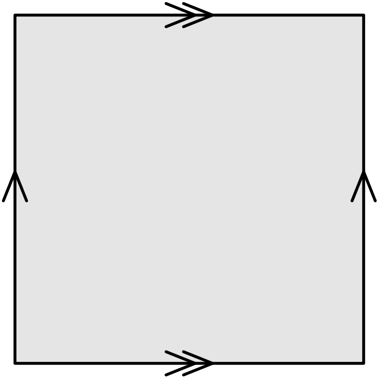
Covering spaces of an elliptic curve that ramify in precisely one point

Ane Anema

6 December 2012

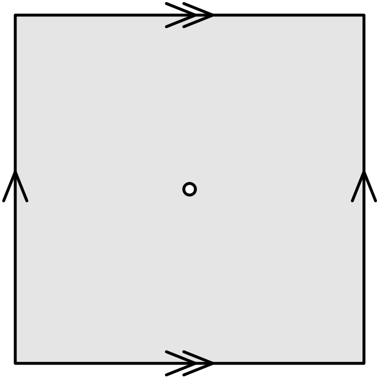
Outline

Torus T



$\pi(T) \cong \mathbb{Z} \times \mathbb{Z}$

Punctured torus S



$\pi(S) \cong \mathbb{Z} * \mathbb{Z}$

- Let $\tilde{S}$ and $\tilde{T}$ be the universal covering spaces of S and T.

Theorem

Let $H \subset \pi(S)$ be a subgroup and $Y \to T$ be the analytic continuation of $\tilde{S}/H \to S$. Then

$$Y \to T \text{ unramified} \iff H \text{ normal}, \ \pi(S)/H \text{ abelian}.$$

- A covering space of the torus is normal and its group of deck transformations is abelian.
- Consider

$$\begin{tikzcd} \tilde{S} \arrow[r] & \tilde{S}/[\pi(S),\pi(S)] \arrow[r] \arrow[d] & S \arrow[d] \\ & \tilde{T} \arrow[r] & T \end{tikzcd}$$

- Let a, b be generators of $\pi(S)$.
- Define $\phi : \langle a, b \rangle \to S_3$ as

$$a \mapsto (12) \quad \text{and} \quad b \mapsto (23)\,.$$

- Consider $X \to S$ corresponding to $H = \ker \phi$, which
    - has six sheets,
    - can be analytically continued to $Y \to T$, and
    - has $\pi(S)/H \cong S_3$.
- Let $X' \to S$ correspond to $H' = \phi^{-1}(\langle (12) \rangle)$, then
    - has three sheets,
    - can be analytically continued to $Y' \to T$, and
    - H' is not normal.

- 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

$$\begin{tikzcd} & C \arrow[dl, "\lambda"'] \arrow[dr, "\chi"] & \\ D \arrow[dr, "\rho"'] & & E' \arrow[dl, "\phi"] \\ & E & \end{tikzcd}$$

- 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.
- Write C for the curve that corresponds to the splitting field of

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

  and $\chi : C \to E'$ for the morphism induced by $k\left(E'\right) \subset k\left(C\right)$.

- Since the coordinate function ξ has

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

then $\chi : C \to E'$ branches only above O' and T', where it has ramification index three.

- Choose the isogeny $\phi : E' \to E$ as

$$(\xi, \eta) \longmapsto \left(\frac{\eta^2}{\xi^2}, \frac{\eta\left(b - \xi^2\right)}{\xi^2} \right).$$

- So $k(E') = k(E)(\xi)$ and $k(C) = k(E)(s)$, where $s^3 = \xi$.
- Extension $k(C)$ of $k(E)$ is Galois with

$$\operatorname{Gal}(k(C)/k(E)) \cong S_3,$$

because s has minimum polynomial $X^6 + (a - x)X^3 + b$

$$(X - s)\left(X - s^2\right)\left(X - s^3\right)\left(X - \frac{\sqrt[3]{b}}{s}\right)\left(X - \frac{\sqrt[3]{b}}{s^2}\right)\left(X - \frac{\sqrt[3]{b}}{s^3}\right)$$

- Let D be the curve with function field $k\left(C\right)^{\{\mathrm{id},\tau\}}$.

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.

- Consider the following elliptic curve over $\mathbb{C}$

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

  with unit element O.
- Also consider the elliptic curve over $\mathbb{C}(B)$ defined by

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

- Let ℓ be a prime number.
- Since $\mathbb{C}(B)(E[\ell])$ is a finite extension of $\mathbb{C}(B)$, then it is a function field of a curve C_ℓ over $\mathbb{C}$.
- The inclusion of function fields induces a morphism

$$\pi_\ell : C_\ell \to B.$$

Theorem

The morphism $\pi_\ell : C_\ell \to B$ is Galois.

Theorem

Let $P \in C_\ell$. If $\pi_\ell(P) \neq O$, then π_ℓ is unramified at P.

Theorem

Let $P \in C_\ell$. If $\pi_\ell(P) = O$, then

- *π_2 is unramified at P,*
- *π_3 is ramified at P with $e_{\pi_3}(P) = 2$,*
- *π_ℓ is ramified at P for $\ell > 3$ with $e_{\pi_\ell}(P) = 2\ell$.*

- Notice that $G_\ell = \mathrm{Gal}\left(\mathbb{C}(C_\ell)/\mathbb{C}(B)\right)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Case $P \in C_\ell$ and $\pi_\ell(P) = Q \neq O$.

- Notice that $E : y^2 = x^3 + ax + b$ over $\mathbb{C}(C_\ell)$ is minimal at P.
- The extension $\widehat{\mathbb{C}(C_\ell)}_P / \widehat{\mathbb{C}(B)}_Q$ is also Galois.
- The $e_{\pi_\ell}(P)$ is equal to the degree of this extension.
- The reduction map restricts to a injective morphism

$$\psi : E\left(\widehat{\mathbb{C}(C_\ell)}_P\right)[\ell] \to \overline{E}_{\text{ns}}(\mathbb{C}),$$

  which is Galois equivariant.
- If $\tau \in \mathrm{Gal}\left(\widehat{\mathbb{C}(C_\ell)}_P / \widehat{\mathbb{C}(B)}_Q\right)$, then for all $S \in E[\ell]$

$$\psi \circ \tau(S) = \tilde{\tau} \circ \psi(S) = \psi(S),$$

  that is $\tau(S) = S$, hence $\tau = \mathrm{id}$.
- Hence π_ℓ is unramified at P.

Case $P \in C_\ell$ and $\pi_\ell(P) = O$ and $\ell = 2$.

- The polynomial $x^3 + ax + b$ is irreducible over $\mathbb{C}(B)$.
  - Suppose reducible, then it has a zero in $\mathbb{C}(B)$ with a pole of order one at O and regular elsewhere.
- The discriminant is a square, so the splitting field has degree at most three.
- Since the Galois group $G_2 \cong \mathbb{Z}/3\mathbb{Z}$ is abelian, then

$$\pi_2 : C_\ell \to B$$

  is unramified at P.
- The curve C_2 again has genus one.

Case $P \in C_\ell$ and $\pi_\ell(P) = O$ and $\ell \geq 3$.

- Let π be an uniformizer at O, then $E : y'^2 = x'^3 + \pi^4 ax' + \pi^6 b$ over $\mathbb{C}(B)$ is minimal at O.
- Notice that E over $\mathbb{C}(B)$ has additive reduction at O.
- Suppose that E over $\mathbb{C}(C_\ell)$ also has additive reduction at P, then define $K = \widehat{\mathbb{C}(C_\ell)}_P$ and consider

$$0 \to E_0(K) \to E(K) \to E(K)/E_0(K) \to 0$$

and the reduction map $E_0(K) \to \overline{E}(\mathbb{C}) \cong (\mathbb{C}, +)$, so that

$$\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \cong E[\ell] \hookrightarrow E(K)/E_0(K),$$

but this is impossible for $l \geq 3$. Therefore E over $\mathbb{C}(C_\ell)$ has multiplicative reduction at P.
- Hence π_ℓ is ramified at P.

Case $P \in C_\ell$ and $\pi_\ell(P) = O$ and $\ell = 3$.

- The 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ contains G_ℓ, and is isomorphic to the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$.
- Since π_3 is ramified, then G_ℓ is non-abelian, hence G_ℓ is the 2-Sylow subgroup.
- Let $H = \{\pm 1\}$ and consider

$$\mathbb{C}(B) \longrightarrow \mathbb{C}(C_\ell)^H \longrightarrow \mathbb{C}(C_\ell).$$

- The $e_{\pi_3}(P) = 2$, because G_ℓ / H is abelian.
- Hence the genus of C_ℓ is three.

Case $P \in C_\ell$ and $\pi_\ell(P) = O$ and $\ell > 3$.

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

$$\mathrm{Gal}\left(\mathbb{C}(t)(E'[\ell])/\mathbb{C}(t)\right) \cong \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

- Define
$$E' : y^2 = x^3 - \frac{27t}{t-1728}x - \frac{54t}{t-1728}$$
over $\mathbb{C}(t)$. It has $j(E') = t$.
- Let $t = j(E) = 6912a^3$, then

$$-\frac{27t}{t-1728} = \left(\frac{2a}{b}\right)^2 a \quad \text{and} \quad -\frac{54t}{t-1728} = \left(\frac{2a}{b}\right)^3 b.$$

- Thus E and E' are isomorphic over $\mathbb{C}(a, b, c)$ for $c^2 = \frac{2a}{b}$.
- Hence $\mathbb{C}(a, b, c, E[\ell]) = \mathbb{C}(a, b, c, E'[\ell])$.

Proofs

$$
\begin{tikzcd}
 & & & \mathbb{C}\left(a,b,c,E\left[\ell\right]\right) & \\
 & & \mathbb{C}\left(a,b,E'\left[\ell\right]\right) \arrow[ur] & & \mathbb{C}\left(a,b,E\left[\ell\right]\right) \arrow[ul] \\
 & \mathbb{C}\left(a,E'\left[\ell\right]\right) \arrow[ur] & & \mathbb{C}\left(a,b\right) \arrow[ul, "G'"'] \arrow[ur, "G_\ell"'] & \\
\mathbb{C}\left(t,E'\left[\ell\right]\right) \arrow[ur] & & \mathbb{C}\left(a\right) \arrow[ul, "G"'] \arrow[ur, "\mathbb{Z}/2\mathbb{Z}"'] & & \\
 & \mathbb{C}\left(t\right) \arrow[ul, "\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})"] \arrow[ur, "\mathbb{Z}/3\mathbb{Z}"'] & & &
\end{tikzcd}
$$

- Since $\mathrm{SL}_2\left(\mathbb{Z}/\ell\mathbb{Z}\right)$ has no normal subgroups of index 2 and 3, then

$$G_\ell \cong \mathrm{SL}_2\left(\mathbb{Z}/\ell\mathbb{Z}\right).$$

- Define an uniformizer $\pi = \frac{2a}{b}$ at O.
- Consider $E : y^2 = x^3 + ax + b$ over $\mathbb{C}((\pi))$.
- Compute

$$a = \pi^{-2}\left(-27 + b^{-2}\right) \qquad \text{and} \qquad b = \pi^{-3}\left(-54 + 2b^{-3}\right)$$

- The curve E is equivalent to

$$E : y^2 = x^3 + \left(-27 + b^{-2}\right)x + \left(-54 + 2b^{-3}\right)$$

over $\mathbb{C}((c))$ with $c^2 = \frac{2a}{b}$. Note that $\Delta = c^{12}$.

- Indeed E has multiplicative reduction modulo c

$$\overline{E} : y^2 = x^3 - 27x - 54 = (x+3)^2(x-6).$$

- Use the theory of the Tate curve.
- There is a $q \in \mathbb{C}((c))$ such that for every finite $L/\mathbb{C}((c))$ there exists a Galois equivariant isomorphism

$$L^*/q^{\mathbb{Z}} \to E(L).$$

  Moreover $v(q) = v(\Delta) = 12$.
- Hence $\mathbb{C}((c))(E[\ell]) = \mathbb{C}((c))\left(\sqrt[\ell]{q}\right)$.
- Consider

$$\begin{tikzcd} & \mathbb{C}((c))(E[\ell]) & \\ \mathbb{C}((\pi))(E[\ell]) \arrow[ur] & & \mathbb{C}((c)) \arrow[ul] \\ & \mathbb{C}((\pi)) \arrow[ul] \arrow[ur] & \end{tikzcd}$$

- In fact $\mathbb{C}((\pi))(E[\ell]) = \mathbb{C}((c))(E[\ell])$, because
  - Recall E has multiplicative reduction over $\mathbb{C}((\pi))(E[\ell])$.
  - The coefficient a transforms as au^4 for some u.
  - Multiplicative reduction requires

$$0 = v\left(u^4 a\right) = 4v(u) - v(a) = 4v(u) - 2e$$

    with e the ramification index. Therefore e is be even.
  - Hence $c \in \mathbb{C}((\pi))(E[\ell])$.
- The ramification index of π_ℓ at P is 2ℓ.
- Compute the genus

$$g(C_\ell) = 1 + \frac{\left(\ell^2 - 1\right)(2\ell - 1)}{4}.$$

Let $\ell > 3$. Adjoin all x-coordinates of points of order ℓ to $\mathbb{C}(B)$.

- Denote this curve by D_ℓ, then

$$C_\ell \longrightarrow D_\ell \longrightarrow B.$$

- Notice that $\mathbb{C}(D_\ell) = \mathbb{C}(C_\ell)^H$ for $H = \{\pm 1\}$.
- Let $Q \in D_\ell$ be a point above O.
- The ramification index of $D_\ell \to B$ at Q is ℓ, because
  - it is either ℓ or 2ℓ, and
  - there is no cyclic subgroup of order 2ℓ in $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$.
- So the genus of D_ℓ is

$$g(D_\ell) = 1 + \frac{(\ell^2 - 1)(\ell - 1)}{4}.$$

Let $\ell > 3$. Adjoin the x, y-coordinates of one point of order ℓ.

- In this case the curve has
  - $\frac{\ell-1}{2}$ points above O with ramification index 2, and
  - $\frac{\ell-1}{2}$ points above O with ramification index 2ℓ.
- The curve has genus

$$1 + \frac{\ell(\ell-1)}{2}.$$

Let $\ell > 3$. Adjoin the x-coordinate of one point of order ℓ.

- This curve has
  - $\frac{\ell-1}{2}$ unramified points above O, and
  - $\frac{\ell-1}{2}$ points above O with ramification index ℓ.
- So the genus is

$$1 + \frac{(\ell-1)^2}{4}.$$

- Using algebraic topology determined a condition on when a branched covering space of the torus is ramified or not.
- Given examples of ramified branched covering spaces of the torus via topology, and their algebraic analoges.
- Constructed a family of branched covering spaces of $4a^3 + 27b^2 = 1$ and computed the Galois group, the ramification indices and the genus.