Algbraicity properties of Heegner points

1. Motivation

Let $K = \mathbf{Q}(\sqrt{D}) \subseteq \mathbf{C}$ be an imaginary quadratic subfield of $\mathbf{C}$. Let N be a positive integer relatively prime to D whose prime factors are split in K. We want to show how to use the main theorems of the classical theory of complex multiplication to prove that Heegner points on $X_0(N)_{/\mathbf{Q}}$ with CM by the full ring of integers of K have residue field isomorphic to the Hilbert class field H of K, and we will likewise apply CM theory to compute the action on these points by $\mathrm{Gal}(H/K)$, as well as complex conjugation (which, together with $\mathrm{Gal}(H/K)$, generates the generalized dihedral group $\mathrm{Gal}(H/\mathbf{Q})$). Of course, from the purely analytic point of view it is hard to "see" that the Heegner points for a $\mathrm{Gal}(H/\mathbf{Q})$-stable subset inside of the H-points of $X_0(N)_{/\mathbf{Q}}$ (let alone that they're even H-points).

Since we only work here with Heegner points with CM by the maximal order, we correspondingly will only state the main theorems of CM for the maximal order. If we were to work with more general Heegner points (with CM by general orders) then we would need the general version of the main theorems of CM and the residue fields on $X_0(N)_{/\mathbf{Q}}$ at the corresponding Heegner points would be isomorphic to certain ring class fields of K (depending on the order in question) rather than the Hilbert class field. Our description of the Galois action would also adapt in an essentially mechanical way. Thus, the underlying method for handling the general case is basically the same as what we use here, but one has to deal with some additional technical complications. Since Gross-Zagier only require these sorts of results for Heegner points with CM by the maximal order, we tailor the exposition to this case.

Here we use the following notation. If $\Lambda \subseteq \mathbf{C}$ is a cocompact lattice (such as a fractional ideal of K), we write $j(\Lambda)$ to denote the j-invariant of the elliptic curve $\mathbf{C}/\Lambda$. Also, if $H \subseteq \mathbf{C}$ denotes the Hilber class field of K then we normalize the isomorphism $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$ of class field theory so that a (non-zero) prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$ corresponds to the *arithmetic* Frobenius element at $\mathfrak{p}$ (i.e., the unique element in the decomposition group at $\mathfrak{p}$ which induces $x \mapsto x^{\mathbf{N}\mathfrak{p}}$ on $\mathscr{O}_H/\mathfrak{P}$ for any prime $\mathfrak{P}$ of $\mathscr{O}_H$ over $\mathfrak{p}$). This normalization for the Artin isomorphism of class field theory is the one used in Lang's *Elliptic Functions*, so our use of Lang as a reference is the reason we follow this normalization (as opposed to the reciprocal normalization which is preferred by Deligne). In general, we write $\sigma_{\mathfrak{b}} \in \mathrm{Gal}(H/K)$ to denote the element corresponding to the ideal class of a fractional ideal $\mathfrak{b}$ of K.

2. Main theorems of complex multiplication

As a general reference, we use Lang's *Elliptic Functions* (2nd. edition) for the development of the classical CM theory (including arbitrary orders in imaginary quadratic fields). His techniques rest on rather hands-on arguments with elliptic functions and Weierstrass equations. In order to state the main theorems for CM, we need to recall some general idelic notation.

Let K be a number field (only the imaginary quadratic case is relevant for us) and $\mathfrak{a}$ a fractional ideal of K. For any idele s of K, we let (s) denote the corresponding fractional ideal of K (with multiplicity $\mathrm{ord}_v(s_v)$ at each $v \nmid \infty$). We have a canonical decomposition

$$K/\mathfrak{a} \simeq \bigoplus_{v \nmid \infty} K_v/\mathfrak{a}_v,$$

and multiplication by s_v on the vth factor sets up an $\mathscr{O}_K$-linear isomorphism

$$s : K/\mathfrak{a} \simeq K/(s)\mathfrak{a}.$$

In the special case when s is a principal idele with generator α then this map is just the multiplication map

$$\alpha : K/\mathfrak{a} \simeq K/\alpha\mathfrak{a}.$$

Another important special case is when s_v is a unit for all $v \nmid \infty$. This is the case when the Artin symbol $(s|K) \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ acts *trivially* on the Hilbert class field of K (essentially by the idelic description of the ideal class group and the idelic formulation of class field theory for K). In this case, $(s)\mathfrak{a} = \mathfrak{a}$ but the map $s : K/\mathfrak{a} \to K/\mathfrak{a}$ is rather far from the identity in general (we will see that relative to an algebraic model for

$\mathbf{C}/\mathfrak{a}$ over H, this action essentially corresponds to the action of $(s|K)$ on $(\mathbf{C}/\mathfrak{a})_{\mathrm{tors}}$, whose coordinates all lie in K^{ab}).

Here is a special case of the first main theorem of complex multiplication (obtained from Theorem 2 in §1, Theorem 5 in §3, and Remark 1 on p. 133, §3, all in Chapter 10 of Lang's book).

Theorem 2.1. *Let $K \subseteq \mathbf{C}$ be an imaginary quadratic subfield of $\mathbf{C}$, and $\mathfrak{a}$ a fractional ideal of K. Let $H \subseteq \mathbf{C}$ be the Hilbert class field of K. Then*

$$j(\mathbf{C}/\mathfrak{a}) \in H$$

and this j-invariant generates H over K.

Moreover, for any fractional ideal $\mathfrak{b}$ of K, we have

$$\sigma_{\mathfrak{b}}(j(\mathfrak{a})) = j(\mathfrak{a}\mathfrak{b}^{-1}).$$

If we had decided to use Deligne's normalization for the Artin isomorphism, there would be $\mathfrak{b}$ rather than $\mathfrak{b}^{-1}$ in the final identity of the theorem.

Corollary 2.2. *For any fractional ideal $\mathfrak{a}$ of K, the elliptic curve $\mathbf{C}/\mathfrak{a}$ admits a Weierstrass model over the subfield $H \subseteq \mathbf{C}$.*

Proof. It is a basic fact from the theory of elliptic curves that an elliptic curve over an algebraically closed field admits a Weierstrass equation whose coefficients lie in the subfield generated over the prime field by the j-invariant. ■

A special case of the second main theorem of CM is the following (extracted from Theorem 3 in §2 of Chapter 10 in Lang's book):

Theorem 2.3. *Let $K \subseteq \mathbf{C}$ be an imaginary quadratic field, and $H \subseteq \mathbf{C}$ its Hilbert class field. Let $\varphi : \mathbf{C}/\mathfrak{a} \simeq A$ be an analytic isomorphism onto a Weierstrass model over $\mathbf{C}$. Let $\sigma \in \mathrm{Aut}(\mathbf{C}/K)$ be a K-automorphism, and s an idele of K with $(s|K) = \sigma|_{K^{\mathrm{ab}}}$. Let A^σ denote the Weierstrass model obtained from applying σ to the coefficients, so the set-theoretic map $(x, y) \mapsto (\sigma(x), \sigma(y))$ induces an isomorphism of abelian groups $A \simeq A^\sigma$.*

Then there exists a unique analytic isomorphism $\psi_\sigma : \mathbf{C}/(s)^{-1}\mathfrak{a} \simeq A^\sigma$ such that the diagram

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r] \arrow[d, "s^{-1}"'] & \mathbf{C}/\mathfrak{a} \arrow[r, "\varphi", "\simeq"'] & A \arrow[d, "\sigma"] \\ K/(s)^{-1}\mathfrak{a} \arrow[r] & \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1} \arrow[r, "\simeq", "\psi_\sigma"'] & A^\sigma \end{tikzcd} \tag{1}$$

commutes. Here, the maps $K/\Lambda \to \mathbf{C}/\Lambda$ are the canonical inclusions.

If we had used Deligne's normalization for the Artin isomorphism, then s^{-1} would be replaced with s in both appearances on the left side of (1).

The proof of this theorem involves a detailed study of Weber functions which explicate torsion in terms of Weierstrass theory. The point is that $K/\mathfrak{a}$ is exactly the torsion subgroup of $\mathbf{C}/\mathfrak{a}$ (and likewise for the bottom row using $(s)^{-1}\mathfrak{a}$), so the commutativity of the diagram certainly requires an understanding of torsion in terms of analytic Weierstrass models. It is perhaps also worth stressing that the proof of Theorem 2.3 proceeds in a series of stages, where one first proves a weaker result for arithmetic Frobenius elements away from some "bad" finite set and then an indirect procedure extends things to the case of general σ.

Observe that uniqueness of ψ_σ (which Lang doesn't mention) is immediate from the denseness of $(\mathbf{C}/\Lambda)_{\mathrm{tors}}$ inside of $\mathbf{C}/\Lambda$. Note that there is no meaningful way to fill in a middle arrow in (1) making a commutative square on either the left or the right. Thus, it is only the retangle (1) which really makes sense.

In the special case where we choose the Weierstrass model to have coefficients in H (which can be done, thanks to Corollary 2.2) and σ is the identity on H, then $A^\sigma = A$ and $\sigma|_{K^{\mathrm{ab}}} = (s|K)$ for an idele s which is a *unit* at all finite places. Thus, as we noted earlier, we then have $(s)^{-1}\mathfrak{a} = \mathfrak{a}$ for all fractional ideals $\mathfrak{a}$ of K. Putting this all together, we get the following consequence of the preceding theorem:

Corollary 2.4. *Let $K \subseteq \mathbf{C}$ be an imaginary quadratic subfield with Hilbert class field H. Let $\mathfrak{a}$ be a fractional ideal of K and $\varphi : \mathbf{C}/\mathfrak{a} \simeq A$ an analytic isomorphism onto a Weierstrass model with coefficients in H. For any $\sigma \in \mathrm{Aut}(\mathbf{C}/H)$ and idele s of K with $\sigma|_{K^{\mathrm{ab}}} = (s|K)$ and $s_v \in \mathscr{O}_v^\times$ for all $v \nmid \infty$, there is a unique analytic isomorphism $\psi_\sigma : \mathbf{C}/\mathfrak{a} \simeq A$ such that the diagram*

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r] \arrow[d, "s^{-1}"'] & \mathbf{C}/\mathfrak{a} \arrow[r, "\varphi", "\simeq"'] & A \arrow[d, "\sigma"] \\ K/\mathfrak{a} \arrow[r] & \mathbf{C}/\mathfrak{a} \arrow[r, "\simeq", "\psi_\sigma"'] & A \end{tikzcd}$$

commutes, where the right vertical map is $(x, y) \mapsto (\sigma(x), \sigma(y))$ (which carries A to itself since σ acts as the identity on the coefficients in H).

Remark 2.5. Clearly $\psi_\sigma = \varphi \circ \xi_\sigma$ for an analytic automorphism ξ_σ of $\mathbf{C}/\mathfrak{a}$, which is to say $\xi_\sigma \in \mathscr{O}_K^\times \subseteq \mathbf{C}$.

This completes our overview of the classical CM theory.

3. Applications of CM theory to algebraicity

We let K be an imaginary quadratic subfield of $\mathbf{C}$ and $\mathfrak{a}$ a fractional ideal of K. Let $\mathfrak{b}$ be a (non-zero) integral ideal of K, so the finite $\mathscr{O}_K$-module

$$(\mathbf{C}/\mathfrak{a})[\mathfrak{b}] \subseteq \mathbf{C}/\mathfrak{a}$$

makes sense, and is the kernel of the natural finite projection map

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1}.$$

A special case of this situation is that described by a Heegner point. We want to prove the following theorem:

Theorem 3.1. *With notation as above, and $H \subseteq \mathbf{C}$ the Hilbert class field of K, the situation*

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1}$$

can be "defined over H".

This can be interpreted in two (equivalent) ways. On the one hand, we can take this to mean that projective models (even Weierstrass models) can be found for the two elliptic curves using H-coefficients in such a way that the analytic projection map can be described (locally for the Zariski topology relative to H-coefficients) in terms of polynomial equations with H-coefficients. But clearly such an ad hoc point of view is inadequate for proving anything. In more sophisticated terms, we are claiming that there exists an isogeny $E \to E'$ of elliptic curves over H whose base change to $\mathbf{C}$ (and resulting analytification) is isomorphic to the given analytic isogeny.

In order to verify statements of this sort, we will use the following basic fact which is a special case of descent theory in algebraic geometry and was known even in the archaic pre-Grothendieck era. If you have questions about the proof, just ask me (it is easier to describe in person than to write out here).

Lemma 3.2. *Let F be a field and F'/F an algebraically closed extension field. Let E be an elliptic curve over F and $\pi' : E_{/F'} \to E'_1$ a separable isogeny of elliptic curves over F'. Then there exists an isogeny*

$$\pi : E \to E_1$$

over F whose base change to F' is isomorphic to π' if and only if the finite subgroup

$$\ker(\pi')(F') \subseteq E(F')$$

is stable under the "coordinate-wise" action of $\mathrm{Aut}(F'/F)$ on $E(F')$.

Now we can prove Theorem 3.1:

Proof. By the algebraicity of the category of complex analytic elliptic curves, the analytic diagram

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1}$$

can be realized as the analytification of an algebraic isogeny between elliptic curves over $\mathbf{C}$. Moreover, we have already noted that $\mathbf{C}/\mathfrak{a}$ may be realized by a Weierstrass equation E with coefficients in H. Let $\varphi : \mathbf{C}/\mathfrak{a} \simeq E(\mathbf{C})$ be an analytic isomorphism.

By the preceding lemma we just have to show that the subgroup $\varphi(\mathfrak{a}\mathfrak{b}^{-1}/\mathfrak{a})$ in $E(\mathbf{C})$ is stable under the action of $\mathrm{Aut}(\mathbf{C}/H)$. Choose $\sigma \in \mathrm{Aut}(\mathbf{C}/H)$. In the notation of Corollary 2.2 and the subsequent remark, we have

$$\sigma(\varphi(\mathfrak{a}\mathfrak{b}^{-1}/\mathfrak{a})) = \varphi(\xi_\sigma((\mathfrak{a}\mathfrak{b}^{-1}/\mathfrak{a}))),$$

where ξ_σ is multiplication by some element in $\mathscr{O}_K^\times$. The right side is visibly $\varphi((\mathfrak{a}\mathfrak{b}^{-1}/\mathfrak{a}))$, so we're done. ■

We now use the arithmetic theory of modular curves, or more specifically the theory for realizing classical analytic modular curves as arising from algebraic curves over $\mathbf{Q}$. From now on, we write $Y_0(N)$ to denote the canonical algebraic curve over $\mathbf{Q}$ (whose analytified base change to $\mathbf{C}$ is naturally analytically identified with the classical analytic construction to now be denoted $Y_0(N)^{\mathrm{an}}$). This is a smooth affine curve over $\mathbf{Q}$. It is an unfortunate fact of life that one cannot view $Y_0(N)$ as a fine moduli scheme. But at the very least, from the theory that makes this algebraic curve over $\mathbf{Q}$ one obtains the following:

Theorem 3.3. *Let F be a subfield of $\mathbf{C}$ and $E \to E'$ a cyclic N-isogeny of elliptic curves over F. Then the point on $Y_0(N)^{\mathrm{an}}$ corresponding to the analytic data $E(\mathbf{C}) \to E'(\mathbf{C})$ is induced by a point in $Y_0(N)(F)$.*

Combining this fact with Theorem 3.1, we obtain:

Corollary 3.4. *Let K be an imaginary quadratic field, and N a positive integer all of whose prime factors are totally split in K. Then all Heegner points on $Y_0(N)^{\mathrm{an}}$ arise from points in $Y_0(N)(H)$.*

We have a generalized semi-direct product decomposition

$$\mathrm{Gal}(H/\mathbf{Q}) \simeq \langle c \rangle \ltimes \mathrm{Gal}(H/K),$$

where c is complex conjugation. The reason for the semi-direct product structure is because the isomorphism $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$ arising from class field theory is *functorial* in the abstract field K and the action of complex conjugation on K induces *inversion* on the ideal class group of K. Indeed, for any fractional ideal $\mathfrak{b}$ of K we see that $\mathfrak{b}\overline{\mathfrak{b}}$ is a principal ideal generated by the norm of $\mathfrak{b}$. Hence, $\overline{\mathfrak{b}}$ represents the inverse ideal class to that of $\mathfrak{b}$.

Since $\mathrm{Gal}(H/\mathbf{Q})$ acts on the set $Y_0(N)(H)$ (as $Y_0(N)$ is an algebraic curve over $\mathbf{Q}$), it makes sense (by Corollary 3.4) to ask how this group acts on Heegner points. Can the action be described in terms of the analytic data $([\mathfrak{a}], \mathfrak{n})$ which we have used to describe Heegner points? Of course the answer is yes. Let's see how it goes.

There are two actions on the set of Heegner points which we want to describe: the action of complex conjugation c and the action of $\mathrm{Gal}(H/K)$. The latter will be approached using CM theory (which only discusses automorphisms of $\mathbf{C}$ that fix the subfield K anyway), and the analysis of c will use the fortunate fact that c acts continuously in a well-understood manner with respect to the analytic topology. Let's begin with the case of c, since it requires no arithmetic theory at all.

Theorem 3.5. *For a Heegner point $x = ([\mathfrak{a}], \mathfrak{n})$ in $Y_0(N)(\mathbf{C})$, we have $c(x) = ([\mathfrak{a}]^{-1}, \overline{\mathfrak{n}})$.*

Proof. Since $[\overline{\mathfrak{a}}] = [\mathfrak{a}]^{-1}$, one can be tempted the declare the entire result as essentially obvious because of vague nonsense along the lines "oh, c is continuous so how could it be otherwise", but that brief argument fails to articulate the role of the *definitions* of the algebraic structures in question and hence is not actually a proof of anything. But of course it is close to the real reason: the general simple behavior of the Weierstrass function $\wp_\Lambda$ and the numbers $g_2(\Lambda)$, $g_3(\Lambda)$ with respect to complex conjugation (and the role of these in explicating the *algebraicity* of the classical *analytic* theory of elliptic curves).

Now let's carefully explain how to translate the naive intuition into a convincing proof. We first recall that the identification of the set $Y_0(N)(\mathbf{C})$ with the classical analytic model $Y_0(N)^{\mathrm{an}}$ uses the canonical algebraicity of the category of elliptic curves over $\mathbf{C}$. In other words, to identify $([\mathfrak{a}], \mathfrak{n})$ with a point on the algebraic curve $Y_0(N)(\mathbf{C})$ we need to give an algebraic model over $\mathbf{C}$ for the analytic situation

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{n}^{-1}\mathfrak{a}.$$

We can equivalently (by the algebraic theory of isogenies and its compatibility with the analytic theory) work with the specification of an algebraic model of the pair $(\mathbf{C}/\mathfrak{a}, \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a})$. Then by the very definition of how such an *algebraic model* gives rise to a point in $Y_0(N)(\mathbf{C})$ it follows that the action of c on such a point corresponds to applying c to the coefficients of the defining equations of such an algebraic model over $\mathbf{C}$.

Let us make this more specific. Using the Weierstrass function $\wp_{\mathfrak{a}}$ associated to the cocompact lattice $\mathfrak{a}$ in $\mathbf{C}$, an algebraic model for $\mathbf{C}/\mathfrak{a}$ is provided by the equation

$$y^2 w = 4x^3 - g_2(\mathfrak{a})x^2 w - g_3(\mathfrak{a})w^3$$

where $g_2(\Lambda)$ and $g_3(\Lambda)$ are the habitual numbers attached to a compact lattice Λ in $\mathbf{C}$:

$$g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{\lambda^4}, \quad g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{\lambda^6}.$$

In this model, the finite subset $\mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a}$ corresponds to the set of points

$$\{[\wp_{\mathfrak{a}}(z), \wp'_{\mathfrak{a}}(z), 1] \in \mathbf{P}^2 \mid z \in \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a}\}$$

where we understand the case $z = 0$ to correspond to $[0, 1, 0]$. If we apply c to the coefficients of the defining Weierstrass equation then by continuity of c and the obvious identities

$$\overline{g_j(\Lambda)} = g_j(\overline{\Lambda})$$

we arrive at the equation

$$y^2 w = 4x^3 - g_2(\overline{\mathfrak{a}})x^2 w - g_3(\overline{\mathfrak{a}})w^3.$$

Since $X - aW, Y - bW$ are the defining equations of the point $[a, b, 1]$ (while $X = W = 0$ are the defining equations of the point $[0, 1, 0]$), we conclude by the continuity of c and the obvious identity

$$\overline{\wp_\Lambda(z)} = \wp_{\overline{\Lambda}}(\overline{z})$$

that c carries the algebraic model of $\mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a}$ over to the set of points

$$\{[\wp_{\overline{\mathfrak{a}}}(z), \wp'_{\overline{\mathfrak{a}}}(z), 1] \in \mathbf{P}^2 \mid z \in \overline{\mathfrak{n}}^{-1}\overline{\mathfrak{a}}/\overline{\mathfrak{a}}\}$$

This shows that applying c to an algebraic model over $\mathbf{C}$ for $([\mathfrak{a}], \mathfrak{n})$ yields an algebraic model over $\mathbf{C}$ corresponding to $([\overline{\mathfrak{a}}], \overline{\mathfrak{n}}) = ([\mathfrak{a}]^{-1}, \overline{\mathfrak{n}})$. Since the subset $Y_0(N)(H) \subseteq Y_0(N)(\mathbf{C})$ is given the intrinsic action from c on H when we use complex conjugation on $\mathbf{C}$ (applied to the coefficients of the defining equations of algebraic models over $\mathbf{C}$), it follows that we have correctly described the action of c on Heegner points when the latter are viewed as points in $Y_0(N)(H)$.

■

With the action of c on Heegner points understood, it remains to work out the action of $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$ on Heegner points $([\mathfrak{a}], \mathfrak{n})$.

Theorem 3.6. *Let $\sigma \in \mathrm{Gal}(H/K)$ correspond to a fractional ideal class $[\mathfrak{b}]$ under the class field theory isomorphism $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$. Then as points in $Y_0(N)(H)$ we have*

$$\sigma([\mathfrak{a}], \mathfrak{n}) = ([\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{n}).$$

Of course, we could describe the equality in this theorem purely in terms of ideal classes rather than in terms of representative elements, but the distinction is minor and in practice we'll certainly be computing with representatives anyway. A more subtle point is to observe that the statement of the theorem certainly depends on how we define the Artin isomorphism of class field theory, for which there's always a question of sign: does the ideal class of a prime ideal $\mathfrak{p}$ correspond to an arithmetic of geometric Frobenius element at $\mathfrak{p}$. We have made the convention to work with arithmetic Frobenius elements because this is the convention uses in Lang's *Elliptic Functions* (to which we have referred for the statements of the main theorems of CM).

If we adopted Deligne's preference to go with geometric Frobenius elements as the more basic concept, then the equality in the theorem would have $\mathfrak{b}$ rather than $\mathfrak{b}^{-1}$ on the right side. Whatever.

Proof. We first choose an isogeny $\pi : E \to E'$ of elliptic curves over H which induces a point in $Y_0(N)(H) \subseteq Y_0(N)(\mathbf{C}) = Y_0(N)^{\mathrm{an}}$ that corresponds to the Heegner point data $\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1}$. We let

$$\varphi : \mathbf{C}/\mathfrak{a} \simeq E(\mathbf{C}), \;\; \varphi' : \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1} \simeq E'(\mathbf{C})$$

denote corresponding compatible analytic isomorphisms making the diagram

$$\begin{tikzcd}
\mathbf{C}/\mathfrak{a} \arrow[r, "\varphi"] \arrow[d] & E(\mathbf{C}) \arrow[d, "\pi_{\mathbf{C}}"] \\
\mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1} \arrow[r, "\varphi'"'] & E'(\mathbf{C})
\end{tikzcd}$$

commute, where the left column is the canonical projection.

Fix a lifting of σ to a K-automorphism of $\mathbf{C}$, again denoted σ, and choose an idele s of K for which $(s|K) = \sigma|_{K^{\mathrm{ab}}}$, so $(s) = \mathfrak{b}$ by the definition of $\mathfrak{b}$ (and our convention for normalizing the Artin isomorphism). By Theorem 2.3, there are unique analytic isomorphism

$$\psi_\sigma : \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1} \simeq E^\sigma(\mathbf{C})$$

and

$$\psi'_\sigma : \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1} \simeq E'^\sigma(\mathbf{C})$$

which fit into respective commutative diagrams of groups

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r] \arrow[d, "s^{-1}"'] & \mathbf{C}/\mathfrak{a} \arrow[r, "\varphi", "\simeq"'] & E(\mathbf{C}) \arrow[d, "\sigma"] \\
K/\mathfrak{a}\mathfrak{b}^{-1} \arrow[r] & \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1} \arrow[r, "\simeq", "\psi_\sigma"'] & E^\sigma(\mathbf{C})
\end{tikzcd}$$

and

$$\begin{tikzcd}
K/\mathfrak{a}\mathfrak{n}^{-1} \arrow[r] \arrow[d, "s^{-1}"'] & \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1} \arrow[r, "\varphi", "\simeq"'] & E'(\mathbf{C}) \arrow[d, "\sigma"] \\
K/\mathfrak{a}\mathfrak{n}^{-1}\mathfrak{b}^{-1} \arrow[r] & \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1}\mathfrak{b}^{-1} \arrow[r, "\simeq", "\psi'_\sigma"'] & E'^\sigma(\mathbf{C})
\end{tikzcd}$$

Now consider the analytic diagram

(2)
$$\begin{tikzcd}
\mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1} \arrow[r, "\psi'_\sigma", "\simeq"'] \arrow[d] & E^\sigma(\mathbf{C}) \arrow[d, "(\pi^\sigma)_{\mathbf{C}}"] \\
\mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{n}^{-1} \arrow[r, "\simeq", "\psi'_\sigma"'] & E'^\sigma(\mathbf{C})
\end{tikzcd}$$

where the left column in the canonical projection. Here is the crucial point: this diagram *commutes.* To check such commutativity, by *continuity* it suffices to compose everything back to the dense torsion subgroup $K/\mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathbf{C}/\mathfrak{a}\mathfrak{b}^{-1}$, and even to compose with the isomorphism

$$s^{-1} : K/\mathfrak{a} \simeq K/\mathfrak{a}\mathfrak{b}^{-1}.$$

But if we use the trivial commutativity of general diagrams

$$\begin{tikzcd} K/\mathfrak{c} \arrow[r] \arrow[d] & \mathbf{C}/\mathfrak{c} \arrow[d] \\ K/\mathfrak{c}' \arrow[r] & \mathbf{C}/\mathfrak{c}' \end{tikzcd}$$

(for fractional ideals $\mathfrak{c} \subseteq \mathfrak{c}'$) and

$$\begin{tikzcd} K/\mathfrak{c} \arrow[r, "s^{-1}", "\simeq"'] \arrow[d] & K/(s)^{-1}\mathfrak{c} \arrow[d] \\ K/\mathfrak{c}' \arrow[r, "\simeq", "s^{-1}"'] & K/(s)^{-1}\mathfrak{c}' \end{tikzcd}$$

(for fractional ideals $\mathfrak{c} \subseteq \mathfrak{c}'$), then everything fits together rather easily, thanks to the characterizing properties of ψ_σ and ψ'_σ when composed back to torsion. It is too painful for me to TeX the corresponding 3-dimensional diagram which puts everything together, so we leave it as a pleasant exercise to see how the jigsaw puzzle works.

With the commutativity of (2) settled, we look at what this diagram says! The left side of (2) is exactly the data corresponding to the Heegner point $([\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{n})$. The right side of (2) is exactly the analytification of the base change to $\mathbf{C}$ of the action of $\sigma \in \mathrm{Gal}(H/K)$ on the original H-model $E \to E'$ in $Y_0(N)(H)$ for our initial Heegner point $([\mathfrak{a}], \mathfrak{n})$. Hence, the commutativity of (2) with analytic isomorphisms across the horizontal directions says exactly that $\sigma \in \mathrm{Gal}(H/K)$ acting on $Y_0(N)(H)$ takes $([\mathfrak{a}], \mathfrak{n})$ over to $([\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{n})$, as desired.

■