18.783 Elliptic Curves
Lecture 21

Andrew Sutherland

April 25, 2022

The first main theorem of complex multiplication

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D, and let

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E) \in \mathbb{C} : \mathrm{End}(E) = \mathcal{O}\}.$$

In the previous lecture we proved that the Hilbert class polynomial

$$H_D(X) := H_{\mathcal{O}}(X) := \prod_{j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} \Big(X - j(E)\Big)$$

has integer coefficients. We defined L to be the splitting field of $H_D(X)$ over $K := \mathbb{Q}(\sqrt{D})$, and showed that there is an injective group homomorphism

$$\Psi\colon\ \mathrm{Gal}(L/K) \hookrightarrow \mathrm{cl}(\mathcal{O})$$

that commutes with the group actions of $\mathrm{Gal}(L/K)$ and $\mathrm{cl}(\mathcal{O})$ on the roots of $H_D(X)$. It remains to show that Ψ is surjective, equivalently, that $H_D(X)$ is irreducible over K.

The decomposition group

Let L/K be a Galois extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K := K \cap \overline{\mathbb{Z}}$ (a "prime" of K). The $\mathcal{O}_L$-ideal $\mathfrak{p}\mathcal{O}_L$ has a unique factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$$

into primes $\mathfrak{q}_i$ of L for which $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$. If $\mathfrak{p}\mathcal{O}_L$ is squarefree $(\mathfrak{p} \nmid \operatorname{disc} \mathcal{O}_K)$ then $\mathfrak{p}$ is unramified in L, and $\operatorname{Gal}(L/K)$ acts transitively on $\{\mathfrak{q}|\mathfrak{p}\} := \{q_1, \ldots, \mathfrak{q}_n\}$.

Definition

Let L/K be a Galois extension of number fields, let $\mathfrak{p}$ be a prime of K that is unramified in L. For each prime $\mathfrak{q} \in \{\mathfrak{q}|\mathfrak{p}\}$ the stabilizer subgroup

$$D_{\mathfrak{q}} := \{\sigma \in \operatorname{Gal}(L/K) : \mathfrak{q}^\sigma = \mathfrak{q}\}$$

is the decomposition group of $\mathfrak{q}$.

Frobenius elements

Let $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ and $\mathbb{F}_\mathfrak{q} := \mathcal{O}_L/\mathfrak{q}$ be the residue fields of the maximal ideals $\mathfrak{p}$ and $\mathfrak{q}$ (the rings $\mathcal{O}_K$ and $\mathcal{O}_L$ are Dedekind domains, so nonzero prime ideals are maximal). These are finite fields of cardinality $\mathrm{N}\mathfrak{p} := [\mathcal{O}_K : \mathfrak{p}]$ and $\mathrm{N}\mathfrak{q} := [\mathcal{O}_L : \mathfrak{q}]$. The image of $\mathcal{O}_K$ in $\mathcal{O}_L/\mathfrak{q}$ is $\mathcal{O}_K/(\mathfrak{q} \cap \mathcal{O}_K) = \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$, so $\mathbb{F}_\mathfrak{p}$ is a subfield of $\mathbb{F}_\mathfrak{q}$.

Each $\sigma \in D_\mathfrak{q}$ fixes $\mathfrak{q}$ and induces an automorphism $\bar\sigma \in \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ via $\bar\sigma(x) := \overline{\sigma(x)}$. When $\mathfrak{p}$ is unramified this defines a group isomorphism

$$D_\mathfrak{q} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$$

Definition

Let L/K be a Galois extension of number fields and $\mathfrak{q}$ a prime of L with $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K$ unramified. The unique $\sigma_\mathfrak{q} \in D_\mathfrak{q}$ for which $\bar\sigma_\mathfrak{q}$ is the Frobenius automorphism $x \mapsto x^{\mathrm{N}\mathfrak{p}}$ is the Frobenius element at $\mathfrak{q}$. The Frobenius elements of $\mathfrak{q}|\mathfrak{p}$ are all conjugate, and we use $\sigma_\mathfrak{p}$ to denote this conjugacy class; $\sigma_\mathfrak{p}$ is a single element when $\mathrm{Gal}(L/K)$ is abelian.

Primes of good reduction

If $E/\mathbb{C}$ has CM by an imaginary quadratic order $\mathcal{O}$ of discriminant $D := \operatorname{disc}\mathcal{O}$, then $j(E)$ is a root of $H_D(X)$ in the splitting field L of $H_D(X)$ over $K := \mathbb{Q}(\sqrt{D})$, and we can choose a Weierstrass model $y^2 = x^3 + Ax + B$ for E with $A, B \in \mathcal{O}_L$ (take $A = 3j(E)(1728 - j(E))$ and $B = 2j(E)(1728 - j(E))^2$, for example).

For primes $\mathfrak{q}$ of L that do not divide $\Delta(E) := -16(4A^3 + 27B^2)$ we can reduce A, B modulo $\mathfrak{q}$ to obtain an elliptic curve $\overline{E}$ over the residue field $\mathbb{F}_\mathfrak{q} := \mathcal{O}_L/\mathfrak{q}$. We then call $\mathfrak{q}$ a prime of good reduction for E (this is all but finitely many primes of L).

More generally, we call $\mathfrak{q}$ a prime of good reduction for E if there is *any* model for E with coefficients in $\mathcal{O}_L$ such that $\mathfrak{q} \nmid \Delta(E)$ (this includes general Weierstrass equations that may have good reduction even at primes above 2). In general there is not a single model that works for all primes of good reduction (there is when $h(D) = 1$).

The first main theorem of complex multiplication

Theorem

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and L the splitting field of $H_D(X)$ over $K := \mathbb{Q}(\sqrt{D})$. The map $\Psi\colon \operatorname{Gal}(L/K) \to \operatorname{cl}(\mathcal{O})$ sending $\sigma \in \operatorname{Gal}(L/K)$ to the unique $\alpha_\sigma \in \operatorname{cl}(\mathcal{O})$ such that $j(E)^\sigma = \alpha_\sigma j(E)$ for $j(E) \in \operatorname{Ell}_{\mathcal{O}}(L)$ is a group isomorphism compatible with the actions of $\operatorname{Gal}(L/K)$ and $\operatorname{cl}(\mathcal{O})$.

Proof: To the board!

Corollary

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D. The Hilbert class polynomial $H_D(x)$ is irreducible over $K = \mathbb{Q}(\sqrt{D})$ and for any $E/\mathbb{C}$ with CM by $\mathcal{O}$ the field $K(j(E))$ is a finite abelian extension of K with $\operatorname{Gal}(K(j(E))/K) \simeq \operatorname{cl}(\mathcal{O})$.

Ring class fields and Kronecker symbols

Definition

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D. The ring class field of $\mathcal{O}$ (and of D) is the splitting field of $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$, equivalently, the field $L = K(j(E))$ generated by the j-invariant of any elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}$.

Definition

Let p be a prime and D an integer. For $p > 2$ the Kronecker symbol is

$$\left(\frac{D}{p}\right) := \#\{x \in \mathbb{F}_p : x^2 = D\} - 1,$$

and $(\frac{D}{2}) = 1$ for $D \equiv \pm 1 \bmod 8$, $(\frac{D}{2}) = -1$ for $D \equiv \pm 3 \bmod 8$, and $(\frac{D}{2}) = 0$ otherwise.

Primes that split completely in the ring class field

Definition

A prime $p \in \mathbb{Z}$ splits completely in a number field L if $p\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ with the $\mathfrak{q}_i$ distinct primes of norm $N\mathfrak{q} = p$ (so $\mathbb{F}_\mathfrak{q} = \mathbb{F}_p$).

Theorem

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D and ring class field L. Let $p \nmid D$ be an odd prime that is unramified in L.[1] *The following are equivalent:*

(i) p *is the norm of a principal $\mathcal{O}$-ideal;*

(ii) $\left(\frac{D}{p}\right) = 1$ *and $H_D(X)$ splits into linear factors in $\mathbb{F}_p[X]$;*

(iii) p *splits completely in L;*

(iv) $4p = t^2 - v^2 D$ *for some integers t and v with $t \not\equiv 0 \bmod p$.*

Proof: To the board!

[1] If p does not divide D then in fact it must be unramified in L.

Factoring primes in imaginary quadratic fields

Lemma

Let K be an imaginary quadratic field of discriminant D with ring of integers $\mathcal{O}_K = [1, \omega]$ and let $p \in \mathbb{Z}$ be prime. Every $\mathcal{O}_K$-ideal of norm p is of the form $\mathfrak{p} = [p, \omega - r]$, where $r \in \mathbb{Z}$ is a root of the minimal polynomial of ω modulo p. The number of such ideals $\mathfrak{p}$ is $1 + \left(\frac{D}{p}\right) \in \{0, 1, 2\}$ and the prime factorization of $p\mathcal{O}_K$ is

$$(p) = \begin{cases} \mathfrak{p}\bar{\mathfrak{p}} & \textit{if } \left(\frac{D}{p}\right) = 1, \\ \mathfrak{p}^2 & \textit{if } \left(\frac{D}{p}\right) = 0, \\ (p) & \textit{if } \left(\frac{D}{p}\right) = -1. \end{cases}$$

with $\mathfrak{p} \neq \bar{\mathfrak{p}}$ when $\left(\frac{D}{p}\right) = 1$.

Corollary

When p divides the conductor $[\mathcal{O} : \mathcal{O}_K]$ there are no proper $\mathcal{O}$-ideals of norm p and otherwise there are $1 - \left(\frac{D}{p}\right) = 0, 1, 2$ when p is inert, ramified, split in K, respectively

Class field theory

Definition

The Hilbert class field of a number field K is a maximal unramified[2] abelian extension.

As conjectured by Hilbert and proved by Furtwängler, if L is the Hilbert class field of K then $\mathrm{Gal}(L/K) \simeq \mathrm{cl}(\mathcal{O}_K)$. The ring class field L of an order $\mathcal{O}$ in an imaginary quadratic field K is the Hilbert class field of K if and only if $\mathcal{O} = \mathcal{O}_K$, since L/K is ramified at primes dividing the conductor of $\mathcal{O}$.

Each number field L is characterized by the set of primes of $\mathbb{Q}$ that split completely in L; for any two number fields these sets are either equal or have infinite difference.

Corollary

Let $\mathcal{O}$ be an order of discriminant D in an imaginary quadratic field K. The splitting field L of $H_D(X)$ over K is unramified at all primes that do not divide the conductor of $\mathcal{O}$. In particular, every rational prime $p \nmid D$ is unramified in L.

[2] This includes "infinite primes" of K; these are always unramified when K is imaginary quadratic.

The norm equation

The equation

$$4p = t^2 - v^2 D \tag{1}$$

in part (iv) of the theorem is known as the norm equation. It arises from the principal $\mathcal{O}$-ideal (λ) of norm p given by part (i), generated by a root $\lambda \in \mathcal{O} \subseteq \mathcal{O}_K$ of $x^2 - tx + p$, which has norm p and trace t. By the quadratic equation

$$\lambda = \frac{-t \pm \sqrt{t^2 - 4p}}{2} = \frac{-t \pm v\sqrt{D}}{2}.$$

Clearing denominators and taking norms yields $\mathrm{N}(2\lambda) = 4\lambda\bar{\lambda} = 4p = t^2 - v^2 D$.

The primes p that split completely in the ring class field of $\mathcal{O}$, are precisely those that satisfy (1) for soem t, v. For $D < -4$ the value of $\pm t$ is uniquely determined by p.

Reducing endomorphims

Let $E/\mathbb{C}$ have CM by an imaginary quadratic order $\mathcal{O}$ of discriminant D and let p be an odd prime that splits completely in the ring class field L for $\mathcal{O}$. Then $j(E)$ is a root of $H_D(X)$ that reduces to a root of $H_D(X)$ in the residue field $\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_p$ of any prime $\mathfrak{q}$ of L above p. Pick a model $y^2 = x^3 + Ax + B$ for E over $\mathcal{O}_L$ such that $\mathfrak{q} \nmid \Delta(E)$

Any nonzero $\varphi \in \operatorname{End}(E)$ is defined by rational functions whose coefficients we can assume lie in $\mathcal{O}_L$, allowing us to reduce them to $\mathbb{F}_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q}$, yielding $\overline{\varphi} \in \operatorname{End}(\overline{E})$ satisfying the characteristic equation of φ. We have an injective ring homomorphism

$$\operatorname{End}(E) \hookrightarrow \operatorname{End}(\overline{E})$$

that is in fact a ring isomorphism (by the Duering lifting theorem).

It is clear that for $j(E) \neq 0, 1728$ we have an isomorphism of endomorphism algebras, and for $\mathcal{O} = \mathcal{O}_K$ of endomorphism rings, since $t \equiv 0 \bmod p$ implies that $\overline{E}$ is ordinary, so $\operatorname{End}(\overline{E})$ must be an order in $K = \mathbb{Q}(\sqrt{D})$.

The Duering lifting theorem

Theorem (Deuring)

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D with ring class field L, and let q be the norm of a prime ideal in $\mathcal{O}_L$ with $q \perp D$. Then $H_D(X)$ splits into distinct linear factors in $\mathbb{F}_q[X]$ and its roots form the set

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) := \{j(E) \in \mathbb{F}_q : \mathrm{End}(E) \simeq \mathcal{O}\}$$

of j-invariants of elliptic curves $E/\mathbb{F}_q$ with CM by $\mathcal{O}$.

Theorem (Deuring lifting theorem)

Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field and let $\phi \in \mathrm{End}(E)$ be nonzero. There exists an elliptic curve E^* over a number field L with an endomorphism $\phi^* \in \mathrm{End}(E^*)$ such that E^* has good reduction modulo a prime $\mathfrak{q}$ of L with residue field $\mathcal{O}_L/\mathfrak{q} \simeq \mathbb{F}_q$, and E and ϕ are the reductions modulo $\mathfrak{q}$ of E^* and ϕ^*.

The CM method

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D < -4$, and let $p \nmid D$ be an odd prime satisfying the norm equation $4p = t^2 - v^2 D$ (via Cornacchia's algorithm).

Given the Hilbert class polynomial $H_D \in \mathbb{Z}[X]$, we can reduce it modulo p and use any root j to construct an elliptic curve $E/\mathbb{F}_p$ defined by $y^2 = x^3 + Ax + B$ by putting $A = 3j(1728 - j)$ and $B = 2j(1728 - j)^2$. We then must have

$$\#E(\mathbb{F}_p) = p + 1 \pm t$$

since π_E has norm p and must therefore have trace $\pm t$ by the norm equation.
By taking a quadratic twist we can achieve either sign.

If we want $\#E(\mathbb{F}_p) = N$ we instead solve $4N = a^2 - v^2 D$ for some discriminant D, put $t := a + 2$, and check if $p := N - 1 + t$ is prime. If so then

$$4p = 4N - 4 + 4t = a^2 - v^2 D - 4 + 4a + 8 = (a+2)^2 - v^2 D = t^2 - v^2 D,$$

and if not we try using a different D.

Summing up the theory of complex multiplication

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D.

$$
\begin{tikzcd}
E \arrow[d, "\text{isomorphism}"] & L \arrow[d, "\text{homethety}"] & \mathfrak{a} \arrow[d, "\text{mod principal ideals}"] & ax^2+bxy+cy^2 \arrow[d, "\mathrm{SL}_2(\mathbb{Z})\text{-equivalence}"] \\
j(E) \arrow[d] & j(L) \arrow[d] & {[\mathfrak{a}]} \arrow[d] & \text{reduced form} \arrow[d] \\
\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) & \{j(L) : \mathcal{O}(L) = \mathcal{O}\} & \mathrm{cl}(\mathcal{O}) & \mathrm{cl}(D)
\end{tikzcd}
$$

Objects: elliptic curves, lattices, proper ideals, binary quadratic forms.
Equivalences: isomorphism, homethety, ideal classes, $\mathrm{SL}_2(\mathbb{Z})$-equivalence.

If we put $K = \mathbb{Q}(\sqrt{D})$ then $\mathrm{Gal}(K(j(E))/K) \simeq \mathrm{cl}(\mathcal{O})$ for any $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$