CFT of IQNF via EC with CM

Marius Leonhardt

25 February 2018

CFT of IQNF via EC with CM?

- CFT = Class Field Theory
- IQNF = Imaginary Quadratic Number Field
- EC = Elliptic Curve
- CM = Complex Multiplication

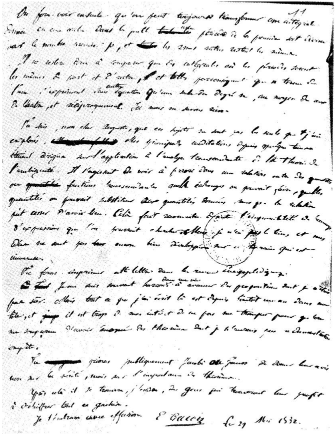
”The theory of complex multiplication is not only the most beautiful part of mathematics but also of all science.”
David Hilbert (1932)

Outline

Goal of CFT

Write down all abelian extensions of a given number field.
What does that mean?

Évariste Galois


Tu prieras publiquement Jacobi ou Gauss de donner leur avis non sur la vérité, mais sur l'importance des théorèmes.
Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.
Je t'embrasse avec effusion. E Galois Le 29 Mai 1832.

Galois theory

Galois theory studies symmetries of equations:

- Let $f(X) \in \mathbb{Q}[X]$ monic.
- Factor it: $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$.
- Permute the roots! Get $\sigma : \mathbb{Q}(\{\alpha_i\}) \to \mathbb{Q}(\{\alpha_i\})$.
- Only allow *field* isomorphisms. These form the Galois group

$$\mathsf{Gal}(\mathbb{Q}(\{\alpha_i\})/\mathbb{Q}).$$

Galois theory: an example

- Take $f(X) = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$
- Get two maps: identity and

$$c\colon \sqrt{2} \mapsto -\sqrt{2}$$

- Thus

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) = \{\mathrm{id}, c\} \cong \mathbb{Z}/2\mathbb{Z}$$

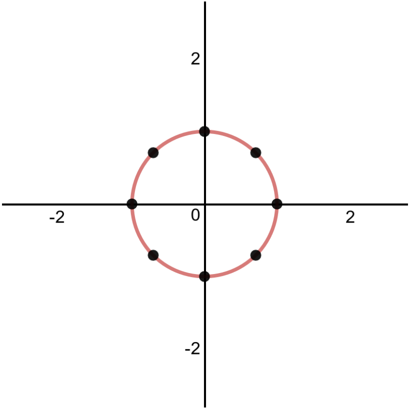
Roots of Unity

- $f(X) = X^N - 1$.
- With $\zeta_N = e^{2\pi i/N}$:

$$f(X) = \prod_{i=0}^{N-1} (X - \zeta_N^i)$$

- Allowed permutations: $\zeta_N \mapsto \zeta_N^a$ with $(a, N) = 1$.

Example $N = 8$:



$$(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right),$$
$$a \longmapsto [\zeta_N \mapsto \zeta_N^a].$$

The Kronecker–Weber Theorem

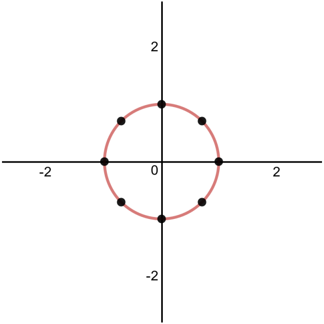
Theorem

Every abelian extension of $\mathbb{Q}$ *is contained in some cyclotomic field* $\mathbb{Q}(\zeta_N)$.

Example

$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$:

$$\zeta_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}, \qquad \zeta_8^2 = i.$$



The Kronecker-Weber Theorem – History

Theorem

Every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_N)$.

Leopold Kronecker

Heinrich Martin Weber

Summary CFT for $\mathbb{Q}$

- Every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_N)$.
- We "understand" $\mathbb{Q}(\zeta_N)$, e.g. $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$.
- $\zeta_N = e^{2\pi i/N}$ are special values of $\exp$.

Explicit CFT for other number fields?

Kronecker's "dearest dream of youth":
Do this for an IQNF K.

Hilbert's 12th Problem:
Do it for any NF K.

Outline

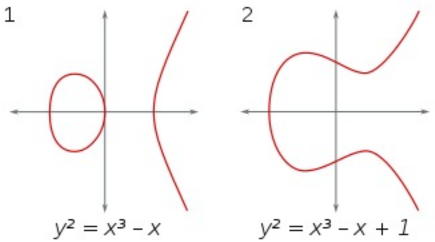
What are elliptic curves?

Definition

An elliptic curve E over $\mathbb{C}$ is the set of all $(x, y) \in \mathbb{C}^2$ satisfying

$$E\colon\ y^2 = x^3 + Ax + B$$

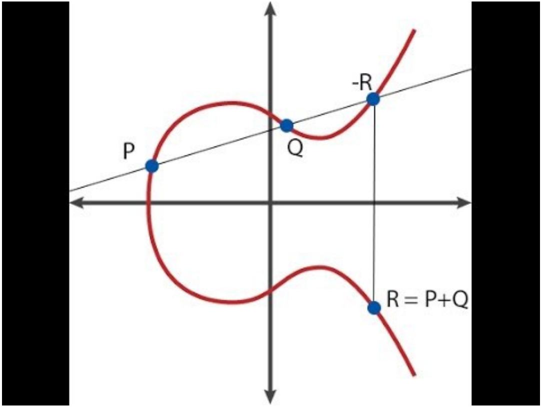
for fixed $A, B \in \mathbb{C}$, $4A^3 + 27B^2 \neq 0$, together with a "point at infinity" called O.



Addition on an elliptic curve

Example

$E\colon y^2 = x^3 + x$. Then $2(x,y) = \left(\frac{x^4-2x^2+1}{4y^2}, \frac{x^6+5x^4-5x^2-1}{8y^3}\right)$.



Symmetries of elliptic curves

Definition

The ring of endomorphism of E is

$$\mathrm{End}(E) := \{\Phi\colon E \to E | \Phi \textit{ morphism of varieties } + \textit{ group hom.}\}.$$

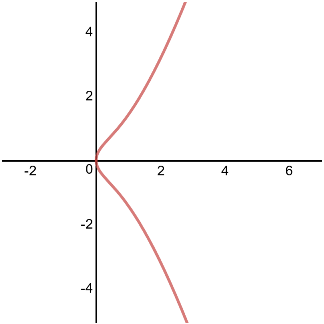
Example

Multiplication by n defines an endomorphism of E. Hence

$$\mathbb{Z} \subset \mathrm{End}(E).$$

Main example for this talk

$$E\colon y^2 = x^3 + x$$



- Multiplication by -1:

$$-1\colon (x, y) \mapsto (x, -y).$$

- Another endomorphism:

$$\Phi\colon (x, y) \mapsto (-x, iy).$$

- $\Phi^2 = -1$. Complex Multiplication

Elliptic Curves and Lattices

Let E be an elliptic curve over $\mathbb{C}$.

Fact

There exists a lattice $\Lambda \subset \mathbb{C}$ and a complex-analytic isomorphism

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{\sim} E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp'(z)) \\ 0 &\longmapsto O. \end{aligned}$$

Here we have used the Weierstraß $\wp$-function of Λ:

$$\wp(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Complex Multiplication

$E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ implies

- $\mathrm{End}(E) \cong \{c \in \mathbb{C} \mid c\Lambda \subset \Lambda\}$.
- $\mathrm{End}(E) = \mathbb{Z}$, or
- $\mathbb{Z} \subsetneq \mathrm{End}(E) \subset K$ for an IQNF K.
  E has complex multiplication (CM) by K.
- For example, $E\colon y^2 = x^3 + x$ has $\mathrm{End}(E) = \mathbb{Z}[i] \subset \mathbb{Q}(i)$.

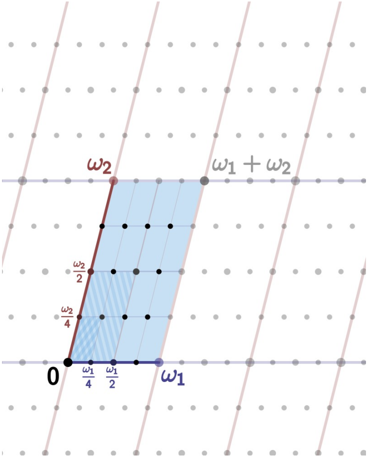
Torsion Points

The N-torsion subgroup of E is

$E[N] := \{P \in E \mid N{\cdot}P = 0\}$.

It looks like

$$E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2.$$



Picture of $E[4]$

Galois action on $E[N]$

- Let $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$.
- Let $\mathbb{Q}(E[N]) := \mathbb{Q}\big(x(P), y(P) \mid P \in E[N]\big)$.

Lemma

$\mathrm{Gal}\left(\mathbb{Q}(E[N])/\mathbb{Q}\right)$ *acts on* $E[N]$.

Proof.

Multiplication by N on E is given by polynomials in x, y, A, B. Hence if $P \in E[N]$ and $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(E[N])/\mathbb{Q}\right)$, then

$$N \cdot (\sigma(P)) = \sigma(N \cdot P) = \sigma(O) = O.$$

□

Galois representation attached to E

Fix a basis of $E[N]$ as a $\mathbb{Z}/N\mathbb{Z}$-module.

Definition

The Galois representation attached to E is

$$\rho_N\colon\ \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

sending σ to the matrix representing the action of σ on $E[N]$.

Lemma

ρ_N is injective.

Outline

Two actions

Now fix

- the imaginary quadratic field $K = \mathbb{Q}(i)$.
- the elliptic curve $E\colon y^2 = x^3 + x$ which has CM by K.

We have two actions:

- the Galois action ρ_N on $E[N]$.
- the CM action by $\mathrm{End}(E) = \mathbb{Z}[i] \subset K$ on $E[N]$, e.g. by

$$\Phi\colon (x, y) \mapsto (-x, iy).$$

When do the two actions commute?

- First Φ, then σ:

$$\sigma(\Phi(x,y)) = \sigma(-x, iy) = (-\sigma(x), \sigma(i)\sigma(y)).$$

- First σ, then Φ:

$$\Phi(\sigma(x,y)) = (-\sigma(x), i\sigma(y)).$$

- Thus we need $\sigma(i) = i$, i.e. σ needs to fix $K = \mathbb{Q}(i)$.
- Hence restrict ρ_N to those σ, i.e. to $\mathrm{Gal}(K(E[N])/K)$.

The abelian extension

- Galois action $\rho_N\colon \operatorname{Gal}(K(E[N])/K) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.
- CM action Φ on $E[N]$, corresponding to $A \in M_2(\mathbb{Z}/N\mathbb{Z})$.

Theorem

The image of ρ_N is abelian.

Proof.

Crucial ingredients:

1. The matrix A.
2. ρ_N and A commute.

$\square$

Concrete example

$$E\colon y^2 = x^3 + x$$

$$E[2] = \{O, (0,0), (\pm i, 0)\}$$

$$E[4] = E[2] \cup \Big\{(1, \pm\sqrt{2}), (-1, \pm i\sqrt{2}), (\alpha, \pm\beta), (-\alpha, \pm i\beta), \\ (\alpha^{-1}, \pm\alpha^{-2}\beta), (-\alpha^{-1}, \pm i\alpha^{-2}\beta)\Big\},$$

where $\alpha = (\sqrt{2} - 1)i$ and $\beta = (1 + i)(\sqrt{2} - 1)$.

$$\boxed{\mathbb{Q}(E[4]) = \mathbb{Q}(\sqrt{2}, i)}$$

The big theorem

Let $K = \mathbb{Q}(i)$ and $E\colon\ y^2 = x^3 + x$.

Theorem (CFT for K)

Every abelian extension of K is contained in some $K(E[N])$.

Remark ("dream of youth")

Using $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, $z \mapsto (\wp(z), \wp'(z))$, can identify

- $E[N]$ with $\frac{1}{N}\Lambda/\Lambda$.
- $K(E[N])$ with $K\left(\wp(t) | t \in \frac{1}{N}\Lambda/\Lambda\right)$.

Summary CFT for $K = \mathbb{Q}(i)$

- Every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_N)$.
- Every abelian extension of K is contained in some $K(E[N])$.
- $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.
- $\rho_N\colon\ \mathrm{Gal}(K(E[N])/K) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.
- $\zeta_N = e^{2\pi i/N}$.
- The coordinates of points in $E[N]$ are given by $\wp(z)$ and $\wp'(z)$.

General IQNF K

Fix an IQNF K and an EC E with CM by K.

Theorem

Every abelian extension of K is contained in some

$$K\big(j(E), x(P) | P \in E[N]\big).$$

Thank you for your attention!