Branched covering spaces of elliptic curves

A.S.I. Anema

25 November 2011

Outline

- Let k be an algebraically closed field.

Equivalent categories

Geometry	Algebra
non-singular projective curve C	function field $k(C)$, i.e. finite extensions of $k(X)$
surjective morphism $C \to D$	inclusion $k(D) \to k(C)$ fixing k
point P on C	discrete valuation v_P of $k(C)$

- Ramification index of $\phi : C \to D$ at P on C is

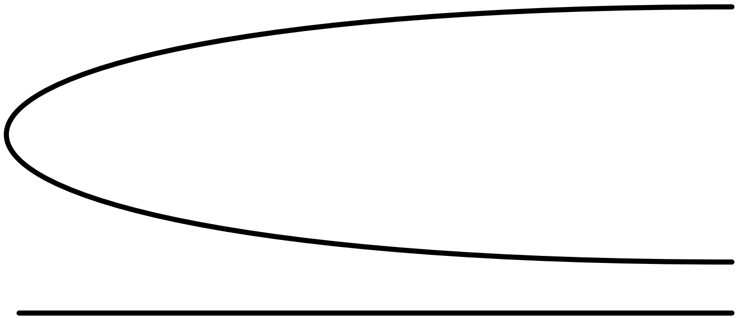
$$e_\phi(P) := v_P\left(t_{\phi(P)}\right).$$

- A branched covering space is a surjective morphism of curves.

Example

Consider $\phi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ defined as $\phi(x) = x^2$. This induces $k(Y) \to k(X)$ with $Y \mapsto X^2$. Now

$$e_\phi(0) = v_0(Y) = v_0\left(X^2\right) = 2.$$

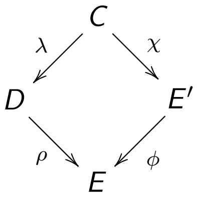


- Let k be an algebraically closed field of char $k \neq 2, 3$.
- Consider the elliptic curve

$$E : y^2 = x^3 - 2ax^2 + \left(a^2 - 4b\right) x$$

over k with $a, b \in k$ such that $b \neq 0$ and $a^2 \neq 4b$.

- The idea is as follows



- Consider the elliptic curve over k

$$E' : \eta^2 = \xi^3 + a\xi^2 + b\xi.$$

- Let $\phi : E' \to E$ be an isogeny of degree two such that

$$\ker \phi = \left\{ O', T' \right\},$$

where $T' = (0, 0) \in E'$ is a point of order two.

- The coordinate function ξ has divisor

$$\operatorname{div} \xi = 2T' - 2O'.$$

- Let C be the curve corresponding to the splitting field of

$$F = X^3 - \xi \in k\left(E'\right)[X]$$

and $\chi : C \to E'$ the morphism corresponding to the inclusion.

- The morphism $\chi : C \to E'$ branches above O' and T' with ramification index three. It does not branch elsewhere.
- Extension $k(C)$ of $k(E)$ is Galois with

$$\mathrm{Gal}\left(k(C)/k(E)\right) \cong S_3.$$

- Consider $H = \{\mathrm{id}, \tau\} \subset \mathrm{Gal}\left(k(C)/k(E)\right)$.
- Let D be the curve with function field $k(C)^H$.

Theorem

The curve D is given by the equation

$$\beta^2 = \left(\alpha^3 - 3c\alpha + a\right)\left(\alpha^2 - 4c\right)$$

and has genus two.

Theorem

The inclusion $k\left(E\right) \to k\left(D\right)$ corresponds to a morphism $\rho : D \to E$ given by

$$\left(\alpha, \beta\right) \longmapsto \left(\alpha^3 - 3c\alpha + a, -\beta\left(\alpha^2 - c\right)\right)$$

and ramifies only at infinity on D. At that point the ramification index is three.

- Let k be an algebraically closed field of char $k = 0$.
- Will construct branched covering spaces of the elliptic curve

$$C : 4a^3 + 27b^2 = 1.$$

- Define $K = k(C)$.
- Consider the elliptic curve over $\bar{K}$

$$E : y^2 = x^3 + ax + b.$$

- Let p be prime. Define $L_p = K(E[p])$.
- The field L_p corresponds to a curve D_p.
- The inclusion $K \to L_p$ induces a morphism $\psi_p : D_p \to C$.

Theorem

Let $P \in D_p$. If $\psi_p(P) \neq O_C$, then ψ_p is unramified at P.

Theorem

Let $P \in D_p$ such that $\psi_p(P) = O_C$. Then

- *ψ_2 is unramified at P,*
- *ψ_3 is ramified at P with $e_{\psi_3}(P) = 2$*
- *and ψ_p is ramified at P for $p > 3$ with $e_{\psi_p}(P) = 2p$*

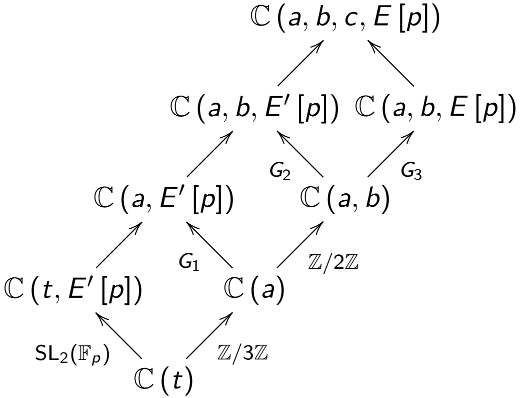
Theorem

If $k = \mathbb{C}$ and $p > 3$, then $\mathrm{Gal}(L_p/K) \cong SL_2(\mathbb{F}_p)$.

- If E' is defined over $\mathbb{C}(t)$ and $j(E') = t$, then

$$\mathrm{Gal}\left(\mathbb{C}\left(t, E'[p]\right) / \mathbb{C}(t)\right) \cong \mathrm{SL}_2\left(\mathbb{F}_p\right).$$

- Let E' be defined over $\mathbb{C}(t)$ such that $t = j(E) \sim a^3$. Then



- Let $P \in D_p$ be a point. Denote $Q = \psi_p(P)$.
- Complete the discrete valuation rings R_P and R_Q. Then

$$\hat{R}_P \cong k[[t_P]] \quad \text{and} \quad \hat{R}_Q \cong k[[t_Q]]$$

with t_P and t_Q uniformizers at P and Q.

- Take the quotient field to obtain $\hat{K}_Q$ and $\hat{L}_{p,P}$.
- The inclusion $R_Q \to R_P$ extends to an inclusion $\hat{K}_Q \to \hat{L}_{p,P}$.

Theorem

In this case $\mathrm{Gal}\left(\hat{L}_{p,P}/\hat{K}_Q\right) \cong \mathbb{Z}/n\mathbb{Z}$ *with* $n = e_{\psi_p}(P)$.

- If $v_P(a) \geq 0$ and $v_P(b) \geq 0$, then the reduced curve of E is

$$\tilde{E} : \tilde{y}^2 = \tilde{x}^3 + a(P)\tilde{x} + b(P).$$

Theorem

If the reduced curve $\tilde{E}$ is non-singular, then there exists a Galois equivariant group homomorphism $\pi : E\left(\hat{L}_{p,P}\right) \to \tilde{E}(k)$. Moreover π restricted to the torsion subgroup is injective.

- If $Q = \psi_p(P) \neq O_C$ and $\sigma \in \mathrm{Gal}\left(\hat{L}_{p,P}/\hat{K}_Q\right)$, then

$$\pi \circ \sigma(R) = \tilde{\sigma} \circ \pi(R) = \pi(R)$$

for all $R \in E[p]$. Hence $\sigma = \mathrm{id}$.

- Let $P \in D_p$ be such that $\psi_p(P) = O_C$.
- Define $t = \frac{a}{b}$ and $u = \frac{a^3}{b^2}$. Notice that t uniformizer at O_C.

$$E : y^2 = x^3 + ax + b = x^3 + ut^{-2}x + ut^{-3}.$$

- Let M be the splitting field of $X^2 - t$ over $\hat{L}_{p,P}$ and $s^2 = t$.
- Change of coordinates $\xi = s^2 x, \eta = s^3 y$ gives

$$E : \eta^2 = \xi^3 + u\xi + u$$

with $\Delta(E) = t^6$ and $j(E) = 1728 \cdot 4\frac{u^3}{t^6}$.
- Via the Tate curve for some $q \in M$ with $v_M(q) = -v_M(j(E))$

$$E\left(\hat{L}_{p,P}\right)[p] \subset E(M)[p] \cong E_q(M)[p] \cong \left(M^*/q^{\mathbb{Z}}\right)[p].$$

- If $z^p = q$ for some $z \in M^*$, then $p \cdot v_M(z) = 6v_M(t)$.

- Let $k = \mathbb{C}$ and $p > 3$.
- Define $L_{p,x} = K\left(x\left(E\left[p\right]\right)\right)$.
- Consider the curve $D_{p,x}$ corresponding to $L_{p,x}$.
- The inclusion $K \to L_{p,x}$ gives $\psi_{p,x} : D_{p,x} \to C$.

Theorem

Let $P \in D_{p,x}$. If $\psi_{p,x}\left(P\right) = O_C$, then $\psi_{p,x}$ is ramified at P with ramification index p, else $\psi_{p,x}$ is unramified at P.

Corollary

The genus of $D_{p,x}$ is

$$g_{D_{p,x}} = \frac{1}{4}\left(p^2 - 1\right)\left(p - 1\right) + 1.$$

- Branched covering spaces of a elliptic curve with a single branch point exist,
  - but not with two sheets.
- Saw explicit example with three sheets.
- It is possible to construct a family of such spaces for

$$C : 4a^3 + 27b^2 = 1$$

and derive the

- Galois group,
- ramification indices,
- genus.