# KOLYVAGIN

Note Title 14/10/2022

## Curve ellittiche CM

14/10/2022
L. Furio

Su $\mathbb{C}$: $\quad \mathbb{C}/\Lambda \longleftrightarrow E: y^2 = 4x^3 - g_2 x - g_3$

$$z \longmapsto (\wp(z), \wp'(z))$$

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

Isogenia: $f: E_1 \to E_2$ algebrica, non costante, $f(\infty) = \infty$

**Prop** $f$ induce un omomorfismo di gruppi

**Def.** Se $E: y^2 = x^3 + ax + b$, $\quad j(E) = 1728 \dfrac{4a^3}{4a^3 + 27b^2}$

**Prop.** $j$ dà una bigezione fra $\{E/\mathbb{C}\}/_{\text{isom}}$ e $\mathbb{C}$.

**Azione di Galois** Data $E/K$ e $\sigma \in \mathrm{Aut}(\overline{K})$, abbiamo

$$E^\sigma : \quad y^2 = x^3 + \sigma(a)x + \sigma(b)$$

Inoltre, data $\varphi : E_1 \longrightarrow E_2$, otteniamo $\varphi^\sigma : E_1^\sigma \longrightarrow E_2^\sigma$

**Def.** $K(E) := K(x,y)$ dove $E : y^2 = x^3 + ax + b$

Data $\varphi : E_1 \longrightarrow E_2$ isogenia, abbiamo $\varphi^* : K(E_2) \longrightarrow K(E_1)$ iniettiva, e posso considerare $K(E_1) / \varphi^* K(E_2)$

**Def.** $\deg \varphi = [K(E_1) : \varphi^* K(E_2)]$

- $\varphi$ e' separabile se $K(E_1) / \varphi^* K(E_2)$ lo e'
  inseparabile
  pur. insep.

- Se $\varphi$ e' separabile, $\deg \varphi = |(\ker \varphi)(\overline{K})|$

**Def.** Se char $K = p$, $E : y^2 = x^3 + ax + b$, poniamo

$$E^{(q)} : y^2 = x^3 + a^q x + b^q$$

e

$$F_q : E \longrightarrow E^{(q)}$$

$$(x,y) \longmapsto (x^q, y^q)$$

**Prop.** $F_q$ e' puramente insep. di grado $q$

$$F_q^* K(x,y) = K(x^q, y^q)$$

**Prop** Ogni isogenia $\varphi : E_1 \longrightarrow E_2$ si scrive come

$$\varphi = \psi \circ F_q$$

per un opportuno $q$ e un'isog. separabile $E_1^{(q)} \xrightarrow{\psi} E_2$

**Differenziali** $\Omega_E := \{ df \mid f \in \overline{K}(E) \} / \sim$, dove la relaz. è generata da

$$d(x+y) = dx + dy$$

$$d(x \cdot y) = x \, dy + y \, dx$$

$$d(a) = 0 \qquad \forall a \in \overline{K}$$

Data $f : E_1 \longrightarrow E_2$ ho $f^* : \Omega_{E_2} \longrightarrow \Omega_{E_1}$

**Def.** I DIFFERENZIALI INVARIANTI sono quegli $\omega \in \Omega_E$ t.c.

$$\tau_P^* \omega = \omega \qquad \forall P \in E(\overline{K})$$

**Es** Per $E: y^2 = x^3 + ax + b$, $\omega = \frac{dx}{y}$ è invariante.

Su $\mathbb{C}$, $\frac{dx}{y} = \frac{d(\wp(z))}{\wp'(z)} = \frac{\wp'(z) \, dz}{\wp'(z)} = dz$ è chiaramente invariante

**Oss.** $\omega$ invariante $\rightsquigarrow$ $f^*\omega$ invariante.

**Prop.** $f: E_1 \longrightarrow E_2$ isogenia. $f$ è separabile $\Leftrightarrow$ $f^*$ è iniettivo

**Def.** $\mathrm{End}(E) := \{ f: E \to E \text{ isogenia} \} \cup \{0\}$

**Prop.** $\mathrm{End}(E)$ è un anello con $+_E$ e $\circ$

**Prop.** $\mathrm{End}(E)$ è uno dei seguenti: $\mathbb{Z}$, un ordine in un campo quadratico immaginario, un ordine in un'algebra di quat. su $\mathbb{Q}$

Inoltre:

- $\mathrm{char}\, K = 0$ $\rightsquigarrow$ solo casi 1 e 2
- $K = \mathbb{F}_q$ $\rightsquigarrow$ " " 2 e 3

**Def.** Sia $K$ un sottocampo di $\mathbb{C}$. Diremo che $E/K$ ha MOLTIPLICAZIONE COMPLESSA (CM) se $\mathrm{End}(E_{\overline{K}})$ e' un ordine in un campo quadr. img.

**Oss.** Dato $\sigma \in \mathrm{Aut}(\overline{K})$, ottengo bigezione $\mathrm{End}(E^\sigma) = \sigma(\mathrm{End}\, E) \overset{\wr\wr}{\phantom{x}}$ $\mathrm{End}\, E$

**Ordini** $\mathcal{O} \subseteq \mathcal{O}_K$, $\mathcal{O} \simeq \mathbb{Z}^2$, $[K:\mathbb{Q}]=2$

Gli ordini sono tutti e soli quelli della forma $\mathbb{Z} + f \cdot \mathcal{O}_K$; chiamiamo $f = [\mathcal{O}_K : \mathcal{O}]$ il CONDUTTORE di $\mathcal{O}$

**Def.** $\mathcal{F}(\mathcal{O}) = \{$sotto-$\mathcal{O}$-moduli f.g. di $K$, invertibili$\}$

$= \{$sotto-$\mathcal{O}$-mod f.g. di $K$ PROPRI$\}$

(Proprio $= \{\alpha \in \mathcal{O} : \alpha I \subset I\} = \mathcal{O}$)

$$Cl(\mathcal{O}) := \mathcal{F}(\mathcal{O}) / Princ(\mathcal{O})$$

## Isogenie su $\mathbb{C}$

$\Lambda, \Lambda' \leq \mathbb{C}$. $\quad \mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda' \iff \exists \alpha \in \mathbb{C}^* \mid \alpha\Lambda = \Lambda'$

Dato $I \in \mathcal{F}(\mathcal{O})$, posso considerare $E_I := \mathbb{C}/I$

Ora, $E_I \simeq E_{I'} \iff I$ omotetico ad $I'$

$\iff [I] = [I']$ in $Cl(\mathcal{O})$

**Def.** $Ell(\mathcal{O}) = \{E/\mathbb{C} \mid End(E) = \mathcal{O}\}/_{iso}$

**Prop.** Sia $E/\mathbb{C}$ con $End(E) = \mathcal{O}$. Allora $E \simeq E_I$ per qualche $I \in \mathcal{F}(\mathcal{O})$

**Prop.** $\mathcal{C}\ell(\mathcal{O}) \curvearrowright \mathcal{E}\ell\ell(\mathcal{O})$ in modo semplicemente transitivo

$$[J] * E_I = E_{JI}$$

**Cor** $|\mathcal{E}\ell\ell(\mathcal{O})| = |\mathcal{C}\ell(\mathcal{O})|$

**Prop.** Se $E \in \mathcal{E}\ell\ell(\mathcal{O})$, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \# \mathcal{C}\ell(\mathcal{O})$

**Dim.** Dato $\sigma \in \mathrm{Aut}(\mathbb{C})$, $\mathrm{End}(E^\sigma) \simeq \mathcal{O} \Rightarrow E^\sigma \in \mathcal{E}\ell\ell(\mathcal{O})$

Ora $j(E^\sigma) = j(E)^\sigma$ ha $\leq \# \mathcal{C}\ell(\mathcal{O})$ coniugati □

**Aritmetica** Sia ora $E/K$, $K$ = campo di numeri, $\mathfrak{p} \triangleleft \mathcal{O}_K$ primo.

**Def.** $E$ ha buona riduz. mod $\mathfrak{p}$ se $\exists \; \mathcal{E}/\mathcal{O}_{K,\mathfrak{p}}$ t.c. $\mathcal{E}_{\mathfrak{p}}$ e' liscia

Posso ridurre anche isogenie: se $\varphi : E_1 \longrightarrow E_2$ e' isog. fra curve con buona riduz. mod $p$. Non e' detto che $\tilde{\varphi}$ sia separabile.

$$\begin{tikzcd}
E_1 \arrow[r, "\varphi"] \arrow[d] & E_2 \arrow[d] \\
\tilde{E}_1 \arrow[r, "\tilde{\varphi}"'] & \tilde{E}_2
\end{tikzcd}$$

Teo $p$ primo, $(p, f) = 1$, $f = \mathrm{Cond}(\mathcal{O})$, $K = \mathrm{Frac}(\mathcal{O})$, $p\mathcal{O} = \mathfrak{p} \cdot \mathfrak{p}'$, $E_1, \dots, E_h$ rappr. di $\mathcal{E}\ell\ell(\mathcal{O})$,

Galois $\to L \supseteq K(j(E_1), \dots, j(E_h))$, $p$ di buona riduz per ogni $E_i$

Allora $\forall\, I \in \mathcal{F}(\mathcal{O})$ abbiamo

$$j(E_I)^p \equiv j(E_{q' \cdot I}) \mod Q,$$

$\forall\ Q \subseteq \mathcal{O}_L$ primo sopra $\mathfrak{q}$.

**Dim.** Equivalentemente, $j(E_{qI})^p \equiv j(E_I) \mod Q$

$$\mathbb{C}/_{qI} \xrightarrow{\lambda} \mathbb{C}/_{I} \quad \leadsto \quad \lambda : E_{qI} \xrightarrow{\lambda} E_I$$

proiez. canonica

$$\mathbb{C}/_{I} \xrightarrow{\sim} \mathbb{C}/_{pI} = \mathbb{C}/_{\mathfrak{q}'\mathfrak{q}I} \longrightarrow \mathbb{C}/_{\mathfrak{q}I} \xrightarrow{\lambda} \mathbb{C}/I$$

**Lemma** $\exists\, r \lhd \mathcal{O}$ primo, $[r] = [\mathfrak{q}']$ in $\mathcal{Cl}(\mathcal{O}_K)$, e $(r, p) = 1$

Ora $[r\mathfrak{q}] = [\mathfrak{q}'][\mathfrak{q}] = [1]$, quindi $r\mathfrak{q} = (\alpha)$

$$\mathbb{C}/I \xrightarrow{\sim} \mathbb{C}/\alpha I \simeq \mathbb{C}/rqI \longrightarrow \mathbb{C}/qI \xrightarrow{\lambda} \mathbb{C}/I$$

$$\begin{tikzcd}
\mathbb{C}/I \arrow[r, "\mu"] \arrow[d] & \mathbb{C}/qI \arrow[r, "\lambda"] \arrow[d] & \mathbb{C}/I \arrow[d] \\
E_I \arrow[r, "\mu"] \arrow[d] & E_{qI} \arrow[r, "\lambda"] \arrow[d] & E_I \arrow[d] \\
\tilde{E}_I \arrow[r, "\tilde{\mu}"] & \tilde{E}_{qI} \arrow[r, "\tilde{\lambda}"] & \tilde{E}_I
\end{tikzcd}$$

dove le riduz sono modulo un primo $Q'$ di un'estensione $L'/L$ su cui $\lambda$, $\mu$ sono definite

Osservo che $\tilde{\lambda} \circ \tilde{\mu} = \widetilde{\lambda \circ \mu} = \tilde{\alpha}$ ; voglio dire che questa e' insep. mod $Q$.

Ora $(\tilde{\lambda} \circ \tilde{\mu})^* : \Omega_{\tilde{E}_I} \longrightarrow \Omega_{\tilde{E}_I}$ è la riduzione di

$$(\lambda \circ \mu)^* = [\alpha]^* : \Omega_{E_I} \longrightarrow \Omega_{E_I} ,$$
$$\omega \longmapsto \alpha \omega$$

e quindi mod $Q$ è la mappa $0$, perché $\alpha \in \triangleleft \subseteq Q$.

Quindi $\widetilde{\lambda \circ \mu}$ è inseparabile. Ma $\tilde{\mu}$ è separabile, quindi $\tilde{\lambda}$ è insep di grado $|\mathcal{O}/\triangleleft| = p$, cioè "è" il Frobenius

(deg $\tilde{\mu}$ è un parente di $r$, coprimo con $p$)

Allora $\tilde{E}_I = \tilde{E}_{\triangleleft I}^{(p)} \Rightarrow j(\tilde{E}_I) = j(\tilde{E}_{\triangleleft I})^p$ $\square$

# CLASS FIELD THEORY & COMPLEX MULTIPLICATION

21/10
Stefanello

## References

① Janusz, Algebraic number fields

② Cox, Primes of the form $x^2+ny^2$

③ Kedlaya, Complex multiplication and explicit class field theory

## 0. Overview

$K$ = nb. field

$$\mathcal{C}\ell_K = \frac{I_K}{P_K} = \frac{\{\text{fractional ideals of } \mathcal{O}_K\}}{\{a\,\mathcal{O}_K \mid a \in \mathcal{O}_K^\times\}}$$

CFT: $\exists\, K_1/K$, the Hilbert class field, which is a finite

Galois extension w/ $\mathrm{Gal}(K_1/K) \simeq Cl_K$, $K_1/K$ everywhere unramified (INCLUDING the infinite places, that is: if $v$ is a real place of $K$, $K_1 \underset{K}{\otimes} K_v \simeq \mathbb{R}^{[K_1/K]}$)

If $K$ is imaginary quadr and $\mathcal{O}$ is an order of $K$, there is a class group $Cl(\mathcal{O})$. We will see that:

1) $\exists\ L/K$ s.t. $\mathrm{Gal}(L/K) \simeq Cl(\mathcal{O})$

2) in fact, $L = K(j(E))$, where $E$ is an ell. curve with CM by $\mathcal{O}$

# 1. Class field theory

$K$ a nb. field

Def. A MODULUS for $K$ is a formal product $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$, where

- $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_K$
- $\mathfrak{m}_\infty$ is a squarefree formal product of embeddings $K \hookrightarrow \mathbb{R}$

Def. Let $\mathfrak{m}$ be a modulus. We consider

$$I_K(\mathfrak{m}) = \langle \text{prime ideals } \mathfrak{p} \text{ of } \mathcal{O}_K : \mathfrak{p} \nmid \mathfrak{m} \rangle < I_K,$$

the subgroup of fractional ideals prime to $\mathfrak{m}$, and

$$P_{K,1}(\mathfrak{m}) = \langle \alpha \mathcal{O}_K \mid \alpha \in \mathcal{O}_K, \ \alpha \equiv 1 \ (\mathfrak{m}_0), \ i(\alpha) > 0 \ \forall i \mid \mathfrak{m}_\infty \rangle$$

**Def.** A GENERALISED CLASS GROUP is a quotient $I_K(\mathfrak{m})/H$, where $H$ contains $P_{K,1}(\mathfrak{m})$

**Rmk** The subscript "1" reminds us of the condition $\equiv 1 \ (\mathfrak{m}_0)$

**Ex.** $\mathfrak{m} = 1 \ (= \mathcal{O}_K)$, $H = P_{K,1}(\mathfrak{m}) \Rightarrow$ the usual class group

Let $L/K$ be a finite Gal ext. and let $\mathfrak{p} \triangleleft \mathcal{O}_K$ be a prime that is unramified in $L$. Fix $\mathfrak{q} \triangleleft \mathcal{O}_L$ over $\mathfrak{p}$.

There exists a unique $\sigma \in \mathrm{Gal}(L/K)$ s.t. $\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$ $\forall x \in \mathcal{O}_L$

**Def.** $\left(\frac{L/K}{\mathfrak{q}}\right)$ is the element above (Artin symbol)

$\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{ \left(\frac{L/K}{\mathfrak{q}}\right) : \mathfrak{q} \mid \mathfrak{p} \right\}$ is a conjugacy class.

If $L/K$ is abelian, $\left(\frac{L/K}{\mathfrak{p}}\right)$ is a set containing a single element, and we denote by $\left(\frac{L/K}{\mathfrak{p}}\right)$ that element.

Let now $L/K$ be abelian, and fix a modulus $\mathfrak{m}$ of $K$ s.t. every prime ramified in $L$ divides $\mathfrak{m}$.

This allows us to define the ARTIN MAP,

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$
$$\prod_i \mathfrak{p}_i^{e_i} \longmapsto \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$$

**Thm** (Artin reciprocity)

- $\Phi_{\mathfrak{m}}$ is surjective
- if $\mathfrak{m}$ is "big enough" (wrt divisibility), then

$$\ker \Phi_{\mathfrak{m}} \supseteq P_{K,1}(\mathfrak{m})$$

$\Rightarrow$ $\mathrm{Gal}(L/K)$ is a generalised class group.

**Thm** (Existence) Let $\mathfrak{m}$ be a modulus for $K$, $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$

There exists a finite abelian ext. $L/K$, unramified away from $\mathfrak{m}$, s.t. $\phi_{\mathfrak{m}} : \dfrac{I_K(\mathfrak{m})}{H} \longrightarrow \mathrm{Gal}(L/K)$ is an isomorphism.

Cor./ex: for $\mathfrak{m} = 1$ and $H = P_{K,1}(\mathfrak{m})$ $\rightsquigarrow$ get $K_1/K$, the Hilbert class field.

## § 2. Class field theory and orders.

$K$ = imag. quadratic field.

Def. An ORDER $\mathcal{O} \subseteq K$ is a subgroup of $K$ s.t.

(i) $\mathcal{O}$ is a f.g. $\mathbb{Z}$-module

(ii) $\mathrm{Span}_{\mathbb{Q}}\, \mathcal{O} = K$

Rmk (i) $\Rightarrow$ $\mathcal{O}$ is integral $\Rightarrow$ $\mathcal{O} \subseteq \mathcal{O}_K$. Hence $\mathcal{O}_K$ is the unique maximal order of $K$

**Def.** The CONDUCTOR of $\mathcal{O}$ is $f = [\mathcal{O}_K : \mathcal{O}] < \infty$

**Prop.** The unique order of conductor $f \geq 1$ is $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$

If $I$ is a fractional ideal of $\mathcal{O}$, we consider the associated order $\{\beta \in K \mid \beta I \subseteq I\} =: \mathcal{A}_I$. It is clear that

$$\mathcal{O} \subseteq \mathcal{A}_I \subseteq \mathcal{O}_K$$

**Def.** $I$ is PROPER if $\mathcal{A}_I = \mathcal{O}$

**Prop.** $I$ is proper $\Leftrightarrow$ $I$ is invertible

**Def.** $I(\mathcal{O}) := \{$proper fractional ideals of $\mathcal{O}\}$. It is a group, containing as a subgroup $P(\mathcal{O}) = \{\alpha \mathcal{O}_K \mid \alpha \in K^\times\}$

**Def.** The CLASS GROUP of $\mathcal{O}$ is $I(\mathcal{O})/P(\mathcal{O})$

**Rmk** Of course, in the case $\mathcal{O} = \mathcal{O}_K$ we get the usual class group.

We now want to realise $Cl(\mathcal{O})$ as a generalised class group in the sense of CFT.

**Step 1** Let $\mathcal{O}$ be the order of conductor $f$

**Def.** $I \triangleleft \mathcal{O}$ is coprime with $N > 0 \iff I + N\mathcal{O} = \mathcal{O} \iff (N(I), N) = 1$, where $N(I) = |\mathcal{O}/I|$.

**Prop.** Fix $S \in I(\mathcal{O})$ and $N > 0$. There exists a proper ideal

$I$ of $\mathcal{O}$ s.t. $[S] = [I]$ in $\mathcal{Cl}(\mathcal{O})$ and $I$ is coprime with $N$.

**Prop.** If $I \trianglelefteq \mathcal{O}$ is coprime to $f$, then $I$ is proper

**Proof.** Let $\beta \in \mathcal{A}_I$. We have

$$\beta \mathcal{O} = \beta(I + f\mathcal{O}) = \beta I + \beta f \mathcal{O} \subseteq I + f\mathcal{O}_K \subseteq \mathcal{O}$$

$\llcorner \beta \in \mathcal{A}_I$

$$\Rightarrow \beta \in \mathcal{O} \Rightarrow \mathcal{A}_I = \mathcal{O}. \qquad \square$$

Let

$$\begin{array}{l} I(\mathcal{O}, f) = \langle I \trianglelefteq \mathcal{O} : I \text{ coprime with } f \rangle \subseteq I(\mathcal{O}) \\ \cup\!| \\ P(\mathcal{O}, f) = \langle \alpha\mathcal{O} : \alpha \in \mathcal{O}, (N(\alpha), f) = 1 \rangle \end{array}$$

**Prop.** The natural map

$$\frac{I(\mathcal{O}, f)}{P(\mathcal{O}, f)} \longrightarrow \frac{I(\mathcal{O})}{P(\mathcal{O})} = Cl(\mathcal{O})$$

is an isomorphism.

**Proof.** We know that $I(\mathcal{O}, f) \longrightarrow I(\mathcal{O})/P(\mathcal{O})$. One checks that $P(\mathcal{O}) \cap I(\mathcal{O}, f) = P(\mathcal{O}, f)$ $\square$

**Step 2** Consider $f\mathcal{O}_K$ as a modulus of $K$ (here, as usual, $f = [\mathcal{O}_K : \mathcal{O}]$)

**Prop.** $I(\mathcal{O}, f) \xrightarrow{\sim} I_K(f \cdot \mathcal{O}_K)$, where $I_K(f \cdot \mathcal{O}_K)$

is the group of fractional ideals of $\underline{\underline{\mathcal{O}_K}}$ that are prime to $\mathfrak{f}$.

This map is norm-preserving, with inverse given by "contraction"

Via this map, $P(\mathcal{O}, \mathfrak{f}) \xrightarrow{\sim} P_{K,\mathbb{Z}}(f\mathcal{O}_K)$, where

$$P_{K,\mathbb{Z}}(\mathfrak{f}\mathcal{O}_K) = \langle \alpha\mathcal{O}_K \mid \alpha \in \mathcal{O}_K,\ \exists k \in \mathbb{Z} \quad (z, f) = 1 \quad \text{s.t.} \quad \alpha \equiv z \bmod f\mathcal{O}_K \}$$

Clearly $P_{K,\mathbb{Z}}(\mathfrak{f}\mathcal{O}_K) \supseteq P_{K,1}(\mathfrak{f}\mathcal{O}_K)$.

By the existence theorem of CFT, $\exists\, K_f/K$ finite, abelian, unramified outside $f\mathcal{O}_K$, s.t.

$$Cl(\mathcal{O}) = \frac{I(\mathcal{O})}{P(\mathcal{O})} \xrightarrow{\sim} \frac{I(\mathcal{O},\mathfrak{f})}{P(\mathcal{O},\mathfrak{f})} \xrightarrow{\sim} \frac{I_K(f\mathcal{O}_K)}{P_{K,\mathbb{Z}}(f\mathcal{O}_K)} \xrightarrow[\sim]{\phi_{f\mathcal{O}_K}} Gal(K_f/K)$$

$$(*) \qquad [S] \underset{\substack{\rightsquigarrow \\ \text{non-explicit}}}{\longmapsto} [I] \longmapsto [I\mathcal{O}_K] \longmapsto \left(\frac{K_f/K}{I\mathcal{O}_K}\right)$$

Rmk
- By abuse of notation, we denote by $\left(\frac{K_f/K}{S}\right)$ the Artin symbol of (the image of) $[S]$
- If $f=1$, we get once again the Hilbert class field

## 3. Description of $K_f$

$K$ quadratic imaginary, $\mathcal{O}$ the order of conductor $f$.

Last time:

$$\begin{aligned} \mathcal{C}\ell(\mathcal{O}) &\xrightarrow{\sim} \mathcal{E}\ell\ell(\mathcal{O}) \\ [I] &\longmapsto E_I := \mathbb{C}/I \end{aligned}$$

Take representatives $E_1, \dots, E_m$ for $\mathcal{E}ll(\mathcal{O})$

**Notation** For $I \in \mathcal{I}(\mathcal{O})$, $j(I) := j(E_I)$. It is an algebraic

INTEGER

**Rmk** $I, I' \in \mathcal{I}(\mathcal{O})$, then $j(I) = j(I') \Leftrightarrow [I] = [I']$ in $Cl(\mathcal{O})$

**Thm** For $\sigma \in Gal(\overline{\mathbb{Q}}/K)$ and $I \in \mathcal{I}(\mathcal{O})$, then

$$\sigma(j(I)) = j(S^{-1}I),$$

where $S \in \mathcal{I}(\mathcal{O})$ s.t. $\left(\frac{K_f/K}{S}\right) = \sigma|_{K_f}$

**Rmk** If $S, S' \in \mathcal{I}(\mathcal{O})$ are s.t. $\left(\frac{K_f/K}{S}\right) = \left(\frac{K_f/K}{S'}\right)$,

then $[S] = [S']$ in $Cl(\mathcal{O})$ (by $(*)$ on page 25), hence $j((S')^{-1}I) = j(S^{-1}I)$

Proof. Let $L/K$ be a Gal ext. s.t. $L \supseteq K_f$, $L \supseteq j(E_1), \dots,$ $j(E_n)$. Consider primes $p \in \mathbb{Z}$ s.t.

1 • $E_1, \dots, E_n$ have good red. at (the primes of $\mathcal{O}_L$ over) $p$

2 • $(p, f) = 1$

3 • $N(\tilde{q}) = p$

4 • $\tilde{q}$ unram. in $L$

5 • $\left(\frac{L/K}{\tilde{q}}\right)$ = conj. class of $\sigma|_L$

( that is, $\exists\, Q \mid \tilde{q}$ in $\mathcal{O}_L$ s.t. $\left(\frac{L/K}{Q}\right) = \sigma|_L$ )

$$\begin{tikzcd}
L \arrow[d, dash] & \mathcal{O}_L \arrow[d, dash] & \\
K \arrow[dd, dash] & \mathcal{O}_K \arrow[d, dash] & \tilde{q} = q\mathcal{O}_K \arrow[d, dash] \\
 & \mathcal{O} \arrow[d, dash] & q \arrow[d, dash] \\
\mathbb{Q} & \mathbb{Z} & p
\end{tikzcd}$$

There exist $\infty$ly many such primes: 1, 2, 4 rule out finitely many primes; 3+5 we get from Chebotarev.

Take such a prime $p$.

$$\sigma(j(I)) \underset{\substack{\uparrow \\ \sigma|_L = \left(\frac{L/K}{Q}\right) \\ j(I)\in \mathcal{O}_L}}{\equiv} j(I)^p \underset{\substack{\uparrow \\ \text{thm. proved} \\ \text{last time}}}{\equiv} j(\mathfrak{q}^{-1} I) \mod Q$$

Recall that $\left(\frac{L/K}{Q}\right) = \sigma|_L \Rightarrow$

$$\begin{array}{c} \left(\frac{K_f/K}{Q\cap \mathcal{O}_{K_f}}\right) \\ \shortparallel \\ \left(\frac{K_f/K}{\tilde{\mathfrak{q}}}\right) \end{array} = \sigma|_{K_f} = \left(\frac{K_f/K}{\mathfrak{q}}\right)$$

So our $q$ works as an $S$ in the statement (in the sense that $\left(\frac{K_f/K}{q}\right) = \sigma|_{K_f}$

For different primes $p$, get the same congruence for different primes $Q$, which implies $\sigma(j(I)) = j(q^{-1}I)$

$\ulcorner$ Easier: just take a $p$ s.t. $p \nmid N_{L/\mathbb{Q}}\left(\prod_{i\neq j}(j(E_i)-j(E_j))\right)$ $\lrcorner$

**Corollary** $K_f = K(j(I))$ for $I \in I(\mathcal{O})$ (equivalently, $K_f = K(j(E))$ for any $E \in \mathcal{E}ll(\mathcal{O})$)

**Proof.** By Galois theory, it suffices to show that $\forall \sigma \in Gal(\overline{\mathbb{Q}}/K)$

$$\sigma|_{K_f} = id \iff \sigma(j(I)) = j(I)$$

Now $\sigma(j(I)) = j(S^{-1}I)$, where $\left(\frac{K_f/K}{S}\right) = \sigma|_{K_f}$

So $\sigma(j(I)) = j(I) \iff j(I) = j(S^{-1}I)$

$\iff [S] = 1$ in $Cl(\mathcal{O})$

$\iff \left(\frac{K_f/K}{S}\right) = \sigma|_{K_f} = id$ $\square$

## A "complete" picture

$$\begin{tikzcd} & \phi_K : \dfrac{I_K}{P_K} \arrow[r] & \mathrm{Gal}(K_1/K) \\ I_K(f\mathcal{O}_K) \arrow[urr, "\text{Artin rec}"] & & \end{tikzcd}$$

$$\ker = P_K \cap I_K(f\mathcal{O}_K) \supseteq P_{K,\mathbb{Z}}(f\mathcal{O}_K)$$

$$\Downarrow$$

$$\mathrm{Gal}(K_f/K) = \mathcal{C}l(\mathcal{O}) \simeq \frac{I_K(f\mathcal{O}_K)}{P_{K,\mathbb{Z}}(f\mathcal{O}_K)} \twoheadrightarrow \frac{I_K(f\mathcal{O}_K)}{P_K \cap I_K(f\mathcal{O}_K)} \simeq \mathcal{C}l_K = \mathrm{Gal}(K_1/K)$$

Hence $K_1 \subseteq K_f$, and $\mathrm{Gal}(K_f/K_1) \simeq \dfrac{P_K \cap I_K(f\mathcal{O}_K)}{P_{K,\mathbb{Z}}(f\mathcal{O}_K)}$

**Prop.** Assume $K \neq \mathbb{Q}(i), \mathbb{Q}(\zeta_3)$. $(\Rightarrow \mathcal{O}_K^\times \simeq \{\pm 1\})$

There is an exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \left(\mathbb{Z}/f\mathbb{Z}\right)^\times \arrow[r] & \left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times \arrow[r, two heads] & \dfrac{P_K \cap I_K(f\mathcal{O}_K)}{P_{K,\mathbb{Z}}(f\mathcal{O}_K)} \arrow[r] & 1 \\
 & & {[\alpha]} \arrow[r, mapsto] & {[\alpha \mathcal{O}_K]} &
\end{tikzcd}$$

and this induces

$$\frac{\left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times}{\left(\mathbb{Z}/f\mathbb{Z}\right)^\times} \xrightarrow{\sim} \mathrm{Gal}\left(K_f/K_1\right)$$

**Rmk** In particular, this gives a formula for $\# \mathcal{Cl}(\mathbb{Z} + f\mathcal{O}_K)$.

**Prop.**

$$\begin{tikzcd} K_f \arrow[d, dash, "\mathcal{C}\ell(\mathcal{O})"] \\ K \arrow[d, dash, "\{id, \tau\}"] \\ \mathbb{Q} \end{tikzcd}$$

$K_f$ is Galois, with group

$$\mathrm{Gal}(K_f/\mathbb{Q}) \simeq \mathrm{Gal}(K_f/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

the action being given by

$$\tau\sigma\tau^{-1} = \sigma^{-1} \quad \forall \sigma \in \mathrm{Gal}(K_f/K)$$

**Summary**

$$\begin{tikzcd} K_f \arrow[d, dash] \arrow[dd, dash, bend right=50, "\mathcal{C}\ell(\mathcal{O})"'] \arrow[ddd, dash, bend left=60, "\mathcal{C}\ell(\mathcal{O}) \rtimes \{1, \tau\}"] \\ K_1 \arrow[d, dash, "\mathcal{C}\ell(\mathcal{O}_K)"] \\ K \arrow[d, dash, "\{1, \tau\}"] \\ \mathbb{Q} \end{tikzcd}$$

# Modular curves and their function fields

28/10/2022
A. Gallese

$\mathbb{H} = \{ z \in \mathbb{C} \mid \Im z > 0 \}$

$SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by

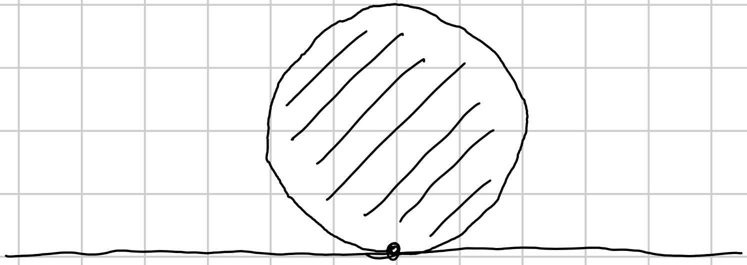
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

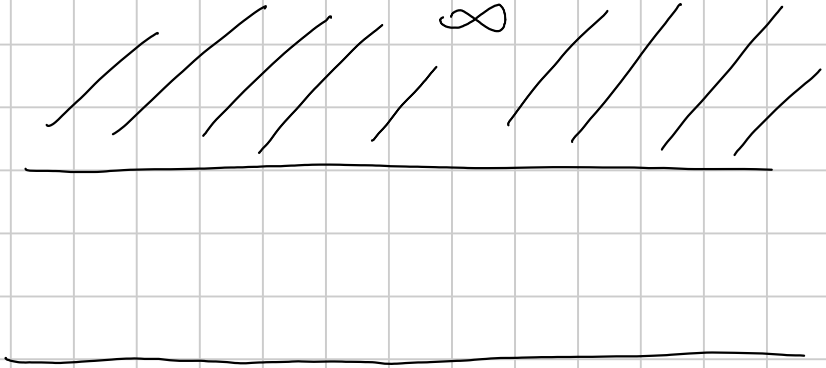
It is secretly an action on the set of lattices in $\mathbb{C}$.

$\mathbb{H}/SL_2(\mathbb{Z}) =: Y(1) \simeq \mathbb{C}$

## Compactification

Let $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. The Topology is generated by the usual opens, together with





$\{q\} \cup$ open disc tg at $q$ to the real line

We set $X(1) := \mathbb{H}^* / SL_2(\mathbb{Z})$. It has a unique reasonable complex structure, which makes it into a compact Riemann surface isomorphic to $\mathbb{P}^1$.

Rmk $\{\pm Id\}$ acts trivially.

## Congruence subgroups

I think the std notation is in fact $\Gamma(1) = SL_2(\mathbb{Z})$

**Def.** $\Gamma(1) := SL_2(\mathbb{Z}) / \{\pm 1\}$

$\Gamma(N) := \left(\text{image in } \Gamma(1) \text{ of}\right) \ker\left(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/_N\mathbb{Z})\right)$

A CONGRUENCE SUBGROUP is a subgroup $\Gamma$ of $\Gamma(1)$ containing $\Gamma(N)$ for some $N \geqslant 1$.

**Def.** The modular curve corresponding to $\Gamma$ is the quotient $X(\Gamma) := \mathbb{H}^* / \Gamma$. It is a compact Riemann surface, and comes equipped with a natural ramified covering map

$$X(\Gamma) \longrightarrow X(1)$$

## Modular forms

A MODULAR FORM OF WEIGHT 2K FOR $\Gamma$ is a function

$f : \mathbb{H} \longrightarrow \mathbb{C}$ s.t.

(i) $f$ is holomorphic on $\mathbb{H}$

(ii) $f$ is holomorphic at the cusps

(iii) $f(\gamma \cdot z) = (cz+d)^{2K} f(z) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Def. Two more important groups:

$$\Gamma_1(N) = \left\{ \gamma \in \Gamma(1) \ : \ \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

$$\Gamma_0(N) = \left\{ \gamma \in \Gamma(1) \ : \ \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$$

## Tower of modular curves

$$\frac{SL_2(\mathbb{Z}/_N\mathbb{Z})}{\pm id}\left\{\begin{array}{l} \left.\begin{array}{c} X(N)\\ |\\ X_1(N)\end{array}\right\}\ \mathbb{Z}/_N\mathbb{Z} \\ \left.\begin{array}{c} |\\ X_0(N)\end{array}\right\}\ (\mathbb{Z}/_N\mathbb{Z})^\times \\ \begin{array}{c}|\\ X(1)\end{array}\end{array}\right.$$

## Examples of modular forms

$$g_2(z) = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^4} \quad \text{is modular of weight } 4 \text{ for } \Gamma(1)$$

$$g_3(z) = 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^6} \quad \text{'' '' '' '' } 6 \text{ '' ''}$$

$$\Delta(z) = g_2(z)^3 - 27\, g_3(z)^2$$

$j(z) := 1728 \dfrac{g_2^3}{\Delta}$ of weight 0 : $j$ is a genuine function on $X(1)$.

**Thm** $j : X(1) \longrightarrow \mathbb{P}^1(\mathbb{C})$ has degree 1, hence is an isomorphism.

$\Rightarrow \mathbb{C}(X(1)) = \mathbb{C}(j)$

**Def.** For $v \in \mathbb{Z}^2$, $v = (c, d)$, we define

$$f^v(\tau) := \frac{g_2(\tau)}{g_3(\tau)}\, \wp_\tau\left(\frac{c\tau + d}{N}\right)$$

where $\wp_\tau$ is the Weierstrass $\wp$ - function with parameter $\tau$.

**Thm.** • $f^v(\tau)$ is $\Gamma(N)$-mod. of weight 0, that is, it's a meromorphic function on $X(\Gamma)$

• $f^v(\tau) = f^w(\tau) \iff v \equiv \pm w \pmod N$

**Pf of part 2** $f^v = f^w \iff \wp_\tau\left(\frac{c_v\tau + d_v}{N}\right) = \wp_\tau\left(\frac{c_w\tau+d_w}{N}\right)$

$$\iff \frac{c_v\tau + d_v}{N} \equiv \pm\left(\frac{c_w\tau+d_w}{N}\right) \mod \mathbb{Z}\oplus\mathbb{Z}\tau$$

(indeed, $\wp_\tau(z) = \wp_\tau(z') \iff z \equiv \pm z' \mod \mathbb{Z}\oplus\mathbb{Z}_\tau$) ☐

**Thm.** $\mathbb{C}(X(N)) = \mathbb{C}(j, \{f^v\})$

**Proof.** We already know $\supseteq$. Now, $\mathbb{C}(X(N)) \supseteq \mathbb{C}(j)$

is Galois with group $SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$.

Let $H$ be the subgroup fixing $f^v(\tau)$ $\forall v$.

One checks easily on the definitions that

$$\gamma \circ f^v(\tau) = f^{v \cdot \gamma}(\tau)$$

Hence $H = \{id\}$, and $\mathbb{C}(j, f^v(\tau)) = \mathbb{C}(X(N))^H = \mathbb{C}(X(N))$.

$\llcorner$ indeed: if $v \cdot \gamma \equiv \pm v \ (N)$ for all $v$, then $\gamma = \pm id$.

Rmk Moreover, $SL_2(\mathbb{Z}/N\mathbb{Z})/_{\{\pm 1\}}$ acts transitively on

$$\frac{(\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}}{\pm 1}$$

$\square$

In an almost identical way, one proves that

$$\mathbb{C}(X_1(N)) = \mathbb{C}\left(j, \ f^{(0,i)} \quad i = 1, \dots, N-1\right);$$

in a different way (but we're not doing it) one can also show $\mathbb{C}\left(X_0(N)\right) = \mathbb{C}\left(j(z), j(Nz)\right)$

## Another description of $\mathbb{C}(X(N))$

Let $E_\tau : \quad y^2 = 4X^3 - g_2(\tau)X - g_3(\tau) \quad \simeq \quad \mathbb{C}/_{\mathbb{Z}\oplus\mathbb{Z}\tau}$.

Under $(x,y) \longmapsto (u^2 x, u^3 y)$ for $u = \sqrt{\dfrac{g_3(\tau)}{g_2(\tau)}}$,

$$E_\tau \simeq \quad y^2 = 4X^3 - \frac{g_2(\tau)^3}{g_3(\tau)^2}X - \frac{g_2(\tau)^3}{g_3(\tau)^2}$$

that is, $$y^2 = 4x^3 - \frac{27\, j(\tau)}{j(\tau) - 1728} x - \frac{27\, j(\tau)}{j(\tau) - 1728}$$

We consider this as an elliptic curve, called $E_j$, over the function field $\mathbb{C}(j)$.

The uniformisation map $\mathbb{C} \longrightarrow E_j$ is

$$z \longmapsto \left( \frac{g_3(\tau)}{g_2(\tau)} \wp_\tau(z), \left(\frac{g_3(\tau)}{g_2(\tau)}\right)^{3/2} \wp_\tau(z) \right)$$

In particular, N-torsion pts have x-coord

$$\frac{g_3(\tau)}{g_2(\tau)} \wp_\tau\left(\frac{a\tau + b}{N}\right) = f^{(a,b)}(\tau)$$

This directly implies that the $f^{(a,b)}(\tau)$ are the x-coords of the N-torsion pts of $E_j$. Hence we can write

$$\mathbb{C}(X(N)) = \mathbb{C}(j, \{f^v\}) = \mathbb{C}(j, x(E_j[N]))$$

what about $\mathbb{C}(j, E_j[N])$ ?

$$\begin{tikzcd}
\mathbb{C}(j, E_j[N]) \arrow[d, dash] \arrow[dd, bend right=60, dash, "H"'] \\
\mathbb{C}(j, x(E_j[N])) \arrow[d, dash] \arrow[d, bend left=60, dash, "SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm id\}"] \\
\mathbb{C}(j)
\end{tikzcd}$$

Let $H := \mathrm{Gal}\left( \mathbb{C}(j, E_j[N]) \,/\, \mathbb{C}(j) \right)$. There is a faithful representation $\rho : H \hookrightarrow \mathrm{Aut}\, E_j[N] \simeq GL_2(\mathbb{Z}/N\mathbb{Z})$

We assume the existence of the Weil pairing. Then

$$\zeta_N = \zeta_N^{\sigma} = e(P, Q)^{\sigma} = e\left(\rho(\sigma) P, \rho(\sigma) Q\right) =$$

$$= e(P,Q)^{\det \rho(\sigma)} \implies \det \rho(\sigma) = +1$$

Hence $H \hookrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$. In particular,

letting $K := \mathrm{Gal}\left( \mathbb{C}(j, E_j[N]) \,/\, \mathbb{C}(j, x(E_j[N])) \right)$,

we have $|K| \leq 2$. Note that $|K| = 2 \iff -\mathrm{id} \in K$, and one concludes easily that

**Thm** $\mathrm{Gal}\left(\mathbb{C}(j, E_j[N]) / \mathbb{C}(j)\right) \simeq SL_2(\mathbb{Z}/N\mathbb{Z})$

## Descending to $\mathbb{Q}$

**Thm**

$$\left.\begin{array}{c} \mathbb{Q}(j, E_j[N]) \\ \Big| \\ \mathbb{Q}(j) \end{array}\right\} \text{Galois w/ group } GL_2(\mathbb{Z}/N\mathbb{Z})$$

**Proof.** We begin by showing that $\mu_N \subseteq \mathbb{Q}(j, E_j[N])$.
Let $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(j, E_j[N], \mu_N) / \mathbb{Q}(j, E_j[N])\right)$. Then

$$\zeta_N^{\sigma} = e(P,Q)^{\sigma} = e(P^{\sigma}, Q^{\sigma}) = e(P,Q) = \zeta_N,$$

so $\sigma$ fixes $\zeta_N$ $\Rightarrow$ $\sigma$ is the identity $\Rightarrow$ the Galois group is trivial $\Rightarrow$ $\mathbb{Q}(j, E_j[N], \mu_N) = \mathbb{Q}(j, E_j[N])$

Next we consider $\mathbb{C}(j, E_j[N])$

$$\begin{tikzcd}
 & \mathbb{C}(j, E_j[N]) \arrow[dl, dash, "{\text{Gal} \simeq SL_2(\mathbb{Z}/N\mathbb{Z}) \text{ as previously shown}}"'] \arrow[dr, dash] & \\
\mathbb{C}(j) \arrow[dr, dash] & & \mathbb{Q}(j, E_j[N]) \arrow[dl, dash, "{SL_2(\mathbb{Z}/N\mathbb{Z}) \text{ by Galois theory}}"] \\
 & L = \mathbb{C}(j) \cap \mathbb{Q}(j, E_j[N]) \arrow[d, dash] & \\
 & \mathbb{Q}(j, \mu_N) \arrow[d, dash, "{\text{Gal} \simeq (\mathbb{Z}/N\mathbb{Z})^{\times}}"] & \\
 & \mathbb{Q}(j) &
\end{tikzcd}$$

On the other hand,

$$\begin{tikzcd} \mathrm{Gal}\Big(\mathbb{Q}(j, E_j[N]) / \mathbb{Q}(j, \mu_N)\Big) \arrow[r, hook, "\rho"] \arrow[dr, dashed] & GL_2(\mathbb{Z}/N\mathbb{Z}) \\ & SL_2(\mathbb{Z}/N\mathbb{Z}). \arrow[u, phantom, "\rotatebox{90}{$\subseteq$}"] \end{tikzcd}$$

by the usual computation:

$$\zeta_N = \zeta_N^{\sigma} = e(P,Q)^{\sigma} = e(\sigma P, \sigma Q) = e(P,Q)^{\det \rho(\sigma)}$$
$$= \zeta_N^{\det \rho(\sigma)}$$

Hence $SL_2(\mathbb{Z}/N\mathbb{Z}) \subseteq \mathrm{Gal}\Big(\mathbb{Q}(j, E_j[N]) / \mathbb{Q}(j, \mu_N)\Big) \subseteq SL_2(\mathbb{Z}/N\mathbb{Z})$.

By cardinality, $\mathrm{Gal}\big(\mathbb{Q}(j, E_j[N]) / \mathbb{Q}(j)\big) \simeq GL_2(\mathbb{Z}/N\mathbb{Z})$

(note that $\mathrm{Gal} \hookrightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$ by the usual rep'n) $\square$

# Fields of def'n of modular curves.

Let $K$ be an intermediate field, corresponding to a subgroup $H$ of $\mathrm{Gal}\left(\mathbb{Q}(j, E_j[N]) / \mathbb{Q}(j)\right)$. Then

$$K \cap \overline{\mathbb{Q}} = \mathbb{Q}(\mu_N)^{\det \rho(H)}$$

The reason is the diagram

$$\begin{tikzcd}
 & & \mathbb{Q}(j, E_j[N]) \arrow[d, dash] \arrow[ddl, dash] \arrow[ddr, dash] & & \\
GL_2(\mathbb{Z}/N\mathbb{Z}) \arrow[ddrr, "\det"] & & K \arrow[dl, dash] & & \overline{\mathbb{Q}} \\
 & \mathbb{Q}(j) \arrow[ddr, dash] & & \mathbb{Q}(\mu_N) \arrow[ur, dash] \arrow[dr, dash] \arrow[ddl, dash] & \\
 & & (\mathbb{Z}/N\mathbb{Z})^\times & & \mathbb{Q}(\mu_N) \cap K \arrow[dll, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Stuff happened (see notes on website)

2/12/2022
L. Speciale

# Heegner points Euler system

Ref. Knapp - Elliptic curves

Milne - Modular forms & mod. functions

Diamond - Shurman - A first course in modular forms

## 1. The Eichler-Shimura construction

Recall A MODULAR PARAMETRIZATION is a finite $\mathbb{Q}$-morphism

$$F : X_0(N) \longrightarrow E$$

F is minimal if $\nexists$ $M<N$ and $F' : X_0(M) \longrightarrow E$ finite

Rmk. Non-minimal parametrisations exist:

$$X_0(NN') \twoheadrightarrow X_0(N) \longrightarrow E$$

- Being modular of level $N$ is invariant under isogeny

**Prop.** If $\omega$ is an invariant differential on $E$, $F^*\omega$ on $X(N)$ is a cusp form w/ integral$^{\star}$ coeffs that is a weak eigenform, that is, $T_n f = a_n f \quad \forall n$ s.t. $(n, N) = 1$

**Thm** Let $f(\tau) = \sum_{n \geqslant 1} a_n q^n$ be a cusp form (with integral coefficients) for $\Gamma_0(N)$, with $a_1 = 1$. Assume $f$ is a strong eigenform ( $T_n f = f \quad \forall n$, including $(n, N) > 1$ ). Then

a) There exists a pair $(E, \nu)$, where $E/\mathbb{Q}$ is an ell.

---

$\star$ certainly rational. Once it's normalised, it's integral curve and $\nu : J(X_0(N)) \longrightarrow E$ is a $\mathbb{Q}$-morphism that exhibits $E$ as a quotient of $J(X_0(N))$ by a codimension - 1 subvariety $A$ of $J_0(N)$

b) $T_n$ stabilises $A$ and acts as mult. by $a_n$ on $E$

c) $\omega$ pulls back to a scalar multiple of $f$

d) (Igusa) We have

$$a_\ell = \ell + 1 - \# E(\mathbb{F}_\ell)$$

with at most finitely many exceptions.

Cor. $L(f, s) \doteq L(E, s)$ up to fin'ly many primes

## Sketch of the construction

$$\mathbb{T} := \mathbb{T}_{\mathbb{Z}} := \mathbb{Z}[T_n \mid n \in \mathbb{Z}] \curvearrowright J_0(N)$$

$$I_f := \{T \in \mathbb{T}_{\mathbb{Z}} \mid Tf = 0\} = (T_n - a_n T_1)_{n \geqslant 1}$$

Set

$$A_f := \frac{J_0(N)}{I_f J_0(N)}.$$

Then $\dim A_f = [K_f : \mathbb{Q}] = 1$, where $K_f = \mathbb{Q}(\{a_n\})$

[This needs to be amended if $K_f \neq \mathbb{Q}$, but we are in that situation]

**Newforms** Notice that there are injections

$$\iota_{r_1,r_2} : S_2\left(\Gamma_0(N)\right) \hookrightarrow S_2\left(\Gamma_0\left(\frac{N}{r_1 r_2}\right)\right) \qquad r_1, r_2 > 1$$

$$f(\tau) \longmapsto f(r_2\tau)$$

We call $S_2(\Gamma_0(N))^{old} = \sum_{\substack{r_1,r_2 \mid N \\ r_1 r_2 > 1}} \iota_{r_1,r_2} \, S_2\left(\Gamma_0\left(\frac{N}{r_1 r_2}\right)\right)$

and $S_2(\Gamma_0(N))^{new}$ = the orthogonal complement wrt Petersson of $S_2(\Gamma_0(N))^{old}$.

Thm (Atkin-Lehner) $f \in S_2(\Gamma_0(N))^{new}$, $f$ weak eigenform $\Rightarrow$ $f$ strong eigenform.

Thm (Carayol) In the notation above, $L(E,s) = L(f,s)$

Can identify the primes of bad reduction of E as being precisely the prime divisors of $E$

**Prop.** The following are equivalent:

(1) $F : X_0(N) \longrightarrow E$ is a minimal param.

(2) $E$ has conductor $N$

(3) $F$ factors via a modular parametrisation coming from the Eichler-Shimura construction, composed with a $\mathbb{Q}$-isogeny

## §2. Verification of the axioms of Euler system

$K/\mathbb{Q}$ imaginary quadratic field of disc. $D$

$N = \mathcal{N}\overline{\mathcal{N}}$ and $p \mid N \Rightarrow p$ splits in $K$

$\varphi : X_0(N) \longrightarrow E$ $E/\mathbb{Q}$ an ell. curve

$n = \prod \ell$, $\ell$ distinct, $(n, DN) = 1$

$\mathcal{O}_n$ = order of conductor $n$

$\mathrm{Pic}\ \mathcal{O}_n = \mathrm{Gal}(K_n/K)$

Define $G_\ell = \mathrm{Gal}(K_n/K_{n/\ell})$ $G_n = \prod_{\ell \mid n} G_\ell$

$x_n$ "=" $\left( j(\mathbb{C}/\mathcal{O}_n), j(\mathbb{C}/\mathcal{N}_n^{-1}) \right) \in X_0(N)(K_n)$

( that is, the pt corresponding to $\mathbb{C}/\mathcal{O}_n \longrightarrow \mathbb{C}/\mathcal{N}_n^{-1}$ )

$y_n = \mathrm{Tr}_{K_n/K}\ \varphi(x_n)$

**Lemma** $n = \ell \cdot m$, $\ell$ prime. Then

$$Tr_\ell(x_n) = T_\ell(x_m) \qquad \Big( Tr_\ell := \sum_{\sigma \in G_\ell} \sigma \Big)$$

as divisors on $X_0(N)$

**Proof** $1 \to G_\ell \to G_n \to G_m \to 1$

There is an isomorphism $\mathrm{Pic}\, \mathcal{O}_n \xrightarrow{\sim} \mathrm{Gal}(K_n/K)$

$$\sigma \longmapsto a_\sigma$$

s.t. $[a_\sigma] * E = E^\sigma$ [ DIFFERENT CONVENTION THAN THE FIRST LECTURES! ]

Given $a_\sigma$ for $\sigma$ in $G_\ell$, $a_\sigma \mathcal{O}_m = \alpha \mathcal{O}_m$ $\alpha \in K^\times$

$\rightsquigarrow$ change $\sigma$ in its class, so that $a_\sigma \mathcal{O}_m \subseteq \mathcal{O}_m$

and $[\mathfrak{a}_\sigma : \mathcal{O}_m] = \ell$.

$$\mathrm{Tr}_\ell \, x_m = \sum_{\sigma \in G_\ell} \left( {}^\sigma j(\mathbb{C}/\mathcal{O}_m), \, {}^\sigma j(\mathbb{C}/\mathfrak{N}_n^{-1}) \right)$$

$$= \sum_{\sigma \in G_\ell} \left( j(\mathbb{C}/\mathfrak{a}_\sigma), \, j(\mathbb{C}/\mathfrak{a}_\sigma \mathfrak{N}_n^{-1}) \right)$$

Last time: $|G_\ell| = \ell + 1$. Moreover, $(\mathfrak{a}_\sigma)$ is an $\ell$-overlattice of $\mathcal{O}_m$. Hence, since the summands are all distinct (since $\mathrm{Pic}^\circ \curvearrowright$ simply transitively),

$$= \sum_{\substack{C \\ \ell\text{-subgp}}} \left( j(\mathbb{C}/\mathcal{O}_m + C), \, j(\mathbb{C}/\mathfrak{N}_n^{-1} + C) \right)$$

**Proposition** (Gross 3.7) We have

(a) $\mathrm{Tr}_\ell \, y_n = a_\ell \, y_m$ in $E(K_m)$

(b) If $\lambda_m$ lies over $\ell$ in $\mathcal{O}_{K_m}$, then $\exists! \, \lambda_n \mid \lambda_m$ in $\mathcal{O}_{K_n}$ and

$$y_n \equiv \mathrm{Frob}(\lambda_m \mid \ell)(y_m) \pmod{\lambda_n}$$

**Proof** For (a), use Eichler-Shimura construction (b) and the previous lemma.

For (b), note that $\lambda_m$ is in the kernel of the Artin map for $K_m/K$, so $\lambda_1$ splits completely in $K_m$.

On the other hand $K_n/K_m$ is tot. ramified at $\lambda_m$, so $\lambda_m \mathcal{O}_{K_n} = \lambda_n^{\ell+1}$

Now $\mathrm{Tr}_\ell\, x_n = \sum_{\sigma \in G_\ell} x_n^{\sigma} \equiv (\ell+1)\, x_n \pmod{\lambda_n}$

since $\sigma$ acts trivially on the residue field $\mathcal{O}_{K_n}/\lambda_n = \mathcal{O}_{K_m}/\lambda_m$.

- $\mathrm{Frob}(\lambda_m | \ell) \equiv \mathrm{Fr}_\ell \pmod{\lambda_m}$
- $\mathrm{Fr}_\ell^2 = \mathrm{id}$ on $\mathbb{F}_\lambda \Rightarrow \hat{\mathrm{Fr}}_\ell = \ell \cdot \mathrm{Fr}_\ell^{-1} = \ell \cdot \mathrm{Fr}_\ell$

Hence: $(\ell+1)\, x_n \equiv \mathrm{Tr}_\ell\, x_n \equiv T_\ell\, x_m \underset{\substack{| \\ \text{Eichler} \\ \text{Shimura}}}{\equiv} (\ell+1)\, \mathrm{Fr}_\ell(x_m) \equiv$

$(\ell+1)\, \mathrm{Frob}(\lambda_m | \ell)(x_m) \mod \lambda_n$

$\Rightarrow x_n \equiv \mathrm{Frob}(\lambda_m | \ell)(x_m) \mod \lambda_n \rightsquigarrow$ apply $\varphi$. $\square$

09/12/2022
L. Stefanello

# Construction of cohomology classes

1. Crash course on profinite cohomology (Wilson, "Profinite gps")
2. Kolyvagin's cohomology classes

## §1. Cohomology

$G$ = profinite group (i.e., Galois groups)

$A$ = (discrete) $G$-module, i.e., the action of $G$ on $A$ is continuous for the discrete topology on $A$

Rmk. $A$ discrete $\iff$ $\forall a \in A$, $\mathrm{Stab}_G(a)$ is open

Ex. $K$ a nb. field, $\underbrace{K \subseteq L}_{\text{finite}} \subseteq \overline{K}$, $G = \mathrm{Gal}(L/K)$,

$E$ an ell. curve $/ K$. Then $E(L)$, $E(L)[p]$ are $G$-modules ( and they're discrete - we won't repeat this every time)

Construction

$\forall n \geq 0$, $C^n(G, A) = \{ f : G^n \longrightarrow A \text{ contin.} \}$ ; $C^0(G,A) = A$

There are differentials $d_n : C^{n-1} \longrightarrow C^n$.

We call $Z^n(G, A) = \ker d_{n+1}$ the COCYCLES

and $B^n(G,A) = \operatorname{Imm} d_n$ the COBOUNDARIES

Def. $H^n(G,A) = Z^n(G,A) / B^n(G,A)$

Ex $H^0(G,A) = \{a \in A \mid g \cdot a - a = 0\} = A^G$

$$H^1(G,A) = \frac{\{f : G \to A \mid f(g_1 g_2) = f(g_1) + g_1 \cdot f(g_2)\}}{\{f : G \to A \mid \exists a \in A : f(g) = g \cdot a - a\}}$$

We will think of $H^n(G,A)$ in general as equivalence classes, modulo a certain relation, of functions $G^n \longrightarrow A$

## Functoriality / change of group

$G_1, G_2$ prof. groups, $A_1, A_2$ modules for $G_1, G_2$,

$\vartheta : G_2 \longrightarrow G_1$ continuous grp. hom, $\varphi : A_1 \longrightarrow A_2$ grp.

homom. We say that $\vartheta$, $\varphi$ are COMPATIBLE if

$$g \cdot \varphi(a) = \varphi(\vartheta(g) \cdot a) \quad \forall a \in A_1, \quad \forall g \in G_2$$

If $\varphi, \vartheta$ are compatible, we get an induced homom.

$$H^n(G_1, A_1) \longrightarrow H^n(G_2, A_2)$$

$$[f] \longmapsto [\varphi f \vartheta],$$

where $(\varphi f \vartheta)(g_1, \dots, g_n) = \varphi(f(\theta(g_1), \dots, \theta(g_n)))$.

Rmk When $G_1 = G_2 = G$, $A, B$ are $G$-modules, and $\varphi : A \to B$ is a homomorphism, then $(id_G, \varphi)$ are compatible $\iff$ $\varphi$ is $G$-equivariant. When this is the case, we get an induced map

$$\varphi : H^n(G,A) \longrightarrow H^n(G,B)$$

$$[f] \longmapsto [\varphi \circ f]$$

**Thm** Let $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\tau} C \longrightarrow 0$ be a short exact seq. of $G$-modules ( in particular, $\varphi$ and $\tau$ are $G$-equivar.)

We have a long exact sequence

$$0 \to A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \to H^2(G,A) \to \cdots$$

Moreover, given $y \in C^G$, $\exists\ x \in B$ s.t. $\varphi(x) = y$.

Take $f : G \longrightarrow B$ given by $g \longmapsto g \cdot x - x$.

It's easy to see that Imm $f \subset A$; we can then consider it as a map $G \to A$, and its class $[f] \in H^1(G,A)$ is $\delta(y)$

**Thm 2**

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 & \text{s.e.s.} & G_1\text{-mod} \\
0 \arrow[r] & X \arrow[r] & Y \arrow[r] & Z \arrow[r] & 0 & \text{s.e.s.} & G_2\text{-mod} \arrow[u, "\vartheta"']
\end{tikzcd}$$

If $\vartheta$ is compatible with $\alpha, \beta, \gamma$, we get a morphism of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & A^{G_1} \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & B^{G_1} \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & C^{G_1} \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & H^1(G_1,A) \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & H^1(G_1,B) \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & H^1(G_1,C) \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & H^2(G_1,A) \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & X^{G_2} \arrow[r] & Y^{G_2} \arrow[r] & Z^{G_2} \arrow[r] & H^1(G_2,X) \arrow[r] & H^1(G_2,B) \arrow[r] & H^1(G_2,C) \arrow[r] & H^2(G_2,A) \arrow[r] & \cdots
\end{tikzcd}$$

## Some important compatible pairs

$G$ a profinite group, $A$ a $G$-module, $H \leq G$ a closed subgp.

① $\vartheta : H \hookrightarrow G$, $\mathrm{id} : A \longrightarrow A$ is compatible

$\rightsquigarrow$ get restriction maps $H^n(G, A) \longrightarrow H^n(H, A)$

② $H \triangleleft G$, $\theta : G \twoheadrightarrow G/H$ the canonical projection,

$\varphi : A^H \hookrightarrow A$. Then $(\vartheta, \varphi)$ is compatible, and we get INFLATION maps $\inf : H^n(G/H, A^H) \longrightarrow H^n(G, A)$

③ $H \triangleleft G$. Fix $x \in G$. $\theta : \begin{array}{l} H \longrightarrow H \\ h \longmapsto x^{-1}hx \end{array}$ $\quad \varphi : \begin{array}{l} A \longrightarrow A \\ a \longmapsto xa \end{array}$

$(\vartheta, \varphi)$ is compatible

$\rightsquigarrow$ get $\bar{x} : H^n(H,A) \to H^n(H,A)$

$\Rightarrow H^n(H,A)$ is a $G/H$ - module

**Thm** (5-terms short exact sequence) There is an exact sequence

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A)^{G/H} \to H^2(G/H, A^H) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^2(G,A)$$ is exact

**Example**

$K$ a nb. field, $\underbrace{K \subseteq L}_{\text{fin. Gal.}} \subseteq \overline{K}$, $G = \mathrm{Gal}(\overline{K}/K)$, $H = \mathrm{Gal}(\overline{K}/L)$

$E/K$ an ell. curve, $A = E(\overline{K})$. The 5-terms SES gives

$$0 \longrightarrow H^1\big(\mathrm{Gal}(L/K), E(L)\big) \xrightarrow{\mathrm{inf}} H^1\big(\mathrm{Gal}(\overline{K}/K), E(\overline{K})\big) \xrightarrow{\mathrm{res}}$$
$$H^1\big(\mathrm{Gal}(\overline{K}/L), E(\overline{K})\big) \longrightarrow H^2\big(\mathrm{Gal}(L/K), E(L)\big) \to \dots$$

## Notation

We write $H^n(K, -)$ for $H^n\big(\mathrm{Gal}(\overline{K}/K), -\big)$ and

$H^n(L/K, -)$ for $H^n\big(\mathrm{Gal}(L/K), -\big)$

## §2. Cohomology classes

**Setup.**

- $E/\mathbb{Q}$ an ell. curve without CM, $\varphi : X_0(N) \longrightarrow E$, $\infty \mapsto 0$
- $K$ quadr. imag., $D := \mathrm{disc}\, K \neq -3, -4$
- Heegner condition: $p \mid N \Rightarrow p$ split in $K$
- $p$ odd, large enough that $\mathrm{Gal}\left( \mathbb{Q}(E[p]) / \mathbb{Q} \right) = GL_2(\mathbb{Z}/p\mathbb{Z})$
- $n$ sqrfree, $n = \prod \ell$, $(\ell, D \cdot N \cdot p) = 1$
- $\left( \frac{K(E[p])/\mathbb{Q}}{\ell} \right) \ni$ complex conjugation $(\Leftrightarrow p \mid \ell + 1)$

- $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ the order of conductor $n$

  $\rightsquigarrow K_n$ the ring class field

- Have Heegner pts $x_n \in X_0(N)(K_n) \rightsquigarrow y_n \in E(K_n)$

  $$y_n = \varphi(x_n)$$

- $G_n = \mathrm{Gal}(K_n/K_1)$, $\quad G_n = \prod G_\ell$ with

  $$G_\ell = \mathrm{Gal}(K_n/K_{n/\ell}) \cong \mathrm{Gal}(K_\ell/K)$$

  cyclic of order $\ell+1$. Fix a generator $\sigma_\ell$.

- $D_\ell = \sum_{i=1}^{\ell} i\,\sigma_\ell^i \in \mathbb{Z}[G_n]$, $\qquad D_n := \prod_{\ell \mid n} D_\ell \in \mathbb{Z}[G_n]$

- $D_n y_n \in E(K_n)$ and the class $[D_n Y_n] \in \left(\frac{E(K_n)}{pE(K_n)}\right)$ is $G_n$ - invariant

## New constructions

$$\begin{tikzcd} K_n \arrow[d, dash] \arrow[d, dash, bend left=60, "G_n"] \arrow[dd, dash, bend left=80, "\mathcal{G}_n"] \\ K_1 \arrow[d, dash] \\ K \end{tikzcd}$$

Let $S$ be a set of representatives for $G_n$ in $\mathcal{G}_n$.

Set $P_n = \sum_{\sigma \in S} \sigma(D_n Y_n)$.

The class of $P_n$ is in $\left(\frac{E(K_n)}{pE(K_n)}\right)^{\mathcal{G}_n}$.

Rmk • $[P_n]$ is indep. of the choice of $S$

- $[P_n]$ DOES depend on the choice of the $\sigma_\ell$, but only up to multiplication by a scalar in $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$

$$\begin{tikzcd}
0 \arrow[r] & E(\overline{K})[p] \arrow[r] \arrow[d, "id"] & E(\overline{K}) \arrow[r, "{[p]}"] \arrow[d, "id"] & E(\overline{K}) \arrow[r] \arrow[d, "id"] & 0 & \circlearrowleft G = Gal(\overline{K}/K) \\
0 \arrow[r] & E(\overline{K})[p] \arrow[r] & E(\overline{K}) \arrow[r, "{[p]}"'] & E(\overline{K}) \arrow[r] & 0 & \circlearrowleft H = Gal(\overline{K}/K_n)
\end{tikzcd}$$

The associated morphism of SES is

$$\begin{tikzcd}
E(K) \arrow[r, "{[p]}"] \arrow[d, hook] & E(K) \arrow[r, "\delta"] \arrow[d, hook] & H^1(K, E[p](\overline{K})) \arrow[r] \arrow[d, "Res"] & H^1(K, E(\overline{K})) \arrow[r, "{[p]}"] \arrow[d, "Res"] & H^1(K, E(\overline{K})) \cdots \arrow[d, "Res"] \\
E(K_n) \arrow[r, "{[p]}"] & E(K_n) \arrow[r, "\delta_n"] & H^1(K_n, E[p](\overline{K})) \arrow[r] & H^1(K_n, E(\overline{K})) \arrow[r, "{[p]}"] & H^1(K_n, E(\overline{K})) \cdots
\end{tikzcd}$$

Let us compute the action of $\delta_n$ on $P_n$.

Fix $1/p \, P_n \in E(\overline{k})$ a p-th division pt of $P_n$.

$$\delta_n(P_n) = \left[\sigma \longmapsto \sigma\left(\frac{1}{p} P_n\right) - \frac{1}{p} P_n\right]$$

From the above, we get the short ex. sequences (+ 5-terms ex. sequences) on the next page.

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & 0 = H^1(K_n/K, E(K_n)[p]) \arrow[d, "infl"] & H^1(K_n/K, E(K_n))[p] \arrow[d, "infl"] & \\
0 \arrow[r] & \frac{E(K)}{pE(K)} \arrow[r, "\delta"] \arrow[d] & H^1(K, E[p]) \arrow[r, "\alpha"] \arrow[d, "\wr"] & H^1(K, E)[p] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \left(\frac{E(K_n)}{pE(K_n)}\right)^{G_n} \arrow[r, "\delta_n"'] & \left(H^1(K_n, E[p])\right)^{G_n} \arrow[r] \arrow[d] & \left(H^1(K_n, E)[p]\right)^{G_n} & \\
 & & 0 = H^2(K_n/K, E(K_n)[p]) & &
\end{tikzcd}$$

**Lemma** $E(K_n)[p] = (0)$

↳ which gives the $0$

**Proof** $E(K_n)[p]$ is $\{0\}$, $\mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$.

As $K_n/\mathbb{Q}$ is normal, if $E(K_n)[p] \simeq (\mathbb{Z}/p\mathbb{Z})$, then $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ stabilises $E(K_n)[p]$, contradiction

If $E(K_n)[p] \simeq (\mathbb{Z}/p\mathbb{Z})^2$, we get a surjective map

$$\mathrm{Gal}(K_n/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}\big(\mathbb{Q}(E[p])/\mathbb{Q}\big)$$

$$GL_2(\mathbb{F}_p)$$

but this is plainly impossible (for $p > 3$) since $\mathrm{Gal}(K_n/\mathbb{Q})$ is solvable while $GL_2(\mathbb{Z}/p\mathbb{Z})$ is not

The large commutative diagram makes sense of the following definitions:

**Def** $c(n) \in H^1(K, E[p])$ s.t. $\operatorname{res} c(n) = \delta_n(P_n)$

$d(n) = \alpha(c(n)) \in H^1(K, E)[p]$

$\tilde{d}(n) \in H^1(K_n/K, E(K_n))[p]$ s.t. $\inf \tilde{d}(n) = d(n)$

**Rmk** (Mc Callum) Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We have

① $c(n)$ sends $\sigma$ to $\sigma\left(\frac{1}{p} P_n\right) - \frac{1}{n} P_n - \frac{1}{p}(\sigma - 1) P_n$,

where $\frac{1}{p}(\sigma-1)P_n$ is the unique $x \in E(K_n)$ s.t. $px = (\sigma - 1)P_n$

The uniqueness of $x$ follows from $E(K_n)[p] = (0)$.

Existence follows from the fact that $[P_n]$ is fixed by $\sigma$ in $\left(\frac{E(K_n)}{pE(K_n)}\right)^{G_n}$

② $\tilde{d}(n)$ sends $\sigma$ to $-1/p\,(\sigma-1)P_n$

Proof ①

$$\begin{array}{ccc} \mathrm{Res}\big(c(n)\big) & = & \mathrm{Res}\left(\left[\sigma \mapsto \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{1}{p}(\sigma-1)P_n\right]\right) \\ \| & & \| \circledast \\ \delta_n[P_n] & = & \left[\sigma \mapsto \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n\right] \end{array}$$

$\circledast$ For $\sigma \in \mathrm{Gal}(\bar{K}/K_n)$, $(\sigma-1)P_n = 0$.

② If we work in $E(\bar{K})$ instead of $E(\bar{K})[p]$,

$\sigma \mapsto \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n$ is a coboundary.

Prop. • $c(n) = 0$ in $H^1(K, E[p]) \iff P_n \in pE(K_n)$

( obvious diagram chasing )

• $d(n) = 0$ in $H^1(K, E)[p] \iff \tilde{d}(n) = 0$

$\iff [P_n]$ comes from $\dfrac{E(K)}{pE(K)}$

$\iff P_n \in E(K) + pE(K_n)$

Rmk For $n=1$, we get $P_1 = \mathrm{tr}_{K_1/K}(y_1) \in E(K)$, hence $d(1)$, $\tilde{d}(1)$ vanish, and

$c(1) = 0 \iff P_1 \in pE(K)$

L. Bertoletti
23/01/2023

# L - functions & elliptic curves

Ref. Diamond - Shurman

Two kinds of L - functions :

- $L(f, s)$ for $f \in M_k(\Gamma_0(N))$
- $L(E, s)$ for $E/\mathbb{Q}$ an elliptic curve

## The case of modular forms

As $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, $f \in M_k(\Gamma_0(N))$ satisfies $f(z+1) = f(z)$,

so $f = \sum_{n \geq 0} a_n q^n$ $\left( q = e^{2\pi i z} \right)$

We define $L(s, f) = \sum_{n \geq 1} a_n / n^s$

## The case of elliptic curves

We define $L(E,s) = \prod_p \det\left(\mathrm{Id} - T\cdot \mathrm{Frob}_p^{-1} \,\middle|\, (V_\ell E^\vee)^{I_p}\right)^{-1}_{T=p^{-s}}$

Let $N = N(E)$ be the conductor.

- If $p \nmid N$, the factor at $p$ is $(1 - a_p p^{-s} + p^{1-2s})^{-1}$,
  where $a_p = p+1 - \# \tilde{E}(\mathbb{F}_p)$
- If $p \mid N$, we'll see

## The connection

If $E/\mathbb{Q}$ is modular, $\exists\, f \in S_2(\Gamma_0(N))$ s.t.

$$L(E,s) = L(f,s)$$

## Good properties

① $L(f,s)$ converges absolutely on $\{\mathrm{Re}\ s > K\}$ ( and even $\{\mathrm{Re}\ s > k/2+1\}$ if $f$ is cuspidal)

② $L(f,s)$ admits an Euler product

③ $L(f,s)$ satisfies a functional equation

} if $f$ is "nice"
normalised Hecke eigenform

## L-functions, modular side

**Lemma** $|a_n| \leq C \cdot n^{k-1}$, and $\leq C \cdot n^{k/2}$ if $f$ is cuspidal

**Idea** $M_k(\Gamma_0(N)) = S_k(\Gamma_0(N)) \oplus \mathcal{E}_k(\Gamma_0(N))$

The series in $\mathcal{E}_k(\Gamma_0(N))$ are explicit and satisfy $|a_n| \leq C \cdot n^{k-1}$

For $f \in S_k(\Gamma_0(N))$,

$$a_n = \frac{1}{2\pi i} \int_{|q|=r} f(q)\, q^{-n} \frac{dq}{q} = \int_0^1 f(x+iy)\, e^{-2\pi i n(x+iy)}\, dy$$

Now $\underbrace{y^{k/2} \cdot |f(x+iy)|}_{\substack{\Gamma_0(N)\text{- invariant} \\ +\text{ bounded at } \infty \\ \Rightarrow \text{ bounded}}} \cdot y^{-k/2} \left| e^{-2\pi i n(x+iy)} \right|$, and trivial estimates

$\square$

## Hecke operators

Let $\Delta := GL_2^+(\mathbb{Z})$, $\Gamma := \Gamma_0(N)$. Define the Hecke algebra $H(\Gamma, \Delta) = \mathbb{Z}[\Gamma \backslash^{\Delta} / \Gamma]$, with product

$$(\Gamma \alpha \Gamma) * (\Gamma \beta \Gamma) = \sum_{i,j} \Gamma \alpha \alpha_i \beta \beta_j \Gamma,$$

where $\Gamma \alpha \Gamma = \coprod \Gamma^{\alpha} \alpha_i$, $\Gamma \beta \Gamma = \coprod \Gamma^{\beta} \beta_i$

$\Gamma^{\alpha} = \Gamma \cap \alpha \Gamma \alpha^{-1}$

The Hecke algebra acts on $M_k(\Gamma_0(N))$, $S_k(\Gamma_0(N))$ via

$$f[\Gamma \alpha \Gamma]_k = \sum f[\alpha_i]_k$$

$$f[\beta]_k = (\det \beta)^{k/2} \cdot j(\beta, z)^{-k} f(\beta \cdot z)$$

(If $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\beta \cdot z = \dfrac{az+b}{cz+d}$ and $j(\beta, z) = cz+d$)

These are called the double coset operator.

Def. • $T_p := p^{k/2-1} \cdot [\Gamma_0(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_0(N)]$, $p$ prime

• $T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \mathbb{1}_N(p) T_{p^{r-2}}$ $\qquad \mathbb{1}_N(p) = \begin{cases} 1 & p \nmid N \\ 0 & p \mid N \end{cases}$

• $T_n = \prod_{p^r \| n} T_{p^r}$

Rmk $\displaystyle\sum_{n=1}^{\infty} T_n/n^s = \prod_p \left(1 - T_p p^{-s} + \mathbb{1}_N(p) p^{k-1-2s}\right)^{-1}$ [formally]

**Def.** (Fricke involution) $w_N = \left[\Gamma_0(N) \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \Gamma_0(N)\right]_k$

Note that $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ normalises $\Gamma_0(N)$. It follows easily that

$$w_N f = f\left[\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\right]_K = N^{k/2} \frac{1}{(Nz)^k} f(-1/Nz)$$

**Def** $f \in S_k(\Gamma_0(N))$ is called a (NORMALISED) HECKE EIGENFORM if $\exists \lambda_n \in \mathbb{C}^\times : T_n f = \lambda_n f \quad \forall n$ (and $a_1 = 1$)

**Fact**

- $T_m, T_n$ commute $\forall m, n$

  $T \cdot T^* = T^* T$
- if $(N, n) = 1$, then $T_n$ is a normal operator for a suitable positive-def scalar product (Petersson)

$\Rightarrow$ the $T_n$ for $(n, N) = 1$ are all simultaneously diagonalisable

**Rmk** If $N = dM$, $f \in S_k(\Gamma_0(M)) \Rightarrow \underset{\iota f}{\underset{\shortparallel}{f}} \in S_k(\Gamma_0(N))$

$$f \in S_k(\Gamma_0(M)) \Rightarrow \underset{\iota_d(f)}{\underset{\shortparallel}{f(dz)}} \in S_k(\Gamma_0(N))$$

**Def** A form is OLD if it belongs to

$$\sum_{\substack{dM=N \\ d,M>1}} \iota\left(S_k(\Gamma_0(M))\right) + \iota_d\left(S_k(\Gamma_0(M))\right)$$

$S_k(\Gamma_0(N))^{new}$ = orthogonal complement to $S_k(\Gamma_0(N))^{old}$ inside $S_k(\Gamma_0(N))$

**Def.** A NEWFORM is a normalised Hecke eigenform in $S_k(\Gamma_0(N))^{new}$

**Fact** $a_m(T_n f) = \sum_{d \mid (m,n)} d^{k-1} \, a_{\frac{m \cdot n}{d^2}}(f) \, \mathbb{1}_N(d)$

**Rmk** If $f = q + a_2 q^2 + \dots$ is an eigenform,

$$\begin{array}{c} a_1(T_n f) = a_n(f) \\ \shortparallel \\ a_1(\lambda_n f) = \lambda_n \cdot a_1(f) = \lambda_n \end{array}$$

$\Rightarrow$ the eigenvalues $\lambda_n$ are the coefficients!

$\Rightarrow$ the symultaneous eigenspaces of all $T_n$ have dim $\leq 1$.

**Rmk** If $f$ is new, $f$ is newform $\Leftrightarrow \begin{cases} a_1 = 1 \\ T_n f = \lambda_n f \text{ for } (n,N)=1 \end{cases}$

**Pf** Let $p|N$. What's $T_p f$? Consider

$$T_p f - a_p(f) \cdot f \in S_k(\Gamma_0(N))^{\text{new}} \cap S_k(\Gamma_0(N))^{\text{old}} = \{0\}$$

Indeed, it's new because $S_k(\Gamma_0(N))^{new}$ is $T_p$-stable and it's old by the (deep) "main lemma" of Atkin-Lehner theory $\square$

**Prop.** $f \in S_k(\Gamma_0(N))$ normalised Hecke eigenform. Then

$$L(s,f) = \prod_p \left(1 - a_p p^{-s} + \mathbb{1}_N(p)\, p^{k-1-2s}\right)^{-1}$$

**Pf.** Apply $\sum_{n \geq 1} T_n / n^s = \prod_p \left(1 - a_p T_p + \mathbb{1}_N(p)\, p^{k-1-2s}\right)^{-1}$ to $f$. $\square$

## The functional equation

$w_N = \left[\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\right]_k$ . Easy to check: $w_N^2 = (-1)^k \cdot \mathrm{id} = \left[\begin{pmatrix} -N & \\ & -N \end{pmatrix}\right]_k$

(in particular, for $k$ even $w_N^2 = \mathrm{id}$)

$\Rightarrow \quad S_k(\Gamma_0(N)) = S_k(\Gamma_0(N))^+ \oplus S_k(\Gamma_0(N))^-$ the eigenspace decomp.

(the eigenvalues of an involution are $\pm 1$)

**Thm** Let $f \in S_k(\Gamma_0(N))^\pm$. Set

$$\Lambda(s, f) = N^{s/2} (2\pi)^{-s} \Gamma(s) \, L(s, f)$$

We have $\Lambda(s, f) = \pm i^k \Lambda(k-s, f)$

**Rmk** If $f$ is a new form, $f$ is automatically an eigenvector for $w_N$. The reason is that $w_N$ commutes with the

$T_n$ for $(n, N) = 1$.

Notation $w_N f = \varepsilon_n f$

Proof of thm

$$\Lambda(s, f) = N^{s/2} \int_0^\infty f(it)\, t^s \frac{dt}{t} \qquad \text{(formal manipulations)}$$

$$\text{(change variables)} = \int_0^\infty f\left(\frac{it}{\sqrt{N}}\right) t^s \frac{dt}{t} = \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right) t^s \frac{dt}{t} + \int_0^1 i^k w_N f\left(\frac{i}{\sqrt{N}\, t}\right) t^{s-k} \frac{dt}{t}$$

$$= \int_1^\infty \left( f\left(\frac{it}{\sqrt{N}}\right) t^s + i^k \varepsilon_f \cdot f\left(\frac{it}{\sqrt{N}}\right) t^{k-s} \right) \frac{dt}{t} \qquad \square$$