CONSTRUCTIONS WITH FRACTIONAL IDEALS

JEREMY BOOHER

In preparation for the proof of the Main Theorem of Complex Multiplication, for an Abelian variety A_0 over K with CM type (Φ, L) we need to construct an isomorphism θ so that

$$\begin{array}{ccc} A_0 & \xrightarrow{\xi_{\sigma,\mathfrak{P}}} & A_0^\sigma \\ & \searrow & \uparrow \theta \\ & & N_\Phi(\mathfrak{p})^{-1} \otimes_{\mathcal{O}_L} A_0 \end{array}$$

This talk will explain what all of the objects in this commutative diagram are, and construct θ. Most of the material comes from Section A.2.6 of the draft CM lifting book [1].[1]

1. The Serre Tensor Construction

The first thing we need to do is make sense of the tensor product of an Abelian variety with CM by $\mathcal{O}_L$ with a finitely generated projective $\mathcal{O}_L$-module. This is an example of the Serre tensor construction.

1.1. **The Construction.** Before discussing the general construction, let us look at the situation over the complex numbers.

Example 1. Let A be an Abelian variety over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_L$. Write $A = V/\Lambda$ where V is a complex vector space and Λ is a lattice in V. Let M be a projective, finitely generated $\mathcal{O}_L$ module. Observe that $M \otimes_{\mathcal{O}_L} V$ is a finite dimensional complex vector space, and $M \otimes_{\mathcal{O}_L} \Lambda$ is a lattice in it. If M is a free module, this is obvious. Otherwise, there is a module N so that $M \oplus N = \mathcal{O}_L^n$, and hence $M \otimes_{\mathcal{O}_L} V$ is a sub-vector space of a finite dimensional complex vector space $\mathcal{O}_L^n \otimes_{\mathcal{O}_L} V$. Likewise, $M \otimes_{\mathcal{O}_L} \Lambda$ sits inside the lattice $\mathcal{O}_L^n \otimes_{\mathcal{O}_L} \Lambda$. Then $A' = (M \otimes_{\mathcal{O}_L} V)/(M \otimes_{\mathcal{O}_L} \Lambda)$ is a complex torus. In fact, it is also the analytification of an Abelian variety. A' is a direct factor of the Abelian variety $\mathcal{O}_L^n \otimes_{\mathcal{O}_L} A = A^n$, so A' is an analytic submanifold of a complex projective manifold. By GAGA, it is algebraic.

Note that the $\mathbb{C}$-valued points of A are just V/Λ, and since M is flat (it is assumed projective),

$$M \otimes_{\mathcal{O}_L} V/\Lambda \simeq A'.$$

In general, let R be a ring, A a R-module scheme over S (an S group scheme with the additional structure of an R-action), and let M be a finitely generated projective R-module. The Serre tensor construction makes sense of $M \otimes_R A$.

Theorem 2. *The functor that sends an S-scheme T to $M \otimes_R A(T)$ is representable by an R-module scheme over S.*

The representing object is denoted $M \otimes_R A$.

Date: May 17, 2012, updated May 23, 2012.

[1]I would like to thank Brian Conrad, Sam Lichtenstein, and Daniel Litt for helpful discussions and advice.

Proof. It is clear that if $M = R^n$, then the functor is represented by A^n.

In general, $M^\vee = \mathrm{Hom}(M, R)$ is finitely generated and projective as M is, and hence finitely presented. Write

$$R^m \to R^n \to M^\vee \to 0.$$

Apply $\mathrm{Hom}_R(\cdot, A(T))$ to get the short exact sequence

$$0 \to \mathrm{Hom}_R(M^\vee, A(T)) \to \mathrm{Hom}_R(R^n, A(T)) \to \mathrm{Hom}_R(R^m, A(T)).$$

Identifying these with tensor products, we have a short exact sequence

$$0 \to M \otimes_R A(T) \to R^n \otimes_R A(T) \to R^m \otimes_R A(T).$$

Thus the functor sending T to $M \otimes_R A(T)$ is representable as it the kernel of a homomorphism between these two representable group functors. □

The Serre tensor construction is very well behaved. Most properties of A are inherited by $M \otimes_R A$, and the proofs tend to be simple given either the construction as a kernel or realizing a projective module as a direct summand of a free module. For example, if A is flat then $M \otimes_R A$ is flat as well [1, 1.7.4]. Other important properties that are preserved include smoothness, properness, and geometric connectedness of fibers. Furthermore, at least in the smooth case, the dimension of $M \otimes_R A$ is the $\mathcal{O}_L$ rank of M times the dimension of A, as can be seen through a computation with tangent spaces.

An important observation we will need later is about base change.

Example 3. Let T be an S-scheme and X a T-scheme. Then

$$(M \otimes_R A)_T(X) = \mathrm{Hom}_S(X, M \otimes_R A) = M \otimes \mathrm{Hom}_S(X, A) = M \otimes A_T(X)$$

so $(M \otimes_R A)_T = M \otimes_R A_T$.

Remark 4. There are also variants of the Serre tensor construction that work for non-projective modules when the base scheme S is a field [1, Proposition 1.7.4.3].

1.2. **Application to CM Abelian Varieties.** Let $(A, \imath)$ and $(A', \imath')$ be Abelian varieties defined over the field K with complex multiplication by L. Assume that $\mathcal{O}_L$ lies in the endomorphism ring of A and A', and that there exists a non-zero $\mathcal{O}_L$-linear map $A' \to A$. (Recall that in practice we can reduce to the case that the complex multiplication is by the maximal order, and that in characteristic 0 over an algebraically closed field the existence of the non-zero $\mathcal{O}_L$ linear map is equivalent to the CM types coinciding - see Proposition 1.5.4.1 of [1]). We are interested in looking at $M := \mathrm{Hom}((A', \imath'), (A, \imath))$ and the evaluation map $M \otimes_{\mathcal{O}_L} A' \to A$.

Proposition 5. *With the notation above, M is an invertible $\mathcal{O}_L$-module, unchanged by extension of the ground field K. If the characteristic of K is zero, the evaluation map $M \otimes_{\mathcal{O}_L} A' \to A$ is an isomorphism.*

Remark 6. If the characteristic of K is not zero, the evaluation map need not be an isomorphism. An example is given in Example 1.7.4.1 of [1].

Proof. Consider $M_{\mathbb{Q}} = \mathrm{Hom}^0((A', \imath'), (A, \imath))$. We claim it is a one dimensional L vector space. It is non-zero by assumption. Denote the ℓ-adic Tate vector space of A by $V_\ell(A)$. For a prime not equal to the characterstic of K, we know that $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} M_{\mathbb{Q}} \to \mathrm{Hom}_{L_\ell}(V_\ell(A'), V_\ell(A))$ is injective. (For a proof, see Theorem 3 of section 19 of [3].) But $\mathrm{Hom}_{L_\ell}(V_\ell(A'), V_\ell(A))$ is a free module of rank 1 over L_ℓ, which forces $M_{\mathbb{Q}}$ to have dimension exactly one as an L vector space.

Now M is a finitely generated torsion free module. It therefore injects into $M_{\mathbb{Q}} \simeq L$, and hence can be identified with a fractional ideal. Therefore M is invertible.

Now let K_s be the separable closure of K, and consider the map

$$M = \mathrm{Hom}((A', \imath'), (A, \imath)) \to \mathrm{Hom}((A'_{K_s}, \imath'), (A_{K_s}, \imath)).$$

It is clearly injective. The image will have finite index: tensor with $\mathbb{Q}$ over $\mathbb{Z}$, and note that both are one dimensional L-vector spaces. Let n be the index. Let $f : A'_{K_s} \to A_{K_s}$ be an L-linear homomorphism. Because nf is defined over K, f is $\mathrm{Gal}(K_s/K)$ equivariant, so the index is one and M is unchanged by extending to the separable closure. For a general field extension, use Chow's lemma, which says the group of homomorphisms is under field extension of a separably closed field.

Now assume that $\mathrm{char}(K) = 0$. We may reduce to the case that $K = \mathbb{C}$ to show that $M \otimes_{\mathcal{O}_L} A' \to A$ is an isomorphism. Using our understanding of CM over the complex numbers, write $A(\mathbb{C}) = (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi/\mathfrak{a}$ and $A'(\mathbb{C}) = (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi/\mathfrak{a}'$ where Φ is the CM type and $\mathfrak{a}$ and $\mathfrak{a}'$ are fractional ideals of $\mathcal{O}_L$. Then $\mathcal{O}_L$-linear homomorphisms are just the endomorphisms of $\mathbb{R} \otimes_{\mathbb{Q}} L$ coming from multiplication by $c \in L$ with $c\mathfrak{a}' \subset \mathfrak{a}$. Thus $M = \mathrm{Hom}_{\mathcal{O}_L}(\mathfrak{a}', \mathfrak{a}) = \mathfrak{a}\mathfrak{a}'^{-1}$. Then the map $M \otimes_{\mathcal{O}_L} A' \to A$ on $\mathbb{C}$ valued points sends $c \otimes x \in \mathfrak{a}\mathfrak{a}'^{-1} \otimes (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi/\mathfrak{a}' \to cx \in (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi/\mathfrak{a}$. This is an isomorphism. To see this, recall that a map of complex tori is an isomorphism if it induces an isomorphism on the homology lattice. But the induced map is $M \otimes_{\mathcal{O}_L} \mathfrak{a}' \to \mathfrak{a}$ given by evaluation, which is clearly an isomorphism. □

The next proposition mimics another familiar property of tensor products.

Proposition 7. *With the notation above, and M any invertible $\mathcal{O}_L$-module, the natural map $M \to \mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A)$ is an isomorphism.*

We will prove this only in characterstic 0, and make some remarks about the general proof at the end. For now, we only need this result for number fields, but later it will be essential to apply it over finite fields.

Proof. Assume that K is a field of characteristic 0. Note that $M \otimes_{\mathcal{O}_L} A$ is an Abelian variety with CM structure coming from A. It is the same dimension as A because M is invertible. The natural map in the statement is the one sending m to the map $e_m : A \to M \otimes_L A$ which sends $x \to m \otimes x$. Observe that e_m is not the zero map by looking at the associated map on Tate modules, which is manifestly non-zero. Thus $\mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A)$ is non-zero, so Proposition 5 implies it is an invertible $\mathcal{O}_L$ module as well.

Now the natural map $M \to \mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A)$ is certainly injective, so the image is of finite index as the target is invertible. To show it is an isomorphism as claimed, we will show it is an isomorphism after tensoring with $\mathbb{Z}_\ell$, which shows that ℓ cannot divide the index. We do this again by embedding in the Tate modules, which is where we need ℓ to not equal the characteristic of K. Consider the composition

$$M_\ell \to \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A) \to \mathrm{Hom}_{\mathcal{O}_{L,\ell}}(T_\ell A, M_\ell \otimes_{\mathcal{O}_{L,\ell}} T_\ell A).$$

The second map is known to be injective. In addition, the composition is obviously injective (it sends $m \to [a \to m \otimes a]$). Therefore the first map is automatically injective, and to show it is surjective it suffices to show the composite map is surjective. Since M_ℓ is a free rank 1 $\mathcal{O}_{L,\ell}$ module, we can choose a basis and identify $M_\ell \otimes_{\mathcal{O}_{L,\ell}} T_\ell A$ with $T_\ell A$ and check that the natural map

$$\mathcal{O}_{L,\ell} \to \mathrm{End}_{\mathcal{O}_{L,\ell}}(T_\ell A)$$

is an isomorphism. Since $T_\ell A$ is free of rank 1 over $\mathcal{O}_{L,\ell}$, this is immediate. □

If $\ell = \mathrm{char}(K)$, a more complicated argument is needed using Dieudonné modules and ℓ-divisible groups. Details are found in Example 1.7.4.1 and Proposition 1.2.5.1 of [1].

2. The Reflex Norm and Fractional Ideals

The goal of this section is to extend the reflex norm to the group of fractional ideals, and find a way to compute with it. Inspiration is taken from Milne's draft of a book on complex multiplication [2].

Let (Φ, L) be a CM type of an Abelian variety. Recall that the reflex field E was defined to be the fixed field of the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ stabilizing Φ. There is a $L \otimes_{\mathbb{Q}} E$ module t_Φ that is a descent to E of the $L \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$-module $V_\Phi = \prod_{\varphi \in \Phi} \overline{\mathbb{Q}}$, where $c \in L$ acts on the φ factor through multiplication by $\varphi(c)$. It should be thought of as the tangent space to an Abelian variety defined over E with CM type Φ, although such an Abelian variety in general does not exist.

The reflex norm is a map between the tori

$$N_\Phi : \mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_m) \to \mathrm{Res}_{L/\mathbb{Q}}(\mathbb{G}_m).$$

On a $\mathbb{Q}$-algebra R, with $c \in E_R^\times$, the norm is the L_R linear determinant of multiplication by c on $t_\Phi \otimes_{\mathbb{Q}} R$, an element of $L_R^\times$. Taking $R = \mathbb{Q}$, this gives the important case $N_\Phi : E^\times \to L^\times$.

We are interested in the reflex norm $N_\Phi : \mathbb{A}_E^\times \to \mathbb{A}_L^\times$. This arises by taking $R = \mathbb{A}_{\mathbb{Q}}$, since $\mathbb{A}_F = \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} F$. We want to descend this to a map of fractional ideals, which requires us to understand the behavior on ideles all of whose components are integral units. One approach involves putting a $\mathbb{Z}[\frac{1}{N}]$ module structure on t_Φ via descent, which is also useful in an alternate proof of Theorem 13 [1, A.2.6].

Instead, we will give a direct argument. Define

$$U_F = \prod_{v \text{ finite}} \mathcal{O}_{F_v}^\times,$$

and note that U_F is a compact open subgroup of $\mathbb{A}_{F,f}^\times$ that contains every compact subgroup. Now general facts about adelic points of algebraic groups imply that the reflex norm induces a continuous map $\mathbb{A}_{E,f}^\times \to \mathbb{A}_{L,f}^\times$, so the image of U_E is compact and hence contained in U_F. So if we let I_F denote the group of fractional ideals of the field F, the reflex norm gives a map

$$\mathbb{A}_{E,f}^\times \to \mathbb{A}_{L,f}^\times \to I_L$$

that factors through U_E. Thus the reflex norm gives a well-defined homomorphism

$$N_\Phi : I_E \to I_L.$$

We would also like a more concrete description of the reflex norm in special cases. Strangely, this can be done by generalizing it.

Let K be a Galois extension of $\mathbb{Q}$ containing all of the embeddings of L into $\overline{\mathbb{Q}}$. We will extend the reflex norm to K by mimicking the usual construction:

$$N_{K,\Phi} : \mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_m) \to \mathrm{Res}_{L/\mathbb{Q}}(\mathbb{G}_m)$$

where for a $\mathbb{Q}$-algebra R, the norm of $c \in K_R^\times$ is the determinant of the multiplication by c map on $(K \otimes_E t_\Phi) \otimes_{\mathbb{Q}} R$. Essentially, we don't descend V_Φ all the way from $\overline{\mathbb{Q}}$ to E, instead stopping at $K \supset E$. The advantage of this extension is that $N_{K,\Phi}$ has a much more explicit description on $K^\times$, while maintaining compatibility with N_Φ. Both of the following Propositions come from the discussion of the reflex norm in Milne's notes [2].

Proposition 8. *This extended reflex norm satisfies $N_{K,\Phi} = N_\Phi \circ N_{K/E}$.*

It should be noted that since $N_{K/E}$ is surjective on the level of algebraic groups, this determines the reflex norm as a map of tori.

Let R be a $\mathbb{Q}$-algebra, and $\varphi \in \Phi$ an embedding of L into K. Denote the map $N_{K/\varphi(L)} \otimes 1 : K \otimes_{\mathbb{Q}} R \to \varphi(L) \otimes_{\mathbb{Q}} R$ by $N_{K/\varphi(L),R}$. Now $\varphi \otimes 1$ is an isomorphism $L \otimes_{\mathbb{Q}} R \simeq \varphi(L) \otimes_{\mathbb{Q}} R$. For $b \in \varphi(L) \otimes_{\mathbb{Q}} R$, denote the (unique) pre-image by $\varphi^{-1}(b)$.

Proposition 9. *For any $a \in (K_R)^\times$,*

$$N_{K,\Phi}(R)(a) = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/\varphi(L),R}(a)).$$

We will prove the second and leave the first as an exercise.

Proof. $N_{K,\Phi}(R)(a)$ is the determinant of multiplication by a map (as a L_R-linear map) on the $K \otimes_{\mathbb{Q}} L$ module $K \otimes_E t_\Phi \otimes_{\mathbb{Q}} R$. But $K \otimes_E t_\Phi$ is isomorphic to $\prod_{\varphi \in \Phi} K_\varphi$, where L acts on K_φ via φ since extending scalars to $\overline{\mathbb{Q}}$ gives V_Φ. Note a acts on each of the factors $K_\varphi \otimes_{\mathbb{Q}} R$ independently. As an L-module, K_φ has a strange action, but K_φ is a $\varphi(L)$ module with the normal action on K coming from the inclusion of fields. Since the norm from K to $\varphi(L)$ is given by the determinant of the multiplication map,

$$\det(m_a : K_\varphi \otimes_{\mathbb{Q}} R \to K_\varphi \otimes_{\mathbb{Q}} R) = \varphi^{-1} N_{K/\varphi(L),R}(a).$$

Multiplying over $\varphi \in \Phi$ proves the proposition. □

Let $\mathfrak{a}$ be a fractional ideal of E, h the class number of $\mathcal{O}_E$, and $n = [K : E]$. Raising any ideal to the h power makes it principal. So writing $\mathfrak{a}^h = (\beta)$ for $\beta \in E$, the functoriality of the reflex norm shows $N_\Phi(\mathfrak{a})^h = N_\Phi(\beta)$, where the left is the reflex norm on fractional ideals and the right is on elements of $E^\times$. If we further raise to the nth power, β^n is a norm from K to E, so the two propositions give a more explicit formula:

$$N_\Phi(\mathfrak{a})^{nh} = N_{K,\Phi}(\beta) = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/\varphi(L)}(\beta))$$

Since the number field norm can also be defined on ideals of K, and is compatible with the norm of elements,

$$N_\Phi(\mathfrak{a})^{nh} = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/\varphi(L)}(\mathfrak{a}^h))$$

Since there is unique prime factorization of fractional ideals, we can conclude:

Corollary 10. *With the notation above,*

$$N_\Phi(\mathfrak{a})^{n} = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/\varphi(L)}(\mathfrak{a}))$$

and that for any place v of L

$$\operatorname{ord}_v N_\Phi(\mathfrak{a}) = \frac{1}{n} \sum_{\varphi \in \Phi} \operatorname{ord}_v \varphi^{-1}(N_{K/\varphi(L)}(\mathfrak{a})).$$

Example 11. Note that this matches the cases of the reflex norm that Brandon gave in his talk. For example, if $L = \mathbb{Q}(\zeta_7)$ and $\Phi = \{\varphi_1, \varphi_2, \varphi_3\}$ with $\varphi_i(\zeta_7) = \zeta_7^i$, then we had that $E = L$. We can take $K = L$, so φ_i are isomorphisms and

$$N_\Phi(a) = \varphi_1^{-1}(a)\varphi_2^{-1}(a)\varphi_3^{-1}(a).$$

3. Hom Modules and Fractional Ideals

Let $(A, \imath)$ be an Abelian variety defined over $\overline{\mathbb{Q}}$ with complex multiplication such that $\imath^{-1}(\operatorname{End}(A)) = \mathcal{O}_L$ and CM type Φ. Pick $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/E)$.

As discussed in Brian's talks, descend A to an Abelian variety $(A_0, \imath_0)$ defined over a finite Galois extension $E \subset K \subset \overline{\mathbb{Q}}$ preserving the CM structure. Choose a large enough K so it contains all of the Galois conjugates of L, is Galois over $\mathbb{Q}$, and so $\operatorname{Hom}((A_0, \imath_0), (A_0^\sigma, \imath_0^\sigma))$ is non-zero (as the CM types are the same, there is some homomorphism over $\overline{\mathbb{Q}}$). Now we know that

$$\operatorname{Hom}((A_0, \imath_0), (A_0^\sigma, \imath_0^\sigma)) = \operatorname{Hom}((A, \imath), (A^\sigma, \imath^\sigma))$$

and that this is an invertible $\mathcal{O}_L$ module according to Proposition 5. Denote it as $\mathfrak{a}_\sigma$: note this is only an $\mathcal{O}_L$ module, not yet a fractional ideal.

Now let $\mathfrak{P}$ be a prime of K over a rational prime $p \nmid N$ such that $\sigma|_K = \left(\frac{K/E}{\mathfrak{P}}\right)$. Let $\mathfrak{p}$ be a prime of E below $\mathfrak{P}$. Note that $\mathfrak{P}$ is unramified as $p \nmid N$.

Lemma 12. *For $n \geq 1$, there is a unique L-linear K homomorphism of Abelian varieties $\xi_{\sigma,n,\mathfrak{P}} : A_0 \to A_0^{\sigma^n}$ that reduces to the q^n-power Frobenius morphism over $k(\mathfrak{P})$, where $q = |k(\mathfrak{p})|$.*

Proof. Brandon talked about how to do this for the q-power Frobenius map. To make this an honest morphism, and not a map in the isogeny category, it was essential that $\mathcal{O}_L \subset \mathrm{End}(A_0)$. The same arguments works for powers of Frobenius. Details are found in the proof of Theorem A.2.3.5 of [1]. Note that this requires that $p \nmid N$, so A_0 has good reduction at $\mathfrak{P}$. □

Taking $n = 1$, the distinguished element endows $L \otimes_{\mathcal{O}_L} \mathfrak{a}_\sigma$ with a distinguished basis and hence identifies it with a fractional ideal $\mathfrak{a}_{\sigma,\mathfrak{P}}$ of L.[2] Note that this ideal will contain $\mathcal{O}_L$. We can reinterpret this as an embedding

$$\mathcal{O}_L = \mathrm{Hom}((A_0, \imath_0), (A_0, \imath_0)) \overset{\xi_{\sigma,\mathfrak{P}} \circ}{\hookrightarrow} \mathrm{Hom}((A_0, \imath_0), (A_0^\sigma, \imath^\sigma)) = \mathfrak{a}_\sigma.$$

Theorem 13. *With the previous notation, $\mathfrak{a}_{\sigma,\mathfrak{P}} = N_\Phi(\mathfrak{p})^{-1}$ where $\mathfrak{p} = \mathfrak{P} \cap E$.*

Proof. First, Corollary 10 makes it transparent that the only prime appearing in $N_\Phi(\mathfrak{p})$ are those lying above p. Likewise, as the isogeny $\xi_{\sigma,\mathfrak{P}}$ has degree p^r for some r, there is an isogeny $\xi' : A_0 \to A_0^\sigma$ so that $\xi_{\sigma,\mathfrak{P}} \circ \xi' = [p^r]$. Thus the quotient $\mathfrak{a}_{\sigma,\mathfrak{P}}/\mathcal{O}_L$ is annihilated by p^r, so $\mathfrak{a}_{\sigma,\mathfrak{P}}$ is a product of primes above p. Therefore to prove the equality of fractional ideals, it suffices to show

$$\mathrm{ord}_v\, \mathfrak{a}_{\sigma,\mathfrak{P}} = -\,\mathrm{ord}_v\, N_\Phi(\mathfrak{p})$$

for any place v lying above p.

Instead of showing this directly, we show that $\mathfrak{a}_{\sigma,\mathfrak{P}}^{f(\mathfrak{P}/\mathfrak{p})}$ has a nice alternate description (where $f(\mathfrak{P}/\mathfrak{p})$ is the residue degree), and relate that to $-f(\mathfrak{P}/\mathfrak{p})\,\mathrm{ord}_v\, N_\Phi(\mathfrak{p})$. This will use the Shimura-Taniyama formula. Finally we will use Corollary 10 to relate the reflex norm to the result of the formula.

We start by considering $\mathfrak{a}_{\sigma^n}$. By Lemma 12, there is a unique element $\xi_{\sigma,n,\mathfrak{P}}$ that descends to the q^n-power Frobenius over $k(\mathfrak{P})$. This identifies $\mathfrak{a}_{\sigma^n}$ with a fractional L-ideal $\mathfrak{a}_{\sigma,n,\mathfrak{P}}$. Since the q^n-power Frobenius is the n-fold composition of the q-power Frobenius, it should be no surprise that $\mathfrak{a}_{\sigma,n,\mathfrak{P}}$ is a power of $\mathfrak{a}_{\sigma,\mathfrak{P}}$.

Lemma 14. *For all $n \geq 1$, $\mathfrak{a}_{\sigma,n,\mathfrak{P}} = \mathfrak{a}_{\sigma,\mathfrak{P}}^n$.*

Proof. This is an equality between fractional ideals, not simply an isomorphism of invertible $\mathcal{O}_L$ modules. To show this, we want to show that $\mathfrak{a}_{\sigma,n+1,\mathfrak{P}} = \mathfrak{a}_{\sigma,\mathfrak{P}}\mathfrak{a}_{\sigma,n,\mathfrak{P}}$, which requires us to construct the following commutative diagram:

$$\begin{array}{ccc} \mathfrak{a}_{\sigma,n} \otimes \mathfrak{a}_{\sigma,1} & \xrightarrow{\quad\sim\quad} & \mathfrak{a}_{\sigma,n+1} \\ & {\scriptstyle \xi_{\sigma,n}\circ\otimes\xi_{\sigma,1}\circ} \searrow \quad \swarrow {\scriptstyle \xi_{\sigma,n+1}\circ} & \\ & \mathrm{Hom}((A_0, \imath_0), (A_0, \imath_0)) = \mathcal{O}_L & \end{array}$$

First, remember that

$$\mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} A_0 \to A_0^\sigma$$

is an isomorphism by Proposition 5. Therefore as any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/E)$ gives an automorphism of K as K/E is Galois, by the base change compatibility of the Serre tensor construction

$$\mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} A_0^\tau \simeq (\mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} A_0)^\tau \simeq A_0^{\tau\sigma}.$$

[2]Throughout this proof, one must be careful about the distinction between abstract invertible $\mathcal{O}_L$-modules and fractional ideals. There is a choice involved in embedding in L, hence the extra subscript.

Note that $1 \otimes \imath_0^\tau$ is identified with $\imath_0^{\tau\sigma}$.

Now taking $\tau = \sigma^n$, we see that

$$\mathfrak{a}_{\tau\sigma} = \mathrm{Hom}((A_0, \imath_0), (A_0^{\tau\sigma}, \imath^{\tau\sigma})) \simeq \mathrm{Hom}((A_0, \imath_0), (\mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} A_0^\tau, 1 \otimes \imath_0^\tau))$$

using this identification. Using it again on τ, we see that

$$\mathfrak{a}_{\tau\sigma} \simeq \mathrm{Hom}((A_0, \imath_0), (\mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} \mathfrak{a}_\tau \otimes_{\mathcal{O}_L} A_0, 1 \otimes 1 \otimes \imath_0)).$$

But by Proposition 7 this is isomorphic to $\mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} \mathfrak{a}_\tau$, so

$$\mathfrak{a}_{\tau\sigma} \simeq \mathfrak{a}_\sigma \otimes_{\mathcal{O}_L} \mathfrak{a}_\tau.$$

Tracing through the isomorphisms, $\xi_{\sigma,n+1,\mathfrak{P}}$ is identified with $\xi_{\sigma,\mathfrak{P}} \otimes \xi_{\sigma,n,\mathfrak{P}}$ because $\xi_{\sigma,\mathfrak{P}} \circ \xi_{\sigma,n,\mathfrak{P}}$ reduces to the q^{n+1}-power Frobenius, and $\xi_{\sigma,n+1,\mathfrak{P}}$ is the unique lift. In terms of fractional ideals, this implies

$$\mathfrak{a}_{\sigma,n+1,\mathfrak{P}} = \mathfrak{a}_{\sigma,\mathfrak{P}} \mathfrak{a}_{\sigma,n,\mathfrak{P}}.$$

Therefore induction implies $\mathfrak{a}_{\sigma,n,\mathfrak{P}} = \mathfrak{a}_{\sigma,\mathfrak{P}}^n$. □

In particular, taking $n = f(\mathfrak{P}|\mathfrak{p})$, we see that $\mathfrak{a}_{\sigma,\mathfrak{P}}^n$ is the invertible $\mathcal{O}_L$ module $\mathrm{End}_K(A_0, \imath_0)$ since that power of Frobenius is the identity. The distinguished element identifying it as a fractional ideal is $\pi_0 = \xi_{\sigma,f(\mathfrak{P}|\mathfrak{p}),\mathfrak{P}}$, a lift of the $|k(\mathfrak{P})|$-power Frobenius. Therefore $\mathfrak{a}_{\sigma,\mathfrak{P}}^n = \pi_0^{-1}\mathcal{O}_L$.

Recall that the Shimura-Taniyama formula (2.1.5.1 of [1]) says that

$$\frac{\mathrm{ord}_v(\pi_0)}{\mathrm{ord}_v q_{\mathfrak{P}}} = \frac{|\Phi_v|}{[L_v : \mathbb{Q}_p]}.$$

This was proven in Dan's talk: recall that $\Phi_v \subset \Phi \subset \mathrm{Hom}_{\mathbb{Q}}(L, K)$ consists of the embeddings of L into K that occur in the CM type and such that the $\mathfrak{P}$-adic place induces v via the embedding.

Proposition 15. *Suppose that* $f(v|p)\,\mathrm{ord}_v(N_\Phi(\mathfrak{p})) = f(\mathfrak{p}|p)|\Phi_v|$. *Then* $\mathrm{ord}_v(\mathfrak{a}_{\sigma,\mathfrak{P}}) = \mathrm{ord}_v(N_\Phi(\mathfrak{p})^{-1})$. *In particular, Theorem 13 holds.*

Proof. By assumption $f(v|p)\,\mathrm{ord}_v(N_\Phi(\mathfrak{p})) = f(\mathfrak{p}|p)|\Phi_v|$. Multiplying by $\frac{-f(\mathfrak{P}|\mathfrak{p})}{f(v|p)}$, we obtain

$$\mathrm{ord}_v(N_\Phi(\mathfrak{p})^{-f(\mathfrak{P}|\mathfrak{p})}) = |\Phi_v| \frac{-f(\mathfrak{P}|\mathfrak{p})}{f(v|p)}.$$

But basic algebraic number theory says $\frac{f(\mathfrak{P}|p)}{f(v|p)} = \frac{f(\mathfrak{P}|\mathfrak{p})\,\mathrm{ord}_v(p)}{[L_v:\mathbb{Q}_p]} = \frac{\mathrm{ord}_v(q_{\mathfrak{P}})}{[L_v:\mathbb{Q}_p]}$. Therefore

$$\mathrm{ord}_v(N_\Phi(\mathfrak{p})^{-f(\mathfrak{P}|\mathfrak{p})}) = -|\Phi_v| \frac{\mathrm{ord}_v(q_{\mathfrak{P}})}{[L_v : \mathbb{Q}_p]} = -\,\mathrm{ord}_v(\pi_0)$$

The last step uses the Shimura-Taniyama formula. Because $\mathfrak{a}_{\sigma,\mathfrak{P}}^{f(\mathfrak{P}|\mathfrak{p})} = \pi_0^{-1}\mathcal{O}_L$, this completes the proof. □

It remains to establish $\frac{f(\mathfrak{p}|p)}{f(v|p)}|\Phi_v| = \mathrm{ord}_v(N_\Phi(\mathfrak{p}))$. Let $n = [K : E]$, and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_s$ denote the primes of $\mathcal{O}_K$ above $\mathfrak{p} \subset \mathcal{O}_E$. They are unramified as $p \nmid N$. Note that $sf(\mathfrak{P}|\mathfrak{p}) = n$. By Corollary 10 it suffices to check that

$$n \frac{f(\mathfrak{p}|p)}{f(v|p)}|\Phi_v| = \mathrm{ord}_v(N_\Phi(\mathfrak{p})) = \sum_{i,\varphi\in\Phi} \varphi^{-1} N_{K/\varphi(L)}(\mathfrak{P}_i).$$

But since the norm of the ideal $\mathfrak{P}_i$ from K to $\varphi(L)$ equals $(\mathfrak{P}_i \cap \varphi(\mathcal{O}_L))^{f(\mathfrak{P}_i|\mathfrak{P}_i\cap\varphi(\mathcal{O}_L))}$, and we am only interested in the place v of L, we only need to consider primes $\mathfrak{P}_i$ and embeddings φ so that $\varphi^{-1}(\mathfrak{P}_i \cap \varphi(\mathcal{O}_L))$ is the prime corresponding to v. In other words, we only need to consider primes $\mathfrak{P}_i$ and φ that pull it back to v. For $\mathfrak{P}_1 = \mathfrak{P}$, these are the primes of Φ_v by definition. Since K/L is Galois, the number is the same for the other primes (s of them total). Finally, note that when

$\varphi(v)$ lies between p and $\mathfrak{P}_i$, we have $f(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{p}|p) = f(\mathfrak{P}_i|\varphi(v))f(\varphi(v)|p)$, and these quantities are independent of φ and $\mathfrak{P}_i$ as K/L and K/E are Galois. Thus we have

$$sf(\mathfrak{P}_i|\varphi(v)) = \frac{n}{f(\mathfrak{P}_i|\mathfrak{p})} f(\mathfrak{P}_i|\varphi(v)) = n\frac{f(\mathfrak{p}|p)}{f(v|p)}.$$

Therefore

$$\sum_{i,\varphi\in\Phi} \operatorname{ord}_v \varphi^{-1} N_{K/\varphi(L)}(\mathfrak{P}_i) = |\Phi_v| n \frac{f(\mathfrak{p}|p)}{f(v|p)}$$

This completes the proof. □

By applying the Serre tensor construction to the inclusion $\mathcal{O}_L \hookrightarrow N_\Phi(\mathfrak{p})^{-1}$ and identifying $\mathcal{O}_L \otimes_{\mathcal{O}_L} A_0$ with A_0, we get a map $j : A_0 \to N_\Phi(\mathfrak{p})^{-1} \otimes_{\mathcal{O}_L} A_0$.

Corollary 16. *There is a unique $\mathcal{O}_L$-linear isomorphism*

$$\theta_{\sigma,\mathfrak{P}} : N_\Phi(\mathfrak{p})^{-1} \otimes_{\mathcal{O}_L} A_0 \simeq A_0^\sigma$$

of Abelian varieties over K making the following diagram commute

$$\begin{array}{ccc} A_0 & \xrightarrow{\xi_{\sigma,\mathfrak{P}}} & A_0^\sigma \\ & \searrow^{j} & \uparrow{\scriptstyle \theta_{\sigma,\mathfrak{P}}} \\ & & N_\Phi(\mathfrak{p})^{-1} \otimes_{\mathcal{O}_L} A_0 \end{array}$$

Proof. Proposition 5 implies that the evaluation map $\operatorname{Hom}((A_0, \imath_0), (A_0^\sigma, \imath_0^\sigma)) \otimes_{\mathcal{O}_L} A_0 \to A_0^\sigma$ is an isomorphism. The theorem shows that the fractional ideal $\mathfrak{a}_{\sigma,\mathfrak{P}}$ associated to $\operatorname{Hom}((A_0, \imath_0), (A_0^\sigma, \imath_0^\sigma))$ equals the fractional ideal $N_\Phi(\mathfrak{p})^{-1}$. This gives the isomorphism $\theta_{\sigma,\mathfrak{P}}$. The diagram commutes because $\mathfrak{a}_\sigma$ is made into a fractional ideal via the map

$$\mathcal{O}_L = \operatorname{Hom}((A_0, \imath_0), (A_0, \imath_0)) \to \operatorname{Hom}((A_0, \imath_0), (A_0^\sigma, \imath_0^\sigma)) = \mathfrak{a}_\sigma$$

given by composition with $\xi_{\sigma,\mathfrak{P}}$. □

Next time Iurie will begin proving the main theorem. One step is to use $\theta_{\sigma,\mathfrak{P}}$, which depends on the descent to K and the choice of $\mathfrak{P}$, to construct a canonical version over $\overline{\mathbb{Q}}$.

References

1. F. Oort C-L. Chai, B. Conrad, *Cm liftings*.
2. J-S Milne, *Complex multiplication*, 2006.
3. D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research, Hindustan Book Agency, 2008.