NOTES ON EULER SYSTEMS ON SHIMURA VARIETIES

JACOB SWENBERG

Contents

1. Introduction

In these notes, we discuss the theory of Euler systems in the cohomology of Shimura varieties.

The primary reference for these notes is Loeffler and Zerbes's notes for the 2018 Arizona Winter School [2].

2. The Bloch–Kato Conjecture

Throughout, let K be a number field, p a prime, and E a finite extension of $\mathbb{Q}_p$. Let V be a finite-dimensional E-valued representation of the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$. In other words, V is a finite-dimensional E-vector space equipped with a continuous homomorphism

$$\rho : G_K \to \mathrm{Aut}_E(V).$$

Definition 2.1. We say that V *comes from geometry* if it is a subquotient of

$$H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)(j) \otimes_{\mathbb{Q}_p} E$$

for some K-variety X and some integers i, j.

Definition 2.2. Let v be a place of K for which V is unramified. Let Frob_v denote an (arithmetic) Frobenius at v, which is well-defined up to conjugation (equivalently, a lift of v to $\overline{K}$). The *local Euler factor of V at v* is

$$P_v(V, t) := \det(1 - t \cdot \rho(\mathrm{Frob}_v^{-1})) \in E[t].$$

We fix an embedding $\overline{\mathbb{Q}} \to \mathbb{C}$, and embeddings $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_\ell}$ for all primes ℓ. This determines inertia subgroups $I_v \subseteq G_{K_v} \subseteq G_K$ for all places v of K. There is some way to define $P_v(V, t)$ for ramified places v of V.

Definition 2.3. Assume that $P_v(V, t)$ has coefficients in $\overline{Q}$ for all v. The *global L-function of V* is

$$L(V, s) := \prod_v P_v(V, q_v^{-s})^{-1}.$$

Conjecture 2.4. *If V is semisimple and comes from geometry, then $L(V, s)$ has a meromorphic continuation to the whole complex plane with finitely many poles, and there is a functional equation relating $L(V, s)$ and $L(V^*, 1 - s)$.*

For each place v of K, we define a subgroup

$$H^1_f(K_v, V) := \begin{cases} \ker(H^1(K_v, V) \to H^1(I_v, V)) & v \nmid p \\ \ker(H^1(K_v, V) \to H^1(K_v, V \otimes_{\mathbb{Q}_p} B_{cris}) & v \mid p. \end{cases} \subseteq H^1(K_v, V).$$

Here, we take continuous cohomology (continuous cocycles modulo continuous coboundaries).

Definition 2.5. The *Bloch–Kato Selmer group of* V is

$$H^1_f(K, V) := \{\alpha \in H^1(K, V) : \mathrm{res}_v(\alpha) \in H^1_f(K_v, V) \text{ for all } v\}.$$

Conjecture 2.6 (Bloch–Kato)**.**

$$\dim H^1_f(K, V) - \dim H^0(K, V) = \mathrm{ord}_{s=0} L(V^*(1), s).$$

Example 2.7. Let $V = \mathbb{Q}_p(1)$. Then $V^*(1) = \mathbb{Q}_p$. Then for all v, we have

$$P_v(\mathbb{Q}_p(1), q_v^{-s})^{-1} = (1 - q_v^{-s})^{-1}.$$

From the product formula for $\zeta_K(s)$, we have

$$L(\mathbb{Q}_p, s) = \zeta_K(s).$$

In particular, $L(\mathbb{Q}_p, s)$ has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ and functional equation. By inspecting the functional equation, one can find that

$$\mathrm{ord}_{s=0} L(\mathbb{Q}_p, s) = r_1 + r_2 - 1,$$

where r_1, r_2 are, respectively, the number of real embeddings and the number of pairs of complex conjugate embeddings of K. On the other hand, $H^0(K, \mathbb{Q}_p(1)) = 0$, and Kummer theory gives

$$H^1_f(K, \mathbb{Q}_p(1)) = O_K^\times \otimes \mathbb{Q}_p.$$

Thus, the Bloch–Kato conjecture is equivalent to Dirichlet's unit theorem in this case.

Example 2.8. Let E be an elliptic curve over a number field F. Let $V = V_pE = T_pE \otimes \mathbb{Q}_p$. Kummer theory gives an injection

$$E(F) \otimes \mathbb{Q}_p \to H^1_f(F, V).$$

The cokernel of this map is zero if the Tate–Shafarevich group of E over F is finite.

Let us compute $L(V^*(1), s)$. It turns out that

$$V \cong H^1_{\acute{e}t}(E_{\overline{F}}, \mathbb{Q}_p)(1).$$

So

$$V^*(1) \cong H^1_{\acute{e}t}(E_{\overline{F}}, \mathbb{Q}_p)^*$$

We have, by the functional equation,

$$P_v(V^*(1), s) = P_v(H^1_{\acute{e}t}(E_{\overline{F}}, \mathbb{Q}_p)^*, s) = P_v(H^1_{\acute{e}t}(E_{\overline{F}}, \mathbb{Q}_p), 1 - s).$$

Since $P_v(H^1_{\acute{e}t}(E_{\overline{F}}, \mathbb{Q}_p), s)$ is the local Euler factor for the Hasse–Weil zeta function of E, we have

$$\operatorname{ord}_{s=0} L(V^*(1), s) = \operatorname{ord}_{s=1} L(E/F, s).$$

Finally, $H^0(F, V^*(1)) = 0$ in this case. We have used finiteness of the Tate–Shafarevich group, the functional equation for L, and the Bloch–Kato conjecture to conclude that

$$\operatorname{rank} E(F) = \dim H^1_f(F, V) = \operatorname{ord}_{s=1} L(E/F, s).$$

This is part of the conjecture of Birch and Swinnerton-Dyer.

3. Euler Systems: A Definition

Let V be a continuous $\mathbb{Q}_p$-valued representation of $G_{\mathbb{Q}}$. Let $T \subset V$ be a G_F-stable $\mathbb{Z}_p$-lattice. Let S be a set of primes including p together with the ramified primes of V. Thus, V is also a G_F-representation for any number field F. Furthermore, on cohomology, we have corestriction maps for an finite extension L/K

$$\operatorname{cor}^L_K : H^i(L, V) \to H^i(K, V).$$

In degree 0, corestriction is just the norm map. Corestriction commutes with connecting maps in long exact sequences on cohomology.

For ℓ not dividing m, we let $\sigma_\ell := \operatorname{Frob}_\ell \in \operatorname{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$.

Definition 3.1. An *Euler system for* (T, S) (also called an *Euler system for* V) is a collection $(c_m)_{m \geq 1}$ where $c_m \in H^1(\mathbb{Q}(\mu_m), T)$, such that

$$\operatorname{cor}^{\mathbb{Q}(\mu_{m\ell})}_{\mathbb{Q}(m)}(c_{m\ell}) = \begin{cases} c_m & \ell \in S \text{ or } \ell \mid m \\ P_\ell(V^*(1), \sigma_\ell^{-1}) \cdot c_m & \text{else.} \end{cases}$$

Intuitively, we pick up Euler factors of $L(V^*(1), s)$ as we take norms.

Theorem 3.2 (Rubin)**.** *Let $(c_n)_n$ be an Euler system for V with $c_1 \neq 0$. Then after some technical assumptions on V, we have*

$$\mathrm{Sel}_{strict}(\mathbb{Q}, V^*(1)) = 0.$$

Remark 3.3. Instead of working over $\mathbb{Q}$, we could work with an arbitrary number field. Then the elements of our Euler system will be indexed by certain ray class fields.

4. Kolyvagin's Euler System

In this section, we exhibit our first example of an Euler system, due to Kolyvagin. This Euler system allowed Kolyvagin to prove that $Ш(E/K)$ is finite for many elliptic curves E over $\mathbb{Q}$ and suitable imaginary quadratic fields K. The main reference for this section is [1].

4.1. **Cast of Characters.** Let p be an odd prime. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. We assume that E does not have CM, which only excludes finitely many elliptic curves. Recall the following theorems

Theorem 4.1 (Serre)**.** *For almost all primes p, the mod-p Galois representation attached to E is surjective. In other words, the homomorphism*

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$$

is surjective.

We will refer to such primes as *Serre primes (for E).*

Theorem 4.2 (Modularity of Elliptic Curves, Wiles, Breuil–Conrad–Diamond–Taylor)**.** *The curve E is modular: there exists a non-constant morphism $\phi : X_0(N) \to E$.*

Moreover, one can choose this parametrization so that the infinity cusp maps to the identity of E.

Recall that the modular curve $X_0(N)$ parametrizes elliptic curves E equipped with a cyclic N-isogeny $E \to E'$. We can construct many such curves using CM-theory. Let K be an imaginary quadratic field of discriminant $-D$ such that all prime factors of N are split. Then we may choose an ideal $\mathfrak{N}$ of O_K such that $O_K/\mathfrak{N} \cong \mathbb{Z}/N$. For simplicity, let us assume that $O_K^\times = \{\pm 1\}$. By embedding $K \to \mathbb{C}$, we have a cyclic N-isogeny of elliptic curves

$$\mathbb{C}/O_K \to \mathbb{C}/\mathfrak{N}^{-1}.$$

This gives a point $x_1 \in X_0(N)(H_K)$, where H_K is the Hilbert class field of K. Mapping via the modular parametrization ϕ gives $y_1 \in E(H_K)$. We set $y_K = N_{H_K/K} y_1 \in E(K)$.

Generally, we consider the orders $O_n = \mathbb{Z} + nO_K$. We restrict to squarefree $n \in \mathbb{N}(S)$, positive integers supported on S where S is the set of primes ℓ not dividing NDp such that $\mathrm{Frob}_\ell \in \mathrm{Gal}(K(E[p])/\mathbb{Q})$ is the conjugacy class of complex conjugation. The set S is infinite by Cebotarev's density theorem.

For $n \in \mathbb{N}(S)$, we let $\mathfrak{N}_n = \mathfrak{N} \cap O_n$, then $O_n/\mathfrak{N}_n \cong \mathbb{Z}/N$, and as above, we obtain a point $x_n \in X_0(N)(K_n)$ (called a *Heegner point*), where K_n is the ring class field corresponding to O_n. In particular, $\mathrm{Gal}(K_n/K) \cong \mathrm{Pic}(O_n)$, and we have an exact diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (O_K/nO_K)^\times/(\mathbb{Z}/n)^\times & \longrightarrow & \mathrm{Pic}(O_n) & \longrightarrow & \mathrm{Pic}(O_K) & \longrightarrow & 1 \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ 1 & \longrightarrow & \mathrm{Gal}(K_n/H_K) & \longrightarrow & \mathrm{Gal}(K_n/K) & \longrightarrow & \mathrm{Gal}(H_K/K) & \longrightarrow & 1. \end{array}$$

Finally, we let $y_n = \phi(x_n) \in E(K_n)$. The Kummer classes associated to these points will form our Euler system.

Recall that the short exact sequence

$$0 \to E[p] \to E \xrightarrow{p} E \to 0$$

gives, for any number field L, a long exact sequence on cohomology

$$\cdots \to E(L) \xrightarrow{p} E(L) \to H^1(L, E[p]) \to H^1(L, E) \xrightarrow{p} H^1(L, E) \to \cdots$$

which can be contracted to

$$0 \to E(L)/pE(L) \to H^1(L, E[p]) \to H^1(L, E)[p] \to 0.$$

Recall that

$$\mathrm{Sel}_p(E/L) := \ker\left(H^1(L, E[p]) \to \prod_v H^1(L_v, E)\right),$$

$$Ш(E/L) := \ker\left(H^1(L, E) \to \prod_v H^1(L_v, E)\right),$$

where the products are taken over all places v of L. By the Snake Lemma, we obtain an exact sequence

$$0 \to E(L)/pE(L) \xrightarrow{\delta} \mathrm{Sel}_p(E/L) \to Ш(E/L)[p] \to 0.$$

The following is due to Kolyvagin.

Proposition 4.3. *Let p be a Serre prime for E. Suppose that $y_K \notin pE(K)$. Then $\mathrm{Sel}_p(E/K)$ is cyclic, generated by δy_K.*

Corollary 4.4. *Let p be a Serre prime for E. Suppose that $y_K \notin pE(K)$. Then $E(K)$ has rank 1 and $Ш(E/K)[p] = 0$.*

For p dividing y_K in $E(K)$, Kolyvagin used a more sophisticated argument using p^n instead of p to show that $Ш(E/K)$ is finite, but we will restrict to showing the above proposition for simplicity. We henceforth will also assume that p is a Serre prime for E.

4.2. **The Norm Relation and Kolyvagin's Derivative.** Let $\ell \in S$ as above. Since $\mathrm{Frob}_\ell = \mathrm{Frob}_\infty \in \mathrm{Gal}(K/\mathbb{Q})$, we have that ℓ is inert in K, then splits completely in $K(E[p])/K$. One consequence of this is that $\widetilde{E}_\ell[p] \cong (\mathbb{Z}/p)^2$, where $\widetilde{E}_\ell$ denotes the reduction of E at ℓ. Recall that the characteristic polynomial of Frob_ℓ on $E[p]$ is $x^2 - a_\ell x + \ell$, whereas the characteristic polynomial of complex conjugation on $E[p]$ is $x^2 - 1$. Thus, we have

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}.$$

Now let $n \in \mathbb{N}(S)$ be squarefree. We let

$$G_n = \mathrm{Gal}(K_n/K_1) \cong (O_K/n)^\times/(\mathbb{Z}/n)^\times \cong \prod_{\ell|n}(O_K/\ell)^\times/(\mathbb{Z}/\ell)^\times \cong \prod_{\ell|n}\mathbb{Z}/(\ell+1).$$

For $\ell \mid n$, we let $G_\ell = \mathrm{Gal}(K_n/K_{n/\ell}) \cong \mathbb{Z}/(\ell+1)$ with a fixed generator σ_ℓ. Then $G_n \cong \prod_{\ell|n} G_\ell$. We let N_{G_ℓ} be the norm from G_n to $G_{n/\ell}$.

Lemma 4.5. $N_{G_\ell} y_n = a_\ell y_{n/\ell}$.

Proof. Let T_ℓ be the ℓ-th Hecke operator as a correspondence on $X_0(N)$. This correspondence has bidegree $\ell + 1$ as a divisor on $X_0(N) \times X_0(N)$. So $T_\ell x_{n/\ell}$ is a degree $\ell + 1$ divisor on $X_0(N)$ consisting of points corresponding to quotients of the curve $x_{n/\ell}$ by subgroups of order ℓ. By magic, these correspond to the $\ell + 1$ conjugates of x_n, and the result follows since

$$N_\ell y_n = \phi(N_{G_\ell} x_n) = \phi(T_\ell x_{n/\ell}) = a_\ell \phi(x_{n/\ell}) = a_\ell y_{n/\ell}.$$

(This needs more explanation) □

We let

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i \in \mathbb{Z}[G_\ell].$$

Lemma 4.6. $(\sigma_\ell - 1)D_\ell = \ell + 1 - N_{G_\ell}$.

Proof.

$$\begin{aligned}(\sigma_\ell - 1)D_\ell &= \sum_{i=1}^{\ell} i\sigma_\ell^{i+1} - \sum_{i=1}^{\ell} i\sigma_\ell^i \\ &= \sum_{i=2}^{\ell+1}(i-1)\sigma_\ell^i - \sum_{i=1}^{\ell} i\sigma_\ell^i \\ &= \ell - \sigma_\ell + \sum_{i=2}^{\ell}(i-1)\sigma_\ell^i - \sum_{i=2}^{\ell} i\sigma_\ell^i \\ &= \ell - \sigma_\ell - \sum_{i=2}^{\ell}\sigma_\ell^i \\ &= \ell - \sum_{i=1}^{\ell}\sigma_\ell^i \\ &= \ell + 1 - N_{G_\ell}.\end{aligned}$$

□

We let

$$D_n := \prod_{\ell | n} D_\ell.$$

Proposition 4.7. $[D_n y_n] \in (E(K_n)/pE(K_n))^{G_n}$.

Proof. For all $\ell \mid n$, we have

$$(\sigma_\ell - 1)D_n y_n = (\ell + 1 - N_{G_\ell})D_{n/\ell} y_n = D_{n/\ell}((\ell+1)y_n - a_\ell y_{n/\ell}) \equiv 0 \pmod{p}.$$

□

We now let

$$P_n := \sum_{\sigma \in G_{K_1/K}} \tilde{\sigma}(D_n y_n),$$

where $\tilde{\sigma} \in G_{K_n/K}$ is a chosen lift of σ. Note that $P_1 = y_K$. The above proposition shows that

$$[P_n] \in (E(K_n)/pE(K_n))^{G_{K_n/K}}.$$

4.3. **Cohomology Classes from Points.** We would like to use the classes $[P_n]$ above to obtain classes in $H^1(K, E[p])$.

We have an exact diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E[p]) & \longrightarrow & H^1(K, E)[p] \longrightarrow \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (E(K_n)/pE(K_n))^{G_{K_n/K}} & \xrightarrow{\delta_n} & H^1(K_n, E[p])^{G_{K_n/K}} & \longrightarrow & H^1(K_n, E)[p]^{G_{K_n/K}}. \end{array}$$

We claim that the middle vertical map (restriction) is an isomorphism. By inflation-restriction, its kernel is $H^1(K_n/K, E(K_n)[p])$ and its cokernel is contained in $H^2(K_n/K, E(K_n)[p])$. However, we have the following:

Proposition 4.8. *$E(K_n)[p] = 0$.*

Proof. Suppose that $E(K_n)[p] \neq 0$. Then as groups, we either have

$$E(K_n)[p] \cong \mathbb{Z}/p \qquad \text{or} \qquad E(K_n)[p] \cong (\mathbb{Z}/p)^2.$$

In the first case, $G_{\mathbb{Q}}$ will stabilize $E(K_n)[p]$, so the image of $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p)$ will be contained in a Borel subgroup. This contradicts p being a Serre prime for E. In the second case, we have $K(E[p]) \subseteq K_n$, so $G_{K_n/\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p)$ is a surjection. But since p is odd, $\mathrm{GL}_2(\mathbb{Z}/p)$ cannot be a quotient of a generalized dihedral group (look at centers). So we have a contradiction in either case. □

Finally, we let

$$\boxed{c(n) := \mathrm{res}^{-1}(\delta_n[P_n]) \in H^1(K, E[p]).}$$

Lemma 4.9. *Let $d(n) \in H^1(K, E)[p]$ be the image of $c(n)$. Then:*

1. *$d(n)$ is the inflation of a cocycle $\widetilde{d}(n) \in H^1(K_n/K, E)[p]$.*
2. *$c(n) \in H^1(K, E[p])$ is trivial if and only if $P_n \in pE(K_n)$.*
3. *$d(n) \in H^1(K, E)[p]$ is trivial if and only if $\widetilde{d}(n) \in H^1(K_n/K, E)[p]$ is trivial if and only if $P_n \in pE(K_n) + E(K)$.*

Proof. For (1), it suffices to see that $d(n)$ is in the kernel of restriction

$$H^1(K, E) \to H^1(K_n, E).$$

This is the right vertical map in the above diagram. However, tracing the right square the other direction shows this triviality. The other statements come from similar diagram chases. □

4.4. **Eigenspaces.** Recall that the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle \cong \mathbb{Z}/2$ acts on $H^1(K, -)$. We have a corresponding decomposition into eigenspaces

$$H^1(K, E[p]) = H^1(K, E[p])^+ \oplus H^1(K, E[p])^-.$$

Let $\epsilon = \pm 1$ be the negative of the sign of the functional equation for $L(E, s)$. Alternatively, ϵ is the eigenvalue of the Fricke involution

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

acting on the eigenform associated to E.

Proposition 4.10. *$c(n) \in H^1(K, E[p])^{\epsilon_n}$ and $d(n) \in H^1(K, E)[p]^{\epsilon_n}$, where $\epsilon_n = \epsilon\mu(n)$, where $\mu(n)$ is the Möbius function.*

Proof. Omitted. □

4.5. **Duality.** Fix a finite place v of K at which E has good reduction. Let O_v denote the ring of integers of K_v, and let k_v denote the residue field. Since E has good reduction at v, we have that inertia at v acts trivially on $E(\overline{K_v})$.

Lemma 4.11. $H^1(K_v^{ur}/K_v, E) = 0$.

Proof. Omitted. □

Corollary 4.12. *The Kummer map gives an isomorphism*

$$E(K_v)/pE(K_v) \cong H^1(K_v^{ur}/K_v, E[p]).$$

Recall that the *Weil pairing*

$$E[p] \times E[p] \to \mu_p$$

is a Galois invariant, non-degenerate, skew-symmetric, bilinear pairing. Combined with the cup product on Galois cohomology, we obtain a pairing

$$\langle \cdot, \cdot \rangle : H^1(K_v, E[p]) \times H^1(K_v, E[p]) \to H^2(K_v, \mu_p) \cong \mathbb{Z}/p,$$

where the last isomorphism comes from the invariant map. This pairing is non-degenerate as a consequence of the following major theorem:

Theorem 4.13 (Local Tate Duality)**.** *Let A be a finite G_{K_v}-module. The cup product and evaluation give a pairing*

$$H^i(K_v, \mathrm{Hom}(A, \mu)) \times H^{2-i}(K_v, A) \to H^2(K_v, \mu) \cong \mathbb{Q}/\mathbb{Z}$$

that, for $0 \leq i \leq 2$, induces an isomorphism

$$H^i(K_v, \mathrm{Hom}(A, \mu)) \cong \mathrm{Hom}(H^{2-i}(K_v, A), \mathbb{Q}/\mathbb{Z}).$$

Proposition 4.14. *The pairing $\langle \cdot, \cdot \rangle$ above induces a non-degenerate pairing*

$$E(K_v)/p \times H^1(K_v, E)[p] \to \mathbb{Z}/p.$$

Proof. This amounts to the fact that $E(K_v)/p \cong H^1(K_v^{ur}/K_v, E[p])$ is its own annihilator under the pairing above. This is due to Tate, and we omit the proof here. □

Now let $L = K(E[p])$. We assumed that D is coprime to Np, so that $\mathcal{G} = \mathrm{Gal}(L/K) \cong \mathrm{GL}_2(\mathbb{Z}/p)$.

Proposition 4.15. *Restricting and evaluating cocycles gives a pairing*

$$[\cdot, \cdot] : H^1(K, E[p]) \times G_L \to E(L)[p].$$

If $s \in H^1(K, E[p])$ is such that $[s, \rho] = 0$ for all $\rho \in G_L$, then $s = 0$.

Proof. Omitted. Follows from an argument due to Serre involving the Hochschild–Serre spectral sequence. □

Let

$$G_{\mathrm{Sel}} = \{\rho \in G_L : [s, \rho] = 0 \text{ for all } s \in \mathrm{Sel}_p(E/K) \subseteq H^1(K, E[p])\}.$$

Let M be the fixed field of G_{Sel}.

Proposition 4.16. *The induced pairing*

$$[\cdot, \cdot] : \mathrm{Sel}_p(E/K) \times \mathrm{Gal}(M/L) \to E(L)[p]$$

is perfect. In particular, we have isomorphisms

$$\mathrm{Sel}_p(E/K) \cong \mathrm{Hom}(\mathrm{Gal}(M/L), E(L)[p]),$$

$$\mathrm{Gal}(M/L) \cong \mathrm{Hom}(\mathrm{Sel}_p(E/K), E(L)[p]).$$

Proof. Omitted. □

We let $H = \mathrm{Gal}(M/L) \cong \mathrm{Hom}(\mathrm{Sel}_p(E/K), E[p])$. Let I be the kernel of δy_K restricted to H. Complex conjugation τ acts on these Galois groups by conjugation.

Lemma 4.17. *We have $H^+/I^+ \cong \mathbb{Z}/p$, and*

$$H^+ = \{(\tau h)^2 : h \in H\}, \qquad I^+ = \{(\tau i)^2 : i \in I\}.$$

Proof. Note that H has odd order, as p is odd. So we can recover H^+ as $H^{1+\tau}$. For $h \in H$, we have

$$h^{1+\tau} = \tau h \tau^{-1} h = (\tau h)^2.$$

A similar argument works for I^+. Then

$$H^+/I^+ \cong (H/I)^+ = E_p^+ \cong \mathbb{Z}/p.$$

□

Proposition 4.18. *Let $s \in \mathrm{Sel}_p(E/K)^{\pm}$. The following are equivalent:*

(1) $s = 0$;

(2) $[s, \rho] = 0$ *for all* $\rho \in H$;

(3) $[s, \rho] = 0$ *for all* $\rho \in H^+$;

(4) $[s, \rho] = 0$ *for all* $\rho \in H^+ - I^+$.

Proof. We prove the case where $s \in \mathrm{Sel}_p(E/K)^+$. The forward implications are clear. Suppose $[s, \rho] = 0$ for all $\rho \in H^+ - I^+$. Then s vanishes on all of H^+ by group theory ($H^+ \neq I^+$). We have a $\mathcal{G}$-map $H \to E[p]$ that preserves $\pm$-eigenspaces, so $s(H) \subset E[p]^-$. But $E[p]$ is a simple $\mathcal{G}$-module, so $s(H) = 0$. By the perfectness of the pairing $[\cdot, \cdot]$, we have $s = 0$. □

4.6. **The Main Propositon.** Throughout this section, we suppose that p is a Serre prime for E and that $y_K \notin pE(K)$. Recall that for $\ell \in S$, we have ℓ is unramified in M, inert in $K/\mathbb{Q}$, and splits in L/K. So Frob_ℓ looks like τh for some $h \in H$.

As preparation for the main proof, we give the following proposition:

Proposition 4.19 (Preparation)**.** *The following are equivalent:*

(1) $c(\ell) = 0$*;*

(2) $c(\ell) \in \mathrm{Sel}(E/K)_p$*;*

(3) $P_\ell \in pE(K_\ell)$*;*

(4) $d(\ell) = 0$*;*

(5) $d(\ell)_v = 0 \in H^1(K_v, E[p])$ *for* v *the place of* K *above* ℓ*;*

(6) $P_1 = y_K \in pE(K_v)$ *for* $v \mid \ell$*.*

(7) $h^{1+\tau} \in I^+$*.*

Proof. Omitted for now. □

We now arrive at the proof of Proposition 4.3.

Proposition 4.20 (Proposition 4.3)**.** *Let* p *be a Serre prime for* E*. Suppose that* $y_K \notin pE(K)$*. Then* $\mathrm{Sel}_p(E/K)$ *is cyclic, generated by* δy_K*.*

Proof sketch. Recall that $\delta y_K = c(1) \in \mathrm{Sel}_p(E/K)^\epsilon$. We first show that $\mathrm{Sel}_p(E/K)^{-\epsilon} = 0$...

It then suffices to show that

$$\mathrm{Sel}_p(E/K)^\epsilon \cong (\mathbb{Z}/p) \cdot \delta y_K.$$

By the Kummer duality above, it suffices to show that $s \in \mathrm{Sel}_p(E/K)^\epsilon$ satisfies $[s, \rho] = 0$ for all $\rho \in I$. By a similar argument as before, we can restrict to I^+, so we take $\rho = (\tau i)^2$ for $i \in I$.

Let $q \in S$ be such that $c(q) \neq 0 \in H^1(K, E[p])$ (which we can do by the above preparation). Let L' be the fixed field of the kernel of $c(q)$ restricted to L. Then L'/L is disjoint from M/L and has Galois group isomorphic to $E[p]$.

Let $\ell \in S$ be such that $\mathrm{Frob}_\ell = \tau i \in \mathrm{Gal}(M/\mathbb{Q})$ and $\mathrm{Frob}_\ell = \tau j \in \mathrm{Gal}(L'/\mathbb{Q})$ with $j^{1+\tau} \neq 1$. By an unstated proposition, one shows that $d(\ell q)_v = 0$ for $v \nmid \ell$ and $d(\ell q)_v \neq 0$ for $v \mid \ell$. By another proposition, $s_v = 0$ for v the place of K above ℓ. By Cebotarev, we can choose several ℓ to get vanishing of s on all of I^+. □

5. Shimura varieties

5.1. **Modular curves, Adelically.** To motivate the Shimura curves we consider, we first show how modular curves can be interpreted adelically. The reference for this section is [3, §38.6].

Let $\mathfrak{H}$ be the complex upper half-plane, our first example of a symmetric space. Recall that $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathfrak{H}$ with stabilizer at i given by $\mathrm{SO}_2(\mathbb{R})$. Note the $\mathrm{SO}_2(\mathbb{R})$ is a maximal compact subgroup of $\mathrm{GL}_2(\mathbb{R})$. This gives an isometry

$$\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \cong \mathfrak{H}.$$

Let $\mathfrak{H}^{\pm} = \mathfrak{H} \cup \mathfrak{H}^{-}$ denote the union of the upper and lower complex half-planes. We similarly obtain a Riemannian isometry

$$\mathrm{GL}_2(\mathbb{R})/\mathbb{R}^{\times}\,\mathrm{SO}_2(\mathbb{R}) \cong \mathfrak{H}^{\pm}.$$

We have the classical modular curve

$$Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \cong \mathrm{GL}_2(\mathbb{Z})\backslash\mathfrak{H}^{\pm},$$

which we can now write as

$$Y(1) = \mathrm{GL}_2(\mathbb{Z})\backslash\,\mathrm{GL}_2(\mathbb{R})/\mathbb{R}^{\times}\,\mathrm{SO}_2(\mathbb{R}).$$

We now suggestively let $G = \mathrm{GL}_2$ (the algebraic group). Recall the ring of adeles $\mathbb{A}$ of $\mathbb{Q}$ has a decomposition

$$\mathbb{A} = \mathbb{Q}_f \times \mathbb{Q}_\infty$$

where $\mathbb{Q}_f$ is the ring of finite adeles and $\mathbb{Q}_\infty = \mathbb{R}$.

Similarly, $G(\mathbb{Q}_{\mathbb{A}})$ has a decomposition

$$G(\mathbb{A}) \cong G(\mathbb{Q}_f) \times G(\mathbb{Q}_\infty).$$

Here $G(\mathbb{Q}_f)$ has a compact open subgroup $G(\widehat{\mathbb{Z}})$ and $G(\mathbb{Q}_\infty)$ has maximal compact subgroup K_∞. As a consequence of strong approximation, we have a bijection

$$G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}}) \cong G(\mathbb{Z})\backslash G(\mathbb{R}).$$

Putting this all together, we have

$$\begin{aligned} Y(1) &= \mathrm{GL}_2(\mathbb{Z})\backslash\,\mathrm{GL}_2(\mathbb{R})/\mathbb{R}^{\times}\,\mathrm{SO}_2(\mathbb{R}) \\ &= (G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}}))/\mathbb{R}^{\times}\,\mathrm{SO}_2(\mathbb{R}) \\ &= G(\mathbb{Q})\backslash G(\mathbb{A})/K \end{aligned}$$

where $K = G(\widehat{\mathbb{Z}}) \times \mathbb{R}^{\times}\,\mathrm{SO}_2(\mathbb{R})$.

5.2. **Review of Quaternion Algebras.** Let B be a quaternion algebra over a totally real number field F. In other words, B is the non-commutative algebra over F generated by i, j such that for some $a, b \in F$, we have

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

For instance, one could take $B = M_2(F)$. The algebra B comes equipped with a *standard (anti)involution* $\beta \mapsto \overline{\beta}$ given on the generators by $\overline{i} = -i$ and $\overline{j} = -j$. This induces a reduced norm map $\nu : B^\times \to F^\times$ where

$$\nu(\beta) = \beta\overline{\beta}.$$

For a place v of F, $B_v := B \otimes_F F_v$ is either isomorphic to $M_2(F_v)$ or the unique division quaternion algebra over F_v. In the former case, we say B is *unramified at* v, and in the latter case, we say that B is *ramified at* v. It is well-known that the set of ramified places of B is finite and of even cardinality.

In particular, if v is a real place of F, then $B_v \cong M_2(\mathbb{R})$ or $B_v \cong \mathbb{H}$. Then $B_v^\times$ has maximal compact subgropu $\mathrm{SO}_2(\mathbb{R})$ or $\mathbb{H}^1$ (norm 1 quaternions). We let r be the number of real ramified places of B and s the number of real unramified places of B. We say B satisfies the *Eichler condition* if $s > 0$.

5.3. **Quaternionic Shimura Varieties.** For this subsection, we also refer to online notes of Jacques Tilouine titled "Quaternionic and Hilbert modular forms and their Galois representations." We describe a slightly more general class of Shimura variety.

We can view $B^\times$ as an algebraic group over F. Let $G := \mathrm{res}^F_{\mathbb{Q}}(B^\times)$. We also define

$$G^* := \{g \in G : \nu(g) \in \mathbb{Q}^\times\},$$
$$G^1 := \{g \in G^* : \nu(g) = 1\}.$$

We let $K_\infty = \mathrm{SO}_2(\mathbb{R})^s \times (\mathbb{H}^1)^r$.

Definition 5.1. Let $U \subseteq G(\mathbb{Q}_f)$ be a compact open subgroup. The *Shimura variety for G of level U* is

$$X(U) := G(\mathbb{Q})\backslash G(\mathbb{A})/U(F_\infty^\times K_\infty).$$

We will eventually see that for U sufficiently small, $X(U)$ has the structure of a smooth complex variety.

Theorem 5.2. *Fujisaki If B is a division algebra, then $X(U)$ is compact for all U.*

6. Building Euler Systems

We now examine some ways of constructing Euler systems. We use Jannsen's "continuous étale cohomology" unless otherwise stated.

6.1. **Hochschild–Serre.** Let X be a variety over a number field K.

Theorem 6.1 (Jannsen's Hochschild–Serre spectral sequence)**.** *For any $n \in \mathbb{Z}$, there exists a convergent spectral sequence*

$$E_2^{ij} = H^i(K, H^j_{et}(X_{\overline{K}}, \mathbb{Q}_p(n))) \Rightarrow H^{i+j}_{et}(X, \mathbb{Q}_p(n)).$$

Let

$$\varphi_i : H^i(X, \mathbb{Q}_p(n)) \to H^0(K, H^i_{et}(X_{\overline{K}}, \mathbb{Q}_p)(n)) = H^i_{et}(X_{\overline{K}}, \mathbb{Q}_p(n))^{G_K}$$

be the corresponding edge morphism in this spectral sequence. This factors as

$$H^i(X, \mathbb{Q}_p(n)) \to E_\infty^{0,i} \hookrightarrow E_2^{0,i}.$$

The kernel of this map is $F^1H^i(X, \mathbb{Q}_p(n))$. We also get an injective map $E_\infty^{1,i-1} \to E_2^{1,i-1}$. Recall that

$$E_\infty^{1,i-1} = F^1H^i(X, \mathbb{Q}_p(n))/F^2H^i(X, \mathbb{Q}_p(n))$$

$$E_\infty^{0,i} = H^i(X, \mathbb{Q}_p(n))/F^1H^i(X, \mathbb{Q}_p(n)).$$

The composition

$$F^1H^i(X, \mathbb{Q}_p(n)) \to E_\infty^{1,i-1} \to E_2^{1,i-1} = H^1(K, H^{i-1}(X_{\overline{K}}, \mathbb{Q}_p(n)))$$

gives us a way to cook up Euler systems. Namely, if our representation is $V = H^{i-1}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n))$ for X a $\mathbb{Q}$-variety, we can find special elements of $F^1H^i(X_{\mathbb{Q}(\mu_m)}, \mathbb{Q}_p(n))$ giving classes in $H^1(\mathbb{Q}(\mu_m), V)$ for varying m.

6.2. **Loeffler–Zerbes' "Bag of Tricks".** We thus seek to construct cohomology classes in $H^i(X, \mathbb{Q}_p(n))$. Loeffler and Zerbes give the following as tools to construct such classes:

(1) Cup products:

$$H^i(X, \mathbb{Q}_p(n)) \otimes H^j(X, \mathbb{Q}_p(m)) \to H^{i+j}(X, \mathbb{Q}_p(n+m)).$$

(2) Kummer maps:

$$\mathcal{O}(X)^\times \to H^1(X, \mathbb{Q}_p(1)).$$

(3) Pushforward maps: for $Z \subset X$ a smooth codimension d subvariety of a smooth variety X, we have

$$H^i(Z, \mathbb{Q}_p(n)) \to H^{i+2d}(X, \mathbb{Q}_p(n+d)).$$

In the case where $i = n = 0$, the element $1 \in H^0(Z, \mathbb{Q}_p)$ gives $1_Z \in H^{2d}(X, \mathbb{Q}_p(d))$ the *cycle class of* Z.

6.3. **Galois Representations Attached to Modular Forms.** Let $f = \sum_n a_n q^n$ be a normalized cuspidal Hecke eigenform of weight 2 and level $\Gamma_1(N)$. Let L be the number field generated by the Fourier coefficients of f. We suppose that L embeds into a p-adic field E and view L as a subfield of E.

Definition 6.2. We let $V_p(f)$ be the largest subspace

$$V_p(f) \subseteq H^1_{et}(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} E$$

on which the Hecke operators $T(\ell)$ act as $a_\ell(f)$ for $\ell \nmid N$.

We list the following facts:

- $V_p(f)$ is a 2-dimensional irreducible p-adic Galois representation.
- $V_p(f)$ is a direct summand of H^1.
- For $\ell \nmid Np$, the local Euler factor at p is given by

$$P_\ell(V_p(f), s) = 1 - a_\ell(f)t + \ell\chi(\ell)t^2,$$

where χ is the character of f.

- If f corresponds to an elliptic curve A, then

$$V_p(f) \cong H^1(A_{\overline{Q}}, \mathbb{Q}_p) \cong V_p(A)(-1).$$

We seek to construct an Euler system for $V_p(f)$. Note that $Y_1(N)$ is an affine curve, so $H^2(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) = 0$. Then Hochschild–Serre gives us a map

$$H^2(Y, \mathbb{Q}_p(1)) \to H^1(\mathbb{Q}, H^1(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)(n)) \to H^1(\mathbb{Q}, V_p(f)).$$

6.4. **Sneaking up on Cyclotomic Fields.** Let X be a $\mathbb{Q}$-variety, We seek to build Euler systems for $H^i(X_{\overline{Q}}, \mathbb{Q}_p(n))$. This requires constructing classes in $H^1(K, H^i(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n)))$ for K varying over cyclotomic fields. Recall the Hochschild–Serre spectral sequence:

$$E_2^{ij}: \quad H^i(K, H^j(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n))) \Rightarrow H^{i+j}(X_K, \mathbb{Q}_p(n)).$$

In particular, we have edge morphisms

$$\varphi_i : H^{i+1}(X_K, \mathbb{Q}_p(n)) \to H^{i+1}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n))^{G_K}$$

and if we set $F^1H^{i+1}(X_K, \mathbb{Q}_p(n))$ to be the kernel of this map, we have a map

$$\psi_i : F^1H^{i+1}(X_K, \mathbb{Q}_p(n)) \to H^1(K, H^i(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n))).$$

We thus will seek classes in $H^i(X_K, \mathbb{Q}_p(n))$ for K varying over cyclotomic fields. It turns out that proving norm relations is easier if we somehow view this as cohomology of a different modular curve.

Recall that for an open compact subgroup $U \subset \mathrm{GL}_2(\mathbb{A}_f)$, we have a $\mathbb{Q}$-curve $X(U)$ whose $\mathbb{C}$-points are

$$X(U)(\mathbb{C}) \cong \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{A}) / U(\mathbb{R}^\times \mathrm{SO}_2(\mathbb{R})).$$

Decomposing $\mathrm{GL}_2(\mathbb{A})$ as $\mathrm{GL}_2(\mathbb{R}) \times \mathrm{GL}_2(\mathbb{Q}_f)$, we may identify

$$X(U)(\mathbb{C}) \cong \mathrm{GL}_2^+(\mathbb{Q}) \backslash [\mathfrak{H} \times \mathrm{GL}_2(\mathbb{A}_f)/U]$$

For example, if

$$U_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) : c \equiv 0, d \equiv 1 \pmod{N} \right\}$$

then $X(U_1(N)) = Y_1(N)$. On the other hand, if we let

$$U_1(N)_m = \{u \in U_1(N) : \det(u) \equiv 1 \pmod{m}\},$$

then

$$X(U_1(N)_m) \cong Y_1(N) \times_{\mathbb{Q}} \mu_m^\circ,$$

where μ_m° is the $\mathbb{Q}$-variety of primitive m-th roots of unity. Note that as $\mathbb{Q}$-schemes,

$$Y_1(N) \times_{\mathbb{Q}} \mu_m^\circ = Y_1(N) \times_{\mathbb{Q}} \operatorname{Spec} \mathbb{Q}(\mu_m) \cong Y_1(N)_{\mathbb{Q}(\mu_m)}.$$

Thus, varying the level of our modular curve achieves the same thing as base changing to various cyclotomic fields.

7. Siegel Units

7.1. **Introducing Siegel Units.** Recall that for a $\mathbb{Q}$-variety X, we have Kummer maps

$$\mathcal{O}(X)^\times \to H^1(X, \mathbb{Q}_p(1)).$$

This gives us a way to construct cohomology classes by using global units on X.

Definition 7.1. Let $U \subset \mathrm{GL}_2(\mathbb{A}_f)$ be a compact open subgroup and $X(U)$ the corresponding (open) modular curve. A *modular unit of level U* is an element of $\mathcal{O}(X(U))^\times$.

Let

$$U(N) = \ker(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N))$$

Proposition 7.2. *Modular units of level $U(N)$ are in bijection with holomorphic functions on $\Gamma(N)\backslash\mathfrak{H}$ that are nonzero away from the cusps, meromorphic at the cusps, and whose q-expansions at the cusps have coefficients in $\mathbb{Q}(\mu_N)$.*

Definition 7.3. Let $(\alpha, \beta) \in (\mathbb{Q}/\mathbb{Z})^2 - 0$. The function $g_{\alpha,\beta}$ is constructed as follows: write

$$(\alpha, \beta) = (a/N, b/N), \qquad a, b, N \in \mathbb{Z}, \quad N \geq 1, \quad 0 \leq a < N.$$

Then setting $q = e^{2\pi i \tau}$ and

$$w = \frac{1}{12} - \frac{a}{N} + \frac{a^2}{2N^2},$$

we let

$$g_{\alpha,\beta}(\tau) = q^w \prod_{n \geq 0}(1 - q^{n+a/N}\zeta_N^b) \prod_{n \geq 1}(1 - q^{n-a/N}\zeta_N^{-b}).$$

Definition 7.4. A Siegel unit is a function of the form

$${}_c g_{\alpha,\beta} = \frac{(g_{\alpha,\beta})^{c^2}}{g_{c\alpha,c\beta}},$$

where $c > 1$ is coprime to 6 and the order of α and β in $\mathbb{Q}/\mathbb{Z}$.

Remark 7.5. According to Loeffler–Zerbes and Sharifi, pretty much all known examples of Euler systems come from Siegel units.

Proposition 7.6. *For $\alpha, \beta \in (\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2 - 0$, the Siegel units ${}_cg_{\alpha,\beta}$ are modular units of level $U(N)$. Moreover, $\mathrm{GL}_2(\mathbb{Z}/N)$ acts on $X(U(N))$ and transforms Siegel units by*

$$ {}_cg_{\alpha,\beta}|\sigma = {}_cg_{(\alpha,\beta)\sigma}. $$

Here, $(\alpha,\beta)\sigma$ denotes right-multiplication of a row vector by $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N)$.

Proposition 7.7. *The function ${}_cg_{0,1/N}$ is a modular unit of level $U_1(N)$.*

Proof. □

7.2. **An alternate definition of Siegel units.** Here is an alternate description of Siegel units. Recall that $Y(N)$ parametrizes elliptic curves with full level N structure. Let $\mathcal{E} \to Y(N)$ denote the universal elliptic curve over $Y(N)$. This elliptic scheme comes equipped with N-torsion sections $\iota_1, \iota_2 : Y(N) \to \mathcal{E}$. For $\alpha, \beta \in (\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2 - 0$, write $\alpha = a/N$ and $\beta = b/N$. Let

$$ \iota_{a,b} = a\iota_1 + b\iota_2 : Y(N) \to \mathcal{E}. $$

We recall the following fact about elliptic curves.

Lemma 7.8. *Let E be an elliptic curve, and let $D = \sum_{x\in E} n_x(x)$ be a divisor on E. Then D is a principal divisor if and only if $\sum_{x\in E} n_x = 0$ and $\sum_{x\in E}[n_x]x = 0 \in E$.*

Let $c > 1$ be an integer coprime to $6N$. Then $c^2(0) - \mathcal{E}[c]$ is a divisor of degree 0 that sums to 0, so is the divisor of some rational function $\theta \in \overline{\mathbb{Q}}(\mathcal{E})^\times$. Note that this divisor is also stable under pushforward along the multiplication by N map $[N] : \mathcal{E} \to \mathcal{E}$, so we can rescale θ so that $[n]_*\theta = \theta$. Since θ only has zeroes and poles along 0 and c-torsion, the pullback ${}_cg_{\alpha,\beta} := \iota_{a,b}^*\theta$ is a global unit on $Y(N)$.

7.3. **The Norm Relation.** We now describe the basic norm relation that Siegel units satisfy.

Proposition 7.9. *Let $\alpha, \beta \in \mathbb{Q}/\mathbb{Z}$ not both zero, and let $A \geq 1$. Let c be coprime to $6A$ and the order of α and β. Then the following relations hold:*

(1) $\prod_{A\alpha'=\alpha} {}_cg_{\alpha',\beta}(\tau) = {}_cg_{\alpha,\beta}(A^{-1}\tau)$;

(2) $\prod_{A\beta'=\beta} {}_cg_{\alpha,\beta'}(\tau) = {}_cg_{\alpha,\beta}(A\tau)$;

(3) $\prod_{A(\alpha',\beta')=(\alpha,\beta)} {}_cg_{\alpha',\beta'}(\tau) = {}_cg_{\alpha,\beta}(\tau)$.

Proof. Note that (1) and (2) together imply (3). Furthermore, suppose (1) is true. Let $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$\begin{aligned}
\prod_{A\beta'=\beta} {}_c g_{\alpha,\beta'}(\tau) &= \prod_{A\beta'=\beta} ({}_c g_{\alpha,\beta'} | JJ^{-1})(\tau) \\
&= \prod_{A\beta'=\beta} {}_c g_{-\beta',\alpha}(-1/\tau) \\
&= {}_c g_{-\beta,\alpha}(-A/\tau) \\
&= ({}_c g_{-\beta,\alpha} | J^{-1}J)(-/A\tau) \\
&= {}_c g_{\alpha,\beta}(A\tau).
\end{aligned}$$

It then suffices to prove (1). We omit the proof for now. □

Let ℓ be a prime, and let $\pi : Y_1(N\ell) \to Y_1(N)$ be the quotient map. Recall that since this is a finite morphism, we may define the *norm* $\pi_* : \mathcal{O}(Y_1(N\ell))^\times \to \mathcal{O}(Y_1(N))^\times$ given by

$$(\pi_* f)(x) = \prod_{y \in \pi^{-1}(x)} f(y).$$

Corollary 7.10. *We have*

$$\pi_*({}_c g_{0,1/N\ell}) = \begin{cases} {}_c g_{0,1/N}, & \ell \mid N, \\ {}_c g_{0,1/N} \cdot ({}_c g_{0,u/N})^{-1}, & \ell \nmid N, \end{cases}$$

where u is the inverse of ℓ mod N when $\ell \nmid N$.

Proof. Let $\tau \in Y_1(N) = \Gamma_1(N)\backslash\mathfrak{H}$. Elements of the fiber of π over τ are given by $\gamma\tau$ for γ in a set of coset representatives of $\Gamma_1(N\ell)\backslash\Gamma_1(N)$.

Suppose first that $\ell \mid N$.

$$\pi_*({}_c g_{0,1/N\ell})(\tau) = \prod_{\gamma \in \Gamma_1(N\ell)\backslash\Gamma_1(N)} {}_c g_{0,1/N\ell}(\gamma\tau) = \prod_{\gamma \in \Gamma_1(N\ell)\backslash\Gamma_1(N)} {}_c g_{(0,1/N\ell)\gamma}(\tau)$$

Note that for $\gamma = \begin{pmatrix} a & b \\ Nc & 1+Nd \end{pmatrix} \in \Gamma_1(N)$, we have

$$(0, 1/N\ell) \begin{pmatrix} a & b \\ Nc & 1+Nd \end{pmatrix} = (c/\ell, 1/N\ell + d/\ell).$$

So γ stabilizes $(0, 1/N\ell)$ if and only if $\gamma \in \Gamma_1(N\ell)$. Furthermore, the orbit of $(0, 1/N\ell)$ under $\Gamma_1(N)$ consists precisely of (α', β') such that $\ell(\alpha', \beta') = (0, 1/N)$ (using that $\ell \mid N$). So

$$\pi_*({}_c g_{0,1/N\ell})(\tau) = \prod_{\ell(\alpha',\beta')=(0,1/N)} {}_c g_{\alpha',\beta'}(\tau) = {}_c g_{0,1/N}(\tau).$$

We omit the proof for $\ell \nmid N$. □

References

[1] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[2] David Loeffler and Sarah Livia Zerbes. Euler systems (arizona winter school 2018 notes).

[3] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021.