618: Special Values

Nir Elber

Spring 2025

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Explicit Class Field Theory

What we didn't do is make the construction at all usable in practice!
This time we will remedy this.

—Kiran S. Kedlaya, [Ked21]

1.1 January 21

It is a surprise to everyone, but I made it on time. This course will have a mailing list because I cannot get access to canvas.

1.1.1 Overview

Let's begin with a rough overview of the course. Last semester, we defined the modular curve $Y(N)_{\mathbb{C}} = \Gamma(N)\backslash\mathcal{H}$ for $\Gamma(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ together with its compactification $X(N)_{\mathbb{C}}$. Note there are two actions.

- Rethinking this construction adelically makes it relatively straightforward to provide a Hecke action by the Hecke ring $\mathbb{T}$.
- Also, we learned that $Y(N)$ and $X(N)$ are defined over $\mathbb{Q}$, even though a priori we only defined their complex points as a Riemann surface; thus, there is a Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $X(N)$.

The importance of these two actions is that they are able to realize instances of the Langlands correspondence by comparing the two actions on $\mathrm{H}^{\bullet}_{\text{ét}}(X(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_\ell)$. This is a special case of a larger process involving Shimura varieties.

Let's explain where the Langlands correspondence is coming in. The point is that certain elliptic curves E can be realized as quotients of $X(N)$. Let f be a weight 2 eigenform for $\Gamma(N)$ defined over $\mathbb{Q}$. Then there is a one-dimensional quotient of $J(N) \coloneqq \mathrm{Jac}\, X(N)$ onto some factor E_f, granting a composite

$$X(N) \to J(N) \to E_f.$$

Because both $X(N)$ and E_f are proper curves, and the map is non-constant, we conclude that this is a quotient. The moral of the story is that we are able to send an "automorphic" modular form to a "motivic" elliptic curve.

Remark 1.1 (Wiles–Taylor)**.** It turns out that every elliptic curve is of the form E_f. However, this is a very hard theorem, and we won't need it for this class.

Remember that $Y(N)$ parameterizes elliptic curves; for example, this provides a good way to build the models over $\mathbb{Q}$. Explicitly, $Y(N)$ can be identified with the moduli space of elliptic curves E together with level-N structure, which amounts to a choice of isomorphism $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$. It should be considered rather coincidental that elliptic curves have appeared here twice. This vanishes in higher generality.

One benefit of having the moduli interpretation is that it tells us that some points of $X(N)$ are special. Namely, one may be interested in the CM elliptic curves in $Y(N) \subseteq X(N)$.

Definition 1.2 (complex multiplication)**.** Fix an elliptic curve E. Then E is said to have *complex multiplication* if and only if $\mathrm{End}(E)_{\mathbb{Q}}$ is larger than $\mathbb{Q}$. In this case, we may say that E admits complex multiplication by $K \coloneqq \mathrm{End}(E)_{\mathbb{Q}}$.

Remark 1.3. If an elliptic curve E has CM, then it turns out that $\mathrm{End}(E)$ is an order of an imaginary quadratic number field. In short, this follows from a classification of the possible endomorphism algebras, which must be division algebras of bounded dimension equipped with a positive (Rosati) involution.

Remark 1.4. It turns out that the CM elliptic curves E in $X(1)$ with $\mathrm{End}(E)_{\mathbb{Q}} = K$ for number field K has E defined over K^{ab}. We will prove this later.

Remark 1.5. If E has complex multiplication by K, then it turns out that the Galois representation lands in $\mathrm{T}_K \coloneqq \mathrm{Res}_{K/\mathbb{Q}} \mathbb{G}_{m,K}$ embedded in $\mathrm{GL}_{2,\mathbb{Q}}$. Roughly speaking, the CM points with complex multiplication by K are the image of the Shimura variety

$$\mathrm{Sh}(\mathrm{T}_K) \to \mathrm{Sh}(\mathrm{GL}_2).$$

The first topic in the class will focus on these CM points and the theory of complex multiplication of elliptic curves at large.

The last topic of the course combines the two (coincidental) appearances of elliptic curves. In particular, for a modular elliptic curve $X(N) \to E_f$, one can ask where the CM points of $X(N)$ go.

Definition 1.6 (Heegner point)**.** Fix a modular elliptic curve $X(N) \to E_f$. Then a point on E_f is a *Heegner point* if and only if it is the image of a CM points from $X(N)$.

For example, one has the following roughly stated theorem.

Theorem 1.7 (Gross–Zagier)**.** The Néron–Tate height pairing of two such Heegner points on E_f is nonvanishing if and only if the following hold.

- The sign $\varepsilon(f_K, 1)$ of the functional equation is -1 (so that $L(f_K, 1) = 0$).
- The derivative $L'(f_K, 1) \neq 0$.

Here, f_K denotes the base-change of f (defined over $\mathbb{Q}$) to K.

The moral of the story is that special values are related to Heegner points.

So far we have discussed the first and last topics of the course. Let's give some of our other topics. The first (and slightly shorter) half of the course will cover explicit class field theory.

- We will talk about explicit class field theory for imaginary quadratic fields K. Not only are CM points of $X(N)$ with CM by K defined over K^{ab}, it turns out that this CM theory can explicitly construct K^{ab}.

Namely, one finds that the j-invariant and torsion points together define K^{ab}. This is analogous to how the Kronecker–Weber theorem constructs $\mathbb{Q}^{\mathrm{ab}}$ by attaching the roots of unity, which are torsion points of $\mathbb{G}_{m,\mathbb{Q}}$.

- Locally, Lubin and Tate constructed the maximal abelian extension of a p-adic field K_v. This is inspired by the above CM theory, but it cannot be done globally over number fields. (Roughly speaking, one can localize the previous construction, but then if one wants to only recover the totally ramified part of K_v^{ab}, one is allowed to only talk about the formal group.) It turns out that one can also use this theory to talk a little about nonabelian extensions; we may or may not mention this.
- However, one can extend these notions to work globally over function fields. This gives rise to the story to geometric class field theory and the theory of shtukas. The goal here is to have some basic notions so that we can listen in during seminars.

The second (and slightly longer) half of the course will build towards the Gross–Zagier formula. We will talk about special values in the special case of a torus T embedding in GL_2.

- The standard L-functions due to Hecke arise from the split maximal torus T inside GL_2. One can also define the Rankin–Selberg L-function attached to modular forms.
- Waldspurger's formula, which roughly speaking tells us that $L(f_K, 1)$ is nonzero if and only if the functional
$$f_0 \mapsto \int_{T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q}})} f_0$$
is nonzero, where we are realizing our functional on the base-change of f. There are two proofs of this result: Waldspurger's original proof by the theta correspondence, and Jacquet's proof using the relative trace formula. We will try to talk about both of them.
- Lastly, we will return to arithmetic from automorphic considerations and discuss the Gross–Zagier formula. The original proof of Gross and Zagier (later generalized by Yuan, Zhang, and Zhang) is based on the theta correspondence. There is another proof due to (Wei) Zhang based on an arithmetic relative trace formula.

1.1.2 Complex Multiplication over $\mathbb{C}$

Fix an elliptic curve E defined over an algebraically closed field K. Then $\mathrm{End}(E)_{\mathbb{Q}}$ can be $\mathbb{Q}$, an imaginary quadratic number field, or an order of a quaternion algebra. To see this, one needs to bound $\dim_{\mathbb{Q}} \mathrm{End}(E)_{\mathbb{Q}}$, which is not totally trivial. This is due to Tate.

Theorem 1.8 (Tate)**.** Fix an elliptic curve E defined over an algebraically closed field K, and choose a prime ℓ not dividing $\mathrm{char}\, K$. Then $\mathrm{End}(E)$ is a free $\mathbb{Z}$-mdule, and the Tate module construction provides an embedding
$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_\ell E).$$

Remark 1.9. Because $T_\ell E \cong \mathbb{Z}_\ell^2$, this tells us that $\mathrm{End}(E)$ needs to be split at ℓ. However, $\mathrm{End}(E)$ itself must be non-split (namely, not $M_2(\mathbb{Q})$) because $\mathrm{End}(E)_{\mathbb{Q}}$ is a division algebra.

Remark 1.10. In characteristic 0, one can realize E over $\mathbb{C}$ as $\mathbb{C}/\Lambda$ for some lattice Λ. Then one is able to explicitly compute $\mathrm{End}\, E$, thereby ruling out the third possibility.

We now see that E having complex multiplication needs to be a free $\mathbb{Z}$-submodule of K, which is an order $\mathcal{O}$. It turns out that $\mathcal{O}$ needs to be contained in $\mathcal{O}_K$: everything in $\mathcal{O}$ satisfies a monic quadratic equation by taking the characteristic polynomial, so $\mathcal{O}$ is integral over $\mathbb{Z}$.

Definition 1.11 (conductor)**.** Fix an order $\mathcal{O}$ inside $\mathcal{O}_K$ for some imaginary quadratic field K. Then we define the *conductor* as $f \coloneqq [\mathcal{O}_K : \mathcal{O}]$, which we note is finite because $\mathcal{O} \subseteq \mathcal{O}_K$ is a sublattice of the same rank. For dimension reasons, one can write $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for some $f \in \mathbb{Z}$, which is called the *conductor*.

Remark 1.12. We claim that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$; by writing $\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$ for some τ, this is the same as asserting $\mathcal{O} = \mathbb{Z} + f\tau\mathbb{Z}$. For index reasons, it is enough to check one inclusion. Well, certainly $\mathbb{Z} \subseteq \mathcal{O}_K$, and $[\mathcal{O}_K : \mathcal{O}] = f$, so $\tau \in \mathcal{O}_K$ has $f\tau \in \mathcal{O}_K$.

Remark 1.13. Over $\mathbb{C}$, one writes $E(\mathbb{C}) = \mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$. Up to homothety, we may write $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathcal{H}$, and then the automorphisms are the homotheties of Λ. Then one finds that E has complex multiplication by K if and only if $\tau \in K$ by computing the automorphism group of this lattice.

Here is one example.

Example 1.14. Take $\Lambda = \mathcal{O}$ for some order $\mathcal{O}$. Then $\mathbb{C}/\Lambda$ has complex multiplication by $\mathcal{O}$ by construction.

However, there may be other examples, even up to homothety, roughly speaking due to the failure of class number 1.

Definition 1.15 (proper)**.** Fix an order $\mathcal{O}$ of an imaginary quadratic field K. A *proper fractional ideal* $\mathfrak{a}$ of $\mathcal{O}$ is a sublattice $\mathfrak{a} \subseteq K$ which is stable under $\mathcal{O}$ and such that $\mathrm{End}(\mathfrak{a}) = \mathcal{O}$.

This gives the following bijection.

Proposition 1.16. Fix an order $\mathcal{O}$ of an imaginary quadratic field K. Isomorphism classes of elliptic curves E with complex multiplication by $\mathcal{O}$ are in bijection with the set of proper fractional ideals $\mathfrak{a} \subseteq K$ taken modulo the principal ideals (i.e., scaling by $\mathcal{O}$).

Proof. For the forward map, write E as $\mathbb{C}/\Lambda$, write Λ (up to scaling in $\mathbb{C}$) as $\mathbb{Z} + \tau\mathbb{Z} \subseteq K$, and then the order is $\mathbb{Z} + \tau\mathbb{Z}$. For the backward map, take E as $\mathbb{C}/\mathcal{O}$. ∎

When $\mathcal{O} = \mathcal{O}_K$, we see that the second set is the class group of $\mathcal{O}_K$. This motivates the following definition.

Definition 1.17 (class group)**.** Fix an order $\mathcal{O}$ of an imaginary quadratic field K. We let $\mathrm{Cl}(\mathcal{O})$ denote the group of proper fractional ideals $\mathfrak{a} \subseteq \mathcal{O}$ taken modulo the principal ideals. We may also write $\mathrm{Pic}(\mathcal{O}) \coloneqq \mathrm{Cl}(\mathcal{O})$.

Remark 1.18. Technically, we have not shown that the collection of proper ideals is closed under multiplication. This will follow from Lemma 1.21, allowing this definition to make sense.

Later in the course, we will see that all these elliptic curves are defined over K^{ab}; for example, when $\mathcal{O} = \mathcal{O}_K$, we find that $\mathbb{C}/\mathcal{O}$ is defined over the Hilbert class field of K. More precisely, we will have a main theorem of complex multiplication.

Theorem 1.19. Fix an imaginary quadratic field K, and let H denote the Hilbert class field. Then $\sigma \in \mathrm{Gal}(H/K)$ corresponds to some ideal class $\mathfrak{a} \subseteq \mathcal{O}_K$ by class field theory.

(a) The elliptic curve $\mathbb{C}/\mathcal{O}_K$ is defined over H. In general, the elliptic curve $\mathbb{C}/\mathfrak{a}$ is defined over K^{ab}.

(b) Compatibility with class field theory: one has $j(\mathbb{C}/\mathcal{O}_K) = j(\mathbb{C}/\mathfrak{a})^\sigma$.

Notably, we need to pay attention to the Galois structure here, so we cannot over $\mathbb{C}$ the entire time. Thus, we need to retell our story of complex multiplication beginning with a more abstract theory from algebraic geometry.

Remark 1.20. We never expect the model of $E = \mathbb{C}/\mathfrak{a}$ over H to be unique. Indeed, one expects to be able to twist it by cocycles in $\mathrm{H}^1(\mathrm{Gal}(\overline{H}/H), \mathrm{Aut}_{\overline{H}} E)$. (This is some general story from Galois descent.) However, we expect this cohomology group to be large in general because $\mathrm{Aut}\, E$ is in general large; this is the same core difficulty making $Y(1)$ merely a coarse moduli space instead of a fine one.

1.2 January 23

Here we go.

1.2.1 Proper Ideals

We would like to move towards proving Theorem 1.19. As usual, K will be an imaginary quadratic field, and we go ahead and fix an order $\mathcal{O} \subseteq \mathcal{O}_K$. For example, we would like to show that E given by $\mathbb{C}/\mathcal{O}$ is in fact defined over an abelian extension of K. Let's begin by getting a better understanding of the class group.

Lemma 1.21. Fix an imaginary quadratic field K and an order $\mathcal{O} \subseteq \mathcal{O}_K$. Then the following are equivalent for a fractional ideal $\mathfrak{a}$ of $\mathcal{O}$.

(a) $\mathfrak{a}$ is proper.

(b) $\mathfrak{a}$ is locally free of rank 1 over $\mathcal{O}$.

(c) There is a fractional ideal $\mathfrak{a}^*$ such that $\mathfrak{a}\mathfrak{a}^* = \mathcal{O}$.

Proof. Let f be the conductor of $\mathcal{O}$. Before doing anything, we introduce some notation: for a lattice $\Lambda \subseteq K$, we define the dual lattice

$$\Lambda^\vee := \{\alpha \in K : \alpha\Lambda \subseteq \mathcal{O}_K\}.$$

For example, we claim that $\Lambda^\vee \cong \mathrm{Hom}_{\mathcal{O}_K}(\Lambda, \mathcal{O}_K)$. Indeed, given $a \in \Lambda^\vee$, multiplication by a produces a morphism $\Lambda \to \mathcal{O}_K$; this map is certainly injective and $\mathcal{O}_K$-invariant. For surjectivity, we choose a morphism $a\colon \Lambda \to \mathcal{O}_K$; by tensoring with $\mathbb{Q}$, this produces a morphism $K \to K$, which must be given by multiplication by some $a \in K$, and we see $a \in \Lambda^\vee$ by construction.

We now show the implications separately.

- We show (c) implies (b). This is some moderately technical commutative algebra. Note $\mathfrak{a}\mathfrak{a}^* = \mathcal{O}$ implies that $\mathfrak{a} \otimes_{\mathcal{O}} \mathfrak{a}^* = \mathcal{O}$. Then for each prime $\mathfrak{p}$ of $\mathcal{O}$, we see that $\mathfrak{a}_\mathfrak{p} \otimes_{\mathcal{O}_\mathfrak{p}} \mathfrak{a}^*_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$.

  Thus, we reduce to the following commutative algebra problem: given a local ring R and two finite R-modules M and N such that there is an isomorphism $\psi\colon M \otimes_R N \to R$, we would like to show that M and N are free of rank 1. It is enough to check that M and N are projective, which implies free (because we are over a local ring) thereby completing the proof after a rank computation. By symmetry, we may focus on M, and we now see that it is enough to realize M inside a free R-module of finite rank.

Well, choose $\xi := \sum_{i=1}^n x_i \otimes y_i$ in $M \otimes_R N$ such that $\psi(\xi) = 1$. Then we consider the composite

$$M = M \otimes R \overset{\psi}{=} M \otimes (M \otimes N) = (M \otimes M) \otimes N \cong (M \otimes M) \otimes N \cong M \otimes (M \otimes N) \overset{\psi}{=} M \otimes R = M,$$

where the $\cong$ is given by swapping the two coordinates. In total, one can compute that this automorphism of M sends $x \in M$ to $x \otimes 1$ to $x \otimes \xi$ to $\sum_i x \otimes x_i \otimes y_i$ to $\sum_i x_i \otimes x \otimes y_i$ to $\sum_i \psi(x \otimes y_i) x_i$. We conclude that the map $M \to R^n$ given by sending x to the n-tuple $(\psi(x \otimes y_i))_i$ is a split monomorphism and hence provides the required embedding.

- We show (b) implies (c). Here, (b) implies that $\mathfrak{a}$ is projective locally of rank 1, so we may think about it as a line bundle, and we know how to invert line bundles: define $\mathfrak{a}^* := \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O})$, which we note is a fractional ideal because (arguing as above) it may be realized as the $\mathcal{O}$-stable sublattice $\{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathcal{O}\}$. Now, $\mathfrak{a}\mathfrak{a}^*$ is isomorphic to $\mathfrak{a} \otimes_{\mathcal{O}} \mathfrak{a}^*$, so it remains to check that

$$\mathfrak{a} \otimes_{\mathcal{O}} \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O})$$

  is isomorphic to $\mathcal{O}$. Well, there certainly is a map to $\mathcal{O}$ given by evaluation, and this map is locally an isomorphism (this amounts to checking the result at $\mathfrak{a} = \mathcal{O}$), so we are done.

- We show (c) implies (a). Choose an endomorphism $\alpha \colon \mathfrak{a} \to \mathfrak{a}$, and we must show that α is given by multiplication by an element of $\mathcal{O}$. Tensoring with $\mathbb{Q}$, we see that α must be a scalar in K which we also call α. Then we want to check $\alpha \in \mathcal{O}$. Well, $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ implies $\alpha\mathfrak{a}\mathfrak{a}^* \subseteq \mathfrak{a}\mathfrak{a}^*$, so $\alpha \in \mathcal{O}$ follows.

- We show (a) implies (c). The key difficulty is gaining access to some proper fractional ideals. We begin with a basic case: if $K = \mathbb{Q}(\alpha)$ with α satisfying the minimal integral polynomial $ax^2 + bx + c$ (so that $a\alpha \in \mathcal{O}_K$), then we claim that $\mathbb{Z} + \alpha\mathbb{Z}$ is a proper fractional ideal of the order $\mathbb{Z} + a\alpha\mathbb{Z}$. Indeed, note that $\beta(\mathbb{Z} + \alpha\mathbb{Z}) \subseteq \mathbb{Z} + \alpha\mathbb{Z}$ if and only if $\beta, \beta\alpha \in \mathbb{Z} + \tau\mathbb{Z}$. So we may write out $\beta = m + n\tau$ for $m, n \in \mathbb{Z}$, but then $\beta\alpha \in \mathbb{Z} + \alpha\mathbb{Z}$ if and only if

$$\beta\alpha - m = n\alpha^2 = -\frac{cn}{a} + \frac{bn}{a}\alpha,$$

  which in turn is equivalent to $a \mid n$. We conclude that $\beta(\mathbb{Z} + \alpha\mathbb{Z}) \subseteq \mathbb{Z} + \alpha\mathbb{Z}$ if and only if $\beta \in \mathbb{Z} + a\alpha\mathbb{Z}$, as required.

  We are now ready to attack the implication directly. Write $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$ for some $\alpha, \beta \in K$; scaling $\mathfrak{a}$ by an element of K does not adjust the hypothesis nor the conclusion, so we may assume that $\beta = 1$. Because $\mathfrak{a}$ is proper, we know that $\mathcal{O} = \mathbb{Z} + a\tau\mathbb{Z}$, where $ax^2 + bx + c$ is the minimal integral polynomial for τ. Now, let $\overline{\mathfrak{a}}$ be the complex conjugate ideal, and we see that

$$\mathfrak{a}\overline{\mathfrak{a}} = \mathbb{Z} + \tau\mathbb{Z} + (\tau + \overline{\tau})\mathbb{Z} + (\tau\overline{\tau})\mathbb{Z}.$$

  Now, $\tau + \overline{\tau} = -b/a$ and $\tau\overline{\tau} = c/a$, so we conclude that $\mathfrak{a} \cdot a\overline{\mathfrak{a}} = \mathcal{O}$, as required. ■

Remark 1.22. In particular, we see that the set of proper ideals is closed under multiplication and inversion, allowing us to define $\mathrm{Cl}(\mathcal{O})$ as we did last class.

Remark 1.23. Alternatively, we see that we can describe $\mathrm{Cl}(\mathcal{O})$ as isomorphism classes of line bundles $\mathrm{Pic}(\mathcal{O})$. Indeed, any fractional ideal produces a line bundle, and principal ideals are trivial line bundles, so we obtain a map $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$. This map is surjective by the above lemma; to see that it is injective, note that a proper fractional ideal $\mathfrak{a} \subseteq K$ which is isomorphic to the unit $\mathcal{O}$ must be principal generated by the image of 1 under the given $\mathcal{O}$-module isomorphism $\mathcal{O} \to \mathfrak{a}$.

1.2.2 An Adelic Class Group

To remind ourselves that class field theory should show up somewhere, we note $\mathrm{Cl}(\mathcal{O})$ comes from a ray class group.

Proposition 1.24. Fix an imaginary quadratic field K and an order $\mathcal{O} \subseteq \mathcal{O}_K$ written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Then $\mathrm{Cl}(\mathcal{O})$ is canonically isomorphic to the following two groups.

(a) Ideal-theoretic: the ray class group of fractional ideals of $\mathcal{O}_K$ (prime to f) modulo the principal ideals (α) (prime to f) such that $\alpha \pmod f$ is in $(\mathbb{Z}/f\mathbb{Z})^\times$.

(b) Adele-theoretic: $T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$, where T is the algebraic group $\mathcal{O}^\times$. Explicitly, T is the subgroup $\mathrm{GL}_{\mathcal{O}}(\mathcal{O}) \subseteq \mathrm{GL}_{\mathbb{Z}}(\mathcal{O})$.

Let's give a few remarks before proceeding with the proof.

Remark 1.25. Let's be more explicit about T. One has that $T(R) = \mathrm{GL}_{R\otimes\mathcal{O}}(R \otimes \mathcal{O})$; here, there may be some confusion about why an R appears in the subscript, but this follows by reminding ourselves that $\mathrm{GL}_{\mathbb{Z}}(\mathcal{O})$ should be thought of as $\mathrm{GL}_2(\mathbb{Z})$ (seen by choosing a basis), so its R-points are $\mathrm{GL}_2(R)$. For example $T_{\mathbb{Q}} = \mathrm{GL}_K(K) = \mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_{m,K}$.

Remark 1.26. We note T is isomorphic to $\mathrm{GL}_{\mathcal{O}}(M) \subseteq \mathrm{GL}_{\mathbb{Z}}(M)$ for any $\mathcal{O}$-module M which is free of rank 1. Indeed, an isomorphism $M \cong \mathcal{O} \otimes_{\mathcal{O}} M$ produces a morphism $\mathrm{GL}_{\mathcal{O}}(\mathcal{O}) \to \mathrm{GL}_{\mathcal{O}}(M)$, which can be checked to be an isomorphism locally everywhere.

Remark 1.27. It is worth keeping in a safe place the isomorphism for (a): one sends an ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ to $\mathfrak{b} \cap \mathcal{O}$.

Remark 1.28. Let's provide some motivation for the bijection between (a) and (b). Over $\mathbb{Q}$, the prototypical class group looks something like

$$\mathbb{Q}^+\backslash\mathbb{A}_{\mathbb{Q},f}^\times / \prod_p (1 + f\mathbb{Z}_p)^\times,$$

which we claim is isomorphic to $(\mathbb{Z}/f\mathbb{Z})^\times$. Roughly speaking, this is by the Chinese remainder theorem. By adjusting an idele by a rational scalar, we may identify $\mathbb{Q}^\times\backslash\mathbb{A}_{\mathbb{Q},f}^\times$ with $\prod_p \mathbb{Z}_p^\times$. Then we see that $\mathbb{Z}_p^\times/(1 + f\mathbb{Z}_p)$ is isomorphic to $\left(\mathbb{Z}/p^{\nu_p(f)}\mathbb{Z}\right)^\times$ by computing the kernel of the surjection $\mathbb{Z}_p^\times \twoheadrightarrow \left(\mathbb{Z}/p^{\nu_p(f)}\mathbb{Z}\right)^\times$ as $1+f\mathbb{Z}_p$. The result now follows by gluing together our primes p together by the Chinese remainder theorem.

Remark 1.29. Let's provide some geometric motivation for the bijection between $\mathrm{Cl}(\mathcal{O})$ and the double quotient (b). Geometrically, we would like to work with a (not necessarily smooth) projective curve C over $\mathbb{F}_q$ with function field $F = \mathbb{F}_q(C)$. Then $\mathrm{Cl}(\mathcal{O})$ becomes $\mathrm{Pic}(C)$, which we claim is in bijection with $F^\times\backslash\mathbb{A}_F^\times/\mathcal{O}_F^\times$. Well, the latter is in bijection with divisors modulo principal divisors, which we note is in bijection with $\mathrm{Pic}(C)$ by looking at the trivializations at various points of $\mathcal{L}$.

Corollary 1.30. Fix an imaginary quadratic field K and an order $\mathcal{O} \subseteq \mathcal{O}_K$ written as $\mathcal{O} = \mathbb{Z} + f\mathbb{Z}$. Then $\mathrm{Cl}(\mathcal{O})$ is finite.

Proof. It is enough to see that $T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$ is finite. Well, by Remark 1.25, we see $T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})$ is the idele class group $K^\times\backslash\mathbb{A}_K^\times$. And because $\widehat{\mathbb{Z}} \subseteq \mathbb{A}_{\mathbb{Q},f}$ is an open subgroup, we see that $T(\widehat{\mathbb{Z}}) \subseteq \mathbb{A}_{K,f}^\times$ continues to be an open subgroup. Properties of the topology of the idele class group allow us to conclude that our double quotient is finite. ∎

Let's now begin the proof.

Proof of Proposition 1.24. Before doing anything, we recall from our computation of T in Remark 1.25 that $T(\mathbb{Q}) = K^\times$ and $T(\mathbb{A}_{\mathbb{Q},f}) = \mathbb{A}_{K,f}^\times$. For this proof, for a $\mathbb{Z}$-algebra R, we will write R_p for the ring $\mathcal{O}$ localized at the set of elements coprime p, and we write $\widehat{R}_p$ for its completion; we do similar for the ring $\mathcal{O}_K$. (However, we still write $\mathbb{Z}_p$ for the completion.)

Let's begin with the isomorphism between (a) and (b), which is more or less purely formal. We have the following steps, following Remark 1.28.

1. Before doing anything, we compute
$$T(\widehat{\mathbb{Z}}) = \prod_p (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times.$$
Now, the natural inclusion $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ means that we can realize $\widehat{\mathcal{O}}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ inside $\widehat{\mathcal{O}}_{K,p} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$. But viewing $\mathcal{O}$ and $\mathcal{O}_K$ as sublattices of K, we see $\mathcal{O} = \mathbb{Z} \oplus f\tau\mathbb{Z}$ (where $\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$), so $\widehat{\mathcal{O}}_p = \mathbb{Z}_p \oplus f\tau\mathbb{Z}_p$. We conclude that
$$\widehat{\mathcal{O}}_p^\times = \left\{\alpha \in \widehat{\mathcal{O}}_{K,p}^\times : \alpha \pmod f \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times\right\}.$$

2. We construct a map from (b) to (a). Begin with an idele $x \in \mathbb{A}_{K,f}^\times$, and we need to produce an ideal. Well, we may adjust by an element of $K^\times$ so that $x_p \pmod f \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times$ for each $p \mid f$. (This condition should be understood by identifying $\mathbb{Z}_p$ with its image in $\widehat{K}_p^\times$.) Then this produces a fractional ideal
$$\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x_{\mathfrak{p}})}.$$
This is coprime to f by construction. Here are checks that this is well-defined.

   - We should check that this map does not depend on the choice of scalar in $K^\times$. Thus, if we adjust again by some other $\alpha \in K^\times$, we want to land in the same ideal class. Because we need $(\alpha x)_p \pmod f \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times$ for each $p \mid f$, we must have $\alpha \pmod f \in (\mathbb{Z}/f\mathbb{Z})^\times$. Then we see that
   $$\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha x_{\mathfrak{p}})} = (\alpha) \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x_{\mathfrak{p}})}$$
   lives in the same ideal class.
   - We check that the ideal class is not change if we adjust x by an element $y \in T(\widehat{\mathbb{Z}})$. Well, for each prime p, we see $y_p \in \widehat{\mathcal{O}}_p^\times$, so $y_p \pmod f \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times$, so the same is true for $x_p y_p$. We conclude that we are producing the fractional ideal
   $$\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x_{\mathfrak{p}} y_{\mathfrak{p}})},$$
   but of course $y_{\mathfrak{p}} \in \widehat{\mathcal{O}}_{K,p}^\times$ means that none of the valuations have actually changed.

   While we're here, we also note that our map is surjective because this is fairly easy: for any ideal in $\mathcal{O}_K$ coprime to f, one can read off its valuations at each prime $\mathfrak{p}$ to recover an idele in $\mathbb{A}_{K,f}^\times$ mapping to that ideal.

3. We show that the constructed map is surjective. Suppose an idele $x \in T(\mathbb{A}_{\mathbb{Q},f})$ goes to a principal ideal, and we want to show that x is trivial in the double quotient. As in the construction of the map, we go ahead and assume that $x_p \pmod f \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times$ for each $p \mid f$. Now, are given some $\alpha \in K$ such that $\alpha \pmod f \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times$ and
$$(\alpha)\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x_{\mathfrak{p}})} = 1.$$
Thus, we see that $\alpha x_{\mathfrak{p}} \in \widehat{\mathcal{O}}_{K,\mathfrak{p}}^\times$ for each prime $\mathfrak{p}$, so this lives in $\widehat{\mathcal{O}}_p^\times$ for each $p \nmid f$ automatically. For $p \mid f$, it remains to note that $\alpha x_{\mathfrak{p}} \in (\mathbb{Z}_p/f\mathbb{Z}_p)^\times$ as well by construction of α. Synthesizing, $\alpha x \in T(\widehat{\mathbb{Z}})$, implying that x is trivial in the double quotient.

It remains to show that $\mathrm{Cl}(\mathcal{O})$ is the same as (b). We follow the idea of Remark 1.29; we have the following steps.

1. We define the map from $\mathrm{Cl}(\mathcal{O})$ to Cartier divisors. Choose $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$. Because $\mathfrak{a}$ is locally free of rank 1, we are granted an open cover $\mathcal{U}$ of $\operatorname{Spec}\mathbb{Z}$ together with some isomorphisms $\varphi_U \colon \mathfrak{a}_U \to \mathcal{O}_U$. Now, for any two $U, V \in \mathcal{U}$, there is a composite isomorphism
$$K = (\mathcal{O}_U)_{\mathbb{Q}} \overset{\varphi_U}{\cong} (\mathfrak{a}_U)_{\mathbb{Q}} = \mathfrak{a}_{\mathbb{Q}} = (\mathfrak{a}_V)_{\mathbb{Q}} \overset{\varphi_V}{\cong} (\mathcal{O}_V)_{\mathbb{Q}} = K$$
of K-modules, so we have produced an element $\alpha_{UV} = \varphi_V \circ \varphi_U^{-1}$ in $\mathcal{O}_{U\cap V}$. For example, by construction, we see that the collection $\{\alpha_{UV}\}_{U,V\in K}$ satisfies a cocycle condition $\alpha_{VW}\alpha_{UV} = \alpha_{UW}$. Thus, we have in fact provided a Cartier divisor.

2. While we're here, we explain that each Cartier divisor $\{\alpha_{UV}\}_{U,V\in\mathcal{U}}$ does in fact produce some $\mathcal{O}$-module $\mathfrak{a}$ which is locally free of rank 1. Indeed, one has "local" line bundles $\mathfrak{a}_U \coloneqq \mathcal{O}_{\mathcal{O}}|_U$ on each $U \in \mathcal{U}$, and the elements $\alpha_{UV} \in \mathcal{O}_{U\cap V}$ provide transition maps $\mathfrak{a}_U|_{U\cap V} \to \mathfrak{a}_V|_{U\cap V}$ which satisfy a suitable cocycle condition. The standard argument gluing sheaves is now able to glue these sheaves into a sheaf $\mathfrak{a}$ on $\mathcal{O}$ which is locally free of rank 1.

3. In the sequel, we will want to be able to check when two Cartier divisors define the same module $\mathfrak{a}$. This amounts to computing the kernel of the map from Cartier divisors to line bundles on $\mathcal{O}$ given in the previous paragraph. (Multiplication of Cartier divisors is defined pointwise on a refinement of the relevant open covers.)

   Well, suppose there is an isomorphism $\psi \colon \mathcal{O} \to \mathfrak{a}$, where $\mathfrak{a}$ arises from the Cartier divisor $\{\alpha_{UV}\}_{U,V\in\mathcal{U}}$. Then each $U \in \mathcal{U}$ produces a composite $(\varphi_U \circ \psi) \colon \mathcal{O} \to \mathcal{O}_U$; thus, we see that ψ amounts to the same amount of data as a tuple of elements $\{\beta_U\}_{U\in\mathcal{U}}$. However, for the morphisms $\beta_U \colon \mathcal{O} \to \mathcal{O}_U$ to glue together to a morphism $\psi \colon \mathcal{O} \to \mathfrak{a}$ (which will be locally an isomorphism and hence globally an isomorphism), we need the diagram
   $$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\beta_U} & \mathcal{O}_U \\ & \searrow^{\beta_V} & \downarrow{\scriptstyle \alpha_{UV}} \\ & & \mathcal{O}_V \end{array}$$
   to commute, which amounts to the equality $\alpha_{UV}\beta_U = \beta_V$.

4. We define a map from Cartier divisors to the double quotient. Choose a Cartier divisor $\{\alpha_{UV}\}_{U,V\in\mathcal{U}}$. To construct our idele in $\mathbb{A}_{K,f}^\times = \prod_p(\widehat{K}_p^\times, \widehat{\mathcal{O}}_{K,p}^\times)$, we fix an open subset $U_0 \in \mathcal{U}$, and we define $S \coloneqq (\operatorname{Spec}\mathbb{Z}) \setminus U_0$, which we note is a finite set. Now, for each $p \in S$, we may choose a neighborhood $U_p \in \mathcal{U}$, allowing us to construct the tuple
   $$(\alpha_{0p})_{p\in S} \in \mathbb{A}_{K,S}^\times \subseteq \mathbb{A}_{K,f}^\times,$$
   where $\alpha_{0p} \coloneqq \alpha_{U_0U_p}$.

   We would like to check that the element in $T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$ depends only on the choice of Cartier divisor. We go through our choices one at a time.

- Choosing a different neighborhood U_p' of p will adjust α_{0p} to some $\alpha_{0p'}$. However, $\alpha_{0p} = \alpha_{p'p}\alpha_{0p'}$ by the cocycle condition, and $\alpha_{p'p} \in \mathcal{O}_p^\times$ (because $p \in U_p \cap U_p'$), so this only adjusts this coordinate by an element of $\mathcal{O}_p^\times \subseteq T(\mathbb{Z}_p)$, which is legal. Thus, the tuple is well-defined in $T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$.
- Shrinking U_0 by (say) removing a prime q adds a new coordinate α_{0q}. However, $\alpha_{0q} \in T(\mathbb{Z}_q)$ because α_{0q} began as providing an isomorphism $\mathcal{O}_{U_0} \to \mathcal{O}_{U_0}$ and hence lives in $\mathcal{O}_{U_0}^\times \subseteq \mathcal{O}_q^\times$. Thus, the tuple is well-defined in $T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$.
- We explain that changing U_0 to some different $U_0' \in \mathcal{U}$ will not change the class. The previous check explains that we may shrink both U_0 and U_0' to not adjust the class, so we may assume that U_0 and U_0' are equal as sets. Then there is some $\alpha_{00'} \in T(\mathbb{Q})$ which allows us to identify $\alpha_{0p} = \alpha_{0'p}\alpha_{00'}$. Thus, the entire tuple is still well-defined in $T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$.

While we're here, we note that the above checks also explain that our map from Cartier divisors to the double quotient is well-defined up to refining the open cover of the Cartier divisor. Because isomorphisms of Cartier divisors really amount to the existence of a common refinement (by tracking through the comments in the previous step), we see that we have in fact defined a map $\mathrm{Cl}(\mathcal{O}) \to T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$.

5. We argue that the map is surjective. Choose some $x \in T(\mathbb{A}_{\mathbb{Q},f})$, which we consider as a double coset in the double quotient. For all $p \nmid f$, we see that $\widehat{\mathcal{O}}_p^\times = \widehat{\mathcal{O}}_{K,p}^\times$. So because $x_p \in \widehat{\mathcal{O}}_{K,p}^\times$ for all but finitely primes p, we see that we can adjust x by an element of $T(\widehat{\mathbb{Z}})$ until $x \in \mathbb{A}_{K,S}^\times$ for some finite set S. Furthermore, for each $p \in S$, we still know $T(\mathbb{Z}_p) \subseteq \widehat{\mathcal{O}}_{K,p}^\times$ is an open subgroup of finite index, so one can still adjust by an element of $T(\widehat{\mathbb{Z}})$ until $x_p \in K_p^\times$ for each $p \in S$.

   We are now ready to construct our Cartier divisor. The index set for our open cover will be $I \coloneqq \{0\} \cup S$, where $U_0 = (\operatorname{Spec}\mathbb{Z}) \setminus S$, and U_p is an open neighborhood of p chosen small enough so that $x_p \in \mathcal{O}_{U_0}^\times$. Now, we define $x_0 \coloneqq 1$ and define
   $$\alpha_{ij} \coloneqq x_j x_i^{-1}$$
   for any $i, j \in S$. Then the tuple $\{\alpha_{ij}\}_{i,j\in I}$ satisfies the cocycle condition and maps to x by construction, so we are done.

6. We argue that the map is injective. Suppose a Cartier divisor $\{\alpha_{UV}\}_{U,V\in\mathcal{U}}$ is trivial in the double quotient after producing the element $x \in \mathbb{A}_{K,f}^\times$; we would like to show that the Cartier divisor corresponds to the trivial line bundle. Working through the construction, we may as well replace $\mathcal{U}$ with the open cover $\{U_0\} \cup \{U_p\}_{p\in S}$ where $S = (\operatorname{Spec}\mathbb{Z}) \setminus U_0$. (One can check that a line bundle is trivial on any open cover.) Because the Cartier divisor is trivial in the double quotient, we are granted $\beta \in K^\times$ and elements $\beta_p \in \widehat{\mathcal{O}}_p^\times$ (for each prime p) such that
   $$\alpha_{0p} = \beta\beta_{0p},$$
   where $\alpha_{0p} = 1$ for $p \notin S$. In particular, we conclude $\beta_{0p} \in K^\times \cap \widehat{\mathcal{O}}_p^\times$, so $\beta_{0p} \in \mathcal{O}_p^\times$. We take a moment to note that we can adjust β by uniformizers of primes $\mathfrak{p}$ not lying over primes $p \in S$ because this will not change $\beta_{0p} \in \mathcal{O}_p^\times$; thus, we may assume $\beta \in \mathcal{O}_{U_0}$.

   We now set $\beta_0 \coloneqq \beta$ and $\beta_p \coloneqq \beta_{0p}$ for each $p \in S$ and note that $\alpha_{ij}\beta_i = \beta_j$ for any $i, j \in \{0\} \cup S$ by construction, which witnesses that the Cartier divisor is equivalent to the trivial one (upon maybe shrinking the open neighborhoods U_p so that $\beta_p \in \mathcal{O}_{U_p}$ for each $p \in S$). ■

Remark 1.31. By construction of all the maps, one can see that the group isomorphisms are $\mathrm{Gal}(K/\mathbb{Q})$-equivariant.

Remark 1.32. The last bijectivity check can be seen as an instance of fpqc descent. Here is an example of the statement we need: for any prime p of $\mathbb{Z}$, the category of free modules over $\mathcal{O} \otimes \mathbb{Z}_{(p)}$ of rank 1 is equivalent to the category of triples $(M_{\mathbb{Q}}, M_p, \tau)$, where $M_{\mathbb{Q}}$ is a rank 1 module over $\mathcal{O} \otimes \mathbb{Q}$, M_p is a free module of rank 1 over $\mathcal{O} \otimes \mathbb{Z}_p$, and τ is an isomorphism between $M_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_p \to M_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. (The forgetful functor can be seen to be fully faithful, and for essential surjectivity, one notes that one can recover M as a $\mathbb{Z}_{(p)}$-module from the data in τ, and the $\mathcal{O}$-module structure is unique.) This sort of statement would allow us to work in formal neighborhoods of p; for example, in the injectivity check, given two $M, M' \in \mathrm{Cl}(\mathcal{O})$, one gets to say that having $M_{(p)} \cong M'_{(p)}$ from the isomorphism on the completion, and then we can glue the isomorphisms together.

1.3 January 28

Here we go.

1.3.1 The Class Group Action

We now relate our order to elliptic curves. For now, this will happen by letting $\mathrm{Cl}(\mathcal{O})$ act on the collection of elliptic curves E. Over $\mathbb{C}$, the action we would like to send $\mathbb{C}/\mathfrak{a}$ to $\mathbb{C}/\mathfrak{a}'$ by the action of the class $\mathfrak{a}(\mathfrak{a}')^{-1}$. However, because we are interested in arithmetic information, we will want to make this construction work in algebraic geometry. Here is our construction.

Definition 1.33. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K. Then an elliptic curve E has complex multiplication by $\mathcal{O}$ if and only if there is an isomorphism $\mathcal{O} \to \mathrm{End}(E)$. We let $Y_{\mathcal{O}}$ denote the set of such elliptic curves up to isomorphism (not necessarily preserving the isomorphism $\mathcal{O} \to \mathrm{End}(E)$).

Remark 1.34. There is no way to fix the isomorphism $\mathrm{End}(E) \to \mathcal{O}$. However, upon choosing such an isomorphism, it becomes unique up to a ring automorphism of $\mathcal{O}$, which upon tensoring up to K provides equivalent data to $\mathrm{Gal}(K/\mathbb{Q})$.

Remark 1.35. Upon choosing an isomorphism $\mathcal{O} \to \mathrm{End}(E)$, taking the differential provides a map

$$\mathcal{O} \to \mathrm{End}_k(\mathrm{Lie}(E)).$$

The right-hand side is k, so we are given a map $K \hookrightarrow k$. Notably, we have not embedded K into k to start out, so this is genuinely new information arising from a choice: changing the isomorphism $\mathcal{O} \to \mathrm{End}_k(E)$ up to the Galois element in $\mathrm{Gal}(K/\mathbb{Q})$ will similarly adjust the embedding $K \hookrightarrow k$ by the same Galois element.

Remark 1.36. We could alternatively choose an embedding $K \subseteq k$ and then let $Y_{\mathcal{O}}$ be the collection of isomorphism classes of elliptic curves E with complex multiplication by $\mathcal{O}$, together with the choice of isomorphism $\mathcal{O} \to \mathrm{End}(E)$ to be compatible with the embedding $K \subseteq k$. The point is that exactly one of the two isomorphisms $\mathcal{O} \to \mathrm{End}(E)$ will be compatible with the embedding $K \subseteq k$ because both are uniquely determined up to an element of $\mathrm{Gal}(K/\mathbb{Q})$.

Definition 1.37. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K embedded in k. Given $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ and $E \in Y_{\mathcal{O}}$, we define the action map

$$\mathfrak{a} \star E \coloneqq \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E).$$

Namely, we have defined an fpqc sheaf $(\mathfrak{a} \star E)(S) \coloneqq \mathrm{Hom}_S(\mathfrak{a}(S), E(S))$ on the category of $\mathcal{O}$-modules (in the category of fpqc k-schemes); here, we are viewing $\mathfrak{a}$ as a constant k-scheme, which then produces an fpqc sheaf.

Remark 1.38. Note that $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)$ of course has an action by $\mathcal{O}$ via its action on $\mathfrak{a}$. Note that the action of $\mathcal{O}$ on E is well-defined (even though merely $E \in Y_{\mathcal{O}}$) because we chose an embedding $K \hookrightarrow k$ to start!

Remark 1.39. Let's check that $\mathfrak{a} \star E$ is in fact represented by a scheme. Because $\mathfrak{a}$ is finitely presented, we have some exact sequence $\mathcal{O}^m \to \mathcal{O}^n \to \mathfrak{a} \to 0$, so

$$0 \to \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E) \to E^n \to E^m,$$

so we realize $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)$ as a commutative group scheme over k. Because $\mathfrak{a}$ is locally free of rank 1 (over $\mathcal{O}$), we may find an open cover $\mathcal{U}$ of $\mathrm{Spec}\,\mathcal{O}$ such that

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)|_U = \mathrm{Hom}_{\mathcal{O}_U}(\mathfrak{a}|_U, E|_U) = \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{O}_U, E_U) = E_U$$

for each $U \in \mathcal{U}$. Thus, we see that $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)|_U$ is connected and dimension 1, which is a fact that glues together to tell us that $(\mathfrak{a} \star E)$ is an elliptic curve.

Example 1.40. Over $k = \mathbb{C}$, we may write $E(\mathbb{C}) = \mathbb{C}/\Lambda$. Then we claim that $(\mathfrak{a} \star E)(\mathbb{C}) \cong \mathbb{C}/\left(\Lambda\mathfrak{a}^{-1}\right)$. (Here, $\Lambda\mathfrak{a}^{-1}$ is the product of these fractional ideals, which is a proper fractional ideal because the product of line bundles is a line bundle; see Lemma 1.21.) Well, as $\mathcal{O}$-modules, we see that

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E(\mathbb{C})) = \mathfrak{a}^{-1} \otimes_{\mathcal{O}} (\mathbb{C}/\Lambda).$$

Then we note $\mathfrak{a}^{-1}$ is a line bundle and hence flat, so we apply $\mathfrak{a}^{-1} \otimes -$ to the exact sequence

$$0 \to \Lambda \to \mathbb{C} \to \mathbb{C}/\Lambda \to 0$$

of $\mathcal{O}$-modules to see that $\mathfrak{a}^{-1} \otimes_{\mathcal{O}} \mathbb{C}/\Lambda$ is isomorphic to $\mathbb{C}/\left(\mathfrak{a}^{-1}\Lambda\right)$, where the embedding $\mathfrak{a}^{-1} \otimes_{\mathcal{O}} \Lambda \hookrightarrow K \subseteq \mathbb{C}$ is given by multiplication.

Now, here is the punchline of our action.

Proposition 1.41. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K. Then the action of $\mathrm{Cl}(\mathcal{O})$ on $Y_{\mathcal{O}}$ is simply transitive.

Proof. Choose two elliptic curves E and E', and we need to show that there is a unique $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ such that $\mathfrak{a} \star E = E'$. For this, we reduce to $\mathbb{C}$: the elliptic curves E and E' are defined with finitely many equations, so they will be defined over an algebraically closed field k of finite transcendence degree over $\mathbb{Q}$, so we define E and E' over $\mathbb{C}$. Then we may write $E(\mathbb{C}) = \mathbb{C}/\Lambda$ and $E'(\mathbb{C}) = \mathbb{C}/\Lambda'$, and according to Example 1.40, we are on the hunt for a unique class $\mathfrak{a}$ such that $\Lambda \star \mathfrak{a}^{-1} = \Lambda'$. This follows from the group structure of $\mathrm{Cl}(\mathcal{O})$. ∎

Corollary 1.42. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K. Then the set $Y_{\mathcal{O}}$ is finite.

Proof. Combine Proposition 1.41 with the finiteness of $\mathrm{Cl}(\mathcal{O})$ given in Corollary 1.30. ∎

1.3.2 The Galois Action

We now add a Galois action to the mix. Note $\mathrm{Gal}(k/\mathbb{Q})$ acts on $Y_{\mathcal{O}}$ by applying some $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ directly to the equations cutting out some $E \in Y_{\mathcal{O}}$ to produce an elliptic curve $\sigma(E)$. Then we can also apply σ to any endomorphism of $\sigma(E)$, so $\sigma(E)$ continues to live in $Y_{\mathcal{O}}$.

Let's check that the Galois action and the $\mathrm{Cl}(\mathbb{Q})$-action behave.

Lemma 1.43. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K embedded in k. Choose $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ and $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$, and fix an embedding $K \subseteq k$. Then, acting on $Y_{\mathcal{O}}$, we have

$$\sigma \circ \mathfrak{a} = \sigma(\mathfrak{a}) \circ \sigma.$$

Proof. Choose some $E \in Y_{\mathcal{O}}$, and we would like to check that $\sigma(\mathfrak{a} \star E) \cong \sigma(\mathfrak{a}) \star \sigma(E)$. We may do this on the level of fpqc sheaves: choose some $\mathcal{O}$-module S (which is some fpqc cover of k), and we see that

$$\begin{aligned}\sigma(\mathfrak{a} \star E)(S) &= \sigma((\mathfrak{a} \star E)(S)) \\ &= \sigma(\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)(S)) \\ &= \sigma(\mathrm{Hom}_S(\mathfrak{a}(S), E(S))).\end{aligned}$$

On the other hand, we find

$$\begin{aligned}(\sigma(\mathfrak{a}) \star \sigma(E))(S) &= \mathrm{Hom}_{\mathcal{O}}(\sigma(\mathfrak{a}), \sigma(E))(S) \\ &= \mathrm{Hom}_S(\sigma(\mathfrak{a})(S), \sigma(E)(S)) \\ &= \mathrm{Hom}_S(\sigma(\mathfrak{a}(S)), \sigma(E(S))).\end{aligned}$$

These two $\mathcal{O}$-modules now agree by pulling out the σ in the last equation. (We are perhaps using some assertion that $\mathcal{O}$ is Galois-stable, so the subscript S does not need to change.) ∎

Note that the action of $\mathrm{Gal}(k/\mathbb{Q})$ on $\mathrm{Cl}(\mathcal{O})$ will factor through $\mathrm{Gal}(K/\mathbb{Q})$, so we really only need to understand the action of the complex conjugation element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Cl}(\mathcal{O})$.

Lemma 1.44. Fix an order $\mathcal{O}$ of a quadratic imaginary field K, and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be the nontrivial element. For any $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$, we have

$$\sigma(\mathfrak{a}) = \mathfrak{a}^{-1}.$$

Proof. We are interested in showing that $\mathfrak{a} \cdot \sigma(\mathfrak{a})$ is trivial in $\mathrm{Cl}(\mathcal{O})$. Using (a) of Proposition 1.24 (and noting the Galois action is the natural one by Remark 1.31), it is enough to check that any prime $\mathfrak{p}$ of $\mathcal{O}_K$ (coprime to f) has $\mathfrak{p} \cdot \sigma(\mathfrak{p}) = (\alpha)$ for some α such that $\alpha \pmod f \in (\mathbb{Z}/f\mathbb{Z})^\times$. Letting $(p) := \mathfrak{p} \cap \mathbb{Z}$ be the prime lying under $\mathfrak{p}$, we find two cases.

- If (p) is split or ramified, then the two primes (counted with multiplicity) above (p) are $\mathfrak{p}$ and $\sigma(\mathfrak{p})$, so $\mathfrak{p} \cdot \sigma(\mathfrak{p}) = (p)$ is trivial in $\mathrm{Cl}(\mathcal{O})$.
- If (p) is inert, then $\mathfrak{p} = \sigma(\mathfrak{p}) = (p)$, so $\mathfrak{p} \cdot \sigma(\mathfrak{p}) = \left(p^2\right)$ continues to be trivial in $\mathrm{Cl}(\mathcal{O})$. ∎

The moral of the story is that we can glue our actions together to produce an action by the semidirect product $\mathrm{Gal}(k/\mathbb{Q}) \rtimes \mathrm{Cl}(\mathcal{O})$.

Here is a punchline of having a Galois action.

Proposition 1.45. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K. Then all elliptic curves $E \in Y_{\mathcal{O}}$ are defined over a fixed algebraic number field.

Proof. Define the subfield $L \subseteq k$ so that $\mathrm{Gal}(k/L)$ is the kernel of the action map $\mathrm{Gal}(k/\mathbb{Q}) \to \mathrm{Sym}(Y_{\mathcal{O}})$. Namely, because $Y_{\mathcal{O}}$ is a finite set (by Corollary 1.42), we see that the kernel of the action map is finite-index; additionally, the action commutes with restriction (suitably understood), so the action map is continuous, so the kernel is an open subgroup of finite index. We conclude that L exists and is finite over $\mathbb{Q}$.

We now check that L works. Given $E \in Y_{\mathcal{O}}$, we would like to know that the equations cutting out E can be descended to L. By Galois descent, it is enough to check that E is isomorphic to $\sigma(E)$ for all $\sigma \in \mathrm{Gal}(k/L)$.[1] However, this last statement is true by construction of L. ∎

Remark 1.46. In fact, the proof shows that the degree of L over $\mathbb{Q}$ is at most $\#\mathrm{Sym}(Y_{\mathcal{O}}) = (\#\mathrm{Cl}(\mathcal{O}))!$.

Example 1.47. If $\mathcal{O}$ has class number 1, then $Y_{\mathcal{O}}$ has only one element, so the proof shows that all the elliptic curves in $Y_{\mathcal{O}}$ are defined over $\mathbb{Q}$! For example, the elliptic curve $E\colon y^2 = x^3 + 1$ has complex multiplication by $\mathbb{Z}[\zeta_3] \subseteq \mathbb{Q}(\zeta_3)$. Note that it is important that $Y_{\mathcal{O}}$ did not keep track of the isomorphism $\mathcal{O} \hookrightarrow \mathrm{End}(E)$ because this does not have to be defined over $\mathbb{Q}$.

We are now ready to (re)state the main theorems of complex multiplication. Roughly speaking, this says that our two Galois actions agree under class field theory.

Notation 1.48. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K embedded in k. Then we define a character $\chi\colon \mathrm{Gal}(k/K) \to \mathrm{Cl}(\mathcal{O})$ by sending σ to the element $\chi(\sigma) \in \mathrm{Cl}(\mathcal{O})$ such that

$$\sigma(E) = \chi(\sigma) \star E.$$

Remark 1.49. Let's check that this χ makes sense. Note that $\chi(\sigma)$ is uniquely defined given E (by Proposition 1.41), and one can check that it does not depend on the choice of E by checking that the equation remains true after replacing E with $(\mathfrak{a} \star E)$ in the equation above (using Lemma 1.43).

Theorem 1.50 (Main)**.** Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K embedded in k. Then χ is a quotient of the (inverse of the) Artin reciprocity map

$$K^\times \backslash \mathbb{A}_{K,f}^\times \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/K)^{\mathrm{ab}},$$

where we realize $\mathrm{Cl}(\mathcal{O})$ as a quotient of the idele class group via Proposition 1.24. This Artin reciprocity map sends a uniformizer $\varpi_{\mathfrak{p}}$ to the arithmetic Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$.

Here is an example corollary, extending Remark 1.46.

Corollary 1.51. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K embedded in k. Fix any $E \in Y_{\mathcal{O}}$.

(a) The elliptic curve E is defined over the ring class field of $\mathcal{O}$ and no smaller extension of K.

(b) The field $K(j(E))$ is the ring class field of $\mathcal{O}$.

(c) We have $[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = \#\mathrm{Cl}(\mathcal{O})$.

[1] This point is somewhat subtle: just because $E \cong \sigma(E)$ for all $\sigma \in \mathrm{Gal}(k/L)$, how do we know that there is actually a model of E with coefficients in L? This sort of question is what the machinery of (Galois) descent is supposed to answer.

Proof. Here we go. Throughout, let H be the ray class field of $\mathcal{O}$.

(a) By Galois descent, it is enough to check that E is isomorphic to $\sigma(E)$ for any $\sigma\,\mathrm{Gal}(k/H)$. Well, $\sigma(E) = \chi(\sigma) \star E$ by definition of χ, so we would like to know that the kernel of χ is $\mathrm{Gal}(k/H)$.

We now apply Theorem 1.50. By definition of H, the Artin reciprocity map provides an isomorphism

$$\mathrm{Cl}(\mathcal{O}) \cong K^\times \backslash \mathbb{A}_{K,f}^\times / \widehat{\mathcal{O}}^\times \cong \mathrm{Gal}(H/K),$$

where the first isomorphism is given by Proposition 1.24. The inverse of this composite is χ by Theorem 1.50, so we conclude that $\mathrm{Gal}(k/H)$ is in fact the kernel of χ.

(b) The field of definition of E is $K(j(E))$ by properties of the j-invariant, so this follows from (a). Let's quickly review the argument that the field of definition of E is $K(j(E))$. The coefficients of E generate $K(j(E))$, so $K(j(E))$ certainly contains the field of definition of E. Conversely, one can write down an elliptic curve cut out by

$$y^2 = x^3 - \frac{27j(E)}{j(E) - 1728}x - \frac{27j(E)}{j(E) - 1728}$$

with j-invariant $j(E)$ and manifestly defined over $K(j(E))$. (Technically, this only works for $j \neq 1728$. For $j = 1728$, one can provide a separate construction of an elliptic curve with j-invariant 1728.) This elliptic curve which is isomorphic to E (over k) because the j-invariant determines isomorphism class over an algebraic closure; thus, E is defined over $K(j(E))$.

(c) The second equality again follows from (a) and the fact that $K(j(E))$ is the field of definition for E; namely, $\#\,\mathrm{Cl}(\mathcal{O}) = [H : K]$.

We will have to work a little harder to show $[\mathbb{Q}(j(E)) : \mathbb{Q}] = \#\,\mathrm{Cl}(\mathcal{O})$. Note $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is equal to the degree of the minimal polynomial of $j(E)$ over $\mathbb{Q}$, which equals the number of Galois conjugates of $j(E)$. However, $\sigma(j(E)) = j(\sigma(E))$, so we see that we are counting the number of j-invariants in Galois orbit of $E \in Y_{\mathcal{O}}$. As discussed in (a), Theorem 1.50 explains how to exchange the Galois action on $Y_{\mathcal{O}}$ with the class group action on $Y_{\mathcal{O}}$ via the character χ. In particular, we see that χ is surjective onto $\mathrm{Cl}(\mathcal{O})$, so the Galois orbit of $E \in Y_{\mathcal{O}}$ is all of $Y_{\mathcal{O}}$ and in particular has size $\#\,\mathrm{Cl}(\mathcal{O})$ (using Proposition 1.41). ∎

In private communication with Professor Yiannis Sakellaridis, I asserted an incorrect version of the following corollary. Here is what I think is a corrected version.

Corollary 1.52. Fix an algebraically closed field k of characteristic 0, and choose an order $\mathcal{O}$ of a quadratic imaginary field K embedded in k. Then the following are equivalent.

(i) The fields of definition of all $E \in Y_{\mathcal{O}}$ are all equal.

(ii) For any $E \in Y_{\mathcal{O}}$, the field $\mathbb{Q}(j(E))$ is Galois over $\mathbb{Q}$.

(iii) For any $E \in Y_{\mathcal{O}}$, the extension $K(j(E))/\mathbb{Q}$ is abelian.

(iv) The class group $\mathrm{Pic}(\mathcal{O})$ is 2-torsion.

Proof. We show the implications separately.

- We show that (i) and (ii) are equivalent. By Theorem 1.50, the character χ is surjective, so the Galois group $\mathrm{Gal}(k/K)$ acts transitively on $Y_{\mathcal{O}}$ (see Proposition 1.41). Thus, fixing any $E_0 \in Y_{\mathcal{O}}$, we find $Y_{\mathcal{O}} = \{\sigma(E_0) : \sigma \in \mathrm{Gal}(k/\mathbb{Q})\}$, so their fields of definition are given by

$$\{\mathbb{Q}(j(\sigma(E_0))) : \sigma \in \mathrm{Gal}(k/\mathbb{Q})\} = \{\sigma(\mathbb{Q}(j(E_0))) : \sigma \in \mathrm{Gal}(k/\mathbb{Q})\}.$$

Thus, all these fields of definition are equal if and only if $\mathbb{Q}(j(E_0))$ is Galois over $\mathbb{Q}$.

- We show that (ii) and (iii) are equivalent. Of course (iii) implies (ii) because any subextension of an abelian extension succeeds at being Galois. For the converse, note that we already know $K(j(E))/\mathbb{Q}$ is Galois by class field theory: one can classify $K(j(E))/K$ as the maximal abelian extension with some prescribed ramification information dictated by the conductor of f, which is then seen to produce a field Galois over $\mathbb{Q}$. Now, given (ii), the fact that $\mathbb{Q}(j(E))/\mathbb{Q}$ is a Galois extension means that in fact it is an abelian extension because then the natural map

$$\mathrm{Gal}(K(j(E))/K) \to \mathrm{Gal}(\mathbb{Q}(j(E))/\mathbb{Q})$$

is an isomorphism. But now $K(j(E)) = K \cdot \mathbb{Q}(j(E))$ is a composite of abelian extensions over $\mathbb{Q}$ and hence abelian.

- We show that (iii) and (iv) are equivalent. The main claim is that the exact sequence

$$1 \to \mathrm{Gal}(K(j(E))/K) \to \mathrm{Gal}(K(j(E))/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1$$

always splits. Indeed, there is a splitting map given by inverting the natural restriction isomorphism

$$\mathrm{Gal}(K(j(E))/\mathbb{Q}(j(E))) \to \mathrm{Gal}(K/\mathbb{Q}).$$

We now proceed with the argument, starting with (iii). Note $\mathrm{Gal}(K(j(E))/\mathbb{Q})$ is now a semidirect product $\mathrm{Gal}(K/\mathbb{Q}) \rtimes \mathrm{Gal}(K(j(E))/K)$, so $\mathrm{Gal}(K(j(E))/\mathbb{Q})$ is abelian if and only if the induced action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Gal}(K(j(E))/K)$ is trivial.

We now translate this into a Galois action on the class group. We need to know when the nontrivial element $\sigma \in \mathrm{Gal}(K(j(E))/\mathbb{Q}(j(E)))$ commutes with $\mathrm{Gal}(K(j(E))/K)$. By the Chebotarev density theorem, it is enough to check this on Frobenius elements $\mathrm{Frob}_{\mathfrak{p}}$. Then using the Artin reciprocity isomorphism

$$\mathrm{Cl}(\mathcal{O}) \to \mathrm{Gal}(K(j(E))/K)$$

given by $[\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}$, we see σ acts on the left by

$$\sigma \mathrm{Frob}_{\mathfrak{p}} \sigma^{-1} = \mathrm{Frob}_{\sigma\mathfrak{p}}$$

and hence on the right by the usual action of $\mathrm{Gal}(K/\mathbb{Q})$ on the class group.

It remains to understand when the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Cl}(\mathcal{O})$ is trivial. Well, the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts by inversion on $\mathrm{Cl}(\mathcal{O})$ by Lemma 1.44, which is a trivial action if and only if $\mathrm{Cl}(\mathcal{O})$ is 2-torsion. ■

Example 1.53. Consider the maximal order $\mathcal{O} = \mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-5})$. It turns out that $\mathrm{Cl}(\mathcal{O}) \cong (\mathbb{Z}/2\mathbb{Z})$. One can show that the minimal polynomial of one of the $j(E)$ for $E \in Y_{\mathcal{O}}$ is

$$x^2 - 1264000x - 681472000.$$

One can compute then that $\mathbb{Q}(j(E)) = \mathbb{Q}(\sqrt{5})$.

BIBLIOGRAPHY

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

[Ked21] Kiran S. Kedlaya. *Notes on Class Field Theory*. 2021. URL: https://kskedlaya.org/papers/cft-ptx.pdf.

List of Definitions