Introduction to arithmetic dynamics

7r1420

Moscow October 2018.

(1) What is arithmetic dynamics?

Strange term coined by J. Silverman in the 90's that mixes two a priori very different subjects.

- arithmetic = study of rational numbers, or equations with integral coefficients in finite extensions of $\mathbb{Q}$.

(ex)

$$\begin{aligned}\Phi_4(z,c) = {} & z^{12} + (6c)z^{10} + z^9 + (3c+15c^2)z^8 + 4cz^7 \\ & + (1+12c^2+20c^3)z^6 + (2c+6c^2)z^5 + (4c+3c^2+18c^3+15c^4)z^4 \\ & + (1+4c^2+4c^3)z^3 + (c+5c^2+6c^3+12c^4+6c^5)z^2 \\ & + (2c+c^2+2c^3+c^4)z + (1+2c^2+3c^3+3c^4+3c^5+c^6).\end{aligned}$$

has no solution $(z,c) \in \mathbb{Q}$. (Morton 1998).

- dynamics = focus on the evolution of a system with time concerns with discrete dynamical systems.

X a set $\quad f: X \to X$ map

$$f^n = f^{\circ n} = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}$$

aim = describe the behaviour of the sequence $\{f^n(x)\}_{n\in\mathbb{N}}$ for all $x \in X$.

if X is only a set : 2 cases

- $\{f^n(x)\}$ is finite → x is <u>preperiodic</u>
- $\{f^n(x)\}$ is infinite → x is <u>wandering</u>.

when x is preperiodic, ∃ minimal $q \geq 0$ ~~natural~~ ~~$p \geq 1$~~ s.t. $f^q(x)$ is periodic. i.e $f^N(f^q(x)) = f^q(x)$ for some N

when x is periodic, ∃ minimal $p \geq 1$ s.t. $f^p(x) = x$
<u>exact period</u>

<u>notation</u> $\text{Prep}(f) = \{x \in X,\ \{f^n(x)\} \text{ is finite}\}$.

$\text{Per}_n(f) = \{\text{periodic points of } f \text{ of period } n\}$

<u>remark</u>: usually one puts more structure on X = topological, smooth, group...

may want to describe the <u>ω - limit set</u>

$$\omega(x) = \bigcap_{n \geq 0} \overline{\bigcup_{m \geq n} \{f^m(x)\}}$$

<u>Arithmetic dynamics</u> = set of problems that arises when looking at the dynamics of algebraic maps defined over a number field.

↳ series of lectures will focus on a big challenge called the uniform boundedness conjecture stated by J. Silverman

Only partial results, very much open.

$\boxed{\text{Aim}}$ Use algebraic methods to count the # of periodic points for dim 1 algebraic dyn. systems

$\boxed{\text{exp}}$ $f_c(z) = z^2 + c$. $z, c \in \mathbb{Q}$

revisited

$$\text{Per}_4(f_c) = \left\{ \text{zeros of } \frac{f_c^4(z) - z}{f_c^2(z) - z} \right\}$$

$$\underset{\Phi_4(z,c)}{\parallel}$$

$$\boxed{\nexists\, c \in \mathbb{Q} \text{ s.t. } f_c \text{ admits a period 4 point defined over } \mathbb{Q}}$$

② Rational functions in one variable

We shall focus our attention to the dynamics of rational maps.
First discuss the algebraic properties of such maps.

- K = field $\quad f \in K(T)$ rational map of degree $d \geq 1$

$$f = \frac{P(T)}{Q(T)} = \frac{\sum a_i T^i}{\sum b_j T^j} \qquad \max\{\deg(P), \deg(Q)\} = d$$

$$P, Q \neq 0.$$

~~and~~. P and Q have no common factor. (*)

recall $K[T]$ is a unique factorization domain

$$(*) \iff \exists\, U, V \in K[T] \quad UP + VQ = 1.$$

$$\overset{\text{when } K \text{ is alg closed}}{\iff} \quad P^{-1}(0) \cap Q^{-1}(0) = \emptyset.$$

- $X = \mathbb{P}^1(K) \overset{\text{def}}{=} K \cup \{\infty\}.$

$f \in K(T)$ induces a natural map on $\mathbb{P}^1(K)$ $\quad f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$

$$\left[\begin{array}{lll} \cdot \text{ if } x \neq \infty & Q(x) \neq 0 & f(x) = \frac{P(x)}{Q(x)} \in K. \\ \cdot \text{ if } x \neq \infty & Q(x) = 0 & f(x) = \infty \\ \cdot \text{ if } x = \infty & & f(\infty) = \begin{cases} a_d/b_d & \text{if } b_d \neq 0. \\ \infty & \text{if } b_d = 0. \end{cases} \end{array}\right.$$

Lemma $\quad \forall x \in \mathbb{P}^1(K) \quad \operatorname{Card} \underset{\mathbb{P}^1(K)}{\underset{\cap}{f^{-1}(x)}} \leq d.$

proof.

$x \neq \infty \quad \notin f^{-1}(x) \qquad f^{-1}(x) = \{ y \in K, \frac{P(y)}{Q(y)} = x \} \qquad \square.$

/ $\boxed{\text{Prop}}$ K alg. closed

To each $x \in \mathbb{P}^1(K)$ is attached an integer $dg_x(f) \in \{1, \dots, d\}$.
$f \in K(T)$
such that

① $$\sum_{y \in f^{-1}(x)} dg_y(f) = d$$

② $f, g \in K(T)$ $$dg_x(f \circ g) = dg_x(g) \times dg_{g(x)}(f)$$

carK=0

③ $$\Big| \sum{}' \left(dg_x(f) - 1 \right) = 2d - 2$$ ~~(if [illegible])~~

- definition of $dg_x(f)$

$x \neq \infty$ $\quad x' = f(x) \neq \infty$

expand $$f(x+T) = \frac{P(x+T)}{Q(x+T)} = \frac{P(x)\,(1 + \sum \alpha_i T^j)}{Q(x)\,(1 + \sum \beta_j T^j)}.$$

in $K[[T]]$ formal power series $(1 + \sum \beta_j T^j)$ is invertible.

$$f(x+T) = f(x)\left(1 + \sum \gamma_i T^i\right) \qquad \gamma_i \in K$$

$$dg_x(f) = \min\{ i \geq 1,\ \gamma_i \neq 0 \}.$$

- ② $x \in K$ $$g(x+T) = g(x) + \gamma T^{dg_x(g)} + o\left(T^{dg_x(g)}\right).$$

$y = g(x)$ $$f(y+T) = f(y) + \beta T^{dg_y(f)} + o\left(T^{dg_y(f)}\right)$$

$$f\big(g(x+T)\big) = f(y) + \beta\left(+ \gamma T^{dg_x(g)} + \text{h.o.t.}\right)^{dg_y(f)} + \text{h.o.t.}$$

$$= f(y) + \beta \gamma^{dg_y(f)} \, T^{dg_x(g)\, dg_y(f)} + \text{h.o.t.}$$

- extend $dg_x(f)$ to $x = \infty$ and $f(x) = \infty$ using ② and

$$\tau(T) = \frac{1}{T}.$$

• ① case $x = 0$ $f^{-1}(x) \not\ni \infty$

$$f(T) = \frac{P(T)}{Q(T)} \quad d = \deg(P) \geq \deg(Q).$$

$$P(T) = \lambda \prod_{i=1}^{r} (T - y_i)^{m_i}$$

$$f^{-1}(0) = \{y_1, \dots, y_r\}$$

<u>claim</u> $\deg_{y_i}(f) = m_i$ ($\Rightarrow$ $d = \sum m_i$ as required).

$$f(T+y_i) = T^{m_i}\left[\lambda \frac{\prod_{j\neq i} (T+y_i-y_j)^{m_j}}{Q(T+y_i)}\right]$$

↑ rational function non vanishing at 0. ///

• ③ $x \in K$ $f(x) \neq \infty$.

$$f(x+T) = f(x)(1+\gamma T^{\deg_x(f)} + \text{hot}).$$

$$f'(x+T) = f(x)\gamma \deg_x(f) T^{\deg_x(f)-1} + \text{hot}.$$

↑ if $\deg_x(f) \wedge \text{car} K = 1$!

x is a root of $f'(T)$ of multiplicity $\deg_x(f) - 1$

$$f'(T) = \frac{P'Q - Q'P}{Q^2}$$

under the assumption $\deg_\infty(f) = 1$

# zeroes of $f' = 2d-2$

w. multiplicities

$\|$

$\deg(P') + \deg(Q) - 1$

↗

highest order term vanishes ! ///

<u>Corollary 1</u> $f, g \in K(T)$

$\deg(f \circ g) = \deg(f) \times \deg(g)$

(apply ① & ②)

<u>Corollary 2</u> car $K = 0$ $f \in K(T)$

$\exists P_f \subset \mathbb{P}^1(K)$ Card $(P_f) \leq 2d-2$

For all $x \notin P_f$ Card $f^{-1}(x) = d$.

4/ <u>Applications</u>

$f \in K(T) \quad d \geq 2$

$\mathrm{Preper}(f, m, n) = \{ x \in \mathbb{P}^1(K) \,,\, f^m(x)$ is periodic of period $n \}$.

is finite.

proof. • $\underset{n}{\mathrm{Per}}(f, n) = \mathrm{Preper}(f, 0, n)$

$\{ f^n(T) = T \} \qquad \deg(f^n) = d^n$.

$$f^n(T) = \frac{P_n(T)}{Q_n(T)}$$

$\mathrm{Per}(f,n) \subseteq \{ P_n(T) = T\, Q_n(T) \}$ Card $\mathrm{Per}(n,f) \leq d^n + 1$.

• $\mathrm{Preper}(f,m,n) = f^{-m}(\mathrm{Per}(f,n))$ Card $\leq d^m (d^n+1)$ ///

Thm. A K alg closed. $d \geq 2$.

$\mathrm{Per} = \bigcup_{n\geq 1} \mathrm{Per}(f,n)$ is infinite

- difficulty a solution of $\{f^n = \mathrm{id}\}$ ~~makes~~ is a solution of $\{f^{nm} = \mathrm{id}\}$ and $p \wedge q = 1$ two primes $\mathrm{Per}(f,p) \cap \mathrm{Per}(f,q) = \emptyset$ the multiplicity might grow.

~~- need to argue that $\mathrm{Per}(f,p)$ is non empty~~

~~- to do so one has to ~~understand~~ interpret dynamically the multiplicity of the root of $P_n - T Q_n$.~~

→ need to define the multiplicity of a fixed periodic point.

Give the proof only for char $K = 0$

6/ if $x \in \mathbb{P}^1(K)$ ⇝ attach $\mu(f, x) \in \mathbb{N}^*$ as follows

$x \in K$ expand $f(x+T) - (x+T) = \sum a_i T^i$

$$\mu(f, x) = \min \{ i, \ a_i \neq 0 \}.$$

$x = \infty$ look at $f\left(\frac{1}{T}\right) - T$

<u>lemma 1</u> $\displaystyle\sum_{f^n(x) = x} \mu(f^n, x) = d^n + 1$

<u>lemma 2</u> for each x $\displaystyle\sup_n \mu(f^n, x) < \infty$

Suppose Per is finite. Replacing f by f^N $N \gg 1$ we may assume

$$\mathrm{Per}(f, n) = \mathrm{Fix}(f) \text{ for all } n$$

$$d^n + 1 \overset{\text{lem ①}}{=} \sum_{f^n(x) = x} \mu(f^n, x) = \sum_{f(x) = x} \mu(f^n, x) \underset{\text{lemma ①}}{<} + \infty$$

Absurd ///

<u>Observation</u> $\left(\begin{smallmatrix}\mathrm{char\,k}\\ \mathbb{Q}\end{smallmatrix}\right)$ Card $\mathrm{Per}(f, n) = d^n + O(1)$ (use some $\mathbb{C}$ dynamics!)

<u>proof of lemma 1</u> $n = 1$ $\infty \notin \mathrm{Fix}(f)$ i.e. $\deg Q = d$.

$P(T) - T\, Q(T)$ has $(d+1)$ solution with mult., x such a solution mult ν.

$$P(T+x) - (T+x)\, Q(T+x) = a\, \cancel{T}^{\nu(x)} + \text{hot} \qquad a \neq 0 \quad \nu \geq 1$$

$Q(x) \neq 0$ hence $\underset{(T+x)}{f(T+x)} = \dfrac{P(T+x)}{Q(T+x)} - (T+x) = \left(aT^{\nu} + \text{hot}\right)\left(Q(x) + \cancel{Q}(1)\right)^{-1}$

$$\Rightarrow \mu(f_1, x) = \nu. \qquad ///$$

<u>proof of lemma 2</u> WLOG $x = 0$

if $\mu \geq 2$ $f(T) = T + aT^{\mu} + \text{hot}$ $f^2(T) = \left(T + aT^{\mu} + \text{ht}\right) + a\left(T + aT^{\mu} + \text{hot}\right)^{\mu}$

$$= T + 2aT^{\mu} + \text{hot}.$$

induction $f^n(T) = T + anT^{\mu} + \text{hot}.$ $\neq 0$ since char $K = 0$

7 if $\mu = 1$ ~~[illegible]~~ $f(T) = \underset{\text{I multiplier}}{\lambda}\, T + \text{hot}.$

↳ TSVP

$p =$ minimal $\{k,\ \lambda^k = 1\}$

$\underline{p = \infty} \Rightarrow \mu(f^n, x) = 1 \quad \forall n$

<u>otherwise</u> $\quad p \nmid n \Rightarrow \mu(f^n, x) = 1$

$\quad mp = n \quad \mu(f^n, x) = \mu((f^p)^m, x) = \mu(f^p, x)$.

<u>Exercise</u> = generalize to char $K > 0$

$\rightsquigarrow$ <u>lemma 2'</u> $\quad x \in \mathbb{P}^1(K) \quad \sup_{n \wedge p = 1} \mu(f^n, x) < \infty$

$\rightsquigarrow$ if $\cup \mathrm{Per}(f^n)$ is finite $\quad$ take $n \wedge p = 1 \quad \cup \mathrm{Per}(f^n) = \mathrm{Fix}(f)$

$$d^n + 1 = \sum \mu(f^n, x) = \sum_{\mathrm{Fix}(f)} \mu(f^n, x) < \infty \qquad \blacksquare$$

③ Preperiodic points over a number field

Number field K is a finite extension of $\mathbb{Q}$.

recall K is a finite dimensional $\mathbb{Q}$-vector space of dimension $[K:\mathbb{Q}]$

K is isomorphic to $\mathbb{Q}[T]/(P)$ $P \in \mathbb{Q}[T]$ irreducible

Fix L/K any field extension (e.g. $L = \mathbb{C}$ $K = \mathbb{Q}$!).

$f \in K(T)$ $d \geq 2$

Lemma Preper(f,L) is a countable set included in the algebraic closure of K in L

proof . - countable set follows from previous lemma

- Preper$(f,m,n,L) = \{x \in L,\ f^m(x) \text{ is periodic of period } n\}$

$$\subseteq \{ \underbrace{f^n(f^m(T)) = f^m(T)}_{\text{polynomial equation with coefficients in } K} \}$$

///

Thm B $f \in K(T)$ $d \geq 2$ K number field

Preper(f,K) is a finite set

Surprising ! in view of thm A

<u>example 1</u>

$M_d(T) = T^d$ $\quad M_d^n(T) = T^{d^n}$

$\text{Preper}(M_d) = \{0\} \cup \{\infty\} \bigcup_{\substack{m \geq 0 \\ n \geq 1}} \{x \in K^\times,\ x^{d^{m+n}} = x^{d^m}\}$

$= \{0\} \cup \{\infty\} \cup \{$roots of units any in K$\}$

$[$if $\zeta \in \Phi_N$ $\zeta^k \in \Phi_N$ for all $k \geq 1]$

if K is alg. closed ⇝ infinite

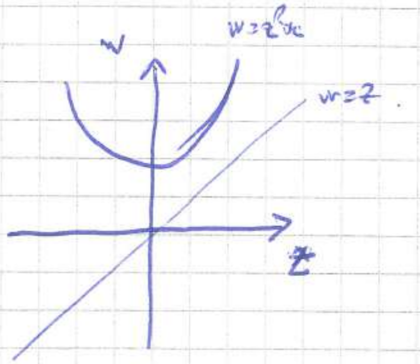
if K is a number field ⇝ finite

indeed $\deg_{\mathbb{Q}}(e^{\frac{2i\pi p}{q}}) = \varphi(q)$ Euler totient function $\xrightarrow{q \to +\infty} \infty$

$p \wedge q = 1$ $\quad \overset{\text{"}}{} \#\{n < q,\ n \wedge q = 1\}$

<u>example 2</u>

$K = \mathbb{R}$ $\quad f_c(z) = z^2 + c$



- $c > 1/4$ $\quad \text{Preper}(f_c, \mathbb{R}) = \emptyset$

$[$indication: $f_c(z) > 0$.

$z > 0 \Rightarrow f_c(z) \geq (1+\varepsilon)|z|\ ]$

- $c = 0$ $\quad \text{Preper}(f_c, \mathbb{R}) = \{0, \pm 1\}$ finite.
- $c < -2$ $\quad \text{Card Per}(f_c, n, \mathbb{R}) = 2^n$.

⇝ basic exercise in dynamics! <u>Lemma</u> ‖ ∃ 2 closed intervals I_+ I_- $|f'|$ on $I_\pm > 1$ $\quad f(I_\pm) \supset I_+ \cup I_-$.

- Various phenomena between

⇝ exercise $\quad c \in]-\frac{3}{4}, 1/4]$ $\#\text{Preper}(f_c, \mathbb{R}) = 3$.

⇝ exercise $\quad c = -2$ $\quad \text{card Per}(f_c, n, \mathbb{R}) = 2^n$ (Tchebyshev!) $\boxed{\text{TSVP}}$

The whole picture is described in the seminal paper of

Milnor & Thurston "on iterated maps of the interval" §8, §9.

~~Thm (MT, Sarkovskii, ...)~~

~~• if $c \leq c_{Fei}$ $\frac{Per(f_c, n, \mathbb{R})}{s^n} \to 1$ for some $s > 1$~~

~~• if $c > c_{Fei}$ $Per(f_c, \mathbb{R})$ is finite.~~

~~$(s = e^{h_{top}(f_c, \mathbb{R})})$ $c_{Fei} = 1{,}401155\ldots$~~

Thm (Sharkovskii, MT, ...) $c_{Fei} = -1{,}401155$.

• $c < c_{Fei}$ $\exists s > 1$ (in fact $s = \exp h_{top}(f, \mathbb{R})$) st. $\overline{\lim}_n \frac{1}{s^n} Per(f_c, n, \mathbb{R}) \geq \alpha > 0$ and finite.

• $c = c_{Fei}$ for each n Card $Per(f_c, n, \mathbb{R})$ $\begin{cases} = n & \text{if } n \text{ is a power of } 2 \\ = 0 & \text{otherwise} \end{cases}$

• $c > c_{Fei}$ $Per(f_c)$ is finite.

→ first statement MT §9

→ second statement MT §14 example 14.6

→ third statement not well treated in the literature. (use renormalization)

in fact $\exists !$ period 2^n attracting orbit and in $\mathbb{R}$ all but the preimages of period 2^{n-1} converge to that point!

9/

~~Thm (Lyubich, Swiatek, Graczyk, Jakobson)~~

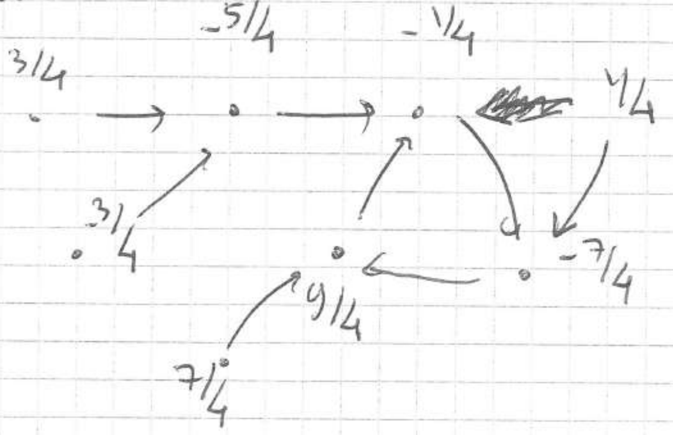
~~① there exists a positive measure of parameters $c \in [-2, \frac{1}{4}]$ s.t. $\# \mathrm{Per}(f_c, \mathbb{R}) \to \infty$~~

~~② there is a open and dense subset of parameters $c \in [-2, \frac{1}{4}]$ s.t. $\# \mathrm{Per}(f_c, \mathbb{R})$ finite~~

(but Preper is infinite !)

<u>example 3</u> $f_{*}(z) = z^2 - \frac{29}{16}$.

closer look



<u>Prop</u> $\mathrm{Card}(\mathrm{Preper}(P_*, \mathbb{Q})) = 1 + 8$

<u>proof</u> ∞ is fixed !

Suppose $z \in \mathbb{Q}$ is preperiodic.

- p prime ≥ 3 recall p-adic norm $|a+b| = |a|$ if $|a| > |b|$

$|z|_p \leq 1$ otherwise $|f_*(z)| = |z|^2$

and by induction $|f^n_*(z)| = |z|^{2^n} \to \infty$

- real norm

$|z| \leq 2$ otherwise

$|z^2 - \frac{29}{16}| \geq 4 - \frac{29}{16} > 2$

$2|z| - \frac{29}{16} \geq (1 + \frac{1}{4})|z|$

- 2-adic norm

$|z|_2 \leq 4$ otherwise $|z|_2 \geq 8$.

$|P^n_*(z)| = |z|^{2^n} \to \infty$

$\leadsto$ only possibilities $z = \frac{p}{q}$ $q = 1, 2, 4$

$|z| < 2$ ///

<u>Conjecture</u> (Poonen) $f_c(z) = z^2 + c$

1. For any $c \in \mathbb{Q}$ $\mathrm{Card}(\mathrm{Preper}(f_c, \mathbb{Q})) \leq 9$

2. For any $c \in \mathbb{Q}$, for any $N \geq 4$ $\mathrm{Per}(f_c, N) \cap \mathbb{Q} = \emptyset$.

$\leadsto$ ① is optimal

$\leadsto$ ② is known for $N = 4$ & 5.

(4) The uniform boundedness conjecture

Far reaching generalization of Poonen's conjecture!

UBC (Silverman)

Fix $N \geq 1$ and $d \geq 2$.
There exists a constant $C = C(N, d)$ s.t. for all number field $K/\mathbb{Q}$ $[K:\mathbb{Q}] \leq N$
for all $f \in K(T)$ of degree d

$$\operatorname{Card}\left(\operatorname{Preper}(f, K)\right) \leq C.$$

↳ version of thm B which is uniform in f

Very partial results are known.

Thm C (Benedetto) There exists a constant $C > 0$ s.t.
$c = \frac{p}{q} \in \mathbb{Q}$ $p \wedge q = 1$ $s =$ number of prime factors of q.

$$\operatorname{Card} \operatorname{Preper}(f_c, \mathbb{Q}) \leq C\,(1 + s \log s).$$

⇝ state (and prove!) later a version for number fields

⇝ version of Benedetto's thm due to Garcí, Troncoso, Vishkautsan.

The conjecture was inspired by deep results in arithmetic geometry that I now would like to explain.

4/ K field of char. 0.

$A, B \in K$ s.t. $4A^3 + 27B^2 \neq 0$.

- $E^*_{(A,B)}(K) = \{(x,y) \in K^2 , \ y^2 = x^3 + Ax + B\}$

$E_{(A,B)}(K) = E_{(A,B)}(K) \cup \{\infty\}$

~~[illegible]~~ remark: × $E^*_{(A,B)}$ is ~~a~~ smooth algebraic curve

× if $K = \mathbb{R}$ or $\mathbb{C}$ $E^*_{(A,B)}$ is a $\mathbb{R} / \mathbb{C}$-manifold

~~Abel.~~ Group law on $E_{(A,B)}(K)$ ∞ = identity element

- if $P = (x,y)$ $-P \overset{def}{=} (x,-y)$.

Convention $-\infty = \infty$

- if $P, Q \in E^*_{(A,B)}(K)$ the line L passing through P and Q intersects E at a third point which we define to be $-(P \oplus Q)$

(if $P = Q$ take the tangent line)

~~[illegible]~~ $\boxed{\text{Prop}}$ $(E_{(A,B)}(K), \oplus)$ is an abelian group

(amounts to check the associativity)

Computations $\phi_2 : E_{A,B}(K) \to E_{(A,B)}(K)$

$[P] \mapsto [P] \oplus [P]$

$P = (x,y)$ tangent line at P

$$\epsilon \longmapsto (x + \epsilon 2y, \ y + \epsilon(3x^2+A)).$$

$$(x+2y\epsilon)^3 + A(x+2y\epsilon) + B = (y + \epsilon(3x^2+A))^2$$

12 $\Leftrightarrow$ $t=0$ or ~~$t(3x^2+A)^3$~~ $+ \ \epsilon(8y^3) + 4\cdot 3y^2x = (3x^2+A)^2$

$$\phi_2(x,y) = \left(+ \left[x + 2y \frac{(3x^2+A)^2 - 12xy^2}{8y^3} \right] , * \right)$$

$$\shortparallel$$

$$+ \left(x + \frac{(3x^2+A)^2}{4(x^3+Ax+B)} - 3x \right)$$

$$= -2x + \frac{(3x^2+A)^2}{4(x^3+Ax+B)} = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3+Ax+B)}$$

$$\phi_2(x,y) = \Bigg(\underbrace{\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3+Ax+B)}}_{= L_{A,B}} , * \Bigg)$$

We have proved.

$\boxed{\text{Prop}}$ $A, B \in K$

Let $\pi : E_{(A,B)}(K) \longrightarrow \mathbb{P}^1(K)$

$$\begin{cases} P = (x,y) \longmapsto x \\ \infty \longmapsto \infty \end{cases}$$

then $\pi \circ \Phi_2 = L_{(A,B)} \circ \pi$

$$\begin{tikzcd} E_{(A,B)}(K) \arrow[r, "\text{doubling}", "\text{map}"'] \arrow[d, "\pi"'] & E_{(A,B)}(K) \arrow[d, "\pi"] \\ \mathbb{P}^1(K) \arrow[r] & \mathbb{P}^1(K) \end{tikzcd}$$

<u>obs</u>. Card $\pi^{-1}(x) = 1$ or 2 $\forall x$. Lattès map.

<u>observations</u> • $\deg(L_{A,B}) = 4 \iff 4A^3 + 27B^2 \neq 0$

• $L_{A,B}$ is conjugated to $L_{\lambda^3 A, \lambda^2 B}$.

• π^{-1} Preper $(L_{A,B})$ = Preper $(\phi_2) = \{ P \in E_{A,B}(k) \; [2^m][P] = 2^n[P] \}$

= Torsion points of $E_{A,B}(k)$

Thm (Mordell-Weil)

K number field
then $E_{(A,B)}(K)$ is a finitely generated abelian group.
In other words $E_{(A,B)}(K) \simeq \mathbb{Z}^r \oplus G$
G = finite abelian group.

UBC for $d=4$ $\Longrightarrow$ $\exists\, C(N)$ s.t. for all number field of degree $\leq N$ for all elliptic curve defined over K

$$\text{Card}\left(\text{Torsion}\left(E_{A,B}(K)\right)\right) \leq C(N).$$

$\hookrightarrow$ very deep theorem due to Mazur $N=1$ i.e $K=\mathbb{Q}$
Merel in full generality.