leq |\cdot|_2$.

By symmetry, $|\cdot|_1 = |\cdot|_2$.

By symmetry, $|\cdot|_1 = |\cdot|_2$.

(∃) one uses the relative norm:

$$N_{K/\mathbb{Q}_p} : K^\times \longrightarrow \mathbb{Q}_p^\times \quad (\text{morphism})$$

$$\underset{K}{\overset{\cup}{x}} \mapsto \det(y \mapsto xy) \quad (\text{seen in } K = e_1\mathbb{Q}_p + \dots + e_n\mathbb{Q}_p)$$

$y \in K$, $xy \in K$; $y \mapsto xy$ is linear.

If $K/\mathbb{Q}_p$ is Galois, $N_{K/\mathbb{Q}_p}(x) = \prod_{\sigma \in Gal(K/\mathbb{Q}_p)} \sigma(x)$.

Define $|x|_K := \left| N_{K/\mathbb{Q}_p}(x) \right|_p^{\frac{1}{n}}$, where $n = [K : \mathbb{Q}_p]$.

$N_{K/\mathbb{Q}_p}(x) \in \mathbb{Q}_p$

It is a norm:

$|x|_K = 0 \iff x = 0$; $|\cdot|_K\big|_{\mathbb{Q}_p} = |\cdot|_p$, $|xy|_K = |x|_K \cdot |y|_K$ are easy.

The point is to prove the triangular inequality.

- $x \mapsto |x|_K$ is C^0 for $\|\cdot\|$ (exercise, it is polynomial in coordinates.)

- by compactness $\exists C$, $|x|_K \geq \frac{1}{C} > 0$ $\forall x$, $\|x\| = 1$.
  $|x|_K \leq C$ $\forall x$, $\|x\| \leq 1$

$$|x+y|_K = \left|y\left(1+\frac{x}{y}\right)\right|_K \leq C|y|_K \qquad \|x\| \leq \|y\|$$

$$|x+y|_K \leq C \max\{|x|_K, |y|_K\} \therefore$$

$$|x+y|_K = |(x+y)^n|_K^{\frac{1}{n}} \leq \underset{\downarrow\, 1}{C^{\frac{1}{n}}} \max\{|x|, |y|\}$$

□

Rem: the fact that it is complete is because $|\cdot|_p$ is equivalent to $\|\cdot\|$, Rem: the fact that it is complete is because $|\cdot|_p$ is equivalent to $\|\cdot\|$, which is complete.

Consequence: $\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$, $|\sigma(x)| = |x|$ $\forall x \in K$.

(by uniqueness of the extension).

Lemme: Assume $[K:\mathbb{Q}_p] < +\infty$. Then:

- $\tilde{K}$ is a finite field extension of $\tilde{\mathbb{Q}}_p = \mathbb{F}_p$.

$f_K = [\tilde{K} : \tilde{\mathbb{Q}}_p] \geq 1$ is called the irreducible degree

- $|K^\times| = p^{\mathbb{Z}p/e_K}$, $e_K \geq 1$, e_K = ramification index.
- $[K:\mathbb{Q}_p] = e_K \cdot f_K$

Proof (Robert, "A course in p-adic analysis", pp 98-100).

$\to (K, |\cdot|) \underset{\text{equivalent}}{\simeq} (\mathbb{Q}_p^n, \|\cdot\|)$, $n = [K:\mathbb{Q}_p]$. $\Rightarrow$ locally compact & complete.

$\Rightarrow K^\circ = \overline{B(0,1)} = \{|x| \leq 1\}$ is compact.

claim: $K^{\circ\circ} = \mathring{B}(0,1) = \{|x| < 1\}$ is also compact, since K° is compact, and $K^{\circ\circ}$ is closed in K°: $x_n \to x$, then $\forall n >> 1$, $|x_n| = |x_\infty|$.

For any residue class $\tilde{\xi} \in \tilde{K}$, choose an element ξ in K. We get the open cover

$$K^\circ = B(0,1) \bigsqcup_{\tilde{\xi} \in \tilde{K}} B(\xi, 1)$$

$B(\xi, 1) = \{x \in K, |x - \xi| < 1\} = \{x \in K^\circ, \tilde{x} = \tilde{\xi}\}$.

By compactness of K°, the cover $B(0,1) \bigsqcup_{\tilde{\xi} \in \tilde{K}} B(\xi,1)$ admits a finite subcover $\Rightarrow \tilde{K}$ is finite (ξ belongs only to $B(\xi,1)$ in the covering).

$|K^\times|$ is a subgroup of $(\mathbb{R}_+^\times, \times)$ $<$ discrete or dense

Since $K^{\circ\circ}$ is compact, $\sup_{\substack{x \neq 0 \\ |x| < 1}} |x|$ is attained. $\Rightarrow |K^\times|$ is discrete

Moreover $|K^\times| \supset |\mathbb{Q}_p^\times|$ $\Rightarrow$ $|K^\times| = p^{\mathbb{Z}/e_K}$

$|x|<1$

Moreover $|K^\times| \supseteq |\mathbb{Q}_p^\times| \Rightarrow |K^\times| = p^{\mathbb{Z}/e_K}$.

How to prove $n = [K:\mathbb{Q}_p] = [\tilde{K}:\mathbb{Q}_p] \times e_K$

choose $\left| \begin{array}{l} \pi \in K^{\circ\circ} \quad |\pi| = p^{1/e_K}. \\ s_1 \dots s_f \in K^\circ \text{ s.t. } \tilde{s}_1 \dots \tilde{s}_f \text{ generate } \tilde{K} \text{ over } \mathbb{F}_p \end{array}\right.$

$f = f_K \rightarrow$

The family $(s_i, \pi^j)_{\substack{1\le i\le f\\ 1\le j\le e}}$ is a basis of $K/\mathbb{Q}_p$ (not easy, see [Robert])