On the Fundamental Group of an Elliptic Curve

Marie-Andrée B.Langlois

University of Calgary

December, 2013

Motivation

- We aimed at getting a better understanding of isogenies of elliptic curves, from an algebraic geometry perspective.
- We were motivated mismatch of results while implementing 2 different algorithms that would find the sizes of isogeny classes of elliptic curves over finite field.

Objectives

This presentation is about the homotopy exact sequence for the fundamental group an elliptic curve E over a finite field $\mathbb{F}_q$

$$1 \longrightarrow \pi_1^{\text{et}}(\overline{E}, \overline{\mathcal{O}}_E) \longrightarrow \pi_1^{\text{et}}(E, \overline{\mathcal{O}}_E) \overset{\mathcal{O}_{\overline{E}}}{\underset{\cdots\cdots}{\longleftarrow}} \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow 1$$

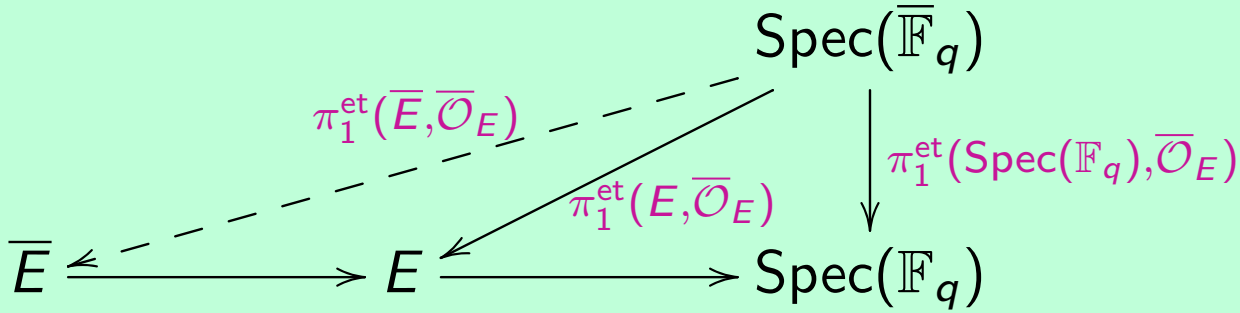
and the relation between $\pi_1^{\text{et}}(E, \overline{\mathcal{O}}_E)$ and the Tate module $T_\ell(E)$, for ℓ prime to q.

Elliptic Curves

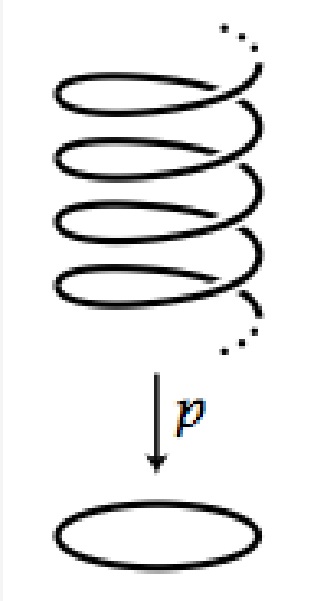
The homotopy exact sequence, and its splitting, comes from the data of an elliptic curve E defined over $\mathbb{F}_q$, where $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$, together with the choice of an geometric point $\overline{\mathcal{O}}_E$.

Recall that for a scheme X defined over K, a geometric point is a morphism from $\mathrm{Spec}(\overline{K})$ to X.

In pink are the fundamental groups that are induced by the given maps:



Topological Fundamental Group



The fundamental group $\pi_1(X, x)$ in topology describes homotopy classes of loops.

Over $\mathbb{C}$, every elliptic curve is just $S^1 \times S^1$, topologically.

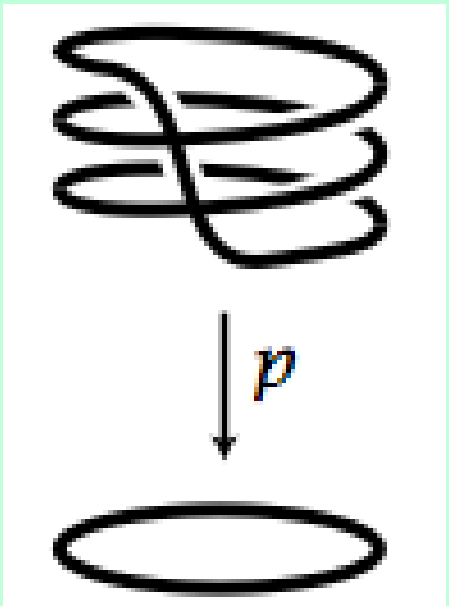
Since $\pi_1(S^1) \cong \mathbb{Z}$, by Van Kampen's theorem $\pi_1(E_{\mathbb{C}}) \cong \mathbb{Z} \times \mathbb{Z}$.

Grothendieck Fundamental Group

Over a finite field we must use the analogue from algebraic geometry: Grothendieck's fundamental group and things are quite different:

$$\pi_1^{\text{et}}(X, \overline{x}) := \varprojlim_{Y, \overline{y}} \text{Aut}_X(Y),$$

for any connected scheme X with geometric point $\overline{x}$, with limit taken over finite Galois covers $f : Y \to X$ and $\overline{y} \mapsto \overline{x}$. ($f$ is Galois if for any $x \in X$, $\text{Aut}(f)$ acts transitively on $f^{-1}(x)$.)



In the figure we see a topological cover, p, of S^1 with covering group $\mathbb{Z}/3\mathbb{Z}$.

Grothendieck Fundamental Group

The algebraic equivalent of $\pi_1(S^1)$ is through coverings of the multiplicative group $\mathbb{G}_{m,\overline{\mathbb{F}}_q}$; the étale covers are maps $z \to z^n$ with covering group $\mu_n(\overline{\mathbb{F}}_q)$ of n-th roots of unity in $\overline{\mathbb{F}}_q$. Then

$$\pi_1^{\text{et}}(\mathbb{G}_{m,\overline{\mathbb{F}}_q}) \cong \varprojlim_{n\in\mathbb{N}^\times} \mu_n \cong \varprojlim_{n\in\mathbb{N}^\times} \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}.$$

Over finite fields we have $\pi_1^{\text{et}}(G_{m,\mathbb{F}_q}) \cong \hat{\mathbb{Z}}(1)$, where $\hat{\mathbb{Z}}(1)$, called the Tate twist, is the Prüfer group equipped with an action of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Galois Group

Recall that the exact sequence uses the Galois group and:

$$\begin{aligned}\mathrm{Gal}(\overline{\mathbb{F}}_q, \mathbb{F}_q) &= \varprojlim_{i\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q) \\ &\cong \pi_1^{\mathrm{et}}(\mathrm{Spec}(\mathbb{F}_q), \mathrm{Spec}(\overline{\mathbb{F}}_q)) \\ &\cong \hat{\mathbb{Z}}.\end{aligned}$$

This topological group is generated by the Frobenius automorphism, $\mathrm{Fr}_q : x \mapsto x^q$.

Tate Module

The Tate module for E is $T_\ell(E) := \varprojlim_{n\in\mathbb{N}} \overline{E}[\ell^n] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and carries an action of $\mathrm{Gal}(\overline{\mathbb{F}}_q, \mathbb{F}_q)$. Note that $\mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. This gives an ℓ-adic Galois representation:

$$\begin{aligned} \rho_E \colon \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) &\to \mathrm{GL}_2(\mathbb{Q}_\ell) \\ \mathrm{Fr}_q &\mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \end{aligned}$$

The characteristic polynomial of $\rho_E(\mathrm{Fr}_q)$ is

$$\lambda^2 - a_q(E)\lambda + q = (\lambda - \alpha)(\lambda - \beta),$$

where $a_q(E) = q + 1 - \#E(\mathbb{F}_q)$ and $|\alpha| = q^{1/2}$ and $|\beta| = q^{1/2}$.

Tate Module

Example: If $E: y^2 = x^3 + 1$ over $\mathbb{F}_{49}$ then $\#E(\mathbb{F}_{49}) = 48$ so the characteristic polynomial of $\rho_E(\mathrm{Fr}_{49})$ is $\lambda^2 - 2\lambda + 49$.

$$\mathrm{Fr}_{49} \mapsto \begin{bmatrix} 0 & 1 \\ -49 & 2 \end{bmatrix}.$$

The Tate module relates to the fundamental group in the following way:

$$T_\ell(E) \cong \pi_1^{\mathrm{et}}(E, \overline{\mathcal{O}}_E)_\ell := \varprojlim_{\ell^n\text{-isogenies}} \mathrm{Aut}_E(Y).$$

From local to global

From an elliptic curve E over $\mathbb{F}_q$ we can build an elliptic over a number field K.

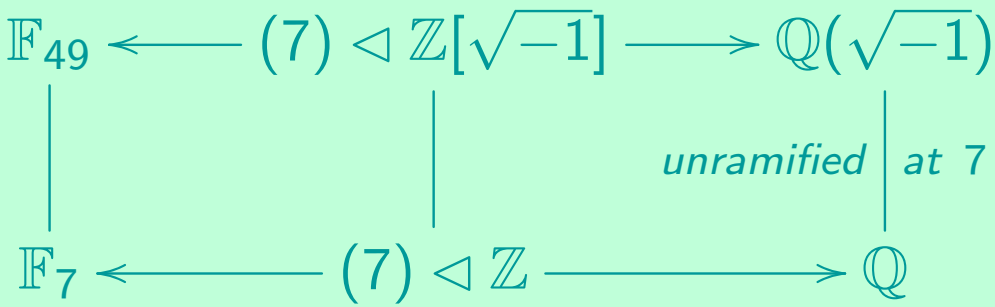
Illustrated with the example $E: y^2 = x^3 + 1$ over $\mathbb{F}_{49}$.

We need to do the following:

(1) Find a number field K satisfying

$$\begin{array}{ccccc} \mathbb{F}_q & \longleftarrow & \mathfrak{p} \lhd \mathcal{O}_K & \longrightarrow & K \\ | & & | & & | \\ & & & \text{unramified} & \text{at } p \\ | & & | & & | \\ \mathbb{F}_p & \longleftarrow & p \lhd \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

From local to global



(2) Find $X/\mathcal{O}_K$ smooth such that:

(i) $X_{\mathbb{F}_q}$ (the special fibre of X at p) is E
(ii) X_K (the generic fibre of X) is an elliptic curve over K
(ii) X is a Néron model for X_K.

Take $y^2 = x^3 + 1$ over $\mathbb{Z}[\sqrt{-1}]$. Key: the group morphisms extended to $\mathbb{Z}[\sqrt{-1}]$. This is a Néron model for $y^2 = x^3 + 1$ over $\mathbb{Q}(\sqrt{-1})$.

From local to global

If X is an abelian projective group scheme over $\mathcal{O}_K$ then it is a Néron model for X_K. This means X is equipped with morphisms:

(a) $m\colon X \times X \to X$, (associativity)

(b) $e\colon \mathrm{Spec}(\mathcal{O}_K) \to X$ (identity)

(c) $\iota\colon X \to X$ (inverse)

satisfying certain properties.

For $y^2 = x^3 + 1$ we need to check that addition is a morphism over $\mathbb{Z}[\sqrt{-1}]$.

Comparaison of Tate Modules

Note that X lives in the diagram below, relating $E = X_{\mathbb{F}_q}$ to X_K:

$$\begin{array}{ccccc} E & \hookrightarrow & X & \hookleftarrow & X_K \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{F}_q) & \hookrightarrow & \mathrm{Spec}(\mathcal{O}_K) & \hookleftarrow & \mathrm{Spec}(K) \end{array}$$

By a Comparison Theorem, $T_\ell(E) \cong T_\ell(X_K)$ and the action $(\circlearrowleft)$ of the Galois group of $\mathrm{Gal}(\overline{K}/K)$ on the Tate module $T_\ell(X_K)$ is unramified at $\mathfrak{p}$.

Galois Action and Fundamental Group

$$\begin{array}{ccc} T_\ell(E) & \cong & T_\ell(X_K) \\ \circlearrowleft & & \circlearrowleft \\ \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) & \longleftarrow & \mathrm{Gal}(\overline{K}/K) \\ \downarrow & & \downarrow \text{ unramified at } p \\ \mathrm{Aut}(T_\ell(E)) & \cong & \mathrm{Aut}(T_\ell(X_K)) \end{array}$$

If we define $E_{\mathbb{C}} := X_K \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\mathbb{C})$, we get that $\pi_1^{et}(\overline{E}, \overline{\mathcal{O}}_E) = \widehat{\pi_1(E_{\mathbb{C}})} = \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$.

From the previous example, this gives us $\widehat{\pi_1(X_{\mathbb{C}}, \mathcal{O}_X)}$ is a group with 2 generators.

This describes the difference between the algebraic and topological fundamental group of an elliptic curve.

Conclusion

Thank you!


Jeffrey Achter, Clifton Cunningham, *Isogeny classes of Hilbert-Blumenthal abelian varieties over finite fields*, 2002.


Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2001.


H.W. Lenstra. *Galois Theory for Schemes*. Electronic edition, 2008.


René Schoof. *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A,1987.


Silverman, J. *The arithmetic of elliptic curves*, Springer, 1985.


Tamas Szamuely. *Galois Groups and Fundamental Groups*. Electronic edition, 2008.