Divisors of a Curve (or K)

- **Defn:** · The free abelian group $\mathrm{Div}(C) := \sum_{P \in C} \mathbb{Z} \cdot P$ is the group of divisors of a smooth projective curve.
  ($P \in C$ iff $\mathcal{O}_{C,P}$ is dvr in $k(C)$) → P is a prime ideal in $k[\bar{x}]$

  Note: $d(P)$ may not be $= 1$.

- Ex. $(P_1 + P_2) + (P_2 - P_1 + P_3) = 2P_2 + P_3$.
  $P_1 - P_1 = 0$.

↳ $\mathrm{Div}(C)$ elements have finite support in the definition. → $\sum_{i \geq 1} P_i$ is not in $\mathrm{Div}(C)$.

- Any element $D \in Div(C)$ is a <u>divisor of K</u>.
- Define the <u>order map</u>, $ord_p : Div(C) \to \mathbb{Z}$, $D \mapsto a_p$

  s.t. $D =: \sum_{P \in C} a_P \cdot P$,

  ▷ ord_p is a group homomorphism

- Define <u>degree map</u>, $d : Div(C) \to \mathbb{Z}$, $D \mapsto \sum_{P \in C} a_P \cdot d(P)$

  s.t. $D =: \sum_{P \in C} a_P \cdot P$.

  ▷ $d(\cdot)$ is a group homomorphism.

- $\ker d(\cdot) =:$ <u>group of deg-0- divisors</u>, denoted by <u>$Div_0(C)$</u>.

- Support of D, $\operatorname{supp}(D) := \{P \in C \mid \operatorname{ord}_P(D) \neq 0\}$.
- D is called integral / positive / effective if $\forall P \in C$, $\operatorname{ord}_P(D) \geq 0$. Write it as $D \geq 0$.
- D_1 divides D_2 if $D_2 - D_1 \geq 0$. Write it as $D_2 \geq D_1$ or $D_1 \leq D_2$.

→ Eg. Integers are divisors of $\langle 0 \rangle$.
→ Points $P \in \operatorname{Div}(C)$ divide $I(C) = \langle x_2^2 - x_1^3 - x_1 \rangle$
→ $P_1 \pm P_2$ "abstract" divisor of "".

→ These divisors (written additively) are new objects.

- Divisors are interesting because each rational fn. $x \in K^*$ has an associated principal divisor, defined as:

$$(x) := \sum_{P \in C} v_P(x) \cdot P \in Div(C) ?$$

▷ (x) is well-defined because $v_P(x) \neq 0$ only for finitely many $P \in C$.

Pf: $\because v(x) = 0$, for all but finitely many $v \in C_K$. □

— Ex. Let $C = Z(x_2^2 x_0 - x_1^3 + x_1 x_0^2) \subset \mathbb{P}_k^2$.
▷ For $f := x_1/x_2 \in K(C)$, what is $(f) = ?$

• $P_1 = \langle x_1, x_0 \rangle = \langle x_1 \rangle_{R_{P_1}}$

$v_{P_1}(f) = v_{P_1}(x_1) - v_{P_1}(x_2) = 1 - 0 = 1.$

• $P_2 = \langle x_1, x_2 \rangle = \langle x_2 \rangle_{R_{P_2}}$ with $x_1 \approx x_2^2$ up to units in R_{P_2}

$\Rightarrow v_{P_2}(f) = v_{P_2}(x_1) - v_{P_2}(x_2) = 2 - 1 = 1$

• $P_3 = \langle x_2, x_1 + x_0 \rangle = \langle x_2 \rangle_{R_{P_3}}$ with $x_2^2 \approx x_1 + x_0$ up to units in R_{P_3}.

$\Rightarrow v_{P_3}(f) = v_{P_3}(x_1) - v_{P_3}(x_2)$
$= 0 - 1 = -1.$

• $P_4 = \langle x_2, x_1 - x_0 \rangle = (x_2)_{R_{P_4}}$, with $x_2^2 \approx x_1 - x_0$ up to units in R_{P_4}.

$\Rightarrow v_{P_4}(f) = v_{P_4}(x_1) - v_{P_4}(x_2)$
$= 0 - 1 = -1.$

▷ $(x_1/x_2) = P_1 + P_2 - P_3 - P_4 \in Div(C)$.

▷ $d(\ \ ) = 0$. $\Rightarrow (f) \in Div_0(C)$.

– Later, we'll prove it for all prin. div.

Qn: Is the converse true, i.e. $\forall D \in Div_0(C)$, $\exists f \in K$, $D = (f)$?

Proposition: The set $Div_a(C) := \{(x) \mid x \in K^*\}$ is a subgroup of $Div(C)$.

Pf: • $(x) + (y) = (xy)$, $\forall x, y \in K^*$.

• Follows from the valuation-axiom. □

▷ $\mathrm{Div}_a(C) \lhd \mathrm{Div}(C)$ & $\mathrm{Div}_0(C) \lhd \mathrm{Div}(C)$.

– Our long-term goal is to compare these subgroups quantitatively!

– For $x, y \in K$ & $D \in \mathrm{Div}(C)$, we write $x \equiv y \bmod D$ if $(x-y) \geq D$ [i.e. $D \mid (x-y)$].

▷ $\equiv_D$ is an equivalence relation on $K = k(C)$.

Pf: $x-y, y-z \geq D \Rightarrow v_p(x-z) \geq \min(v_p(x-y), v_p(y-z))$

$\geq \min(\mathrm{ord}_p(D), \mathrm{ord}_p(D)) = \mathrm{ord}_p(D)$.

$\Rightarrow \quad x - 3 \geq D$. $\square$

- We want to now study the "approximation thm" in greater detail, wrt D.

- Defn: For $D \in \mathrm{Div}(C)$, define subset of fns.

$$L(D) := \{0\} \cup \{x \in K^* \mid (x) \geq -D\}.$$

↖ $L(D)$-sheaf

↳ It collects fns. whose poles are not any worse than D.

- For $S \subseteq C$, define a <u>restricted</u> divisor (of D) $\underline{D_S} := \sum_{P \in S} \operatorname{ord}_P(D) \cdot P$.
- $\underline{L(D)_S} := \{0\} \cup \{ x \in K^* \mid (x)_S \geq -D_S \}$.
  → restricted $L(D)$-sheaf
  ↳ only about zeros/poles in S

- Ex. $S \cap \operatorname{supp}(D) = \emptyset \Rightarrow {}^{0\neq} x \in L(D)_S$ iff $(x)_S \geq 0 \iff \forall P \in S,\ v_P(x) \geq 0 \iff$
$$x \in \bigcap_{P \in S} R_P .$$

▷ $L(D) \subseteq L(D)_S$. 事实: $(x) \geq -D \Rightarrow (x)_S \geq -D_S$. □

Proposition: (i) $L(D)_S$ is a k-vector space.

(ii) $D_1 \geq D_2 \Rightarrow L(D_1)_S \supseteq L(D_2)_S$.

(iii) $S \subseteq S' \Rightarrow L(D)_S \supseteq L(D)_{S'}$.

(iv) $D_S = D'_S \Rightarrow L(D)_S = L(D')_S$.

Pf:

(i) $v_p(x), v_p(y) \geq -\mathrm{ord}_p(D) \Rightarrow \forall \alpha, \beta \in k$,

$v_p(\alpha x + \beta y) \geq$ " $\Rightarrow$

[$x, y \in L(D)_S \Rightarrow \alpha x + \beta y \in L(D)_S$] $\Rightarrow$ done.

(ii) $x \in L(D_2)_S \Rightarrow (x)_S \geq -(D_2)_S \geq -(D_1)_S$

$\Rightarrow x \in L(D_1)_S \Rightarrow$ done.

(iii) & (iv): Similar. $\square$

– We want to now "measure" how big is $L(D')$ compared to $L(D)$ when $D' \geq D$.

Theorem: Let $D_S' \geq D_S$ in $\mathrm{Div}(C)$ for finite $S \subseteq C$. Then, $\dim_k L(D')_S / L(D)_S = d(D_S') - d(D_S)$.

Pf: Idea – Induction on $\sum_{P \in S} \mathrm{ord}_P(D'-D)$. We'll use the finiteness of S to invoke the approx. thm on $v_P(\cdot)$ for $P \in S$.

Induction step: Let $D_S' - D_S = \sum_{i=1}^{h} Q_i$ for $h > 1$. Consider the tower of spaces:

$$L(D)_S \subseteq L(D+Q_1)_S \subseteq \cdots \subseteq L(D+Q_1+\cdots+Q_h)_S = L(D')_S$$

$$\Rightarrow \dim_k L(D')_S / L(D)_S = \sum_{i=1}^{h} \dim_k L(D+Q_1+\cdots+Q_i)_S \,/\, L(D+Q_1+\cdots+Q_{i-1})_S$$

$$= (\text{by base case}) \sum_{i=1}^{h} d(Q_i) = d(D'_S - D_S)$$

$$= d(D'_S) - d(D_S).$$

Claim (base case): $\dim_k L(D+Q)_S / L(D)_S = d(Q)$.

Pf: Idea: $S =: \{P_1 := Q, P_2, \cdots, P_n\} \subseteq C$ & $d(Q) =: d$.

- We'll develop the k-basis by using that of the residue field $k_Q := R_Q / M_Q \cong k$.

- Let $x_1', \dots, x_d' \in R_Q$ be the k-basis of R_Q (when seen mod M_Q).
- By the approx. thm., we can find another k-basis $x_1, \dots, x_d \in R_Q$ s.t. $\begin{cases} v_Q(x_j - x_j') \geq 1, & \forall j \in [d]. \\ v_Q(x_j) \geq 0, & \forall j, \forall P \in S \setminus \{Q\}. \end{cases}$
- Also, by the approx. thm., find an element $u \in K^*$ s.t. $v_P(u) = -\mathrm{ord}_P(D+Q)$, $\forall P \in S$.

$$\Rightarrow u \in L(D+Q)_S .$$

▷ $x \in L(D+Q)_S \Rightarrow xu^{-1} \in R_Q$.

[Pf: $v_Q(xu^{-1}) = v_Q(x) - v_Q(u) \geq -\mathrm{ord}_Q(D+Q) + \mathrm{ord}_Q(D+Q) = 0. \Rightarrow xu^{-1} \in R_Q.$ □]

$\Rightarrow$ $xu^{-1} \in R_Q$ has a <u>unique</u> expression:

$$xu^{-1} = \sum_{j\in[d]} a_j x_j + x' \quad ; \quad a_j \in k \ \&\ x' \in \mathcal{M}_Q .$$

$$\Rightarrow \quad x = \Big(\sum_{j\in[d]} a_j\cdot(x_j u)\Big) + (x'u) \ .$$

▷ $v_Q(x'u) = v_Q(x') + v_Q(u) \geq 1 - \mathrm{ord}_Q(D+Q)$

$= -\mathrm{ord}_Q(D)$.

▷ For other $P \in S$: $v_P(x'u) \geq -\mathrm{ord}_P(D)$.

- $v_P(x) \geq -\mathrm{ord}_P(D)$
- $v_P(x_j u) \geq 0 - \mathrm{ord}_P(D)$

& use the eqn.

$\Rightarrow$ Thus, $x'u \in L(D)_S$.

$\Rightarrow \dim_k L(D+Q)_s / L(D)_s \leq d$. [As we did it $\forall x \in L(D+Q)_s$.]

- Further, in case some $\sum_{j\in[d]} a_j (x_j u) =: y \in L(D)_s$, for a_j's in k, then:

$\Rightarrow \sum a_j x_j = y u^{-1}$. Going mod M_Q,

$\Rightarrow y u^{-1} \equiv \sum a_j x_j \equiv \sum_{j=1}^{d} a_j x_j'$ is nonzero in k_Q.

$\Rightarrow v_Q(yu^{-1}) = 0 \Rightarrow v_Q(y) = v_Q(u)$
$= -\text{ord}_Q(D) - 1$

$\Rightarrow y \notin L(D)_s \Rightarrow \lightning$.

$\Rightarrow$ $\dim_k L(D+Q)_S / L(D)_S \geq d$ as well!

$\Rightarrow$ Base case is done $\Rightarrow$ Thm is done. $\square$

- This gives us "weak" estimate for $L(D)$:

Corollary 1: For any $D' \geq D$ in $Div(C)$,
$\dim_k L(D')/L(D) \leq d(D') - d(D)$.

Pf: • Let us use $S := \mathrm{supp}(D) \cup \mathrm{supp}(D')$.

▷ $L(D') \subseteq L(D')_S$; $L(D) \subseteq L(D)_S$; $L(D) \subseteq L(D')$.

$\Rightarrow$ $L(D')/L(D) \hookrightarrow L(D')_S / L(D)_S$ is an injection.

- $L(D')/L(D) = L(D') / L(D') \cap L(P)_S$
$\cong (L(D') + L(D)_S) / L(D)_S \subseteq L(D')_S / L(D)_S$.
gives the injection.
- Now the thm gives: $\dim_k L(D')/L(D) \leq d(D') - d(D)$. □

Corollary 2: $\ell(D) := \dim_k L(D)$ is finite, $\forall D \in Div(C)$.

Pf: • Let $D_0 > 0$ be s.t. $D \geq -D_0$.
▷ $L(-D_0) = \{x \in K^* \mid (x) \geq D_0\} \cup \{0\} = \{0\}$.
$\Rightarrow \nexists x$ as we need zeros but no poles.
• Thm $\Rightarrow \ell(D) = \dim_k L(D)/L(-D_0) \leq d(D) + d(D_0) < \infty$. □

▷ $D' \geq D \Rightarrow \ell(D') - d(D') \leq \ell(D) - d(D)$. [Cor. 1]

$\Rightarrow$ $\ell(D')$ gets "closer" to degree, as $D' \uparrow$.

Qn: · Does large enough D satisfy $\ell(D) = d(D)$?
· Does $\ell(D) - d(D) \to -\infty$?

↳ Studying this leads Riemann to genus of the curve.

→ First, we try to understand (x) & $\mathrm{Div}_0(C)$.

Degree of principal divisors

- For an $x \in K^*$, define the <u>divisor of zeros</u>
$(x)_0 := \sum \{v_P(x) \cdot P \mid v_P(x) > 0\}$ $\in Div(C)$,

and the <u>divisor of poles</u> $(x)_\infty := -\sum \{v_P(x) \cdot P \mid v_P(x) < 0\}$
$\in Div(C)$ & positive.

▷ $(x) = (x)_0 - (x)_\infty$.

▷ $d((x)_0) = d((x)_\infty)$.

Pf: Why? □

Theorem: $\forall x \in K \setminus \bar{k}$, $d((x)_0) = d((x)_\infty) = [K : k(x)]$.

Pf: • Let $N := [K : k(x)] < \infty$ ($\because \operatorname{tr.deg} K = 1$).

• $D := (x)_0$ with support S.

• First, we show: $d(D) \leq N$. [Idea: Use $L(0)_S$]

• Let $y_0, \rightsquigarrow y_N \in L(0)_S$ be fns.

$\Rightarrow \exists\, f_0, \rightsquigarrow f_N \in k[x]$, not all zero, s.t.

$$\sum_{0 \leq i \leq N} f_i y_i = 0.$$

(by defn. of N)

• Wlog, not all the $a_j := f_j(0)$ are zero.

• Rewrite the dependence as: $\sum_j a_j y_j = -x \cdot \sum_j g_j y_j$.

where $a_j + x \cdot g_j := f_j$.

$\Rightarrow \forall P \in S,\ v_P(\sum a_j y_j) = v_P(x) + v_P(\sum g_j y_j)$

$\geq v_P(x) + \min_j (v_P(g_j) + v_P(y_j))$

[Pole of g_j can only be ∞, but $\infty \notin S$.] $\quad \geq 0 \quad \geq 0$

$\geq v_P(x) = \mathrm{ord}_P(D)$.

$\Rightarrow \sum_{j=0}^{N} a_j y_j \in L(-D)_S$

$\Rightarrow \dim_k L(0)_S / L(-D)_S \leq N$.

- We know that $LHS = d(0) - d(-D) = d(D)$

  $\Rightarrow d(D) \leq N$.

- Next, we show: $d(D) \geq N$. [Idea: Use $L((x^e)_\infty)$.]
- Let $y_1, \ldots, y_N$ be a $k(x)$-basis of K s.t. they are integral over $k(x)$. [Existence?]

[Eg. $xy_1^2 + y_1 + x^2 = 0$ is a minpoly over $k[x]$.
$\Rightarrow x^2y_1^2 + xy_1 + x^3 = 0 \Rightarrow (xy_1)^2 + (xy_1) + x^3 = 0$
$\Rightarrow (xy_1)$ is an integral basis!]

· Also, $\{ x^i y_j \mid i \in [t], j \in [N] \} =: \underline{B}$ are k-linear-indep., for any $t \in \mathbb{N}$.

▷ y is integral over $k[x]$ & $v_p(y) < 0 \Rightarrow v_p(x) < 0$.
[Pf: Eg. $y^2 + x \cdot y + (x^2+1) = 0 \Rightarrow v_p(y^2) = v_p(\cdot)$ of one of the other three monomials $\Rightarrow \cdots$
$v_p(y^d) = v_p(y^i x^j) \Rightarrow v(y^{d-i}) = v(x^j) \Rightarrow v_p(x) < 0$.]

$\Rightarrow$ Poles of y_j are shared by x.

$\Rightarrow$ For large enough $s \in \mathbb{N}$, the divisors

$\{ \underbrace{(x^{s+t})_\infty}_{\to \text{(is big enough)}} + (x^i y_j) \mid i \in [t],\ j \in [N] \}$ are all positive.

$\Rightarrow$ $x^i y_j \in L((x^{s+t})_\infty) \Rightarrow B \subseteq L((x^{s+t})_\infty)$.

$\Rightarrow$ $\ell((x^{s+t})_\infty) \geq |B| = Nt$.

- $(x^{s+t})_\infty \geq (x)_\infty \Rightarrow \ell((x^{s+t})_\infty) \leq d((x^{s+t})_\infty) + \ell((x)_\infty) - d((x)_\infty)$

$\Rightarrow Nt \leq (s+t-1) \cdot d((x)_\infty) + \ell((x)_\infty)$. (*)

$\Rightarrow N \leq d((x)_\infty)$.

→ Repeat this pf for $1/x$; since $k(x) = k(x^{-1})$

$\Rightarrow d((1/x)_\infty) \geq N$

$d(\mathcal{D}) = d((x)_0) \leq$

$\Rightarrow d(\mathcal{D}) = N$.

& $d((x)_\infty) = N$. □

Corollary: (1) $\forall\, x \in K^*$, $d((x)) = 0$.

(2) $0 \to Div_a(C) \xrightarrow{\subseteq} Div_0(C) \xrightarrow{\subseteq} Div(C) \xrightarrow{d(\cdot)} \mathbb{Z}$

is a sequence of (abelian gp.) homomorphisms.

– This allows us to define:

Defn: • $\underline{Cl(C) := Div(C)/Div_0(C)}$ is the group of divisor classes.

• $\underline{Cl_0(C) := Div_0(C)/Div_0(C)}$ is the group of divisor classes of deg = 0.

▷ $0 \xrightarrow{\subseteq} Cl_0(C) \xrightarrow{\subseteq} Cl(C) \xrightarrow{d(\cdot)} \mathbb{Z}$ is an exact sequence of gp. homo,

↖ i.e. img of a map = ker of the subsequent map

Qn: Is $d(\cdot)$ an onto map?

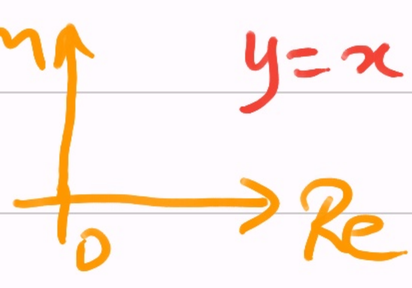
→ Defn of $d(C)$ on $\mathrm{Div}(C) / \mathrm{Div}_a(C) =: Cl(C)$.

$\forall x$, $d(D+(x)) \overset{?}{=} d(D)$

$\leq$ $d(D) + d((x)) = d(D)$.

→ Next, we do Riemann's genus thm.

A detour on genus: In complex analysis a curve C is "drawn" as a Riemann surface.



$y = x$ vs. $y^2 = x$ vs. $y^2 = x + x^3$ over $\mathbb{C}$.

- A "hole" is characterized by drawing loops.

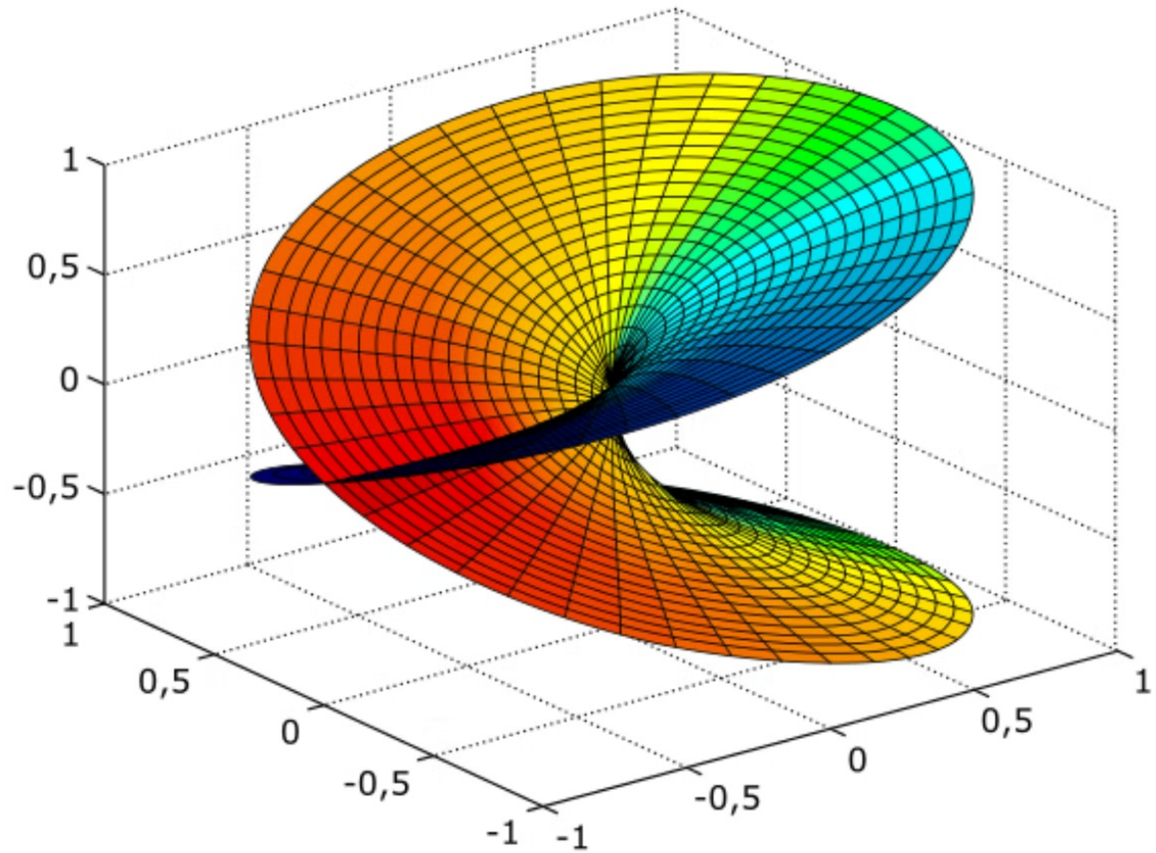
Riemann surface of the complex curve $y^2 = x$.

↳ vertical axis has $\mathrm{Re}(\sqrt{x})$.

↳ color denotes $\mathrm{Im}(\sqrt{x})$.

↳ base plane denotes $x \in \mathbb{C}$.

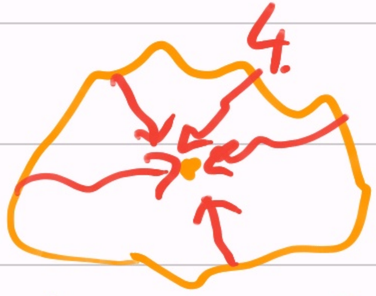
↳ Has <u>no</u> holes (genus = 0)



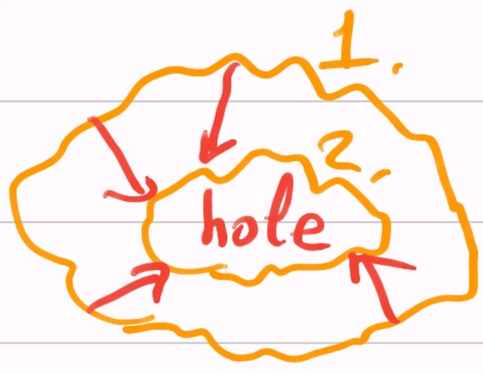
Courtesy Wikipedia

→ Two loops are called equivalent if there is a nice transformation.

genus(C) :=
#holes in C
(in Riemann surface)



loop4 ≡ pt.
= 0 loops
= g(C).



loop1 ≠ loop2
⇒ g(C) > 0.

▷ Torus is genus 1.

Qn: Do fns K(C) "know" about g(C)?

→ Riemann (1857) showed: $\min_D (\ell(D) - d(D) - 1) = -g(C)$.

← Since we don't have any way to define $g(C)$ over $\mathbb{F}_p$, we intend to take this "thm" as a defn.

For any field k, curve C,

Theorem (Riemann, 1857): $\exists\ g := g(C,k) \in \mathbb{N}_{\geq 0}$ s.t. $\forall\ x \in K \setminus \bar{k}$, $\min_{m \in \mathbb{N}} \{\ell((x^m)_\infty) - 1 - d((x^m)_\infty)\} = -g$.

[We call this g the genus of k.]

- $\forall D \in \mathrm{Div}(C)$, $\ell(D) - 1 - d(D) \geq -g$.

Pf: • Begin with an $x \in K \setminus \overline{k}$.

• Let $N := [K : k(x)]$ & large enough $s \in \mathbb{N}_{>0}$.

• We know from the previous pf. that: $\forall t \in \mathbb{N}$,

$$Nt \leq \ell((x^{s+t})_\infty).$$

• Writing $m = s+t$, we deduce: $\forall m \geq s$,

$$\ell((x^m)_\infty) - d((x^m)_\infty) \geq Nt - m \cdot N = -sN.$$

$\Rightarrow$ The integer $\underline{M_x} := \min_{m \geq 0} \{\ell((x^m)_\infty) - d((x^m)_\infty)\}$

exists.

[Note: $N \leq \deg_c$ & $s \leq \deg_c \Rightarrow g \leq \deg_c^2$.]

[eg. $f(x,y) = 0$ of $\deg(f)$ is $\deg_c$.]

→ Let's work with any $D \in \mathrm{Div}(C)$.

• $D =: D_0 - D_\infty$, where $D_0, D_\infty \geq 0$.

$\Rightarrow \quad D_0 \geq D$.

$\Rightarrow \quad \ell(D) - d(D) \geq \ell(D_0) - d(D_0)$.

• Also, $(x^m)_\infty \geq -D_0 + (x^m)_\infty$.

$\Rightarrow \ell(-D_0 + (x^m)_\infty) - d(-D_0 + (x^m)_\infty) \geq \ell((x^m)_\infty) - d((x^m)_\infty)$

$\geq \mu_x$.

$\Rightarrow \ell(-D_0 + (x^m)_\infty) \geq -d(D_0) + d((x^m)_\infty) + \mu_x$

$= -d(D_0) + mN + \mu_x > 0$, (large m)

$\Rightarrow \exists\, z \in L(-D_0 + (x^m)_\infty)$ s.t. $(x^m)_\infty \geq D_0 - (z)$

$\Rightarrow \ell(D_0) - d(D_0) \geq \ell((x^m)_\infty) - d((x^m)_\infty) \geq \mu_x$.

$$[\ L(D_0) \xrightarrow{\sim} L(D_0 - (z)) \ : \ f \mapsto fz\ ]$$

$\Rightarrow \ell(D) - d(D) \geq \mu_x$, $\forall D \in Div(C)$.

$\Rightarrow$ μ_x (or genus) is indep. of x.
It only depends on K & k.

□

→ For alg. closed $k(=\bar{k})$, $g(K)$ is called the arithmetic genus of the curve C.

↳ It matches the (classical) genus over $\mathbb{C}$. (Read as an exercise.)

→ Riemann's bf gives an algo. to compute genus. Eg. $y^2 = F(x)$ over $\mathbb{F}_p$.

- Compute $\ell((x^n)_\infty)$.

$$L((x^n)_\infty) = \{ f \in K^* \mid (f) + (x^n)_\infty \geq 0 \}.$$

- $(x^n)_\infty$ is easy to compute.
- $f = \dfrac{a(x) + y\,b(x)}{c(x) + y\,d(x)}$ for unknown a, b, c, d.
- $(f) \geq -(x^n)_\infty$ gives a k-lr. system to find a, b, c, d. $\Rightarrow$ We get a basis.

Corollary: $g \geq 0$.

Pf: • We've $\ell(D) - d(D) \geq 1-g$.

$\Rightarrow \ell(0) - d(0) \geq 1-g \Rightarrow 1 \geq 1-g$

$\Rightarrow g \geq 0$. □

- **Defn:** The **deg of speciality** of a divisor D is $\delta(D) := \ell(D) - d(D) + g - 1 \geq 0$.

- How does $\delta(D)$ change with D?

This was answered, in an exact way, by Gustav Roch (1865) (Riemann's student).

- Ex. $K = k(x)$ & $k = \bar{k}$: $C = \mathbb{P}^1$. What's $g(C)$?

Pick $P \in \mathbb{P}^1$; $\ell(P) - 1 = 1$; $d(P) = 1$

$\Rightarrow \ell(P) - 1 - d(P) = 0 =: g(C)$

▷ $L(P) = \langle 1, \frac{1}{x-\alpha} \rangle_k$; $\left(\frac{1}{x-\alpha}\right) = -P + \infty$

$\| \text{pt.}(\alpha)$

$\geq -P$

- $\ell(mP) - 1 = m$ & $d(mP) = m$; $\forall m \geq 1$

$\Rightarrow g(\mathbb{P}^1) = 0$.

- We now prove Roch's theorem:

Theorem (Riemann-Roch, 1865): $\exists$ canonical divisor W, $\forall D \in \mathrm{Div}(C)$: $\delta(D) = \ell(W - D)$.

Idea: W-D is kind of a dual of D.
Can we realize it as $\approx \mathrm{Hom}_k(K/L(D), k)$.

Adeles

- We'll achieve this by using more abstract "fns." than K, namely adèles (or repartition by Chevalley).

Defn: · For curve C, a tuple $r = (r_P \mid P \in C)$ of rational fns. is called an adele if $v_P(r_P) \geq 0$, except for finitely many, $P \in C$.
· r_P is the P-th component of adele r.

- The set of all adeles, & $\overline{\sigma}$, is $\mathbb{A}$.

Proposition 1: (i) $\exists$ embedding $K \hookrightarrow \mathbb{A}$.
(ii) $\mathbb{A}$ is a K-algebra (not a field).
(iii) $\forall P \in C$, $v_P(\cdot)$ extends from K to $\mathbb{A}$.
(iv) The analog of $L(D)$ in $\mathbb{A}$ is called $\mathbb{A}(D)$.

Pf:
(i) Map $x \in K$ to tuple $\underline{r} := (x \mid P \in C)$. ($r_P$)
We know: $v_P(x) = 0$, except for finitely many $P \in C$. $\Rightarrow$ $\underline{r} \in \mathbb{A}$. [From now on, we'll use x & $\underline{r}$ interchangeably for fns. x.]

(ii) Let $r =: (r_p)$ & $r' =: (r'_p)$ be in A.

• Define $r + r' := (r_p + r'_p)$ & $rr' := (r_p \cdot r'_p)$.

• $v_p(r_p + r'_p) < 0 \Rightarrow v_p(r_p)$ or $v_p(r'_p) < 0$.

$\Rightarrow r + r' \in A$

• $v_p(r_p \cdot r'_p) < 0 \Rightarrow v_p(r_p)$ or $v_p(r'_p) < 0$

$\Rightarrow r \cdot r' \in A$.

$\Rightarrow A$ is K-algebra.

(iii) $v_p : A \longrightarrow \mathbb{Z}$; $r \longmapsto v_p(r_p)$.

$\Rightarrow v_p(\cdot)$ satisfies the val-axioms.

(iv) Let $D \in Div(C)$. $\underline{A(D) := \{r \in A \mid \forall P \in C, v_p(r) \geq -ord_p(D)\}}$. $\triangleright$ $A(D)$ is k-vec. space. $\square$

Proposition 2: (i) Adele r has an associated divisor $D_r \geq 0$. [i.e. $r \in \mathbb{A}(D_r)$.]
[$D_r \approx r_\infty$ here]

(ii) $D' \geq D \Rightarrow \dim_k \mathbb{A}(D')/\mathbb{A}(D) = d(D') - d(D)$.

(iii) $\dim_k \mathbb{A}/(\mathbb{A}(D)+K) = \delta(D) := \ell(D) - d(D) + g - 1$

Pf: (i) Define $D_r := \sum \{ -v_P(r).P \mid P \in C,\ v_P(r) < 0 \}$.
- Its a divisor, as it's a finite sum.
- $r \in \mathbb{A}(D_r)$. [It's like $(x)_\infty$.]

(ii) • Let $S := \mathrm{supp}(D') \cup \mathrm{supp}(D)$.
• It suffices to show: $L(D')_S / L(D)_S \cong \mathbb{A}(D')/\mathbb{A}(D)$.
[$\because \dim_k LHS = d(D') - d(D)$.]

- Start with the map $\varphi : L(D)_S \longrightarrow A(D)$

$$x \longmapsto r_x$$

where, $\underline{(r_x)_p} := \begin{cases} x, & \text{if } p \in S \\ 0, & \text{else} \end{cases}$.

▷ φ is a K-linear homomorphism.

- Thus, φ extends to an injection:

$$\varphi : L(D')_S / L(D)_S \longrightarrow A(D') / A(D).$$

Claim: φ is onto.

Pf: . Let $r \in A(D')$.

. By approx. thm., $\exists\, u \in K : v_p(u - r_p) \geq -\mathrm{ord}_p(D)$, $\forall p \in S$.

$$\Rightarrow \quad v_p(u) \geq \min\{v_p(u-r_p),\ v_p(r_p)\}$$
$$\geq \min\{-\mathrm{ord}_p(D),\ -\mathrm{ord}_p(D')\}$$
$$= -\mathrm{ord}_p(D'); \qquad \forall P \in S.$$

$$\Rightarrow \quad u \in L(D')_S.$$

- Consider its image $\varphi(u) =: r_u$. We'll show: $r_u - r \in A(D)$. (Done!)

- $\forall P \in S,\ v_p(r_u - r) = v_p(u - r_p) \geq -\mathrm{ord}_p(D)$.
- $\forall P \in C \setminus S,\ v_p(r_u - r) = v_p(0 - r_p) \geq -\mathrm{ord}_p(D') = 0$.

$$\Rightarrow \forall P \in C,\ v_p(r_u - r) \geq -\mathrm{ord}_p(D) \Rightarrow r_u - r \in A(D).$$

$\Rightarrow \varphi$ is <u>onto</u>. $\square$

(iii) · Firstly, $\dim_k \mathbb{A}/(\mathbb{A}(D)+k) \leq \delta(D)$:
Suppose $\exists\, h$ adeles $r_1, \rightsquigarrow r_h \in \mathbb{A}$ which are k-lr.indep. mod $(\mathbb{A}(D)+k)$ and pick max.h. [$\leq \delta(D)+1$]

· By (i), get divisors $D_{r_1}, \rightsquigarrow D_{r_h} > 0$ s.t.
$\forall i \in [h]$, $r_i \in \mathbb{A}(D_{r_i})$.

· $D' := \mathrm{lcm}(D_{r_1}, \dots, D_{r_h}) \Rightarrow r_i \in \mathbb{A}(D')$.

$\Rightarrow r_1, \rightsquigarrow r_h$ is a basis of $(\mathbb{A}(D')+k)/(\mathbb{A}(D)+k)$.

· $(\mathbb{A}(D')+k)/(\mathbb{A}(D)+k) \cong \mathbb{A}(D') / (\mathbb{A}(D') \cap (\mathbb{A}(D)+k))$

[Extend a k-basis of denominator to the numerator.]
[$(U+V)/U \cong V/(V \cap U)$.]

- $A(D')/(A(D') \cap (A(D)+K)) \cong A(D')/(L(D')+A(D))$
- $\cong (A(D')/A(D))/((L(D')+A(D))/A(D))$
- $\cong$ (") / ($L(D')/(A(D) \cap L(D'))$)
- $\cong (A(D')/A(D))/(L(D')/L(D))$

which has $\dim_k = (d(D')-d(D)) - (\ell(D')-\ell(D))$

$= (\ell(D)-d(D)) - (\ell(D')-d(D'))$

$\leq (\ell(D)-d(D)) - (1-g)$

$= \delta(D)$. $\Rightarrow h \leq \delta(D)$

$\Rightarrow \dim_k A/(A(D)+K) \leq \delta(D)$.

- Next, we show: $\dim_k A/(A\mathcal{D}+k) \geq \delta(\mathcal{D})$.
- By Riemann's thm., $\exists D_0$ s.t. $\ell(D_0) - d(D_0) = 1-g$.
- Let $D' := \operatorname{lcm}(D, D_0)$. $\Rightarrow \ell(D') - d(D') = 1-g$.
- Also, $\dim_k (A(D')+k)/(A\mathcal{D}+k)$
  $= (\ell(D') - d(D')) - (\ell(D') - d(D'))$ [by above]
  $= \delta(D)$

$\Rightarrow \dim_k A/(A\mathcal{D}+k) \geq \delta(D)$.

$\Rightarrow$ " $= \delta(D)$. $\square$

$\rightarrow$ $A/(A\mathcal{D}+k)$ is a <u>good</u> <u>dual</u> of $L(D)$.
  $\rightarrow$ It's a new sheaf.

Differentials

- We'll now study the k-vector-space $A/(A\mathcal{O})+K)$ via its dual:

Defn: • A differential of K is a map $w \in \mathrm{Hom}(A/(A\mathcal{O})+K), k)$, for some $\mathcal{O} \in \mathrm{Div}(C)$.

- Ex. adeles / diff. of K $\approx$ tangent-space differentials like dx, dy. ($dx^2 = 2x.dx$)

• Denote $\Omega(\mathcal{O}) := \mathrm{Hom}(A/(A\mathcal{O})+K), k)$.

▷ $w \in$ annihilates $A(\mathcal{O})+K$.

▷ $D' \geq D \Rightarrow \Omega(D') \subseteq \Omega(D)$.

- Set of all <u>differentials of K</u> is:

$$\underline{\Omega}_{K/k} := \bigcup_{D \in \mathrm{DIV}(C_K)} \Omega(D) .$$

<u>Proposition</u>: (i) Ω is a K-vector-space.

(ii) $\dim_K \Omega_{K/k} = 1$

(eg. $y^2 = x^3 \Rightarrow 2y\,dy = 3x^2\,dx$)

<u>Pf</u>: (i) Let $w \in \Omega(D)$ & $x \in K$.

- Define $x \cdot w$ to be the map: $A/(A(D)+k) \longrightarrow k$

$r \longmapsto w(r \cdot x)$. ▷ $w(r) = 0 \Leftrightarrow x w\left(\frac{r}{x}\right) = 0$.

- Pick another $\omega' \in \Omega(D')$, for $D' \in Div(C)$.
- Consider $E := \gcd(D, D')$. $\Rightarrow E \leq D, D'$.
- Define $\omega + \omega' : A/(A(E)+k) \longrightarrow k$

$$x \longmapsto \omega(x) + \omega'(x).$$

- $\omega|_{A(E)+k} = 0$ ($\because A(E)+k \subseteq A(D)+k$)

& $\omega'|_{A(E)+k} = 0$.

$\Rightarrow \omega + \omega' \in \Omega(E) \Rightarrow \omega + \omega' \in \Omega$. □

▷ $\Omega(D) + \Omega(D') \subseteq \Omega(\gcd(D, D'))$.

& $x \cdot \omega \in \Omega(D + (x))$.

[$\omega|_{A(D)+k} = 0 \Rightarrow x \cdot \omega|_{x^{-1} \cdot A(D)+k} = 0$

As, $x + D \geq 0 \Leftrightarrow (x^{-1})(x) + D + (x) \geq 0$.]

(ii) · Let $\omega \in \Omega(D)$ & $\omega' \in \Omega(D')$ be two nonzero differentials in $\Omega_{K/k}$.

- Pick a positive divisor $E > 0$. [$\Rightarrow \ell(-E) = 0$.]
- Consider two k-lr. homomorphisms:

$$L(D+E) \xrightarrow{\quad i : x \mapsto x\omega \quad} \Omega(-E)$$

$$L(D'+E) \xrightarrow{\quad i' : x' \mapsto x'\omega' \quad} \Omega(-E)$$

[
- $\omega(r) = 0$ if $x\omega\left(\frac{r}{x}\right) = 0$
- $r + D \geq 0 \Rightarrow \frac{r}{x} + (x) + D \geq 0$
$\Rightarrow \frac{r}{x} - E \geq 0$.
]

▷ i & i' are injective.

[Pf: $x\omega = 0 \Leftrightarrow x\omega|_A = 0 \Leftrightarrow \forall r \in A,\ \omega(rx) = 0$
$\Leftrightarrow \forall r' \in A,\ \omega(r') = 0. \Leftrightarrow \omega = 0.$]

Idea: The two embeddings overlap in $\Omega(-E)$.

- $\dim_K(\mathrm{img}(i)) + \dim_K(\mathrm{img}(i'))$

$= \ell(D+E) + \ell(D'+E)$

$\geq d(D+E)+1-g + d(D'+E)+1-g$

$= 2\cdot d(E) + d(D+D') + 2(1-g)$

$> d(E)+g-1$ [Pick $d(E)$ large enough]

$= \ell(-E) - d(-E) + g - 1$ [$\ell(-E)=0$]

$= \delta(-E) = \dim_K A/(A(-E)+K) = \dim_K \Omega(-E)$.

$\Rightarrow \mathrm{img}(i) \cap \mathrm{img}(i') \neq \{0\}$

$\Rightarrow \exists\, x, x' \in K^*, \quad xw = x'w' \Rightarrow w' = \frac{x}{x'}\cdot w$

$\Rightarrow \dim_K \Omega = 1.$ □

- Pick a generator ω of $\Omega_{K/k}$ & consider its associated divisor $D_\omega =: W$.
(canonical divisor of K/k)

Proposition: (i) For any $0 \neq \omega \in \Omega_{K/k}$, the set $M(\omega) := \{ D \in \mathrm{Div}(C) \mid \omega \in \Omega(D) \}$ has a unique maximal element, denoted by (ω). (wrt $\geq$ in $\mathrm{Div}(C)$)

(ii) $\forall x \in K^*$, $\omega \in \Omega$: $(x\omega) = (\omega) + (x)$.

Pf: (i) Why's $d(D)$ bounded in $M(\omega)$?

- $i : L(D) \longrightarrow \Omega(0)$; $x \mapsto x\omega$

is a k-linear injection. $\Rightarrow$ $\ell(D) \leq \delta(0)$

$\Rightarrow \ell(D) \le \delta(0) = \ell(0) - d(0) + g - 1 = g$.

- Also, $\ell(D) - d(D) = \delta(D) + 1 - g \ge 1 - g$ $\forall D \in M(w)$

$\Rightarrow d(D) \le \ell(D) + g - 1 \le 2g - 1. < \infty$.

$\Rightarrow \exists$ maximal element $D_w \in M(w)$.

- Let another maximal element be D'_w.
- Consider $\Omega(\text{lcm}(D_w, D'_w))$.

$\triangleright = \Omega(D_w) \cap \Omega(D'_w)$.

[Pf: Use $A(D) + A(D') = A(\text{lcm}(D, D'))$. $\square$]

$\Rightarrow w \in \Omega(\text{lcm}(D_w, D'_w))$.

$\Rightarrow$ (by maximality) $D_w = D'_w$

$\Rightarrow$ D_w is unique in $M(w)$, denoted (w). $\square$

(ii) • $w \in \Omega((w)) \iff xw \in \Omega((w)+(x))$.

• $\because d((x)) = 0 \Rightarrow$ max. deg in $M(xw)$ is $d((w))$.

$\Rightarrow$ (by maximality) $(xw) = (w)+(x)$. (Exercise)

▷ $\Omega_{K/k} \xrightarrow{(\cdot)} Div(C) \longrightarrow Cl(C)$

$w \longmapsto (w) \longmapsto (w) \bmod Div_a(C)$

- Defn: The $\mathrm{img}(w)$, for generator w, above is called the canonical class of K (or C).

Thm (Riemann-Roch, 1865): Let $D \in \mathrm{Div}(C)$ & W be a divisor in the canonical class of C. Then,

- $\Omega(D) \cong L(W-D)$
- $\delta(D) = \ell(D) - d(D) + g - 1 = \ell(W-D)$.

Pf: • Consider $\varphi : L(W-D) \longrightarrow \Omega(D)$; $(\omega) := W$.
$y \longmapsto y\omega$
↑ generates Ω.

- φ is k-lr. injection.
- Let $\omega' \in \Omega(D)$. $\Rightarrow \exists x \in K^*$, $\omega' = x \cdot \omega$.
- Also, $(\omega') \geq D$. $\Rightarrow$ $(x\omega) = (\omega) + (x) \geq D$
  $\Rightarrow W + (x) - D \geq 0$ $\Rightarrow$ $x \in L(W-D)$ is a pre-image of ω' $\Rightarrow$ φ is a k-lr. surjection.

$\Rightarrow \varphi$ is an isomorphism

$\Rightarrow \quad \delta(D) = \ell(D) - d(D) + g - 1 = \ell(W-D).$ □

Corollary 1: $\ell(W) = g$ & $d(W) = 2g-2$.

Pf: • Riemann-Roch $(D=0) \Rightarrow g = \ell(W)$.

• " $(D=W) \Rightarrow g - d(W) + g - 1 = 1$

$\Rightarrow \quad d(W) = 2g-2.$ □

Corollary 2: $d(D) > d(W) = 2g-2 \Rightarrow \ell(D) - d(D) = 1-g$.

Pf: • $d(W-D) < 0 \Rightarrow \ell(W-D) = 0 \Rightarrow \delta(D) = 0.$ □

Corollary 3: $d(D) > d(W) \Rightarrow \exists D' \geq 0$, $D' \sim D$ in $Cl(C)$.

Pf: • Cor. 2 $\Rightarrow$ $\ell(D) - d(D) = 1-g$

$\Rightarrow \ell(D) = d(D) + 1 - g > 2g-2+1-g = g-1 \geq 0$

$\Rightarrow \ell(D) > 0 \Rightarrow \exists x \in L(D)$.

$\Rightarrow D' := D + (x) \geq 0$.

$\rightarrow$ I.e. high-deg $D \sim \sum_i P_i$ for $P_i \in C$, for $\leq d(D)$ many points.

▷ $D_0 := b \cdot \infty$ (with $b \geq 2g-1$). Cor. 2 $\Rightarrow$

$\ell(D_0) - b = 1 - g$.

Qn: Compute W efficiently, given k ?

Jacobian variety (sketch)

- Consider the subset of $Div_0(C)$: (take $k=\bar{k}$)

$$J(C) := \left\{ \sum_{i\in[g]} P_i - g\cdot\infty \;\middle|\; P_1,\dots,P_g \in C \right\}$$

▷ $J(C) \cong Cl_0(C)$.

Pf: Idea: For divisor $D_Y \geq 0$ of $\deg = g-1$, define subset

$$\mathcal{D}_Y := \{ D \in Div_0(C) \mid \ell(D+(2g-1)\infty - D_Y) = 1 \}.$$

$\exists f \in L(D')$: ($D' := D+(2g-1)\infty - D_Y$; $d(D')=g$)

$\Rightarrow D' + (f) \geq 0 \Rightarrow D + (2g-1)\infty - D_Y \sim \sum_{i\in[g]} P_i$.

→ Going over all $\{D_Y\}_Y$ covers $Div_0(C)$.

• Define $\mathcal{C}_\gamma := \left\{ \sum_{i=1}^{g} P_i - g\cdot\infty \;\middle|\; D \in \mathcal{D}_\gamma \;\&\; \sum_{i\in[g]} P_i := D + (2g-1)\infty - D_\gamma + (f) \right\}$.

▷ $\mathcal{C}_\gamma$ is a quasi-PV, $\forall\gamma$.

▷ $\bigcup_\gamma \mathcal{C}_\gamma = J(C) \cong Cl_0(C)$.

↖ PV ↖ group

• Gluing the open-patches $\{\mathcal{C}_\gamma\}_\gamma$, we make $J(C)$ a variety, and an abelian group.

▷ $\dim J(C) = g$ (as a smooth projective variety).

-ex. For $g=1$ (elliptic curve C), $J(C) \cong C$.

• $(P_1-\infty)+(P_2-\infty) = (P_3-\infty) \Leftrightarrow P_1+P_2+P_3'-3\infty = (\ell)$.

where, $(P_3'-\infty)+(P_3-\infty)=(\ell')$ $\in K^+$

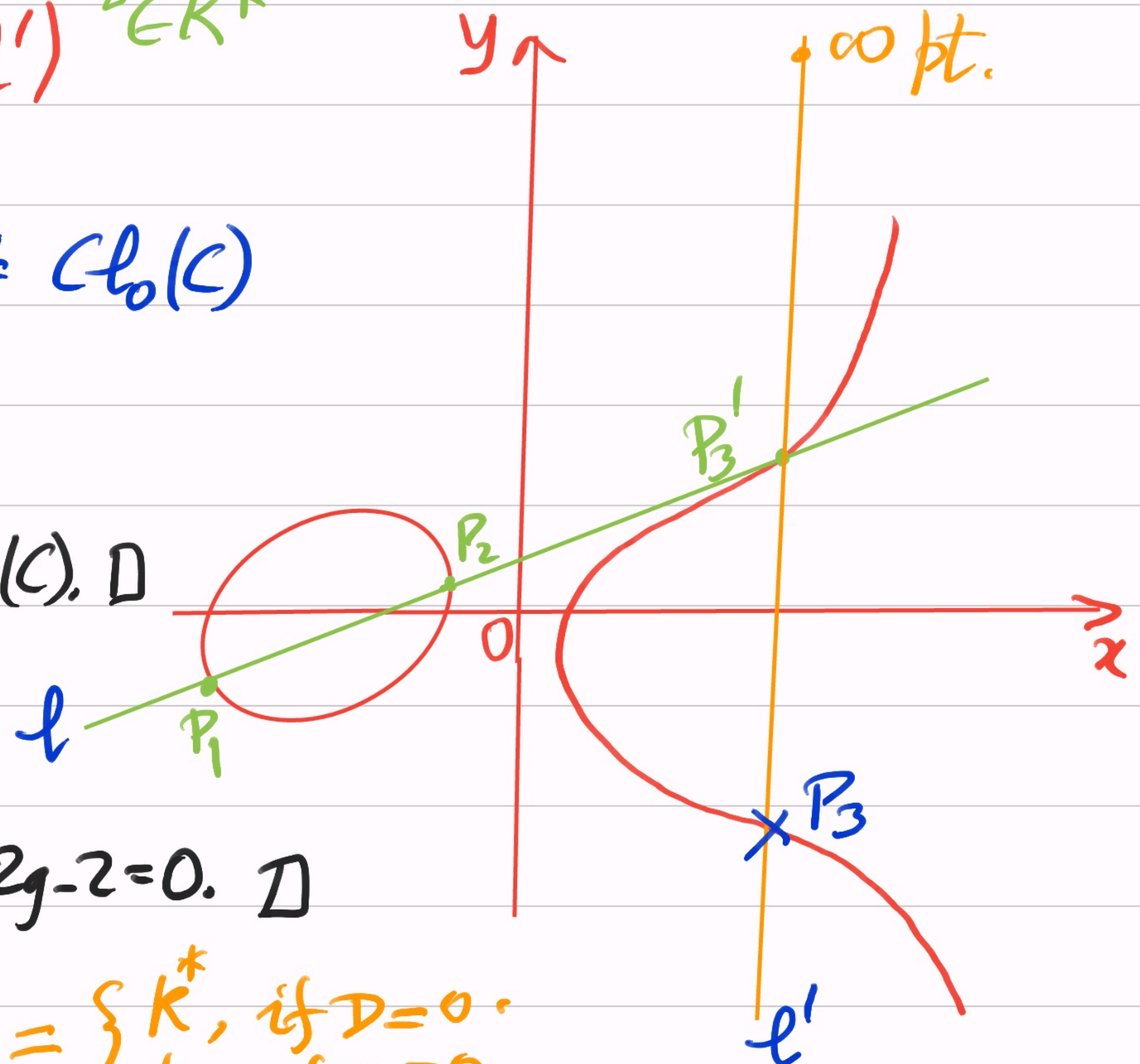
▷ $g(C)=1 \Rightarrow J(C) \cong C \cong Cl_0(C)$
$\cong \{P-\infty \mid P \in C\}$.

Pf: · For $P \neq Q \in C$,
$P-\infty \not\equiv Q-\infty \mod Div_0(C)$. □
[$P-Q=(g) \Rightarrow$ ↯]

▷ $g(C)=1 \Rightarrow W = \infty-\infty = 0$.

Pf: As, $\ell(W)=g=1$ & $d(W)=2g-2=0$. □

▷ $g(C)=1 \Rightarrow \Omega(D) = L(-D) = \begin{cases} K^*, & \text{if } D=0. \\ \phi, & \text{if } D>0. \end{cases}$



- $J(C)$ is a 'junction of many math. areas:
  - It has geometry (high-dim g variety).
  - It has graph structure & $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ as automorphisms.
  - It knows the topology (genus=g) of curve C.
  - It's the class-group of trdeg=1 fn. fields.

- Over $k=\mathbb{F}_p$, $Frob_p : (x,y) \mapsto (x^p, y^p)$ acts on $J(C)$ as a $\mathbb{Z}$-linear map.

Qn: What's the characteristic polynomial of $Frob_p$ on $J(C)$?