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]

Part I

Explicit Class Field Theory

Theme 1
Complex Multiplication

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 $J(N) := \operatorname{Jac} X(N)$ 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 $\operatorname{End}(E)_{\mathbb{Q}}$ is larger than $\mathbb{Q}$. In this case, we may say that E admits complex multiplication by $K := \operatorname{End}(E)_{\mathbb{Q}}$.

Remark 1.3. If an elliptic curve E has CM, then it turns out that $\operatorname{End}(E)$ 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 $\operatorname{End}(E)_{\mathbb{Q}} = K$ 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 $\mathrm{T}_K := \operatorname{Res}_{K/\mathbb{Q}} \mathbb{G}_{m,K}$ embedded in $\mathrm{GL}_{2,\mathbb{Q}}$. Roughly speaking, the CM points with complex multiplication by K are the image of the Shimura variety

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

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 non-vanishing 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 $\operatorname{char} K$. 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 $f := [\mathcal{O}_K : \mathcal{O}]$, 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 $\operatorname{End}(\mathfrak{a}) = \mathcal{O}$.

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 $\operatorname{Cl}(\mathcal{O})$ denote the group of proper fractional ideals $\mathfrak{a} \subseteq \mathcal{O}$ taken modulo the principal ideals. We may also write $\operatorname{Pic}(\mathcal{O}) := \operatorname{Cl}(\mathcal{O})$.

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 $\sigma \in \operatorname{Gal}(H/K)$ 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 $\mathrm{H}^1(\operatorname{Gal}(\overline{H}/H), \operatorname{Aut}_{\overline{H}} E)$. (This is some general story from Galois descent.) However, we expect this cohomology group to be large in general because $\operatorname{Aut} E$ 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 $\Lambda^\vee \cong \operatorname{Hom}_{\mathcal{O}_K}(\Lambda, \mathcal{O}_K)$. 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 $\xi \coloneqq \sum_{i=1}^n x_i \otimes y_i$ 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 $\mathfrak{a}^* \coloneqq \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O})$, 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

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

  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 $\operatorname{Cl}(\mathcal{O})$ as we did last class.

Remark 1.23. Alternatively, we see that we can describe $\operatorname{Cl}(\mathcal{O})$ as isomorphism classes of line bundles $\operatorname{Pic}(\mathcal{O})$. Indeed, any fractional ideal produces a line bundle, and principal ideals are trivial line bundles, so we obtain a map $\operatorname{Cl}(\mathcal{O}) \to \operatorname{Pic}(\mathcal{O})$. 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 $\widehat{\mathcal{O}}_p\coloneqq\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p$ inside $\widehat{\mathcal{O}}_{K,p}\coloneqq\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p$. 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_py_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 $\mathfrak{a}_U := \mathcal{O}_{\mathcal{O}}|_U$ 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

$$\begin{tikzcd} \mathcal{O} \arrow[r, "\beta_U"] \arrow[dr, "\beta_V"'] & \mathcal{O}_U \arrow[d, "\alpha_{UV}"] \\ & \mathcal{O}_V \end{tikzcd}$$

   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 $S := (\operatorname{Spec}\mathbb{Z}) \setminus U_0$, 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 $\alpha_{0p} := \alpha_{U_0U_p}$.

   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 $\operatorname{Cl}(\mathcal{O}) \to T(\mathbb{Q})\backslash T(\mathbb{A}_{\mathbb{Q},f})/T(\widehat{\mathbb{Z}})$.

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 $\operatorname{Gal}(K/\mathbb{Q})$-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

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

Namely, we have defined an fpqc sheaf $(\mathfrak{a} \star E)(S) := \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E(S))$; 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 $\operatorname{Spec} \mathcal{O}$ 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 $\operatorname{Cl}(\mathcal{O})$ 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 $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$ 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 $\operatorname{Cl}(\mathcal{O})$. ■

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 $\operatorname{Cl}(\mathcal{O})$ given in Corollary 1.30. ■

1.3.2 The Galois Action

We now add a Galois action to the mix. Note $\operatorname{Gal}(k/\mathbb{Q})$ acts on $Y_{\mathcal{O}}$ by applying some $\sigma \in \operatorname{Gal}(k/\mathbb{Q})$ 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 $\operatorname{Cl}(\mathbb{Q})$-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 $\sigma \in \operatorname{Gal}(k/\mathbb{Q})$ and $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$, 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

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

On the other hand, we find

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

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

Lemma 1.45. Fix an order $\mathcal{O}$ of a quadratic imaginary field K, and let $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ be the nontrivial element. For any $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$, we have

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

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

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

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

Here is a punchline of having a Galois action.

Proposition 1.46. 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

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

where we realize $\operatorname{Cl}(\mathcal{O})$ 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 $\operatorname{Frob}_\mathfrak{p}$.

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

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 $\sigma \operatorname{Gal}(k/H)$. Well, $\sigma(E) = \chi(\sigma) \star E$ by definition of χ, so we would like to know that the kernel of χ is $\operatorname{Gal}(k/H)$.

We now apply Theorem 1.51. By definition of H, the Artin reciprocity map provides an isomorphism

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

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 $\operatorname{Gal}(k/H)$ 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, $\# \operatorname{Cl}(\mathcal{O}) = [H : K]$.

We will have to work a little harder to show $[\mathbb{Q}(j(E)) : \mathbb{Q}] = \# \operatorname{Cl}(\mathcal{O})$. 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 $\operatorname{Cl}(\mathcal{O})$, so the Galois orbit of $E \in Y_\mathcal{O}$ is all of $Y_\mathcal{O}$ and in particular has size $\# \operatorname{Cl}(\mathcal{O})$ (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 $\operatorname{Pic}(\mathcal{O})$ 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 $\operatorname{Gal}(k/K)$ acts transitively on $Y_{\mathcal{O}}$ (see Proposition 1.42). Thus, fixing any $E_0 \in Y_{\mathcal{O}}$, we find $Y_{\mathcal{O}} = \{\sigma(E_0) : \sigma \in \operatorname{Gal}(k/\mathbb{Q})\}$, so their fields of definition are given by

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

  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

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

  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

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

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

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

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

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

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

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

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

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

  It remains to understand when the action of $\operatorname{Gal}(K/\mathbb{Q})$ on $\operatorname{Cl}(\mathcal{O})$ is trivial. Well, the nontrivial element of $\operatorname{Gal}(K/\mathbb{Q})$ acts by inversion on $\operatorname{Cl}(\mathcal{O})$ by Lemma 1.45, which is a trivial action if and only if $\operatorname{Cl}(\mathcal{O})$ 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 $\operatorname{Cl}(\mathcal{O})(N)$ 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 $\operatorname{Cl}(\mathcal{O})(\infty)$ 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 $\operatorname{Cl}(\mathcal{O})(\infty)$ of pairs $(\mathfrak{a}, \tau)$ where $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$ 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

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

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

$$\begin{tikzcd}
K_p \arrow[d, "\gamma"'] & \mathfrak{a}_U \otimes_{\mathbb{Z}_U} \mathbb{Q}_p \arrow[l, "\varphi"'] \arrow[r, "\tau_p"] \arrow[d, equal] & K_p \arrow[d, equal] \\
K_p & \mathfrak{a}_V \otimes_{\mathbb{Z}_V} \mathbb{Q}_p \arrow[l, "\psi"'] \arrow[r, "\tau_p"] & K_p
\end{tikzcd}$$

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

$$\begin{tikzcd} K_p \arrow[d, equal] & \mathfrak{a}_U \otimes_{\mathbb{Z}_U} \mathbb{Q}_p \arrow[l, "\varphi"'] \arrow[r, "\tau_p"] \arrow[d] & K_p \arrow[d, equal] \\ K_p & \mathfrak{a}_V \otimes_{\mathbb{Z}_V} \mathbb{Q}_p \arrow[l] \arrow[r, "\tau_p'"] & K_p \end{tikzcd}$$

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

$$\begin{tikzcd} \mathrm{Cl}(\mathcal{O})(\infty) \arrow[r] \arrow[d] & K^\times\backslash\mathbb{A}_K^\times \arrow[d] \\ \mathrm{Cl}(\mathcal{O}) \arrow[r] & K^\times\backslash\mathbb{A}_K^\times/T(\widehat{\mathbb{Z}}) \end{tikzcd}$$

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 $\operatorname{Pic}(\mathcal{O})$ on $Y_{\mathcal{O}}$ naturally extends to an action of $\operatorname{Cl}(\mathcal{O})(N)$ 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 $(\mathfrak{a}, \tau_{\mathfrak{a}}) \in \operatorname{Cl}(\mathcal{O})(\infty)$ 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

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

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

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

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 $\operatorname{Hom}(\mathfrak{a}, E)$ 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 $\operatorname{Hom}(\mathfrak{a}, E)$ 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

$$\begin{tikzcd} \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}', E))[N] \arrow[r, "\tau"] \arrow[d, equal] & \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}/N, \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}'/N, E[N])) \arrow[d, equal] \\ \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a} \otimes \mathfrak{a}', E)[N] \arrow[r, "\tau"] & \operatorname{Hom}_{\mathcal{O}}((\mathfrak{a} \otimes \mathfrak{a}')/N, E[N]) \end{tikzcd}$$

  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 $\operatorname{Cl}(\mathcal{O})(N)$ 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 $(\mathfrak{a}, \tau_{\mathfrak{a}}) \in \operatorname{Cl}(\mathcal{O})$ such that $(\mathfrak{a}, \tau_{\mathfrak{a}}) \star (E, \tau) = (E', \tau')$. By Proposition 1.42, there is a unique $\mathfrak{a} \in \operatorname{Cl}(\mathcal{O})$ 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

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

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

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

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

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

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, $\sigma \in \operatorname{Gal}(k/\mathbb{Q})$ will act on $Y_{\mathcal{O}}(N)$ by

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

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 $\operatorname{Gal}(k/\mathbb{Q})$ on $Y_{\mathcal{O}}(\infty)$. Similarly, we note that there is a Galois action on $\operatorname{Cl}(\mathcal{O})(N)$ by

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

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 $\operatorname{Gal}(K/\mathbb{Q})$.

Before continuing, let's say something about how this story fits in with Shimura varieties. Embed $K \subseteq \mathbb{C}$. Set $\mathcal{H}^{\pm} := \mathbb{C} \setminus \mathbb{R}$, 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 $T := \operatorname{Res}_{\mathcal{O}/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}}$ as usual, and then T is the desired torus, and one finds that we have a morphism of Shimura varieties given by

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

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 $\chi\colon \operatorname{Gal}(k/K) \to \operatorname{Cl}(\mathcal{O})(\infty)$ 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 $\operatorname{Frob}_{\mathfrak{p}}$.

Remark 1.67. Let's explain why χ is a well-defined character. Because $\operatorname{Cl}(\mathcal{O})(\infty)$ 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 $\operatorname{Gal}(\overline{\mathbb{Q}}/H)$ 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 $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $Y_{\mathcal{O}}$ to produce a Galois action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $Y_{\mathcal{O}}(\infty)$, so one may wonder if it will eventually recover the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/H)$ 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 $\operatorname{Gal}(\overline{K}/K)$. 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
$$\begin{tikzcd} K^\times\backslash\mathbb{A}_K^\times \arrow[r, "\mathrm{Art}_K"] & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \arrow[dl, "\chi"] \\ \mathrm{Cl}(\mathcal{O})(\infty) \arrow[u] \end{tikzcd}$$
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
$$\begin{tikzcd} K^\times\backslash\mathbb{A}_K^\times \arrow[r, "\mathrm{Art}_K"] & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \arrow[dl, "\chi"] \arrow[d, "\chi_N"] \\ \mathrm{Cl}(\mathcal{O})(\infty) \arrow[u] \arrow[r, two heads] & \mathrm{Cl}(\mathcal{O})(N) \end{tikzcd}$$
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
$$\begin{tikzcd} K^\times\backslash\mathbb{A}_K^\times \arrow[r, "\mathrm{Art}_K"] & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \arrow[d, "\chi_N"] \\ \mathrm{Cl}(\mathcal{O})(\infty) \arrow[u] \arrow[r, two heads] & \mathrm{Cl}(\mathcal{O})(N) \end{tikzcd}$$
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 $\tau_{\mathfrak{p}} : \mathfrak{p}_p \to \widehat{\mathcal{O}}_p$ 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.

$$\begin{tikzcd}
& & \overline{E}^{(p)}[N] \\
\mathcal{O}/N & \overline{E}[N] \arrow[l, "\tau"'] \arrow[r] \arrow[ur] & \overline{\mathfrak{p}\star E}[N] \arrow[u] \\
& \operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/N, \overline{E}[N]) \arrow[u, equal] \arrow[r] & \operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/N, \overline{\mathfrak{p}\star E}[N]) \arrow[u, equal]
\end{tikzcd}$$

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

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

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 Homework 1

Our exposition follows [Ser10, Section 3].

1.5.1 The Composite of Hilbert Class Fields

Throughout, it will be helpful to remember the "profinite completion" notation as

$$\widehat{\mathcal{O}}_K = \prod_{v<\infty} \mathcal{O}_{K,v}.$$

This is an isomorphism of rings.

We begin with some general result on class field theory.

Lemma 1.73. Fix a totally imaginary number field K, and let H be the Hilbert class field of the order $\mathcal{O}_K$. Then the restriction of the global Artin map

$$\mathcal{O}_K^\times \backslash \widehat{\mathcal{O}}_K^\times \to \operatorname{Gal}(K^{\mathrm{ab}}/H)$$

is a surjection of topological groups.

Proof. We begin with the usual global Artin map as

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

Note that this map is surjective by [NSW08, Corollary 8.2.2], where we note that we have removed the archimedean complexes (which are all complex here!). Now, an idele class $x \in K^\times \backslash \mathbb{A}_{K,f}^\times$ fixes H if and only if $x_v \in \mathcal{O}_{K,v}^\times$ for all finite places v, which is equivalent to $x \in \widehat{\mathcal{O}}_K^\times$.[5] Thus, the global Artin map restricts to a continuous surjection

$$\mathcal{O}_K^\times \backslash \widehat{\mathcal{O}}_K^\times \to \operatorname{Gal}(K^{\mathrm{ab}}/H),$$

which is what we wanted. ■

As a first attempt to constructing K^{ab}, we take the union of all the Hilbert class fields as we vary over orders $\mathcal{O} \subseteq \mathcal{O}_K$. This gets pretty close.

Proposition 1.74. Fix a totally imaginary quadratic number field K. Let $K^?$ be the composite of the Hilbert class fields $H_\mathcal{O}$ as $\mathcal{O}$ varies over orders in $\mathcal{O}_K$, and let $K^{??}$ be the composite of $K^?$ and $\mathbb{Q}^{\mathrm{ab}}$. Then $\operatorname{Gal}(K^{\mathrm{ab}}/K^{??})$ is a product of groups of order 2.

Proof. We characterize the subgroup $O \subseteq \mathcal{O}_K^\times \backslash \widehat{\mathcal{O}}_K^\times$ corresponding to $\operatorname{Gal}(K^{\mathrm{ab}}/K^{??}) \subseteq \operatorname{Gal}(K^{\mathrm{ab}}/H)$. In particular, Lemma 1.73 tells us that we would like to show that $\operatorname{Art}_K(O)$ is a product of groups of order 2. Quickly, we note that we merely check that $\operatorname{Art}_K(O)$ is 2-torsion, for then O becomes a vector space over $\mathbb{F}_2$ and thus a product of groups of order 2.

Anyway, we will have $x \in \mathcal{O}_K^\times \backslash \widehat{\mathcal{O}}_K^\times$ being in O if and only if $\operatorname{Art}_K(x) \in \operatorname{Gal}(K^{\mathrm{ab}}/H)$ fixes $K^{??}$. This splits into two checks.

1. We require $\operatorname{Art}_K(x)$ to fix $H_\mathcal{O}$ for each order $\mathcal{O} \subseteq \mathcal{O}_K$. In other words, for each $f \geq 1$, we must have $\operatorname{Art}_K(x)$ fix $H_{\mathcal{O}_f}$, where $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ is the order of conductor f. By definition of $H_{\mathcal{O}_f}$, this is equivalent to having $x \in \mathcal{O}_K^\times \backslash \widehat{\mathcal{O}}_f^\times$ for each $f \geq 1$. Now, we recall from the proof of Proposition 1.24 that
$$\widehat{\mathcal{O}}_f^\times = \left\{ y \in \widehat{\mathcal{O}}_K^\times : y \pmod f \in (\mathbb{Z}/f\mathbb{Z})^\times \right\}.$$
Thus, fixing a representative $x \in \widehat{\mathcal{O}}_K^\times$ in the quotient, we see that for each $f \geq 1$, we are granted some unit $u_f \in \mathcal{O}_K^\times$ such that $u_f x \in \widehat{\mathcal{O}}_f^\times$. However, for f sufficiently divisible, we see that $\mathcal{O}_K^\times$ will embed into $\mathcal{O}_K/(f)$, meaning that there will be at most one unit u_f (up to sign) satisfying $u_f x \in \widehat{\mathcal{O}}_f^\times$. Thus, we see that there will in fact be a single unit $u \in \mathcal{O}_K^\times$ (not depending on f) such that $ux \in \widehat{\mathcal{O}}_f^\times$ for all $f \geq 1$, which upon taking the limit over f means that $ux \in \widehat{\mathbb{Z}}^\times$. In other words, we are requiring that our $x \in \mathcal{O}_K^\times \backslash \widehat{\mathcal{O}}_K^\times$ actually comes from $\mathbb{Z}^\times \backslash \widehat{\mathbb{Z}}^\times$.
2. We require $\operatorname{Art}_K(x)$ to fix $\mathbb{Q}^{\mathrm{ab}}$. In other words, we need $\operatorname{Res}_{\mathbb{Q}^{\mathrm{ab}}} \operatorname{Art}_K(x)$ to be trivial. Thus, we recall that the square
$$\begin{array}{ccc} K^\times \backslash \mathbb{A}_{K,f}^\times & \xrightarrow{\operatorname{Art}_K} & \operatorname{Gal}(K^{\mathrm{ab}}/K) \\ {\scriptstyle \mathrm{N}_{K/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle \operatorname{Res}} \\ \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q},f}^\times & \xrightarrow{\operatorname{Art}_\mathbb{Q}} & \operatorname{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \end{array}$$

[5] Technically, one only knows that we can adjust x by an element of $K^\times$ to live in $\widehat{\mathcal{O}}_K^\times$. Please forgive me for this sort of abuse of notion throughout.

commutes. Now, in light of the previous check, we would like to check when some $ux \in \widehat{\mathbb{Z}}^\times$ (where $\widehat{\mathbb{Z}}^\times$ is implicitly embedded in $\widehat{\mathcal{O}}_K^\times \subseteq \mathbb{A}_{K,f}^\times$) vanishes in $\operatorname{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. Equivalently, we would like to check when

$$\mathrm{N}_{K/\mathbb{Q}}(ux) = x^2$$

lives in the kernel of the global Artin map $\operatorname{Art}_\mathbb{Q}$. However, the restriction of the global Artin map $\operatorname{Art}_\mathbb{Q}$ to $\widehat{\mathbb{Z}}^\times \to \operatorname{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ is injective (one could use [NSW08, Corollary 8.2.2] again). Thus, $x^2 \in \widehat{\mathbb{Z}}^\times$ only succeeds at being in the kernel of $\operatorname{Art}_\mathbb{Q}$ only if it is already trivial.

The above two checks combine to show that O is a 2-torsion group, as required. ■

Remark 1.75. Recall from Corollary 1.52 that $H_\mathcal{O}$ is the field of definition of some $E \in Y_\mathcal{O}$ (over K). Thus, one can view $K^?$ as the extension of K obtained by adjoining all j-invariants $j(\mathcal{O})$ as $\mathcal{O} \subseteq \mathcal{O}_K$ varies over all orders.

Remark 1.76. Recall from the Kronecker–Weber theorem that $\mathbb{Q}^{\mathrm{ab}}$ is the maximal cyclotomic extension of $\mathbb{Q}$. Thus, we can also view $K^{??}$ the extension of $K^?$ achieved by adjoining all roots of unity.

1.5.2 The Composite of Torsion

Again, fix an imaginary quadratic field K. In order to actually compute K^{ab}, we add in some torsion. We will work with the maximal order $\mathcal{O}_K$, for convenience, and we will let H be the Hilbert class field. Fix an elliptic curve $E \in Y_{\mathcal{O}_K}$. Let's quickly explain why adding torsion could help.

Lemma 1.77. Fix an imaginary quadratic field K with Hilbert class field H. For $E \in Y_{\mathcal{O}_K}$, let H_E be the extension obtained by adding in the coordinates of the torsion points E_{tors} of E to H. Then $\operatorname{Gal}(H_E/H)$ embeds in $\widehat{\mathcal{O}}_K^\times$ via the Galois action on E_{tors}.

Proof. Quickly, we recall from Corollary 1.52 that E has a model over H. Let TE be the product $\prod_p T_pE$ of the Tate modules. Because E has complex multiplication by $\mathcal{O}_K$, one may choose compatible level structure trivializations $E[n] \to \mathcal{O}_K/n\mathcal{O}_K$, eventually producing a level structure trivialization

$$\tau\colon TE \to \widehat{\mathcal{O}}_K.$$

Now, each $\sigma \in \operatorname{Gal}(\overline{H}/H)$ induces a compatible system of $\mathcal{O}$-linear morphisms $\sigma\colon E[n] \to E[n]$ for each n, so we get a canonical map

$$\operatorname{Gal}(\overline{H}/H) \to \operatorname{Aut}_\mathcal{O} TE.$$

Further, note that $\sigma \in \operatorname{Gal}(\overline{H}/H)$ fixes TE if and only if it fixes all torsion points of E, which is equivalent to fixing H_E; thus, the above Galois representation factors as an injective map

$$\operatorname{Gal}(H_E/H) \hookrightarrow \operatorname{Aut}_\mathcal{O} TE.$$

The result follows after using the level structure isomorphism τ. ■

Remark 1.78. In particular, it follows that H_E/H is an abelian extension.

We would like to descend the extension H_E/H to an abelian extension of K, which we will then check produces K^{ab}. Ultimately, this will require us to produce a Galois representation of $\operatorname{Gal}(K^{\mathrm{ab}}/K)$, but constructing such a thing from a fixed $E \in Y_{\mathcal{O}_K}$ does not make sense because E is not defined over K in general. Instead, we will have to use the fact that $\operatorname{Gal}(H/K)$ acts on $Y_{\mathcal{O}_K}$ to use the entire torsor of elliptic curves in $Y_{\mathcal{O}_K}$ to produce a Galois representation of $\operatorname{Gal}(\overline{K}/K)$.

Eventually, we will want to make arguments akin to Proposition 1.74 in order to prove our theorem, so it will help to start using class field theory.

Notation 1.79. Fix an imaginary quadratic field K with Hilbert class field H. For $E \in Y_{\mathcal{O}_K}$, we define θ_E as the composite representation

$$\mathbb{A}_H^\times \stackrel{\text{Art}}{\to} \operatorname{Gal}(\overline{H}/H) \to \operatorname{Aut}_{\mathcal{O}} TE \cong \widehat{\mathcal{O}}_K^\times,$$

where the last isomorphism is obtained by choosing a level structure isomorphism for TE.

Lemma 1.80. Fix an imaginary quadratic field K with Hilbert class field H, and choose some $E \in Y_{\mathcal{O}_K}$. For any $x \in \widehat{\mathcal{O}}_H^\times$, we have

$$\theta_E(x) \operatorname{N}_{H/K}(x) \in \mathcal{O}_K^\times.$$

Proof. The main idea is to compare the Galois and class group actions on (E, τ), where $\tau \colon TE \to \widehat{\mathcal{O}}_K$ is a choice of level structure trivialization.

Let's be more explicit. The following computation is potentially off by a sign, but it is not so significant. By Theorem 1.66, we see that

$$\operatorname{Art}_K(\operatorname{N}_{H/K}(x))(E, \tau) = (\mathcal{O}_K, \operatorname{N}_{H/K}(x)) \star (E, \tau).$$

(In particular, $\operatorname{N}_{H/K}(x)$ is trivial in $\operatorname{Cl}(\mathcal{O}_K)$, so the corresponding line bundle is $\mathcal{O}_K$; we are using x for our choice of trivialization.) We now compute both sides.

- On the left, we find $\operatorname{Art}_K(\operatorname{N}_{H/K}(x)) = \operatorname{Art}_H(x)$ by compatibility of the global Artin map in extensions. In particular, this Galois element fixes H, so it fixes our chosen model E over H. However, it does adjust the level structure isomorphism to $\left(E, \tau \circ \operatorname{Art}_K(\operatorname{N}_{H/K}(x))^{-1}\right)$ by definition of this Galois action.

- On the right, we note $\mathcal{O} \star E = E$, so the elliptic curve is still fixed. As for the level structure isomorphism, we have

$$\begin{array}{ccccccc} E[N] & \to & \operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/N\mathcal{O}, E[N]) & \to & \operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/N\mathcal{O}, \mathcal{O}/N\mathcal{O}) & \to & \mathcal{O}/N\mathcal{O} \\ p & \mapsto & (1 \mapsto p) & \mapsto & (1 \mapsto \tau(\operatorname{N}_{H/K}(x)p)) & \mapsto & \tau(\operatorname{N}_{H/K}(x)p) \end{array}$$

  by tracking through the construction.

In total, we see that

$$\left(E, \tau \circ \operatorname{Art}_K(\operatorname{N}_{H/K}(x))^{-1}\right) = \left(E, \tau \circ \operatorname{N}_{H/K}(x)\right),$$

so there is an automorphism $u \in \operatorname{Aut}(E)$ such that

$$\tau \circ \operatorname{Aut}_H(x)^{-1} = \tau \circ \operatorname{N}_{H/K}(x) \circ u.$$

Undoing τ and applying the definition of θ_E, we find that $\theta_E(x) \operatorname{N}_{H/K}(x) = u^{-1}$, so the result follows. (Note $\operatorname{Aut}(E) = \mathcal{O}_K^\times$!) ■

The above lemma allows us to make the following definition.

Notation 1.81. Fix an imaginary quadratic field K with Hilbert class field H, and choose some $E \in Y_{\mathcal{O}_K}$. Then we define the homomorphism $\rho_E \colon \widehat{\mathcal{O}}_H^\times \to \mathcal{O}_K^\times$ by $\rho_E \coloneqq \theta_E \cdot \operatorname{N}_{H/K}$.

We now see that the presence of these units $\mathcal{O}_K^\times$ (i.e., nontrivial automorphisms of E) will present a problem when we are trying to glue together the various Galois actions. Thus, our next step is to quotient them out. This presents the following cases.

Lemma 1.82. Fix an imaginary quadratic field K with Hilbert class field H, and choose some fixed $E \in Y_{\mathcal{O}_K}$. Then there is a model of E over H equipped with a cyclic projection $\pi\colon E \to \mathbb{P}^1$ with Galois group $\mathcal{O}_K^\times = \operatorname{Aut}(E)$.

Proof. Our proof will be explicit, though it will require some casework. Everything in sight is characteristic 0, so we may write out a model for E over H as cut out from $\mathbb{P}^2$ by the homogeneous equation $Y^2Z = X^3 + aXZ^2 + bZ^3$. It will be helpful to note that there is a map $x\colon E \to \mathbb{P}^1$ given on affine points by $(x, y) \mapsto x$ and mapping together the points at infinity. We now have the following cases.

- Suppose that $K \notin \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$. Then $\mathcal{O}_K^\times = \{\pm 1\}$, and we define π to be x. Namely, we see that $\pi([X : Y : Z]) = \pi([X' : Y' : Z'])$ if and only if $[X : Y : Z] = [X : \pm Y : Z]$, which is equivalent to $[X : Y : Z]$ and $[X' : Y' : Z']$ being in the same orbit by $\mathcal{O}_K^\times = \{\pm 1\}$.
- Suppose that $K = \mathbb{Q}(i)$ so that $\mathcal{O}_K = \{\pm 1, \pm i\}$. We work with the explicit model $E_0\colon Y^2Z = X^3 + X$, and we note that $i \in \mathcal{O}_K$ may act by fixing the point at infinity and sending $i\colon (x, y) \mapsto (-x, iy)$. (In particular, we see that this is an endomorphism of E of order 4, so it induces an injection $\mathbb{Z}[i] \hookrightarrow \operatorname{End}(E_0)$, which becomes an isomorphism because $\operatorname{End}(E_0)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field.) As such, we see that affine points (x, y) and (x', y') are in the same orbit if and only if $x = \pm x'$.

  Thus, in this case, we set π to be x^2 (namely, the value of x^2 on affine points, still sending the point to infinity to $[1 : 0] \in \mathbb{P}^1$), and we see that $\pi([X : Y : Z]) = \pi([X' : Y' : Z'])$ if and only if these are both the point at infinity or having these be affine points (x, y) and (x', y') with $x = \pm x'$. This last condition is equivalent to having our points be in the same orbit by $\mathcal{O}_K^\times$.
- Suppose $K = \mathbb{Q}(\zeta_3)$ so that $\mathcal{O}_K = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. We work with the explicit model $E_0\colon Y^2Z = X^3 + Z^3$, and we note that $\zeta_3 \in \mathcal{O}_K$ may act by fixing the point at infinity and sending $\zeta_3\colon (x, y) \mapsto (\zeta_3 x, y)$. (In particular, this is certainly an endomorphism of order 3, which then induces the needed injection $\mathbb{Z}[\zeta_3] \hookrightarrow \operatorname{End}(E_0)$.) As such, we see that affine points (x, y) and (x', y') are in the same orbit if and only if $x^3 = (x')^3$.

  Thus, in this case, we set π to be x^3 as in the previous case, and we conclude in the same way that π is a cyclic projection with Galois group $\mathcal{O}_K^\times$. ■

Remark 1.83. It is worth noting that the construction of π is totally explicit as soon as we have a chosen model for E. This will later enable us to rather explicitly write down abelian extensions of K from torsion points of E.

Remark 1.84. In fact, provided we are working with models of E in short Weierstrass form $Y^2Z = X^3 + aXZ^2 + bZ^3$, the specific choice of model in the last two cases doesn't matter to the construction of π.

- When $K = \mathbb{Q}(i)$, then we see that we are looking for elliptic curves with j-invariant 1728, which all look like $Y^2Z = X^3 + aXZ^2$. Of course, we then see that we can still take $i\colon (x, y) \mapsto (ix, -y)$, so the same argument goes through with the same π.
- When $K = \mathbb{Q}(\zeta_3)$, then now we want elliptic curves with j-invariant 0, which all look like $Y^2Z = X^3 + bZ^3$. The action by ζ_3 can still be taken as $(x, y) \mapsto (\zeta_3 x, y)$, so the same argument still goes through with the same π.

Notation 1.85. Fix an imaginary quadratic field K with Hilbert class field H, and choose some fixed $E \in Y_{\mathcal{O}_K}$. Choose a model of E over H, and choose a cyclic projection $\pi\colon E \to \mathbb{P}^1$ with Galois group $\mathcal{O}_K^\times$. Then we set

$$L(E) := H(\pi(E_{\text{tors}})).$$

More precisely, we are asking to adjoin the affine points, which can be identified with elements of $\overline{H}$ already. (The point at infinity does not help us because it is defined over H.)

Anyway, we are now ready to prove our theorem.

Theorem 1.86. Fix an imaginary quadratic field K with Hilbert class field H, and choose some fixed $E \in Y_{\mathcal{O}_K}$. Then $L(E)$ is the maximal abelian extension of K.

Proof. Note that fixing $L(E)$ is the same as fixing torsion up to units, which is equivalent to fixing $TE/\mathcal{O}_K^\times$. In other words, the extension $L(E)$ of H can be described as given by the kernel of

$$\overline{\rho}\colon \operatorname{Gal}(\overline{H}/H) \to \operatorname{Aut}_{\mathcal{O}_K}\left(TE/\mathcal{O}_K^\times\right).$$

We note that $\overline{\rho}$ in fact factors through $\operatorname{Aut}_{\mathcal{O}_K} TE$, which is abelian (it is $\widehat{\mathcal{O}}_K^\times$), so we may as well pass to the abelianization, meaning that $L(E)$ can be described as given by the kernel of

$$\overline{\rho}\colon \operatorname{Gal}(H^{\mathrm{ab}}/H) \to \operatorname{Aut}_{\mathcal{O}_K}\left(TE/\mathcal{O}_K^\times\right).$$

We now use class field theory. Because $\operatorname{Art}_H\colon H^\times\backslash\mathbb{A}_{H,f}^\times \to \operatorname{Gal}(H^{\mathrm{ab}}/H)$ is surjective, it is enough to check that $\overline{\rho}(\operatorname{Art}_H(x))$ is trivial if and only if $\operatorname{Art}_H(x)|_{K^{\mathrm{ab}}}$ is trivial. We now compare these two conditions.

- Note that $\overline{\rho}(\operatorname{Art}_H(x))$ is trivial if and only if the Galois action by $\operatorname{Art}_H(x)$ (which we recall is succinctly given by $\theta_E(x)$) only ever adjusts elements of E by units. By Lemma 1.80, it is equivalent to ask for $\mathrm{N}_{H/K}(x) \in \mathcal{O}_K^\times$.
- By compatibility of the global Artin maps, $\operatorname{Art}_H(x)|_{K^{\mathrm{ab}}}$ is trivial if and only if $\operatorname{Art}_K(\mathrm{N}_{H/K}(x))$ is trivial. Note $\operatorname{Art}_K(\mathrm{N}_{H/K}(x))$ already fixes H, so we may as well take $\mathrm{N}_{H/K}(x) \in \mathcal{O}_K^\times\backslash\widehat{\mathcal{O}}_K^\times$ by definition of the Hilbert class field. But now [NSW08, Corollary 8.2.2] explains that the Artin map being trivial on such an element $\mathrm{N}_{H/K}(x)$ requires $\mathrm{N}_{H/K}(x) \in \mathcal{O}_K^\times$.

The above two checks complete the proof. ■

Remark 1.87. We note that the above theorem implies that $L(E)$ is independent of the choice of E. One can also imagine showing this more directly by noting that two $E, E' \in Y_{\mathcal{O}_K}$ will have an isogeny $\varphi\colon E \to E'$ between them (as this can be seen on the level of $\mathbb{C}$-points). This isogeny allows us to relate the Galois action on the torsion of E to the Galois action on E', provided that we can ensure that φ has a relatively small field of definition, which is technically not obvious.

Theme 2
Lubin–Tate Theory

Completion is a goal, but we hope it is never the end.

—Sarah Lewis

2.1 February 4

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

2.1.1 Remarks on Hilbert's 12th Problem

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

> **Theorem 2.1** (Kronecker–Weber)**.** The field $\mathbb{Q}^{\text{ab}}$ 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 $\mathbb{Q}^{\text{ab}} = \mathbb{Q}^{\text{cyclo}}$, as usual.

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

> **Theorem 2.2** (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 2.3. 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.

2.1.2 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 2.4 (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 2.5. 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 2.6. As a slightly formal comment, we remark that the composite $F(G_1(\underline{X}),\ldots,G_n(\underline{X}))$ 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 $F(G_1(\underline{X}),\ldots,G_n(\underline{X}))$, 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.

Remark 2.7. Technically speaking, we have defined a 1-dimensional formal group. There is a generalization to higher dimensions, which more or less proceeds by adding variables to our power series.

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 2.8 (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 2.9. 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 2.10. 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 2.11. 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 2.12. 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

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

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

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

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

Example 2.13. Let's explain what we are trying to generalize. Take $K = \mathbb{Q}_p$. Then $\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}_p^{\text{unr}}$, 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.

2.2 February 6

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 $\mathcal{O}$.

2.2.1 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 2.14. 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

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

Remark 2.15. 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 2.16. For example, we could take $\widehat{K} \in \{K, K^{\text{unr}}, \widehat{\overline{K}}\}$. In particular, the extension need not be finite or even algebraic.

Definition 2.17 (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

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

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

Remark 2.18. 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 2.19 (Lubin–Tate)**.** 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 formal $\mathcal{O}$-module $\mathcal{G}_\varpi$ (defined up to isomorphism) such that

$$K_\varpi := K(\mathcal{G}[\mathfrak{p}^\infty])$$

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

Remark 2.20. Let's give some indication of what is going on under the hood. We will find that $T_\varpi G_\varpi$ is a free rank-1 module over $\mathcal{O}$. Then the Galois action of $\operatorname{Gal}(K^{\text{ab}}/K)$ on $T_\varpi G_\varpi$ 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 $v \in T_\varpi G_\varpi$. 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 2.21. Roughly speaking, the "uniqueness up to isomorphism" corresponds to choosing a different "local coordinate" at the identity of the ambient group scheme.

Remark 2.22. 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.

2.2.2 Relation to Complex Multiplication

The proof of Theorem 2.19 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

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

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

$$\begin{tikzcd} K_v^\times \arrow[r, hook] \arrow[d, hook] & \operatorname{Gal}(K_v^{\text{ab}}/K_v) \arrow[d, dashed] \\ K^\times \backslash \mathbb{A}_{K,f}^\times \arrow[r, hook] & \operatorname{Gal}(K^{\text{ab}}/K) \end{tikzcd}$$

and so $\operatorname{Gal}(K_v^{\text{ab}}/K_v)$ embeds into $\operatorname{Gal}(K^{\text{ab}}/K)$. Thus, abelian extensions of K_v can be found as closed subgroups of $\operatorname{Gal}(K_v^{\text{ab}}/K_v)$, which then produce closed subgroups of $\operatorname{Gal}(K^{\text{ab}}/K)$. 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 2.23. Note $\mathcal{G}_E$ has an $\mathcal{O}_K$-action coming from E, and $T_\varpi\mathcal{G}_E$ 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

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

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 2.19 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 2.24. 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 $\operatorname{Frob}_{\mathfrak{P}}$ as an endomorphism of $\overline{E}$ will lift to an endomorphism of E. If $\operatorname{End}\overline{E}$ is an order in a quadratic field K, then there is nothing to do because we are forced to have $\operatorname{End}\overline{E} = \mathcal{O}_K = \operatorname{End} E$. Otherwise, $\operatorname{End}\overline{E}$ 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

$$\operatorname{End}_{\mathcal{O}} E \to \operatorname{End}_{\mathcal{O}} \overline{E}$$

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

Remark 2.25. Note that we used the trick of noting $\operatorname{End}_{\mathcal{O}} \overline{E} = \operatorname{End}_{\mathcal{O}} E$ 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 $\operatorname{Lie} E = \mathcal{O}_K$ by multiplication-by-$\sigma(\mu)$,[1] which is nontrivial in $\mathcal{O}_K \subseteq \mathcal{O}_L/\mathfrak{P}$ because $\sigma(\mu) \notin \mathfrak{P}$ by construction!

[1] 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 $\mathcal{O}_K$.

- 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 $\operatorname{Frob}_{\mathfrak{P}}$ must be an endomorphism in $\operatorname{End} E = \mathcal{O}_K$, so we may find $\mu \in \mathcal{O}_K$ with $\mu = \operatorname{Frob}_{\mathfrak{P}}$. For example, this implies that $\mathrm{N}_{K/\mathbb{Q}}\,\mu = \deg \operatorname{Frob}_{\mathfrak{P}} = \#\mathbb{F}_{\mathfrak{P}}$ is a power of p, so $\mu \in \mathfrak{p}$. Now, the dual of $\operatorname{Frob}_{\mathfrak{P}}$, labeled $\operatorname{Frob}_{\mathfrak{P}}^\vee$ must be equal to $\sigma(\mu)$ because
$$\mu\sigma(\mu) = \mathrm{N}_{K/\mathbb{Q}}\,\mu = \deg \operatorname{Frob}_{\mathfrak{P}} = \operatorname{Frob}_{\mathfrak{P}} \circ \operatorname{Frob}_{\mathfrak{P}}^\vee.$$
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
$$\operatorname{Frob}_{\mathfrak{P}}^\vee = \sigma(\mu) = u\operatorname{Frob}_{\mathfrak{P}}$$
stays purely inseparable, so the morphism $[\deg \operatorname{Frob}_{\mathfrak{P}}]$ 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 $\widehat{\mathfrak{p}}$.

2.2.3 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 2.26 (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
$$[\varpi] \equiv X^{\#\mathbb{F}_{\mathfrak{p}}} \pmod{\mathfrak{p}}.$$

Remark 2.27. 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 2.28. 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 2.29. Let's try to motivate the condition $[\varpi] \equiv X^{\#\mathbb{F}_{\mathfrak{P}}} \pmod{\mathfrak{p}}$. 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 $\operatorname{Frob}_{\mathfrak{P}}$ was found in $\operatorname{End}(E) = \mathcal{O}_K$, 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 2.26. One can optimize a significant amount of the argument by passing to the following general proposition.

Notation 2.30. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$, and set $q := \#\mathbb{F}_\mathfrak{p}$. 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 2.31. 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 $\ell_1(X_1, \ldots, X_n)$, there is a unique power series $\ell(X_1, \ldots, X_n) \in \mathcal{O}[[X_1, \ldots, X_n]]$ satisfying the following.

(a) $\ell(X_1, \ldots, X_n) \equiv \ell_1(X_1, \ldots, X_n) \pmod{(X_iX_j)_{ij}}$, where $(X_iX_j)_{ij}$ 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 $(X_1, \ldots, X_n)$, 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 2.32. 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 2.31 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 2.31.
- 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 2.31. ■

Definition 2.33 (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. If the uniformizer ϖ is unclear, we may write $\mathcal{G}_{\varpi,f}$.

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 2.34. 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 2.31. 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 2.31: 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 2.35. 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 $[a]_f := [a]_{f,f}$.

Example 2.36. We see $[1]_f = X$ because $X \equiv X \pmod{X^2}$ and commutes with f.

Example 2.37. We see $[\varpi]_f = f$ because $f(X) \equiv \varpi X \pmod{X^2}$ and commutes with f.

Corollary 2.38. 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 as a time as any to prove Theorem 2.26.

Proof of Theorem 2.26. 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 $f_\bullet := [\varpi]_{\mathcal{G}_\bullet}$ 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 2.36 with Corollary 2.38, 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 2.38 tells us that there is a ring homomorphism $\mathcal{O} \to \operatorname{End} \mathcal{G}_f$ given by $a \mapsto [a]_f$. (Note that $1 \mapsto \operatorname{id}_{\mathcal{G}_f}$ by Example 2.36.) Lastly, we see that $[\varpi] = f$ has $[\varpi] \equiv X^{\#\mathbb{F}_\mathfrak{p}} \pmod{\mathfrak{p}}$ by Example 2.37, completing the construction. ■

2.3 February 11

Let's continue Lubin–Tate theory.

2.3.1 Remarks on Models

The proof of Theorem 2.24 raises a bizarre question: what is the element $\mu \in \mathcal{O}$ which induces the Frobenius action by $\operatorname{Frob}_\mathfrak{P}$ on E? (Here, we are using the notation of the proof of Theorem 2.24.) However, this question does not make sense: the hunt for an element μ depends on a choice of model of E over H.

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

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

Because $\operatorname{Aut}_\mathcal{O}(E) = \mathcal{O}^\times$, we see that the Galois action is trivial, so this is $\operatorname{Hom}_{\text{cont}}(\operatorname{Gal}(\overline{\mathbb{Q}}/H), \mathcal{O}^\times)$. By choosing $\mathfrak{p}$ and then $\mathfrak{P}$ carefully, we may assume that E actually admits a model over $\mathcal{O}_\mathfrak{P}$ (namely, we want $\mathfrak{p}$ to be totally split or similar). Then the model of the reduction $\pmod{\mathfrak{P}}$ of E is going to be defined up to an element of

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

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

To be explicit, let's choose some $c\colon \operatorname{Gal}(\overline{\mathbb{F}}_\mathfrak{P}/\mathbb{F}_\mathfrak{P}) \to \mathcal{O}^\times$, and let's figure out what the new elliptic curve E' is.

Remark 2.39. For motivation, let's give the general construction. More generally, if we are dealing with a class of geometric objects X (e.g., schemes) which satisfy some version of descent over a field K (namely, objects X' over K which are isomorphic over K^{sep} can be described by a form over K^{sep} along with some descent data), then forms of X over K can be identified with $\mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathrm{Aut}_{\overline{K}}(X))$. To give the map in one direction, suppose that we have a form X' equipped with a specified isomorphism $\varphi\colon X_L \to X'_L$ over a finite Galois extension L/K. This produces a diagram

$$\begin{tikzcd} X_L \arrow[r, "\sigma"] \arrow[d] & X_L \arrow[r, "\varphi"] \arrow[d] & X'_L \arrow[r, "\sigma^{-1}"] \arrow[d] & X'_L \arrow[r, "\varphi^{-1}"] \arrow[d] & X_L \arrow[d] \\ \operatorname{Spec} L \arrow[r, "\sigma"] & \operatorname{Spec} L \arrow[r, equal] & \operatorname{Spec} L \arrow[r, "\sigma^{-1}"] & \operatorname{Spec} L \arrow[r, equal] & \operatorname{Spec} L \end{tikzcd}$$

from which the cocycle $c\colon \mathrm{Gal}(L/K) \to \mathrm{Aut}_{\overline{K}}(X)$ is given by the above composite: $c(\sigma) = \varphi^{-1} \circ \sigma^{-1} \circ \varphi \circ \sigma$, so for $x \in X(\overline{K})$, we have $\sigma(\varphi(c(\sigma)(x))) = \varphi(\sigma(x))$.

We may identify $E'_{\overline{K}} = E_{\overline{K}}$, so the concern is the descent down to K. Given $x \in E(\overline{K})$, the new Galois action (which we denote by $\cdot'$) is given by

$$\sigma \cdot x = \sigma \cdot' c(\sigma)x,$$

essentially by construction of σ. Note that E' continues to have good reduction at $\mathfrak{P}$ because we chose our cocycle to factor through $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}})$. In total, we see that the Frobenius action has been adjusted by the unit $c(\sigma)$: if E had $[\mu] = \mathrm{Frob}_{\mathfrak{P},E}$, then we will have $\left[c(\sigma)^{-1}\mu\right] = \mathrm{Frob}_{\mathfrak{P},E'}$.

2.3.2 Proof of Lubin–Tate Theory

Let's relate this back to Lubin–Tate theory. The moral of the story is that the Lubin–Tate group $\mathcal{G}$ provided by Theorem 2.26 really does not care about the choice of uniformizer ϖ: adjusting ϖ really only adjusts $\mathcal{G}$ up to essentially a choice of model.

Lemma 2.40. Fix a p-adic field $(K, \mathcal{O}, \mathfrak{p})$. Choose two uniformizers ϖ and ϖ'. Then the Lubin–Tate formal groups $\mathcal{G}_\varpi$ and $\mathcal{G}_{\varpi'}$ are isomorphic over the ring of integers $\widehat{\mathcal{O}}$ of the completion $\widehat{K}$ of K^{unr}.

Proof. For brevity, let our formal groups by $\mathcal{G}$ and $\mathcal{G}'$, and we let F and F' be the formal group laws.

Write $\varpi' = \varpi u$ for some unit $u \in \mathcal{O}^\times$, and we would essentially like to twist $\mathcal{G}_{\varpi'}$ by a 1-cocycle corresponding to u to exhibit the isomorphism. However, note that there is some complication because we need to know that sending $\mathrm{Frob}_\mathfrak{p} \mapsto u$ actually extends to a continuous map $\mathrm{Gal}(K^{\mathrm{unr}}/K) \to \mathrm{Aut}_{\widehat{\mathcal{O}}}\, \mathcal{G}_{\varpi,\widehat{\mathcal{O}}}$.[2] Let $\breve{\mathcal{O}}$ be the ring of integers in K^{unr}. It turns out that we extend to a continuous map to merely $\mathrm{Gal}(K^{\mathrm{unr}}/K) \to \mathrm{Aut}\,\mathcal{G}_{\breve{\mathcal{O}}}$ if and only if u has finite order, which does not need to be the case! One could work with $\mathcal{G}_{\breve{\mathcal{O}}/\mathfrak{p}^\bullet}$ for some power $\mathfrak{p}^\bullet$ because the coefficients are now finite; then we can take the limit as $\mathfrak{p}^\bullet$ increases in power, so we do get our desired 1-cocycle.

Everything still satisfies descent, so the choice of 1-cocyle produces a twist $\widetilde{\mathcal{G}}$ of $\mathcal{G}$, still defined over $\mathcal{O}$, with Galois action given by

$$\sigma \cdot f(X) = \sigma \cdot' f([u]X)$$

for $f \in \widehat{\mathcal{O}}[[X]]$. We would like to show that $\widetilde{\mathcal{G}}$ is isomorphic to $\mathcal{G}'$. Thus, we are on the hunt for a power series $\varphi \in \widehat{\mathcal{O}}[[X]]$ witnessing the isomorphism. This formal power series can be constructed (and checked to work) using Proposition 2.31.

Roughly speaking, one needs to know that one has φ with an inverse function φ^{-1} (both in $\widehat{\mathcal{O}}[[X]]$) such that

$$\sigma(f\varphi)\left(\varphi^{-1}(X)\right) = (\sigma \cdot' f)(X).$$

Then one can check everything formally. ■

[2] If we only wanted to a homomorphism out of the Weil group $W_{K^{\mathrm{unr}}/K} = \mathbb{Z}$ instead of $\mathrm{Gal}(K^{\mathrm{unr}}/K)$, then this would not be a concern.

Remark 2.41. The Galois descent described above basically comes from the following example: suppose $V = \mathcal{O}$, and given a 1-cocycle $c\colon W_K \to \mathcal{O}^\times$ given by sending Frobenius to some unit $u \in \mathcal{O}^\times$. Then we get a new action $\star$ of Galois on $V_{\widehat{\mathcal{O}}}$ given by $\sigma \star v := u \cdot \sigma v$; we claim that the $\star$-fixed points $V_{\widehat{\mathcal{O}}}^{\sigma\star}$ is still $\mathcal{O}$. This boils down to something analogous to Hilbert's theorem 90.

Example 2.42. Let's try to compute $\mathcal{G}_{-p}$ for $K = \mathbb{Q}_p$. Once one writes out the Galois cocycle, one finds that $\mathcal{G}_{-p}$ is $\widehat{\mathrm{U}}_1$, where U_1 is the kernel of the norm map $\mathrm{N}\colon \mathbb{G}_{m,\mathbb{Q}_p^2} \to \mathbb{G}_{m,\mathbb{Q}_p}$. To be explicit, one should write $\mathbb{Q}_{p^2} = \mathbb{Q}_p(\sqrt{D})$ for some D, and then we see that $\mathrm{U}_1(\mathbb{Z}_p)$ consists of pairs (X, Y) (thought of as $X + Y\sqrt{D}$) such that $X^2 - DY^2 = 1$.

We are now ready to prove Theorem 2.19. Of course, $\mathcal{G}_\varpi$ will be the Lubin–Tate group. Recall that

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

where $q := \#\mathbb{F}_{\mathfrak{P}}$. Note that we are free to choose an object $\mathcal{G}_\varpi$ from the isomorphism class, and our proof of existence allows us to choose $[\varpi]$ to be anyone in $\mathcal{F}_\varpi$, so we take $[\varpi] = \pi X + X^q$. Note that the formal group law for $\mathcal{G}_\varpi$ is potentially complicated, but this choice of $[\varpi]$ will be easier for our calculation. Then $\mathcal{G}[\mathfrak{p}^n]$ consists of the roots of $[\varpi^n] = [\varpi]^{\circ n}$. However, one can calculate that $[\varpi]^{\circ n}$ is a separable polynomial of degree q^n. This implies that $\mathcal{G}_\varpi[\mathfrak{p}^n]$ and $\mathcal{O}/\mathfrak{p}^n$ have the same order q^n; thus, choosing $a \in \mathcal{G}_\varpi[\mathfrak{p}^n] \backslash \mathcal{G}_\varpi\left[\mathfrak{p}^{n-1}\right]$, we see that the induced map $\mathcal{O}/\mathfrak{p}^n \to \mathcal{G}[\mathfrak{p}^n]$ given by $u \mapsto ua$ must be injective.

Let's say a bit about why $[\varpi]^{\circ n}$ is separable. Define

$$\Phi_n(X) := \frac{[\varpi]^{\circ(n+1)}(X)}{[\varpi]^{\circ n}(X)},$$

which we can compute as $[\varpi]^{\circ(n-1)}(X)^{q-1} + \varpi$. By induction, one finds that this is an Eisenstein polynomial of degree $(q-1)q^{n-1}$, so for example it is irreducible. Thus, $[\varpi]^{\circ n}$ is a product of irreducible polynomials of all different degrees, thereby proving that it is separable.

In fact, the fact that our polynomial is Eisenstein implies that its roots are totally ramified over K, so we are in fact constructing a totally ramified extension of K. More precisely, we see that the extension $K(\mathcal{G}_\varpi[\mathfrak{p}^n])/K$ is a totally ramified Galois extension of degree $(q-1)q^{n-1}$. Now, set $K_n := K(\mathcal{G}_\varpi[\mathfrak{p}^n])$ and $K_\varpi = \bigcup_{n\ge1} K_n$ for brevity, and we see that we have constructed a character

$$\mathrm{Gal}(K_n/K) \to \mathrm{Aut}_{\mathcal{O}}(\mathcal{G}_\varpi[\mathfrak{p}^n]).$$

In fact this, character is surjective because the Galois action is transitive on the roots of the irreducible polynomial $\Phi_n(X)$. Now, this character extends in the limit to a character

$$\eta_\varpi\colon \mathrm{Gal}(K_\varpi/K) \to \mathrm{Aut}_{\mathcal{O}}(T_\varpi\mathcal{G}_\varpi).$$

This right-hand side is isomorphic to $\mathcal{O}^\times$, and we will treat it as such.

It remains to show that the above map is identified with local the local Artin map. In particular, we want to show that $\eta_\varpi(\mathrm{Art}_K(\varpi^n u)) = u$. Recall local class field theory provides local Artin map $K^\times/\mathrm{N}_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$ for abelian extensions L/K. Thus, for example, we see that $\mathrm{Art}_K\,\varpi$ acts trivially on K_∞ under the local Artin map because it is a norm (as seen from the Eisenstein polynomial constructed before!), so $\eta(\mathrm{Art}_K(\varpi)) = 1$. As such, it remains to see that $\eta_\varpi(\mathrm{Art}_K\,u) = u$ for units $u \in \mathcal{O}^\times$. Well, it is actually simply enough to check $\eta_\varpi(\mathrm{Art}_K\,\varpi') = \varpi'$ for other uniformizers ϖ', for which we will show

$$\eta^{-1}(u)\sigma = \mathrm{Art}_K\,\varpi'.$$

This will more or less follow formally from having $\mathcal{G}_{\varpi,\widehat{\mathcal{O}}} \cong \mathcal{G}_{\varpi',\widehat{\mathcal{O}}}$. Approximately speaking, we can think about these both as groups on $\widehat{\mathcal{O}}[[X]]$, and there is some Galois cocycle relating the two.

We would like to show that $\eta_\varpi(\operatorname{Art}_K \varpi') = u$, where u is chosen with $\varpi' = \varpi u$, and we already know that $\eta_{\varpi'}(\operatorname{Art}_K \varpi') = 1$. Thus, we will be done if we can show a statement of the form

$$\eta_{\varpi'}(\tau) \stackrel{?}{=} \eta_\varpi(\tau)u^{\operatorname{val}(\tau)},$$

where val is the valuation of $\mathfrak{p}$. Now using the 1-cocycle from earlier, we know that $\tau \star u = [u]^{\operatorname{val}(\tau)} \cdot \tau x$, where the left action is the one given by ϖ' and the right one is given by ϖ. This translates into the desired equality, so we are done.

2.4 February 13

I didn't have time to edit my notes from last class. Maybe I will do it over the weekend.

2.4.1 Where We're Going

For the next few classes, we will provide a guide to class field theory for function fields. Let's compare two stories.

- We remark that Lubin–Tate theory provides an understanding of $\operatorname{Gal}(K^{\mathrm{ab}}/K)$, but we remark that the local Langlands correspondence provides a full description of $\operatorname{Gal}(\overline{K}/K)$ by using the moduli of p-divisible groups. We remark that one can understand p-divisible groups by semilinear algebra (using Dieudonné modules). Roughly speaking, these can be generalized to local Shimura varieties, and then Scholze explains how to pass from here to local shtukas.
- On the other hand, for function fields $\mathbb{F}_q(\Sigma)$ (where Σ is some curve over $\mathbb{F}_q$) has a description of its abelian closure via geometric class field theory, but in fact one can go to the full algebraic closure (as in the local case) by working with the moduli of shtukas. There is a classical story before shtukas (akin to working with elliptic curves) known as Drinfeld modules.
- Returning to our story of complex multiplication, we note that our CM theory is more or less working with moduli of abelian varieties, which in our situation come down to Shimura varieties of PEL type. This story can be generalized to more general Shimura varieties, and one would like to have some notion of shtuka, but such a thing is not available yet.

2.4.2 p-Divisible Groups

Looking at the above remarks, our first task is to move to formal p-divisible groups (such as our Lubin–Tate groups) to p-divisible groups. (Here, p-divisible simply means that $[p]\colon \mathcal{G} \to \mathcal{G}$ is finite.) Namely, we will produce a fully faithful embedding between these categories, where formal p-divisible groups get sent to connected p-divisible groups. As for our bases, we fix a perfect field k of characteristic $p > 0$, and we would like our base A to be an Artinian local ring with residue field k. (For example, one can recover local fields by taking some kind of limit over k.)

Non-Example 2.43. The formal group $\widehat{\mathbb{G}}_a$ has formal group law given by $F[[X,Y]] = X + Y$. Multiplication by p is given by $[p] = pX$. Thus, this is not a p-divisible group (over, say, the ring of integers $\mathcal{O}$ of a local field).

Example 2.44. We work with the Lubin–Tate formal group $\mathcal{G}_\varpi$. Then $[\varpi]\colon \mathcal{G}_\varpi \to \mathcal{G}_\varpi$ is a finite map with finite kernel $\mathcal{G}_\varpi[\mathfrak{p}]$. Taking a power of ϖ, we find that $[p]\colon \mathcal{G}_\varpi \to \mathcal{G}_\varpi$ continues to be a finite map. More precisely, if $(p) = \mathfrak{p}^e$, then our kernel $\mathcal{G}_\varpi[\mathfrak{p}^e]$ becomes a finite group scheme of order $q^e = p^{[K:\mathbb{Q}_p]}$. This exponent $[K : \mathbb{Q}_p]$ is called the "height."

Now, given a formal p-divisible groups $\mathcal{G}$, we see that we have a sequence of finite groups

$$1 \hookrightarrow \mathcal{G}[p] \hookrightarrow \mathcal{G}\left[p^2\right] \hookrightarrow \cdots .$$

This motivates the following definition.

Definition 2.45. A *p-divisible group* over a base local ring A is a sequence of finite flat abelian group schemes

$$\mathcal{G}_0 \hookrightarrow \mathcal{G}_1 \hookrightarrow \mathcal{G}_2 \hookrightarrow \cdots$$

such that $\mathcal{G}_n$ is the kernel of $[p^n]\colon \mathcal{G}_{n+1} \to \mathcal{G}_{n+1}$ (which we assume to be finite) and such that there is a surjection $[p]\colon \mathcal{G}_{n+1} \to \mathcal{G}_{n+1}$. The p-divisible group is *connected* if and only if every $\mathcal{G}_\bullet$ is connected (at the special fiber). The *height* of this p-divisible group is $\log_p |G_1|$.

Remark 2.46. There is a lot of ambient symmetry. For example, one can take duals to receive some Cartier duality.

Example 2.47. For $\widehat{\mathbb{G}}_m$, we see that we get the p-divisible group $\mathcal{G}_n = \mu_{p^n}$, which is indeed connected. We remark that the Zariski cotangent space of $\mathcal{G}_n$ is $\mathbb{Z}/p^n\mathbb{Z}$.

A priori, it is a bit bizarre that one can recover a full formal p-divisible group by just understanding the p-torsion. Roughly speaking, the point is to pass to the limit of torsion to recover a formal neighborhood of the identity; for example, in the above example, taking the limit over $\mathbb{Z}/p^n\mathbb{Z}$ recovers a formal neighborhood $\mathbb{Z}_p$ of the identity.

To explain a bit of what we've done, we note that our theory of complex multiplication worked with a moduli space of elliptic curves with complex multiplication, which is a discrete moduli space. Then Lubin–Tate theory worked with some moduli space of Lubin–Tate groups (maybe with level structure to keep track of the Tate module), which was again discrete. So our next step, perhaps, is to discuss moduli of p-divisible groups.

Remark 2.48. With complex multiplication, we had to fix an order $\mathcal{O}$. With Lubin–Tate theory, we had to fix a uniformizer ϖ. In our moduli space of p-divisible groups, we will have to fix something to build our moduli space as well, which will be the special fiber. These choices must occur (roughly speaking) because we eventually need to produce some totally ramified extensions, and there is no canonical way to do this.

Next class, we will set up the local Langlands correspondence for $\mathbb{Q}_p$ by using the moduli of p-divisible groups of height h. In particular, such objects produce h-dimensional Galois representations.

Remark 2.49. It is now enough to only work with $\mathbb{Q}_p$ because understanding the algebraic closure of our local p-adic fields is the same as $\overline{\mathbb{Q}}_p$.

2.5 February 18

Before we do anything, let's find a sign in Lubin–Tate theory that the reciprocity map

$$\operatorname{Art}\colon \mathbb{Q}_p^\times \to \operatorname{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$$

restricts to $\mathbb{Z}_p^\times \to I_p$, where I_p is the inertial subgroup, and the inverse map $I_p \to \mathbb{Z}_p^\times$ is given by the cyclotomic character. One way to see this is by Lubin–Tate theory, where we need to compute the character η_p, which can be done by using the explicit Lubin–Tate formal group.

Another way to see this is by global class field theory (and the Kronecker–Weber theorem), which explains that one has

$$\mathbb{Q}_p^\times \hookrightarrow \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \simeq \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$$

at "finite level" $\mathbb{Q}(\zeta_N) \subseteq \mathbb{Q}^{\mathrm{ab}}$; namely, we see that $u \in \mathbb{Z} \setminus p\mathbb{Z}$ in $\mathbb{Q}_p^\times$ goes to a u-power Frobenius on the left, up to a sign depending on the normalization of class field theory.

2.5.1 Cartier Duality

Today we continue with our p-divisible groups.

Definition 2.50. Fix a base ring A. Then a *finite group G over A* is a finite abelian group scheme over A which is locally free over A.

Remark 2.51. Explicitly, we are asking for the coordinate ring $A[G]$ of G to be a Hopf algebra which is locally free and of finite rank over A.

Example 2.52. Fix a ring A. Then one has constant groups $\mathbb{Z}/N\mathbb{Z}$ and μ_N.

Example 2.53. The kernel of an isogeny of abelian varieties is also seen to be a finite group over the base.

Example 2.54. Over $\overline{\mathbb{F}}_p$, we let α_p be the kernel of Frobenius fitting into the diagram

$$1 \to \alpha_p \to \mathbb{G}_a \stackrel{(\cdot)^p}{\to} \mathbb{G}_a.$$

In particular, we see that $\alpha_p = \operatorname{Spec} \overline{\mathbb{F}}_p[x]/(x^p)$.

Let's give a little structure theory.

Lemma 2.55. Fix a finite group G over a base ring A. Then the connected component $G^\circ \subseteq G$ is a subgroup, and the quotient $G^{\text{ét}} := G/G^\circ$ is étale. In short, there is a short exact sequence

$$1 \to G^\circ \to G \to G^{\text{ét}} \to 1.$$

Proof. The fact that G° is a subgroup is a rather formal fact. We won't check that the quotient is étale, but the idea is that the only obstruction to being separable should come down to having a large infinitesimal neighborhood. ■

These finite groups have a theory of "Cartier" duality, analogous to Pontryagin duality in harmonic analysis.

Definition 2.56 (Cartier dual)**.** Fix a base finite group G over a base ring A. Then we define the *Cartier dual* as the sheaf $\operatorname{Alg}(A) \to \operatorname{AbGrp}$ given by

$$G^\vee \colon R \mapsto \operatorname{Hom}(G(R), R^\times).$$

Remark 2.57. Let's check that $G^\vee$ is represented by an affine scheme over A which is locally free over A. Indeed, one finds that the Hopf algebra $A[G^\vee]$ should be

$$\operatorname{Hom}(A[G], A),$$

where $A[G]$ is the Hopf algebra of G. One sees that the above is locally free of finite rank over A because the same was true of $A[G]$, and one sees that $A[G]$ is a Hopf algebra of an abelian group because implies the same for $A[G^\vee]$ essentially by interchanging the multiplication and comultiplication.

Remark 2.58. The above remark explains why $G^{\vee\vee} = G$.

Example 2.59. Consider $A = \mathbb{F}_p$.

- If $\gcd(p, N) = 1$, then the dual of $\mathbb{Z}/N\mathbb{Z}$ is μ_N. Note that both of these schemes are étale over A.
- The dual of $\mathbb{Z}/p\mathbb{Z}$ is μ_p. Note that $\mathbb{Z}/p\mathbb{Z}$ is étale while μ_p is connected.
- The dual of α_p is α_p. Note that these are both connected.

These can be seen by explicitly writing out the multiplication and comultiplication everywhere.

Remark 2.60. Cartier duality provides a contravariant exact functor.

This whole connected and étale business is a bit subtle on the duality, so we pick up some definitions, motivated by the above calculations.

Definition 2.61. Fix a finite group G over a perfect field k.

- We say G is *unipotent* if and only if $G^\vee$ is connected.
- We say G is *multiplicative* if and only if G is étale.

Example 2.62. Over $\mathbb{F}_p$, we see that $\mathbb{Z}/p\mathbb{Z}$ and α_p are both unipotent, and μ_N is multiplicative.

Remark 2.63. This notion is poorly behaved when working with different characteristics simultaneously. The problem is that the duals in different characteristics are likely to behave differently depending on (for example) when the characteristic divides the order.

We now see that a group G can be split into pieces which are étale multiplicative, étale unipotent, connected multiplicative, and connected unipotent. Notably, no two groups of any individual pair of adjectives will have any no nontrivial morphisms between each other: connected and étale groups have no nontrivial morphisms between each other, and the same is carries over for the duals.

We now recall some of our story of p-divisible groups.

Definition 2.64 (formal p-divisible group)**.** A *formal p-divisible group* is a formal group $\mathcal{G}$ together with a p-power map $[p]\colon \mathcal{G} \to \mathcal{G}$ which makes the underlying map $A[[X]] \to A[[X]]$ into a free module of finite rank over itself.

Remark 2.65. Note that this implies that $\mathcal{G}[p]$ is a finite group over A: namely, $\mathcal{G}[p]$ is $A[[X]]$ modulo the power series given by $[p]$, and then we see that

Remark 2.66. Eventually, we will find that if A is a perfect field, then $\mathcal{G}[p]$ has prime-power order, and it turns out to have no component which is étale multiplicative.

2.5.2 Witt Vectors

We would like to classify p-divisible groups, which will eventually turn into some semilinear algebra in the form of Dieudonné modules.

This requires some discussion of Witt vectors. We will not go into the formal definition involving power series here. Instead, let's give a little motivation. One can view the ring $\mathcal{O} := k[[t]]$ as being a formal neighborhood of $0 \in \mathbb{A}^1_k$. For example, an element $\gamma \in k[[t]]$ can be thought of as the germ of some arc going through $\gamma(0) \in \mathbb{A}^1_k$. The moral is that we can think of $k[[t]]$ as the k-points of some infinite-dimensional "arc space" $L^+\mathbb{A}^1_k$ of $\mathbb{A}^1_k$. It is not so hard to actually describe $L^+\mathbb{A}^1_k$: it should be an inverse limit

$$L^+\mathbb{A}^1 = \varprojlim L^+_n\mathbb{A}^1,$$

where $L^+_n\mathbb{A}^1 = \mathbb{A}^{n+1}$ contains information of the first $(n+1)$ coefficients for the arc here. One can find a ring structure on these schemes (the multiplication map can be seen on the level of the coordinates), and we see that the $\mathbb{F}_q$-points are $\mathcal{O}$.

This perspective provides some new insights. For example, we see that $\mathcal{O}^\times$ are the $\mathbb{F}_q$-points of a Zariski open subset which is dense. Indeed, $\mathcal{O}^\times$ consists of the condition that the constant term is nonzero, which is a Zariski open and dense condition. This provides a new topology for us to do some interesting sheaf theory.

The Witt vectors bring this story to characteristic 0. Namely, one finds that W is an inverse limit of some ring schemes W_n. Given a perfect field k of positive characteristic, one finds that $W(k)$ is some complete local ring with residue field k.

Example 2.67. One finds $W(\mathbb{F}_q) = \mathbb{Z}_q$. The idea is to take some sequence $(a_0, a_1, \ldots)$ to the power series

$$a_0 + a_1^{1/p}p + a_2^{1/p^2}p^2 + \cdots,$$

where the coefficients are elements of $\mathbb{F}_p$ embedded into $\mathbb{Z}_p$ via the Teichmüller lift. One can reverse-engineer this to figure out how to write out addition and multiplication of the tuples; in particular, the twists are present so that addition and multiplication are only polynomial in the variables if we take the above $1/p^\bullet$-twists.

The moral of the story is that we managed to think of $\mathbb{Z}_q$ as the $\mathbb{F}_q$-points of a (limit of) scheme(s).

Importantly, $W(k)$ comes with a Frobenius F.

Definition 2.68. Fix a perfect field k of positive characteristic p, and let σ be the Frobenius on k. Then we define the *(relative) Frobenius* $F\colon W \to W$ by

$$F \cdot (a_1, a_2, \ldots) := (\sigma(a_1), \sigma(a_2), \sigma(a_3), \ldots).$$

There is also a dual operation called the Verschiebung. Roughly speaking, this morphism should be the Cartier dual of the Frobenius $F\colon W_n \to W_n$, where now we think of W_n a group over k (flat of dimension n).

Definition 2.69. Fix a perfect field k of positive characteristic p. On the level of the power series, $V\colon W(k) \to W(k)$ is given by shifting coordinates over to the right by 1 by

$$V\colon (a_0, a_1, a_2, \ldots) \mapsto (0, a_0, a_1, \ldots).$$

For example, we see that V is nilpotent on the W_ns and hence nilpotent in the limit on W_∞.

Example 2.70. One can use the formulae to compute

$$p \cdot (a_0, a_1, a_2, \ldots) = (0, a_0^p, a_1^p, \ldots),$$

so one finds $p = FV = VF$.

Remark 2.71. It turns out that W_n (now viewed as a functor) is a p-power torsion unipotent group over k, which can be seen from the construction we did not give: one should let W_n^m be the subgroup whose first m entries all vanish, and then $W_n^{m+1} \subseteq W_n^m$ is a normal subgroup with quotient $\mathbb{G}_a$.

2.6 February 20

Here we go.

2.6.1 Frobenius and Verschiebung

Let's write down a Frobenius and Verschiebung for finite groups. For motivation, we recall the construction of the relative Frobenius. Fix a scheme X over a field k of positive characteristic p. Then we draw the following pullback diagram.

$$\begin{tikzcd}
X \arrow[dr, dashed, "F_{X/k}"] \arrow[drr, bend left, "\sigma"] \arrow[ddr, bend right] & & \\
& X^{(p)} \arrow[r, "\sigma"] \arrow[d] & X \arrow[d] \\
& \operatorname{Spec} k \arrow[r, "\sigma"] & \operatorname{Spec} k
\end{tikzcd}$$

Concretely, $X^{(p)}$ is $X \to \operatorname{Spec} k$ pulled back everywhere by Frobenius. On affine open subsets of finite type, one writes $U = \operatorname{Spec} k[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$, and then $X^{(p)}$ is cut out by the same variables but where the coefficients of the polynomials are $\sigma(f_\bullet)$. Then we note that our map $F_{X/k}$ above is the relative Frobenius, which is understood to send the variables $x_\bullet \mapsto x_\bullet^p$ on affine open subsets of finite type.

We are now ready to define the Frobenius and Verschiebung.

Definition 2.72 (Frobenius)**.** Fix an affine commutative group G over a field k of positive characteristic p. This is the map $F_G \colon G \to G^{(p)}$ given in the above construction.

Remark 2.73. Let's give a more concrete definition when the group is finite. Write $A = k[G]$ for the underlying Hopf algebra of G. Then our map $A^{(p)} \to A$ is given by

$$a \mapsto \underbrace{(a \otimes \cdots \otimes a)}_{p} \mapsto a^p,$$

where the last map is the k-linear multiplication.

For the Verschiebung, one should imagine taking a Cartier dual.

Definition 2.74 (Verschiebung)**.** Fix an affine commutative group G over a field k of positive characteristic p. Let A be the underlying Hopf algebra, and then we define the Verschiebung morphism $G^{(p)} \to G$ to be given by $A \to A^{(p)}$ by the composite

$$\begin{array}{ccccc} A & \to & (A \otimes \cdots \otimes A)^{S_p} & \to & A^{(p)} \\ a & \mapsto & a \otimes \cdots \otimes a & \mapsto & a \end{array}$$

where the last map is uniquely defined by sending those invariant tensors as shown.

Remark 2.75. Note that this last map notably sends $(ca \otimes \cdots \otimes ca) \mapsto c^p a$, which explains why the target should be $A^{(p)}$ and A: this last map is not k-linear but only σ-semilinear!

For each of our finite group examples, let's explain what happens to the Frobenius and Verschiebung.

Example 2.76. Because Frobenius acts by 0 on α_p, we see that the Verschiebung is 0 as well.

Example 2.77. Frobenius acts as an isomorphism on the constant groups $\mathbb{Z}/N\mathbb{Z}$ for any N.

Example 2.78. Frobenius acts by 0 on μ_p and as an isomorphism on μ_N when $\gcd(p, N) = 1$.

This suggests the following classification.

Proposition 2.79. Fix a finite group G over a base field k of positive characteristic p.

(a) Then G is connected if and only if the Frobenius F is nilpotent.

(b) Then G is étale if and only if the Frobenius F is an isomorphism.

(c) Dually, G is unipotent if and only if the Verschiebung V is nilpotent.

(d) Dually, G is multiplicative if and only if the Verschiebung V is an isomorphism.

These last two conditions have more intuitive descriptions.

Proposition 2.80. Fix a finite group G over a base field k of positive characteristic p.

(a) The group G is unipotent if and only if G embeds into as a subgroup of upper-triangular unipotent matrices. More abstractly, there is a filtration of normal subgroups with quotients embedding in $\mathbb{G}_a$.

(b) The group G is multiplicative if and only if G embeds into a split torus.

2.6.2 Semilinear Algebra for Fun and Profit

We are now ready to state a classification theorem.

Theorem 2.81. Fix a perfect field k of positive characteristic p. Then the rings W_n generate the category of affine unipotent finite type abelian groups over k in the following sense: the functor $G \to M(G)$ given by

$$M \colon G \mapsto \varinjlim \operatorname{Hom}(G, W_\bullet)$$

is a contravariant fully faithful embedding into $\operatorname{End}(W_\infty)$-modules, where $W_\infty = \varinjlim W_n$.

Remark 2.82. More succinctly, we can think about the functor M as

$$\operatorname{Hom}(G, W_\infty),$$

where W_∞ is some direct limit. For example, one can think of $W_\infty(\mathbb{F}_p)$ as $\mathbb{Q}_p/\mathbb{Z}_p$ because the direct limit morphisms are approximately compatible with identifications

$$W_n(\mathbb{F}_p) = \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p \subseteq \mathbb{Q}_p/\mathbb{Z}_p.$$

Remark 2.83. This is a fairly typical statement in representation theory: one has a category we'd like to understand, so we pick up some particularly interesting objects $W_\bullet$ in it, and it turns out that we can read off the entire category from these elements as modules in some sense.

This is a nice result because it tells us that our p-power unipotent groups are found in some linear algebra.

Let's spend a moment describing $\operatorname{End}(W_\infty)$. Of course, W has an action on W_∞: admittedly one has to twist the action a bit because the embeddings $W_n \to W_{n+1}$ are not actually W-equivariant, but one can fix it by defining

$$w \star x := \sigma^{1-n}(w_n)x$$

for $w \in W$ and $x \in W_n$, where the multiplication on the right is happening in W_n. But there are more endomorphisms: there is a Frobenius morphism $F\colon W_\infty \to W_\infty$ (glued together from the Frobenius morphism above), and there is a Verschiebung V morphism. In fact, we claim that these are all the endomorphisms.

Definition 2.84 (Dieudonné module)**.** Fix a perfect field k of positive characteristic. Then we define the *Dieudonné ring* as being generated by the Witt vectors $W(k)$ and two extra variables F and V subject to the requirements

$$\begin{cases} F \circ \lambda = \sigma\lambda \circ F, \\ V \circ \sigma\lambda = \lambda \circ V, \\ F \circ V = V \circ F = p, \end{cases}$$

where $\lambda \in W(k)$.

Lemma 2.85. Fix a perfect field k of positive characteristic. Then $\operatorname{End}_k W_n = D_k/D_kV^n$ for any $n \geq 0$, and $\operatorname{End}_k W_\infty = D_k$.

Remark 2.86. The essential image of M in Theorem 2.81 can now be described as requiring that V acts as a nilpotent operator.

Remark 2.87. One can now restrict Theorem 2.81 to an equivalence between the category finite unipotent groups over k and the category of D_k-modules which have finite length as a $W(k)$-module.

With the above remark in hand, we are able to classify all p-power torsion groups with some Cartier duality.

Theorem 2.88. Fix a perfect field k of positive characteristic p. Then there is an equivalence M of categories between the category of finite p-power torsion abelian groups over k and the category of D_k-modules of finite length as a $W(k)$-module. It is categorized as follows.

(i) If G is unipotent, then $M(G)$ is defined as in Theorem 2.81.

(ii) For any finite G, one has $M(G^\vee) = M(G)^\vee$.

Remark 2.89. In particular, it is true that étale-étale groups are never p-power torsion.

We now go back to classify p-divisible groups. Here is our result.

Theorem 2.90. Fix a perfect field k of positive characteristic p. For a p-divisible group $\mathcal{G} = \{G_n\}_{n\geq 1}$, we define the functor M out of p-divisible groups by

$$M\mathcal{G} := \varprojlim M(G_\bullet).$$

Then M is an equivalence between the following two categories.

- The category of p-divisible groups (of height h).
- The category of D_k-modules which are free of rank h as $W(k)$-modules and such that $FV = p$.

Remark 2.91. The condition that we have a D_k-action on M with $FV = p$ can be recast as requiring that our modules have a σ-semilinear endomorphism F (over $W(k)$) such that $pM \subseteq FM$. Roughly speaking, one can construct V uniquely from this condition by attempting to invert the isomorphism

$$pM[1/p] \cong FM[1/p].$$

Remark 2.92. The rank condition comes about because one finds that $\deg G_n = p^{nh}$ for each $n \geq 1$.

Lastly, we go all the way back to formal p-divisible groups. Because we haven't yet, let's give a definition.

Definition 2.93. A *formal p-divisible group* $\mathcal{G}$ of dimension d consists of the data of a formal group law on the formal neighborhood $A := k[[X_1, \ldots, X_d]]$ such that the multiplication map $[p]\colon \mathcal{G} \to \mathcal{G}$ is an isogeny (i.e., the induced map $[p]\colon A \to A$ presents A as a locally free module over itself).

Remark 2.94. There is a functor sending such formal p-diivisible groups $\mathcal{G}$ to p-divisible groups given by

$$\mathcal{G} \mapsto \{\mathcal{G}[p^n]\}_{n\geq 1}.$$

This functor is fully faithful, and it preserves dimensions in some sense.

Remark 2.95. There is a way to read the dimension of $\mathcal{G}$ off of only(!) the p-divisible group $\{G_n\}_{n\geq 1}$ where $G_n := \mathcal{G}[p^n]$. Roughly speaking, it turns out that one can do some tangent space computations: the dimension of G is the dimension of the k-vector space $M(G)/FM(G)$. Notably, it turns out that $h(G) = h(G')$, but it turns out that $\dim \mathcal{G} + \dim \mathcal{G}' = h$.

Example 2.96. Here are two examples.

- The p-divisible group $G = \mathbb{Q}_p/\mathbb{Z}_p$ has dimension 0 because it is étale everywhere.
- The p-divisible group $G = \mu_{p^\infty}$ has dimension 1 because it comes from the formal group $\widehat{\mathbb{G}}_m$.

Do note that both of these examples have height 1.

Remark 2.97. Our CM and Lubin–Tate stories can be seen as explaining what happens with our formal groups of dimension 1 and varying height. Similarly, local Langlands for $\mathrm{GL}_2(\mathbb{Q}_p)$ works with dimension 1 and varying height. However, there is a use for higher dimension: abelian varieties of dimension g produce formal p-divisible groups of height $2g$, and abelian varieties are relevant to us because they produce the CM theory for CM fields.

2.6.3 A Little Local Langlands

Let's finish today's lectures by indicating what local Langlands looks like for GL_h, for fixed height h.

Let's build a tower of moduli spaces. We begin with a moduli space $\mathcal{M}_0$ of (connected) one-dimensional p-divisible groups of height h (over $\mathbb{Z}_p$ or something like this). By some Dieudonné theory, there is only one such object over an algebraically closed field, so we are essentially studying twists. More generally, for $n \geq 0$, we let $\mathcal{M}_n$ be the moduli space of one-dimensional p-divisible groups of height h but with p^n-level structure; for example, in the étale case, we choose to fix an isomorphism $G_n \cong \left(\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}\right)^h$. This produces a tower

$$\cdots \to \mathcal{M}_{n+1} \to \mathcal{M}_n \to \mathcal{M}_{n-1} \to \cdots \to \mathcal{M}_2 \to \mathcal{M}_1 \to \mathcal{M}_0,$$

and we will call the limiting tower by $\mathcal{M}_\infty$. We would like to say that something about $\mathrm{H}^\bullet(\mathcal{M}_\infty)$ realizes the local Langlands correspondence. Namely, we would like to have something like

$$\mathrm{H}^\bullet(\mathcal{M}_\infty) \approx \bigoplus_{\rho\colon W_{\mathbb{Q}_p} \to \mathrm{GL}_h(\mathbb{Q}_p)} \rho \boxtimes \mathrm{LLC}(\rho),$$

where ρ is a representation of the Weil group $W_{\mathbb{Q}_p}$, and $\mathrm{LLC}(\rho)$ is a representation of $\mathrm{GL}_h(\mathbb{Q}_p)$. Here are some reasons why this doesn't work.

(i) Morally, the trivializations admit some action by $\mathrm{GL}_h(\mathbb{Z}_p)$ instead of $\mathrm{GL}_h(\mathbb{Q}_p)$, so something must be a bit wrong.

(ii) There is an additional action by a group $J = \operatorname{Aut} \mathcal{G}_0$, where $\mathcal{G}_0$ is the unique connected one-dimensional p-divisible group of height h over $\overline{\mathbb{F}}_p$. Concretely, $\mathcal{G}_0$ can be realized as $W(\overline{\mathbb{F}}_p)^h = \mathbb{Z}_{p^\infty}^h$, where we twist the Frobenius σ-action by the automorphism

$$\sigma \star v = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ p & 0 & 0 & \cdots & 0 & 0 \end{bmatrix} (\sigma v).$$

Then one can realize J as the units of some division algebra, which one can see from some explicit construction of the Dieudonné module of $\mathcal{G}_0$. One finds that J looks like the units in some division algebra D.

To fix this, maybe we should write something like

$$\mathrm{H}^\bullet(\mathcal{M}_\infty) \approx \bigoplus_{\rho\colon W_{\mathbb{Q}_p}\to \mathrm{GL}_h(\mathbb{Q}_p)} \rho \boxtimes \mathrm{LLC}(\rho) \boxtimes \mathrm{JL}(\mathrm{LLC}(\rho)),$$

where the last term is a representation of $D_h(\mathbb{Q}_p)$. This still doesn't work. Here are some more reasons.

(iii) The moduli space $\mathcal{M}_\infty$ doesn't even make sense. We swept the trivializations under the rug, but they present a genuine problem to make $\mathcal{M}_\infty$ live over $\mathbb{Z}_p$ because our groups are frequently connected over the special fiber. Instead, $\mathcal{M}_0$ will only be able to be pro-representable over Artinian algebras: it sends an Artinian local ring A with residue field k to a pair $(\mathcal{G}, \iota)$, where $\mathcal{G}$ is a p-divisible group over A, and $\iota\colon \mathcal{G}_0 \to \mathcal{G}|_k$ is some isomorphism.

We will now only be able to lift $\mathcal{M}_0$ to the formal scheme $\operatorname{Spf}\mathbb{Z}_p$.

(iv) Continuing with the level structures for higher $\mathcal{M}_n$s, there are two approaches to fix the level structure. For example, one can use Drinfield's level structures, which simply fail to be an isomorphism. Alternatively, one can work with Rapaport–Zink spaces, which essentially remove the special fiber of our formal scheme $\operatorname{Spf}\mathbb{Z}_p$, which becomes a rigid analytic space. This is akin to more modern approaches via the Fargues–Fontaine curve. Removing the special fiber now helps because torsion points (and hence our level structures) succeed at making sense away from the special fiber.

(v) Any kind of rigid cohomology of $\mathrm{H}^\bullet(\mathcal{M}_n)$ we choose will be enormous. The problem is that we end up looking at some sort of meromorphic functions on a non-compact space, so one needs to do some fixing.

To fix this, one should add some finiteness conditions coming from vanishing cycles next to the special fiber. Roughly speaking, one looks at fibers of the cohomology varying over the one-dimensional base (which is roughly $\mathbb{Z}_p$), and there is a notion of nearby vanishing cycles which helps make the cohomology a bit smaller. Intuitively, the idea is that one wants to do some kind of compactification akin to what needs to happen with modular curves.

(vi) We now only have an action of $\mathrm{GL}_h(\mathbb{Z}_p)$, not of the desired $\mathrm{GL}_h(\mathbb{Q}_p)$. It is possible (e.g., done by Scholze) to use merely the action of $\mathrm{GL}_h(\mathbb{Z}_p)$ to produce the reciprocity map. Harris–Taylor do succeed at defining some $\mathrm{GL}_h(\mathbb{Q}_p)$ in a rather ad-hoc way. Lastly, we mention that one can use Rapoport–Zink spaces can be used to get the action more cleanly. Roughly speaking, one passes to the category of formal groups with morphisms given by (quasi-)isogenies, where we are now forced to not look at Tate modules with integral structure but instead with rational structure.

We remark that we already saw this difficulty present in Lubin–Tate theory: our Lubin–Tate groups merely had an action of $\mathcal{O}^\times = \mathrm{GL}_1(\mathcal{O})$, and it was rather non-obvious how to then recover the full reciprocity map from the inertia part.

(vii) At this point, our moduli space should be taken as triples (G, ι, α), where G is the formal group, ι is a trivialization at the special fiber, and α is a level structure of the rational Tate module. Thus, there are three commuting actions: one has Galois action by a Weil group acting on the torsion itself, one has an action of $\mathrm{GL}_h(\mathbb{Q}_p)$ on the level structure α, and one has an action of automorphisms at the special fiber on ι. The cohomology now decomposes into a sum of pieces which look like

$$\rho \boxtimes \rho' \boxtimes \mathrm{LLC}(\rho'),$$

which is a representation of $J(\mathbb{Q}_p)\times \mathrm{GL}_h(\mathbb{Q}_p)\times W(\mathbb{Q}_p)$ (where the first group comes from the Jacquet–Langlands correspondence, and the last group is the Weil group).

2.7 Homework 2

In this section, we work out some examples related to Dieudonné modules. Before going any further, we set up some notation. Throughout, k denotes a perfect field of positive characteristic p, and W denotes the ring scheme of Witt vectors. Whenever appropriate, F and V are the Frobenius and Verschiebung morphisms, respectively. As in our Dieudonné theory, it will be helpful to define the pro-group

$$W_\infty := \varinjlim W_n.$$

We remark that various parts of the following discussion were motivated by the discussion here.

2.7.1 Some Cartier Duals

Before getting into any heavy computation, we give the Hopf algebra structure of the algebraic groups $\mathbb{G}_a$ and $\mathbb{G}_m$.

Lemma 2.98. For any ring k, we give the Hopf algebra structure on $\mathbb{G}_a$.

Proof. The group scheme $\mathbb{G}_a$ is defined on the level of R-points by returning the additive group $\mathbb{G}_a(R) := R$. On the level of sets, we thus see that $\mathbb{G}_a$ is represented by the affine scheme $\operatorname{Spec} k[t]$, where the point is that

$$\mathbb{G}_a(R) = \operatorname{Mor}_k(\operatorname{Spec} R, \mathbb{G}_a) = \operatorname{Hom}_k(k[t], R) = R,$$

where the last equality is given by $f \mapsto f(t)$.

It remains to give the comultiplication and coidentity on $k[t]$. The coidentity $\operatorname{Spec} k \to \mathbb{G}_a$ needs to pick out $0 \in \mathbb{G}_a(R)$ for each R, so it will be given by the map $k[t] \to k$ defined as $t \mapsto 0$. The comultiplication $m\colon \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$ corresponds to the addition map $R \times R \to R$ on R-points, which on the level of the schemes comes from the ring map $m^\sharp\colon k[t] \to k[t] \otimes_k k[t]$ by

$$m^\sharp(t) := (t \otimes 1) + (1 \otimes t).$$

Indeed, a pair $(r, s) \in R \times R$ corresponds to a ring homomorphism $\varphi^\sharp\colon k[t] \otimes_k k[t] \to R$ given by $\varphi^\sharp(t \otimes 1) = r$ and $\varphi^\sharp(1 \otimes t) = s$. Then we require that $m \circ \varphi$ to correspond to the R-point $r + s \in \mathbb{G}_a(R)$, which can be computed via $(m \circ \varphi)^\sharp(t) = r + s$. ■

Lemma 2.99. For any ring k, we give the Hopf algebra structure on $\mathbb{G}_m$.

Proof. We proceed as in the previous lemma, but we will be a bit briefer because many of the arguments are similar.

- On R-points, we have $\mathbb{G}_m(R) = R^\times$, so we find that $\mathbb{G}_m = \operatorname{Spec} k\left[t, t^{-1}\right]$ as schemes.
- For the coidentity, we need to pick out $1 \in \mathbb{G}_m(R)$ for each R, so this is given by the scheme map $\operatorname{Spec} k \to \mathbb{G}_m$ defined by the ring map $k\left[t, t^{-1}\right] \to k$ via $t \mapsto 1$.
- For the comultiplication, we need to define the ring map which gives the natural transformation $\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ defined by multiplication. Well, $m^\sharp\colon k\left[t, t^{-1}\right] \to k\left[t, t^{-1}\right] \otimes k\left[t, t^{-1}\right]$ defined by

  $$m^\sharp(t) := (t \otimes t)$$

  can be checked to work. ■

We now compute some duals of some finite groups.

Exercise 2.100. For any ring k of positive characteristic p, we show that the Cartier dual of the finite group α_p is α_p.

Proof. Because we should do it at least once, we prove this using the definition of Cartier duality by characters, working directly with the algebraic group $\alpha_p^\vee(R) := \operatorname{Hom}_R(\alpha_{p,R}, \mathbb{G}_{m,R})$.

1. We begin by giving the Hopf algebra structure. By definition, α_p is given on R-points by
$$\alpha_p(R) \coloneqq \{r \in R : r^p = 0\}.$$
In particular, we see that the inclusion $\alpha_p(R) \subseteq R$ defines an embedding $\alpha_p \hookrightarrow \mathbb{G}_a$. For example, the definition of α_p implies that α_p is represented by the scheme $\operatorname{Spec} k[t]/(t^p)$, where $f\colon \operatorname{Spec} R \to \operatorname{Spec} k[t]/(t^p)$ corresponds to $f^\sharp(t) \in \alpha_p(R)$. Thus, the natural inclusion $\iota\colon \alpha_p \hookrightarrow \mathbb{G}_a$ is seen to be given on schemes by $\iota^\sharp(t) = t$ (e.g., by plugging in some test ring R). Because we already know the coidentity and comultiplication on $\mathbb{G}_a$, the same data now passes to the closed subscheme: our coidentity $\operatorname{Spec} k \to \alpha_p$ is given on rings by $t \mapsto 0$, and our comultiplication $\alpha_p \times \alpha_p \to \alpha_p$ is given by $t \mapsto (t \otimes 1) + (1 \otimes t)$.

2. We now begin our duality computation. For a general ring k of positive characteristic p, we would like to compute the group scheme $\operatorname{Hom}_k(\alpha_p, \mathbb{G}_m)$, for which by base-changing it is enough to just compute the k-points for now. This embeds into the set
$$\operatorname{Mor}_k(\alpha_p, \mathbb{G}_m) = \mathbb{G}_m\left(k[t]/(t^p)\right),$$
which of course consists of the units in $k[t]/(t^p)$. Well, because the Frobenius is the zero map on $k[t]/(t^p)$, we see that any polynomial $f(t) \in k[t]/(t^p)$ has $f(t)^p = f(0)$ and therefore is a unit if and only if $f(0) \in k^\times$.

3. Let's unwind the morphism $\alpha_p \to \mathbb{G}_m$ given by some such polynomial f so that we can check when it is a homomorphism of groups. On R-points, we may consider some $r \in \alpha_p(R)$, which corresponds to the ring homomorphism $k[t]/(t^p) \to R$ defined by $t \mapsto r$. Then composing with f appropriately sends this to the ring homomorphism $k\left[t, t^{-1}\right] \to R$ given by $t \mapsto f(r)$, which of course corresponds to $f(r) \in \mathbb{G}_m(R)$. Thus, we are interested in when the map
$$\begin{aligned} \alpha_p &\to \mathbb{G}_m \\ r &\mapsto f(r) \end{aligned}$$
is actually a group homomorphism.

4. We now check which f produce a homomorphism. For example, we must have $f(0) = 1$. More generally, we must have $f(r+s) = f(r)f(s)$ to hold for any $r, s \in \alpha_p(R)$; this implies having $f(s+t) = f(t)f(s)$ for $s, t \in k[s,t]/(s^p, t^p)$, and this latter condition can be seen to be sufficient as well. Now, write $f(t) = \sum_{i=0}^\infty a_i t^i$ (for example, $a_0 = 1$) so that
$$f(s+t) = \sum_{i,j \ge 0} a_{i+j} \binom{i+j}{j} s^i t^j \qquad \text{and} \qquad f(s)f(t) = \sum_{i,j\ge 0} a_i a_j s^i t^j.$$
In particular, looking at the coefficients of $s^i t$, this implies that $a_{i+1}(i+1) = a_i a_1$ for each $i \ge 0$, so we are forced to have
$$f(t) = \sum_{i=0}^{p-1} \frac{a_1^i}{i!} t^i$$
and so $a_1^p = 0$. On the other hand, for any $a \in \alpha_p(R)$, the polynomial $f_a(t) \coloneqq \sum_{i=0}^{p-1} \frac{a^i}{i!} t^i$ can be seen to satisfy $f(s+t) = f(s)f(t)$: the coefficient of $s^i t^j$ is
$$a^{i+j} \cdot \frac{1}{(i+j)!} \binom{i+j}{j} = a^{i+j} \cdot \frac{1}{i!j!}.$$

5. At this point, we have produced a bijection $\alpha_p(k) \to \operatorname{Hom}_k(\alpha_p, \mathbb{G}_m)$ given by $a \mapsto f_a$. We will be done as soon as we check that this upgrades to a natural isomorphism of groups. To check that this is an isomorphism, we must check that $f_{a+b}(t) = f_a(t) f_b(t)$, which is true because the coefficient of t^i is
$$\frac{(a+b)^i}{i!} = \sum_{m+n=i} \frac{a^m b^n}{m!n!}.$$

Lastly, for naturality, we suppose that we have a ring homomorphism $\varphi\colon k \to k'$, and we note that the diagram

$$\begin{tikzcd} \alpha_p(k) \arrow[r] \arrow[d] & \operatorname{Hom}_k(\alpha_p, \mathbb{G}_m) \arrow[d] & a \arrow[r, mapsto] \arrow[d, mapsto] & (r \mapsto f_a(r)) \arrow[d, mapsto] \\ \alpha_p(k') \arrow[r] & \operatorname{Hom}_{k'}(\alpha_p, \mathbb{G}_m) & \varphi(a) \arrow[r, mapsto] & (r \mapsto f_{\varphi(a)}(r)) \end{tikzcd}$$

commutes. ■

Exercise 2.101. For any $n \geq 1$, we show the groups $\mathbb{Z}/n\mathbb{Z}$ and μ_n are Cartier dual.

Proof. Because it is significantly faster, we will show that these two groups are Cartier dual by appealing to their Hopf algebra structure.

1. We give the Hopf algebra structure on μ_n. Recall

$$\mu_n(R) = \left\{r \in R^\times : r^n = 1\right\},$$

so μ_n has a natural inclusion into $\mathbb{G}_m$. In particular, we see that $\mu_n = \operatorname{Spec} k[t]/\left(t^n - 1\right)$, and the inclusion $\mu_n \hookrightarrow \mathbb{G}_m$ is a closed embedding given on rings by the map $k\left[t, t^{-1}\right] \to k[t]/\left(t^n - 1\right)$ defined by $t \mapsto t$. The coidentity and comultiplication data are just inherited from $\mathbb{G}_m$.

2. We now give the Hopf algebra structure on $\mathbb{Z}/n\mathbb{Z}$. Recall

$$\mathbb{Z}/n\mathbb{Z}(R) = \operatorname{Mor}_{\text{cts}}(\operatorname{Spec} R, \mathbb{Z}/n\mathbb{Z}),$$

which becomes a group via the addition on $\mathbb{Z}/n\mathbb{Z}$. Thus, the functor $\mathbb{Z}/n\mathbb{Z}\colon \mathrm{Alg}_k \to \mathrm{Set}$ is represented by the affine scheme

$$\bigsqcup_{*\in\mathbb{Z}/n\mathbb{Z}} \operatorname{Spec} k = \operatorname{Spec} k^{\mathbb{Z}/n\mathbb{Z}}.$$

We may alternatively write $k^{\mathbb{Z}/n\mathbb{Z}}$ as $k_0 \times \cdots \times k_{n-1}$, where each $k_\bullet$ equals k. The coidentity $\operatorname{Spec} k \to \operatorname{Spec} k^{\mathbb{Z}/n\mathbb{Z}}$ needs to pick out $0 \in \mathbb{Z}/n\mathbb{Z}(R)$ for each R, so it is given by embedding $k \hookrightarrow k_0 \hookrightarrow k^{\mathbb{Z}/n\mathbb{Z}}$. Lastly, the comultiplication m is given on the $k_\bullet$s by gluing together the diagonal embeddings

$$k_i \hookrightarrow \bigoplus_{i_1+i_2=i} k_{i_1} \otimes k_{i_2} \subseteq k^{\mathbb{Z}/n\mathbb{Z}} \otimes k^{\mathbb{Z}/n\mathbb{Z}},$$

where indices are taken $\pmod n$. To check that this works, we choose $r, s \in \mathbb{Z}/n\mathbb{Z}(R)$, which correspond to some maps $r^\sharp, s^\sharp\colon k^{\mathbb{Z}/n\mathbb{Z}} \to R$, and we can see that $m^\sharp \circ (r, s)$ is adding appropriately by checking on the $k_\bullet$s.

3. The Cartier dual of μ_n should be given by the dual Hopf algebra of the Hopf algebra $k[\mu_n]$. Thus, we would like to show that $k[\mu_n]^\vee$ is $k[\mathbb{Z}/n\mathbb{Z}]$. We begin by noting that there is a vector-space isomorphism $\varphi\colon k[\mu_n]^\vee \to k[\mathbb{Z}/n\mathbb{Z}]$ given by sending the dual basis $\{\ell_1, \ldots, \ell_{n-1}\} \subseteq k[\mu_n]^\vee$ of $\left\{1, t, \ldots, t^{n-1}\right\} \subseteq k[\mu_n]$ to the standard basis $\{e_0, \ldots, e_{n-1}\} \subseteq k^{\mathbb{Z}/n\mathbb{Z}}$. It remains to argue that φ preserves the Hopf algebra structures.

   - The identity $1 \in k[\mu_n]$ produces the coidentity $\mathrm{ev}_1\colon \ell \mapsto \ell(1)$ of $k[\mu_n]^\vee$, which by definition of φ goes to the coidentity $e_0 \in k[\mathbb{Z}/n\mathbb{Z}]$.
   - The coidentity $k[\mu_n] \to k$ is given by $t \mapsto 1$, which produces the identity $\ell_1 + \cdots + \ell_{n-1} \in k[\mu_n]^\vee$, which is sent to the identity $e_0 + \cdots + e_{n-1} \in k^{\mathbb{Z}/n\mathbb{Z}}$.
   - The multiplication in $k[\mu_n]$ is given by $t^i \cdot t^j = t^{i+j}$, which defines a comultiplication on $k[\mu_n]^\vee$ which sends ℓ_i to

   $$\sum_{i_1+i_2=i} \ell_{i_1} \otimes \ell_{i_2}.$$

   This is the correct comultiplication on $k[\mathbb{Z}/n\mathbb{Z}]$.

- The comultiplication in $k[\mu_n]$ is given by $t \mapsto t \otimes t$, which produces the multiplication given by extending the conditions
$$\ell_i \otimes \ell_j \mapsto \begin{cases} \ell_i & \text{if } i = j, \\ 0 & \text{else,} \end{cases}$$
k-linearly. This does in fact give the multiplication on $k^{\mathbb{Z}/n\mathbb{Z}}$. ■

2.7.2 Some Dieudonné Modules

In this subsection, we will compute some Dieudonné modules.

Notation 2.102. Fix a ring R of characteristic p. Then we define ${}_mW_n$ as the kernel of the m-fold Frobenius map $F^m \colon W_n \to W_n^{(p^m)}$.

Example 2.103. Because $W_1 = \mathbb{G}_a$, we see that ${}_1W_1 = \alpha_p$.

Remark 2.104. It turns out that the Cartier dual of ${}_mW_n$ is ${}_nW_m$. For example, we showed in Exercise 2.100 that the dual of $\alpha_p = {}_1W_1$ is itself.

Exercise 2.105. Fix a perfect field k of positive characteristic p. The Dieudonné module $M({}_nW_n)$ is isomorphic to the Dieudonné module $D_k/\left(D_kF^n + D_kV^n\right)$.

Proof. We proceed in steps.

1. We compute the order of ${}_nW_n$. In fact, we claim that the order of ${}_mW_n$ is p^{mn}, which we will show by induction. We begin with the base cases ${}_0W_0 = {}_1W_0 = {}_0W_1 = 0$, which has order 0. Then, for any n and m, we note that there are short exact sequences
$$0 \to {}_1W_n \to {}_{m+1}W_n \xrightarrow{F} {}_mW_n \to 0$$
and
$$0 \to {}_mW_n \xrightarrow{V} {}_mW_{n+1} \twoheadrightarrow {}_mW_1 \to 0$$
from which we see that $\#({}_{m+1}W_n) = \#({}_mW_n) \cdot \#({}_1W_n)$ and $\#({}_mW_{n+1}) = \#({}_mW_n) \cdot \#({}_mW_1)$. The claim now follows by induction on m and n.

2. We upper-bound the length of the $W(k)$-module $D_k/(D_kF^n + D_kV^n)$. Note that any element of D_k can be written as a finite polynomial in the form
$$\sum_{m<0} a_mV^{-m} + a_0 + \sum_{m>0} a_mF^m,$$
where $a_m \in W(k)$ for each m. Thus, any element in the quotient $D_k/\left(D_kF^n + D_kV^n\right)$ can be written as a polynomial in the form
$$\sum_{m=1}^{n-1} a_{-m}V^m + a_0 + \sum_{m=1}^{n-1} a_mF^m.$$
In fact, for an element of $D_k/\left(D_kF^n + D_kV^n\right)$ in the above form, we see that $a_{-m}V^m$ has a_m only defined up to $p^{n-m}W(k)$ because $p^{n-m}V^m \in D_kV^n$, so we may view a_m as an element of the quotient $W(k)/p^{n-m}W(k) = W_{n-m}(k)$, which is a $W(k)$-module of length $n-m$. A similar remark holds for the terms a_mF^m, so upon taking the appropriate filtrations, we see that the length of the total $W(k)$-module is bounded above by
$$1 + 2 + \cdots + (n-1) + n + (n-1) + \cdots + 2 + 1 = n^2.$$

3. We exhibit an injection $D_k/\left(D_kF^n+D_kV^n\right)\to M({}_nW_n)$ of Dieudonné modules. In light of the embedding ${}_nW_n\subseteq W_n\subseteq W_\infty$, it is enough to exhibit a map $D_k\to\operatorname{Hom}_k({}_nW_n,W_n)$ and show that its kernel is $D_kF^n+D_kV^n$. Well, there is certainly a map $D_k\to\operatorname{Hom}_k(W,W)$ because D_k is the endomorphism algebra of W; further, we can see that all the endomorphisms in D_k descend to endomorphisms $W_n\to W_n$ and hence restrict to morphisms ${}_nW_n\to W_n$.

   Now, certainly F^n and V^n induce the zero morphism ${}_nW_n\to W_n$ because F^n and V^n vanish on ${}_nW_n$. It remains to show that these two elements generate the kernel. Well, the previous step established a "normal form" for elements in $D_k/\left(D_kF^n+D_kV^n\right)$ as given by polynomials

$$\sum_{m=1}^{n-1}a_{-m}V^m+a_0+\sum_{m=1}^{n-1}a_mF^m,$$

   where $a_{\pm m}\in W_{n-|m|}(k)$ for each m. It is enough to show that each of the elements produces a nonzero homomorphism ${}_nW_n\to W_n$ when at least one of the coefficients is nonzero. This can be checked on $k[t]/\left(t^{p^n}\right)$-points, where we have to take a nilpotent thickening to ensure that ${}_nW_n$ has some points.

4. In light of the bounds on the lengths on $D_k/\left(D_kF^n+D_kV^n\right)$ and $M({}_nW_n)$ as $W(k)$-modules, the injection provided in the previous step completes the proof. ■

Remark 2.106. The previous exercise shows that $M(\alpha_p)=M({}_1W_1)$ is isomorphic to the $W(k)$-module $W_1(k)=k$ where F and V both act by 0.

An understanding of ${}_nW_n$ allows us to prove the following duality result.

Proposition 2.107. Fix a perfect field k of positive characteristic p. For a connected unipotent group G, we have $M(G^\vee)=M(G)^\vee$.

Proof. The point is to check the group ${}_nW_n$ and then reduce to this case. For brevity, we set ${}_nE_n:=M({}_nW_n)$, which we view as the endomorphism algebra of ${}_nW_n$.

1. We check the result for $G={}_nW_n$. Because ${}_nW_n^\vee={}_nW_n$, this amounts to checking that ${}_nE_n^\vee={}_nE_n$. This is more or less a direct computation, for which we will not write out all the details. The proof of Exercise 2.105 describes elements in ${}_nE_n$ as being represented by polynomials

$$\sum_{m=1}^{n-1}a_{-m}V^m+a_0+\sum_{m=1}^{n-1}a_mF^m,$$

   where $a_{\pm m}\in W_{n-|m|}(k)$ for each m. The proof actually shows that this is a unique decomposition for any element in ${}_nE_n$, so we conclude that

$${}_nE_n\cong W_1(k)\oplus W_2(k)\oplus\cdots\oplus W_{n-1}(k)\oplus W_n(k)\oplus W_{n-1}(k)\oplus\cdots\oplus W_2(k)\oplus W_1(k)$$

   as $W(k)$-modules. We now see that ${}_nE_n$ is self-dual as a $W(k)$-module, and the duality flips the action of F and V in such a way to make ${}_nE_n$ also self-dual as a D_k-module.

2. We prove the general case. Let p^n be the order of G, and then we see that any map $G\to W_\infty$ must factor through ${}_nW_n$ because G is killed by p^n. Thus, we may write $M(G)=\operatorname{Hom}_k(G,{}_nW_n)$, and the same argument shows $M(G^\vee)=\operatorname{Hom}_k(G^\vee,{}_nW_n)$.

   We will slowly move $M(G^\vee)$ to $M(G)^\vee$. Because $(\cdot)^\vee$ is an anti-equivalence, we see that

$$M(G^\vee)=\operatorname{Hom}_k(G^\vee,{}_nW_n)=\operatorname{Hom}_k({}_nW_n,G).$$

   Now, we would like $M(G)$ to appear, so we use the fact that M is an anti-equivalence as well to see that

$$\operatorname{Hom}_k({}_nW_n,G)=\operatorname{Hom}_{D_k}(M(G),M({}_nW_n)=\operatorname{Hom}_{D_k}(M(G),{}_nE_n).$$

We would now like to make $M(G)^\vee$ to appear, so we use the fact that $(\cdot)^\vee$ (on Dieudonné modules) is an anti-equivalence on $W(k)$-modules of finite length (which can be checked more or less directly by breaking everything into cyclic modules) to see that

$$\operatorname{Hom}_{D_k}(M(G), {}_nE_n) = \operatorname{Hom}_{D_k}({}_nE_n^\vee, M(G)^\vee) = \operatorname{Hom}_{D_k}({}_nE_n, M(G)^\vee).$$

Now, certainly $\operatorname{Hom}_{D_k}(D_k, M(G)^\vee) = M(G)$, so we are really interested in showing that all morphisms $D_k \to M(G)^\vee$ contain $F^nD_k + V^nD_k$ in the kernel. Well, we already argued at the beginning of this step that F^n and V^n vanish on $M(G)$ because G has order p^n, so the same is true of $M(G)^\vee$. ■

Exercise 2.108. Fix a perfect field k of positive characteristic p. The Dieudonné module $M(\mathbb{Z}/p^n\mathbb{Z})$ is isomorphic to $W_n(k) \subseteq W_\infty(k)$.

Proof. We proceed in steps.

1. For completeness, we check that $W_n(k)$ is a $W(k)$-module of length n. The "filtration" induced by taking kernels in the sequence

$$W_n(k) \twoheadrightarrow W_{n-1}(k) \twoheadrightarrow \cdots \twoheadrightarrow W_2(k) \twoheadrightarrow W_1(k) \twoheadrightarrow 0$$

implies that $W_n(k)$ certainly has length at most n. On the other hand, we note that the quotients

$$\frac{W_{i+1}(k)}{W_i(k)} = \frac{W(k)/p^{i+1}W(k)}{W(k)/p^iW(k)} \simeq \frac{W(k)}{pW(k)}$$

is a simple $W(k)$-module (it is isomorphic to the field k), so the above filtration is maximal.

2. Note that $\mathbb{Z}/p^n\mathbb{Z}$ is étale, so it has order equal to $\#\mathbb{Z}/p^n\mathbb{Z}(k) = p^n$. Thus, $M(\mathbb{Z}/p^n\mathbb{Z})$ should be a $W(k)$-module of length n, so we will be able to conclude that $M(\mathbb{Z}/p^n\mathbb{Z}) = W_n(k)$ as $W(k)$-modules as soon as we produce an injection $W_n(k) \hookrightarrow M(\mathbb{Z}/p^n\mathbb{Z})$. We will actually exhibit an injection $W_n(k) \hookrightarrow \operatorname{Hom}_k(\mathbb{Z}/p^n\mathbb{Z}, W_n)$ of $W(k)$-modules, where W_n has the $W(k)$-action induced by $W_n(k) \hookrightarrow W_\infty(k)$.

   Well, for $\alpha \in W_n(k)$, we define a natural transformation $\operatorname{ev}_\alpha \colon \mathbb{Z}/p^n\mathbb{Z} \to W_n$ on k-points by $\operatorname{ev}_\alpha \colon z \mapsto z\alpha$, which makes sense because $W_n(k)$ is p^n-torsion.[3] This definition on k-points reveals that our map $\operatorname{ev}_\bullet \colon W_n(k) \hookrightarrow \operatorname{Hom}_k(\mathbb{Z}/p^n\mathbb{Z}, W_n)$ is an injective group homomorphism, and it is $W(k)$-invariant because

$$\operatorname{ev}_{\lambda\alpha}(z) = z\lambda\alpha = (\lambda \operatorname{ev}_\alpha)(z).$$

3. The previous step provides an isomorphism $\operatorname{ev}_\bullet \colon W_n(k) \to \operatorname{Hom}_k(\mathbb{Z}/p^n\mathbb{Z}, W_n)$ of $W(k)$-modules. Because F and V commute with the action of $\mathbb{Z}$ (after all, $F, V \colon W(k) \to W(k)$ are ring endomorphisms), we see that $\operatorname{ev}_\bullet$ is also an isomorphism of Dieudonné modules, so we are done. ■

Exercise 2.109. Fix a perfect field k of positive characteristic p. The Dieudonné module $M(\mathbb{Q}_p/\mathbb{Z}_p)$ is isomorphic to $W(k)$.

Proof. Note $\mathbb{Q}_p/\mathbb{Z}_p$ is simply $\varinjlim \mathbb{Z}/p^\bullet\mathbb{Z}$, where the transition maps $\mathbb{Z}/p^n\mathbb{Z} \hookrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$ are given by mutliplication-by-p. Thus,

$$M(\mathbb{Q}_p/\mathbb{Z}_p) = \varprojlim M(\mathbb{Z}/p^\bullet\mathbb{Z}),$$

where the transition maps are given by

$$\begin{tikzcd} W_{n+1}(k) \arrow[r] \arrow[d, "\operatorname{ev}_\bullet"'] & W_n(k) \arrow[d, "\operatorname{ev}_\bullet"] \\ M\left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right) \arrow[r, "p"] & M(\mathbb{Z}/p^n\mathbb{Z}) \end{tikzcd} \qquad \begin{tikzcd} \alpha \arrow[r, mapsto] \arrow[d, mapsto] & \alpha \arrow[d, mapsto] \\ (1 \mapsto \sigma^{-n-1}\alpha) \arrow[r, mapsto] & (1 \mapsto p\sigma^{-n-1}\alpha) \end{tikzcd}$$

[3] The same definition works on R-points whenever $\operatorname{Spec} R$ is connected, so we can produce a definition for arbitrary R by passing to connected components.

where the vertical isomorphisms are given by Exercise 2.108, where we have implicitly adjusted the isomorphisms so that all maps in sight are $W(k)$-invariant. (Note that $\sigma^{-n}\alpha \in W_n(k)$ goes to the same element as $V\sigma^{-n}\alpha \in W_{n+1}(k)$ in $W_\infty(k)$!) Thus, we see that we get the $W(k)$-module $W(k)$ after passing to the inverse limit. The Frobenius element acts by σ everywhere, even after adjusting the $W(k)$-action, so we see that this Dieudonné module is in fact $W(k)$. In particular, we are recalling that we do not have to define a Verschiebung because it is now uniquely given by the Frobenius element and the condition $FV = VF = p$. ■

Exercise 2.110. Fix a perfect field k of positive characteristic p. The Dieudonné module $M(\mu_{p^n})$ is isomorphic to the $W(k)$-module $W_n(k) \subseteq W_\infty(k)$, where $F = p\sigma$ and $V = \sigma^{-1}$.

Proof. By construction of M, we have

$$M(\mu_{p^n}) = M(\mathbb{Z}/p^n\mathbb{Z})^\vee = \operatorname{Hom}_{W(k)}(W_n(k), W_\infty(k)).$$

Note that $W_n(k)$ is V^n-torsion, so the right-hand side is actually $\operatorname{Hom}_{W_n(k)}(W_n(k), W_n(k))$. Now, we note that there is an embedding of $W(k)$-modules $W_n(k) \hookrightarrow \operatorname{Hom}_{W_n(k)}(W_n(k), W_n(k))$ given by sending $\alpha \in W_n(k)$ to the map $\alpha\colon \lambda \mapsto \lambda\alpha$. Because $M(\mu_{p^n})$ needs to be a $W(k)$-module of length n, we conclude that this embedding is an isomorphism.

It remains to describe the action of F and V. For F, we note that the diagram

$$\begin{tikzcd} W_n(k) \arrow[r] \arrow[d, "F"'] & \operatorname{Hom}_{W(k)}(W_n(k), W_n(k)) \arrow[d, "F"] \\ W_n(k) \arrow[r] & \operatorname{Hom}_{W(k)}(W_n(k), W_n(k)) \end{tikzcd} \qquad \begin{tikzcd} \alpha \arrow[r, mapsto] \arrow[d, mapsto] & (1 \mapsto \alpha) \arrow[d, mapsto] \\ \sigma(p\alpha) \arrow[r, mapsto] & (1 \mapsto \sigma(\alpha V1)) \end{tikzcd}$$

commutes, and for V, we note that the diagram

$$\begin{tikzcd} W_n(k) \arrow[r] \arrow[d, "V"'] & \operatorname{Hom}_{W(k)}(W_n(k), W_n(k)) \arrow[d, "V"] \\ W_n(k) \arrow[r] & \operatorname{Hom}_{W(k)}(W_n(k), W_n(k)) \end{tikzcd} \qquad \begin{tikzcd} \alpha \arrow[r, mapsto] \arrow[d, mapsto] & (1 \mapsto \alpha) \arrow[d, mapsto] \\ \sigma^{-1}(\alpha) \arrow[r, mapsto] & \left(1 \mapsto \sigma^{-1}(\alpha F1)\right) \end{tikzcd}$$

commutes. ■

Exercise 2.111. Fix a perfect field k of positive characteristic p. The Dieudonné module $M(\mu_{p^\infty})$ is isomorphic to the $W(k)$-module $W(k)$, where $F = p\sigma$.

Proof. The same argument as in Exercise 2.109 shows that $M(\mu_{p^\infty}) = \varprojlim M(\mu_{p^\bullet})$ is $W(k)$ as a $W(k)$-invariant and that the isomorphism $M(\mu_{p^\infty}) \to W(k)$ is σ-invariant as well. In particular, the action of F on the finite quotients $W_n(k)$ of $M(\mu_{p^\infty})$ are all given by the same endomorphism $p\sigma$, so we conclude that the action of F on $W(k)$ should be given by $p\sigma$ as well. ■

2.8 February 25

Today we will say something about shtukas.

2.8.1 Drinfeld's Shtukas

We would like to do explicit class field theory (and eventually the Langlands correspondence) for function fields $\mathbb{F}_q(C)$, which is the field of functions on a curve C over $\mathbb{F}_q$, and we may assume that the curve is smooth proper because we are only interested in this function field. Shtukas will provide a global analogue for our Drinfeld modules.

Here is our definition of a shtuka.

Definition 2.112 (shtuka)**.** Fix a test scheme S over $\mathbb{F}$. An *S-Shtuka of rank h on C* is a triple $(\mathcal{E}, x, \tau)$ as the following.

- $\mathcal{E}$ is a vector bundle of rank h on $C \times S$.
- x is some finite collection of points $\{x_i\}_{i \in S} \subseteq C(S)$.
- τ is an isomorphism of vector bundles outside the points x between $\mathcal{E}$ and its Frobenius twist $\operatorname{Frob}_S^* \mathcal{E}$.

One typically refers to the points x as "legs."

Here, Frob_S refers to the relative Frobenius.

Example 2.113. Let's explain how to associate a shtuka to a Dieudonné module. Indeed, a Dieudonné module M is a free module over $W(k)$, which can be thought of as a vector bundle over $\operatorname{Spec} \mathbb{Z}_p$ together with a Frobenius-semilinear isomorphism F; further, this F becomes an isomorphism after "removing" the special point and hence defines a shtuka.

We note further that the Dieudonné module had more data: the map F extends over the leg (which is the special fiber), which is not required for a general shtuka.

The above example motivates us to understand what happens to τ at the legs x of a shtuka. Notably, we would like to understand how precisely τ fails to be an isomorphism at the legs.

For this, fix a shtuka $(\mathcal{E}, x, \tau)$. In a neighborhood of some twist x_i, we may choose two isomorphisms $\mathcal{E} \otimes \mathcal{O} \cong \mathcal{O}^h$ and $\operatorname{Frob}_S^* \mathcal{E} \otimes \mathcal{O} \cong \mathcal{O}^h$, where $\mathcal{O} := \mathcal{O}_{x_i}$. Then τ is providing an morphism of $\mathcal{O}^h$ which upgrades to an isomorphism after inverting a uniformizer. The moral of the story is that we have produced an element of $\operatorname{GL}_h(\operatorname{Frac}\mathcal{O})$, but it is only defined in the double coset space

$$\operatorname{GL}_h(\mathcal{O}) \backslash \operatorname{GL}_h(\operatorname{Frac}\mathcal{O}) / \operatorname{GL}_h(\mathcal{O}).$$

One can now use the Cartan decomposition to expand out this double coset space using "dominant" coweights; in short, one sends a dominant weight $(\lambda_1 \geq \cdots \geq \lambda_h)$ of GL_h to the element $(t^{\lambda_1}, \ldots, t^{\lambda_h})$, where $t \in \mathcal{O}$ is a uniformizer.

Example 2.114. The trivial cocharacter corresponds to having the trivial double coset element, which corresponds to the isomorphism τ extending over the legs.

Remark 2.115. The condition $FM \supseteq pM$ for a Dieudonné module is then asking for the double coset element to look like $(p, \ldots, p, 1, \ldots, 1)$, which corresponds to the cocharacter having values in $\{-1, 0, +1\}$, which corresponds to being a miniscule coweight. In general, miniscule conditions should be thought of as avoiding difficult technicalities (locally, where we must pass to diamonds) or being possible at all (globally).

Remark 2.116. Adding in a height h constraint to the Dieudonné module corresponds to controlling

$$\dim_k M/FM = h,$$

which controls the number of 1s we can have in the cocharacter.

2.9 February 27

Today we continue discussing shtukas.

2.9.1 Shtukas in Geometric Class Field Theory

Fix a smooth projective irreducible curve C over a finite field $\mathbb{F}_q$, and we will work with the function field $K := \mathbb{F}_q(C)$. We would like to construct its field extensions; for today, we will be content with abelian extensions (and thus use geometric class field theory), and actually today we will focus on constructing the maximal abelian unramified extension of K. Note that adding an unramified condition is helpful because

$$\operatorname{Gal}(K^{\mathrm{unr}}/K) = \pi_1^{\text{ét}}(C, \overline{\eta}),$$

where $\overline{\eta}\colon K^{\mathrm{sep}} \hookrightarrow C$ is some geometric point.

Remark 2.117. In short, $\pi_1^{\text{ét}}(C, \overline{\eta})$ is the Tannakian group of the category of finite étale covers of C. In a few more words, we recall that there is an equivalence between finite étale covers $C' \to C$ to finite sets with an action by $\pi_1^{\text{ét}}(C, \overline{\eta})$ given by sending $C' \to C$ to the fiber $C'_{\overline{\eta}}$. The reason that $\pi_1^{\text{ét}}(C, \overline{\eta})$ only sees unramified extensions of K is because we are looking for merely étale covers of C.

Thus, we are currently interested in computing the subfield of K^{sep} coming from $\pi_1^{\text{ét}}(C, \overline{\eta})^{\mathrm{ab}}$. By (geometric) class field theory, we are looking at

$$\pi_1^{\text{ét}}(C, \overline{\eta})^{\mathrm{ab}} \cong \widehat{K^\times \backslash \mathbb{A}_K^\times / \widehat{\mathcal{O}}_K^\times},$$

where the $\widehat{\mathcal{O}}_K^\times$ is present because we are on the hunt for an unramified extension. Do note that there is a decomposition

$$0 \to \pi_1^{\text{ét}}(C_{\overline{\mathbb{F}}_q}, \overline{\eta}) \to \pi_1^{\text{ét}}(C, \overline{\eta}) \to \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to 0,$$

so we may as well focus on trying to produce a cover with Galois group $\pi_1^{\text{ét}}(C_{\overline{\mathbb{F}}_q}, \overline{\eta})$. We will the get the remaining $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ extensions by extending the field of coefficients.

We now recall that this right-hand side is the completion of $\operatorname{Pic} C$; note that $\operatorname{Pic} C$ upgrades to a scheme $\operatorname{Pic}_{C/\mathbb{F}_q}$, which is a moduli space of rigidified line bundles. In order for this moduli space to be well-defined, it is helpful to assume that C has an $\mathbb{F}_q$-rational point $\infty \in C(\mathbb{F}_q)$; we will identify η and ∞ in the sequel. Then $\operatorname{Pic}_{C/\mathbb{F}_q}$ on S-points classifies isomorphism classes of pairs $(\mathcal{L}, \alpha)$ of line bundles $\mathcal{L}$ on $C \times S$ together with a trivialization $\alpha\colon \mathcal{L}|_{S\times\infty} \to \mathcal{O}_S$ at ∞.

Remark 2.118. If we wanted to remove the rigidification, we can work without it as $\operatorname{Pic}_{C/\mathbb{F}}/\mathbb{G}_m$, in which case the identification with $K^\times \backslash \mathbb{A}_K^\times / \widehat{\mathcal{O}}_K^\times$ becomes an identification of bundles.

Notably, $\operatorname{Pic}_{C/\mathbb{F}_q}$ lives in the short exact sequence

$$0 \to \operatorname{Jac}_C \to \operatorname{Pic}_{C/\mathbb{F}_q} \overset{\deg}{\to} \mathbb{Z} \to 0,$$

where $\operatorname{Jac}_C = \operatorname{Pic}^\circ_{C/\mathbb{F}_q}$. In fact, this is an avatar of the short exact sequence of the previous paragraph: after taking abelianizations and completions appropriately, class field theory provides an isomorphism

$$\begin{tikzcd}
0 \arrow[r] & \pi_1^{\text{ét}}(C_{\overline{\mathbb{F}}_q}, \overline{\eta}) \arrow[r] \arrow[d] & \pi_1^{\text{ét}}(C, \overline{\eta}) \arrow[r] \arrow[d] & \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q) \arrow[r] & \widehat{\operatorname{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)} \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & 0
\end{tikzcd}$$

of short exact sequences.

2.9.2 The Lang Map

Recall that our end goal is to produce a large abelian étale cover $C' \to C$; in particular, we want a cover with Galois group $\operatorname{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q)$. The idea is to produce a large cover of Jac_C and then pull back along the Abel–Jacobi map $\mathrm{AJ}\colon C \to \operatorname{Jac}_C$ (which is given by $p \mapsto [p] - \deg p[\infty]$ on closed points). In other words, we would like an isogeny $\operatorname{Jac}_{C/\mathbb{F}_q} \to \operatorname{Jac}_{C/\mathbb{F}_q}$ with kernel given by the $\mathbb{F}_q$-rational points. This is the Lang map.

Definition 2.119 (Lang map)**.** Fix a group scheme G over a finite field $\mathbb{F}_q$. Let $\sigma\colon G \to G$ denote the absolute Frobenius morphism. (Namely, σ is the identity on topological spaces, and σ is the q-power map on structure sheaves.) Then the *Lang map* is the map $L\colon G \to G$ given by

$$L(g) := \sigma(g)g^{-1}.$$

Theorem 2.120 (Lang)**.** Fix a connected group scheme G of finite type over a finite field $\mathbb{F}_q$. Then the Lang map $L\colon G \to G$ is surjective.

Remark 2.121. We are essentially trying to show that $\mathrm{H}^1(W_{\overline{\mathbb{F}}_q}, G(\overline{\mathbb{F}}_q))$ is trivial. Indeed, this implies that each 1-cocycle $c\colon W_{\overline{\mathbb{F}}_q} \to G(\overline{\mathbb{F}}_q)$ takes the form $\mathrm{Frob}_q \mapsto \sigma(g)g^{-1}$ for some g. In particular, we can define a 1-cocycle as sending Frob_q to some general point of $G(\overline{\mathbb{F}}_q)$ (and extending to be a 1-cocycle), and then it must be a coboundary. We remark that this also implies that the continuous $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), G(\overline{\mathbb{F}}_q))$ is trivial.

Remark 2.122. Here is another example application, just for fun: if $X = H\backslash G$ is some homogeneous space, then $X(\mathbb{F}_q) = H(\mathbb{F}_q)\backslash G(\mathbb{F}_q)$. This follows by taking Galois cohomology of the exact sequence

$$1 \to H(\overline{\mathbb{F}}_q) \to G(\overline{\mathbb{F}}_q) \to X(\overline{\mathbb{F}}_q) \to 1.$$

Anyway let's prove Theorem 2.120.

Proof of Theorem 2.120. This is a statement about $\overline{\mathbb{F}}_q$-points, so we may adjust the scheme structure so that G is geometrically reduced. For some $x \in G(\overline{\mathbb{F}}_q)$, and we consider the coboundary action of G on G given by $g \cdot x := \sigma(g)xg^{-1}$. We claim that each x lies in an open orbit, which will complete the proof because there is only one open orbit because G is connected. (Namely, we find that all points live in the same orbit of the coboundary action, so in particular, they are in the same orbit as the identity).

It remains to show the claim that any given $x \in G(\overline{\mathbb{F}}_q)$ lies in an open orbit, for which it is enough to check that the map $G_{\overline{\mathbb{F}}_q} \to G_{\overline{\mathbb{F}}_q}$ given by $g \mapsto \sigma(g)xg^{-1}$ is surjective on tangent spaces, where σ is now the relative Frobenius (it is the base-change of σ to $\overline{\mathbb{F}}_q$). We may check this at the identity of the first $G_{\overline{\mathbb{F}}_q}$. For this computation, we consider the more general map $G \times G \to G$ given by $(g_1, g_2) \mapsto \sigma(g_1)xg_2^{-1}$; at the identity, this map is zero on the g_1 coordinate (it is the Frobenius) and an isomorphism on the g_2 coordinate (because inversion is negation). Thus, the composite

$$G \xrightarrow{\Delta} G \times G \to G,$$

which we see is given by $g \mapsto \sigma(g)xg^{-1}$, is surjective on tangent spaces at the identity. ■

Corollary 2.123. Fix an abelian variety A over a finite field $\mathbb{F}_q$. Then $L\colon A \to A$ is an étale isogeny.

Proof. We showed that L is surjective, so it is an isogeny. We checked that it is smooth in the previous proof, so the result follows. ■

Remark 2.124. For example, this implies that $\ker L$ is smooth over $\mathbb{F}_q$. Note that $\ker L \subseteq A$ has geometric points $\ker L(\overline{\mathbb{F}}_q) = A(\mathbb{F}_q)$. In fact, $\ker L$ is a constant group scheme.

2.9.3 The Shtuka Covering

We may now define the étale cover $C' \to C$ to be the base-change sitting in the following diagram.

$$\begin{tikzcd} C' \arrow[r, "\mathrm{AJ}"] \arrow[d] & \mathrm{Jac}_{C/\mathbb{F}_q} \arrow[d, "L"] \\ C \arrow[r, "\mathrm{AJ}"] & \mathrm{Jac}_{C/\mathbb{F}_q} \end{tikzcd} \tag{2.1}$$

Let's compute the fiber over $\overline{\infty}$ on the left: this corresponds to the identity of Jac_C, and so the fiber over this identity is supposed to be $\ker L$, which we know to be $\mathrm{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q)$. Now, deck transformations are able to act on this fiber, so we produce an action map

$$\pi_1^{\text{ét}}(C, \overline{\eta}) \to \mathrm{Aut}(\mathrm{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q)).$$

By fixing the base-point $0 \in \mathrm{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q)$, we produce a function α from $\pi_1^{\text{ét}}(C, \overline{\eta})$ to $\mathrm{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q)$, which we will check to be a homomorphism later. Our main claim is that

$$\alpha(\mathrm{Frob}_c) \stackrel{?}{=} \mathrm{AJ}(c)$$

for each closed point $c \in C$. This allows us to explicate some class field theory.

Theorem 2.125. Fix everything as above. Consider the Weil group $W(C, \overline{\eta})$. Then we define the map $\varphi\colon W(C, \overline{\eta}) \to \mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)$ by

$$\varphi(\gamma) := \alpha(\gamma) + \deg(\gamma)[\infty].$$

Then φ is the inverse of the reciprocity map.

Proof. The map is certainly continuous, so we may check it on a dense subset of $W(C, \overline{\eta})$. Thus, we may check it on Frobenius elements Frob_c for closed points $c \in C$, where it follows from the main claim as soon as we recall that $\mathrm{AJ}(c) = [c] - \deg(c)[\infty]$. ■

Let's now prove the main claim. We need to unravel what Frob_c means: it is the image of the Frobenius through

$$\pi_1^{\text{ét}}(c, \overline{c}) \hookrightarrow \pi_1^{\text{ét}}(C, \overline{c}).$$

In particular, to live in this subgroup, Frob_c is required to fix the geometric point $\overline{c} \hookrightarrow C$, so it will fix the scheme-theoretic points. Furthermore, to be the Frobenius, it needs to act as $q^{\deg(c)}$-Frobenius on the residue field of c. We would like to know that $\mathrm{AJ}(c)$ (which acts by multiplication on the fiber of $C' \to C$) agrees with this action of Frob_c.

Remark 2.126. We've gone pretty far from shtukas, so now let's have them return: it turns out that C' is the moduli space Sht^0 of shtukas for the group GL_1 with the legs in $C \times \{\infty\}$ and coweights $(1, -1)$. This can be seen by tracking around the diagram (2.1). For example, for each closed point $c \in C$ of degree 1, we produce the line bundle $\mathcal{O}([c] - [\infty])$, and its fiber through L consists of the rigidified line bundles $\mathcal{L}$ such that $\sigma(\mathcal{L}) \otimes \mathcal{L}^{-1} \cong \mathcal{O}([c] - [\infty])$. In other words, we are admitting an isomorphism $\sigma(\mathcal{L}) \cong \mathcal{L}([c] - [\infty])$ (chosen by the rigidifications!) and hence defines a shtuka with the legs c and ∞. The coweights are read off of the divisor $[c] - [\infty]$.

We are now ready to prove the claim. We want to know that the deck transformation Frob_c is the same as the action of $\mathrm{AJ}(c)$ on $\mathrm{Jac}_{C/\mathbb{F}_q}(\mathbb{F}_q)$. Indeed, note $\mathrm{AJ}(c)$ acts by $\mathcal{L} \mapsto \mathcal{L}([c] - \deg(c)[\infty])$. Thus, on the fiber over c, we find

$$\mathcal{L}([c] - \deg(c)[\infty]) \cong \sigma^{\deg(c)}(\mathcal{L}),$$

which of course agrees with the action of Frob_c on the line bundle! (Namely, it is fixing the fiber, and it is acting by Frobenius on residue fields.)

2.10 March 4

Today we continue with our discussion of geometric class field theory.

2.10.1 Recovering Class Field Theory

The following content is extremely sketchy. We would like to show that the map

$$\alpha\colon \pi_1(C,\overline{\eta})^{\mathrm{ab}} \to \widehat{\mathrm{Pic}_C(\mathbb{F}_q)}$$

is an isomorphism, recovering class field theory. We already know that it is surjective because of our construction: it is not hard to see that we surject onto $\mathrm{Pic}_C(\mathbb{F}_q)$ by our construction, so we successfully hit a dense subset by the continuous map α.

For the injectivity, it is enough to check this on the level of (enough) characters. Fix $\Lambda := \mathbb{Z}_\ell$ for $\ell \neq p$ (or more generally, any ring of integers in any finite extension of $\mathbb{Q}_\ell$), and we will show that the induced map

$$\mathrm{Hom}(\widehat{\mathrm{Pic}_C(\mathbb{F}_q)}, \Lambda^\times) \to \mathrm{Hom}(\pi_1(C,\overline{\eta}), \Lambda^\times)$$

is surjective. This will achieve the required injectivity after looping over all ℓ. Now, this right-hand side is given by a one-dimensional ℓ-adic local system, so we would like a geometric avatar for the left-hand side.

Definition 2.127 (character local system)**.** Fix a smooth commutative algebraic group G over $\overline{\mathbb{F}}_q$. A *character local system* on G is a pair $(\mathcal{L},\psi)$ where $\mathcal{L}$ is a one-dimensional local system, and

$$\psi\colon m^*\mathcal{L} \to \mathrm{pr}_1^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}$$

is an isomorphism satisfying a cocycle condition expected by an associativity law. We let $\mathrm{CharLoc}(G)$ denote this group of character local systems.

Example 2.128. Given a character $\chi\colon G(\overline{\mathbb{F}}_q) \to \Lambda^\times$, one can construct the local system $\mathcal{L}_\chi$ on G as being trivialized by the Lang map $L\colon G \to G$ and twisted by ψ upstairs; in particular, the multiplication arises from having a multiplication upon restriction along L. Conversely, given a character local system $(\mathcal{L},\psi)$, one can take trace of the Frobenius in order to define a map

$$\mathrm{CharLoc}(G) \to \mathrm{Hom}(\widehat{G(\overline{\mathbb{F}}_q)}, \Lambda^\times).$$

Remark 2.129. It turns out that local systems, constructed in the above manner, are able to produce all characters of a given finite group which looks like $G(\mathbb{F}_q)$, if we allow more Frobenius traces and more local systems.

The moral of the story is that we are looking for an isomorphism

$$\mathrm{AJ}^*\colon \mathrm{CharLoc}(\mathrm{Pic}_C) \to \mathrm{Loc}^1_C(C)$$

given by class field theory. Namely, we would like to find an inverse for this map.

Remark 2.130. For motivation, let's recall why Pic_C is a variety. It is enough to check that Pic^d_C is a scheme for any d. For this, we note that Pic_C has a covering by the sheaf of pairs $(\mathcal{L},s)$ of a line bundle together with a nonzero section s; by reading off the zeroes of s, we see that the sheaf of such pairs are simply given by effective divisors, which of course is $\bigsqcup_{d\geq 0} C^{(d)}$. Now, for large enough degree d (compared to the genus), Riemann–Roch explains how many sections a line bundle has: on degree d, we get a fiber bundle $C^{(d)} \to \mathrm{Pic}^d$ with fibers $\mathbb{P}^{d-g+1}$. Figuring out how to take a quotient completes the construction.

The remark explains that we may understand local systems on Pic_C as basically local systems on $C^{(d)}$ (because the fibers of the covering are simply connected for $d \gg 0$!), so we can imagine taking a local system $\mathcal{L}$ on C and producing a local system $\mathcal{L}^{(d)}$ on $C^{(d)}$ by some kind of symmetric power construction.

Remark 2.131. Let's record one step which checks that the produced sheaf $r(\mathcal{L})$ on Pic^d is actually a character local system. We will check what happens under the "Hecke operators" $T_c \colon \operatorname{Pic} \to \operatorname{Pic}$ given by twisting by a closed point $c \in C$: for $d \gg 0$, it turns out that

$$T_c^* r(\mathcal{L})|_{\operatorname{Pic}_C^{d+1}} = r(\mathcal{L})|_{\operatorname{Pic}_C^d} \otimes \mathcal{L}_c,$$

so we see that $r(\mathcal{L})$ is a "Hecke eigensheaf." One can then use this property to extend $r(\mathcal{L})$ uniquely to all of Pic_C and then check that it is the inverse of AJ^*.

Remark 2.132. More generally, it is true that shtukas produces a map from "automorphic representations" (which look like representations of $\operatorname{Pic}_C(\mathbb{F}_q)$) to "Galois representations" (which look like representations of $\pi_1^{\text{ét}}(C, \overline{\eta})$).

Part II

Special Values

THEME 3

WALPSBURGER'S THEOREM

3.1 March 4

Let's now say a few words about what the second part of the course is going to be about.

3.1.1 Waldspurger's Theorem

We are interested in the theorems of Waldspurger and Gross–Zagier, which are related to the embedding $T \to G$ of the torus $\operatorname{Res}_{K/\mathbb{Q}} \mathbb{G}_{m,K}$ (where $K/\mathbb{Q}$ is imaginary quadratic) and $G = \mathrm{GL}_{2,\mathbb{Q}}$. Now, for any group H over $\mathbb{Q}$, we have an adelic quotient $[H] \coloneqq H(\mathbb{Q})\backslash H(\mathbb{A}_{\mathbb{Q}})$. Thus, so the embedding $T \hookrightarrow G$ produces a map $[T] \hookrightarrow [G]$, which roughly corresponds to the choice of an elliptic curve with CM by K.

Now, let δ_T be the pushforward of the Haar measure on $[T]$ to a distribution on $[T \times G]$; after fixing a level structure, this is basically a finite sum over the CM points. Then Waldspurger's theorem explains how to compute $\langle \delta_T, \delta_T \rangle$. Of course, it is a little tricky to make sense of such an inner product, but we will side-step this issue by only looking at some components.

Theorem 3.1 (Waldspurger, rough version)**.** For any irreducible automorphic representation $\chi \boxtimes \pi$ of $T \times G$, the corresponding isotypic component of $\langle \delta_T, \delta_T \rangle$ is proportional to the central value $L(\chi \times \pi, 1/2)$.

Namely, to compute this isotypic component, one may instead compute

$$\sum_{\varphi} \langle \varphi, \delta_T \rangle \langle \delta_T, \chi \otimes \varphi \rangle,$$

where φ varies over some orthnormal basis of π. But now we see that this sum is

$$\sum_{\varphi} \left| \int_{[T]} \varphi(t)\chi(t)\, dt \right|^2,$$

and this is what we will choose to compute.

3.2 March 6

Today we continue with the overview of our main theorems.

3.2.1 The Gross–Zagier Formula

For the Gross–Zagier formula, we consider the map $\mathrm{Sh}_T \to \mathrm{Sh}_T \times \overline{\mathrm{Sh}}_G$. Thus, we are producing some divisor on a variety, and the Gross–Zagier formula explains how to compute its height.

Theorem 3.2 (Gross–Zagier, rough version)**.** For any irreducible automorphic representation $\chi \boxtimes \pi$ of $T \times G$ (where π_∞ is a weight-2 modular form), the corresponding isotypic component of $\langle \mathrm{Sh}_T, \mathrm{Sh}_T \rangle_{\mathrm{NT}}$ (where NT denotes the Néron–Tate height) is proportional to the central value $L'(\chi \times \pi, 1/2)$.

Once again, let's be more precise about what this inner product means. Choose a weight-2 cusp form $f \in S_2(\Gamma)$ for some congruence subgroup Γ. Then $\overline{\mathrm{Sh}}_G = X(\Gamma)$, which surjects onto the abelian variety A_f attached to f. The composite

$$\mathrm{Sh}_T \subseteq \mathrm{Sh}_G \subseteq \overline{\mathrm{Sh}}_G \twoheadrightarrow A_f$$

produces the so-called Heegner points $t \mapsto [t]$ of A_f. Then we want to compute the height of the divisor $\sum_{t \in \mathrm{Sh}_T(\Gamma)} \chi(t)[t]$.

Remark 3.3. As we have written the two theorems, they appear to be quite similar, and indeed, all known proofs of the Gross–Zagier formula are inspired by corresponding proofs of Waldspurger's theorem. However, in the current setting, there is no way to prove both at the same time.

Remark 3.4. In the function field setting, it is possible to give a uniform proof. Roughly speaking, Waldspurger's theorem is about shtukas with zero legs, and the Gross–Zagier formula is about shtukas with one leg.

Remark 3.5. The classical application of the Gross–Zagier formula is to argue that the Heegner points are producing non-torsion points because their Néron–Tate height is nonzero. This has an application to the Birch and Swinnerton-Dyer conjecture. We note that the difference between $L'(\chi \times \pi, 1/2)$ and $L'(E, 1)$ is merely one of automorphic vs. motivic normalization of L-functions.

3.2.2 Automorphic L-Functions

We will need to define the L-function $L(\chi \times \pi, s)$. Let's begin with the general formalism of automorphic L-functions.

Throughout this section, fix a reductive group G over a global field F. Recall that one can realize an automorphic form π (which is some kind of representation of $G(\mathbb{A}_F)$) as a subrepresentation $\pi \subseteq C^\infty([G])$. Further, π factors as $\pi = \bigotimes_v' \pi_v$, where π_v is unramified for all but finitely many v (taken to be nonarchimedean), meaning that $\pi_v^{K_v} \neq 0$ (where $K_v := G(\mathcal{O}_v)$ comes from a choice of integral model) and hence produces a nonzero module of the local Hecke algebra $\mathcal{H}(G_v, K_v)$.

Now, by the Satake isomorphism, this Hecke algebra can be realized as $\mathbb{C}[X_v]$ where X_v is some variety; thus, irreducible $\mathcal{H}(G_v, K_v)$-modules can be realized as $\mathbb{C}$-points in

$$\mathrm{Hom}(\mathcal{H}, \mathbb{C}) = X_v(\mathbb{C}).$$

It is worth having a more explicit description of X_v: recall that there is a dual group $\check{G}$ and then a description of the L-group as ${}^L G = \check{G} \rtimes \mathrm{Gal}(\overline{F}/F)$, and then for a nonarchimedean place v, we have

$$X_v := \check{G}\mathrm{Fr}_v / \check{G} = \operatorname{Spec} \mathbb{C}[\check{G}\mathrm{Fr}_v]^{\check{G}},$$

where the quotient is taken in the sense of geometric invariant theory. (Here, $\check{G}$ acts on $\check{G}\mathrm{Fr}_v$ by conjugation.) Morally speaking, $X_v(\mathbb{C})$ should be thought of as semisimple Frobenius-twisted conjugacy classes in $\check{G}$. In particular, $c_v \in X_v(\mathbb{C})$ produces a homomorphism $W_{\mathbb{Q}_p} \to {}^L G$ taking the Frobenius to $c_v \mathrm{Fr}_v$. We may call $c_v \in X_v(\mathbb{C})$ a "Satake parameter" and the map $W_{\mathbb{Q}_p} \to {}^L G$ a "Langlands parameter."

In total, we see that π_v (when unramified) admits a Langlands parameter $c_v(\pi_v) \colon W_{\mathbb{Q}_p} \to {}^L G$, which is trivial on inertia.

Remark 3.6. The local Langlands conjecture asks one to attach a Langlands parameter $W_v \to {}^L G$ for any irreducible representation π_v of $G(F_v)$, not necessarily unramified. Of course, the previous sentence does not technically have content because we would like the association to satisfy some coherence conditions pinning it down.

Definition 3.7. Fix a reductive group G over a number field F. Assume the local Langlands conjecture for G_v for all places v. Choose some algebraic representation $r\colon {}^L G \to \operatorname{GL}(V)$. For some irreducible representation π of $G(\mathbb{A}_F)$, write $\pi = \bigotimes_v \pi_v$, and we define

$$L(\pi, r, s) := \prod_v L(\pi_v, r, s),$$

where $L(\pi_v, r, s)$ is defined as the local Artin L-function:

$$L(\pi_v, r, s) := L(r \circ \varphi_v, s) := \frac{1}{\det\left(1 - q_v^{-s} r\varphi_v(\operatorname{Fr}_v); V^{r\varphi_v(I_v)}\right)},$$

where φ_v is the local Langlands parameter.

Remark 3.8. Consider $G = \operatorname{GL}_{2,F}$ so that $\check{G} = \operatorname{GL}_{2,\mathbb{C}}$, and we take $r\colon \operatorname{GL}_2 \to \operatorname{GL}_{k+1}$ to be the kth symmetric power. Then a Satake parameter of π_v viewed as a conjugacy class looks like $\operatorname{diag}(\alpha_v, \beta_v)$ for some α_v and β_v. Thus, we can compute

$$L(\pi_v, r, s) = \prod_{i=0}^{k} \frac{1}{1 - q_v^{-s} \alpha_v^i \beta_v^{k-i}}.$$

It is worth recording the following conjecture, which explains the expected analytic properties.

Conjecture 3.9 (Langlands)**.** Suppose π is an automorphic irreducible representation of $G(\mathbb{A}_F)$. Then $L(\pi, r, s)$ admits a meromorphic continuation to $\mathbb{C}$ (with prescribed poles) and a functional equation of the form

$$L(\pi, r, s) = \varepsilon(\pi, r, s) L(\pi^\vee, r, 1-s),$$

where $\varepsilon(\pi, r, s)$ is $\varepsilon(\pi, r, 1/2)$ times an exponential in $\frac{1}{2} - s$.

Remark 3.10. Technically speaking, this is a "second-order" conjecture because it already depends on the local Langlands conjecture!

Remark 3.11. The Langlands functoriality conjecture predicts that the homomorphism $r\colon {}^L G \to \operatorname{GL}(V)$ yields a map ℓ_r from automorphic representations of G to automorphic representations of $\operatorname{GL}_{\dim V}$ which is compatible with L-functions:

$$L(\pi, r, s) = L(\ell_r(\pi), \operatorname{Std}, s).$$

Thus, we could realize $L(\pi, r, s)$ as an L-function for the group GL_n and the standard representation, where the conjecture is already known by Godement–Jacquet (extending Riemann–Iwasawa–Tate for GL_1).

Notation 3.12. There is some standard simplified notation for our L-functions. If G is classical, we may write $L(\pi, s)$ for $L(\pi, \mathrm{Std}, s)$. If $G = G_1 \times G_2$ is a product of two classical groups, we may write $L(\pi_1 \times \pi_2, s)$ for $L(\pi_1 \boxtimes \pi_2, \otimes, s)$, where $\otimes$ is the tensor product representation on the dual side.

Remark 3.13. Conjecture 3.9 is known in the listed cases when the classical group is GL_n.

For our applications, our map $r\colon {}^LG \to \mathrm{GL}(V)$ will factor through $\mathrm{Sp}(V)$. In this case, it turns out that

$$\varepsilon\left(\pi, r, \frac{1}{2}\right) = \pm 1.$$

Roughly speaking, one knows (in general) that we can expand $\varepsilon(\pi, r, s) = \prod_v \varepsilon(\pi_v, r, s)$, and it turns out that these local root numbers $\varepsilon(\pi_v, r, 1/2)$ are also ± 1. For example, $\varepsilon(\pi_v, r, 1/2)$ in the Iwasawa–Tate case is realized as some normalized Gauss sum.

We are now ready to return to our situation with $T = \operatorname{Res}_{K/\mathbb{Q}} \mathbb{G}_{m,K}$ and $G = \mathrm{GL}_2$.

- Note $\check{T} = \mathbb{G}_{m,\mathbb{C}}^2$ and so ${}^LT = \mathbb{G}_m^2 \rtimes \mathrm{Gal}(K/\mathbb{Q})$, where the Galois action acts by permuting the two factors (seen by tracking through the Galois action on $\check{T}$). In particular, ${}^LT$ is isomorphic to GO_2.
- For $G = \mathrm{GL}_2$, we see ${}^LG = \mathrm{GL}_{n,\mathbb{C}} \times \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We are interested in automorphic representations $\chi \boxtimes \pi$ of $T \times G$, and we will further be interested in those which admit T^Δ functionals, where T^Δ is the diagonal copy of T embedded in $T \times G$. For example, we want the restriction of $\chi \boxtimes \pi$ to $\mathbb{G}_m \subseteq T \times G$ to be trivial, which amounts to asking for $\chi\omega_\pi = 1$, where ω_π is the central character of π. Thus, we may as well think about $\chi \boxtimes \pi$ as being an automorphic representation of $\widetilde{G} \coloneqq (T \times G)/\mathbb{G}_m$, where $\mathbb{G}_m$ is embedded diagonally. Then one can compute

$${}^L\widetilde{G} = \mathrm{GO}_2 \times_{\mathbb{G}_m} \mathrm{GL}_2$$

In particular, the tensor product representation r embeds ${}^L\widetilde{G}$ into Sp_4. Thus, we may define

$$L(\chi \times \pi, s) \coloneqq L(\chi \boxtimes \pi, r, s),$$

which by construction is symplectic, and we know that its ε-factor should be ± 1 as the central point.

3.3 March 13

We continue. As usual, K is an imaginary quadratic field.

3.3.1 A Little on Automorphic Representations

Let's recall a working definition of automorphic representation.

Definition 3.14 (automorphic representation)**.** Fix a reductive group G over a number field F. Then an *automorphic representation* of G is an irreducible representation π of $G(\mathbb{A}_F)$ equipped with an embedding $\pi \hookrightarrow C^\infty([G])$.

Remark 3.15. This definition is not technically correct. We should allow subquotients of finite-length modules, and we should only work with $(\mathfrak{g}, K)$-modules at the real infinite places.

Remark 3.16. It turns out that π admits a restricted tensor product decomposition $\pi \cong \bigoplus_v' \pi_v$. Being a restricted tensor product means that π_v is unramified for almost all v (namely, $\pi_v^{G(\mathcal{O}_v)} \neq 0$), and then we require that an element of $\bigoplus_v' \pi_v$ takes the value of the $G(\mathcal{O}_v)$-fixed vector for all but finitely many v.

Example 3.17. Work with $G = \mathrm{GL}_{2,\mathbb{Q}}$. Choose $f \in S_2(\Gamma_0(N))$ to be a Hecke eigenform for T_p for p away from N. Some argument involving double quotients explains how f produces some $F \in C^\infty([G])$, which then spans some automorphic representation π of $G(\mathbb{A}_\mathbb{Q})$. It turns out that π_∞ then lives in the short exact sequence

$$0 \to \pi_\infty \to \mathrm{Meas}^\infty\left(\mathbb{P}^1(\mathbb{R})\right) \to \mathbb{C} \to 0.$$

Remark 3.18. Let's give a more explicit description of the previous example. Suppose further that f has rational coefficients so that the quotient $J_0(N) \to A_f$ corresponding to f is an elliptic curve. We also suppose that f (and thus A_f) does not have complex multiplication. Then it turns out that the finite part $\pi_f \cong \bigoplus_{p<\infty}' \pi_p$ is given by

$$\pi_f = \varinjlim \mathrm{Hom}(J_0(N), A_f)_\mathbb{Q}.$$

Notably, this becomes a representation of $G(\mathbb{A}_{\mathbb{Q},f})$ by the action locally. One checks this by understanding how the $G(\mathbb{A}_{\mathbb{Q},f})$ action on A_f corresponds to the Hecke action on f.

3.3.2 Fixing our Theorems

We now begin fixing our theorem. We will focus on cases where $\chi \boxtimes \pi$ has trivial central character, which means that it descends to an automorphic representation of $(T \times G)/\mathbb{G}_m$, where this $\mathbb{G}_m$ is embedded diagonally. Then we see that we should also mod out our embedding $T \hookrightarrow (T \times G)$ by $\mathbb{G}_m$ which becomes the embedding

$$T/\mathbb{G}_m \hookrightarrow (T \times G)/\mathbb{G}_m.$$

Now, $T/\mathbb{G}_m$ is simply U_1, so our pairings should really be taken over U_1. Thus, in Waldspurger's formula, we will want to integrate over U_1 instead of T.

For the Gross–Zagier formula, we choose a Hecke eigenform $f \in S_2(\Gamma)$ for some congruence subgroup Γ and with rational coefficients (as in Remark 3.18); let $F \in \pi_f$ be the distinguished element of the cuspidal automorphic representation. Further, we choose a CM point P given by an embedding $\mathrm{Sh}_T \to \mathrm{Sh}_T \times \mathrm{Sh}_G$. Now, it turns out that there is a distinguished Hodge class of line bundles in Sh_G, which provides a good choice of Abel–Jacobi map

$$\mathrm{AJ}\colon \mathrm{Sh}_G \to J,$$

where J is technically an inverse limit $\varprojlim J_0(N)$. In particular, the image of $P \in X_0(N)$ is defined over K^{ab}, so its image in the Jacobian is as well.

We now use χ to define a divisor. Viewing F as an element of $\mathrm{Hom}(J, E_f)_\mathbb{Q}$, we see that we can write down $F(P)$ as morally being an element of $E_f(K^{\mathrm{ab}})_\mathbb{Q}$. Then we may integrate

$$P_\chi(F) := \int_{\mathrm{Gal}(K^{\mathrm{ab}}/K)} \chi(\tau) F(\tau(P))\, d\tau.$$

Because χ is an idele class character $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \overline{\mathbb{Q}}\times$ (where we have used class field theory), it descends to a finite quotient of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Similarly, P is defined over some finite extension of K. Thus, this integral really descends to a finite sum. In total, we are producing an element in $E_f(K^{\mathrm{ab}}) \otimes_\mathbb{Z} \overline{\mathbb{Q}}$.

Remark 3.19. The theory of complex multiplication explains that the Galois action on P should agree with what we find with the reciprocity map. In particular, viewing P as an element $z_0 \in \mathcal{H}$ of the upper-half plane, then $\tau(P)$ is simply

$$\left[z_0, \mathrm{Art}_K^{-1}(\tau)\right] \in \mathcal{H} \times .$$

Now, the Gross–Zagier formula is about the inner Néron–Tate height of $\langle P_\chi(F), P_{\chi^{-1}}(\widetilde{F})\rangle_{\mathrm{NT}}$, where $\widetilde{F}$ is the corresponding element of the contragredient $\widetilde{\pi}_f$.

> **Remark 3.20.** There is something bizarre about the current formulation: we would like the Néron–Tate height to be proportional to $L'(1/2, \pi \times \chi)$, but the divisor we constructed depends on a choice of modular form $f \in \pi$!

Let's try to remedy the above remark. Note that there is a canonical pairing

$$\pi_f \otimes \widetilde{\pi}_f \to \mathbb{C},$$

which is $\left(T(\mathbb{A}_f), \chi^{-1}\right) \times (T(\mathbb{A}_f), \chi)$-equivariant. Thus, we improve our formulation to ask for

$$\left\langle P_\chi(F), P_{\chi^{-1}}(\widetilde{F})\right\rangle_{\mathrm{NT}} = cL'\left(\frac{1}{2}, \pi_f \times \chi\right)\prod_p \alpha_p\left(F_p \otimes \widetilde{F}_p\right),$$

where c is some global explicit constant, and $\alpha_p \colon \pi_p \otimes \widetilde{\pi}_p \to \mathbb{C}$ is the canonical pairing; explicitly,

$$\alpha_p\left(F_p \otimes \widetilde{F}_p\right) \approx c_p \int_{T(\mathbb{Q}_p)/\mathbb{Q}_p^\times} \chi_p(t)\left\langle \pi_p(t)F, \widetilde{F}\right\rangle\, dt.$$

The cs and c_ps are some explicit constants; for example, the c_ps should be chosen so that the product is 1 for all but finitely many terms. Namely, we should take the c_ps to come from some Tamagawa measures.

This motivates us to go back and adjust the statement of the Waldspurger formula as follows: we have

$$\sum_\varphi \int_{[T/\mathbb{G}_m]} \chi(t)\varphi(t)\, dt \cdot \int_{[T/\mathbb{G}_m]} \chi^{-1}(t)\widetilde{\varphi}(t)\, dt = cL\left(\frac{1}{2}, \pi \times \chi\right)\prod_p \alpha_p(\varphi_p \otimes \widetilde{\varphi}_p),$$

where the α_ps are some similarly scaling factors. For example, one needs to choose constants c_p so that $\alpha_p(\varphi_p \otimes \widetilde{\varphi}_p)$

> **Remark 3.21.** We now see that one can view both of our theorems as providing Euler product decompositions of our "geometrically motivated" objects.

There is a representation-theoretic obstruction to the statement of our current theorems. There is a theorem of Saito–Tunnell which states that

$$\operatorname{Hom}_{T(\mathbb{Q}_v)}(\chi_v \boxtimes \pi_v, \mathbb{C})$$

vanishes unless $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$, where $\eta_v = \varepsilon(1/2, \pi_v \times \chi_v)$ is the local root number. (In fact, this result holds for more general quadratic extensions, but we will not need this. This is an instance of a more general phenomenon called the Gan–Gross–Prasad conjectures.) Do note that $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ reads as $1 \cdot 1 = 1$ for all but finitely many v.

The problem here is that our left-hand side of both theorems will vanish unless $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ holds for every prime p! To fix this, Gross and Zagier imposed a "Heegner condition" that f should be a new form for $\Gamma_0(N)$ such that each $p \mid N$ has $p^2 \nmid N$ and p is split or ramified in K, which implies that $\eta_p(-1) = \varepsilon_p(-1)$. (If $K = \mathbb{Q}(\sqrt{-D})$, then this Heegner condition is asking for $D \pmod{4N}$ to be a square.)

Let's now relate this to ε-factors. Recall that we have a global functional equation of the form

$$L(s, \pi \times \chi) = \varepsilon(s, \pi \times \chi)L(1-s, \pi \times \chi),$$

and we see that the sign $\varepsilon := \varepsilon(1/2, \pi \times \chi)$ admits a product factorization as $\prod_v \varepsilon_p(1/2, \pi \times \chi)$. So if we are given $\prod_v \chi_v(-1)\eta_v(-1) = 1$ by the Heegner condition, we find the following.

Let's now fully correct the Waldspurger formula. If $\varepsilon = -1$, then Waldspurger's formula has no content: $L(1/2, \pi \times \chi)$ vanishes, and the local representation-theoretic obstruction tells us that $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ failing to hold at some p implies that the Euler product also vanishes. On the other hand, $\varepsilon = 1$ may find some content in $L(1/2, \pi \times \chi)$, but of course it is possible for $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ to fail at an even number of places. Thus, the theorem as stated is wrong, and to fix it, we should pass from GL_2 to the inner form $D^\times$ (where D is a quaternion algebra over $\mathbb{Q}$). Then we find that the theorem as stated holds where we choose D of the form $D_\Sigma^\times$, where Σ is the even set of places where $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ fails. Here, D_Σ is the element of the Brauer group chosen by the short exact sequence

$$0 \to \operatorname{Br} F \to \bigoplus_v \operatorname{Br} F_v \to \mathbb{Q}/\mathbb{Z} \to 0.$$

We now turn to the Gross–Zagier formula. If $\varepsilon = 1$, then $L'(1/2, \pi \times \chi) = 0$ for functional equation reasons. To study its left-hand side, then we find a representation-theoretic failure at ∞: because $K_\infty = \mathbb{C}$, we see that $\eta_\infty(-1) = -1$, but $\chi_\infty = \varepsilon_\infty = 1$. Because $\varepsilon = 1$, we see that $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ fails at an odd set of finite primes p. In total, $\operatorname{Hom}_{T(\mathbb{A}_f)}(\pi_f \otimes \chi, \mathbb{C})$ vanishes, so the left-hand side must vanish.

On the other hand, having $\varepsilon = -1$ may reveal some content. Namely, $\chi_v(-1)\eta_p(-1) = \varepsilon_p(-1)$ will fail at an even set Σ of finite places p. This time around, we replace $\mathrm{GL}_{2,\mathbb{Q}}$ with its inner form $D_\Sigma^\times$, and the Shimura variety $\mathrm{Sh}_{\mathrm{GL}_2}$ is replaced by an inverse limit of Shimura curves. Then one can recover the correct Gross–Zagier theorem.

3.4 April 8

Welcome back.

3.4.1 Recollections on Waldspurger's Formula

For context, we are working in the context of smooth admissible representations. Globally over a number field F, this means that we are looking at some kind of representation π of $G(\mathbb{A}_F)$, which then has a decomposition into a restricted tensor product $\bigotimes_v' \pi_v$. For our setup, we take G to be a suitable form of GL_2: let K/F be a quadratic extension (where F will be set to $\mathbb{Q}$ later), we let T be the torus $\operatorname{Res}_{K/F} \mathbb{G}_{m,F}$, which is naturally embedded in $G := \mathrm{GL}_F(K)$, which is non-canonically isomorphic to GL_2.

Now, for χ and π automorphic representations of T and G (respectively), we may set $\widetilde{G} := (T \times G)/\mathbb{G}_m$. For Waldspurger's formula, we set $\delta_T \colon \chi \boxtimes \pi \to \mathbb{C}$ to be the distribution given by integration over $\int_{[\mathbb{G}_m \backslash T]}$. Waldspurger's formula will compute the spectral decomposition of δ_T. Morally, we would like to expand

$$\langle \delta_T, \delta_T \rangle \approx \int_{\widehat{\widetilde{G}}} \langle \delta_T, \delta_T \rangle_{\chi \boxtimes \pi} \, d(\chi \boxtimes \pi)$$

in terms of the special values $L(1/2, \pi \times \chi)$. We can think about $\langle \delta_T, \delta_T \rangle_{\chi \boxtimes \pi}$ formally as $\sum_{\varphi \in \mathrm{ON}(\pi)} |\ell_\chi(\varpi)|^2$ (here, $\mathrm{ON}(\pi)$ is an orthonormal basis), where

$$\ell_\chi(\varphi) := \int \varphi(t)\chi(t) \, dt$$

for $\varphi \in \pi$. However, this latter sum is infinite, so we must do some regularization. Here are two ways to regularize.

- Perhaps we can try to write a formula for $|\ell_\chi|^2$ directly as some map $\pi \otimes \overline{\pi} \to \mathbb{C}$.

- Alternatively, we can add a Schwarz function to smoothen the sum. Choose a Schwarz function f on $G(\mathbb{A}_F)$, and we will instead compute $\langle f \cdot \delta_T, \delta_T \rangle$, where $f \cdot \delta_T$ refers to some convolution

$$(f \cdot \varphi)(x) := \int_{G(\mathbb{A}_F)} f(g)\varphi(xg) \, dg.$$

In particular, we may manipulate

$$\begin{aligned}\langle f\cdot\delta_T,\delta_T\rangle_{\chi\boxtimes\pi} &= \sum_\varphi \langle f\cdot\delta_T,\chi\varphi\rangle\overline{\langle\chi\varphi,\delta_T\rangle} \\ &= \sum_\varphi \int_{[T]} f^\vee\cdot\varphi(t)\chi(t)\,dt\overline{\int_{[T]}\varphi(t)\chi(t)\,dt},\end{aligned}$$

where $f^\vee(g) := f\left(g^{-1}\right)$. This sum is now finite: for example, on nonarchimedean places, f becomes compactly supported, so $f\cdot\varphi$ must live in J-invariants of π for some open subgroup $J\subseteq G(F_v)$, which is a finite-dimensional space due to the smoothness of π.

These approaches are in fact equivalent. Namely, having the first computation done implies that we ought to be able to compute $\langle f\cdot\delta_T,\delta_T\rangle_{\chi\boxtimes\pi}$ because our final sum above may as well be plugging $(f\cdot\varphi)\otimes\widetilde{\varphi}$ into $\ell_\chi\otimes\ell_{\chi^{-1}}$. Conversely, given the second computation, we note that the map $S(G(\mathbb{A}_F))\to\operatorname{End}(\pi)$ given by $f\mapsto(f\cdot-)$ surjects onto the "smooth" endomorphisms of π (namely, having finite-dimensional output), so if we want to compute $(\ell_\chi\otimes\ell_{\chi^{-1}})(\varphi_1\otimes\varphi_2)$, we simply choose f_1 and f_2 so that their endomorphisms project π and $\widetilde{\pi}$ onto the spans of φ_1 and φ_2 (respectively). Then $\ell_\chi(\varphi_1)\ell_{\chi^{-1}}(\varphi_2)$ is seen to be proportional to the sum

$$\sum_\varphi \ell_\chi(f_1\cdot\varphi)\ell_{\chi^{-1}}(f_2\cdot\widetilde{\varphi}),$$

but this last sum is an instance of the computation of $\langle f\cdot\delta_T,\delta_T\rangle_{\chi\boxtimes\pi}$.

Remark 3.22. Here is a more succinct way to give the previous paragraph. The construction of ℓ_χ implies that $\ell_\chi\otimes\ell_{\chi^{-1}}$ lives in

$$\operatorname{Hom}_{T(\mathbb{A}_F)\times T(\mathbb{A}_F)}(\pi\otimes\widetilde{\pi},\mathbb{C}_{\chi^{-1}\boxtimes\chi}).$$

On the other hand, the functional $f\mapsto\langle f\cdot\delta_T,\delta_T\rangle$ lives in

$$\operatorname{Hom}_{T(\mathbb{A}_F)\times T(\mathbb{A}_F)}(S(G(\mathbb{A}_F)),\mathbb{C}_{\chi\boxtimes\chi^{-1}}),$$

possibly up to correcting some signs. Then the equivalence of our two computations comes down to the image of $S(G(\mathbb{A}_F))$ in endomorphisms (thought of as $\widetilde{\pi}\widehat{\otimes}\pi$) is large enough so that we can read off the value of any functional.

Remark 3.23. For reference, it is true that

$$\dim\operatorname{Hom}_{T(\mathbb{A}_F)\times T(\mathbb{A}_F)}(\pi\otimes\widetilde{\pi},\mathbb{C}_{\chi^{-1}\boxtimes\chi}) = 1.$$

Now, Waldspurger's formula provides a local decomposition of $\ell_\chi\otimes\ell_{\chi^{-1}}$ as

$$\ell_\chi\otimes\ell_{\chi^{-1}}\approx\prod_v\alpha_v,$$

where $\alpha_v\in\operatorname{Hom}_{T(F_v)\times T(F_v)}(\pi_v\otimes\widetilde{\pi}_v,\mathbb{C}_{\chi^{-1}\boxtimes\chi})$ is defined by

$$\alpha_v(\varphi\otimes\widetilde{\varphi}) = \int_{\mathbb{G}_m\backslash T(F_v)}\langle\pi(t)\varphi,\widetilde{\varphi}\rangle\,dt.$$

Here, the $\approx$ in our statement means that the equality is only true up to some explicit volume factors which notably depend on choices of Haar measures.

Let's explain what this has to do with special values. If v is nonarchimedean with K_v/F_v unramified, and if we further assume $\pi_v^{G(\mathcal{O}_v)}\neq 0$ and $\chi_v|_{T(\mathcal{O}_v)}=1$ and $\varphi\otimes\widetilde{\varphi}\in\pi_v^{G(\mathcal{O}_v)}\otimes\widetilde{\pi}_v^{G(\mathcal{O}_v)}$, then we are going to recover something about our local L-factors. (Note that these hypotheses hold for all but finitely many v.) Namely, one can calculate

$$\alpha_v(\varphi\otimes\widetilde{\varphi})\approx\frac{L(1/2,\pi_v\times\chi_v)}{L(1,\operatorname{Ad},\pi_v)L(1,\eta_v)},$$

where $\eta\colon\mathbb{A}_K^\times\to\mathbb{C}^\times$ is the quadratic (Dirichlet) character associated to K/F.

Remark 3.24. These conditions are potentially bizarre. Suppose that v splits in two up in K, meaning that $K_v = F_v \oplus F_v$. Then we note $\mathbb{G}_m \backslash T$ is just U_1, which is the kernel of the norm map $K^\times \to F^\times$. But now $\mathrm{U}_1(K_v) = F_v^\times$ because the norm map $F_v \times F_v \to F_v$ is just the product.

We are now ready for a statement.

Theorem 3.25 (Waldsburger's formula)**.** Fix notation as above. For a set S of places of F which is large enough, we have

$$\ell_\chi \otimes \ell_{\chi^{-1}} \approx \frac{L^S(1/2, \pi \times \chi)}{L^S(\pi, \mathrm{Ad}, 1) L^S(\eta, 1)} \prod_{v \in S} \alpha_v,$$

up to some volume factors.

Remark 3.26. In terms of our second question, we may equivalently ask for our functional $S(G(\mathbb{A}_F)) \to \mathbb{C}$ to suitably factor into local pieces when the input $f \in G(\mathbb{A}_F)$ does.

Let's recall something about our L-functions. To do this appropriately, we think of T as GSO_2, where the ambient quadratic form is given by the norm; similarly, we can think of G as GSO_3. (Here, $\mathrm{GSO}_\bullet$ refers to $\mathrm{SO}_\bullet$ plus scalars and is in particular connected, unlike $\mathrm{GO}_\bullet$ which may be disconnected.) Now, $\check{T}$ is still GSO_2 and has ${}^L T = \mathrm{GO}_2$ due to a nontrivial Galois action. Similarly, $\check{G} = \mathrm{GSp}_2$. Now, one may compute that

$$\check{\tilde{G}} = \left(\check{T} \times \check{G}\right)^{\det = 1} = \left(\mathrm{GSO}_2 \times \mathrm{GSp}_2\right)^{\det=1},$$

where the point is that the modding out by $\mathbb{G}_m$ is turned into a determinant 1 condition. Thus, we see that ${}^L\widetilde{G}$ will have a standard four-dimensional symplectic representation r given by χ and π, so we can build a degree four L-function $L(\chi \boxtimes \pi, r, s)$.

This construction of the L-function is not very helpful for us. Instead, we will use the theory of base change. Morally, note that there is an embedding of Langlands parameters $W_F \to {}^L G$ to Langlands parameters $W_K \to {}^L G$ simply by embedding the Weil groups. Thus, we expect to have a "base-change" functor from automorphic representations of G_F to automorphic representations of G_K which agrees with this. This is conjectural for general extensions K/F, but it is known if K/F is quadratic (due to Langlands) or solvable (due to Arthur–Clozel). The moral is that we can think of π has a base-change to some automorphic representation $\Pi_{K/F}$ of G_K, and we will have

$$L(\chi \times \pi, s) = L(\chi \otimes \Pi_{K/F}, \mathrm{Std}, s),$$

where now the right-hand side is the standard L-function for (a form of) $\mathrm{GL}_{2,K}$. Perhaps one is confused because the right-hand side is an L-function of degree 2, but this is okay because K/F is a quadratic extension which absorbed a factor of 2.

For simplicity, we will take $\chi = 1$ (so that the central character ω_π of π is trivial) for the remainder of the course. Then it turns out that

$$L(\chi \times \pi, s) = L(\pi, s) L(\pi \otimes \eta, s).$$

Let's explain this in terms of Langlands parameters. Taking $\chi = 1$ amounts to taking the trivial Langlands parameter of ${}^L T$, but ${}^L T$ already has some Galois action, so it amounts to the canonical projection $W_F \to \mathrm{Gal}(K/F)$. Thus, tensoring with π basically gives us two copies of π, one for each character of $\mathrm{Gal}(K/F)$, so we get $\pi \oplus \pi\eta$.

Anyway, these are now some standard L-functions, which have integral representations, allowing us to do some computations. Namely, we would like to compare $\langle \delta_T, \delta_T \rangle_\pi$ to $\langle \delta_A, \delta_{A,\eta} \rangle_\pi$ where A is the diagonal torus of elements of the form $\left[\begin{smallmatrix} * & \\ & 1 \end{smallmatrix}\right]$. In fact, we will show the following.

Theorem 3.27 (Jacquet)**.** Fix everything as above. Then for $f \in S(G(\mathbb{A}_F))$, one can construct $f' \in S(G(\mathbb{A}_F))$ such that

$$\langle f \cdot \delta_T, \delta_T \rangle = \langle f' \cdot \delta_A, \delta_{A,\eta} \rangle.$$

Further, for $h \in S(G(F_v))^{G(\mathcal{O}_v) \times G(\mathcal{O}_v)}$, we have $h * f = h * f'$.

Let's explain the application to Waldspurger's theorem. The left-hand side admits a spectral decomposition

$$\langle f \cdot \delta_T, \delta_T \rangle = \int_{\widehat{G}} \underbrace{\langle f \cdot \delta_T, \delta_T \rangle_\pi}_{J_\pi(f) :=} \, d\pi,$$

so we give the right-hand side a similar spectral decomposition, writing

$$\langle f' \cdot \delta_A, \delta_{A,\eta} \rangle = \int_{\widehat{G}} \langle f \cdot \delta_A, \delta_{A,\eta} \rangle_\pi \, d\pi.$$

Now, one can try to use Hecke algebras to try to separate the contribution of each π on each side matches up. For example, if $\langle f \cdot \delta_T, \delta_T \rangle_\pi$ is not identically zero, then $\langle f \cdot \delta_A, \delta_{A,\eta} \rangle_\pi$ will also not be identically zero, which by an argument with the functional equation implies that $L(\pi, 1/2)L(\eta \otimes \eta, 1/2)$ fails to vanish.

3.5 April 10

We continue.

3.5.1 The Relative Trace Formula

Recall our standing assumption that χ is trivial, which means that the central character of π is trivial, which means that π descends to an automorphic form of $G = \mathrm{PGL}_2$. We would now like to say something about relative trace formulae. For $f \in S(G(\mathbb{A}_F))$, we recall that $f \cdot \delta_T$ is the distribution

$$(f \cdot \delta_T)(x) = \int_{G(\mathbb{A}_F)} \delta_T(xg) f(g) \, dg,$$

where $x \in G(F) \backslash G(\mathbb{A}_F)$. Ultimately, we are interested in computing $\langle f \cdot \delta_T, \delta_T \rangle$ for Waldspurger's formula, so let's say a bit about how one can manipulate this object. For general φ, we note

$$\begin{aligned}
\langle f \cdot \delta_T, \varphi \rangle &= \int_{G(F)\backslash G(\mathbb{A}_F)} \varphi(x)(f \cdot \delta_T)(x) \, dx \\
&= \int_{G(F)\backslash G(\mathbb{A}_F)} \int_{G(\mathbb{A}_F)} \delta_T(xg) f(g) \varphi(x) \, dg \, dx \\
&= \int_{G(F)\backslash G(\mathbb{A}_F)} \delta_T(y) \int_{G(\mathbb{A}_F)} f(g) \varphi\left(yg^{-1}\right) \, dg \, dy,
\end{aligned}$$

where we have applied the variable substitution $y = xg$ at the end. We are now integrating over the distribution $\delta_T(y)$, so we can write this integral as

$$\langle f \cdot \delta_T, \varphi \rangle = \int_{[T]} \int_{G(\mathbb{A}_F)} f\left(g^{-1}\right) \varphi(yg) \, dg \, dy.$$

This rearranges into

$$\int_{G(\mathbb{A}_F)} f\left(g^{-1}\right) \int_{[T]} \varphi(yg) \, dy \, dg = \int_{T(\mathbb{A}_F)\backslash G(\mathbb{A}_F)} \underbrace{\int_{T(\mathbb{A}_F)} f\left(g^{-1}t\right) \, dt}_{\Phi^\vee(g) :=} \int_{[T]} \varphi(yg) \, dy \, dg.$$

Combining the integrals, we are left with

$$\int_{T(F)\backslash G(\mathbb{A}_F)} \Phi^\vee(g) \varphi(g) \, dg$$

by keeping track of the ambient invariance of everything in sight. (Namely, we see that φ is being integrated over $T(F)\backslash T(\mathbb{A}_F)$, so we may as well combine the integrals suitable.) Now, φ is further $G(F)$-invariant (it is a function on $G(F)\backslash G(\mathbb{A}_F)$), so we can rewrite the integral as

$$\int_{G(F)\backslash G(\mathbb{A}_F)} \varphi(g) \left(\sum_{\gamma \in T(F)\backslash G(F)} \Phi^\vee(\gamma g) \right) dg.$$

This is now basically a pairing of some sum with φ, so the moral is that $f \cdot \delta_T$ is basically equal to this "theta" $\theta(f_T^\vee)$ series of $\Phi^\vee$. Thus, we are able to write

$$\langle f \cdot \delta_T, \delta_T \rangle = \int_{[T]} \theta\left(f_T^\vee\right)(t)\, dt.$$

One can check that there are no convergence issues. (Namely, δ_T has finite support given by the CM points, so $f \cdot \delta_T$ has compact support and is of rapid decay, so the pairing has rapid decay as well.) Additionally, we remark that a direct computation can check that this expression is left- and right-invariant by $T(\mathbb{A}_F)$. This is giving us two ways to think about the pairing $\langle f \cdot \delta_T, \delta_T \rangle$.

- Writing $\langle f \cdot \delta_T, \delta_T \rangle = \langle \delta_T, f^\vee \cdot \delta_T \rangle$ lets us see this as a functional on $S(G(\mathbb{A}_F))$ which is left- and right-invariant by $T(\mathbb{A}_F)$. So this is a distribution on $T\backslash G/T$.
- Writing this as $\int_{[T]} \theta(f_T^\vee)(t)\, dt$ lets us see this as a $T(\mathbb{A}_F)$-invariant functional on $S(T\backslash G)$. So this is a distribution on X/T where $X = T\backslash G$.
- If we can write $f = f_1^\vee \cdot f_2$, then we find that

$$\langle f \cdot \delta_T, \delta_T \rangle = \langle f_2 \cdot \delta_T, f_1 \cdot \delta_T \rangle = \left\langle \theta(f_{2,T}^\vee), \theta(f_{1,T}^\vee) \right\rangle.$$

  This last expression is invariant under the action of the diagonal embedding by G into $S(X) \otimes S(X)$, where $X = T\backslash G$. So this is a distribution on $(X \times X)/G$, which is again basically the same thing.

Viewing θ as a "Poincaré series," we note the second is writing a Fourier expansion of θ, and the third is an inner product of Poincaré series.

We are now able to say something about the relative trace formula. Morally, it is an equality between a spectral and geometric expansion of the functional $f \cdot \langle f \cdot \delta_T, \delta_T \rangle$. We can even now say something about what this spectral expansion is: it follows by doing a spectral decomposition of functions in $L^2([G])$. Let's explain how this works for $G = \mathrm{PGL}_2$. Here, $L^2([G])$ decomposes as

$$\bigoplus_{\pi \text{ cuspidal}} \pi \oplus \bigoplus_{\dim \chi = 1} \mathbb{C}_\chi \oplus \int I_B^G(\chi)\, d\chi.$$

Let's explain these terms. The first sum is over the "discrete series" cuspidal representations of G. The second sum is over the one-dimensional characters. Lastly, the last integral refers to the "continuous spectrum"; the integral means that we are taking a Hilbert space direct sum. Note that we already see a continuous spectrum on $L^2(\mathbb{R})$ because this decomposes into a Hilbert space direct sum of the characters. Note the integral is taken over unitary idéle class characters on the central torus $A \cong \mathbb{G}_m$, which we think about as a quotient of the Borel subgroup by its unipotent radical.

Remark 3.28. The reason we write the decomposition in the above form is that it explains that any $\varphi_1, \varphi_2 \in L^2([G])$ will have inner product $\langle \varphi_1, \varphi_2 \rangle$ equal to a sum over the cuspidal and character pieces plus the value of an integral over the continuous spectrum.

Let's say something about the characters of G. Note that there are no nontrivial algebraic characters: they would have to be powers of $\det$, but only the trivial character is trivial on the diagonal copy of $\mathbb{G}_m \subseteq G$. On the other hand, there are many characters of $G(\mathbb{A}_F)$: note that one can produce lots of characters on $[\mathrm{GL}_2]$

by taking determinant to $\mathbb{A}_F^\times$ and then applying an idéle class character χ to $\mathbb{C}^\times$. One can check that this factors through $[G]$ as soon as χ is quadratic, so our characters are basically quadratic idéle class characters.

We are now ready to give the spectral side of the relative trace formula. Put simply, we are able to write

$$\langle\theta(f_{2,T}^\vee),\theta(f_{1,T}^\vee)\rangle = \int_{\widehat{G}}\langle\theta(f_{2,T}^\vee),\theta(f_{1,T}^\vee)\rangle_\pi\,d\pi,$$

where these inner products are

$$\sum_{\varphi\in\mathrm{ON}(\pi)}\langle\theta(f_{2,T}^\vee),\varphi\rangle\langle\overline{\varphi},\theta(f_{1,T}^\vee)\rangle,$$

where the sum is taken over an orthonormal basis of π. Using what we already know about these pairings, we can re-expand these θs to see this equals

$$\sum_{\varphi\in\mathrm{ON}(\pi)}\langle f_2\cdot\delta_T,\varphi\rangle\langle\overline{\varphi},f_1\cdot\delta_T\rangle = \sum_{\varphi\in\mathrm{ON}(\pi)}\int_{[T]}f_2^\vee\cdot\varphi(t)\,dt\int_{[T]}f_1^\vee\cdot\overline{\varphi}(t)\,dt.$$

We now hope to obtain a geometric expansion for this functional. Then we hope to be able to compare it to a relative trace formula for $\langle f\cdot\delta_A,\delta_{A,\eta}\rangle$, which should produce Waldspurger's formula.

Let's now say something about the geometric expansion. To begin, we note that we may expand

$$\langle\theta(\Phi_1),\theta(\Phi_2)\rangle_{[G]} = \int_{G(F)\backslash G(\mathbb{A}_F)}\sum_{(\gamma_1,\gamma_2)\in X\times X(F)}\Phi_1(x_1g)\Phi_2(x_2g)\,dg.$$

We now divide this up by $G(F)$ orbits as

$$\int_{G(F)\backslash G(\mathbb{A}_F)}\sum_{\xi\in(X\times X)(F)/G(F)}\sum_{\gamma\in G_\xi(F)\backslash G(F)}\Phi_1\otimes\Phi_2(\xi\gamma g),$$

which can be recombined into the sum

$$\sum_{\xi\in X\times X(F)/G(F)}\mathrm{vol}([G_\xi])\int_{G_\xi(\mathbb{A}_F)\backslash G(\mathbb{A}_F)}\Phi_1\otimes\Phi_2(\xi g)\,dg$$

of orbital integrals. This is great we are now integrating over purely adelic objects, so good choices of Φ_1 and Φ_2 will turn these integrals into purely local problems. We take a moment to remark that one can alternatively work with other formulations of our pairing to give different kinds of orbital integrals.

At long last, here is our statement.

Theorem 3.29 (Relative trace formula)**.** Fix everything as above. Then

$$\int_{\widehat{G}}\langle\theta(f_{2,T}^\vee),\theta(f_{1,T}^\vee)\rangle_\pi\,d\pi$$

equals

$$\sum_{\xi\in X\times X(F)/G(F)}\mathrm{vol}([G_\xi])\int_{G_\xi(\mathbb{A}_F)\backslash G(\mathbb{A}_F)}\theta(f_{2,T}^\vee)\otimes\theta(f_{1,T}^\vee)(\xi g)\,dg,$$

There are similar expressions for the pairing $\langle f\cdot\delta_A,\delta_{A,\eta}\rangle$, but some regularization is needed because our integrals are no longer compactly supported. What saves us in this case is that we are comparing δ_A with the twist $\delta_{A,\eta}$, so one is able to create cancellation by playing the characters off of each other.

Let's at least explain what the orbital integrals look like. For example, when looking at the expression over $A\backslash G/A$, we choose some $[\xi]\in A\backslash G/A$ and $f\in S(G(\mathbb{A}_F))$, and then our orbital integral looks like

$$\int_{A_\xi\backslash A\times A(\mathbb{A}_F)}f\left(a_1^{-1}\xi a_2\right)\eta(a)\,d^\times a.$$

Next time, we will explain how to relate the two relative trace formulae. Notably, we will upgrade Theorem 3.27 to compare the two geometric sides with a notable equality of the orbital integrals for any chosen ξ.

3.6 April 17

I missed last class, so this will be rough.

3.6.1 Matching on the Geometric Side

We have been interested in two functionals RTF^T and RTF^A of $S(G(\mathbb{A}_F))$, which are invariant $T \times T$ and $A \times (A, \eta)$-invariant respectively. We have two expansions for these functionals, one geometric and one automorphic. The automorphic one is already somewhat understood. The geometric side is given by some sum

$$\sum_{\xi \in T(F) \backslash G(F)/T(F)} \mathrm{Vol}([T_\xi])\mathcal{O}_\xi$$

of orbital integrals.

Last class, we discussed that it is easier to sum over the GIT quotient $T\backslash G//T = \operatorname{Spec} F[G]^{T\times T}$, which is canonically isomorphic to $A\backslash G//A$, which are both birational with $\mathbb{A}^1$ via the map $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto ad/(ad-bc)$. In particular, for open $U \subseteq \mathbb{A}^1$, say avoiding 0 and 1, we find that $A\backslash G|_U$ is isomorphic to $A \times U$, which tells us that the contribution to the relative trace formula for $\xi \notin \{0,1\}$ are given by the orbital integrals

$$\mathcal{O}_\xi^A(\varphi_A) = \int_{A(\mathbb{A}_F)} \varphi_A(\xi a)\eta(a)\, da \qquad \text{and} \qquad \mathcal{O}_\xi^T(\varphi_T) = \int_{T(\mathbb{A}_F)} \varphi_T(\xi t)\, dt,$$

where $\varphi_A \in S(A\backslash G)$ and $\varphi_T \in S(T\backslash G)$. These now split into some local integrals, so we now find that we have local orbital integrals which we call $\pi_{A!}\varphi_A(\xi) \in C^\infty(U)$ and $\pi_{T!}\varphi_T(\xi) \in C^\infty(U)$. We are now ready to state a more precise form of Theorem 3.27.

Theorem 3.30. Fix everything as above.

(a) Matching: for each f, there is f' such that $\pi_{T!}(f) = \pi_{A!}(f')$.

(b) Fundamental lemma for Hecke algebra: if v is nonarchimedean and K_v/F_v is unramified, and if $f \in \mathcal{H}(G(F_v), G(\mathcal{O}_v))$, then we may take $f' = f$.

Remark 3.31. If K_v/F_v is split, there is nothing to do because A and T both refer to the split torus.

This matching of terms on the geometric side of the relative trace formula is something of a miracle. Surely it is expected because Waldspurger's theorem produces a matching of the relative trace formulae on the automorphic side. Our identification away from $\xi \in \{0,1\}$ above tells us that the content of the above theorem is producing the matching for $\xi \in \{0,1\}$. It remains to understand limits approaching the "singularities." By applying an automorphism of G, we may as well focus on $\xi = 1$.

For $X = A\backslash G$, we find that $\mathbb{P}^1 \times \mathbb{P}^1 \setminus \Delta\mathbb{P}^1 \cong X$ by $(x,y) \mapsto \frac{x}{x-y}$. We are thus interested in the behavior around the singularity $(\infty, 0)$. To visualize, we linearize X: there is a birational A-equivariant map $\mathbb{A}^2 \to X$ given by $(x,y) \mapsto (x^{-1}, y)$, where A acts on $\mathbb{A}^2$ by $a \cdot (x,y) = (a^{-1}x, ay)$, and importantly, this map is an isomorphism in a neighborhood of $(0,0) \mapsto (\infty, 0)$. (Note that these orbits are hyperbolas now.) This linearization then tells us how to handle the matching around $\xi = 1$.

Remark 3.32. This linearization is not a miracle: its existence is a consequence of Luna's étale slice theorem.

Let's now do our matching. Choose $f \in S^2(\mathbb{A}^2)$. Then we produce a function $\pi_{A!}f(\zeta)$, where $\zeta \in \mathbb{A}^2$ is our coordinate, and then the Mellin transform

$$(\mathcal{M}\pi_{A!}f)(\chi) = \int_{F^\times} \pi_{A!}f(\zeta)\chi^{-1}(\zeta)\, d^\times\zeta,$$

which can be thought of as a double Tate integrals, but now its simple poles live at $\chi \in \{1, \eta\}$. By undoing the Mellin transform, we find that $\pi_{A!}f(\zeta) = c_1(\zeta) + \eta(\zeta)c_2(\zeta)$, where $c_1, c_2 \in C^\infty(U)$ are some smooth functions. Going all the way back to our coordinate $\xi \in X$, we see that $\pi_{A!}f(\xi) = c_1(\xi) + \eta(\xi - 1)c_2(\xi)$ in a neighborhood of $\xi = 1$ (where we technically changed the smooth function silently).

We now turn to the non-split torus T. Well, note that T is basically given by A after applying a Galois twist in $\mathrm{H}^1(\mathrm{Gal}(\overline{F}/F), \mathrm{Aut}(G, A))$. Note that this Galois group can be seen to be $\mathrm{H}^1(\mathrm{Gal}(K/F), \mathbb{Z}/2\mathbb{Z})$, where the canonical generator of $\mathrm{Aut}(G, A)$ is given by conjugation by the nontrivial Weyl element. Thus, we can apply this automorphism everywhere in the previous discussion. For example, we still admit a linearization $\mathbb{A}^2 \to T\backslash G$, but now the T-action on $\mathbb{A}^2$ must be twisted: it is the natural action of T on $V \coloneqq \mathrm{Res}_{K/F} \mathbb{A}^1$. (For example, the orbits can be seen to be circles in $\mathbb{A}^2$ because the quotient map $V \twoheadrightarrow V//T = \mathbb{A}^1$ is simply the norm. Note we already saw this norm in the split case when dealing with $A\backslash G$.)

> **Remark 3.33.** The quotient $V \twoheadrightarrow V//T$ is now no longer surjective on F-points: indeed, the norm map $\mathrm{N}_{K/F} \colon K^\times \to F^\times$ is not surjective! Nonetheless, our fibers are always a trivializable T-torsor, which is already trivial when $\zeta \in F^\times$ is in the image of the norm map and trivializing over an extension otherwise. The fiber over 0 has a single point over F, but there are two lines over $\overline{F}$ which are swapped by the Galois action.

We now claim that the collection of functions $\pi_{T!}(S(F^2))$ are just given by restrictions of smooth functions $S(F)$ to the image of $\mathrm{N}_{K/F}(K)$. Surely we are looking at functions on $\mathrm{N}_{K/F}(K)$, but to see that they should be smooth, we note that the image of $\pi_{T!}(f)$ is the same as $\pi_{T!}(\widetilde{f})$ where $\widetilde{f}$ is the average of f over the T-orbit. Because T is compact, we know $\widetilde{f}$ continues to be smooth! So $\pi_{T!}(\widetilde{f}) = \widetilde{f}|_{\mathrm{N}_{K/F}(K)}$.

Let's now think about what our matching is asking for. After linearization, for each $f \in S(F^2)$, we would like to find $f' \in S(F^2)$ with $\pi_{T!}(f) = \pi_{A!}(f')$. Now, the direction of the matching is important. Note that $\pi_{T!}(f)$ looks like

$$c1_{\mathrm{N}_{K/F}(K^\times)} = \frac{c}{2} + \eta\frac{c}{2}$$

for some smooth function c. This has the form of the functions $\pi_{A!}(f')$ we computed previously, so matching is confirmed!

> **Remark 3.34.** To check the fundamental lemma claim, one can directly compute that this formula sends $1_{\mathcal{O}_F^2}$ to $1_{\mathcal{O}_F^2}$. This is a basic case of the Hecke algebra check we wanted.

Let's review our intended application for a moment. This comparison of relative trace formulae is able to show that if π-component of the relative trace formula for T is nonzero, then the same is true for the π-component of the relative trace formula for A. This implies a weak version of Waldspurger's formula because it provides non-vanishing of our L-functions by checking what the π-component of RTF^A is.

If we wanted to go the other way, we need to be able to do more matching. We even knew that we would have problems much earlier because we have been working with PGL_2 instead of with division algebras. The moral is that we should look at $G' = PD^\times$ where D is the division algebra over F we described long ago. Then it turns out that there is a canonical identification with $T\backslash G//T$ and $T\backslash G'//T$ with $\mathbb{A}^1$ so that we have

$$\mathbb{A}^1(F) = \mathrm{im}(T(F)\backslash G(F)) \cup \mathrm{im}(T(F)\backslash G'(F))$$

away from 0 and 1. In fact, one can check that the fibers over the $T(F)$-points on the left factor or the right factor, so we get the extra degree of freedom we lost from earlier! Keeping track of everything, one can check that this does in fact let us recover the full matching in the opposite direction. This sort of thing is required for a full proof of Waldspurger's formula instead of our mere non-vanishing corollary.

3.7 April 22

Today we complete our discussion of Waldspurger's formula.

3.7.1

For the time being, we work locally over some F_v. Another way to look at Theorem 3.30 is that the two projections $\pi_T\colon (T\backslash G/T) \to \mathbb{A}^1$ and $\pi_A\colon (A\backslash A/A) \to \mathbb{A}^1$ produces an inclusion

$$\pi_{T!}(S(T\backslash G)) \subsetneq \pi_{A!}(S(A\backslash G))$$

which is compatible with the spherical Hecke algebra (in the sense discussed in the statement of the fundamental lemma). It is desirable to upgrade the above into a full equality so that one can prove a full form of Waldspurger's formula. Of course, the problem is that we only had access to "half" of the space with $\pi_{T!}$.

To attain a full matching, we need to add in the missing piece. Note that $Y := T\backslash G$ lives over $\mathbb{A}^1$, and its fibers (away from 0 and 1) are some T-torsors (because $T\backslash G//T \to \mathbb{A}^1$ is an isomorphism). Half the time, the fiber over $\xi \in \mathbb{A}^1$ is the trivial torsor (namely, when ξ is a norm), and otherwise the fiber is empty. Now, let R be the nontrivial T-torsor, and we find that

$$Y^R := (Y \times_T R) = Y \times_G (G \times_T R)$$

has fibers which are now nontrivial over the other ξs! In other words, when the fiber over some ξ is R (and in particular the empty T-torsor), we find that the fiber over ξ of Y^R becomes $R \times_T R$, which is T because T has only two T-torsors.

Remark 3.35. The automorphisms of G as a G-variety (with left action by translation) is simply given by G acting on the right. Analogously, the automorphisms of G acting on some G-torsor will again simply be given by a form of G because this group must become G once the G-torsor is trivialized.

Remark 3.36. Let's think a bit about forms. Note that there is a sequence of maps

$$\mathrm{H}^1(\mathrm{Gal}_F, G) \to \mathrm{H}^1(\mathrm{Gal}_F, \mathrm{Inn}\, G) \to \mathrm{H}^1(\mathrm{Gal}_F, \mathrm{Aut}(G)).$$

The last group parameterizes forms of G, and the middle groups classifies inner forms, and the first groups classifies pure inner forms (or G-torsors). Notably, the data of an inner form might be more than merely a form of G which happens to be in the image of the map from the middle group to the right group.

Example 3.37. Take $G = \mathrm{GL}_n$.

- Then $\mathrm{H}^1(\mathrm{Gal}_F, G(\overline{F}))$ is trivial: this is parameterizing G-torsors, which are vector bundles over $\operatorname{Spec} F$, which are just vector spaces over F. There is only one such vector space, up to isomorphism.
- Continuing, $\mathrm{H}^1(\mathrm{Gal}_F, \mathrm{Inn}\, G) = \mathrm{H}^1(\mathrm{Gal}_F, \mathrm{PGL}_n(\overline{F}))$. Now, PGL_n can be thought of as automorphisms of $\mathbb{P}^n$ or as automorphisms of $M_n(\overline{F})$, so this parameterizes forms of $\mathbb{P}^n$ or central simple algebras over F of dimension n^2. Note that this can be mapped to the Brauer group $\mathrm{H}^2(\mathrm{Gal}_F, \mathbb{G}_m)$ via a suitable long exact sequence. The corresponding forms of G are the ones which look like $D^\times$.
- Lastly, $\operatorname{Aut} G = \operatorname{Inn} G \rtimes (\mathbb{Z}/2\mathbb{Z})$, where the extra $\mathbb{Z}/2\mathbb{Z}$ comes from the inverse transpose automorphisms. Thus, the forms given by $\mathrm{H}^1(\mathrm{Gal}_F, G)$ can either be inner of the form $D^\times$ (where D is a central simple algebra of dimension D) or a unitary group (which corresponds to Galois acting nontrivially on the $\mathbb{Z}/2\mathbb{Z}$ piece).

Example 3.38. Take $G = \mathrm{SO}_n$. Note SO_n is automorphisms of the data of a vector space V of dimension n, a quadratic form q up to isomorphism, and a nonzero vector ω in $\wedge^n V$ (to keep track of orientation), though we need an extra condition so that q and ω have a coherence condition (namely, the discriminant of q agrees with ω).

Example 3.39. Similarly, $\mathrm{H}^1(\mathrm{Gal}_F, \mathrm{O}_n(\overline{F}))$ classifies quadratic spaces (V, q) of dimension n, which are notably by the quotient

$$\frac{(\mathrm{O}_n\backslash\mathrm{GL}_n)(F)}{\mathrm{GL}_n(F)}.$$

Example 3.40. Take $G = T$ to be the torus above, which we see is SO_2 because it is the kernel of some quadratic form.

- Then $\mathrm{H}^1(\mathrm{Gal}_F, T)$ is given by the space of quadratic spaces of dimension 2 with discriminant equal to the discriminant of the norm map $\mathrm{N}_{K/F}$ (viewed as a class in $F^\times/F^{\times 2}$).
- The torus T is abelian, so it has no inner forms.
- Lastly, $\mathrm{Aut}\, T = \mathrm{Aut}\, T$ because this is some abelian group.

Notably, Y^R is seen to be a torsor of G^R; note that T admitting no inner forms means that T must then still act on Y^R (on the right) and hence embeds in the automorphism group G^R! More generally, there is a map from T-torsors to G-torsors by taking $(G \times_T -)$, so one can take automorphisms suitably to see this action.

Now, the discussion above tells us that G^R should be something which looks like $\mathrm{P}D^\times$, where D is a quaternion algebra.

Remark 3.41. Let's discuss how quaternion algebras come about. Locally, there is an invariant map $\mathrm{inv}_v \colon \mathrm{Br}\, F_v \to \mathbb{Q}/\mathbb{Z}$ which is an isomorphism when v is nonarchimedean (and is an isomorphism on $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ when v is archimedean). Thus, there are only two quaternion algebras. Globally, there is a short exact sequence

$$0 \to \mathrm{Br}\, F \to \bigoplus_v \mathrm{Br}\, F_v \overset{\sum \mathrm{inv}}{\to} \mathbb{Q}/\mathbb{Z} \to 0,$$

so the quaternion algebras (given by 2-torsion) can simply be parameterized by some finite set Σ of places with even cardinality to denote the locations of $1/2$ of a tuple in $\bigoplus_v \mathrm{Br}\, F_v = \bigoplus_v \mathbb{Q}/\mathbb{Z}$. We will let D_Σ denote the corresponding quaternion algebra.

Remark 3.42. It follows from the theory of central simple algebras that having an embedding $K^\times \hookrightarrow D^\times$ (where $[K : F] = 2$ and $[D : F] = 2^2$) forces D to split over K; i.e., $D_K^\times = \mathrm{GL}_{2,K}$. Locally, this means that every quadratic extension of F_v embeds into $D^\times$. (Yiannis (casually) claims that one can prove local class field theory in this manner.) Turning this into some global statement, suppose that D splits over a global extension K/F. For places v of F where D_v is non-split, there are two cases.'

- If v is split in K, then D_v will continue to be non-split over every completion in $K \otimes F_v$.
- If v is non-split in K, then K_v is some field and hence embeds into D_v, so D_v automatically splits over K_v.

Concretely, for our D_Σ, if D_Σ splits over K/F, then we are forced to have this be true locally, so each $v \in \Sigma$ must be non-split in K.

The moral of the story is that, locally, we can upgrade the proof from last class to produce an isomorphism

$$\pi_{T!}(S(T\backslash G)) \oplus \pi_{T!}\left(S(T\backslash G^R)\right) \cong \pi_{A!}(S(A\backslash G)).$$

The moral is that each summand deals with half of a matching statement. Globally, one needs a relative trace formula RTF_R^T for the pair $\left(G^R, T\right)$ for a given form R of T, which must then look like $\mathrm{P}D^\times$ for some quaternion algebra D. The geometric expansion then looks like

$$\mathrm{RTF}_R^T(f) = J_0(f) + J_1(f) + \sum_{\xi \in U(F)} \mathcal{O}_\xi(f),$$

where $\mathcal{O}_\xi(f)$ continues to be the same orbital integral, and J_0 and J_1 are some contributions coming from 0 and 1.

At long last, here is our upgraded global matching statement.

Theorem 3.43. For all $(f_R) \in \bigoplus_R S\left(T\backslash G^R(\mathbb{A}_F)\right)$, there exists is $f' \in S(A\backslash G(\mathbb{A}_F))$ such that

$$\sum_R \mathrm{RTF}_R^T(f_R) = \mathrm{RTF}^A(f').$$

The opposite is also true (namely, for all f', there exists f). Furthermore, these mappings are compatible with spherical Hecke algebras: if v is a place of F where K/F is unramified, and f_R is unramified at v (notably, $f|_{G^R} = 0$ if R is ramified at v), then f' can also be taken to be unramified at v; further, the action by the Hecke algebra $\mathcal{H}(G(F_v), G(\mathcal{O}_v))$ agrees on both sides.

This gives a full geometric comparison of our relative trace formulae. It remains to do spectral comparison. Namely, moving now to the spectral side, there is an equality

$$\bigoplus_R \int_{\widehat{G_R}} J_{R,\pi}^T(f)\,d\pi = \int_{\widehat{G}} J_\pi^A(f')\,d\pi,$$

for suitably interpretations of these integrals. Notably, the left-hand side is made of terms which look like $\int_{[T]} \varphi_1(t)\,dt\overline{\int_{[T]} \varphi_2(t)\,dt}$, and the right-hand side is made of terms like $\int_{[A]} \varphi_1(a)\,da\overline{\int_{[A]} \varphi_2(a)\eta(a)\,da}$. We are hoping to achieve an equality like

$$\sum_R J_{R,\pi}^T(f) \stackrel{?}{=} J_\pi^A(f').$$

This then proves that the non-vanishing $L(\pi, 1/2)L(\pi\otimes\eta, 1/2) \neq 0$ is equivalent to having some R for which $J_{R,\pi}^T(f) \neq 0$ (i.e., the integral over $[T]$ restricted to the π-component is nonzero).

Remark 3.44. Technically, this does not make sense: π on the right is an automorphic form of PGL_2 while π on the left is an automorphic form of $\mathrm{P}D^\times$, where D is given by R. To fix this, we could use the Jacquet–Langlands correspondence: we note that G^R and G are still isomorphic almost everywhere locally, so one can hope to build a bijection between these automorphic forms by requiring there to be some π^R to be isomorphic to a given π at the places where G^R is isomorphic to G. (Note this property determines at most one automorphic form π^R by strong multiplicity one.)

Let's discuss how to do this spectral isolation. Fix a large finite set of places Σ: Σ should contain nonarchimedean places, places ramified for K/F, and maybe more later on to include some ramified places for our automorphic form π of G. We now fix some matching functions $(f_{\Sigma,R})$ and f'_Σ locally over the places of Σ, and we will let our matching functions away from Σ vary. For example, there is a Hecke algebra action by

$$\mathcal{H}^\Sigma \coloneqq \bigoplus_{v\notin\Sigma}{}' \mathcal{H}(G(F_v), G(\mathcal{O}_v)),$$

and we go ahead and define functionals RTF_Σ^T and RTF_Σ^A on $\mathcal{H}^\Sigma$ by taking $h \mapsto \mathrm{RTF}^\bullet(h\otimes f_\Sigma)$. Now, the spectral decomposition of the relative trace formula yields

$$\mathrm{RTF}_\Sigma^A(h) = \int_{\widehat{G}} J_\pi^A(h\otimes f'_\Sigma)\,d\pi,$$

and we see that this integral vanishes for π unramified outside Σ because we are acting by this unramified test function $h\otimes f'_\Sigma$ there. On the other hand, for π unramified outside Σ, we get contribution by the Hecke eigenvalue $\widehat{h}(\pi)$ to see

$$\mathrm{RTF}_\Sigma^A(h) = \int_{\widehat{G}} \widehat{h}(\pi) J_\pi^A(1_{G(\mathcal{O}^\Sigma)}\otimes f'_\Sigma)\,d\pi.$$

One has a similar spectral expansion on the other side of our comparison of relative trace formulae, writing

$$\mathrm{RTF}_{\Sigma}^{T}(h) = \sum_{R} \int_{\widehat{G^R}} \widehat{h}(\pi^R) J_{\pi^R}^{A}(1_{G(\mathcal{O}^\Sigma)} \otimes f_\Sigma)\, d\pi.$$

Let's now use something about the Hecke algebra: by the Iwasawa decomposition, we see $\mathcal{H}(G(F_v), \mathcal{O}(F_v))$ is simply $\mathbb{C}[T_v]$, where T_v is the class $G(\mathcal{O}_v)\left[\begin{smallmatrix} \varpi_v & \\ & 1 \end{smallmatrix}\right]G(\mathcal{O}_v)$. Then some π produces a functional $\pi_v \colon h \mapsto \widehat{h}(\pi_v)$ on the Hecke algebra. Thus, $\mathcal{H}^\Sigma$ can be thought of as a polynomial algebra on the polynomial ring over the letters $\{T_v\}_{v\in\Sigma}$, and we see that $\widehat{h}(\pi)$ and $\widehat{h}(\pi^R)$. Thus, our comparison of relative trace formula is more or less an equality of two large measures against these polynomial rings.

Bibliography

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. 2nd ed. Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg, 2008.

[Ser10] Jean-Pierre Serre. "Complex Multiplication". In: *Algebraic Number Theory: Proceedings of an Instructional Conference*. Ed. by J. W. S. Cassels and A. Fröhlich. 2nd ed. London Mathematical Society, 2010.

[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