Elliptic Curve

Haiyang Wang

21st / Aug / 18

Let $g(x) \in k[x]$.

Let $f(x,y) = y^2 - g(x)$

E.X. Ex. when $\mathrm{Char}(k) \neq 2$ and $g(x)$ has degree d with distinct root, then all pts in $\underbrace{Z_f(\bar{k})}_{\text{pts of an affine hyperelliptic curve (when } d \geq 4)}$ are non-singular.

Note the automorphism $(x,y) \longrightarrow (x,-y)$

It induces $$Z_f(\bar{k}) \longrightarrow Z_f(\bar{k})$$ $$(a,b) \longmapsto (a,-b).$$

$$F = \text{ff of } k[x,y]/f(x,y) \longrightarrow (\text{it is a field})$$

then $F \longrightarrow F$

$x \longmapsto$

Fix k

when $\deg g = 3$, and F is the homog of f

then $X_F(\bar{k}) = Z_f(\bar{k}) \sqcup \{(0:1:0)\}$ and

and then $g(x)$ has distinct roots in $\bar{k}$.

$X_F(\bar{k})$ is everywhere non-singular.

E.X. Say $k = \mathbb{R}$, Investigate $Z_f(\mathbb{R}) \subseteq \mathbb{R}^2$.

Endow $Z_f(\mathbb{R})$ with the topology induced from $\mathbb{R}^2$. Now we can discuss connect componets of $Z_f(\mathbb{R}^2)$!

Let $g(x) \in \mathbb{R}[x]$, $\deg(g) \geq 2$.

Draw all possible "graph" of $y = g(x)$ when $\deg(g) = 3$

From there, deduce the possible "shapes" fn $Z_f(\mathbb{R})$ when $f(x,y) = y^2 - g(x)$. What are the possible configuration of connected componets!

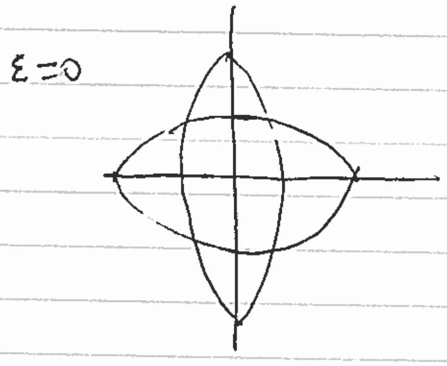
Fn $\deg d \geq 4$

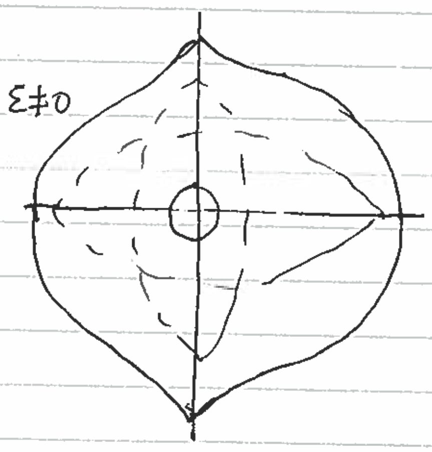
(a). what is the maximal # of connected components that $Z_f(\mathbb{R})$ can have

(c) Can a connected component be just a simple pt! How many such (degenerate) connected components can $Z_f(\mathbb{R})$ have?

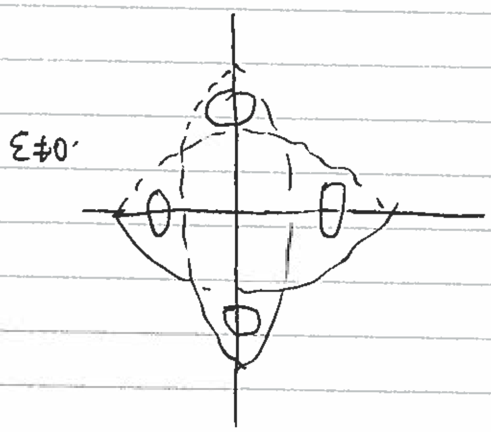
Rk: For $f(x,y)$ of degree d, classifying the connected the connected componts is an open Hilbert Problem.

Ex. $\left.\begin{matrix} g(x,y) \\ h(x,y) \end{matrix}\right\}$ ellipes. $f(x,y) = g(x,y)h(x,y) + \varepsilon \in \mathbb{R}[x,y]$.





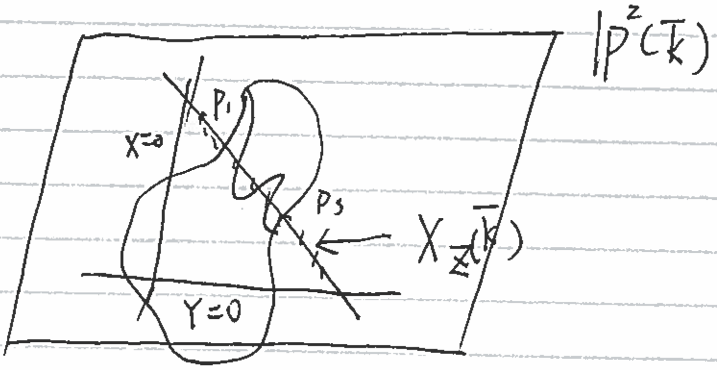
(oval compact).



Ex. Let $F(x,y,z) \in k[x,y,z]$ irreducible. (of postive deg). Then $X_F(\bar{k}) \neq \emptyset$

Falting's k number field, F hom of degree $d \geq 4$

$f(x,y) \rightsquigarrow$ homog $F(x,y,z)$



$$X_F(\bar{k}) = Z_f(\bar{k}) \sqcup \{p_1, \dots, p_s\}$$

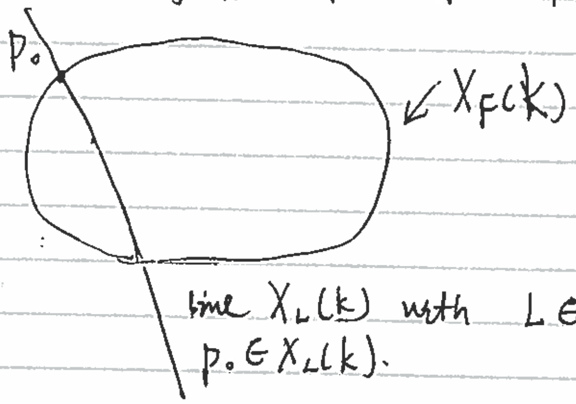
- What happens for $d \leq 3$?

Ex. Let $p_1, p_2 \in \mathbb{P}^2(k)$, Then there exist a linear homogenus $L(x,y,z) \in \underline{k}[x,y,z]$, such that $p_1, p_2 \in X_L(k)$.
↳ (line defined over k) #

$d=1$, Trivial $\deg L = 1$, $L \in k[x,y,z]$.
then $X_L(k) \simeq k \sqcup \{1pt\}$.

$d=2$, .

(Thm) let k be any field, let $F \in k[x,y,z]$ be homogenuous of deg 2, Assume k infinite.
Then, either $X_F(k) = \emptyset$ or $X_F(k)$ is infinite.
(*) Almost true as stated.
Sketch of pf: Assume $p_0 \in X_F(k)$.



line $X_L(k)$ with $L \in k[x,y,z]$ and $p_0 \in X_L(k)$.

Then all lines are of the form $y = mx$, $m \in k$.
The intersection $X_F(k) \cap X_L(k)$ is obtained by:
$f(x, mx) = 0$
$\hookrightarrow$ deg 2 polynomial in general.

we know $f(0,0) = 0$. So this poly in general factors
and has a s root in k
So, in general,
$$X_F(k) \cap X_L(k) = \{$$

Since there are ∞-many lines since k is infinite.
~~not~~ $\Rightarrow X_F(k)$ is infinite

Rk. The statement is easy to prove when f is reducible.
(Assume F irreducible).

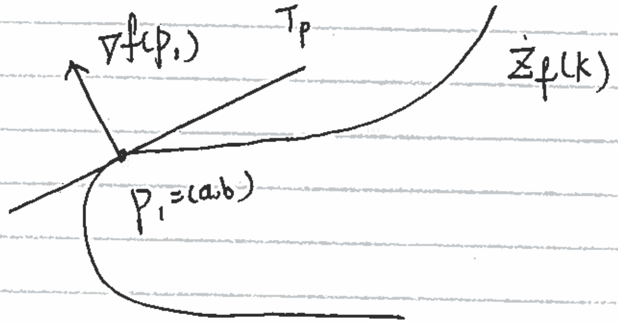
Case
$d=3$

($P_1 \neq P_2$).

E.x. Assume $\deg F = 3$ (F homogeneous in $k[x,y,z]$). Let $P_1, P_2 \in X_F(k)$. Let $L \in k[x,y,z]$ s.t. $P_1, P_2 \in X_L(k)$
(homogeus 1)
If $X_F(k) \cap X_L(k) \neq \{P_1, P_2\}$
then show that $X_F(k) \cap X_L(k) = \{P_1, P_2, P_3\}$
$\hookrightarrow$ (P_3 in k)

we have produced $P_3 \in X_F(\underline{k})$ by 2 given pts $\underline{P_1}, P_2 \in X_{\underline{F}}(\underline{k})$

* degenerate case $P_1 = P_2$. if $P_1 \in X_F(k)$ is non singular,
we can consider the tangent line to $X_F(k)$ at P_1.
(unique line passing $P_1 = (a:b:1)$ and $\perp$ to $\vec{\nabla}_f(a,b)$



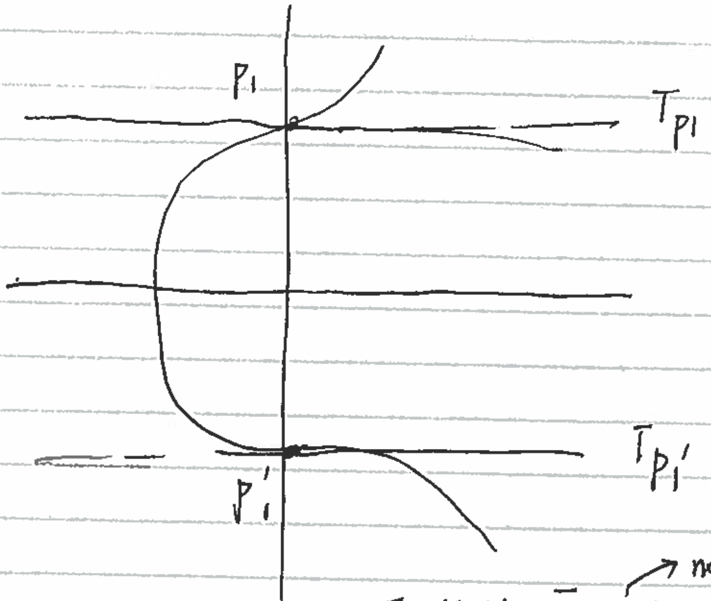
key: T_{p_1} can be defined by a polynomial in $k[x,y]$

Σ.X.

Σ.X. Formula in general for the tangent line at $p=(a:b:c)$ $\in X_F(k)$ using $\vec{\nabla} F(p)$.

Σ.X. Assume $p_1 \in X_F(k)$ nonsingular, if the tangent line at p_1 intersect $X_F(\bar{k})$ in another pt, ⇒ this point is in $X_F(k)$.

Σ.X. Consider $f(x,y) = y^2-(x^3+d^2) \in k[x,y]$.
2 pts: $(0,d)$, $(0,-d)$ $(\text{char}(k) \neq 2)$



$T_{p_1} \cap X_F(\bar{k}) = \{p_1\}$. → not intersect infinitely.

$X_F(k) \cap T_{p_0}$

Thm (Merel 1996). Let k be a number field. Let $F \in k[x,y,z]$ hom of deg 3, and assume $X_F(\bar{k})$ is everywhere nonsingular,
Assume that $\exists\, P_0 \in X_F(k)$

Consider the sequence $\{P_1, \dots\} \subseteq X_F(k)$ obtained using the tangent line.
Then there exists an integer n_0 depending on $[k:\mathbb{Q}]$ only.
such that
if $|\{P_1 \dots\}| > n_0$
$\Rightarrow \{P_1, \dots\}$ is infinite
(uniform bound)

$$\begin{array}{ccc} \mathrm{ff}(k[x,y]/(f)) & \longrightarrow & \mathrm{ff}(k[t]) \\ x & \longrightarrow & g(t) \\ y & \longrightarrow & h(t) \end{array}$$

23rd / Aug / 18

Important tool : reduction module p.

let $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, $p \in \mathbb{Z}$, prime.

$$\mathbb{Z}[x_1, \dots, x_n] \longrightarrow \mathbb{Z}[x_1, \dots, x_n]/(p) \cong (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n].$$

$$f = \sum a_{ij} x^i y^j \dashrightarrow \bar{f} = \sum \bar{a}_{ij} x^i y^j$$

So.

$$\begin{tikzcd} \mathbb{Z}^n \arrow[r] & (\mathbb{Z}/p\mathbb{Z})^n \\ Z_f(\mathbb{Z}) \arrow[u, phantom, "\cup"] \arrow[r] & Z_{\bar{f}}(\mathbb{Z}/p\mathbb{Z}) \end{tikzcd}$$

If $Z_{\bar{f}}(\mathbb{Z}/p\mathbb{Z}) = \phi$, then $Z_f(\mathbb{Z}) = \phi$

Rk. If $Z_f(\mathbb{Z}) \neq \phi$, then $\forall s \geq 1$

$$Z_{f \bmod p^s}(\mathbb{Z}/p^s\mathbb{Z}) \neq \phi$$

(can solve $f(x_1, \dots, x_n) \equiv 0 \mod p^s \quad \forall s$).

$\varprojlim \mathbb{Z}/p^s\mathbb{Z} =: \mathbb{Z}_p$ p-adic integers.

we have

$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$

and $Z_f(\mathbb{Z}) \subseteq Z_f(\mathbb{Z}_p)$.

"problem" There is no good reduction map

$$Z_f(\mathbb{Q}) \dashrightarrow Z_{\bar{f}}(\mathbb{Z}/p\mathbb{Z})$$

E.x. $y^2 = 14x^3 + 2 \qquad (\frac{1}{2}, \frac{1}{2}) \overset{\bmod 2}{\dashrightarrow} ?$

In general, ring O, maximal ideal M,

rendaction field $O/M = k(M) = k$

$f \in O[x_1, \dots, x_n]$

$\Rightarrow$ a reduction map $Z_f(O) \longrightarrow Z_f(k)$

when O is a domain, let $k := ff(O)$

[illegible] (frac. field

hom $f \Rightarrow F$.

would $X_F(k) \dots > X_{F \bmod M}(k)$.

Def Define a reduction map

$$\mathbb{P}^2(k) \longrightarrow \mathbb{P}^2(k)$$

$$(a:b:c) \longmapsto ?$$

$k = ff(\mathcal{O})$. $\quad a = \frac{a_1}{a_2} \quad a_1, a_2 \in \mathcal{O}$

$b = \frac{b_1}{b_2} \quad b_1, b_2 \in \mathcal{O}$

$c = \frac{c_1}{c_2} \quad c_1, c_2 \in \mathcal{O}$

clear denominator

$$\begin{tikzcd}
(a_2b_2c_2)(a;b;c) = (a_1(b_2c_2), b_1(a_2c_2), c_1(a_2b_2)) \arrow[d, "\mathrm{Mod}\ M"] \\
(\overline{a_1b_2c_2}, \overline{b_1a_2c_2}, \overline{c_1a_2b_2})
\end{tikzcd}$$

! it may happen that mod M, we get $(\bar{0}, \bar{0}, \bar{0})$, which is not in $\mathbb{P}^2(k)$.

We should try to clear the denominators, s.t. the new vectors is not in $M \times M \times M$.

1. This may not true, even $\mathcal{O}$ is UFD.

e.g. $\mathcal{O} = \mathbb{F}[u,v] \subset k = \mathbb{F}(u,v)$; $\quad M = (u,v)$

Consider $(\frac{1}{u} : \frac{1}{v} : 1) \in \mathbb{R}^2(k)$.

$$\downarrow uv$$

$$(v : u : uv)$$

Claim: We can do that!

if O is PID

O is a Dedekind domain.

O is a local PID (also called discrete valuation ring).

Assume O is a PID, Then $M = \overset{\text{Maximal ideal}}{(\pi)}$. for some $\pi \in O$

$$\forall a \in O, \quad a = \pi^{\operatorname{ord}_\pi(a)} \cdot \alpha \quad \text{with } \alpha \in O,\ \alpha \notin (\pi).$$

Then $\frac{a}{b} \in k$, $a, b \in O$: $\operatorname{ord}_\pi(\frac{a}{b}) = \operatorname{ord}_\pi(a) - \operatorname{ord}_\pi(b)$.

Given $(a,b,c) \in k^3$, let $r = \min(\operatorname{ord}_\pi(a), \operatorname{ord}_\pi(b), \operatorname{ord}_\pi($

↳ (valuation of π)

Let $\lambda := \pi^{-r}$, Then $(\lambda a, \lambda b, \lambda c) \in O^3$
and one of the coefficient has $\operatorname{ord}_\pi = 0$ $:\Rightarrow \notin (\pi)$.

So mod (π)
$(\overline{\lambda a}, \overline{\lambda b}, \overline{\lambda c}) \neq (\bar{0}, \bar{0}, \bar{0})$

Def:
$$\mathbb{P}^2(k) \longrightarrow \mathbb{P}^2(k)$$
$$(a:b:c) \longmapsto (\overline{\lambda a} : \overline{\lambda b} : \overline{\lambda c})$$

Ex.

1) Show that reduction map is well-def

2) Show that it does not depend on the choice of π,
a generator for $M = (\pi)$: (Maximal ideal)

- Let $F(x,y,z) \in k[x,y,z]$ homo of deg d

We can clear denominators and $\lambda \in k^*$, s.t. $\lambda F \in \mathcal{O}[x,y,z]$.

with $\mathcal{O}$ a PID, and $M=(\pi)$ is maximal, we can find $\lambda \in k^*$ with

$$(*) \begin{cases} \lambda F \in \mathcal{O}[x,y,z] \\ \overline{\lambda F} = \lambda F \bmod M \\ \qquad \neq 0 \text{ in } (\mathcal{O}/M)[x,y,z] \end{cases}$$

Then define

$$\begin{tikzcd}
\mathbb{P}^2(k) \arrow[r, "red"] & \mathbb{P}^2(k) \\
X_F(k) = X_{\lambda F}(k) \arrow[u, phantom, "\cup"] \arrow[r] & X_{\overline{\lambda F}}(k) \\
(a:b:c) \arrow[u, phantom, "\in"] \arrow[r, mapsto] & red(a:b:c)
\end{tikzcd}$$

Ex. Check that this does not depend on the choice of $\lambda \in k^*$ with $(*)$.

* Back to $F(x,y,z) \in \mathbb{Q}[x,y,z]$

we want to study $X_F(\mathbb{Q})$

For each p, $red: X_F(\mathbb{Q}) \longrightarrow \underbrace{X_{\overline{\lambda_p F}}(\mathbb{Z}/p\mathbb{Z})}$

(the target is easier to study).

* $X_{\overline{\lambda_p F}}(\mathbb{Z}/p\mathbb{Z}) \subseteq \underbrace{\mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})}_{\text{has } p^2+p+1 \text{ points.}}$

Ex. $\mathbb{P}^n(k) = (\mathbb{A}^n(k)) \sqcup (\mathbb{A}^{n-1}(k)) \sqcup \quad \sqcup (\mathbb{A}^1(k)) \sqcup (\cdot pt)$

$$|\mathbb{P}^n(k)| = |k|^n + |k|^{n-1} + \dots + |k| + 1.$$

E.g. To study $X_F(\mathbb{Q})$, we want to study the finite sets $\{X_{\bar{\lambda}_p F}(\mathbb{Z}/p\mathbb{Z}),\ p \text{ prime}\}$.

E.g. $X_{\bar{\lambda}_p F}(\mathbb{Z}/p\mathbb{Z})$ might be empty for some p.

Take $x^{p-1} + y^{p-1} + z^{p-1} =: F$

$$\downarrow \quad (x^{p-1} = 0 \text{ or } 1).$$

$$x^{p-1} + y^{p-1} + z^{p-1} = \begin{cases} 0, 1, 2, 3. \end{cases}$$

Since $a^{p-1} \begin{cases} 0 \\ 1 \end{cases} \quad \forall a \in \mathbb{Z}/p\mathbb{Z}$.

(local info at p

we find that $x^{p-1} + y^{p-1} + z^{p-1}$ is not zero when $p > 3$ for any $(a:b:c) \in \mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})$.

Big Thm in (Arithmetic geometry).

Package together information obtained for each p into a "nice function", usually of the form.

$$L(X_F/\mathbb{Q}, s) = \prod_{\text{prime } p} \left(\begin{array}{l} \text{some expression obtained} \\ \text{from invariance of the} \\ \text{reduction } X_{\bar{\lambda}_p F}(\mathbb{Z}/p\mathbb{Z}) \end{array} \right).$$

Then try to evaluate S. $L(s)$ at some special value of s, or compute some residues of $L(S)$ at some other, and try to express "special values" in terms of objects

* we will get back to this when we discuss the Birch and Swinnerton – Dyer conjecture, this worth 1 million \$)

Last topic : Simple fields, in this case: finite field. $\mathbb{F}_q$ or $\mathbb{Q}_p$ local field)

Recall: for each prime p, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ a finite field.

Ex: (a) Every finite field F is a finite extension of $\mathbb{Z}/p\mathbb{Z}$ for some p

in particular, $|F| = p^m$, for some m, and

$m = [F : \mathbb{Z}/p\mathbb{Z}]$

(b) Fix an alg. closure $\overline{\mathbb{Z}/p\mathbb{Z}}$ of $\mathbb{Z}/p\mathbb{Z}$

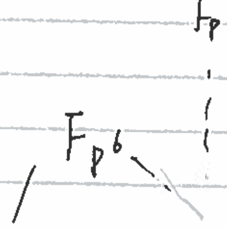
$\overline{\mathbb{F}_p}$ $\mathbb{F}_p$

Given p and $m \geq 1$, there exists (up to isomorphism) a unique field $\mathbb{F}_q$, $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \overline{\mathbb{F}_p}$

with $q = p^m$.

* Obvious, there is an algorith to de whether $Z_p(\mathbb{F}_q) \neq \emptyset$ test ~~ing~~ ~~all~~ the elements of $(\mathbb{F}_q)^n$ ($\underline{n}$ = # variables of f)

we have



Def. $a_m = |Z_f(\mathbb{F}_{p^m})| < \infty$

$$\leq (p^m)^n.$$

$*$ Consider the following power series, called the Zeta fcn associated to $f(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$.

$$Z(f, T) := \exp\left(\sum_{m=1}^{\infty} a_m \frac{T^m}{m} \right)$$

Ex. compute it for $\mathbb{A}^1/_{\mathbb{F}_p}$ $(f(x,y) = y)$. $k[x,y]/_{(y)} \cong k[x]$

$\operatorname{Spec} k[x] \cong \mathbb{A}^1$ [illegible]

28 Aug/2

Fix $\mathbb{F}_q$, $q = p^r$ for some $r \geq 1$

+ F homogenous in $\mathbb{F}_q[x_1, \dots, x_n]$.

?
$$a_n := \begin{cases} |Z_f(\mathbb{F}_{q^n})| \\ |X_F(\mathbb{F}_{q^n})| \end{cases}$$

* Zeta function:

$$\left.\begin{array}{l} Z(X_F/\mathbb{F}_q, T) \\ Z(Z_f/\mathbb{F}_q, T) \end{array}\right\} := \underbrace{\exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)}$$

a power series need to check that this composition of power series can be done (Dino - IAG).

⚠ $\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$

Ex. $\mathbb{P}^1(k) = \mathbb{A}^1(k) \cup \{1\,pt\}$.

$a_n := |\mathbb{P}^1(\mathbb{F}_{q^n})| = q^n + 1$

$$\sum_{n=1}^{\infty} a_n \frac{T^n}{n} = \sum_{n=1}^{\infty} q^n \frac{T^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n} = \log\left(\frac{1}{1-qT}\right) + \log\left(\frac{1}{1-T}\right).$$

$$\boxed{\begin{array}{l} \frac{1}{1-T} = 1 + T + T^2 + \dots \\ \\ \int \frac{1}{1-T}\, dT = T + \frac{T^2}{2} + \frac{T^3}{3} + \dots \\ \quad \parallel \\ -\log(1-T) = \log\left(\frac{1}{1-T}\right) \end{array}}$$

So, $Z(\mathbb{P}^1/\mathbb{F}_q, T) = \exp(\quad + \quad)$

and $Z(\mathbb{A}^1/\mathbb{F}_q, T) = \frac{1}{1-qT}$.

* The "prototype" for $Z(X/\mathbb{F}_q, T)$ is the Riemann. ζ-fcn.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

$$= \prod_{p \text{ primes}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right)$$

$$= \prod_{p \text{ prime}} \left(\frac{1}{1-p^{-s}} \right)$$

$\zeta(s)$: Zeta-function for the ring $A = \mathbb{Z}$.

* Given any ring A s.t. $\forall M \in Max(A)$.
s.t. $|A/M| < \infty$

Define $\zeta_A(s) = \prod_{M \in Max(A)} \frac{1}{1-|A/M|^{-s}}$.

(number field has finite Residue field)

$A = \mathcal{O}_K$. $K/\mathbb{Q}$ number field.

$\zeta_A(s)$ = Dedekind ζ-function of $K/\mathbb{Q}$

* For $A = \mathbb{F}_q[t]$.

$\forall M \in Max(A)$: $|A/M| = q^{\deg(M)}$ (

$$\zeta_A(s) = \prod \frac{1}{1-|A/\;|^{-s}}$$

$T := q^{-s}$, so $|A/M|^{-s} = T^{\deg(M)}$

and $$Z(\overset{A}{\overset{\shortparallel}{\mathbb{F}_q[t]}}, T) = \prod_{M \in Max(\mathbb{F}_q[t])} \frac{1}{1-T^{\deg(M)}}$$

$$\overset{?}{=} \frac{1}{1-qT}$$ (Zeta function of affine line).

Note: $\forall \alpha \in \overline{\mathbb{F}_q}$

$$\begin{tikzcd} ev_\alpha : \mathbb{F}_q[t] \arrow[r, "\text{(evaluation)}"] & \overline{\mathbb{F}_q} \\ t \arrow[r, mapsto] & \alpha . \end{tikzcd}$$

$\ker(ev_\alpha) =$ maximal ideal.

* Given $M \in Max(A)$ $M = (f(t))$, $f(t)$ de.

We get d maps:

$$\begin{tikzcd} ev_{\alpha_i} : \mathbb{F}_q[t] \arrow[r] & \overline{\mathbb{F}_q} \\ t \arrow[r, mapsto] & \alpha_i = \text{root of } f(t) \text{ in } \overline{\mathbb{F}_q} . \end{tikzcd}$$

$$\boxed{|\mathbb{F}_{q^n}| = \sum_{d|n} d \cdot \underbrace{(\#\text{ of irreducible monic poly of deg } d \text{ in } \mathbb{F}_q[t])}_{\substack{\#\text{ of maximal ideal of deg } d. \\ M \in Max(A)}}}$$

☆

We want

$$\prod_{M\in Max(A)} \frac{1}{1-T^{\deg M}} \overset{?}{=} \frac{1}{1-qT}.$$

$$\Leftrightarrow \sum_{M\in Max(A)} \log \frac{1}{1-T^{\deg M}} = \log\frac{1}{1-qT}$$

$$\Leftrightarrow \sum_{M\in Max(A)} \left(T^{\deg M} + \frac{T^{2\deg M}}{2} + \dots\right) = qT + q^2\frac{T^2}{2}+\cdots$$

$$\Leftrightarrow \text{LHS.} = \underset{\uparrow}{*}T + *T^2+\cdots$$

$$\underbrace{\# M \text{ with } \deg M = 1.}_{q}$$

$$\underbrace{2\cdot(\# \text{ of } M \text{ with } \deg M=2) + \# M \text{ with } \deg M=1)}_{q^2}.$$

By ☆, we know

(Rieman - Zeta function in IAG).

Def: · Zeta function for any scheme. $\boxed{\text{k-alg of finite type.}}$

Without tools:

$Z_f(k)$.

with tools:

Let $A := k[x,y]/(f)$.

$Z = (\operatorname{spec} A, A)$

$Z(k) := \mathrm{Hom}_k(A, k).$

We have

$$Z_f(k) \xrightarrow{\sim 5} Z(k).$$

$$(a,b) \longmapsto ev_{(a,b)} \qquad \begin{aligned} A &\longrightarrow k \\ x &\longmapsto a \\ y &\longmapsto b. \end{aligned}$$

Closed pts of ~~X~~ Spec(A): maximal ideal in A
$= \mathrm{Max}(A)$.

* Let X be a scheme with a morphism

$$X \longrightarrow \mathrm{Spec}(A)$$

This morphism is called of finite type, if X can be coverd by finite many open subsets, with
$U_i \simeq \mathrm{Spec}(A_i)$, A_i k-alge of finite type)

Def. * When $k = \mathbb{F}_q$ and $X \longrightarrow \mathrm{Spec}\,\mathbb{F}_q$ is of finite type.

define $Z(X/\mathbb{F}_q, T) \overset{\text{def.}}{=} \prod_{\substack{p \text{ Closed pt} \\ \text{of } X}} \left| \dfrac{1}{1 - T^{\deg(p)}} \right|$

(becuse $X/\mathbb{F}_q$ are finite type)

where $\deg(p) \overset{\text{def}}{=} \cancel{\mathcal{O}_{X,p}/M_{X,p}}\ \deg_{\mathbb{F}_q}(\mathcal{O}_{X,p}/M_{X,p}) < \infty$

$U = \mathrm{Spec}(A)$.

and $\mathcal{O}_{X,p}/M_{X,p} = A/(\text{that max ideal})$.

Note: $Z(X/\mathbb{F}_q, T)$ is a "local" object: a product of term for each closed pt of X.

* If X is a pt: for example $X = \mathrm{Spec}(\mathbb{F}_{q^n})$

then

$$\begin{tikzcd} Z(\mathrm{Spec}(\mathbb{F}_{q^n}, T) \arrow[d, leftrightarrow] & \overset{def}{=} & \frac{1}{1-T^n} \arrow[d] \\ Z(\mathrm{Spec}\,\mathbb{F}_{q^n} \to \mathrm{Spec}\,\mathbb{F}_q, T) \arrow[ru] & & \text{deg is } n. \end{tikzcd}$$

* If $X = X_1 \sqcup X_2 \Rightarrow Z(X,T) = Z(X_1,T)\cdot Z(X_2,T)$.

Rk. (In general) A curve over k is a scheme of finite type. $X \longrightarrow \mathrm{Spec}\,k$, such that if $X = \bigcup X_i$, X_i irreducible component of X, then $\dim X_i = 1$ $\forall i$,

Rk. Let $a_n := |X(\mathbb{F}_{q^n})|$

then $Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)$

* Given $f(x,y) \in k[x,y]$, of degree d, get homogenous F of

(with strong topology)

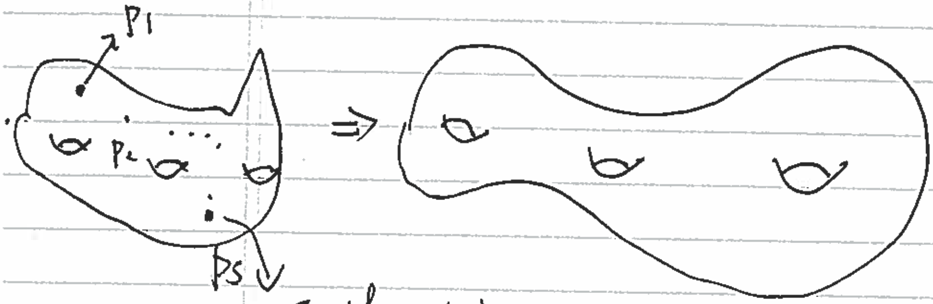
Let $k = \mathbb{C}$, and assume $X_F(\mathbb{C})$ non-singular everywhere.

$*$ Picture for $Z_f(\mathbb{C}) \subseteq X_F(\mathbb{C})$ ← 1 dimesional complex variet

⇒ 2 dimension real variety and it is compact (Closed $\mathbb{P}^2(\mathbb{C})$)

(objec

(manifol



"multiple doughnut"

s points missing.

g = genus = # of "handles".

Key fact: ① The genus can be defined for any smooth projective geometrically integral curve over any field of k.

Def: $$g := \underbrace{\dim_k H^1(X, \mathcal{O}_X)}_{\text{finite dimension for ``nice curve''}} \geq 0$$

Rk. For "nice curve", $H^0(X, \mathcal{O}_X) \cong k$.

Note: $H^i(X, \mathcal{O}_X)$ can be defined completely algebraically.

(PS). 28th Aug 18.

Ex. Suppose $|X_F(\mathbb{F}_{q^n})| = q^n+1$ $\forall n$, $X_F(\overline{\mathbb{F}_q})$ is everywhere nonsingular $\overset{?}{\Rightarrow}$ $\mathbb{F}_q(X_F) \cong \mathbb{F}_q(t)$.

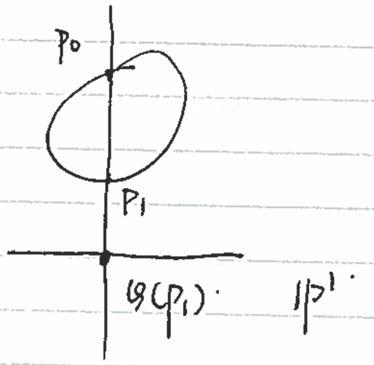
$\hookrightarrow$ function field.

$\Rightarrow$ Curve $X_F/\mathbb{F}_q$ is isomor over $\mathbb{F}_q$ to $\mathbb{P}^1/\mathbb{F}_q$.

$\mathbb{P}^1/k$: $x+y+z=0$ in $\mathbb{P}^2$

But quadratic $=0$ might have no k-pts, Get a "point" after a quartic ext $x^2+y^2+z^2=0$ no pts in $\mathbb{R}$

$$\begin{tikzcd} X \arrow[r] & \mathbb{P}^1 \\ p \arrow[r, mapsto] & \varphi(p) \end{tikzcd}$$



* Given X/k of genus $g \geq 1$, and a pt in $X(k)$.
$\exists$ a variety with group structure, and a map.

$$\begin{tikzcd} X \arrow[r] & A \\ p \arrow[r, mapsto] & O_A \end{tikzcd}$$

that is universal with respect to maps from X to varieties with group structure.

Given X

$$\begin{tikzcd} X \arrow[dr] & \\ p \arrow[dr] & B \\ & O_B \end{tikzcd}$$

Same Zeta function $\Rightarrow$

$\exists \alpha : \mathrm{Jac}(X) \longrightarrow \mathrm{Jac}(X')$, defined over $\mathbb{F}_q$

surjective with finite kernel.

(when $g=1$: $X=A$).

$H^0(np_0) = \{ f \in \mathbb{F}_q(X_F) \mid f$ has at most a pole of

of order n at p_0 and nowhere else$\}$

$$\dim_{\mathbb{F}_q} H^0(np_0) = \underset{\uparrow}{n} \deg(p_0) + 1 - g \, .$$

$\hookrightarrow$ (Riemann-Roch).

n large enough

Thu 30th Aug 18

key facts: Let k be any field, and let X/k be a smooth projective geometrically integral curve, the genus of X/k can be defined as.
as $g := \dim_k(H^1(X, \mathcal{O}_X))$

* If $F \in k[x,y,z]$ is $\overset{\text{homogeous}}{\text{irreducible}}$ in $\bar{F}[x,y,z]$, and $X_F(\bar{k})$ is everywhere nonsingular, then the genus of the smooth projective geometrically integral curve associated to F as $g := \dfrac{(d-1)(d-2)}{2}$
where $d = \deg(F)$, when k is perfect.

Eg. Lines and conic have genus 0, $d=1$ or $d=2$
If $d=3$, $g=1$
$d=4$, $g=3$
Caution: no smooth curve has genus two)
(However: $y^2 = \underbrace{x^5 + a_4 x^4 + \dots + a_0}_{=g(x)}$ defines an abstract curve of genus 2 when $g(x)$ has distinct root and $\mathrm{char}(k) \neq 2$)

Back to $\mathbb{F}_p$ — NB: $k = \mathbb{F}_p$
The conjecture include: → (SPGI).
Let $X/\mathbb{F}_q$ be a "nice" curve of genus g, Let
Weil Conj (~1940 for Curves by Weil
$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right)$
$|a_n| = |X(\mathbb{F}_{q^n})|$.

~1970 for all varieties by Deligne).

(i) $Z(X/\mathbb{F}_q, T)$ is a rational function. More precisely, there exists $h(T) = 1 + \dots + q^g T^{2g} \in \mathbb{Z}[T]$.
s.t. $Z(X/\mathbb{F}_q, T) = \dfrac{h(T)}{(1-qT)(1-T)}$

* factor $\underbrace{1 + \dots + q^g T^{2g}}_{h(T)} = \prod_{i=1}^{2g} (1 - \alpha_i T)$ for some $\alpha_i \in \mathbb{C}$.

1 hdat $\sum \; n \; T^n \quad \sum^{2g} \log(1-\alpha_i T) - \log(1-q \dots) \dots (1-T)$.

$$\Rightarrow a_n = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n$$

Suppose given $a_1, \dots, a_{2g}$. So the power sums

$\sum_{i=1}^{2g} \alpha_i^n$ are determined by $i=1,\dots,2g$

These power sums determine the ele sym fcns in $\alpha_1, \dots, \alpha_{2g}$,

So, we have determined $\ell(X) = \prod_{i=1}^{2g} (x - \alpha_i)$

But, $\ell(x) = X^{2g} \prod_{i=1}^{2g} (1 - \alpha_i \frac{1}{x})$

chang $\frac{1}{x} = T$ $\quad \ell(\frac{1}{T}) T^{2g} = h(T)$,

we have determined the Zeta func $Z(X/\mathbb{F}_q, T)$.

Next Que: the $a_n \leq q^{2n} + q^n + 1$

if $X_F(\mathbb{F}_{q^n}) \subseteq \mathbb{P}^2(\mathbb{F}_{q^n})$ not all curve can be embeded in projective plane.

$$|a_n|_{\mathbb{C}} = |q^n + 1 - \sum \alpha_i^n|_{\mathbb{C}}$$
$$\leq q^n + 1 + \sum |\alpha_i|_{\mathbb{C}}^n$$

Rk. $\ell(x) \in \mathbb{Z}[x]$ because $h(T) \in \mathbb{Z}[T]$.

So, $\alpha_1, \dots, \alpha_{2g}$ are algebraic integers (roots of $\ell(x)$).

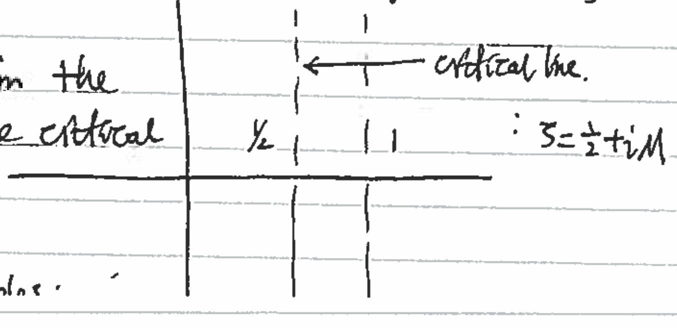
Zeta fun & Riemann Zeta fcn.

Note: $\frac{1}{\alpha_1}, \dots, \frac{1}{\alpha_{2g}}$ are the Zeros of $Z(X/\mathbb{F}_q, T)$.

Thm (Weil for curves (if $\neq 0$). Hass for elliptic curve $n/f \geq 0$)

(Analogue of Rieman hypothesis) $|\alpha_i|_{\mathbb{C}} = \sqrt{q}$ $\quad \forall i=1, \dots 2g$.

Riemann hypothesis. $\zeta(s)$ The Zero of $\zeta(s)$ in the critical strip are on the critical line.



* Recall change of variables:

If our Zero "are on the critical line".

$$\frac{1}{\alpha_i} = q^{-(\frac{1}{2}+i\mu)}$$

$$\left|\frac{1}{\alpha_i}\right| = q^{-1/2}\cdot \underset{\overset{\shortparallel}{1}}{\underline{|q^{i\mu}|_{\mathbb{C}}}}$$

$$\Rightarrow |\alpha_i|_{\mathbb{C}} = q^{1/2}$$

Consequence. From $a_n = q^n+1-\sum_{i=1}^{2g}\alpha_i^n$.

we get.

$$a_n \le q^n+1+2g(\sqrt{q})^n.$$

$$q^n+1-2g(\sqrt{q})^n \le a_n.$$

In particular, $q+1-2g\sqrt{q} \le a_1 \le q+1+2g\sqrt{q}$.

If g is small to q, then $q+1-2g\sqrt{q}>0$

$\Rightarrow a_1>0 \Rightarrow X(\mathbb{F}_q)>0$.

E.g. * $g=0$, $a_n = q^n+1$, $\forall n$.

$$Z(X/\mathbb{F}_q, T) = \frac{1}{(1-qT)(1-T)}$$

* $g=1$, $q+1-2\sqrt{q} = (\sqrt{q}-1)^2>0$.

So $X(\mathbb{F}_q)\neq\emptyset$.

$$Z(X/\mathbb{F}_q, T) = \frac{1+\beta T+qT^2}{(1-qT)(1-T)}$$

E.X. Write down β in terms of a_1.

* Important thing with arithmetic.

Let $f(x_1,\dots,x_n)\in k[x_1,\dots,x_n]$. f is called

E.g. $x^2+1 \in \mathbb{Q}[x,y]$. $x^2+1 = (x-i)(x+i) \in$

$X_f(\mathbb{Q}) = \phi$ $X_f(\mathbb{R}) = \phi$

$X_f(\mathbb{C})$ union of 2 disjoint lines.

※ ring of functions, $A = \mathbb{Q}[x,y]/(x^2+1)$ is integral domain.

$\underline{ff(A)}$ = function field over $\mathbb{Q}$.

$\mathbb{C}[x,y]/x^2+1 \cong \mathbb{C}(n) \times \mathbb{C}[v]$.

Rk. we have $\mathbb{Q} \subseteq A$. But in A, we have also "class of x", which is not in $\mathbb{Q}$, but algebraic over $\mathbb{Q}$, $(\text{class of } x)^2 = -1$.

Ex. $K := \mathbb{F}_p(u,v)$

$f(x,y) := 1 + ux^p + vy^p \in k[x,y]$.

(Every element can take pth root)

$f(x,y) = (1 + \sqrt[p]{u}\,x + \sqrt[p]{v}\,y)^p$ in $K(\sqrt[p]{u}, \sqrt[p]{v})[x,y]$

* $f \in k[x,y]$ is irreducible, $f \in \bar{k}[x,y]$ is reducible.

$$\begin{tikzcd}
 & K(\sqrt[p]{u}, \sqrt[p]{v}) \arrow[dl, dash, "p"] \arrow[dr, dash, "p"'] & \\
K(\sqrt[p]{u}) = k(\sqrt[p]{u}, v) \arrow[dr, dash, "p"] & & k(u, \sqrt[p]{v}) = k(\sqrt[p]{v}) \arrow[dl, dash, "p"'] \\
 & k = \mathbb{F}_p(u,v) &
\end{tikzcd}$$

$A = k[x,y]/(f)$

$\underline{A'} := k(\sqrt[p]{u})[x,y]/(f)$

Def. Let F/k be a field extension, Then k is alg closed in F, if $\forall g \in F \backslash k$, g is not alg over k.

(function field).

* Let k be perfect, Let $f(x,y) \in k[x,y]$ irreducible,
Let $F := \mathrm{ff}(k[x,y]/(f))$.
Then f is geometrically irreducible $\Leftrightarrow$ k is alg closed in F.

4th Sept 2018

Ex.* Let $F(x,y) \in k[x,y]$ homogeneous of degree $d \geq 2$, then F is not geometrically irreducible.

Thm: (-a misstated thm before) Let $F \in k[x,y,z]$ be homogeneous of deg 2, and irreducible, Suppose that $X_F(k) \neq \phi$, Then (i) either $X_F(k) = \{P_0\}$ with P_0 singular and F not geometrically irreducible (ii) or $X_F(\bar{k})$ is everywhere nonsingular, F is geometrically irreducible, and the function field $k(X_F)$ is k isomorphic to $k(t)$ (We say that the curve defined by F is parametrizable)

Ex. $x^2+y^2 \in \mathbb{R}[x,y]$

$Z_f(\mathbb{R}) = \{(0,0)\}$

pf: Let $P_0 \in X_F(k)$.

using a translation, assuming that $P_0 := (0:0:1)$.

dehomogenize ~~to~~ F to get $f(x,y) = a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}$, $\in k[x,y]$.

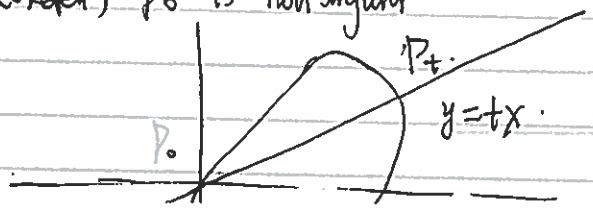
Then, P_0 is non-singular

$\Leftrightarrow a_{10}x + a_{01}y \neq 0$.

(Case 1)(sketch). (By Ex*) f is not geometrically irreducible.

$\Rightarrow (0,0)$ is the only k rational pt (since f is irreducible.

(Case 2) (sketch) P_0 is non singular.



$$f(x, tx) = x(a_{10} + a_{01}t + x(a_{20} + a_{11}t + a_{02}t^2))$$

$P_t = (x(t), y(t))$ with

$$x(t) = \frac{-(a_{10} + a_{01}t)}{a_{20} + a_{11}t + a_{02}t^2}.$$

$$y(t) = t(x(t))$$

* $x(t)$ not constant

cannot have $a_{01} = a_{11} = a_{02} = 0$

otherwise, $f(x,y) = a_{10}x + a_{20}x^2$ not irreducible.

* We get a k-homomorphism

$$\begin{tikzcd} \text{(function field)} & k(X_F) \arrow[l] \arrow[r] & k(t) \arrow[r] & \text{(simplest function field)} \\ & \text{class of } x \arrow[r, mapsto] & x(t) & \\ & \text{class of } y \arrow[r, mapsto] & y(t) & \end{tikzcd}$$

* If not constant, it is injective.

* It's surjective, since $\frac{y}{x} \to t$.

Next? Plane curve of degree 3?

Ex. Let $F \in k[x,y,z]$ be geometrically irreducible of degree 3

ⓐ. Then $X_F(\bar{k})$ has at most one singular point.

ⓑ. Assume that $(0:0:1) \in X_F(k)$ is singular, then

$\exists$ a k-isomorphism $k(X_F) \longrightarrow k(t)$.

D.b

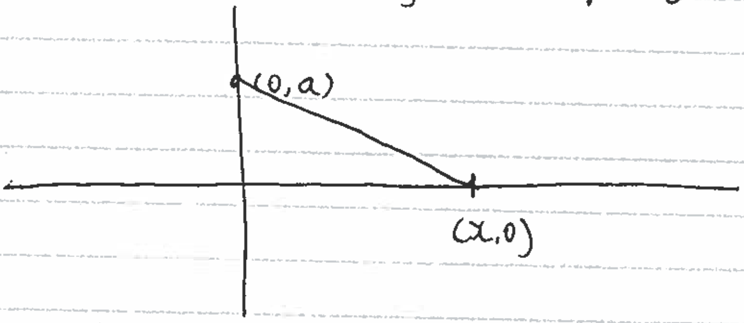
* Other possibility:
Curves in $\mathbb{A}^3$ defined by 2 equations of degree 2?

E.g. where such a curve occurs in nature.
A rational distance set in $\mathbb{R}^2$ is a set of pts

S ~~n~~ s.t.
$\forall\, s,t \in S,\ \text{dist}(s,t) \in \mathbb{Q}$

E.g. $S = \mathbb{Q} \subseteq \{(x,0) \in \mathbb{R}^2\}$
$\text{dist}(s,t) = |t-s| \in \mathbb{Q}$ if both $s,t \in \mathbb{Q}$

E.g.

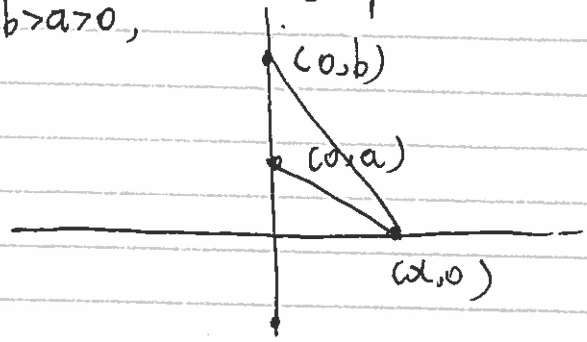


dist is $\sqrt{x^2+a^2}$.

Consider the set $S = \left\{ (x,0) \mid x^2+a^2=y^2,\ x,y \in \mathbb{Q} \right\}$

$\cup \{(0,a), (0,-a)\}\quad a \in \mathbb{Q}$

E.g. (G. Huff, UGA, early 1950's)
Let $b>a>0$,



Can find an infinite rational distance set with 3 or more pts outside a line?

* Need the system $\begin{cases} x^2+a^2=y^2 \\ x^2+b^2=z^2 \end{cases}$

to have ∞-many solutions $(x,y,z) \in \mathbb{Q}^3$.

Def (rational curve :$\Leftrightarrow$ its function field $\simeq k[t]$).

Que.* $X_{a,b}(\mathbb{Q}) = \left\{ (\alpha,\beta,\gamma) \in \mathbb{Q}^3 \;\middle|\; \begin{matrix} \alpha^2+a^2=\beta^2 \\ \alpha^2+b^2=\gamma^2 \end{matrix} \right\}$

Can you find $a,b \in \mathbb{Q}$, s.t $|X_{a,b}(\mathbb{Q})|$ is ~~∞~~ ∞?

R.k $X_{a,b}(\mathbb{Q}) \supseteq \{(0,\pm a,\pm b) \in \mathbb{Q}^3\}$

If homogenize, $\left[\begin{matrix} x^2+a^2t^2=y^2 \\ x^2+b^2t^2=z^2 \end{matrix} \right.$,

get $(1:\pm1:\pm1:0) \in \mathbb{P}^3(\mathbb{Q})$.

* Consider the curve $Y_{a,b}$ given by

$V^2=(x^2+a)(x^2+b)$

with the map $\varphi: X_{ab}(\overline{\mathbb{Q}}) \longrightarrow Y_{a,b}(\overline{\mathbb{Q}})$ deg 2 isogeny

$(x,y,z) \longmapsto (x,yz)$.

$\boxed{\text{Ex.}}$ We get a k-homomorphis of function field

$\varphi^*: k(Y_{ab}) \longrightarrow k(X_{ab})$

Ex. a) The degree of $k(X_{a,b})$ to $\varphi^* k(Y_{a,b})$ is 2.

b) $P \in Y_{a,b}(\overline{\mathbb{Q}})$, $|\varphi^{-1}(P)| = 2$.

(In general, we not expect to have ~~$\#$~~ $|\varphi^{-1}(P)| = 2$ always).

Fact*: At least ~~..~~ a ~~field~~ finite extension of k,

a $\overset{\text{curve}}{\vee}$ given by $y^2 = g(x)$ with $\deg(g) = 4$, "can be given" by an equation $Y^2 = h(X)$ with $\deg h = 3$

Idea: Let $g(x) \in k[x]$, and let L/k, be such that $\exists \alpha \in L$, with ~~$g(\alpha)$~~ $g(\alpha) = 0$.
Then we can translate in $L[x]$ and get an equation
$y^2 = x(a_3 x^3 + a_2 x^2 + a_1 x + a_0)$ $a_i \in L$

$*$ Divide by x^4

$$\left(\frac{y}{x^2}\right)^2 = a_3 + a_2 \frac{1}{x} + a_1 \frac{1}{x^2} + a_0 \frac{1}{x^3}$$

Set $\overline{Y} = \frac{y}{x^2}$, $\overline{X} = \frac{1}{x}$.
$\Rightarrow$ $\overline{Y}^2 = a_0 \overline{X}^3 + a_1 \overline{X}^2 + a_2 \overline{X} + a_3$ deg 3 in $L[x]$.

In Fact* "can be given" means that the two curves have isomorphic function field.

$*$ The change of variables give.
(a) a $\underset{L}{\boxed{k}}$-isomorphism between the function field of $y^2 = g(x)$ to the function field associated to $\overline{Y}^2 = h(\overline{X})$

Rk: If the curve $y^2 = g(x)$, $g(x) \in k[x]$ of deg 4 and w/o multiple root and char(k) $\neq 2$. (no singular pt) $\rightarrow$ char(k)$\neq 2$.

(i.e. $Z_{y^2-g(x)}(\bar{k})$ everywhere non-singular)

and $Z_{y^2-g(x)}(k) \neq \phi$, then there is a change of variable to an equation of the form:
$v^2 = h(u)$., w, deg $h = 3$.

* Def. (official scheme based def of Elliptic curve)

An elliptic curve over k is a smooth proper geometrically Integral curve $E|k$ of genus 1, along with a fixed pt $p_0 \in E(k)$.

Thm. Every such pair $(E/k, p_0)$ is k-isomorphic to a smooth plane projective curve given by an affine equation

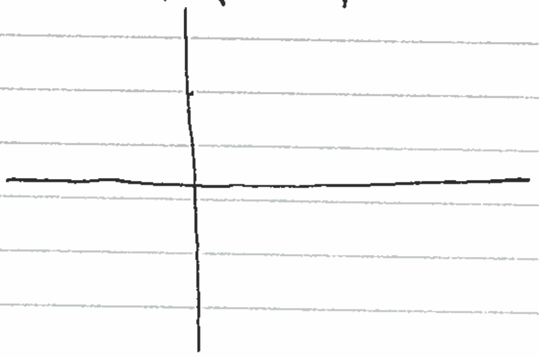
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
$a_i \in k$.

The point $p_0 \Leftrightarrow [0:1:0]$.

6th/sept/18 Thr

Recall: Work of Huff (1948)

Student Peeples (1954)



$$\begin{cases} x^2+a^2=y^2 \\ x^2+b^2=z^2 \end{cases}$$

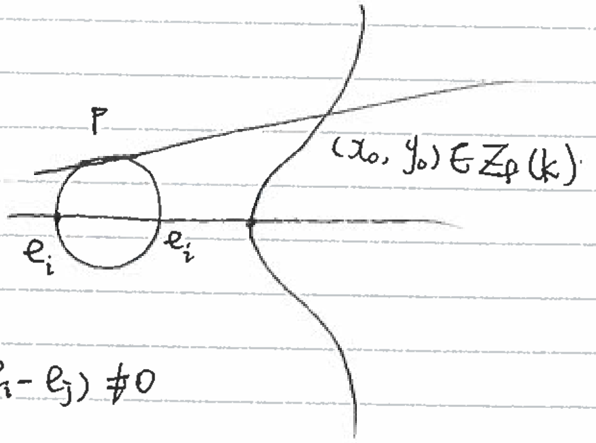
$a \neq b$, fixed

define an elliptic curve (curve of genus 1 with a $\mathbb{Q}$-rational pt).

Huff Que: find a, b, s.t. there are ∞ $\mathbb{Q}$-rational pts.

Thm. (Huff Sensene for $\mathbb{Q}$ in 1941) 1948

Suppose we have a curve given by



$y^2 = (x+e_1)(x+e_2)(x+e_3)$

$e_i \in k$, number field $\quad \prod_{i \neq j} (e_i - e_j) \neq 0$

Let $(x_0, y_0) \in Z_f(k) \rightarrow P_*$.

There exists $(x_1, y_1) \in Z_f(\underline{k})$ s.t. $T_p \cap Z_f(k) \ni (x_0, y_0)$

$\Longleftrightarrow$ x_0+e_1, x_0+e_2, x_0+e_3 are all square in k.

Thm. Let k be any field. Let X/k be a smooth projective geometrically integral curve of genus 1 with $X(k) \neq \phi$; then X/K is isomorphic over k to a plane curve given by a Weierstrass equation. $y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^6$.

$a_i \in k$

Note: this projective plane curve alway has a point $(0:1:0)$.

* (Further simplification)

If $\mathrm{Char}(k) \neq 2$, can cancel the square.

(dehomogenize). $\div 2$.

$$\underbrace{y^2+(a_1x+a_3)y+\frac{1}{4}(a_1x+a_3)^2}_{\longrightarrow\ \bar{Y}^2}$$

$$= x^3+\frac{1}{4}b_2x^2+\frac{1}{2}b_4x+\frac{1}{4}b_6$$

$$b_2 = a_1^2+4a_2$$
$$b_4 = a_1a_3+2a_4$$
$$b_6 = a_3^2+4a_6$$

Make chang $y = 2\bar{Y}$, and multiply by 4 the old equ.

$$y^2 = 4\bar{Y}^2 = 4x^3+b_2x^2+2b_4x+b_6$$

If $\mathrm{char}(k) \neq 3$. set $x = \bar{X}-\frac{b}{12}$.

$$\bar{X}^3 = (x-\frac{b_2}{12})^3 = x^3-3(\frac{b_2}{12})x^2+\dots$$

$$y^2 = 4(x^3+\frac{b_2}{4}x^2+\dots)$$

$$= 4x^3-\frac{1}{12}c_4x-\frac{1}{216}c$$

$$c_4 = b_2^2-24b_4$$
$$c_6 = -b_2^2+36b_2b_4-216b_6$$

* Multiply by $2^4 3^6$, and set $\bar{Y} = 2^2 3^3 y$ $\quad \bar{X} = 6^2 x$.

This gives $\bar{Y}^2 = \bar{X}^3-27c_4\bar{X}-54c_6$

(Don't want denominator).

represent this curve is non-singular

$\Leftrightarrow$ x^3+Ax+B has disjoint roots in $\bar{K}$.

$\Leftrightarrow$ $\operatorname{dis}(X^3+AX+B) \neq 0$

* $\operatorname{disc}(g(x)) = \operatorname{resultant}(g(x), g'(x))$. *.

In our case,

$\operatorname{disc}(X^3+AX+B)$

$$\boxed{g'(x) = 3x^2+A}$$

$$\left|\begin{array}{ccccc} 1 & 0 & A & B & \\ & 1 & 0 & A & B \\ 3 & 0 & A & & \\ & 3 & 0 & A & \\ & & 3 & 0 & A \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\end{array}}\right\} \deg g' \\ \left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} \deg g \end{array}$$

$= 4A^3+27B^2.$

* Applies to our equation.

$\operatorname{dis}(X^3-27c_4X-54c_6)$

$= 4(-27c_4)^3+27(-54c_6)^2.$

$= -27^3\cdot 4(c_4^6-c_6^2)$ (char(K) $\neq 2,3$) $\Rightarrow$ Coeff $\neq 0$.

$27\cdot 64$

*

Def: (Discrim of the original Weierstrass equation) in the a_i's

$1728\Delta = c_4^3 - c_6^2$

and $\Delta \in \mathbb{Z}[a_i]$

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_0$
with $a_i \in k$, define a everywhere non-singular curve
$\iff \Delta \neq 0$.

* (disc $\neq 0 \iff$ the curve is non singular).

Defn Another way to define genus.
Let X/k be a curve and $P \in X$.
we have 2 objects associated with X & P.

$$\mathcal{O}_{X,P} \subseteq k(X)$$

ring of function in $k(X)$ defined at

function field

Ex. E.g. Given $f(x,y) \in k[x,y]$ geom irreducible.

we get $k(X_f) = ff\left(k[x,y]/(f)\right)$.

$A(X_f) = k[x,y]/(f)$ functions defined

Let $M = \underline{(x,y)} \subset A$.

$P = (0,0)$

Then $\mathcal{O}_{X,P} := A_M$

$$= \left\{ \frac{g}{h} \in A \,\middle|\, h \notin M \right\}$$

$h(x,y) = h(0,0) + \text{higher order}$

i.e. $h(0,0) \neq 0$

key fact. $\cdot P$ is non-singular

$\Leftrightarrow M A_M = (x,y) A_M$ is in fact principal. and A_M is a local PID.

$*$ This allows us to make sense

$$\forall g \in k(X_f): \ g \text{ has } \begin{cases} \text{a zero of order } n \text{ at } p \\ \\ \text{a pole of order } n \text{ at } p. \end{cases}$$

A_M has a valuation: ord_M

g has order $n \Leftrightarrow \text{ord}_M(g) = n \geq 0$

g has pole $n \Leftrightarrow \text{ord}_M(g) = -n. > 0$

Def: Fix $n \geq 1$, and $p \in X$.

$$H^0(X, np) = \left\{ g \in k(X) \;\middle|\; \begin{array}{l} \text{ord}_p(g) \geq -n. \\ \forall p' \neq p \\ \text{ord}_{p'}(g) \geq 0 \end{array} \right\}$$

$\Uparrow$

a vector space $*$.

equality

not a vector space with equation

$\boxed{\text{degree of residue field at } p \Leftrightarrow \text{degree of } p}$

when n is large enough:

$$\dim_k H^0(X, np) = 1 + n\deg(p) - \underset{\text{constant!}}{\overset{\text{(same } g \text{ for } \forall p\text{)}}{g}}$$

↳ (Part of R-R thm)

* (when $g=1$, big enough means $n \geq 1$)

Pick a smooth curve X/k of genus 1, assume $p \in X(k)$
so that $\deg p = 1$, then
$\dim_k H^0(X, np) = n$

$H^0(X, p) = \langle 1 \rangle$ constant fcn.

$\cap|$

$H^0(X, 2p) = \langle 1, x \rangle$ → basis for the k-space.

x must have a pole of order 2 at p.

$\cap|$

$H^0(X, 3p) = \langle 1, x, y \rangle$ → y must have a pole of order 3 at p.

$\cap|$

$H^0(X, 4p) = \langle 1, x, y, x^2 \rangle$ → x^2 has a pole of order 4.

$\cap|$

$H^0(X, 5p) = \langle 1, x, y, x^2, xy \rangle$

$H^0(X, 6p) = \langle 1, x, y, x^2, xy, \substack{y^2 \\ x^3} \rangle$.

↖ poles of order exactly 6.