Resolving Singularity (Blowing-up!)

- The process is called blowing-up because a singular point (x_1, x_2) is being mapped to the point (x_1, yx_1, y) [eg. $(0,0) \mapsto (0,0,1)$]

- The properties we want in this process are:

Property I: $A(\tilde{X})_{\langle x_1, y\rangle}$ is a local domain with unique maximal ideal, now principal.

- Eg. It is: $\langle x_1, y\rangle = \langle y^2, y\rangle = \langle y\rangle$ in $A(\tilde{X})$, while: $\langle x_1, x_2\rangle$ is non-principal in $A(X)$.

- <ins>Defn</ins>: A ring R is called <ins>dvr</ins> (discrete valuation ring) if it is a local domain with the max. ideal <ins>principal</ins>.

- Eg. $\left(k[x_1,y]/\langle y^2-x_1\rangle\right)_{\langle x_1,y\rangle}$ is a dvr.

$\left(k[x_1,x_2]/\langle x_2^2-x_1^3\rangle\right)_{\langle x_1,x_2\rangle}$ is <ins>non</ins>-dvr.

$\mathbb{Z}$ is <ins>not</ins> local, though every max. ideal is principal. ($\Rightarrow \mathbb{Z}$ is non-dvr)

<u>Property II</u>: Consider as before $k \overset{\mathfrak{m} \triangleleft}{\subset} R \subset K$, where $K = k(R)$ & $\mathfrak{m} \triangleleft R$ is the unique max. ideal; $k \cong R/\mathfrak{m}$ is the residue.

(a <u>dvr</u>)

Then, $\exists\, v : K^* \longrightarrow \mathbb{Z}$ that satisfies "metric" like properties.

- <u>Defn</u>: A <u>discrete valuation</u> of K is a map $v : K^* \to \mathbb{Z}$ s.t. $\forall \alpha, \beta \in K^*$, $v(\alpha \cdot \beta) = v(\alpha) + v(\beta)$

$[v(0) := \infty]$ & $v(\alpha + \beta) \geq \min(v(\alpha), v(\beta))$.

- Eg. in the example above $R = (k[x_1, y]/\langle y^2 - x_1 \rangle)_{\langle x_1, y \rangle}$ is a dvr.

Any element $\alpha \in K = k(R)$, can be written as:

$$\alpha =: \frac{a(x_1) + y \cdot b(x_1)}{c(x_1)} \qquad [(a+yb)(a-yb) = a^2 - x_1 b^2]$$

- We define $v : K^* \to \mathbb{Z}$ via the uniformizer y: Express $\alpha =: y^e \cdot \alpha'$, where $\alpha' \in R \setminus m$; $e \in \mathbb{Z}$. Call $v(\alpha) := e$. $\triangleright$ v is a valuation.

- Eg. $v(x_1) = v(y^2) = 2$.

$v(x_2) = v(yx_1) = v(y^3) = 3$.

$v(1+x_1) = 0$ $\quad [\because 1+x_1 \in R \setminus \langle y \rangle]$

$v(1/x_1) = -2$.

Proposition: If R is dvr, then $\exists$ valuation $v : K^* \to \mathbb{Z}$. Further,

- $\{\alpha \in K \mid v(\alpha) \geq 0\} = R$
- $\{\alpha \in K \mid v(\alpha) > 0\} = m$ $[\{\alpha \in K \mid v(\alpha) < 0\} = K \setminus R]$
- $\{\alpha \in K \mid v(\alpha) = 0\} = R^*$ (:= units in R).

Pf:
- dvr $R \Rightarrow m =: \langle u \rangle$, where u is called a uniformizer of R in K.
- Express any $\alpha \in K$, as $\alpha =: u^e \cdot \alpha'$, $\alpha' \in R \setminus m$.
- Define $v(\alpha) := e$. $\square$

D If a field K has a valuation $v: K^* \to \mathbb{Z}$, then $\exists$ local domain R of $\mathrm{trdeg}_k = 1$.

Pf: • v defines R & $\mathfrak{m}$.

• v on $R \setminus \mathfrak{m}$ is >0 $\Rightarrow$ $R \setminus \mathfrak{m}$ has only units.

$\Rightarrow$ R is local.

• Ex: $\Rightarrow$ $\mathfrak{m}$ is principal $\Rightarrow$ $\mathrm{trdeg}_k R = 1$. $\square$

Property III: dvr R is integrally closed in K.

- Defn: R is called i.c. if a monic polynomial $f(x) =: x^n + a_{n-1} x^{n-1} + \dots + a_0 \in R[x]$ with root $\alpha \in K$ $\Rightarrow$ $\alpha \in R$.

- Eg. $\mathbb{Z}$ is <u>i.c.</u> in $\mathbb{Q}$. [Gauss Lemma]
  - Say, $\alpha^2 + 2\alpha + 3 = 0$ & $\alpha \in \mathbb{Q}$; $\alpha =: a/b$, $a, b \in \mathbb{Z}$

    $\Rightarrow a^2 + 2ab + 3b^2 = 0$.

    $\Rightarrow b \mid a \Rightarrow \alpha \in \mathbb{Z}$.

<u>Idea:</u> To resolve singularity at P in X, we should take the <u>integral closure</u> of the germs $\mathcal{O}_{X,P}$ in $K(X)$.

Proposition: For local domain R with fraction-field K of $\mathrm{trdeg}_k K = 1$, TFAE:

(i) R is dvr,

(ii) K has a valuation, with valuation ring R,

(iii) R is integrally closed in K.

Pf: [(ii) $\Rightarrow$ (iii)]: Let $v: K^* \to \mathbb{Z}$ be the valuation.

- Say, $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ with a_i's in R, and $\alpha \in K$.

$\Rightarrow n \cdot v(\alpha) = v(\alpha^n) = v(a_{n-1}\alpha^{n-1} + \dots + a_0) \geq v(a_i \alpha^i)$ $\forall i$.

$\Rightarrow \quad n \cdot v(\alpha) \geq i \cdot v(\alpha) \quad \Rightarrow v(\alpha) \geq 0$

$\Rightarrow \quad \alpha \in R.$

D Let u be a least-value element in $\mathfrak{m} = \{\alpha \in K \mid v(\alpha) > 0\}$. Then, $\mathfrak{m} = \langle u \rangle_R$.

[Pf: let $v(u_1) = v(u_2)$ be the least.

$\Rightarrow \quad v(u_1/u_2) = 0 \quad \Rightarrow \quad u_1/u_2 \in R^*$

$\Rightarrow \quad \langle u_1, u_2 \rangle_R = \langle u_1 \rangle_R = \langle u_2 \rangle_R$. □]

$\Rightarrow$ [(ii) $\Leftrightarrow$ (i)].

[(iii) $\Rightarrow$ (i)]: Consider elements $\alpha, \beta \in \mathfrak{m}$.

Since, $\operatorname{trdeg} K = 1$, we've an annihilator $F(\alpha, \beta) = 0$.

• Let e_1 be the least-degree in $\operatorname{supp}(F)$. Then, F gives (w.l.o.g.):

$$(\alpha/\beta)^{e_1} + f_1(\alpha/\beta) = \beta^{e_2} \cdot f_2(\alpha/\beta, \beta),$$

where f_1, f_2 are polynomials over k; $e_2 > 0$, $\deg f_1 < e_1$.

• This gives a relationship that is monic in α/β:

As, $(\alpha/\beta)^{e_1} \cdot c_0(\alpha,\beta) = \sum_{i<e_1} (\alpha/\beta)^i \cdot c_i(\beta)$

where, $c_0(\alpha,\beta)$ is unit in R & $c_i(\beta) \in K[\beta]$.

$\Rightarrow (\alpha/\beta)$ is a root of $Y^{e_1} - \sum_{i<e_1} Y^i \cdot c_i(\beta)/c_0(\alpha,\beta)$,

which is monic in $R[Y]$.

$\Rightarrow \alpha/\beta \in R$. [$\because R$ is i.c. in K]

$\Rightarrow \langle \alpha,\beta\rangle_R = \langle \beta\rangle_R$ = principal.

$\Rightarrow$ By doing this for $\alpha,\beta \in \mathfrak{m}$, we get $\mathfrak{m}$ principal

$\Rightarrow R$ is dvr. $\square$

— Next, we find all the valuations of
$$K = k(x) = K(\mathbb{A}^1).$$

— Eg. $K = \mathbb{Q}$; $\mathfrak{m} \triangleleft R \subset \mathbb{Q}$; $R = \mathbb{Z}_{(p)}$ is dvr.
residue field $k = R/\mathfrak{m} \cong \mathbb{F}_p$.
valuation $v(a/b) := \max(e : p^e | a) - \max(e : p^e | b)$.

Qn: Are there any other valuations on $\mathbb{Q}$?
↳ No other discrete val.
↳ non-discrete : $a/b \mapsto |a/b| \in \mathbb{R}$.

- **Defn:** For an irreducible $f \in k[x]$, define a subring (of K), $R_f := \{ g/h \in K : f \nmid h \}$.

Theorem: The (distinct) dvr of K are:
R_f, for irreducible $f \in k[x]$; and
$R_{x^{-1}}$, viewing x^{-1} as an irreducible in $k[x^{-1}]$.

- Q. What about $\overset{f:=}{1/(x-1)}$? Suppose this gives a valuation $v(\cdot)$ on $K = k(x)$. Then, $\frac{x}{x-1} = 1 + \frac{1}{x-1}$ is unit in R_f.

$\Rightarrow R_f = R_{x^{-1}} \Rightarrow (x-1)^{-1}$ & x^{-1} give identical valuations.

• Eg. $v_f(x) = v(x-1+1)$; $v(x-1)=-1$ & $v(1)=0$.
$v(x) = -1$ wrt $f=(x-1)^{-1}$ or x^{-1}.
[▷ $f^e \cdot u + f^{e+1} \cdot v = f^e \cdot (u + f \cdot v) \Rightarrow$ $\underline{v(a+b) = \min(v(a), v(b))}$, if $v(a) \neq v(b)$.]

▷ $1/(x-\alpha)$, $\alpha \in k$, give identical valuations.
(i.e. around pt. $\alpha + \infty$)

Pf: • f resp. x^{-1} can be used to define a valuation.
$\Rightarrow$ R_f & $R_{x^{-1}}$ are dvrs. [Exercise]

• [No other valuations]: Let R be a valuation ring in K, with unique max. ideal $\mathfrak{m}$ & valuation $v(\cdot)$.

Case I: $[x \in R]$: $\Rightarrow k[x] \subseteq R$

$\Rightarrow \mathfrak{m} \cap k[x] \neq \{0\}$ [Else, $k[x]^*$ is unit in R

$\Rightarrow k[x]^* \subseteq R \setminus \mathfrak{m} \Rightarrow v = 0 \Rightarrow$ ↯]

$\Rightarrow \mathfrak{m} \cap k[x] \lhd k[x]$ is prime & nonzero.

$\Rightarrow \mathfrak{m} \cap k[x] = \langle f \rangle_{k[x]}$, for irreducible $f(x)$.

$\Rightarrow \mathfrak{m} = \langle f \rangle_R$. $\Rightarrow v = v_f$. done.

Case II: $[x \notin R]$: $\Rightarrow x^{-1} \in R \Rightarrow k[x^{-1}] \subseteq R$

- By the above case, we get $\mathfrak{m} = \langle f(x^{-1}) \rangle_R \subsetneq R$.
- Also, x^{-1} is not a unit in $R \Rightarrow f(x^{-1}) \mid x^{-1}$

$\Rightarrow \mathfrak{m} = \langle x^{-1} \rangle_R \Rightarrow R = R_{x^{-1}}$. $\square$

Extension of valuation rings (to $K(C)$) curve

- Any field K of $\mathrm{trdeg}_k = 1$ can be written a
$$k \subset \underbrace{k(x)}_{\text{pure transcendental}} \underbrace{\subseteq K}_{\text{finite algebraic extn.}}$$

Theorem: Let R be a local domain in K & m_R be its uniq. max. ideal. Then, $\exists$ dvr B in K, with uniq. max. ideal m_B s.t. $\underbrace{R \subseteq B \;\&\; m_R \subseteq m_B}_{B \text{ dominates } R}$.

[Eg. R is dvr in $k(x)$, but non dvr in K.]

Pf: • If R is integrally closed in K, then R is already dvr. done.

• Say, R is not i.c., then consider a local domain B that is an integral closure of R.

[$\mathcal{F} := \{$ local domain R' dominating $R \mid 1 \notin \mathfrak{m}_{R'} \supseteq \mathfrak{m}_R\}$.

Let R^* be a maximal element in $\mathcal{F}$. Note: $R \in \mathcal{F}$.

$\Rightarrow$ R^* is i.c.]

$\Rightarrow$ B is dvr in K, that extends R. $\square$

- Eg. $X = Z(x_2^2 - x_1^3)$; $R = A(X)_{\langle x_1, x_2 \rangle}$.

  R is non dvr in $K(X)$.

  - Since, $y := x_2/x_1 \in K(X)$ is not in R.

- So, we introduce this to get $B = A[y]$, which is dvr in $K(X)$, that extends R.

Qn: How do we repeat this to resolve many singular points?

$\triangleright$ A curve has only finite singular points.
$\rightarrow$ (closed set)

- Consider any $\mathrm{trdeg}_k = 1$ field K. We want to think of it as an <u>abstract curve</u>, via valuations.

- <u>Defn</u>: • Let $\underline{C_K} := \{v \mid \text{valuation } v \text{ on } K \text{ wrt dvr } R_v \text{ \& uniq. max. ideal } m_v\}$.

• <u>Closed sets</u> of C_K be defined as those subsets of C_K that are finite, or C_K itself.

• <u>Open sets</u> of C_K be defined as complement of the closed sets.

• For open $U \subseteq C_K$ define the <u>regular fns. ring</u> as

$$\underline{\mathcal{O}(U)} := \bigcap_{v \in U} R_v .$$

▷ Each $f \in \mathcal{O}(U)$ defines a distinct function
$U \longrightarrow k$; $v \longmapsto (f \bmod \mathfrak{m}_v) \in k \cong R_v/\mathfrak{m}_v$.
$=: f(v)$

▷ Fns. $f, g \in \mathcal{O}(U)$ are the same iff $f \equiv g \bmod \mathfrak{m}_v$, for $v \in U$. [i.e. $f-g \in \bigcap_{v \in U} \mathfrak{m}_v$.]

▷ Since $\mathfrak{m}_v$ is principal & infinite U, this means $f-g=0$ in K.
(Exercise)

▷ $\forall f \in K$, $\exists$ open $U \subseteq C_k$ st. $f \in \mathcal{O}(U)$.

Pf: • $f = g/h$, for g & h polynomials.
• f is not defined at $v \in C_k$ iff $h \equiv 0 \bmod \mathfrak{m}_v$.

$\Rightarrow$ these bad pts. v form a closed set.

$\Rightarrow$ $f = g/h$ defined on open $U \subseteq C_k$. $\square$

Defn: • We call C_k, together with regular fns. functor $\mathcal{O}(\cdot)$ & fn. field K, an abstract curve.

• A morphism $\varphi: X \to Y$ between curves/ abstract curves is a continuous map s.t. $\forall$ open $V \subseteq Y$, $\forall f \in \mathcal{O}_Y(V)$, $f \circ \varphi \in \mathcal{O}_X(\varphi^{-1}(V))$.

pull-back

open

▷ Every non-sing. quasi-proj. curve is isomorphic to an abstract curve.

Pf: • Let X be a non-sing. quasi-proj. curve.

• $\phi : X \longrightarrow Y := C_{K(X)}$.

$P \longmapsto v_P$ (valuation corr to pt. P)

▷ as, $\mathcal{O}_{X,P}$ is dvr iff $P \in X$ is non-sing.

Exercise: What's the inverse of ϕ?

[Handle the dvr "R_{Y_x}" via the projective space's "pt. at ∞".]

$\square$

Existence of non-sing. models

Theorem: Let $k \subset K$ be trdeg=1 field extension. Then, the abstract curve C_K is isomorphic to a non-singular projective curve.

Pf: • Idea: Glue the finitely many non-sing. models, one for each singular pt. in X $(K(X)=X)$, together via some "cartesian" product.

dvr

• For pt. $v \in C_K$, we've $\mathfrak{m}_v \subset R_v \subset K$ defined.

• Pick valuation v_1 (that's unresolved in given X). See dvr R_{v_1} as $\mathcal{O}_{v_1, P_1}$ of some non-singular pt. P_1 in a quasi-affine curve V_1.

$\Rightarrow R_{V_1} \cong \mathcal{O}_{V_1,P_1}$ & $Z(\mathfrak{m}_{V_1}) \cap V_1 = \{P_1\}$.

▷ $\exists$ open $U_1 \subset C_K$ that is realized by V_1.

- Do this for finite steps to get $\{V_i \mid i \in [m]\}$ & $\{P_i \mid i \in [m]\}$ & $\{U_i \mid i \in [m]\}$.

▷ $C_K = \bigcup_{1 \le i \le m} U_i$; isomorphism $\varphi_i : U_i \xrightarrow{\sim} V_i \hookrightarrow Y_i$

[Suitable $cl(V_i)$ in proj. space] $\Rightarrow$ non-sing. projective curve

[Eg. $y^2 = x^5 + x \to y^2 z^3 = x^5 + x z^4$

$\rightsquigarrow$ <u>Exercise</u>: Make this smooth proj.?]

▷ $C_K \setminus U_i$ is finite.

<u>Claim</u>: φ_i extends to $\overline{\varphi_i} : C_K \to Y_i$ (morphism).

<u>Pf</u>: - Eg. $\varphi_i : U_i \to Y_i$ extends uniquely to

$$\varphi_i^! : U_i \cup \{p\} \longrightarrow Y_i \quad .$$

- Let $\varphi_i : \bar{a} \mapsto (f_0(\bar{a}) : f_1(\bar{a}) : \cdots : f_n(\bar{a}))$ via fns. $f_0, \to f_n$ on an open patch.
- Try defining $\overline{\varphi_i} : p \mapsto (f_0(p) : \cdots : f_n(p))$.

Qn: What if $f_i(p) = 0$, $\forall i$?

- Idea: Consider $\{v_p(f_i) \mid i \in [0 \dots n]\}$.

Let $v_p(f_s)$ be the min.

Consider $\overline{\varphi_i} : p \mapsto \left(\frac{f_0(p)}{f_s(p)} : \cdots : 1 : \cdots : \frac{f_n(p)}{f_s(p)} \right)$.

$\Rightarrow$ This can be repeated for more p's. $\square$

- Now, use these Φ_i's to define the common morphism:

$$\Phi : C_K \longrightarrow \prod_{i=1}^{m} Y_i$$
$$v \longmapsto SE(\Phi_i(v) \mid i \in [m])$$

& define $Y := cl(\Phi(C_K))$ in projective space (big enough).

- Eg. The "cartesian product" is called <u>Segre embedding</u>. It maps $(x_0 : x_1) \times (y_0 : y_1)$ to $(x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1)$; $\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3$

<u>SE</u>: $\mathbb{P}^n \times \mathbb{P}^{n'} \longrightarrow \mathbb{P}^{(n+1)(n'+1)-1}$.

$\Rightarrow$ C_k has been realized as a non-sing. proj. curve with the same $\mathcal{O}(\cdot)$ functor.

[any curve $X \rightsquigarrow C_{k(X)} \rightsquigarrow$ this.] $\square$

$\mathbb{A}^n_k$ or $\mathbb{P}^n_k$ $\longleftarrow\!\!\longrightarrow$ $K(\mathbb{A}^n_k)$; $\operatorname{trdeg}_k - 1$.

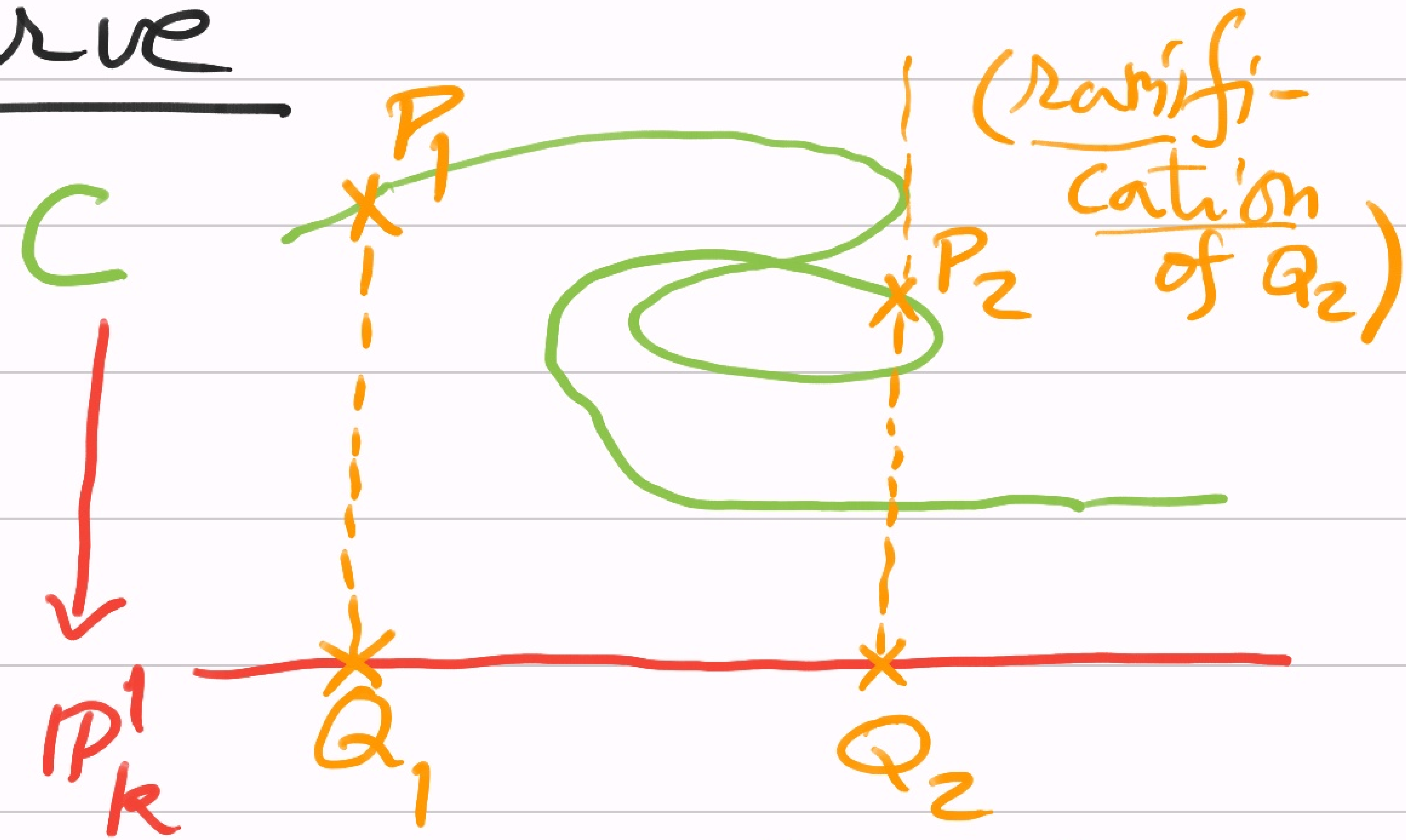
non-sing. pt. $P \in X$ $\longleftrightarrow$ $\mathcal{O}_{X,P}$ is dvr in $K(X)$ & $\operatorname{rk} T_{X,P} = 1$

non-sing. proj. curve X; $C_{K(X)}$ $\longleftrightarrow$ $K(X)$

$T_{X,P}$ $\longleftrightarrow$ $T_{X,P}^{\vee} \cong \mathfrak{m}_P/\mathfrak{m}_P^2$.

- Now, we study only non-sing. curves.
- Use non-sing. $\approx$ simple $\approx$ smooth.

Points on a smooth curve



▷ Smooth proj. curve C covers the projective line $\mathbb{P}^1_k$, if $k = \overline{k}$.

$k \subset k(x) \subset K := K(C)$

Pf: • Pt. $P \in C$ gives a dvr $\mathcal{O}_{C,P}$ $\Rightarrow$ $\mathcal{O}_{C,P} \cap k(x)$ is dvr

$\Rightarrow$ gives the pt. $Q \in \mathbb{P}^1_k$ via the uniformizer.

- pt. $Q \in \mathbb{P}^1_k$ gives dvr $R \subset k(x)$;
  extend it to $\tilde{R} \subset K(C)$
  $\Rightarrow$ gives pt. $P \in C$ via the uniformizer.
  [$\tilde{R}$ & P are <u>not</u> unique]

$\square$

<u>Qn</u>: For finite field $\mathbb{F}_q$, what is
$\left| |C(\mathbb{F}_q)| - |\mathbb{P}^1_{\mathbb{F}_q}| \right| = ?$

$\mathbb{P}^1_{\mathbb{F}_q}$: $(q+1)$

pt. corr. to dvr in k; it may be a <u>cluster</u> of <u>conjugates!</u>

- <u>Defn</u>: Think of K over $k(\bar{x}) = \mathbb{F}_q(\bar{x})$. A pt. $P \in C_k$ defines a <u>valuation</u> v_P on K given by $\mathcal{O}_{C,P}$.

- Residue field at P is $k_P := \mathcal{O}_{C,P}/\mathfrak{m}_P$.

  (Possibly $k_P \supsetneq k$. Eg. $\mathbb{F}_{q^2} \cong \mathbb{F}_q[x_1]/\underbrace{(x_1^2 - \alpha)}_{\text{prime ideal}}$)
- The degree of P is $d(P) := [k_P : k]$.

Proposition: (i) $d(P) < \infty$

(ii) $\bigcap_{i>0} \mathfrak{m}_P^i = \{0\}$

(iii) If $\mathfrak{m}_P =: \langle u \rangle \mathcal{O}_{C,P}$, then $\forall \alpha \in K$,

$v_P(\alpha) = i$: largest $i \in \mathbb{N}$ s.t. $\alpha \in u^i \mathcal{O}_{C,P}$.

Pf: (i) Let $\mathfrak{m}_P =: \langle u \rangle \mathcal{O}_{C,P}$. It can be seen that

$$d(P) = |Z(u) \cap C(\bar{k})| < \infty.$$

" # conjugates under Galois action of k_P/k.

(ii) Let ${}^{K \ni} y \in \bigcap_{i \geq 0} m_p^i$. $\Rightarrow$ $u^i \mid y$, $\forall i \geq 0$.

$\Rightarrow$ $y = 0$.

(iii) Clear from the defn. of v_p earlier. $\square$

— $f \in K(C)$ gives $\{ v_p(f) \mid P \in C \}$.

Qn: Given RHS does there exist an f?

— We'll now show that f can be reconstructed that matches a finite part of RHS; but not the whole part!

Theorem (Approximate val.): Let K be the fn. field of a curve C. Let $p_1, \ldots, p_h \in C$ be distinct with corr. valuations $v_1, \ldots, v_h \in G_K$. Let $u_1, \ldots, u_h \in K$ & $m_1, \ldots, m_h \in \mathbb{Z}$.

offset fns. mult.

Then, $\exists u \in K$, $\forall i \in [h]$, $v_i(u - u_i) \geq m_i$.

Pf: • Base case $[h=1]$: $v_1(\underline{\underline{u}} - u_1) \geq m_1$

Let α_1 be p_1's uniformizer. Consider $u := u_1 + \alpha_1^{m_1}$.

• Induction step $[h>1]$, assuming up to $h-1$.

Claim 1: Given $e_1, \ldots, e_{h-1} \in \mathbb{Z}$, $\exists u \in K$, $\forall i \in [h-1]$, $v_i(u) = e_i$.

Pf: • Find w_i's s.t. $\forall i \in [h-1]$, $v_i(w_i) = e_i$

• Consider the system: $\forall i \in [h-1]$, $v_i(u-w_i) \geq e_i+1$.

$\Rightarrow$ By ind. hyp. (of Thm), we get $u \in K$.

$\Rightarrow v_i(u) = v_i(u-w_i+w_i) = v_i(w_i) = e_i$. $\square$

Claim 2: $v_1, \ldots, v_h$ are $\mathbb{Q}$-linear-independent.

Pf: • Suppose not. Let $v_h(u) = \sum_{i \in [h-1]} r_i \cdot v_i(u)$, $\forall u \in K$, for some $r_i \in \mathbb{Q}$

• $[h=2 \;\&\; r_1 > 0]$: $\Rightarrow \{z \in k : v_1(z) \geq 0\} = \{z \in k : v_2(z) \geq 0\}$

$\Rightarrow$ dvr's $R_{v_1} = R_{v_2} \Rightarrow p_1 = p_2 \Rightarrow \lightning$.

$[r_1 < 0]$: Find $z, z' \in K$, $\forall i \in [h-1]$,

$v_i(z) = 1$, $v_i(z') = 0$; if $r_i \geq 0$.

$v_i(z) = 0$, $v_i(z') = 1$; if $r_i < 0$.

[z, z' exist from Claim-1.]

$\Longrightarrow v_h(z) \geq 0$ & $v_h(z') < 0$ [Use the additive prop. of $v(\cdot)$]

$\triangleright$ $\forall i \in [h-1]$, $v_i(z+z') = \min(0,1) = 0$

$\Longrightarrow v_h(z+z') \geq 0$.

Also, $v_h(z+z') = \min(v_h(z), v_h(z')) < 0$

$\Longrightarrow$ ↯.

Case $[h \geq 3$ & r_i's $\geq 0]$: Rewrite $v_1(u)$ in terms of $v_2(u), \ldots, v_h(u)$ $\Longrightarrow$ Go to previous case. $\square$

- Next time we'll design u of the form:

$$u := \sum_{i\in[h]} x_i u_i \quad , \text{ for } x_i \in K.$$

-Eg. $v_1(u-u_1) = v_1\left((x_1-1)u_1 + \sum_{i=2}^{h} x_i u_i \right) \geq m_i$.

<u>Claim 3:</u> $\exists\, z_1, \to z_h \in K^*$ st. $\det\left((v_i(z_j))\right)_{h\times h} \neq 0$.

Pf: $\cdot\ rk_{\mathbb{Q}}\left\{ \bar{r} \in \mathbb{Q}^h \mid \sum_{i=1}^{h} r_i \cdot v_i(z_1) = 0 \right\} = h-1.$

<u>Exercise</u>: $\exists\, z_1 \in K^*$ because $\{v_i | i\}$ are $\mathbb{Q}$-l.i.

- Consider $rk_{\mathbb{Q}}\left\{ \bar{r} \in \mathbb{Q}^h \mid \sum r_i \cdot v_i(z_1) = 0 \ \&\ \sum r_i \cdot v_i(z_2) = 0 \right\}$

$h-2 =$ for some $z_2 \in K^*$. (Plug the I in the II eqn.)

• On repeating this, we get $z_1, \ldots, z_h \in K^*$ s.t. <u>no</u> (nonzero) $\mathbb{R}$-linear combination of $\{v_1(z_j), \ldots, v_h(z_j)\}$ vanishes, simultaneously for $j \in [h]$.

$\Rightarrow V := ((v_i(z_j)))_{h \times h}$ is invertible. $\square$

– Now, we move to the induction-step (find u):

→ Solve for c's s.t. $\sum_{j \in [h]} c_{jm} \cdot v_i(z_j) = \begin{cases} -1, & \text{if } i = m \\ 1, & \text{else} \end{cases}$ $\forall i, m \in [h]$

(as $h \times h$-matrix)

▷ $V \cdot c = \begin{pmatrix} -1 & & 1 \\ & -1 & \\ 1 & & \ddots \; -1 \end{pmatrix}$.

- Pick $d \in \mathbb{N}$ s.t. $\{d \cdot c_{jm} \mid j, m \in [h]\} \subset \mathbb{Z}$.
- Define $y_m := \prod_{j \in [h]} z_j^{dc_{jm}}$, $\forall m \in [h]$.

▷ $v_i(y_m) = \begin{cases} -d, & \text{if } i = m \\ d, & \text{else} \end{cases}$

- Define $x_m := (1 + y_m^{-1})^{-1} \in K^*$, $\forall m \in [h]$.

▷ For $i \neq m$, $v_i(x_m) = -v_i(1 + y_m^{-1}) = -(-d) = d$.

▷ For $i = m$, $v_m(x_m - 1) = v_m\left(\frac{y_m}{y_m + 1} - 1\right) = v_m\left(\frac{-1}{y_m + 1}\right)$
$= d$.

· Set $u := \sum_{i \in [h]} x_i u_i$ [Fix d large enough, s.t. $d + v_i(u_j) \geq \max(m_1, \dots, m_h)$ $\forall i, j \in [h]$]

$$\Rightarrow u - u_i = u_i \cdot (x_i - 1) + \sum_{\substack{m \in [h] \\ i \neq m}} x_m \cdot u_m$$

$\triangleright$ $v_i(u - u_i) \geq m_i$. $\forall i \in [h]$

$d + v_i(u_i)$ $d + v_i(u_m)$

$\Rightarrow$ completes the induction-step. $\square$

Corollary: Let $S \subset C$ be finite. Let $\{m_P \mid P \in S\} \subset \mathbb{Z}$. Then, $\exists f \in K(C)^*$, $\forall P \in S$, $v_P(f) = m_P$.

Warning: $Z(f) \cup Z(1/f) \supsetneq S$.

<u>Ex</u>: Take $C = \mathbb{P}^1$ & find f's for S.

$\to$ Now, the goal is to study the set of <u>all</u> fns. in $K = K(C)$ whose zeros are <u>at least</u> that in $S \subset C$.

- The formal construct, of much use here, is: the <u>divisor group</u>.