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 $(\mathfrak{a} \star E)(S) \coloneqq \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E(S))$; 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 an elliptic curve. Because $\mathfrak{a}$ is finitely presented, we have some exact sequence $\mathcal{O}^m \to \mathcal{O}^n \to \mathfrak{a} \to 0$, so there is a short exact sequence

$$0 \to (\mathfrak{a} \star E) \to E^n \to E^m$$

of fpqc sheaves, so we realize $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)$ as a commutative group scheme over k.

To check that $\mathfrak{a} \star E$ is an elliptic curve, we restrict $(\mathfrak{a} \star E)$ as a sheaf to the category of fpqc covers S of k equipped with an $\mathcal{O}$-action, in which case $(\mathfrak{a} \star E)(S) = \mathrm{Hom}_{\mathcal{O}(S)}(\mathfrak{a}(S), E(S))$. Because $\mathfrak{a}$ is locally free of rank 1 (over $\mathcal{O}$), we may find an open cover $\mathcal{U}$ of $\mathrm{Spec}\,\mathcal{O}$ trivializing $\mathfrak{a}$ so that

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

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

Remark 1.40. We take a moment to note that we have produced a well-defined group action. For example, adjusting $\mathfrak{a}$ or E up to isomorphism of course only adjusts $\mathfrak{a} \star E$ up to isomorphism, which can be seen by tracking through the construction. Additionally, we see that $\mathcal{O} \star E = \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}, E) = E$, which can be seen on the level of the sheaves. Lastly, we note that

$$(\mathfrak{a} \otimes \mathfrak{b}) \star E = \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a} \otimes \mathfrak{b}, E) = \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathrm{Hom}_{\mathcal{O}}(\mathfrak{b}, E)) = \mathfrak{a} \star (\mathfrak{b} \star E)$$

by the tensor–hom adjunction.

Example 1.41. 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 1.42. 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 1.41, 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 1.43. 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 1.42 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 1.44. 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 fpqc cover S of k, and we see that

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

On the other hand, we find

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

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 $\mathcal{O}$ 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 1.45. 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 $(p) \coloneqq \mathfrak{p} \cap \mathbb{Z}$ 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 1.46. 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 1.43), 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 1.47. 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 1.48. 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 $\mathbb{Q}$.

1.3.3 Stating the Main Theorem

We are now ready to (re)state the main theorems of complex multiplication. Roughly speaking, this says that our two actions agree under class field theory. Formally, we write down a character χ to measure how the two actions interact.

Notation 1.49. 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 1.50. Let's check that this χ makes sense. Note that $\chi(\sigma)$ is uniquely defined given E (by Proposition 1.42), 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 1.44).

And here is our theorem.

[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.

Theorem 1.51 (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 1.47.

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

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 1.51. 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 1.51, 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 1.51 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 1.42). ∎

Remark 1.53. The algebraic numbers $j(E)$ for $E \in Y_{\mathcal{O}}$ are called "singular moduli" in the literature. There is a relation to supersingular elliptic curves.

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 1.54. 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 1.51, the character χ is surjective, so the Galois group $\mathrm{Gal}(k/K)$ acts transitively on $Y_{\mathcal{O}}$ (see Proposition 1.42). 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 $\mathrm{Gal}(K/\mathbb{Q}) \ltimes \mathrm{Gal}(K(j(E))/K)$, 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 right by
$$\sigma \mathrm{Frob}_{\mathfrak{p}} \sigma^{-1} = \mathrm{Frob}_{\sigma\mathfrak{p}}$$
and hence on the left 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 1.45, which is a trivial action if and only if $\mathrm{Cl}(\mathcal{O})$ is 2-torsion. ∎

Example 1.55. 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 $\mathbb{Q}(j(E)) = \mathbb{Q}(\sqrt{5})$.

1.4 January 30

Starting next week, we will meet in Krieger 204. Office hours are right after class.

1.4.1 Adding Level Structure

As usual, we let $\mathcal{O}$ be an order of an imaginary quadratic field K of conductor f; throughout, we fix an embedding of K into a fixed algebraically closed field k of characteristic 0.

We begin today by sharpening our main theorem. We began by saying that we are interested in K^{ab}, but it is not enough to look at the Hilbert class field of $\mathrm{Cl}(\mathcal{O})$, and it is even not enough to look at the union of all the Hilbert class fields.

Remark 1.56. Let's describe some fields we cannot from this Hilbert class field construction. By class field theory, we see that we are interested in knowing how small

$$\bigcap_f \widehat{\mathcal{O}}_f^\times \subseteq \mathbb{A}_K^\times$$

is, where $\mathcal{O}_f \subseteq \mathcal{O}_K$ is the order of conductor f. This can be seen in the computation of $\widehat{\mathcal{O}}_f^\times$ executed in Proposition 1.24; we will run this computation on the homework.

To get the remaining abelian extensions, we add level structure. Level structure is an important notion in the realm of moduli spaces (and Shimura varieties more specifically), so this is a natural thing to do.

Notation 1.57. Fix an algebraically closed field k of characteristic 0 and an order $\mathcal{O}$ of an imaginary quadratic field K. Given a positive integer N, we define $Y_{\mathcal{O}}(N) \subseteq Y(N)$ as collections of pairs (Y, τ) where $E \in Y_{\mathcal{O}}$ and $\tau\colon E[N] \to (\mathcal{O}/N\mathcal{O})$ is an isomorphism. We also write $Y_{\mathcal{O}}(\infty)$ to mean keeping track of "full" level structure, which amounts to having an isomorphism

$$\tau\colon \varprojlim_N E[N] \to \widehat{\mathcal{O}}^2.$$

Remark 1.58. The last isomorphism amounts to having a list of isomorphisms $T_pE \cong \mathcal{O} \otimes \mathbb{Z}_p$ for all primes p (via the Chinese remainder theorem).

Remark 1.59. We quickly check that $E[N]$ is in fact free of rank 1 over $\mathcal{O}/N\mathcal{O}$, which explains why these level structure maps τ can all exist. The definition of everything can come down to an algebraically closed field of finite transcendence degree over $\mathbb{Q}$, so it suffices to check this over $\mathbb{C}$. But now $E(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$, so the N-torsion is isomorphic to $\frac{1}{N}\mathfrak{a}/\mathfrak{a}$, which we see is in fact free of rank 1 over $\mathcal{O}/N\mathcal{O}$.

The class group action on $Y_{\mathcal{O}}$ now upgrades to a richer action of the idele class group. We begin by explaining how to add level structure to the class group. The following result is essentially a refinement of Proposition 1.24.

Notation 1.60. Fix an order $\mathcal{O}$ of an imaginary quadratic field K. For positive integer $N \geq 1$, we define the group $\mathrm{Cl}(\mathcal{O})(N)$ as consisting of isomorphisms classes of pairs $(\mathfrak{a}, \tau)$ where $\mathfrak{a}$ is a line bundle, and $\tau\colon \mathfrak{a}/N\mathfrak{a} \to \mathcal{O}/N\mathcal{O}$ is some isomorphism. Similarly, we define the group $\mathrm{Cl}(\mathcal{O})(\infty)$ as consisting of isomorphisms classes of pairs $(\mathfrak{a}, \tau)$ where $\mathfrak{a}$ is a line bundle, and τ is a level structure isomorphism

$$\widehat{\mathcal{O}} \cong \varprojlim_N \mathfrak{a}/N\mathfrak{a}.$$

Remark 1.61. Let's explain how this is a group: two pairs $(\mathfrak{a}, \tau)$ and $(\mathfrak{a}', \tau')$ can be multiplied by the tensor product $(\mathfrak{a} \otimes \mathfrak{a}', \tau \otimes \tau')$, where $(\tau \otimes \tau')$ is the composite

$$\widehat{\mathcal{O}} = \widehat{\mathcal{O}} \otimes \widehat{\mathcal{O}} \cong \varprojlim_N \mathfrak{a}/N\mathfrak{a} \otimes \varprojlim_N \mathfrak{a}'/N\mathfrak{a}' = \varprojlim_N (\mathfrak{a} \otimes \mathfrak{a}')/N(\mathfrak{a} \otimes \mathfrak{a}').$$

For example, the identity is $(\mathcal{O}, \mathrm{id}_{\widehat{\mathcal{O}}})$, and inverses can be constructed by inverting the line bundle.

Lemma 1.62. Fix an order $\mathcal{O}$ of an imaginary quadratic field K. Then the isomorphism (b) of Proposition 1.24 upgrades to an isomorphism between $K^\times \backslash \mathbb{A}_K^\times$ and the group $\mathrm{Cl}(\mathcal{O})(\infty)$ of pairs $(\mathfrak{a}, \tau)$ where $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ and τ is a level structure isomorphism

$$\widehat{\mathcal{O}} \cong \varprojlim_N \mathfrak{a}/N\mathfrak{a}.$$

Proof. We proceed as in the proof of (b) of Proposition 1.24. We begin by describing the map. Fix some pair $(\mathfrak{a}, \tau)$, and we remark that the data of τ (by the Chinese remainder theorem) provides equivalent data to a collection of isomorphisms

$$\tau_p\colon \widehat{\mathcal{O}}_p \to \varprojlim_\bullet \mathfrak{a}/p^\bullet\mathfrak{a},$$

and this right-hand side is simply $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. To define our map, choose an open subset $U \subseteq \operatorname{Spec} \mathbb{Z}$ such that there is an isomorphism $\varphi\colon \mathfrak{a}_U \to \mathcal{O}_U$. Then for each prime p, we define α_p as the image of 1 under the long composite

$$K_p = \mathcal{O}_U \otimes_{\mathbb{Z}_U} \mathbb{Q}_p \overset{\varphi}{\cong} \mathfrak{a}_U \otimes_{\mathbb{Z}_U} \mathbb{Q}_p = \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \overset{\tau_p}{\cong} \widehat{\mathcal{O}}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = K_p.$$

We now check that the tuple $(\alpha_p)_p$ defines an element of $\mathbb{A}_K^\times$ and then provides a well-defined bijection to $K^\times \backslash \mathbb{A}_K^\times$.

- We claim that $(\alpha_p)_p \in \mathbb{A}_K^\times$. Certainly $\alpha_p \in K_p^\times$ for all p, because the long composite is an isomorphism of K_p-modules. Additionally, for each $p \in U$, we see that the long composite can also be seen as

  $$\widehat{\mathcal{O}}_p = \mathcal{O}_U \otimes_{\mathbb{Z}_U} \mathbb{Z}_p \overset{\varphi}{\cong} \mathfrak{a}_U \otimes_{\mathbb{Z}_U} \mathbb{Z}_p = \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p \overset{\tau_p}{\cong} \widehat{\mathcal{O}}_p,$$

  allowing us to conclude that $\alpha_p \in \widehat{\mathcal{O}}_p^\times$ for all $p \in U$. So we are done after noting that all but finitely many primes live in U.

- We claim that the class of $(\alpha_p)_p$ in $K^\times \backslash \mathbb{A}_K^\times$ does not depend on the choice of U. Well, suppose that we are given two local trivializations $\varphi\colon \mathfrak{a}_U \to \mathcal{O}_U$ and $\psi\colon \mathfrak{a}_V \to \mathcal{O}_V$, which produce the elements $(\alpha_p)_p \in \mathbb{A}_K^\times$ and $(\beta_p)_p \in \mathbb{A}_K^\times$. Well, the image of 1 under the composite

  $$K = \mathcal{O}_U \otimes_{\mathbb{Z}_U} \mathbb{Q} \overset{\varphi}{\cong} \mathfrak{a}_U \otimes_{\mathbb{Z}_U} \mathbb{Q} = \mathfrak{a}_V \otimes_{\mathbb{Z}_V} \mathbb{Q} \overset{\psi}{\cong} \mathcal{O}_V \otimes_{\mathbb{Z}_V} \mathbb{Q} = K$$

  produces some $\gamma \in K$. Then the construction of γ makes the left square of the diagram

  $$\begin{array}{ccccc} K_p & \xleftarrow{\varphi} & \mathfrak{a}_U \otimes_{\mathbb{Z}_U} \mathbb{Q}_p & \xrightarrow{\tau_p} & K_p \\ {\scriptstyle\gamma}\downarrow & & \| & & \| \\ K_p & \xleftarrow{\psi} & \mathfrak{a}_V \otimes_{\mathbb{Z}_V} \mathbb{Q}_p & \xrightarrow{\tau_p} & K_p \end{array}$$

commute, thereby showing $\alpha_p = \gamma\beta_p$ for all primes p. Thus, our idele is well-defined in $K^\times\backslash\mathbb{A}_K^\times$.

- We claim that the idele class also does not depend on the isomorphism class of $(\mathfrak{a},\tau)$. This is a matter of tracking everything through: an isomorphism $(\mathfrak{a},\tau)\cong(\mathfrak{a}',\tau')$ amounts to an isomorphism $\mathfrak{a}\cong\mathfrak{a}'$ commuting with the choice of level structure isomorphisms τ and τ', thereby producing a commutative diagram

$$\begin{array}{ccccc} K_p & \xleftarrow{\varphi} & \mathfrak{a}_U\otimes_{\mathbb{Z}_U}\mathbb{Q}_p & \xrightarrow{\tau_p} & K_p \\ \| & & \downarrow & & \| \\ K_p & \longleftarrow & \mathfrak{a}_V\otimes_{\mathbb{Z}_V}\mathbb{Q}_p & \xrightarrow{\tau_p'} & K_p \end{array}$$

  once we choose a local trivialization $\varphi\colon\mathfrak{a}_U\to\mathcal{O}_U$. So we see that the ideles produced by $(\mathfrak{a},\tau)$ and $(\mathfrak{a}',\tau')$ are the same.

- We quickly note that the given map is a group homomorphism: multiplication of pairs is given by $(\mathfrak{a},\tau)\cdot(\mathfrak{a}',\tau')=(\mathfrak{a}\otimes\mathfrak{a}',\tau\otimes\tau')$ (where we are viewing $\mathrm{Cl}(\mathcal{O})$ as providing isomorphism classes of line bundles). Then running the above construction to take two trivializations $\varphi\colon\mathfrak{a}_U\to\mathcal{O}_U$ and $\varphi'\colon\mathfrak{a}_U'\to\mathcal{O}_U$ (for U small enough), we see that we can take the tensor product of the two composites $K_p\to K_p$ (one for $\mathfrak{a}$ and one for $\mathfrak{a}'$) to reveal that the trivialization $(\varphi\otimes\varphi')\colon(\mathfrak{a}\otimes\mathfrak{a}')_U\to\mathcal{O}_U$ yields the product of the ideles given by $\mathfrak{a}$ and $\mathfrak{a}'$ respectively.

- We check that our map extends the one of Proposition 1.24. Namely, we must check that the diagram

$$\begin{array}{ccc} \mathrm{Cl}(\mathcal{O})(\infty) & \longrightarrow & K^\times\backslash\mathbb{A}_K^\times \\ \downarrow & & \downarrow \\ \mathrm{Cl}(\mathcal{O}) & \longrightarrow & K^\times\backslash\mathbb{A}_K^\times/T(\widehat{\mathbb{Z}}) \end{array}$$

  commutes, where the bottom map is given by Proposition 1.24.

  This amounts to recasting the bottom map as follows. The bottom map takes $\mathfrak{a}\in\mathrm{Cl}(\mathcal{O})$, chooses a local trivialization $\varphi\colon\mathfrak{a}_U\to\mathcal{O}_U$, and then it produces an idele $(\alpha_p)_p$ by letting α_p be the image under the composite

$$K_p=\mathcal{O}_U\otimes_{\mathbb{Z}_U}\mathbb{Q}_p\overset{\varphi}{\cong}\mathfrak{a}_U\otimes_{\mathbb{Z}_U}\mathbb{Q}_p=\mathfrak{a}_{U_p}\otimes_{\mathbb{Z}_{U_p}}\mathbb{Q}_p\overset{\tau_p}{\cong}\mathcal{O}_{U_p}\otimes_{\mathbb{Z}_{U_p}}\mathbb{Q}_p=K_p,$$

  where $\tau_p\colon\mathfrak{a}_{U_p}\to\mathcal{O}_{U_p}$ is some other chosen local trivialization. It is now relatively clear that this map is simply the above map after being forced to find of all "level structure isomorphisms" τ_p.

- We check that the given map is injective. Suppose some pair $(\mathfrak{a},\tau)$ produces an idele $(\alpha_p)_p\in\mathbb{A}_K^\times$ which is actually some element $\alpha\in K^\times$. Then we must show that $(\mathfrak{a},\tau)$ is trivial. Note that the idele is certainly trivial in the double quotient $K^\times\backslash\mathbb{A}_K^\times/T(\widehat{\mathbb{Z}})$, so Proposition 1.24 allows us to assume that $\mathfrak{a}$ is trivial and hence equal to $\mathcal{O}$.

  Thus, we may choose the local trivialization φ to be the identity $\mathcal{O}=\mathcal{O}$, and we see that α_p becomes the image of 1 under the isomorphism $\tau_p\colon\widehat{\mathcal{O}}_p\to\widehat{\mathcal{O}}_p$. For example, this implies that $\alpha\in\mathcal{O}^\times$. Thus, we see that the isomorphism $\alpha\colon\mathcal{O}\to\mathcal{O}$ provides an isomorphism between $(\mathcal{O},\tau)$ and the identity $(\mathcal{O},\mathrm{id})$ of $\mathrm{Cl}(\mathcal{O})(\infty)$.

- We check that the given map is surjective. By the surjectivity that we already have from Proposition 1.24, it is enough to surject onto $T(\widehat{\mathbb{Z}})$. Well, note that any $\tau\in T(\widehat{\mathbb{Z}})$ induces an automorphism $\tau\colon\widehat{\mathcal{O}}^\times\to\widehat{\mathcal{O}}^\times$ (given by multiplication). Then the pair $(\mathcal{O},\tau)\in\mathrm{Cl}(\mathcal{O})(\infty)$ goes to $\tau\in T(\widehat{\mathbb{Z}})$ by construction: use $\mathrm{id}\colon\mathcal{O}\to\mathcal{O}$ for the local trivialization, and then the produced idele can be seen to be τ by construction. ■

Lemma 1.63. Fix an algebraically closed field k of characteristic 0 and an order $\mathcal{O}$ of an imaginary quadratic field K embedded in k. Then the action of $\mathrm{Pic}(\mathcal{O})$ on $Y_{\mathcal{O}}$ naturally extends to an action of $\mathrm{Cl}(\mathcal{O})(N)$ on $Y_{\mathcal{O}}(N)$, where N is either a positive integer or ∞.

Proof. We argue for $N = \infty$ because the claim at finite level follows from the same argument. Given pairs $(\mathfrak{a}, \tau_{\mathfrak{a}}) \in \mathrm{Cl}(\mathcal{O})(\infty)$ and $(E, \tau_E) \in Y_{\mathcal{O}}(\infty)$, we need to define some $(\mathfrak{a}, \tau_{\mathfrak{a}}) \star (E, \tau_E)$. To extend the existing class group action, we need to produce a pair of the form $(\mathfrak{a} \star E, \tau_\star)$, where $\tau_\star$ is some chosen level structure isomorphism. Well, we simply define $\tau_\star$ as the composite

$$\begin{aligned}\varprojlim (\mathfrak{a} \star E)[N] &= \varprojlim \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)[N] \\ &= \varprojlim \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E[N]) \\ &= \varprojlim \mathrm{Hom}_{\mathcal{O}/N\mathcal{O}}(\mathfrak{a}/N\mathfrak{a}, E[N]).\end{aligned}$$

Now, $\tau_{\mathfrak{a}}$ amounts to a compatible system of isomorphisms $\mathfrak{a}/N\mathfrak{a} \to \mathcal{O}/N\mathcal{O}$, and τ_E amounts to a compatible system of isomorphisms $E[N] \to \mathcal{O}/N\mathcal{O}$, so we see that they determine an isomorphism

$$\begin{aligned}\varprojlim (\mathfrak{a} \star E)[N] &= \varprojlim \mathrm{Hom}_{\mathcal{O}/N\mathcal{O}}(\mathfrak{a}/N\mathfrak{a}, E[N]) \\ &\overset{\tau}{\cong} \varprojlim \mathrm{Hom}_{\mathcal{O}/N\mathcal{O}}(\mathcal{O}/N\mathcal{O}, \mathcal{O}/N\mathcal{O}) \\ &= \widehat{\mathcal{O}}\end{aligned}$$

on the level of the inverse limit. This provides the action map.

It remains to check that we have actually defined a group action. Here are our checks.

- We note that changing $(\mathfrak{a}, \tau_{\mathfrak{a}})$ or (E, τ_E) up to isomorphism only adjusts $\mathrm{Hom}(\mathfrak{a}, E)$ up to isomorphism and then adjusts the level structure isomorphism $\tau_\star$ again up to isomorphism, essentially by construction.
- Note that $(\mathcal{O}, \mathrm{id}) \star (E, \tau_E) = (E, \tau_E)$ by tracking through the construction. In short, all expressions which look like $\mathrm{Hom}(\mathfrak{a}, E)$ get compressed into a single E, so the last isomorphism marked τ is simply τ_E.
- We check that $(\mathfrak{a}, \tau) \star ((\mathfrak{a}', \tau') \star (E, \tau_E)) = (\mathfrak{a} \otimes \mathfrak{a}', \tau \otimes \tau') \star (E, \tau_E)$. We already know that this is true without level structure, so it is enough to check that the level structure morphisms agree. Well, the tensor–hom adjunction can be seen to be natural enough to produce a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}', E))[N] & \xrightarrow{\tau} & \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}/N, \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}'/N, E[N])) \\ \| & & \| \\ \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a} \otimes \mathfrak{a}', E)[N] & \xrightarrow{\tau} & \mathrm{Hom}_{\mathcal{O}}((\mathfrak{a} \otimes \mathfrak{a}')/N, E[N]) \end{array}$$

  from which the claim follows upon taking an inverse limit over N everywhere. ∎

Lemma 1.64. Fix an algebraically closed field k of characteristic 0 and an order $\mathcal{O}$ of an imaginary quadratic field K embedded in k. Then the group $\mathrm{Cl}(\mathcal{O})(N)$ acts simply transitively on $Y_{\mathcal{O}}(N)$, where N is either a positive integer or ∞.

Proof. We argue for $N = \infty$ because the claim at finite level follows from the same argument. For two pairs $(E, \tau), (E', \tau') \in Y_{\mathcal{O}}(\infty)$, we need to show that there is a unique $(\mathfrak{a}, \tau_{\mathfrak{a}}) \in \mathrm{Cl}(\mathcal{O})$ such that $(\mathfrak{a}, \tau_{\mathfrak{a}}) \star (E, \tau) = (E', \tau')$. By Proposition 1.42, there is a unique $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ such that $\mathfrak{a} \star E = E'$, so it remains to show that $\tau_{\mathfrak{a}}$ is unique. Thus, we are looking for $\tau_{\mathfrak{a}}$ so that

$$\varprojlim \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}/N, E[N]) \overset{\tau'}{\cong} \widehat{\mathcal{O}}$$

is given by $f \mapsto \tau f \tau_{\mathfrak{a}}$. Equivalently, we are looking for $\tau_{\mathfrak{a}}$ so that

$$\varprojlim \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}/N, \mathcal{O}/N\mathcal{O}) \overset{\tau' \circ (\tau \circ -)}{\cong} \widehat{\mathcal{O}}$$

is given by $f \mapsto f\tau_{\mathfrak{a}}$. Well, one can certainly choose some compatible system of level structure isomorphisms $\mathfrak{a}/N \to \mathcal{O}/N\mathcal{O}$ (because $\mathfrak{a}$ is a line bundle, by working one prime at a time), and upon doing this, we see that we are looking for $\tau_{\mathfrak{a}} \in \widehat{\mathcal{O}}^{\times}$ so that the induced isomorphism

$$\varprojlim \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/N\mathcal{O}, \mathcal{O}/N\mathcal{O}) \cong \widehat{\mathcal{O}}$$

is given by $f \mapsto f\tau_{\mathfrak{a}}$. Now, this $\tau_{\mathfrak{a}}$ exists and is unique because the left-hand side is simply $\widehat{\mathcal{O}}$. ■

As before, we should add in a Galois action. For example, $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ will act on $Y_{\mathcal{O}}(N)$ by

$$\sigma(E, \tau) \coloneqq \left(\sigma(E), \tau \circ \sigma^{-1}\right),$$

where $\tau \circ \sigma^{-1}$ refers to the composite

$$\sigma(E)[N] = \sigma(E[N]) \overset{\sigma^{-1}}{\to} E[N] \overset{\tau}{\to} \mathcal{O}/N\mathcal{O}.$$

We won't check that this is actually a group action, though we remark that it can be done directly. By taking the inverse limit, we recover a group action of $\mathrm{Gal}(k/\mathbb{Q})$ on $Y_{\mathcal{O}}(\infty)$. Similarly, we note that there is a Galois action on $\mathrm{Cl}(\mathcal{O})(N)$ by

$$\sigma(\mathfrak{a}, \tau_{\mathfrak{a}}) \coloneqq \left(\sigma(\mathfrak{a}), \tau_{\mathfrak{a}} \circ \sigma^{-1}\right),$$

and one can check that this is a well-defined group actions by doing essentially the same checks; once again, there is an analogous action at infinite level by taking an inverse limit everywhere.

Remark 1.65. We also remark that $\sigma((\mathfrak{a}, \tau_{\mathfrak{a}}) \star (E, \tau_E)) = \sigma(\mathfrak{a}, \tau_{\mathfrak{a}}) \star \sigma(E, \tau_E)$. Without the level structures, this follows from Lemma 1.44, and checking that the level structures agree is a matter of noting that every part of the construction of the action in Lemma 1.62 commutes with applying the automorphism of $\mathrm{Gal}(K/\mathbb{Q})$.

Before continuing, let's say something about how this story fits in with Shimura varieties. Embed $K \subseteq \mathbb{C}$. Set $\mathcal{H}^{\pm} \coloneqq \mathbb{C} \setminus \mathbb{R}$, which we note is a Hermitian symmetric domain for GL_2, and it can be described as the family of homomorphisms $\mathrm{U}(1) \to \mathrm{GL}_2$ (as groups over $\mathbb{R}$),[2] which we note are described by sending $\left[\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right]$ to i.[3]

Now, the homomorphism belonging to τ is called a "special point" because it arises from a morphism of Shimura varieties. Roughly speaking, the point is that the stabilizer of τ contains a maximal torus defined over $\mathbb{Q}$. To be formal, set $T \coloneqq \mathrm{Res}_{\mathcal{O}/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}}$ as usual, and then T is the desired torus, and one finds that we have a morphism of Shimura varieties given by

$$T(\mathbb{Q}) \setminus T(\mathbb{A}_{\mathbb{Q},f}) \to \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f}) \times \mathcal{H}^{\pm}\right)$$

sending $[a]$ to $[(a, \tau)]$, where τ is defined by satisfying $\mathcal{O} = \mathbb{Z} \oplus \tau\mathbb{Z}$. Notably, even though the left-hand side does not depend on the choice of E or even of $\mathcal{O}$, but the morphism itself does because it needed us to choose a τ (though the choice of τ is removed when we mod out by $\mathrm{GL}_2(\mathbb{Q})$). Importantly, this right-hand side has a moduli interpretation in terms of elliptic curves with (full) level structure, so Lemma 1.63 is explaining what is coming out of this map given $a \in K^{\times} \backslash \mathbb{A}_{K,f}^{\times}$.

On the other hand, we see that there is a Galois action on the moduli interpretation $Y(\infty)$ of the right-hand Shimura variety. Roughly speaking, our main theorem of complex multiplication with this added level structure simply says that the Galois action pulled back to the idele class group $K^{\times} \backslash \mathbb{A}_{K,f}^{\times}$ is given by class field theory.

[2] We work with $\mathrm{U}(1)$ instead of $\mathbb{S}$ because we are allowed to ignore centers everywhere.
[3] One could also send it to $-i$; the sign choice here is a little arbitrary.

Theorem 1.66 (Main with level structure)**.** Fix an algebraically closed field k of characteristic 0 and an order $\mathcal{O}$ of an imaginary quadratic field K. Define $\chi\colon \mathrm{Gal}(k/K) \to \mathrm{Cl}(\mathcal{O})(\infty)$ by

$$\sigma(E,\tau) = \chi(\sigma) \star (E,\tau)$$

for $(E,\tau) \in Y_{\mathcal{O}}(\infty)$. Then χ, when composed with the isomorphism to $K^\times\backslash\mathbb{A}_K^\times$ given by Lemma 1.62, is the inverse of the Artin reciprocity map sending a uniformizer at $\mathfrak{p}$ to the arithmetic Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$.

Remark 1.67. Let's explain why χ is a well-defined character. Because $\mathrm{Cl}(\mathcal{O})(\infty)$ acts simply transitively on $Y_{\mathcal{O}}(\infty)$, certainly $\chi(\sigma)$ is uniquely determined by a single (E,τ). To get all $(E',\tau') \in Y_{\mathcal{O}}(\infty)$, use Lemma 1.64 to write $(E',\tau') = (\mathfrak{a},\tau_{\mathfrak{a}}) \star (E,\tau)$ and then apply Remark 1.65, writing

$$\sigma((\mathfrak{a},\tau_{\mathfrak{a}}) \star (E,\tau)) = \sigma(\mathfrak{a},\tau_{\mathfrak{a}}) \star \chi(\sigma) \star (E,\tau) = \chi(\sigma) \star ((\mathfrak{a},\tau_{\mathfrak{a}}) \star (E,\tau)).$$

Lastly, χ is a group homomorphism by its uniqueness: note

$$\chi(\sigma\sigma') = \sigma\sigma'(E,\tau) = \chi(\sigma) \star \chi(\sigma') \star (E,\tau).$$

Remark 1.68. For general Shimura varieties, no moduli description may be available, so one cannot "prove" the above theorem. Instead, one simply requires that these sorts of special point actions agree with class field theory, and then this is used to defined canonical models.

Remark 1.69. Choose $E \in Y_{\mathcal{O}}$, which we know is defined over the Hilbert class field H of $\mathcal{O}$. If we fix a model of E over H, then we obtain a Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/H)$ on the Tate module $T_\ell E$. However, we note that all the elliptic curves in $Y_{\mathcal{O}}$ are isogenous, which can be checked over $\mathbb{C}$: all proper ideals $\mathfrak{a}$ of $\mathcal{O}$ are homothetic because the embedding $\mathfrak{a} \subseteq \mathcal{O}$ has finite cokernel. Because isogenies of elliptic curves gives rise to an isomorphism of Tate modules, we then would expect the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $Y_{\mathcal{O}}$ to produce a Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on our chosen $T_\ell E$. However, these isomorphisms are only defined up to automorphisms of E, which amount to a choice of unit in $\mathcal{O}^\times$.

Remark 1.70. The main theorem of complex multiplication provides an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $Y_{\mathcal{O}}(\infty)$, so one may wonder if it will eventually recover the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/H)$ on our Tate module. The previous remark basically says that we can only recover this Galois action on the Tate module up to a unit in $\mathcal{O}^\times$. This will be explained further on the homework.

1.4.2 Proof of the Main Theorem

In this subsection, we will prove Theorem 1.66. By ignoring all the level structure, Theorem 1.51 follows as well. Philosophically, everything we have done so far has been rather formal, more or less amounting to defining and computing some actions.

We now must do something difficult. Roughly speaking, we are interested in comparing an automorphic "Hecke" action coming from the adelic quotient $K^\times\backslash\mathbb{A}_{K,f}^\times$ with a Galois action coming from $\mathrm{Gal}(\overline{K}/K)$. We take a moment to remark that this is not too different from relating the coefficients of a modular form (which is an automorphic object) to an elliptic curve (which is a motivic object), which is achieved via the Eichler–Shimura congruence relation. In short, the proof of the Eichler–Shimura congruence relation takes a reduction $\pmod p$ and then reduces everything to a statement about isogenies of elliptic curves over finite fields.

Let's proceed with the proof. We proceed in steps.

1. We remark that it is enough to check the result at finite level N. Indeed, the theorem amounts to checking that the triangle

$$\begin{array}{ccc} K^\times\backslash\mathbb{A}_K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ \uparrow & \swarrow_{\chi} & \\ \mathrm{Cl}(\mathcal{O})(\infty) & & \end{array}$$

commutes, where Art_K is the global Artin map, and the left map is the isomorphism of Lemma 1.62. Establishing the result at finite level N amounts to checking that the outer square of the diagram

$$\begin{array}{ccc} K^\times\backslash\mathbb{A}_K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ \uparrow & \swarrow_{\chi} & \downarrow{\scriptstyle \chi_N} \\ \mathrm{Cl}(\mathcal{O})(\infty) & \twoheadrightarrow & \mathrm{Cl}(\mathcal{O})(N) \end{array}$$

commutes, where χ_N is induced by the right triangle. Because some $(\mathfrak{a},\tau) \in \mathrm{Cl}(\mathcal{O})(\infty)$ is uniquely determined by its reductions to all finite levels (because we could then recover $(\mathfrak{a},\tau)$ by taking a suitable inverse limit), this is enough.

We take a moment to note that χ_N can be defined by requiring

$$\sigma(E,\tau) = \chi_N(\sigma)\star(E,\tau)$$

for $(E,\tau) \in Y_{\mathcal{O}}(N)$, which is a well-defined character by Remark 1.67. It makes the right triangle commute by construction of χ_N (and noting that one may simply forget some amount of level structure at any time in the process).

2. Because $\mathrm{Cl}(\mathcal{O})(N)$ acts simply transitively on $Y_{\mathcal{O}}(N)$ (see Lemma 1.64), it is enough to fix a pair $(E,\tau) \in Y_{\mathcal{O}}(N)$ and check the commutativity of our square

$$\begin{array}{ccc} K^\times\backslash\mathbb{A}_K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \\ \uparrow & & \downarrow{\scriptstyle \chi_N} \\ \mathrm{Cl}(\mathcal{O})(\infty) & \twoheadrightarrow & \mathrm{Cl}(\mathcal{O})(N) \end{array}$$

by checking the action of the result in the bottom-right on our chosen (E,τ). Now, all pairs in $Y_{\mathcal{O}}(N)$ are defined over some fixed number field L (namely, one can give each E a model defined over L and further ensure that $E[N]$ is defined over L). Note that this makes the Galois action of $\mathrm{Gal}(\overline{K}/K)$ on (E,τ) factor through $\mathrm{Gal}(L/K)$.

We now define a set S of primes $\mathfrak{p}$ of K which has density 1, and we will more or less check the commutativity of the above square on the Frobenius elements $\mathrm{Frob}_{\mathfrak{p}}$ for $\mathfrak{p} \in S$. This will be enough because each element of $\mathrm{Gal}(L/K)$ takes the form $\mathrm{Frob}_{\mathfrak{p}}$ for some such prime $\mathfrak{p}$ by the Chebotarev density theorem.

   (i) We require that each $\mathfrak{p} \in S$ is totally split over the prime (p) of $\mathbb{Q}$ and is unramified all the way up in L. This cuts out a density-1 subset of primes.

   (ii) We remove from S the primes $\mathfrak{p}$ for which each E has bad reduction over any prime $\mathfrak{P}$ of L lying over $(p) = \mathfrak{p}\cap\mathbb{Z}$. This removes only finitely many primes.

   (iii) We further remove from S any primes $\mathfrak{p}$ which divide the level N or the conductor f of $\mathcal{O}$. This again only removes finitely many primes.

   (iv) Lastly, we remove from S any prime $\mathfrak{p}$ lying under some prime $\mathfrak{P}$ of L dividing $j(E)-j(E')$ for any pair of distinct $E, E' \in Y_{\mathcal{O}}$. (Note $j(E)$ and $j(E')$ are already integral at $\mathfrak{P}$ by the good reduction assumption.) This again only removes finitely many primes because $Y_{\mathcal{O}}$ is a finite set.

We remark that (iii) above is only possible because we passed to finite level.

3. We take a moment to set up some notation. For clarity, for each $\mathfrak{p} \in S$, we choose a uniformizer $\varpi_{\mathfrak{p}} \in K^\times \backslash \mathbb{A}_K^\times$ at $\mathfrak{p}$, and we will show we can write "$(\mathfrak{p}, \tau_{\mathfrak{p}})$" for the corresponding element in $\mathrm{Cl}(\mathcal{O})(\infty)$. Here, writing $\mathfrak{p}$ for an element of $\mathrm{Cl}(\mathcal{O})$ is slight abuse of notation, but we note that $\mathfrak{p} \cap \mathcal{O}$ is in fact a line bundle because $\mathfrak{p} \nmid f$: localizing at an open subset U containing f (but avoiding p), we see $\mathcal{O}_{K,U} = \mathcal{O}_U$, so $\mathfrak{p}$ has its inverse; and over f, $\mathfrak{p} \cap \mathcal{O}$ localizes to $\mathcal{O}$.

   As such, we will write $\mathfrak{p}$ for $\mathfrak{p} \cap \mathcal{O}$ whenever possible. Additionally, we note $\mathfrak{p} \in \mathrm{Cl}(\mathcal{O})$ corresponds to the class of $\varpi_{\mathfrak{p}} \in K^\times \backslash \mathbb{A}_K^\times / T(\widehat{\mathbb{Z}})$ (where $T = \mathrm{Res}_{\mathcal{O}/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}}$), which can be seen by construction of the map: away from p, we see that we have a local trivialization map $\mathfrak{p}_U = \mathcal{O}_U$, meaning that the produced idele (following Lemma 1.62) is given by a uniformizer at $\mathfrak{p}$.[4] We denote $\tau_{\mathfrak{p}} \colon \mathfrak{p}_p \to \widehat{\mathcal{O}}_p$ as the corresponding trivialization to this idele $\varpi_{\mathfrak{p}} \in K^\times \backslash \mathbb{A}_K^\times$.

   Tracking around the diagram, we now see that we are interested in showing

$$(\mathfrak{p}, \mathrm{id}) \star (E, \tau) \stackrel{?}{=} \chi_N(\mathrm{Frob}_{\mathfrak{p}}) \star (E, \tau)$$

   for each $\mathfrak{p} \in S$. Here, $\mathrm{id} \colon (\mathfrak{p} \cap \mathcal{O})/N(\mathfrak{p} \cap \mathcal{O}) \to \mathcal{O}/N\mathcal{O}$ is the level structure isomorphism obtained from noting that we may show this after localizing away from N and in particular at p so that $(\mathfrak{p} \cap \mathcal{O})_N = \mathcal{O}_N$. Anyway, evaluating both sides, we would like to show that

$$(\mathrm{Hom}_{\mathcal{O}}(\mathfrak{p}, E), \tau) \stackrel{?}{=} \left(\mathrm{Frob}_{\mathfrak{p}}(E), \tau \circ \mathrm{Frob}_{\mathfrak{p}}^{-1}\right).$$

4. We are now ready for the main claim, which is more or less a reduction of the desired equality given in the previous step. Fix a prime $\mathfrak{P}$ of L lying over $\mathfrak{p} \in S$. For any $(E', \tau') \in Y_{\mathcal{O}}(N)$, we denote the reduction modulo $\mathfrak{P}$ by $(\overline{E}', \overline{\tau}')$. Notably, the reduction $E'[N] \to \overline{E}'[N]$ is an isomorphism because $\mathfrak{P} \nmid N$.

   Note that the inclusion $\mathfrak{p} \subseteq \mathcal{O}$ induces a map $\pi \colon E \to (\mathfrak{p} \star E)$, which is non-constant and hence an isogeny. We then claim that the reduction

$$\overline{\pi} \colon \overline{E} \to \overline{\mathfrak{p} \star E}$$

   is isomorphic to the Frobenius morphism $\mathrm{Frob} \colon \overline{E} \to \overline{E}^{(p)}$ (as morphisms over $\overline{E}$). For continuity reasons, let's go ahead and prove the claim.

   Any morphism of curves over $\mathbb{F}_{\mathfrak{P}}$ can be separated into a purely inseparable part (which must then be an iterated Frobenius) followed by a separable part; this can be seen on the level of the extension of function fields. Because the Frobenius morphism is degree p and purely inseparable (which is visible on the level of the function fields), it will then be enough check that the above morphism has degree p and is purely inseparable, from which the claim follows by using the aforementioned decomposition. Here are our two checks.

   - We claim that $\overline{\pi}$ has degree p. Reduction preserves degree (for example, this can be seen on the level of the Tate module because the natural reduction map $T_\ell E \to T_\ell \overline{E}$ is an isomorphism away from $\mathfrak{P}$), so it is enough to check that the map $E \to (\mathfrak{p} \star E)$ has degree p. Similarly, degree is preserved by field extension, so we may compute this degree after base-changing to $\mathbb{C}$, allowing us to write $E(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$ for some proper ideal $\mathfrak{a} \subseteq \mathcal{O}$ and so

$$(\mathfrak{p} \star E)(\mathbb{C}) = \mathbb{C}/\left(\mathfrak{a}\mathfrak{p}^{-1}\right)$$

     by Example 1.41. Tracking through Example 1.41 reveals that the map $\overline{\pi} \colon E \to (\mathfrak{p} \star E)$ is given by a choice of isomorphism $\mathfrak{p}^{-1} \otimes_{\mathcal{O}} \mathbb{C} \to \mathbb{C}$, which has degree $[\mathcal{O} : \mathfrak{p} \cap \mathcal{O}]$ by a determinant computation. Now, because $\mathfrak{p} \nmid f$, we see that $[\mathcal{O} : \mathfrak{p} \cap \mathcal{O}] = [\mathcal{O}_K : \mathfrak{p}] = p$ (where the first equality is seen by localizing f).

[4] One may need to adjust a sign here to ensure that the uniformizer belongs to $\mathfrak{p}$ and not its inverse.

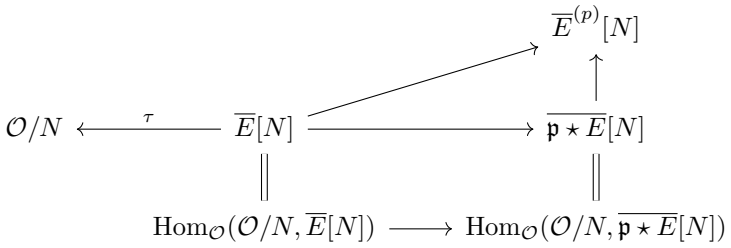
- We claim that $\overline{\pi}$ is purely inseparable. It is enough to check that the map vanishes on tangent spaces. Namely, we would like to show that the natural map $\pi^*\Omega_{\overline{\mathfrak{p}\star E}/\mathbb{F}_{\mathfrak{P}}} \to \Omega_{\overline{E}/\mathbb{F}_{\mathfrak{P}}}$ vanishes. Because taking differentials commutes with base-change, it is enough to check that $\pi^*\Omega_{(\mathfrak{p}\star E)/\mathbb{C}} \to \Omega_{E/\mathbb{C}}$ factors through some endomorphism $\alpha\colon \Omega_{E/\mathbb{C}} \to \Omega_{E/\mathbb{C}}$ where $\alpha \in \mathfrak{p}$. Dualizing differentials yields the tangent space, and we see that the computation of the previous step reveals that the morphism on differentials is some map $\mathbb{C} \to \mathbb{C}$ factoring through an isomorphism $\mathfrak{p}^{-1} \otimes_{\mathcal{O}} \mathbb{C} \to \mathbb{C}$, which indeed factors through the dual of some endomorphism $\alpha\colon \mathbb{C} \to \mathbb{C}$ for $\alpha \in \mathfrak{p}$ (up to homothety).
  Let's give a second, more Lie-theoretic argument. It is enough to check that the induced map $\operatorname{Lie}\overline{\pi}\colon \operatorname{Lie}\overline{E} \to \operatorname{Lie}(\overline{\mathfrak{p}\star E})$ vanishes, for which we choose to understand $\operatorname{Lie}\pi$. The main claim is that
  $$\operatorname{Lie}(\mathfrak{p}\star E) \stackrel{?}{=} \mathfrak{p}\star \operatorname{Lie} E,$$
  which can be checked by giving $\mathfrak{p}$ a finite presentation $\mathcal{O}^m \to \mathcal{O}^n \to \mathfrak{p} \to 0$ and noting that applying $\operatorname{Hom}_{\mathcal{O}}(-,E)$ and taking the kernel commute. Under the above equality, we find that $\operatorname{Lie}\pi$ is then induced by the embedding $\mathfrak{p} \hookrightarrow \mathcal{O}$. Because $\mathfrak{p} \subseteq \mathfrak{P}$, this map will then vanish $\pmod{\mathfrak{P}}$ by its construction.

5. We show the desired equality described at the end of the third step on the level of the elliptic curves. To begin, we claim that $\mathfrak{p}\star E \cong \operatorname{Frob}_{\mathfrak{p}}(E)$. The previous step showed that $\overline{\mathfrak{p}\star E} \cong \overline{E}^{(p)}$, so we see that
   $$j(\mathfrak{p}\star E) \equiv j(\operatorname{Frob}_{\mathfrak{p}}(E)) \pmod{\mathfrak{P}}.$$
   By construction of S (namely, condition (iv)), having this equivalence forces the required isomorphism.

6. We take a moment to note that the isomorphism $\mathfrak{p}\star E \to \operatorname{Frob}_{\mathfrak{p}}(E)$ can be chosen to agree with the isomorphism found after the reduction in the previous step. This is slightly tricky because the isomorphism described was constructed abstractly using j-invariants.
   For brevity, let $\varphi\colon (\mathfrak{p}\star E) \to \operatorname{Frob}_{\mathfrak{p}}(E)$ be any chosen isomorphism, and we note that it is well-defined up to an element of $\operatorname{Aut}\operatorname{Frob}_{\mathfrak{p}}(E) = \operatorname{Aut}(E) = \mathcal{O}^\times$. As such, we would like for the reduction diagram
   $$\begin{array}{ccc} \mathfrak{p}\star E & \xrightarrow{\varphi} & \operatorname{Frob}_{\mathfrak{p}}(E) \\ \downarrow & & \downarrow \\ \overline{\mathfrak{p}\star E} & \longrightarrow & \overline{E}^{(p)} \end{array}$$
   to commute up to an element of $\mathcal{O}^\times$; note that it currently commutes up to an element of $\operatorname{Aut}\overline{E}^{(p)} = \operatorname{Aut}\overline{E}$ (by the relevant uniqueness of the isomorphism in the bottom row), and $\operatorname{Aut}\overline{E}$ is potentially bigger than $\operatorname{Aut}E$! (More formally, we would like this diagram to agree after taking torsion.)
   The idea will be to restrict from general automorphisms of $\overline{E}$ to $\mathcal{O}$-linear ones. As such, we quickly claim that φ is $\mathcal{O}$-linear. Indeed, φ must induce a k-linear map on the level of the Lie algebras, so conjugation by φ is not allowed to induce complex conjugation on $\mathcal{O}$ because we have embedded $\mathcal{O} \subseteq K \subseteq k$ (see Remark 1.36).
   Thus, because φ is seen to be $\mathcal{O}$-linear, we see that the diagram will at worst commute up to an element of $\operatorname{Aut}_{\mathcal{O}}\overline{E}^{(p)} = \operatorname{Aut}_{\mathcal{O}}\overline{E}$. Thus, it remains to show that $\operatorname{Aut}_{\mathcal{O}}\overline{E} = \mathcal{O}^\times$. To begin, note that $\operatorname{End}_{\mathcal{O}}(\overline{E})_{\mathbb{Q}} = K$: if $\operatorname{End}\overline{E} \subseteq K$, then there is nothing to say; otherwise, $\operatorname{End}(\overline{E})$ is a quaternion algebra with maximal subfield K, so the centralizer of K is itself, and we are still done. Thus, we only have to check that $\alpha \in \operatorname{Aut}_{\mathcal{O}}(\overline{E})$ as an element of K will live in $\mathcal{O}$. There are two cases for denominators.

   - Note that α cannot have any denominators at the primes over p: because p is coprime to the conductor, we know $\mathcal{O}_p = \mathcal{O}_{K,p}$, and α is integral over $\mathbb{Z}$ must be in $\mathcal{O}_{K,p}$.
   - For M coprime to p, we know that α must induce an isomorphism $\overline{E}[M] \to \overline{E}[M]$, which after applying a level structure isomorphism means that multiplication by α is an isomorphism $\mathcal{O}/M\mathcal{O} \to \mathcal{O}/M\mathcal{O}$ of $\mathcal{O}$-modules. (Note that we have used the fact that α is $\mathcal{O}$-linear here!) Thus, α cannot have any denominators at any primes above any rational prime dividing M.

7. It remains to check the compatibility of the level structure morphisms. Because N-torsion is defined over the reduction, we may as well check that our level structure isomorphisms are equal over $\mathbb{F}_{\mathfrak{P}}$. For this, we write down the following large commutative diagram.



Here, the square commutes by definition of the top horizontal map, and the triangle commutes by the previous step. Notably, there is no ambiguity in the vertical isomorphism of the triangle as explained at the end of the previous paragraph.

By definition, the level structure isomorphism $(\mathfrak{p}\star E)[N] \to \mathcal{O}/N\mathcal{O}$ is given by following the bottom of the square and then composing with τ. Additionally, the level structure isomorphism $\overline{\mathrm{Frob}_{\mathfrak{p}}(E)}[N] \to \mathcal{O}/N\mathcal{O}$ is given by following the top of the diagram. However, the commutativity of the diagram implies that these two level structure isomorphisms are compatible with the isomorphism $\mathfrak{p}\star E \cong \mathrm{Frob}_{\mathfrak{p}}(E)$, so we are done.

Remark 1.71. The main claim in step 4 does not require all conditions (i)–(iv) of S. The proof only requires (i)–(iii), and (iv) is used later in the last steps.

Remark 1.72. We remark that one can remove condition (iv) from the proof if we reorganize the argument somewhat, as follows. Extend L to be large enough so that the composite

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\mathrm{Art}_K^{-1}} \mathbb{A}_K^{\times}/K^{\times} \to Y_{\mathcal{O}}(N)$$

factors through $\mathrm{Gal}(L/K)$. Then we are interested in showing the equality $\chi_N(\sigma) = \mathrm{Art}_K^{-1}(\sigma)$ for all $\sigma \in \mathrm{Gal}(L/K)$, or equivalently $\sigma(E) \cong \mathrm{Art}_K^{-1}(\sigma)\star E$ (with the equipped level structure). To check this last isomorphism, it is enough to check it after reduction for enough $\mathfrak{p}$ for which $\sigma = \mathrm{Frob}_{\mathfrak{p}}$ because the difference of the j-invariants have only finitely many prime factors.

1.5 February 4

We began class by reviewing the proof of the Main theorem of class field theory. Today we start Lubin–Tate theory.

1.5.1 Remarks on Hilbert's 12th Problem

Let's state the Kronecker–Weber theorem in motivating way.

Theorem 1.73 (Kronecker–Weber)**.** The field $\mathbb{Q}^{\mathrm{ab}}$ equals the field $\mathbb{Q}$ adjoining the torsion points of the group scheme $\mathbb{G}_{m,\mathbb{Q}}$.

Namely, the torsion points of $\mathbb{G}_{m,\mathbb{Q}}$ are the roots of unity, so this amounts to saying that $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyclo}}$, as usual.

From our theory of complex multiplication, we showed the following, which is roughly Kronecker's Jugendtraum.

Theorem 1.74 (Kronecker's Jugendtraum)**.** Fix an imaginary quadratic number field K. Then K^{ab} is the field K after adjoining the torsion points of a certain group scheme.

This group scheme was typically an elliptic curve with complex multiplication, but sometimes we had to take a quotient for reasons related to units.

The moral of the story is that one may look for a group scheme G over $\overline{\mathbb{Q}}$ such that its torsion points generate K^{ab} for a given number field K. Perhaps we would expect to see some similar torsor of an idele class group and Galois group so that we could tell a similar story. Such a thing does not exist for general number fields currently, but there is something for function fields using the theory of shtukas.

Remark 1.75. Note that the above examples all had $\dim G = 1$. This roughly has to do with the fact that we are looking for abelian extensions. For CM fields K, one can attempt to look at more extensions by looking at the Galois action on the moduli space of abelian varieties.

Lubin–Tate theory answers our call for an explicit class field theory, but it does not work for number fields: instead, we will work with local p-adic fields. We remark that many of our arguments will work in positive characteristic as well, but we will not pay so much attention to this.

1.5.2 Overview of Lubin–Tate Theory

Let's give a quick "lay of the land" for Lubin–Tate theory. Instead of working with an algebraic group G, we will work with the local analogue, which is a formal group. Approximately speaking, a formal group expressed a group in a formal neighborhood of the identity.

By way of motivation, let G be a 1-dimensional commutative algebraic group, and we let $0 \in G$ be the identity. Then the formal neighborhood $\widehat{G}_0$ of the identity amounts to a formal group. For example, if G is a group over a field K of dimension 1, then G in a neighborhood of the identity looks something like $K[[X]]$, and there is a multiplication law which roughly amounts to a formal power series in $K[[X,Y]]$. Roughly speaking, this includes the tangent space (and hence the Lie algebra) as a quotient, but we will also be interested in keeping track of higher-order data. Here is our definition.

Definition 1.76 (formal group)**.** Fix a ring A. Then a *formal group law* F over A is a formal power series $F(X,Y) \in A[[X,Y]]$ which satisfies the following conditions.

(a) Associativity: $F(F(X,Y),Z) = F(X,F(Y,Z))$.

(b) Identity: $F(0,Y) = Y$ and $F(X,0) = X$.

(c) Additivity: $F(X,Y) \equiv X + Y \pmod{X^2, XY, Y^2}$.

If in addition $F(X,Y) = F(Y,X)$, then we say that F is *commutative*. A *formal group* $\mathcal{G}$ is the data of the formal group law $F_{\mathcal{G}}$ but labeled separately.

Remark 1.77. Perhaps one should try to distinguish between the formal group law F and the actual (infinitesimal) formal group that it defines. We will not attempt to do so.

Remark 1.78. As a slightly formal comment, we remark that the composite $F(G_1(\underline{X}), \dots, G_n(\underline{X}))$ of formal power series is well-defined provided that none of the $G_\bullet$s have constant terms. The point is that $G_\bullet(\underline{X})^n$ will only have terms of degree at least n, so if we want to compute the coefficient of some term in $F(G_1(\underline{X}), \dots, G_n(\underline{X}))$, we only have to compute terms of each $G_\bullet$ up to the prescribed degree. Using this construction of composition, it is not hard to check things such as an associative law $(f \circ g) \circ h = f \circ (g \circ h)$ by reducing to a computation of lower-order terms for polynomials.

Technically speaking, we have defined a 1-dimensional formal group. Here, the fact that we are working with $A[[X,Y]]$ is meant to signify that we are working in a formal neighborhood. Namely, if we simply ignored all the higher-order data, we could recover a Lie algebra.

With any object, we want to have homomorphisms.

Definition 1.79 (homomorphism)**.** Fix a ring A. Then a *homomorphism* of formal groups $\mathcal{G}_1$ and $\mathcal{G}_2$ over A is the data of a formal power series $f \in XA[[X]]$ such that

$$F_{\mathcal{G}_2}(f(X), f(Y)) = f(F_{\mathcal{G}_1}(X,Y)).$$

Note that these composites make sense because all power series in sight lack a constant term.

With homomorphisms, we may define modules.

Definition 1.80. Fix rings $\mathcal{O}$ and A with a homomorphism $h\colon \mathcal{O} \to A$. Then a *formal $\mathcal{O}$-module over A* is a commutative 1-dimensional formal group $\mathcal{G}$ equipped with a homomorphism $\mathcal{O} \to \operatorname{End}\mathcal{G}$ lifting h at the level of Lie algebras. Explicitly, we require that the endomorphism $[\alpha] \in XA[[X]]$ of $\mathcal{G}$ belonging to some $\alpha \in \mathcal{O}$ satisfies

$$[\alpha] \equiv h(A)X \pmod{X^2}.$$

Remark 1.81. Morally, the Lie algebra condition is just asserting that our $\mathcal{O}$-action makes sense. The condition in this definition should be compared with Remark 1.35.

Let's see an example.

Example 1.82. Consider F which is the formal group law coming from $\mathbb{G}_m$. Namely, for $z \in \mathbb{G}_m$, we want our coordinate to be $X = z - 1$. Then we calculate

$$F(X,Y) = (X+1)(Y+1) - 1 = X + Y + XY,$$

and it can be checked to be a formal group law. For each integer $n \in \mathbb{Z}$, there is an endomorphism on $\mathbb{G}_m$ given by $z \mapsto z^n$, which we can map back to an endomorphism on the level of the formal group as providing the endomorphism $[n] = (X+1)^n - 1$. One can check directly that this is an endomorphism:

$$F([n]X, [n]Y) = (X+1)^n(Y+1)^n - 1 = [n]F(X,Y).$$

Remark 1.83. If $A = \mathbb{Z}_p$, then it turns out that the action by $\mathbb{Z}$ above can be extended to an action by $\mathbb{Z}_p$. Namely, for $n \in \mathbb{Z}_p$, one has a formal power series

$$[n] = \sum_{i \geq 1} \binom{n}{i} X^i.$$

This cannot be trivial: it works for $\mathbb{Z}_2$, but it does not work for $\mathbb{Z}_4$!

Next time, we will attempt to explain the preceding remark. Approximately speaking, we will show that with $A = \mathcal{O}$ (for local field K) and uniformizer ϖ admits a unique formal $\mathcal{O}$-module F_ϖ over $\mathcal{O}$ such that

$$[\varpi_K]X \equiv X^q \pmod{\mathfrak{p}_K}.$$

For example, it follows that the torsion $F_\varpi[\mathfrak{p}^n]$ are contained in some maximal ideal $\widehat{\mathfrak{p}}$ belonging to an algebraic closure of K. Thus, we can define a Tate module

$$T_\varpi F_\varpi \coloneqq \varprojlim F_\varpi[\mathfrak{p}^\bullet].$$

It turns out that $T_\varpi F_\varpi$ is a free $\mathcal{O}$-module of rank 1, so the Galois action on torsion here grants a character

$$\mathrm{Gal}(\overline{K}/K) \to \mathcal{O}^\times.$$

This turns out to produce the "totally ramified" part of local class field theory. Explicitly, if $\mathrm{Art}_K \colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the local Artin reciprocity map, then the fixed field $K_\varpi \coloneqq \left(K^{\mathrm{ab}}\right)^{\mathrm{Art}_K(\varpi)}$ is generated by the torsion elements $\bigcup_{n\geq 0} F_\varpi\left[\mathfrak{p}_K^n\right]$.

Example 1.84. Let's explain what we are trying to generalize. Take $K = \mathbb{Q}_p$. Then $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}_p^{\mathrm{unr}}$, where the unramified extensions are simply given by prime-to-p cyclotomic extensions. We will find that the uniformizer $p \in \mathbb{Z}_p$ produces the formal group law $X^p - X$, whose torsion gives exactly the p^∞th roots of unity μ_{p^∞}.

One can even recover some part of the theory of complex multiplication here.

1.6 February 4

Today we actually start Lubin–Tate theory. Throughout, for brevity, we may refer to a p-adic local field as a triple $(K, \mathcal{O}, \mathfrak{p})$ to mean that K is a p-adic field, $\mathcal{O}$ is its ring integer, and $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$.

1.6.1 The Main Theorem

Now, K is a p-adic field with rings of integers $\mathcal{O} \subseteq K$. For a base ring A, we have a notion of a formal $\mathcal{O}$-module law F over A.

We now discuss a construction which we will use throughout Lubin–Tate theory.

Notation 1.85. Fix a p-adic field K with ring of integers $\mathcal{O}$ and maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$. Let $(\widehat{K}, \widehat{\mathcal{O}}, \widehat{\mathfrak{p}})$ be a complete extension of $(K, \mathcal{O}, \mathfrak{p})$. Given a formal $\mathcal{O}$-module $\mathcal{G}$ over the base ring $\mathcal{O}$, we note that $\widehat{\mathfrak{p}}$ becomes a group with addition given by

$$a +_{\mathcal{G}} b \coloneqq \mathcal{G}_F(a, b).$$

Remark 1.86. Let's explain why this is a group. The fact that $\widehat{\mathfrak{p}}$ consists of elements of absolute value strictly less than 1, the power series $F(X, Y) \in \mathcal{O}[[X, Y]]$ will converge absolutely, so this definition at least makes sense. Then $\widehat{\mathfrak{p}}$ becomes a group under this addition by directly translating the conditions of the formal group law.

Example 1.87. For example, we could take $\widehat{K} \in \{K, K^{\mathrm{unr}}, \widehat{\overline{K}}\}$. In particular, the extension need not be finite or even algebraic.

Definition 1.88 (Tate module)**.** Fix a p-adic field K with ring of integers $\mathcal{O}$ and maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$. Let $(\widehat{K}, \widehat{\mathcal{O}}, \widehat{\mathfrak{p}})$ be a completion of the algebraic closure of $(K, \mathcal{O}, \mathfrak{p})$. Given a formal $\mathcal{O}$-module $\mathcal{G}$ over the base ring $\mathcal{O}$, we define the torsion subgroup

$$\mathcal{G}[\mathfrak{p}^n] \coloneqq \{x \in \widehat{\mathfrak{p}} : [a]x = 0\}$$

for any $n \geq 0$. We also write $\mathcal{G}[\mathfrak{p}^\infty] \coloneqq \bigcup_{n\geq 0} \mathcal{G}[\mathfrak{p}^n]$ and the Tate module $T_{\mathfrak{p}}\mathcal{G} = \varprojlim \mathcal{G}[\mathfrak{p}^\bullet]$.

Remark 1.89. Choose a uniformizer $\varpi \in \mathfrak{p}$. Then we claim that $\mathcal{G}[\mathfrak{p}^n] = \mathcal{G}[\varpi^n]$ for each $n \geq 0$. Indeed, certainly $\mathcal{G}[\mathfrak{p}^n] \subseteq \mathcal{G}[\varpi^n]$ because $\varpi^n \in \mathfrak{p}^n$. For the reverse inclusion, we note that any $a \in \mathfrak{p}^n$ takes the form $a = \varpi^n b$ for some $b \in \mathcal{O}$, so $\mathcal{G}[a] \subseteq \mathcal{G}[\varpi^n]$. We conclude that $\mathcal{G}[\mathfrak{p}^n] = \bigcap_{a \in \mathfrak{p}^n} \mathcal{G}[a]$ is contained in $\mathcal{G}[\varpi^n]$.

Now, here is our main theorem.

Theorem 1.90. Fix a p-adic field K with ring of integers $\mathcal{O}$ and maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$, and let $\varpi \in \mathfrak{p}$ be a uniformizer. Then there is a unique formal $\mathcal{O}$-module $\mathcal{G}_\varpi$ (up to isomorphism) such that

$$K_\pi \coloneqq K(\mathcal{G}[\mathfrak{p}^\infty])$$

is a maximal totally ramified abelian extension of K; it is in fact the such extension fixed by $\operatorname{Art}_K(\varpi) \in \operatorname{Gal}(K^{\mathrm{ab}}/K)$, where $\operatorname{Art}_K \colon K^\times \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ is the local Artin map.

Remark 1.91. Let's give some indication of what is going on under the hood. We will find that $T_{\mathfrak{p}} G_\varpi$ is a free rank-1 module over $\mathcal{O}$. Then the Galois action of $\operatorname{Gal}(K^{\mathrm{ab}}/K)$ on $T_{\mathfrak{p}} G_\varpi$ will induce a character $\eta_\varpi \colon \operatorname{Gal}(\overline{K}/K) \to \mathcal{O}^\times$ defined by

$$\eta_\varpi(\sigma) \cdot v = \sigma(v)$$

for any $v \in T_{\mathfrak{p}} G_\varpi$. We will show that η_ϖ is characterized by having $\operatorname{Art}_K^{-1}(a) = \varpi^\bullet \eta_\varpi(a)$ for some power $\varpi^\bullet$.

Remark 1.92. Roughly speaking, the "uniqueness up to isomorphism" corresponds to choosing a different "local coordinate" at the identity of the ambient group scheme.

Remark 1.93. For some torsion point $x \in \mathcal{G}[\mathfrak{p}^\infty]$, we note that the ring $\mathcal{O}[x]$ (and hence the field $K(x)$) is well-defined up to isomorphism of $\mathcal{G}$. Indeed, a homomorphism $\varphi \colon \mathcal{G} \to \mathcal{G}'$ translates x to $\varphi_F(x)$, which we note converges absolutely because $x \in \widehat{\mathfrak{p}}$. Then the completeness of $\mathcal{O}[x]$ (because $K(x)$ is finite over K) implies hat $\varphi_F(x) \in \mathcal{O}[x]$. Thus, if φ is an isomorphism, we find $\mathcal{O}[x] = \mathcal{O}[\varphi_F(x)]$.

We are going to use the $\mathfrak{p}$-torsion to construct the maximal ramified extensions of K.

1.6.2 Relation to Complex Multiplication

The proof of Theorem 1.90 is rather elementary: one simply needs to manipulate certain power series with certain constraints. To motivate the following discussion, let's relate Lubin–Tate theory to the theory of complex multiplication we already built.

As before, we let K be a quadratic imaginary extension of $\mathbb{Q}$. We know that the action of $\operatorname{Gal}(\overline{K}/K)$ on $Y_{\mathcal{O}_K}(\infty)$ produces a character

$$\operatorname{Gal}(K^{\mathrm{ab}}/K) \to K^\times \backslash \mathbb{A}_{K,f}^\times,$$

which provides some version of explicit class field theory. We remark that an explicit computation of this map requires the choice of an elliptic curve E with complex multiplication by an order $\mathcal{O} \subseteq \mathcal{O}_K$; in the sequel, we will go ahead and take $\mathcal{O} = \mathcal{O}_K$.

For a choice of finite prime v (and a prime of $\overline{K}$ lying over it), we suppose that we want to understand the abelian extensions of K_v. Compatibility between local and global class field theory produces a commutative diagram

$$\begin{array}{ccc} K_v^\times & \hookrightarrow & \operatorname{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \vdots \\ K^\times \backslash \mathbb{A}_{K,f}^\times & \hookrightarrow & \operatorname{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

and so $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$ embeds into $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Thus, abelian extensions of K_v can be found as closed subgroups of $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$, which then produce closed subgroups of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. The commutativity of the diagram now translates into the statements that abelian extensions of K_v can be found as localizations of abelian extensions of K.

For simplicity, we will assume that the Hilbert class field H of $\mathcal{O}_K$ is contained in K_v, so E is defined over K_v, and we will assume that E has good reduction at v. Namely, E becomes defined over $\mathcal{O}_v$, and a formal neighborhood of the identity $e \in E$ produces a formal group $\mathcal{G}_E$ over $\mathcal{O}_v$.

Remark 1.94. Note $\mathcal{G}_E$ has an $\mathcal{O}_K$-action coming from E, and $T_{\mathfrak{p}}\mathcal{G}_E$ also has an action by $\mathcal{O}_v$, but it is not clear that these actions will agree.

Now, we are interested in constructing a maximal totally ramified abelian extension of K_v. If ℓ is a rational prime away from $\mathfrak{p}$, then the Galois action

$$\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \to \mathrm{Aut}\, T_\ell E$$

has finite image for topological reasons: this is a homomorphism from a v-adic group to an ℓ-adic group. So when we are on the hunt for totally ramified extensions, we should be looking for torsion at $\mathfrak{p}$.

Now, Theorem 1.90 explains that we may as well look at $\mathfrak{p}$-torsion for $\mathcal{G}_E$ already living in the maximal ideal $\widehat{\mathfrak{p}}$ associated to a completion of the algebraic closure $\overline{K}$. This means that we expect the $\mathfrak{p}$-power-torsion to reduce to 0 in a reduction, and this is something that we can check directly.

Theorem 1.95. Fix an elliptic curve E with complex multiplication by an order $\mathcal{O}$ over some imaginary quadratic field K. Suppose that E has good reduction at some prime $\mathfrak{P}$ of the Hilbert class field H of $\mathcal{O}$, and let (p) be the rational prime lying under $\mathfrak{P}$. Then the reduction $\overline{E}$ at $\mathfrak{P}$ is supersingular if and only if there is a unique prime $\mathfrak{p}$ in K over (p).

Proof. The hypotheses and conclusion are all isogeny-invariant: namely, the good reduction by the Néron–Ogg–Shafarevich criterion, the supersingular by the criterion given by p-torsion, and the uniqueness of the prime $\mathfrak{p}$ does not depend on E at all. Thus, we can use an isogeny to transform E into an elliptic curve with complex multiplication by $\mathcal{O}_K$; explicitly, there is an isogeny over $\mathbb{C}$ because all the lattices with CM by an order in K are homothetic.

Having $\mathcal{O} = \mathcal{O}_K$ is helpful for the following reason: we claim that $\mathrm{Frob}_{\mathfrak{P}}$ as an endomorphism of $\overline{E}$ will lift to an endomorphism of E. If $\mathrm{End}\,\overline{E}$ is an order in a quadratic field K, then there is nothing to do because we are forced to have $\mathrm{End}\,\overline{E} = \mathcal{O}_K = \mathrm{End}\,E$. Otherwise, $\mathrm{End}\,\overline{E}$ is an order in a quaternion algebra, then we note that the Frobenius commutes with the action by $\mathcal{O}$, so we instead claim that the reduction

$$\mathrm{End}_{\mathcal{O}}\, E \to \mathrm{End}_{\mathcal{O}}\, \overline{E}$$

is surjective, which will complete the claim paragraph. Because $\mathrm{End}(\overline{E})_{\mathbb{Q}}$ is a quaternion algebra, we see that K is a maximal subfield, so its centralizer is itself, so certainly $\mathrm{End}_{\mathcal{O}}(E)_{\mathbb{Q}} = K = \mathrm{End}_{\mathcal{O}}(\overline{E})_{\mathbb{Q}}$. However, any element in any of these endomorphism rings must be integral over $\mathbb{Z}$, so we conclude that $\mathrm{End}_{\mathcal{O}}(E) = \mathcal{O}_K = \mathrm{End}_{\mathcal{O}}(\overline{E})$.

Remark 1.96. Note that we used the trick of noting $\mathrm{End}_{\mathcal{O}}\,\overline{E} = \mathrm{End}_{\mathcal{O}}\,E$ previously at the end of the proof of the main theorem of complex multiplication.

We now proceed with the proof. There are two cases.

- Suppose that (p) splits as $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in K. In particular, $\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{p} = p$. We would like to check that $\overline{E}$ fails to be supersingular, which means that we are on the hunt for a nontrivial element in $\overline{E}[p]$. Note that it is enough to find a separable endomorphism of $\overline{E}$ of p-power degree: the kernel will be nontrivial because the morphism is separable, and it provides p-power torsion for degree reasons.

  Choose $\mathfrak{p} \in \{\mathfrak{p}_1, \mathfrak{p}_2\}$ lying under $\mathfrak{P}$, and let $\sigma(\mathfrak{p})$ be the other prime, which we note is the complex conjugate. We may choose some positive integer m so that $\mathfrak{p}^m$ is principal; say $\mathfrak{p}^m = \mu\mathcal{O}_K$. Then $\sigma(\mathfrak{p})^m = \sigma(\mu)\mathcal{O}_K$. We claim that $\sigma(\mu)\colon E \to E$ is the required morphism. Here are our checks.

  - The degree can is p-power because $\deg \mu = \deg \sigma(\mu)$, and $\mu\sigma(\mu) = \mathrm{N}_{K/\mathbb{Q}}\,\mu = p^m$.
  - To see that $\sigma(\mu)$ is separable after the reduction, we note that $\sigma(\mu)$ acts on the tangent space $\mathrm{Lie}\, E = \mathcal{O}_K$ by multiplication-by-$\sigma(\mu)$,[5] which is nontrivial in $\mathcal{O}_K \subseteq \mathcal{O}_L/\mathfrak{P}$ because $\sigma(\mu) \notin \mathfrak{P}$ by construction!

- Suppose that (p) has only prime upstairs in K, and let $\mathfrak{p}$ be the prime living above it. Then we recall from previously that $\mathrm{Frob}_{\mathfrak{P}}$ must be an endomorphism in $\mathrm{End}\, E = \mathcal{O}_K$, so we may find $\mu \in \mathcal{O}_K$ with $\mu = \mathrm{Frob}_{\mathfrak{P}}$. For example, this implies that $\mathrm{N}_{K/\mathbb{Q}}\,\mu = \deg \mathrm{Frob}_{\mathfrak{P}} = \#\mathbb{F}_{\mathfrak{P}}$ is a power of p, so $\mu \in \mathfrak{p}$. Now, the dual of $\mathrm{Frob}_{\mathfrak{P}}$, labeled $\mathrm{Frob}_{\mathfrak{P}}^\vee$ must be equal to $\sigma(\mu)$ because

$$\mu\sigma(\mu) = \mathrm{N}_{K/\mathbb{Q}}\,\mu = \deg \mathrm{Frob}_{\mathfrak{P}} = \mathrm{Frob}_{\mathfrak{P}} \circ \mathrm{Frob}_{\mathfrak{P}}^\vee.$$

  Thus, we also find that $\sigma(\mu) \in \mathfrak{p}$; it must have the same valuation, so we are granted some unit $u \in \mathcal{O}_K^\times$ such that $\sigma(\mu) = u\mu$: they have the same norm and thus both generate the same principal ideal (which is a power of (p))! Then

$$\mathrm{Frob}_{\mathfrak{P}}^\vee = \sigma(\mu) = u\mathrm{Frob}_{\mathfrak{P}}$$

  stays purely inseparable, so the morphism $[\deg \mathrm{Frob}_{\mathfrak{P}}]$ is purely inseparable, so $\overline{E}[p] = 1$. We conclude that $\overline{E}$ is supersingular. ■

The moral of the story is that when $K_{\mathfrak{p}}/\mathbb{Q}_p$ is in fact quadratic (namely, there is more than one prime of K living above (p)), all p-power torsion of E can be seen on the level of $\widehat{\mathfrak{p}}$ with group structure given by $\mathcal{G}_E$. Thus, we are actually allowed to look at some formal group with $\widehat{\mathfrak{p}}$.

Remark 1.97. The proof above raises a bizarre question: what is the element $\mu \in \mathcal{O}_K$ which induces the Frobenius action by $\mathrm{Frob}_{\mathfrak{P}}$ on E? However, this question does not make sense: the hunt for an element μ depends on a choice of model of E over H.

Letting E be defined over the Hilbert class field H of $\mathcal{O}_K$, we note that its model is not unique and indeed depends on the choice of cocycle in the continuous cohomology group

$$\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/H), \mathrm{Aut}_{\mathcal{O}}(E)).$$

Because $\mathrm{Aut}_{\mathcal{O}}(E) = \mathcal{O}^\times$, we see that the Galois action is trivial, so this is $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\mathbb{Q}}/H), \mathcal{O}^\times)$. Then the reduction $\pmod{\mathfrak{P}}$ of E is going to be defined up to an element of

$$\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\mathbb{Q}}_{\mathfrak{P}}/\mathbb{Q}_{\mathfrak{P}}), \mathcal{O}^\times) \supseteq \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}}), \mathcal{O}^\times) = \mathcal{O}^\times.$$

Upon changing the model, it turns out that $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{End}\, E$ gets twisted by a unit in $\mathcal{O}^\times$ so the desired μ is seen to be only defined up to a unit.

1.6.3 Construction of Some Formal Groups

We now begin saying something about Lubin–Tate groups. We return to K being a p-adic field with ring of integers $\mathcal{O}$ and maximal ideal $\mathfrak{p}$.

Theorem 1.98 (Lubin–Tate)**.** Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. For a given uniformizer $\varpi \in \mathfrak{p}$, there is a unique (up to isomorphism) formal $\mathcal{O}$-module $\mathcal{G}$ over the base $\mathcal{O}$ such that

$$[\varpi] = X^{\#\mathbb{F}_{\mathfrak{p}}} \pmod{\mathfrak{p}}.$$

[5] This equality of morphisms can be checked after base-changing with $\mathbb{C}$, where the nature of the complex multiplication is clear when everything is presented as $\mathbb{C}$ modulo some lattice with endomorphisms given by $\mathcal{O}_K$.

Remark 1.99. We recall that $[\varpi]$ being an endomorphism of $\mathcal{G}$ already requires that

$$[\varpi] \equiv \varpi X \pmod{X^2},$$

which does reduce to $0 \pmod{\mathfrak{p}, X^2}$.

Example 1.100. Let $\mathcal{G}$ be the formal group attached to $\mathbb{G}_m$ with formal group law $\mathcal{G}_F[X,Y] = (X+1)(Y+1)-1$. For a rational prime p, our endomorphism is given by

$$[p](X) = (X+1)^p - 1,$$

which we note is $X^p \pmod{p}$.

Remark 1.101. Let's try to motivate the condition $[\varpi] = X^{\#\mathbb{F}_\mathfrak{p}} \pmod{\mathfrak{p}}$. We again return to the setting of complex multiplication with the imaginary quadratic field K and elliptic curve E with complex multiplication by $\mathcal{O}_K$. Assuming good enough reduction everywhere, we found that $\mathrm{Frob}_\mathfrak{p}$ was found in $\mathrm{End}(E) = \mathcal{O}_K$, say equal to some $\mu \in \mathcal{O}_K$. Thus, it is natural to expect that we have an endomorphism which reduces to $X^{\#\mathbb{F}_\mathfrak{p}} \pmod{\mathfrak{p}}$.

Let's now try to move towards a proof of Theorem 1.98. One can optimize a significant amount of the argument by passing to the following general proposition.

Notation 1.102. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$, and set $q \coloneqq \#\mathbb{F}_\mathfrak{p}$. For a uniformizer ϖ of K, we define the collection $\mathcal{F}_\varpi$ as the set of $f(X) \in \mathcal{O}[[X]]$ such that

$$f(X) \equiv \begin{cases} \varpi X & \pmod{X^2}, \\ X^q & \pmod{\mathfrak{p}}. \end{cases}$$

Proposition 1.103. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$ and a uniformizer ϖ. For $f, g \in \mathcal{F}_\varpi$ and a linear polynomial $\ell_1(X_1, \dots, X_n)$, there is a unique power series $\ell(X_1, \dots, X_n) \in \mathcal{O}[[X_1, \dots, X_n]]$ satisfying the following.

(a) $\ell(X_1, \dots, X_n) \equiv \ell_1(X_1, \dots, X_n) \pmod{(X_i X_j)_{ij}}$, where $(X_i X_j)_{ij}$ refers to modding out by terms of degree at least 2.

(b) $f \circ \ell = \ell \circ g^n$.

Proof. The proof is quite elementary, more or less boiling down to a manipulation of some polynomials. For brevity, we will write $\underline{X}$ for the full tuple $(X_1, \dots, X_n)$, and we let I_d denote the ideal of $\mathcal{O}[[\underline{X}]]$ consisting of polynomials of degree strictly larger than d. Note that each class $\mathcal{O}[[\underline{X}]]/I_d$ is uniquely represented by a polynomial of degree d.

We will construct ℓ inductively. Indeed, note that a power series ℓ has equivalent data to a sequence of polynomials $\{\ell_d\}_{d \geq 1}$ where

$$\ell_{d'} \equiv \ell_d \pmod{I_{d+1}}$$

whenever $d' \geq d$. Namely, one can reconstruct ℓ by reading the terms of degree at most d from ℓ_d. So we are tasked with constructing such a sequence $\{\ell_d\}_{d \geq 1}$ of polynomials of degree d with the given ℓ_1 (in order to satisfy (i)) and so that

$$f \circ \ell_d \equiv \ell_d \circ g^n \pmod{I_{d+1}}$$

in order to satisfy (ii). (Namely, once we are done constructing ℓ, we see that the computation of the terms of degree at most d of both $f \circ \ell$ and $\ell \circ g^n$ is allowed to reduce all the power series to only looking at terms of degree at most d.) The construction of the $\{\ell_d\}_{d \geq 1}$ will show that ℓ exists; in fact, we will show that these

polynomials ℓ_d are unique, which then shows that the terms of ℓ of degree at most d are unique and thus that ℓ itself is unique.

Let's now proceed with the computation, which we do inductively; note that ℓ_1 have been given. Suppose that we have already constructed ℓ_d uniquely, and we would like to show that ℓ_{d+1} is unique. If ℓ_{d+1} exists, then its terms of degree at most d must agree with ℓ_d by the uniqueness, so we may as well look for ℓ_{d+1} of the form $\ell_d + q_{d+1}$, where q_{d+1} is some homogeneous polynomial of degree $d+1$. On one hand, we see

$$(f \circ \ell_{d+1}) \equiv (f \circ \ell_d) + \varpi q_{d+1} \pmod{I_{d+2}}.$$

On the other hand, we see

$$(\ell_{d+1} \circ g^n) \equiv (\ell_d \circ g) + \varpi^{d+1} q_{d+1} \pmod{I_{d+2}},$$

where we have quietly used the fact that $q_{d+1}(\varpi \underline{X}) = \varpi^{d+1} q_{d+1}(\underline{X})$. Thus, we see that we want to show that there is a unique homogeneous polynomial q_{d+1} of degree $d+1$ such that

$$q_{d+1} \equiv \frac{1}{\varpi} \cdot \frac{(f \circ \ell_d) - (\ell_d \circ g^n)}{\varpi^d - 1} \pmod{I_{d+2}}.$$

The right-hand term on the right-hand side certainly defines a power series in $\mathcal{O}[[X]]$ (note $\varpi^d - 1 \in \mathcal{O}^\times$), so to check that the entire right-hand side defines a power series in $\mathcal{O}[[X]]$, it is enough to check that

$$(f \circ \ell_d) - (\ell_d \circ g^n) \stackrel{?}{\equiv} 0 \pmod{\varpi}.$$

Well, $f(X) \equiv g(X) \equiv X^{\#\mathbb{F}_\mathfrak{p}} \pmod{\mathfrak{p}}$, so this check reduces to using the Frobenius automorphism of $\mathbb{F}_\mathfrak{p}$. ■

Everything that follows is essentially a corollary of the proposition. As one application of the proposition, we define the required "Lubin–Tate" formal groups.

Corollary 1.104. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. For a given uniformizer $\varpi \in \mathfrak{p}$ and $f \in \mathcal{F}_\varpi$, there is a unique commutative 1-dimensional formal group $\mathcal{G}$ over $\mathcal{O}$ such that f is an endomorphism.

Proof. Proposition 1.103 explains that there is a unique power series $F \in \mathcal{O}[[X, Y]]$ such that $F(X, Y) \equiv X + Y \pmod{X^2, XY, Y^2}$ and $f(F(X, Y)) = F(f(X), f(Y))$, so it remains to check that this F is actually a commutative formal group law.

- Associativity: note that each $G \in \{F_f(X, F_f(Y, Z)), F_f(F_f(X, Y), Z)\}$ has constant term 0, linear terms $X + Y + Z$, and satisfies $G \circ f^3 = f \circ G$. However, such G is unique by Proposition 1.103.
- Commutativity: note that each $G \in \{F_f(X, Y), F_f(Y, Z)\}$ has constant term 0, linear terms $X + Y$, and satisfies $G \circ f^2 = f \circ G$. However, such G is unique by Proposition 1.103. ■

Definition 1.105 (Lubin–Tate formal group)**.** Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. For a given uniformizer $\varpi \in \mathfrak{p}$ and $f \in \mathcal{F}_\varpi$, we define the *Lubin–Tate formal group* $\mathcal{G}_f$ to be the unique commutative 1-dimensional formal group $\mathcal{G}$ over $\mathcal{O}$ such that f is an endomorphism.

We expect these formal groups to be isomorphic to each other and to be $\mathcal{O}$-modules. Thus, we will want an ample supply of homomorphisms and endomorphisms between them. Let's see this.

Corollary 1.106. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. Further, fix a uniformizer $\varpi \in \mathfrak{p}$ and elements $f, g \in \mathcal{F}_\varpi$.

(a) For each $a \in \mathcal{O}$, there is a unique power series $[a]_{g,f} \in X\mathcal{O}[[X]]$ such that $[a]_{g,f}(X) \equiv aX \pmod{X^2}$ and $[a]_{g,f} \circ f = g \circ [a]_{g,f}$.

(b) The power series $[a]_{g,f}$ is a homomorphism $\mathcal{G}_f \to \mathcal{G}_g$ of formal groups.

Proof. Note (a) follows directly from Proposition 1.103. For (b), we let F_f and F_g be the corresponding formal groups, and we see that we would like to show that

$$F_g \circ [a]_{g,f}^2 = [a]_{g,f} \circ F_f.$$

For this, we use Proposition 1.103: both sides have vanishing constant term, linear terms equal to $aX + aY$, and we see that

$$F_g \circ [a]_{g,f}^2 \circ f^2 = g \circ F_g \circ [a]_{g,f}^2,$$

and

$$[a]_{g,f} \circ F_f \circ f^2 = g \circ [a]_{g,f} \circ F_f,$$

completing the proof by uniqueness. ∎

Notation 1.107. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. Further, fix a uniformizer $\varpi \in \mathfrak{p}$ and elements $f, g \in \mathcal{F}_\varpi$. For each $a \in \mathcal{O}$, we let $[a]_{g,f} \colon \mathcal{G}_f \to \mathcal{G}_g$ be the induced formal group homomorphism. If $f = g$, we may simply write $[a]_f \coloneqq [a]_{f,f}$.

Example 1.108. We see $[1]_f = X$ because $X \equiv X \pmod{X^2}$ and commutes with f.

Example 1.109. We see $[\varpi]_f = f$ because $f(X) \equiv \varpi X \pmod{X^2}$ and commutes with f.

Corollary 1.110. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. Further, fix a uniformizer $\varpi \in \mathfrak{p}$ and elements $f, g, h \in \mathcal{F}_\varpi$ and $a, b \in \mathcal{O}$.

(a) We have $[a+b]_{g,f} = [a]_{g,f} + [b]_{g,f}$.

(b) We have $[a]_{h,g} \circ [b]_{g,f} = [ab]_{h,f}$.

Proof. All power series in sight have no constant term. For (a), both sides produce a power series q with linear term $(a+b)X$ and satisfying $q \circ f = g \circ q$. For (b), both sides produce a power series q with linear term abX and satisfying $q \circ f = h \circ q$. ∎

Now is as good a time as any to prove Theorem 1.98.

Proof of Theorem 1.98. We begin with uniqueness up to isomorphism. Pick up two such formal groups $\mathcal{G}_1$ and $\mathcal{G}_2$. Because $\mathcal{G}_\bullet$ is an $\mathcal{O}$-module, we see the power series $f_\bullet \coloneqq [\varpi]_{\mathcal{G}_\bullet}$ satisfies $f_\bullet(X) \equiv \varpi X \pmod{X^2}$. Thus, by hypothesis, we see that $f_\bullet \in \mathcal{F}_\varpi$, so we see that $\mathcal{G} = \mathcal{G}_{f_\bullet}$ by the uniqueness of this formal group. So we have left to show that the formal groups

$$\{\mathcal{G}_f : f \in \mathcal{F}_\varpi\}$$

are all isomorphic. Well, $[1]_{g,f} \colon \mathcal{G}_f \to \mathcal{G}_g$ and $[1]_{f,g} \colon \mathcal{G}_g \to \mathcal{G}_f$ are inverse homomorphisms: combining Example 1.108 with Corollary 1.110, we see that they compose to $[1]_f = X$ and $[1]_g = X$.

For existence, we see that we will want to choose our $\mathcal{G}$ to be of the form $\mathcal{G}_f$ for some f, and we see that Corollary 1.110 tells us that there is a ring homomorphism $\mathcal{O} \to \operatorname{End} \mathcal{G}_f$ given by $a \mapsto [a]_f$. (Note that $1 \mapsto \mathrm{id}_{\mathcal{G}_f}$ by Example 1.108.) Lastly, we see that $[\varpi] = f$ has $[\varpi] \equiv X^{\#\mathbb{F}_\mathfrak{p}} \pmod{\mathfrak{p}}$ by Example 1.109, completing the construction. ∎

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