since $d f(t_1,\dots,t_n) = \sum_{i=1}^{n} \frac{\partial f}{\partial t_i}(t_1,\dots,t_n) \cdot dt_i$

- $\Omega_{k(t_1,\dots,t_n)/k} = \bigoplus_{i=1}^{n} k(t_1,\dots,t_n)\cdot dt_i$ (vector space of rank n)

(combine last example with $d(f/g) = \frac{g\,df - f\,dg}{g^2}$).

Abbreviate $\Omega_{\bar{k}(C)/\bar{k}} =: \Omega_C$

Ex: $\Omega_{\mathbb{P}^1} = \Omega_{\bar{k}(\mathbb{P}^1)/\bar{k}}$
$= \bar{k}(t)\cdot dt$
where $\bar{k}[\mathbb{A}^1] = \bar{k}[t]$

Prop: ① For any curve C, Ω_C is a $\bar{k}(C)$-vector space of dimension 1. (think through the case $C = \{f = 0\} \subset \mathbb{A}^2$)

② For $x \in \bar{k}(C)\setminus\bar{k}$, $\Omega_C = \bar{k}(C)dx$ if and only if $\bar{k}(C)/\bar{k}(x)$ is separable. (eg, if $\operatorname{char} k = 0$)

The divisor of a differential form.

Aim: Define $\operatorname{div}(\omega) \in \operatorname{Div}(C)$ for $\omega \in \Omega_C$ when C is a nonsingular projective curve.

$$\operatorname{div}(\omega) = \sum_{P \in C} v_P(\omega)\,[P]$$

Fix $\omega \in \Omega_C$.

Let $P \in C$. $\mathcal{O}_{C,P}$ is a DVR. Let $t \in \mathcal{O}_{C,P}$ be a uniformizer. Prop (2): provided $\bar{k}(C)/\bar{k}(t)$ is separable, $\omega = g \cdot dt$ for a unique $g \in \bar{k}(C)$. But t being a uniformizer guarantees $\bar{k}(C)/\bar{k}(t)$ separable (easy: for details, see Silverman II.1.4)

Notation: write $\frac{\omega}{dt} = g$ and define $\forall P \in C$,

$v_P(\omega) = v_P\left(\frac{\omega}{dt}\right)$.

($\omega \in \Omega_C$, $\frac{\omega}{dt} \in \bar{k}(C)$)

Fact: $v_P(\omega) = 0$ for all but finitely many $P \in C$.

Thus $\mathrm{div}(\omega)$ is a well-defined element of $\mathrm{Div}(C)$.

Fact: $f \in \mathcal{O}_{C,P} \Rightarrow \frac{df}{dt} \in \mathcal{O}_{C,P}$ (t a uniformizer at P).

Exercise/reading: think through these facts for plane curves.

Defn (1) C as above. A canonical divisor on C is any $K_C = \mathrm{div}(\omega)$ for $\omega \in \Omega_C \setminus 0$. $\dim\{f \in \bar{k}(C) \mid \mathrm{div}(f) \geq -K_C\}$

(2) The genus of C is $\ell(K_C)$ for any canonical divisor. (2') This equals

$\dim\left(\{\omega \in \Omega_C \mid v_P(\omega) \geq 0 \ \forall P \in C\}\right)$ — call this Ω_C

Why (2): Fix $\omega_0 \in \Omega_C \setminus 0$. Set $K_C = \mathrm{div}(\omega_0)$

$$\Omega_C^{reg} \rightleftarrows L(K_C) = \{f \in \bar{k}(C) \mid \mathrm{div} f \geq -K_C\}$$

$$f \cdot \omega_0 \longleftarrow f$$

$$\omega \longmapsto f \text{ such that } \omega = f \cdot \omega_0$$

(div fω = div f + div ω ≥ 0)

Examples $C = \mathbb{P}^1$ $\Omega_C = \bar{k}(t)dt$. Let $\omega = dt$

Compute $\mathrm{div}(\omega)$. For $P \in \mathbb{A}^1$, $v_P(dt) = v_P(1 \cdot d(t-P))$ (unif at P)

$= v_P(1) = 0$.

For $P = \infty \in \mathbb{P}^1 \setminus \mathbb{A}^1$, a unif. at P is $1/t$

and $v_\infty(dt) = v_\infty(-t^2 \, d(1/t)) = v_\infty(-t^2) = -2$.

Thus $\mathrm{div}(dt) = -2 \cdot [\infty]$

Similarly for any $\omega \in \Omega_{\mathbb{P}^1}$, $\omega = f \cdot dt$ (some f)

$\mathrm{div}(\omega) = \mathrm{div}(f) - 2 \cdot [\infty]$, and $\boxed{\deg(\mathrm{div}(\omega)) = -2}$

(so $\deg(K_C) = -2$). In particular no $\omega \neq 0$ is everywhere regular: $\dim L(K_C) = \dim \Omega_C^{reg} = 0$

(genus of $\mathbb{P}^1$ is zero).

(2) C: the projective nonsingular curve associated to $y^2 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ for $\lambda_1, \lambda_2, \lambda_3 \in \bar{k}$ pairwise distinct and $\mathrm{char} k \neq 2$.

Exercise: $\mathrm{div}\left(\frac{dx}{y}\right) = 0$, and $g(C) = 1$. (PSet 4)

($\frac{dx}{y}$: everywhere regular!)

one rule you might do: at $(\lambda_i, 0) = P_i$, a uniformizer of $\mathcal{O}_{C,P_i}$

$f(x,y) = y^2 - (x-\lambda_1)(x-\lambda_2)(x-\lambda_3) \rightsquigarrow \left(\frac{\partial f}{\partial x}(P_i) \; \frac{\partial f}{\partial y}(P_i)\right) = (\neq 0 \;\; 0)$

tan line is $c(x-\lambda_i)$ for some c. so y is a uniformizer at P_i

$\rightsquigarrow v_{P_i}\left(\frac{dx}{y}\right) = \cdots$

Genus — some topological motivation

(not logically necessary for us)

C nonsingular projective curve / $\mathbb{C}$. We've seen (or defined) $g(C) = \dim \Omega_C^{reg} = \{\omega \in \Omega_{\mathbb{C}(C)/\mathbb{C}} \mid v_P(\omega) \geq 0 \ \forall P \in C\}$.

$C(\mathbb{C}) \hookrightarrow \mathbb{P}^n(\mathbb{C})$ is in a natural way a complex manifold of dimension 1 (Riemann surface) and is compact.

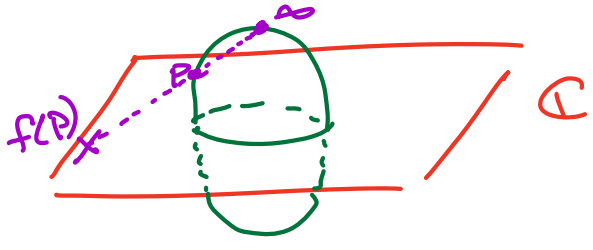
Eg: $C = \mathbb{P}^1$. $\mathbb{P}^1(\mathbb{C})$ = two copies of $\mathbb{C}$, U_0 and U_1, glued along $U_0 - \{0\} \xrightarrow{\sim} U_1 - \{0\}$, $z \longmapsto 1/z$.

In particular, $C(\mathbb{C})$ is a compact orientable real surface, hence is homeomorphic to a many-holed torus:

0 holes 1 hole 2 holes ...

Theorem: $g(C)$ = number of holes of the corresponding real surface (the "genus" of the surface)

Ex:



f: (sphere) $\xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$

$(\infty f)P \longmapsto f(P)$

$\infty \longmapsto \infty$

Fields of definition

• Let C be a nonsingular projective curve over $k \subset \bar{k}$. (Always assume irreducible, and remains so over $\bar{k}$, unless I say otherwise.)

• From now on assume k is perfect. $\bar{k}/k$ is then separable, and $G_k = \mathrm{Gal}(\bar{k}/k)$ is "the" absolute Galois group of k.

↖ field automorphisms of $\bar{k}$ that are the identity on k.

$\rightsquigarrow$ $k(C)$, with k algebraically closed in $k(C)$ (i.e. $\bar{k} \cap k(C) = k$) corresponding to irr. of C.

and $\mathrm{trdeg}_k k(C) = 1$

$\rightsquigarrow$ $\Omega_{k(C)/k}$ a rank 1 $k(C)$-vector space

$\rightsquigarrow$ $K_C = \mathrm{div}(\omega)$ for some $\omega \in \Omega_{k(C)/k} \setminus 0$

, which is a divisor defined over k:

divisors defined over k

Defn: $\mathrm{Div}_k(C) = \{ D \in \mathrm{Div}(C) \ (= \mathrm{Div}_{\bar{k}}(C)) \mid \sigma(D) = D \ \forall \ \sigma \in G_k \}$

Here G_k acts on $\mathrm{Div}(C)$ because:

let $D \in Div(C)$. $D = \sum_{P \in C} c_P \cdot [P]$ $\quad c_P \in \mathbb{Z}$.

Since C is defined over k ($C \hookrightarrow \mathbb{P}^n$ is the zero locus of some homogeneous $F_1, \dots, F_r$ in $k[x_0, \dots, x_n]$; $P = [p_0, \dots, p_n] \in C \iff$

$\forall i$ $F_i(p_0, \dots, p_n) = 0 \overset{\forall i}{\iff} F_i(\sigma(p_0), \dots, \sigma(p_n)) = 0$

$\iff \sigma P := [\sigma(p_0), \dots, \sigma(p_n)] \in C$), G_k acts on C, hence acts on $Div(C)$ via

$$\sigma\left(\sum_P c_P[P]\right) = \sum_P c_P[\sigma(P)].$$

(2) $D \in Div_k(C)$ is not equivalent to $D = \sum c_P[P]$ where $P \in C(k)$ whenever $c_P \neq 0$.

Eg: $C = \mathbb{P}^1$, $k = \mathbb{Q}$ $\rightsquigarrow$ $D = [i, 1] + [-i, 1]$ lies in $Div_{\mathbb{Q}}(\mathbb{P}^1)$.

But $\omega \in \Omega_{k(C)/k}$ does have $\underset{K_C}{div(\omega)} \in Div_k(C)$.

Riemann-Roch over k: For $D \in Div_k(C)$, $L(D) = \{ f \in \bar{k}(C)^\times \mid div(f) \geq -D \}$ has a basis of $f \in k(C)$. (Pf: "Galois descent" for vector spaces – PSet 4).

So when we apply R-R (over $\bar{k}$) with $D \in Div_k(C)$, we get information about

functions in $L(D) \cap k(C)$.

At last: elliptic curves

Defn: An elliptic curve over k is a pair $(E, \mathcal{O})$ where
- E is a nonsingular projective curve over k with genus 1
- $\mathcal{O} \in E(k)$.

Example: Take $E \hookrightarrow \mathbb{P}^2$ given by $\{[X,Y,Z] \in \mathbb{P}^2 : Y^2Z = X^3 + aXZ^2 + bZ^3\}$ where $a, b \in k$, and (to ensure nonsingularity) $\mathrm{char} k \neq 2$ and $t^3 + at + b \in k[t]$ having distinct roots. Earlier-referenced exercise (Set 4) shows $g(E) = 1$. Let $\mathcal{O} = [0,1,0]$. Then $(E, \mathcal{O})$ is an elliptic curve over k.

Non-example: Take $C \hookrightarrow \mathbb{P}^3$ to be the nonsingular projective curve over $\mathbb{Q}$ we associated to the affine curve $\{w^2 = 2 - 2pz^4\} \subset \mathbb{A}^2$ where $p \equiv 1 \bmod 8$ and $\left(\frac{2}{p}\right)_4 \neq 1$. Then (PSet 4) $g(C) = 1$, but we've seen $C(\mathbb{Q}) = \emptyset$, so C can't be "upgraded" to an elliptic curve over $\mathbb{Q}$.

But $\forall \ell$, $C(\mathbb{Q}_\ell) \neq \emptyset$, and so for any choice of $P \in C(\mathbb{Q}_\ell)$, (C, P) is an elliptic curve over $\mathbb{Q}_\ell$.

We'll next show any elliptic curve is given by a particularly simple cubic equation in $\mathbb{P}^2$.

We'll need a few facts about maps of algebraic curves. (See the review session!)

Recall: C nonsingular projective curve over k.

- Functions $f_0, \dots, f_n \in k(C)$ (not all 0) define a rational map (over k)

$$\phi : C \dashrightarrow \mathbb{P}^n \quad \text{given by}$$

$$P \longmapsto [f_0(P), \dots, f_n(P)] \text{ wherever}$$

this makes sense.

- ϕ is regular at $P \in C$ if $\exists\, g \in \bar{k}(C)$: all $gf_i \in \mathcal{O}_{C,P}$ and not all $gf_i \in m_{C,P}$ ($gf_i(P)$ not all zero)
- ϕ is a morphism if it is regular everywhere
- For a projective subvariety $Y \subset \mathbb{P}^n$, ϕ is a morphism $C \to Y$ if moreover $\phi(C) \subset Y$.

Fact 1 Any $\phi : C \dashrightarrow \mathbb{P}^n$ is a morphism

(use: $\forall P$, $\mathcal{O}_{C,P}$ is a DVR.)

exercise (provable using stuff we've covered)

Fact 2 Let Y also be a projective curve. Any morphism $C \to Y$ is either constant or surjective

Any non-constant $C \xrightarrow{\phi} Y$ induces an inclusion $\phi^* : k(Y) \hookrightarrow k(C)$ making $k(C)/k(Y)$ a finite

extension. $\deg(\phi) := [k(C):k(Y)]$.

Key example: $f \in k(C)\setminus k$ gives

$[f,1] = \phi : C \longrightarrow \mathbb{P}^1$ of degree

$[k(C):k(f)]$.

Fact 3 For any non-constant morphism $\phi: C \to Y$ of nonsingular projective curves, $\deg(\phi)$ can be calculated as follows:

for any $y \in Y$, let $t_y \in \mathcal{O}_{C,y}$ ($\subset k(Y)$) be a uniformizer.

$\phi^*(t_y) \in k(C)$ vanishes at all $P \in \phi^{-1}(y)$.

Let

$e_\phi(P) = v_P(\phi^*(t_y))$ be the ramification index of ϕ at P. Then

$$\deg(\phi) = \sum_{P \in \phi^{-1}(y)} e_\phi(P).$$

$B \subset L$; $\{\beta_i\} = "\phi^{-1}(Q)"$, $"e_i = e_\phi(\beta_i)"$

$\mathbb{Z} \subset G$

$pB = \prod \beta_i^{e_i}$, $|B/pB| = |\prod B/\beta_i^{e_i}| = \prod |B/\beta_i|^{e_i}$

Example: $f \in k(C)\setminus k$, $[f,1] = \phi : C \longrightarrow \mathbb{P}^1$

Let $y = \infty$ (or 0); then

$$\deg(\phi) = -\sum_{\substack{\text{poles } P \\ \text{of } f}} v_P(f)$$

$\leftarrow P : \frac{1}{f}(P) = 0$

Lorenzini, *An Invitation to Arithmetic Geometry*

$$= \sum_{\substack{\text{zeroes} \\ P \text{ of } f}} v_P(f)$$

$\leftarrow P : f(P) = 0$ (i.e. $f \in m_{C,P} \subset \mathcal{O}_{C,P}$)

Fact 4: For a morphism $C \xrightarrow{\phi} Y$ of nonsingular projective curves, ϕ is an isomorphism ($\exists$ a morphism $\psi: C \to Y$: $\phi \circ \psi = id$, $\psi \circ \phi = id$) iff $\deg(\phi) = 1$.