ALGEBRAIC FORMULATION OF THE MAIN THEOREM OF CM

BRANDON LEVIN

1. Introduction

The goal of this talk is to introduce the algebraic form of the Main Th'm of CM and show that it implies the "down to earth" form of the main th'm stated in Mike's lecture. Along the way, we will introduce several important technical concepts used in the proof of the main theorem including $\mathbb{Q}$-polarization and the reflex torus. We follow very closely the presentation given in Appendix A of the CM book [2] by Chai, Conrad and Oort.

The main th'm in its most concrete form describes the Galois action on any CM abelian over a given base field K (CM is always defined over K). In Mike's talk, he stated it as follows:

Theorem 1.1. *Let (A, i) be a CM abelian variety over a number field $K \subset \overline{\mathbb{Q}}$, and let (L, Φ) be its CM-type.*

- (i) *The reflex field $E \subset \overline{\mathbb{Q}}$ is contained in K*
- (ii) *There exists a unique algebraic Hecke character $\epsilon : \mathbb{A}_K^\times \to L^\times$ such that for each ℓ, the continuous homomorphism*

$$\phi_\ell : Gal(K^{ab}/K) \to L_\ell^\times$$
$$\phi_\ell(a) = \epsilon(a)\epsilon_{alg}(a_\ell^{-1})$$

is equal to the ℓ-adic representation of $Gal(K^{ab}/K)$ on the ℓ-adic Tate module $V_\ell(A)$.

- (iii) *The algebraic part of ϵ is*

$$\epsilon_{alg} = N_\Phi \circ Nm_{K/E},$$

where $N_\Phi : Res_{E/Q}\mathbb{G}_m \to Res_{L/Q}\mathbb{G}_m$ denotes the reflex norm.

- (v) *If v is a finite place of K then A has good reduction at v if and only if $\varepsilon|_{\mathcal{O}_{K_v}^\times} = 1$, in which case for the reduction $\overline{A}/\kappa_v$, and any uniformizer π_v of $\mathcal{O}_{K_v}$, we have $\epsilon(\pi_v) = \mathrm{Fr}_{\overline{A},q_v}$, where $q_v = \#\kappa_v$.*

At the end of the lecture, we will give a construction ε, and deduce from the algebraic main theorem that it has the properties above. The proof of the main theorem will require us to relate our construction today to the reflex norm N_Φ via the formula of Taniyama-Shimura. Mike already gestured toward this when he pointed out that property (iii) and (v) essentially pins down ε. One difficulty in Mike's perspective is it is unclear how to define ε at the bad primes.

There are various motivations for our next move which is to free ourselves from our particular abelian variety A_0 over the field K and instead work at the level of CM abelian varieties over $\overline{\mathbb{Q}}$ at the expense of adding more data. The new formulation will yield huge technical advantages by allowing us to change ground fields in any given proof. Another motivation is everything we do should morally depend only on the CM-type.

The rough idea is given an abelian variety (A, i) with CM by L over $\overline{\mathbb{Q}}$ and if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E)$, we want to describe the action

$$[\sigma] : V_\ell(A) \to V_\ell(A^\sigma)$$

for every prime ℓ. By "describe," I mean given an L-linear isogeny $\varphi_\sigma : A^\sigma \to A$ (which is compatible with polarizations in some sense), we give a formula for the composite $V_\ell(\varphi_\sigma) \circ [\sigma]$ as an endomorphism of $V_\ell(A)$.

We end with some notation: L will always be a CM field and K a number field. The internal complex conjugation on L is given by $c \mapsto c^*$. For an abelian variety A, we define the restricted product

$$V_f(A) = \prod_\ell{}' V_\ell(A).$$

We denote the finite adeles of the number field K by $\mathbb{A}_{K,f}$.

2. $\mathbb{Q}$-POLARIZATIONS

Recall for an abelian variety A over a field k, a polarization is an symmetric isogeny $\psi : A \to A^\vee$ over k which is positive definite, in the sense that the pullback along $(1, \psi) : A \to A \times A^\vee$ of the Poincare bundle is ample. We record some facts about polarizations for later use.

Proposition 2.1. *Over an algebraically closed field k, any polarization $\psi : A \to A^\vee$ is given by the Mumford construction $\psi_{\mathcal{L}} : x \mapsto t_x^*(\mathcal{L}) \otimes \mathcal{L}^{-1}$ for some ample line bundle $\mathcal{L}$.*

Proof. See Mumford [1] §22 Th'm 2 and the discussion following. □

Proposition 2.2. *Let K be a field of characteristic 0, A an abelian variety over K, and $\psi : A \to A^\vee$ a homomorphism. Let $K \hookrightarrow \mathbb{C}$ be any embedding. Then ψ is a polarization iff $\psi_{\mathbb{C}}$ is. In the analytic theory, a polarization is equivalent to a positive definite Hermitian form H on* $\mathrm{Lie}(A(\mathbb{C}))$ *such that* *the skew-symmetric form* $E = \operatorname{Im} H$ *takes integral values on the lattice* $H_1(A(\mathbb{C}), \mathbb{Z}) \subset \operatorname{Lie}(A(\mathbb{C}))$. *We will write*

$$\psi_{\mathbb{Z}} := (2\pi i)E : H_1(A(\mathbb{C}), \mathbb{Z}) \times H_1(A(\mathbb{C}), \mathbb{Z}) \to \mathbb{Z}(1)$$

and note that this determines H.

Remark 2.3. Note that $\psi_{\mathbb{Z}}$ is (1) skew-symmetric and (2) the complex avatar of the Weil pairing, so we should also recall that any polarization ψ also induces a non-degenerate skew-symmetric pairing

$$e_{\psi,\ell} : T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1)$$

given by $\langle x, \psi(y)\rangle$, where $\langle \cdot, \cdot \rangle$ is the ordinary Weil pairing between $T_\ell(A)$ and $T_\ell(A^\vee)$. For $K = \mathbb{C}$, we have $e_{\psi,\ell} = (\psi_{\mathbb{Z}})_{\mathbb{Z}_\ell}$.

Definition 2.4. A $\mathbb{Q}$-polarization is an element of $\operatorname{Hom}^0(A, A^\vee)$, which is positive rational multiple of a polarization.

There is nothing fancy going on here. We are literally just allowing positive rational denominators in our polarizations. If you multiple any $\mathbb{Q}$-polarization by a large positive integer, you get an honest polarization $A \to A^\vee$. In some sense, this is just bookkeeping device, but a useful one.

In the analytic theory, this is the same as considering skew-symmetric pairings

$$\psi_{\mathbb{Q}} : H_1(A(\mathbb{C}), \mathbb{Q}) \times H_1(A(\mathbb{C}), \mathbb{Q}) \to \mathbb{Q}(1)$$

induced by a positive definite Hermitian forms as before.

Let (A, i) be an abelian variety over a field K of char 0 with complex multiplication by L.

Recall the following results from Arnav's lectures:

1. When $A^\vee$ is given CM by L using the formula $i^\vee(c) = (i(c^*))^\vee$, then its CM type is the same as that of A.
2. For $(A, i)/L$ as above, there exists a L-linear polarization over F. Arnav proved this by descent from the algebraic closed case.

It will be useful to characterize the space of L-linear polarization over F.

Lemma 2.5. *The set of* L*-linear* $\mathbb{Q}$*-polarizations on* A *over* F *is a homogeneous space under the subgroup of totally positive elements in the maximal totally real subfield* L^+ *of* L.

Proof. Any two L-linear polarizations ψ, ψ' in $\operatorname{Hom}^0(A, A^\vee)$ are related by multiplication by an element $c \in L^\times$. So the question is when is $\psi \circ c$ still a $\mathbb{Q}$-polarization. This is evidently independent of replacing ψ by a positive multiple of ψ. A short calculation shows that $\psi \circ c$ symmetric is equivalent to $c \in L^+$. We can check positivity over $\mathbb{C}$.

To check the positivity condition, we consider the particular explicit polarization given in Mumford [1] §22 of a CM abelian variety. Roughly, $\mathrm{Lie}(A(\mathbb{C})) \cong \prod_{\tau_i \in \Phi} \mathbb{C}_{\tau_i}$, and the Hermitian form is given by $\sum_{i=1}^{g} \beta_i x_i \overline{y_i}$ for $\beta_i \in \mathbb{R}_{>0}$. When we modify by $i(c)$, this changes the constants $\beta_i \mapsto \tau_i(c)\beta_i$ and from there, it is clear, since each real embedding is represented in the restrictions of the τ_i. $\square$

Recall the following fact which Mike mentioned in his lecture (which follows from L being self-centralizing in the endomorphism algebra):

Lemma 2.6. *Let (A_0, i_0) and (A_0', i_0') be abelian varieties with CM type (L, Φ) over a number field K. Assume that $\mathrm{Hom}_L^0(A_0, A_0')$ is nonzero. Let β be a place of K of good reduction with residue κ. Then, the reduction map*

$$\mathrm{Hom}_L^0(A_0, A_0') \to \mathrm{Hom}_L^0(\overline{A}_0, \overline{A}_0')$$

on L-linear isogenies is bijective.

Why introduce $\mathbb{Q}$-polarization again? The reason is that they will provide the necessary rigidity to make our new algebraic formulation of the main theorem work.

Consider (A, i, ψ) an abelian variety with complex multiplication of type (L, Φ) over $\overline{\mathbb{Q}}$, where ψ is a L-linear polarization. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E)$. Then, the triple

$$(A^\sigma, i^\sigma, \psi^\sigma) = \overline{\mathbb{Q}} \otimes_{\sigma, \overline{\mathbb{Q}}} (A, i, \psi)$$

has the same type as (A, i) because σ is trivial on the reflex field. Arnav proved that there exists some L-linear isogeny $\zeta : A^\sigma \to A$. We say that $\zeta \in \mathrm{Hom}^0(A^\sigma, A)$ is $\mathbb{Q}$-compatible with ψ if

$$\zeta^\vee \circ \psi \circ \zeta = q_\zeta \cdot \psi^\sigma,$$

for some positive rational number q_ζ i.e. conjugation by ζ preserves the rational ray corresponding to ψ. Note we can make the same defintion for any $\zeta \in \mathrm{Hom}^0(A, A^\sigma)$.

Note there is no subscript σ or ψ on q, because by computing degrees we always get that $q_\zeta = \deg(\zeta)^{1/g}$. The main result of this section will be that such an isogeny always exists.

Remark 2.7. If ζ is compatible for a particular ψ, then it is for all L-linear polarizations. Any other polarization is given by $\psi \circ i(c)$ for some $c \in L^+$ totally positive. Then,

$$(\psi \circ i(c))^\sigma = \psi^\sigma \circ i^\sigma(c)$$

and

$$\zeta^\vee \circ (\psi \circ i(c)) \circ \zeta = \zeta^\vee \circ \psi \circ \zeta \circ i^\sigma(c)$$

since ζ is L-linear.

Where will find such an isogeny? The only place we could; we will choose a realization of A over a suitable number field and then pick a suitable relative Frobenius which we can lift to the generic fiber. Later, we will characterize the dependence on choices.

Theorem 2.8. *Let* (A, i, ψ) *an abelian variety with complex multiplication of type* (L, Φ) *over* $\overline{\mathbb{Q}}$*, where* ψ *is an* L*-linear polarization. Let* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E)$*. There exists an* L*-linear isogeny*

$$\varphi_\sigma : A^\sigma \to A$$

which is $\mathbb{Q}$*-compatible with* ψ*.*

Proof. The idea is choose an suitable descent of A to a number field such that φ_σ will be the lift of an appropriate Frobenius element.

Pick (A_0, i_0, ψ_0) a descent of the CM abelian variety over a number field K Galois over E. If necessary, we can also increase K so that

$$\mathrm{Hom}^0_L(A_0^\sigma, A_0)$$

is non-zero.

Consider $\sigma|_K$. There are infinitely many places v of K such that $\mathrm{Fr}_v = \sigma|_K$, and so we can choose one v such that A_0 has good reduction at v. Let $\overline{A}_0$ denote the reduction at v. Let $w = v|_E$ and q be the size of residue field of E at w. There is a relative Frobenius isogeny

$$\mathrm{Fr}_q : \overline{A}_0 \to \overline{A}_0^{(q)},$$

where $\overline{A}_0^{(q)}$ is the appropriate Frobenius twist. By Lemma 2.6, Fr_q^{-1} lifts to a unique $\mathbb{Q}$-isogeny $\varphi_\sigma : A^\sigma \to A$. Note that the inverse is taken in the isogeny category. Note also it is unclear if one can lift Fr_q to an honest isogeny as we don't have a good control on integrality properties in the reduction map. This will be important to sort out later.

Since reduction is injective, the identity $\varphi_\sigma^\vee \circ \psi \circ \varphi_\sigma = a \cdot \psi^\sigma$ becomes

$$(\mathrm{Fr}_q^{-1})^\vee \circ \overline{\psi}_0 \circ \mathrm{Fr}_q^{-1} = a \cdot \mathrm{Fr}_q^{-1}(\overline{\psi}_0).$$

for some positive rational a. By some suitable rearrangement in the isogeny category, this is equivalent to

$$\mathrm{Fr}_q^\vee \circ \overline{\psi}^{(q)} \circ \mathrm{Fr}_q = a\overline{\psi}$$

for some polarization $\overline{\psi}$ of $\overline{A_0}$, where we take a to be $1/q$. It is a technical fact that the reduction of a polarization is still a polarization.

Replacing $\overline{\psi}$ by a suitable positive multiple, we can assume $\overline{\psi} = \psi_{\mathcal{L}}$ for a an ample line bundle $\mathcal{L}$ on $\overline{A}_0$. In the end, it boils down then to the following identity

$$\mathrm{Fr}_q^*(\mathcal{L}^{(q)}) \cong \mathcal{L}^{\otimes q}$$

which follows from the Cech description of line bundles for example. □

Corollary 2.9. *The L-linear isogeny φ_σ constructed in Th'm 2.8 is unique up to left multiplication by $c \in L^\times$ such that $Nm_{L/L^+}(c) \in \mathbb{Q}^\times$.*

Proof. Let $c \in L$ and consider the isogeny $i(c) \circ \varphi_\sigma$. We have

$$\varphi_\sigma^\vee \circ i(c)^\vee \circ \psi \circ i(c) \circ \varphi_\sigma = \varphi_\sigma^\vee \circ \psi \circ \varphi_\sigma \circ i_\sigma(cc^*) = q\psi^\sigma \circ i_\sigma(cc^*)$$

where we use the $i(c)^\vee = i^\vee(c^*)$ and L-linearity everywhere. If $q\psi^\sigma \circ i_\sigma(cc^*) = q'\psi^\sigma$, then $cc^* = q'/q \in \mathbb{Q}^\times$. □

Remark 2.10. The set of c above are the $\mathbb{Q}$ points of a torus T as follows: The norm map is an algebraic homomorphism $\underline{L}^\times \to (\underline{L}^+)^\times$. The algebraic group $\mathbb{G}_m = \underline{\mathbb{Q}}^\times$ is naturally a closed subgroup of $(\underline{L}^+)^\times$. We define the algebraic torus T to be the inverse image of $\mathbb{G}_m$ under the map Nm_{L/L^+}. Working over $\overline{\mathbb{Q}}$ shows that his inverse image is connected, so that it is a torus. Thus, φ_σ is well-defined up to the left multiplication by $T(\mathbb{Q})$.

3. Algebraic Main Theorem

Our goal, recall, is to describe the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ on adelic Tate module $V_f(A)$. In order to describe it however, we had to make an auxiliary choice of a certain L-linear $\mathbb{Q}$-isogeny $\varphi_\sigma : A^\sigma \to A$.

The compositve $V_f(\varphi_\sigma) \circ [\sigma] \in \mathrm{Aut}_L(V_f(A))$ so in fact is $\mathbb{A}_{L,f}$-linear for the natural $\mathbb{A}_{L,f}$ action on $V_f(A)$. We saw in Mike's talk that in each factor $V_\ell(A)$, $L \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ was its own centralizer so a priori, $V_f(\varphi_\sigma) \circ [\sigma]$ gives rise to an element $c_\ell \in (L \otimes \mathbb{Q}_\ell)^\times$ for each ℓ. If $\varphi_\sigma \circ [\sigma]$ was an honest morphism (not just in the isogeny category), then c_ℓ would be integral at all ℓ. Since we want to allow φ_σ to have rational denominators, we end up with an element

$$\mu_{\sigma,\varphi_\sigma} \in \mathbb{A}_{L,f}^\times.$$

The elements $\mu_{\sigma,\varphi_\sigma}$ running over all σ and all φ describe the Galois action on (A, i). To remove the dependence on φ_σ, we have to take quotient of $\mathbb{A}_{L,f}^\times$. The set of isogenies φ_σ ia a torsor for $L^\times$ given by post-composition on A. Without doing any of the work of the previous section, we could have constructed a continuous homomorphism

$$\mu : \mathrm{Gal}(\overline{\mathbb{Q}}/E) \to L^\times \backslash \mathbb{A}_{L,f}^\times.$$

And if we were only interested in elliptic curves, this would work just fine. The technical difficulty which led us to the world of $\mathbb{Q}$-polarizations is that the target space for general L is not Hausdorff so even though μ is continuous, one CANNOT readily deduce that μ factors through the topological abelianization $\mathrm{Gal}(E^{\mathrm{ab}}/E)$ since the kernel need not be closed. Adding the polarization compatibility to φ_σ will force μ to factor through an algebraic subgroup $T \subset \underline{L}^\times$ for which we'll see that $T(\mathbb{Q})\backslash T(\mathbb{A}_f)$ is Hausdorff.

The algebraic main theorem then says that μ is determined by the reflex norm.

Example 3.1. Let $L = \mathbb{Q}(i, \sqrt{2})$ be the biquadratic CM field. Then, $L^\times$ contains the infinite subgroup $(3 + 2\sqrt{2})^n$ of units with norm 1. For any place v of L, these are element of $\mathcal{O}_v^\times$. For any modulus m on L, the subgroup $(\mathcal{O}_v/m_v)^\times$ is finite so an appropriate power of $3 + 2\sqrt{2}$ will be congruent to $1 \mod m_v$ for all v. Thus, $L^\times$ is not discrete in $\mathbb{A}_{L,f}^\times$ and hence the quotient is not Hausdorff. Note that if we included the complex places, we would not have this problem because $(3 + 2\sqrt{2})^n$ is very far from 1 in the archimedian norm.

Proposition 3.2. *Let ψ be a L-linear polarization of (A, i). The subgroup of $\mathbb{A}_{L,f}^\times = \underline{L}^\times(\mathbb{A}_f)$ which preserves e_ψ up to homothety is $T(\mathbb{A}_f)$ where T is the reflex torus defined in Remark 2.10.*

Proof. Let $\langle \cdot, \cdot \rangle$ denote the ordinary Weil pairing. By abuse of notation, we also use i to denote the linear extension of $i : L \to \mathrm{End}(V_f(A))$ to $\mathbb{A}_{L,f}$ together with the induced complex conjugation $c \mapsto c^*$. For $a \in \mathbb{A}_{L,f}$, consider that

$$e_\psi(i(a)x, i(a)y) = \langle i(a)x, \psi(ay)\rangle = \langle i(a)x, i^\vee(a)\psi(y)\rangle = \langle (i^\vee(a))^\vee ax, \psi(y)\rangle.$$

Using that $i^\vee(a) = (i(a^*))^\vee$, we get that

$$e_\psi(ax, ay) = e_\psi(i(a^* a)x, y)$$

Since e_ψ is $\mathbb{A}_f$-linear and non-degenerate, then this is a scalar times $e_\psi(x, y)$ iff $i(a^* a) \in \mathbb{A}_f$. And this exactly characterizes the points of $T(\mathbb{A}_f)$. ☐

The fact that φ_σ is compatible with the polarization ψ implies that $\mu_{\sigma,\varphi_\sigma}$ preserves e_ψ up to homothety with the scaling factor $\chi_f(\sigma)\deg(\varphi_\sigma)^{1/g} \in \mathbb{A}_{L,f}^\times$, where χ_f is the product over all the ℓ-adic cyclotomic characters. Thus, we have defined an element

$$\mu_{\sigma,\varphi_\sigma} \in T(\mathbb{A}_f).$$

Proposition 3.3. *The elements $\mu_{\sigma,\varphi_\sigma}$ define a continuous homomorphism*

$$\mu : \mathrm{Gal}(\overline{\mathbb{Q}}/E) \to T(\mathbb{Q})\backslash T(\mathbb{A}_f)$$

where the topology on the left comes from the topology on $\mathbb{A}_{L,f}^\times$.

Proof. See CM book [2] Lemma A.2.4.1. The fact that it is a homomorphism is a diagram chase. Continuity follows from continuity of the action of the Galois group on the Tate module for any chosen descent (A_0, i_0) of A. □

The following key technical lemma is the main reason for introducing polarizations to the mix:

Lemma 3.4. *The quotient* $T(\mathbb{Q})\backslash T(\mathbb{A}_f)$ *with the topology induced from* $\mathbb{A}_{L,f}^\times$ *is Hausdorff.*

Proof. This is Lemma A.2.4.2 in the CM book [2] whose proof we follow closely. We will show that $T(\mathbb{Q})$ is discrete in $T(\mathbb{A}_f)$.

It is clear that $\mathbb{G}_m = \underline{\mathbb{Q}} \subset T$ so we can consider the exact sequence of algebraic groups over $\mathbb{Q}$

$$1 \to \mathbb{G}_m \to T \to \overline{T} \to 1.$$

If we assume the $\overline{T}(\mathbb{Q}) \subset \overline{T}(\mathbb{A}_f)$ is discrete, then any sequence in $T(\mathbb{Q})$ approaching 1 has an image in $\overline{T}(\mathbb{Q})$, which stabilizes to 1. Thus, we get a sequence in $\mathbb{Q}^\times$ approaching 1 in $\mathbb{A}_f^\times$, but $\mathbb{Q}^\times$ intersects the compact open given by integral elements at all places in $\{\pm 1\}$ so that sequence must actual stabilize to 1 so $T(\mathbb{Q})$ is discrete.

As we mentioned before, if we use the full ideles then there is no issue, so $\overline{T}(\mathbb{Q}) \subset \overline{T}(\mathbb{A}) = \overline{T}(\mathbb{R}) \times \overline{T}(\mathbb{A}_f)$ is discrete. Assume $\overline{T}(\mathbb{R})$ is compact. Then, for any sequence $x_n \in \overline{T}(\mathbb{Q})$ which is converging to 1 in $\overline{T}(\mathbb{A}_f)$, we can consider the projection onto $\overline{T}(\mathbb{R})$. By compactness, there is subsequence x_{n_i} which converges in $\overline{T}(\mathbb{R})$ so x_{n_i} converges in $T(\mathbb{A})$ and hence it becomes constant.

Hilbert Th'm 90 tells us that $T(\mathbb{R})/\mathbb{R}^\times\ \overline{T}(\mathbb{R})$ is a topological isomorphism. The group $T(\mathbb{R})$ is the closed subgroup of elements

$$(z_1, \dots, z_g) \in \prod_{L^+ \subset \mathbb{R}} (L \otimes_{L^+} \mathbb{R})^\times$$

whose image under Nm_{L/L^+} lies in the diagonal $\mathbb{R}^\times$. This is identified with the subgroup of points in $(\mathbb{C}^\times)^g$ such that $|z_i| = |z_j|$ for all i, j. Any such g-tuples can be scaled by an element of $\mathbb{R}^\times$ so that $|z_i| = 1$ for all i. Thus, $T(\mathbb{R})/\mathbb{R}^\times$ is a quotient of $(S^1)^g$ and hence is compact.

□

Corollary 3.5. *The map* μ *factors through the topological abelianization* $\mathrm{Gal}(E^{ab}/E)$. *Furthermore, using the reciprocity map (arithmetic normalization) of global class field theory, we get a group homomorphism*

$$\mu : E^\times \backslash \mathbb{A}_{E,f}^\times \twoheadrightarrow \mathrm{Gal}(E^{ab}/E) \to T(\mathbb{Q})\backslash T(\mathbb{A}_f).$$

Proof. The fact that we still get a surjection using just the finite ideles follows from the fact that E is CM and hence has no real places so the infinite part is connected. □

Finally, we can state the main theorem.

Theorem 3.6. *The map μ is induced by $s \mapsto N_\Phi(s)^{-1} \in T(\mathbb{A}_f)$, where $N_\Phi : \underline{E}^\times \to \underline{L}^\times$ is the reflex norm.*

3.1. **Reflex Norm and Reflex Torus.** We review these two key concepts and in particular show that reflex norm N_Φ factors through the reflex torus T defined in Remark 2.10.

Remark 3.7. None of this is perceived in the case of elliptic curves and imaginary quadratic fields because $T = \underline{L}^\times$.

Associated to (L, Φ), we have seen in a previous lecture that we get a vector space t_Φ over E of dimension g, which is the tangent space of a hypothetical abelian variety over E with CM-type (L, Φ) which may not exist. It has the property that

$$t_\Phi \otimes_E \overline{\mathbb{Q}} = \oplus_{\varphi \in \Phi} \overline{\mathbb{Q}}_\varphi$$

as a $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} L$-module.

Definition 3.8. The *reflex norm* is the algebraic map

$$N_\Phi : \underline{E}^\times \to \underline{L}^\times,$$

which is given on $\mathbb{Q}$-points by $e \mapsto \det_L(e \mid t_\Phi)$.

Example 3.9.

1. If L is an imaginary quadratic field and $\varphi : L \to \overline{\mathbb{Q}}$ is an embedding which gives Φ, then $E = \varphi(L)$. The tangent space t_Φ is just one-dimensional over L and so $N_\Phi = \varphi^{-1} : E \to L$.
2. Let $L = \mathbb{Q}(\zeta_7)$ and $\Phi = \{\varphi_1, \varphi_2, \varphi_3\}$, then we saw that $E = \mathbb{Q}(\zeta_7) \subset \overline{\mathbb{Q}}$. Then t_Φ has dimension 3 over L and the reflex norm $N_\Phi : \underline{E}^\times \to \underline{L}^\times$ is given by

$$e \mapsto \varphi_1^{-1}(e)\varphi_2^{-1}(e)\varphi_3^{-1}(e).$$

3. Let $L = \mathbb{Q}(\zeta_7)$ and $\Phi = \{\varphi_1, \varphi_2, \varphi_4\}$, then we saw that $E = \mathbb{Q}(\sqrt{-7})$. Since t_Φ is dim 3 over E, it must be 1 dim over L. Thus, N_Φ is given by a single embedding $\varphi : \mathbb{Q}(\sqrt{-7}) \hookrightarrow \mathbb{Q}(\zeta_7)$. Which one? Well $\varphi_1^{-1}, \varphi_2^{-1}$, and φ_4^{-1} all induce the same map on $\mathbb{Q}(\sqrt{-7})$ so the common restriction of those three.

Looking at the above examples, one notices that

$$\mathrm{Nm}_{L/L^+} \circ N_\Phi = \mathrm{Nm}_{E/\mathbb{Q}}.$$

This holds in general (see CM book [2] Prop 2.1.4.6). We could have done the above construction with any subset of embedding, but this particular property is special to the case of a CM-type.

It is clear then that N_Φ lands in the torus preimage of $\underline{\mathbb{Q}}^\times \subset \underline{L}^\times$, which is our reflex torus T or T_Φ.

4. Applications: Alg Main Th'm implies Classical Main Th'm

In this section, we apply the algebraic form of the main th'm to deduce some nice results for CM abelian varieties. For a given descent (A_0, i_0) of $A/\overline{\mathbb{Q}}$, we will construct from μ, the algebraic Hecke character ε discussed last lecture.

The main theorem says that μ is induced by N_Φ. We begin by reversing the construction of μ a bit.

Proposition 4.1. *For all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E)$ and $s \in \mathbb{A}_{E,f}^\times$ such that $r_E(s) = \sigma|_{E^{\mathrm{ab}}}$, there exist a unique L-linear isogeny $\varepsilon_{\sigma,s} : (A, i) \to (A^\sigma, i^\sigma)$ such that*

$$[\sigma] = V_f(\varepsilon_{\sigma,s}) \cdot N_\Phi(s^{-1}).$$

Proof. By the main th'm, N_Φ^{-1} is identified modulo $T(\mathbb{Q})$ with the map given by μ. Thus, as an element of $T(\mathbb{A}_f) \subset \mathbb{A}_{L,f}^\times$, $N_\Phi(s^{-1})$ lies in the coset for $T(\mathbb{Q}) \subset L^\times$ given by $\{\mu_{\sigma,\varphi_\sigma}\}$ running over all $\varphi_\sigma : A^\sigma \to A$ which are compatible with the polarization.

Thus, $N_\Phi(s^{-1}) = \mu_{\sigma,\varphi_\sigma}$ for some φ_σ and so we can take $\varepsilon_{\sigma,s} = \varphi_\sigma$. □

Note immediately the similarity of form between

$$[\sigma] = V_f(\varepsilon_{\sigma,s}) \cdot N_\Phi(s^{-1})$$

and Mike's formula

$$\phi_\ell(\sigma) = \varepsilon(a) \cdot \varepsilon_{\mathrm{alg}}(a_\ell^{-1}).$$

Let $K \subset \overline{\mathbb{Q}}$ be a number field such that $A/\overline{\mathbb{Q}}$ descends to an abelian variety (A_0, i_0) over K so in particular $E \subset K$. Let $\sigma \in G_K$, and consider any $a \in \mathbb{A}_{K,f}^\times$ such that $r_K(a) = \sigma|_{K^{\mathrm{ab}}}$. Functoriality of the reciprocity maps says that $a_E = \mathrm{Nm}_{K/E}(a)$ maps to $\sigma|_{E^{\mathrm{ab}}}$ under r_E.

Now, by the previous proposition, we have an isogeny $\varepsilon_{\sigma,a_E} : A^\sigma = A \to A$ such that

$$V_f(\sigma) = \varepsilon_{\sigma,a_E} \cdot (N_\Phi \circ \mathrm{Nm}_{K/E}(a^{-1})).$$

As we have seen multiple times in this seminar, the Galois action on $V_f(A_0)$ is abelian so the left side only depends on $\sigma|_{K^{\mathrm{ab}}}$ and thus only on a. Thus, in fact, ε_{σ,a_E} only depends on a, denote this then by ε_a.

Theorem 4.2. *For K, (A_0, i_0) as above. The map*

$$a \in \mathbb{A}_{K,f}^{\times} \mapsto \varepsilon_a$$

is an algebraic Hecke character with algebraic part $N_\Phi \circ Nm_{K/E}$.

Proof. Note that implicitly we are setting $\varepsilon(a)$ be the unique $k \in L$ such that $\varepsilon(a) = i(k)$. As an endomorphism of A, $\varepsilon(a)$ is determined by what it does on the ℓ-adic Tate module for any individual ℓ. The formula

$$V_\ell(r_K(a)) \cdot (N_\Phi \circ \mathrm{Nm}_{K/E}(a_\ell)) = \varepsilon(a)$$

makes it clear that ε is a homomorphism and since r_K is trivial on $K^\times$, it is also clear what $\varepsilon_{\mathrm{alg}}$ is. The only thing to check then is the ε is continuous where L is given the discrete topology.

Again considering the formula above show, we see that ε is continuous for the topology of $L^\times$ as a subset of $L_\ell^\times$. This tells us that for a small open subgroup U, $\varepsilon(U) \cong 1 \mod \ell^n$. We want to show that perhaps by shrinking U further we get $\varepsilon(U) = 1$. The idea is to show that $\varepsilon(a)$ is finite order for $a \in U' \subset U$.

Roughly by extending L and shrinking U, we can force $\varepsilon(a)$ to be compatible with a polarization. By analyzing the degree of $\varepsilon(a)$, which is controlled by the congruence class of a, we find that the rational multiplier is 1 so $\varepsilon(a)$ commutes with polarization. Any automorphism which respects a polarization if finite order. □

We have constructed Mike's algebraic Hecke character. Note the ε should perhaps be ε_{A_0}, because it really depends on the particular descent A_0. It is not hard to see that the algebraic part does not depend on the embedding $K \subset \overline{\mathbb{Q}}$, but the full ε does. The last thing to check is that it satisfies property (v), compatibility at good places.

Theorem 4.3. *(CM Book* [2] *A.2.5.9) For (A_0, i_0) a CM abelian variety over a number field $K \subset \overline{\mathbb{Q}}$. Let ε be the associated algebraic Hecke character on $\mathbb{A}_K^\times$ which is trivial on $K_\infty^\times$. Pick a prime $\mathfrak{p}$ of K.*

1. *The abelian variety has good reduction at $\mathfrak{p}$ of K if and only if $\varepsilon_{\mathfrak{p}}$ is trivial on $\mathcal{O}_{\mathfrak{b}}^\times$.*
2. *For a prime $\mathfrak{b}$ of good reduction, the element $\varepsilon(\pi_{\mathfrak{p}}) \in L^\times$ reduced to the Frobenius over $\kappa(\mathfrak{p})$ under the reduction of A_0 modulo $\mathfrak{p}$.*

Proof. Choose a prime ℓ not dividing $\mathfrak{p}$. By Neron-Ogg-Shafarevich, it suffices to show that ε is trivial on $\mathcal{O}_{\mathfrak{p}}^\times$ if and only if ϕ_ℓ is trivial on inertia. If r_K is Artin reciprocity map, then our formula says

$$\phi_\ell(r_K(a)) = \varepsilon(a) \cdot \varepsilon_{\mathrm{alg}}(a_\ell^{-1})$$

for any finite idele $a \in \mathfrak{a}_{K,f}^{\times}$. For $a \in \mathcal{O}_{\mathfrak{p}}^{\times}$, $a_\ell = 1$ so we get

$$\phi_\ell(r_K(a)) = \varepsilon(a)$$

so ε is trivial on $\mathcal{O}_{\mathfrak{p}}^{\times}$ iff ϕ_ℓ is trivial on $r_K(\mathcal{O}_{\mathfrak{p}}^{\times}) = I_{\mathfrak{p}}$.

Use the same ℓ as above. The reciprocity map under our normalization sends $r_K(\pi_{\mathfrak{p}})$ to the arithmetic Frobenius map $\mathrm{Fr}_{\mathfrak{p}}$. Again, $(\pi_{\mathfrak{p}})_\ell = 1$ so

$$\varepsilon(\pi_{\mathfrak{p}}) = \phi_\ell(\mathrm{Fr}_{\mathfrak{p}})$$

acting on the ℓ-adic rational Tate module. The relative Frobenius isogeny $\mathrm{Fr}_{\kappa(\mathfrak{p})}$ of the reduction $\overline{A}_0$ also acts on the ℓ-adic Tate module by Frobenius. The reduction map is injective as is the inclusion $\mathrm{End}(A) \hookrightarrow \mathrm{End}(V_\ell(A))$ so we must have that $\varepsilon(\pi_{\mathfrak{p}})$ reduces to the Frobenius map. ☐

References

[1] D. Mumford, *Abelian varieties*, Oxford Univ. Press, 1970.

[2] C-L. Chai, B. Conrad, F. Oort, *CM Liftings*, currently at math.stanford.edu/ conrad/papers/CMbook.pdf.