JPNMS PhD Colloq.: CFT of IQNF via EC with CM

class field theory — imag. quadr. number field — elliptic curves — complex multiplication

please ask questions! So I should probably tell you what all the letters in the title mean. So the goal today is to explain what CFT is about and how the what role CM plays here. I'll start with a quote from David Hilbert:

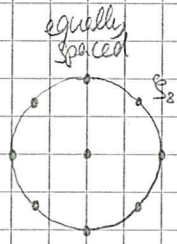
Plan today: "The theory of complex multiplication is not only the most beautiful part of mathematics but of the whole of science."

I want to give you a glimpse of this beauty

## ① CFT for $\mathbb{Q}$

o/w too hard

Question Task: Write down all finite (abelian) Galois extensions of $\mathbb{Q}$!




Example: Roots of unity - let $\xi_n := e^{2\pi i/n}$ → solves $X^n - 1 = \prod_{k=0}^{n-1} (X - \xi_n^k)$

→ Galois extension

→ have isomorphism $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma \longmapsto a(\sigma)$ s.t. $\sigma(\xi_n) = \xi_n^{a(\sigma)}$

→ Big theorem (Kronecker-Weber): Every finite abelian extension of $\mathbb{Q}$ is a subfield of some $\mathbb{Q}(\xi_n)$.

(Gauss sum example for $\mathbb{Q}(\sqrt{p})$? Or just say: e.g. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\xi_8)$)

New task: Do the same for any given number field $K$!

- Note: $L/K$ abelian $\not\Rightarrow$ $L/\mathbb{Q}$ abelian
- "Kronecker's Jugendtraum": Do this in close analogy to $\mathbb{Q}_{ab}$ by adjoining values of a transcendental function.
- ✓ by class field theory → roughly: says $\exists$ family of fields $K_{\mathfrak{m}}$ ("ray class fields") s.t. every abelian ext. $L/K$ is contained in some $K_{\mathfrak{m}}$, + can describe $\mathrm{Gal}(K_{\mathfrak{m}}/K)$

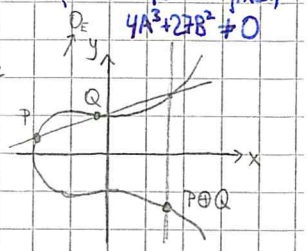
  ✗ not very explicit, i.e. I do not know which complex numbers belong to $K_{\mathfrak{m}}$

BUT: For IQNFs $K$ (e.g. $K = \mathbb{Q}(i)$), this can be done using elliptic curves with complex multiplication.

5-7min

## (2) EC

**Def.** An elliptic curve $E$ over $\mathbb{C}$ is the set of all $(x,y) \in \mathbb{C}^2$ satisfying $y^2 = x^3 + Ax + B$, $A,B \in \mathbb{C}$ fixed, $4A^3+27B^2 \neq 0$, together with a "point at $\infty$" called $O$.




They are fascinating because: Can use geometric procedure to add 2 points on $E$

↳ $E$ is a group variety! ABELIAN

↳ If $A,B \in \mathbb{Q}$, can look at $E(\mathbb{Q})$. (for us always $A,B \in$ number field $\supseteq H$)

**Def.:** $\mathrm{End}(E) := \{\phi : E \to E \mid$ morphism (of varieties) + group hom.$\}$ endomorphism ring

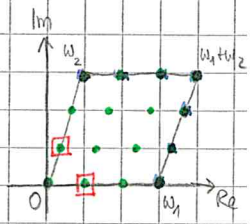
$\cup\ [\cdot]$

$\mathbb{Z}$ as "multiplication-by-$n$" is given by ~~pol~~ rational functions in coord's.

**Example:** $E: y^2 = x^3 + x$ has the endom. $\phi : (x,y) \mapsto (-x, iy)$

↳ $\phi^2 : (x,y) \mapsto (x,-y) = [-1] \Rightarrow \phi^2 + 1 = 0$ : $\phi \hat{=}$ multipl. by $i$ ↷ CM.

$\Rightarrow \phi \notin \mathbb{Z}$




- **Elliptic Curves over $\mathbb{C}$:**

**Fact:** $\exists$ lattice $\Lambda \subset \mathbb{C}$ & complex-analytic isom. $\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ (given by Weierstraß $\wp$) ← complex torus

$\Rightarrow \mathrm{End}(E) = \{f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \mid f$ holomorph & $f(z_1+z_2) = f(z_1)+f(z_2)\} \mod \Lambda\}$

skip

$= \{f : \mathbb{C} \to \mathbb{C} \mid$ holomorph & $f(z_1+z_2) \overset{\text{on nhood of } 0}{=} f(z_1)+f(z_2) \in \Lambda\}$ ↓ $\Lambda$ discrete, holom. maps are open

$= \{f : \mathbb{C} \to \mathbb{C} \mid$ holom. & $f(z_1+z_2) = f(z_1)+f(z_2)+c_0\}$ ← $c_0 = -f(0) \overset{\text{wlog}}{=} 0$ ↓ look at derivative at $z$: $f'(z) = f'(0)$

$= \{f : \mathbb{C} \to \mathbb{C} \mid f(z) = cz$ for some $c \in \mathbb{C}$ s.t. $c\cdot\Lambda \subset \Lambda\}$

$\cong \{c \in \mathbb{C} \mid c\cdot\Lambda \subset \Lambda\}$ (ring isom.)

Choosing a basis for $\Lambda$, it's not hard to check

Say $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \notin \mathbb{R}$. $c = r+s\cdot\tau$

$c\cdot\tau = t+u\cdot\tau \to \tau = \frac{t}{c-u}$

$\mathrm{End}(E) \cong \mathbb{Z}$ or $\mathrm{End}(E) \cong$ an imaginary quadratic field $K$ (even an 'order'). $\Rightarrow c^2 - (r+u)c + ru - st = 0$

**Example above:** $\mathrm{End}(E) \cong \mathbb{Z}[i] \subseteq \mathbb{Q}(i) =: K$.

- **$n$-torsion points**

- From picture we see: $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. → choose basis / ~~Easy~~ This is $E[3]$!

**Lemma:** $\mathbb{Q}(E[n])/\mathbb{Q}$ is Galois. (explain notation) for $E/H$ EC

$E$ EC $/\mathbb{Q}(\tau)$

**Proof:** $\sigma \in \mathrm{Aut}(\mathbb{C}/H)$, $P \in E[n] \Rightarrow [n](\sigma(P)) = \sigma([n](P)) = 0$, so $\sigma(P) \in E[n]$. l.p., only finitely many conjugates of $P$ $\Rightarrow$ ✓

**Def.** Galois representation $\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$

$\sigma \mapsto \rho_n(\sigma)$ ~~basis~~: matrix repres. $\sigma$ on $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

(Recall: $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \to \{GL_1(\mathbb{Z}/n\mathbb{Z})\}$.

**Lemma:** $\rho_n$ is injective.

**Proof:** $\rho_n(\sigma) = \begin{pmatrix}1&0\\0&1\end{pmatrix} \Rightarrow \sigma = \mathrm{id}$ on $E[n]$. But then $\sigma = \mathrm{id}$ on $\mathbb{Q}(E[n]) \Rightarrow$ done. ▨

20 min

## (3) CM

Now: Fix an IQNF $K$ ~~(eg. $K=\mathbb{Q}(i)$)~~ ex.: $K=\mathbb{Q}(i)$

and an EC $E/H$ with CM by $\mathcal{O}_K$ (i.e. $\mathrm{End}(E)=\mathcal{O}_K$) $E: y^2=x^3+x$, $H=\mathbb{Q}$

- In our examples:

Have Galois action $\rho_n$ on $E[n]$

& CM action $\phi$ on $E[n]$ } When do they commute? ← because $\phi$ is a group hom.

In our examples: $\sigma(\phi(x,y)) = \sigma(-x, iy) = (-\sigma(x), \sigma(i)\sigma(y))$

$\phi(\sigma(x,y)) = (-\sigma(x), i\,\sigma(y))$ } Need $\sigma(i)=i$, i.e. $\sigma|_K = \mathrm{id}$

→ We restrict $\rho_n$ to $\mathrm{Gal}(K_n/K) \to GL_2(\mathbb{Z}/n\mathbb{Z})$

$K_n := K(E[n])$

**Theorem:** $\mathrm{im}(\rho_n)$ is abelian.

**Proof:** (a) $\phi \leftrightarrow$ matrix $A \in GL_2(\mathbb{Z}/n\mathbb{Z})$

$\phi^2+1=0 \leftrightarrow A^2+1=0 \Rightarrow A \in GL_2(\mathbb{Z}/n\mathbb{Z})$.

More calculation (a bit tricky): $A$ not a scalar matrix.

→ Assume $A \equiv \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \pmod{\ell}$, some $\ell \mid n$

$\Rightarrow \phi(P) = mP \quad \forall P \in E[n] \subseteq E[n]$. (*)

Using complex conjug., not hard to show $2mP = \mathcal{O}$ $\forall P \in E[\ell]$ ⇒ $\ell \mid 2$: Typically can explicitly calculate matrix

or $\ell \mid m$. Then (*): $\phi(P)=0$ $\forall P \in E[\ell]$ as $\phi^2(P)=-P$.

(b) "Linear Algebra": If $H \leq GL_2(\mathbb{Z}/n\mathbb{Z})$, $A$ not scalar, s.t. $\forall h \in H: hA=Ah$, then $H$ is abelian.

↖ Put $A$ in form $\left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right)$ & explicitly calculate. (over field: no problem to change basis. over $GL_2(\mathbb{Z}/p^e\mathbb{Z})$: a bit tricky)

**Example:** $n=4$: can write down formulae for $[4]$ & find all 4-torsion points on $E$

⇝ $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{2})$ : then abelian over $\mathbb{Q}(i)$.

---

**General $K$** We used that: • $[n]$-mult. is def. over ~~$K(E)$~~ $\mathbb{Q}$ — in general ~~$K=\mathbb{Q}(j(E))$~~ (If $E$ has CM, then $j(E)$ is algebraic / $\mathbb{Q}$)

• CM action $\phi$ is def. over $\mathbb{Q}(i)$ — — over $H := K(j(E))$

⇒ we will get $H(E[n])/H$ abelian – but not nec. abelian /$K$.

Solution: Use only x-coord's of points in $E[n]$ (or, in some special cases, a Weber fct. $h_E: E \to \mathbb{P}^1$)

& we'll get $\underbrace{K(j(E), h_E(E[n]))}_{=: K_n}$ /$K$ abelian.

↓

**Big theorem:** Every abelian extension of $K$ is contained in some $K_n$. 30 min

[ **Remark** (Jugendtraum) Using $\mathbb{C}/\Lambda \to E(\mathbb{C})$, $z \mapsto (\wp(z), \wp'(z))$ (for $\Lambda \subset K$), one has $K_n = K\left(j(E), \wp(t) \mid t \in \frac{1}{n}\Lambda/\Lambda < K/\Lambda\right)$

+ can describe $\mathrm{Gal}(K_n/K)$-action on $t$

⇒ all one could hope for. ]

**Remark:** ~~For general $K$, These are the only~~ $\mathbb{Q}$ and IQNFs are the only number fields for which this is known.

Probably can generalises to "CM fields", but won't get ALL abelian extensions.

## (4) ~~The main theorem of CM~~ Generalisations

We've studied the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on $E(\mathbb{C})_{\mathrm{tors}}$ (careful: $E$ may change to ${}^{\sigma}E$)

[Main theorem of CM: $E/\mathbb{C}$ EC with CM by $\mathcal{O}_K$, choose lattice $\Lambda \subset K$ s.t. $\Theta: \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$.

Then ${}^{\sigma}E$ has lattice $s\cdot\Lambda$, and $\exists!\ \Theta': \mathbb{C}/s\cdot\Lambda \xrightarrow{\sim} {}^{\sigma}E(\mathbb{C})$ s.t. $\sigma$ is given on torsion points by

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\Theta}_{\sim} & E(\mathbb{C})_{\mathrm{tors}} \\ \downarrow \cdot s & & \downarrow \sigma \\ K/s\Lambda & \xrightarrow[\Theta']{\sim} & {}^{\sigma}E(\mathbb{C})_{\mathrm{tors}} \end{array}.$$

Here $s \in \mathrm{art}_K^{-1}(\sigma|_{K^{\mathrm{ab}}}) \in \mathbb{A}_K^{\times}$ is an idèle. ]

Now look at the moduli space $M_{EC}$ of ECs over $\mathbb{C}$ (+ additional structure) up to isom. $\rightsquigarrow$ $M$ is an algebraic curve! (over some number field $L$)

Tony nachmal fragen (Michael hat da auch was erzählt)

points of $M_{EC}$ $\longleftrightarrow$ $\{\text{ECs over } \mathbb{C}\}/\sim$

$\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ ↺

$\cup$

ECs with CM by $K$

$\{\text{~~CM ECs over C~~}\}/\sim$

↺

$\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Not hard: extends to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Actions coincide!

~~Higher~~ This has many powerful applications!

- Higher dimensional picture: EC $\rightsquigarrow$ AV

points of $M_{AV}$ $\longleftrightarrow$ $\{\text{AVs (+polar. + level-structure +...)}\}/\sim$

$\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ ↺

but does not extend!

$\cup$

$\{\text{AVs with CM by } K\}/\sim$

↺

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Even extends to $\mathrm{Gal}(\overline{\mathbb{Q}}/K_+) \rtimes S_{[K_+:\mathbb{Q}]}$

My task atm: Understand this action.