Local Tate Duality for Elliptic Curves: Dual Isogenies, Weil Pairings, and Hilbert Symbols

Hurui Yao

October 9, 2026

Abstract: This report displays local Tate duality for a degree-two isogeny $\varphi : E \to E'$ between elliptic curves with good reduction over a finite extension $K/\mathbb{Q}_p$, where $p \neq 2$. We construct the dual isogeny and the pairing on the isogeny kernels, and identify the induced cohomological pairing with the quadratic Hilbert symbol. The key step identifies the local Kummer images with the unramified cohomology subgroups, which correspond in square-class coordinates to the subgroup U of unit square classes. The identity $U^{\perp} = U$ under the Hilbert symbol then yields the central orthogonality theorem: $L_{\varphi}^{\perp} = L_{\hat{\varphi}}$ and $L_{\hat{\varphi}}^{\perp} = L_{\varphi}$. This establishes perfect pairings between the corresponding quotients of rational point groups and isogeny-torsion subgroups of the Weil–Châtelet groups. An explicit example over $\mathbb{Q}_5$ illustrates the Kummer images and computes a nonzero local pairing value.

Assumptions and Notations

The following assumptions and notations are those used throughout the whole report.

(1) K: a finite extension of $\mathbb{Q}_p$, with $p \neq 2$ and $\operatorname{char} K = 0$.
(2) $\overline{K}$: a fixed algebraic closure of K.
(3) $G_K = \operatorname{Gal}(\overline{K}/K)$: the absolute Galois group.
(4) $v_K : K^\times \to \mathbb{Z}$: the normalized valuation; $v_K(0) = +\infty$.
(5) $\mathcal{O}_K = \{a \in K : v_K(a) \geq 0\}$: the valuation ring.
(6) $\mathfrak{m}_K = \{a \in K : v_K(a) > 0\}$: the maximal ideal of $\mathcal{O}_K$.
(7) ϖ: a uniformizer, so $v_K(\varpi) = 1$ and $\mathfrak{m}_K = \varpi\mathcal{O}_K$.
(8) $k = \mathcal{O}_K/\mathfrak{m}_K = \mathbb{F}_q$: the residue field, of cardinality q.
(9) $K^{\mathrm{ur}} \subset \overline{K}$: the maximal unramified extension of K.
(10) $I_K = \operatorname{Gal}(\overline{K}/K^{\mathrm{ur}})$: the inertia group.
(11) $G_k = \operatorname{Gal}(\overline{k}/k)$: the absolute Galois group of the residue field.
(12) $\mathrm{Frob}_q \in G_k$: arithmetic Frobenius, $a \mapsto a^q$.
(13) E, E': elliptic curves over K, with identities O, O'.
(14) $\varphi : E \to E'$: a K-isogeny of degree two.
(15) $\widehat{\varphi} : E' \to E$: its dual, to be constructed in the main text.
(16) $M = E[\varphi] = \ker(\varphi : E(\overline{K}) \to E'(\overline{K}))$.
(17) $N = E'[\widehat{\varphi}] = \ker(\widehat{\varphi} : E'(\overline{K}) \to E(\overline{K}))$.
(18) $\mu_2 = \{1, -1\} \subset K^\times$: the square roots of unity.
(19) $D = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$: the additive target group, with elements written 0 and $\frac{1}{2}$.
(20) $S_K = K^\times/K^{\times 2}$: the square-class group; $[a]$ is the class of a.
(21) $U = \operatorname{im}(\mathcal{O}_K^\times \to S_K)$: the subgroup of unit square classes.
(22) $H^i(K, A) = H^i_{\mathrm{cont}}(G_K, A)$: continuous cohomology, with discrete coefficients A.

Elliptic-curve and cohomology groups are written additively; $K^\times$, S_K, and μ_2 are written multiplicatively. Thus the identity in S_K is 1. Good reduction is imposed only in the local duality argument.

Contents

1 Preliminaries **5**

1.1 Elliptic Curves and Isogenies 5
1.2 Local Fields and Unramified Extensions 6
1.3 Low-Degree Galois Cohomology 7
1.4 Local Class Field Theory and the Hilbert Symbol 8
1.5 Good Reduction and Formal Groups 9
1.6 Finite Pairings and Torsors 10

2 Divisor Classes and Dual Isogenies **11**

2.1 Points and Divisor Classes of Degree Zero 11
2.2 Constructing the Dual Isogeny 11
2.3 Interpreting the Dual Isogeny as Pullback 13
2.4 The Dual Kernel and Functions for the Pairing 13

3 Degree-Two Isogenies and the Kernel Pairing **15**

3.1 An Explicit Pair of Degree-Two Isogenies 15
3.2 Constructing the Kernel Pairing by Divisor Pullback 17
3.3 Nondegeneracy of the Kernel Pairing 19
3.4 An Explicit Computation in the Running Example 20

4 Hilbert Symbols and the Cohomological Pairing on the Kernels **22**

4.1 Kummer Theory for the Multiplicative Group and Square-Class Coordinates 22
4.2 Constructing the Cohomological Pairing 23
4.3 The Orthogonal Complement of the Unit Square Classes 25

5 Kummer Exact Sequences and Coordinate Formulas **28**

5.1 The Two Kummer Exact Sequences 28
5.2 Kummer Coordinates for the Isogeny in the Running Example 29
5.3 Kummer Coordinates for the Dual Isogeny 31
5.4 The Local Kummer Images 32

6 Local Duality under Good Reduction **33**

6.1 The Isogenies on the Kernels of Reduction 33
6.2 The Kummer Images Are Unramified 34
6.3 The Orders of the Kummer Images 35
6.4 Unit Square Classes and the Orthogonal-Complement Theorem 36
6.5 From Orthogonal Complements to Finite-Level Local Duality 37

7 An Explicit Computation over $\mathbb{Q}_5$ **40**
7.1 The Curves and the Square-Class Group 40
7.2 Explicit Generators of the Kummer Images 40
7.3 The Quadratic Hilbert Symbol 41
7.4 A Nonzero Value of the Local Tate Pairing 42

1 Preliminaries

This section will give some basic definitions and theorems needed in the following sections, including elliptic curves, local fields, Hilbert symbol and class field theory. All the materials in this section come from ***Elliptic Curves*** and ***Class Field Theory*** by J. S. Milne

1.1 Elliptic Curves and Isogenies

Definition 1.1.1. An **elliptic curve** over F is a smooth, projective, geometrically connected genus-one curve with $O \in E(F)$. For $\operatorname{char} F \neq 2$, it admits a model (**Weierstrass model**)

$$y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6, \qquad O = [0:1:0], \qquad \Delta = 16\operatorname{disc}(f) \neq 0.$$

If $\operatorname{char} F \neq 2, 3$, one may use $y^2 = x^3 + Ax + B$, with $\Delta = -16(4A^3 + 27B^2)$.

If the residue characteristic is 3, eliminating x^2 need not preserve integrality. Integral models may therefore retain this term.

Theorem 1.1.2 (Group law and torsion)**.** *The point O determines a commutative algebraic group structure on E. Put*

$$\tau_P(Q) = Q + P, \qquad [n](P) = nP, \qquad E[n] = \ker([n] : E(\overline{F}) \to E(\overline{F})).$$

For $n \geq 1$, $\deg[n] = n^2$. If $\operatorname{char} F \nmid n$, then $[n]$ is separable and $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$ as abstract groups.

For the model above, $-(x, y) = (x, -y)$. If $P_i = (x_i, y_i)$ and $P_1 + P_2 = (x_3, y_3)$, the addition formulas are

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & x_1 \neq x_2, \\ (3x_1^2 + 2a_2x_1 + a_4)/(2y_1), & P_1 = P_2,\ y_1 \neq 0, \end{cases}$$
$$x_3 = \lambda^2 - a_2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

The remaining cases use $P + (-P) = O$ and $P + O = P$. In odd characteristic, $E[2] = \{O\} \cup \{(r, 0) : f(r) = 0\}$.

Definition 1.1.3. An **isogeny** $\psi : E_1 \to E_2$ is a nonconstant algebraic group homomorphism. **Its degree** is $\deg \psi = [F(E_1) : \psi^* F(E_2)]$; it is **separable** when this extension is separable.

Theorem 1.1.4 (Isogenies and quotients)**.** *Isogenies are finite and surjective, and degrees multiply under composition. An identity-preserving nonconstant morphism between elliptic curves is an isogeny. For a separable isogeny, $\#\ker\psi = \deg\psi$; every characteristic-zero isogeny is separable.*

If $H \subset E(\overline{K})$ is a finite and Galois stable subgroup, a K-isogeny $q_H : E \to E/H$ with kernel H exists. Every K-homomorphism $f : E \to C$ of elliptic curves killing H factors uniquely as $f = \overline{f} \circ q_H$.

For a degree-two K-isogeny, $\ker\psi = \{O, T\}$ and $T \in E_1(K)$: Galois fixes its unique nonzero element. This implies neither rationality of all $E_1[2]$ nor surjectivity of $E_1(K) \to E_2(K)$.

1.2 Local Fields and Unramified Extensions

Definition 1.2.1. The principal unit group $U_1 = 1 + \mathfrak{m}_K$ is distinct from $U \subset S_K$. A chosen uniformizer gives

$$K^\times = \varpi^{\mathbb{Z}} \times \mathcal{O}_K^\times, \qquad \mathcal{O}_K^\times / U_1 \simeq k^\times.$$

For a finite extension L/K, let $e = e(L/K)$ and $f = f(L/K)$ be the **ramification index** and **residue degree**:

$$v_L|_{K^\times} = e\, v_K, \qquad [L:K] = ef.$$

The extension is **unramified** if $e = 1$.

Theorem 1.2.2 (Hensel's lemma)**.** *If $F(X) \in \mathcal{O}_K[X]$ and $a_0 \in \mathcal{O}_K$ satisfy*

$$F(a_0) \equiv 0 \pmod{\mathfrak{m}_K}, \qquad F'(a_0) \not\equiv 0 \pmod{\mathfrak{m}_K},$$

there is a unique $a \equiv a_0 \pmod{\mathfrak{m}_K}$ with $F(a) = 0$.

Since $p \neq 2$, applying this to $X^2 - u$ yields

$$U_1 \xrightarrow[\sim]{z \mapsto z^2} U_1, \qquad u \in K^{\times 2} \iff \overline{u} \in k^{\times 2} \quad (u \in \mathcal{O}_K^\times).$$

Consequently,

$$S_K \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (k^\times / k^{\times 2}), \qquad |S_K| = 4, \qquad |U| = 2.$$

If $\varepsilon \in \mathcal{O}_K^\times$ has nonsquare residue, representatives are

$$S_K = \{1, \varepsilon, \varpi, \varepsilon\varpi\}, \qquad U = \{1, \varepsilon\}.$$

Theorem 1.2.3 (Unramified extensions and inertia)**.** *Inside $\overline{K}$, there is a unique unramified extension of degree r for each $r \geq 1$, with residue field $\mathbb{F}_{q^r}$. If $\overline{\varepsilon}$ is nonsquare, $K(\sqrt{\varepsilon})/K$ is the unramified quadratic extension. There is an exact sequence*

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow G_k \longrightarrow 1, \qquad G_k \simeq \widehat{\mathbb{Z}} = \overline{\langle \mathrm{Frob}_q \rangle}.$$

Arithmetic Frobenius is $a \mapsto a^q$; its inverse is geometric Frobenius. A lift to G_K is determined only modulo I_K.

Theorem 1.2.4 (Norms)**.** *For a finite extension L/K, the norm $N_{L/K} : L^\times \to K^\times$ satisfies*

$$v_K(N_{L/K} a) = f(L/K) v_L(a).$$

If L/K is Galois, $N_{L/K}(a) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(a)$. If it is unramified, then

$$N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times.$$

These are the local-field inputs to the later Hilbert-symbol argument. No orthogonality assertion about U is assumed here.

1.3 Low-Degree Galois Cohomology

Definition 1.3.1 (Continuous cohomology)**.** A discrete G_K-module A **has continuous action** if every element has open stabilizer. Put $C^r = \mathrm{Map}_{\mathrm{cont}}(G_K^r, A)$, with $C^0 = A$, and use the differentials

$$\begin{aligned}(d^0 a)(\sigma) &= \sigma a - a,\\ (d^1 c)(\sigma,\tau) &= \sigma c_\tau - c_{\sigma\tau} + c_\sigma,\\ (d^2 z)(\sigma,\tau,\rho) &= \sigma z(\tau,\rho) - z(\sigma\tau,\rho) + z(\sigma,\tau\rho) - z(\sigma,\tau).\end{aligned}$$

Define $H^0(K,A) = A^{G_K}$ and $H^i(K,A) = \ker d^i / \operatorname{im} d^{i-1}$ for $i = 1, 2$.

A 1-cocycle satisfies $c_{\sigma\tau} = c_\sigma + \sigma c_\tau$; a 1-coboundary is $c_\sigma = \sigma a - a$. For trivial action, $H^1(K,A) = \mathrm{Hom}_{\mathrm{cont}}(G_K, A)$. With multiplicative coefficients, these become $c_{\sigma\tau} = c_\sigma \sigma(c_\tau)$ and $c_\sigma = \sigma(a)/a$. The modules $\overline{K}^\times$ and $E(\overline{K})$ are given the discrete topology in cohomology.

Theorem 1.3.2 (Long exact sequence)**.** *An exact sequence $0 \to A \to B \to C \to 0$ of discrete continuous modules induces*

$$\begin{aligned}0 \to A^{G_K} \to B^{G_K} \to C^{G_K} \xrightarrow{\partial} H^1(K,A) \to H^1(K,B) \to H^1(K,C)\\ \xrightarrow{\partial} H^2(K,A) \to H^2(K,B) \to H^2(K,C) \to \cdots.\end{aligned}$$

For $c \in C^{G_K}$ and a lift $b \in B$, $\partial(c) = [\sigma \mapsto \sigma b - b]$. Changing the lift changes the representative by a coboundary.

Theorem 1.3.3 (Inflation–restriction)**.** *For a closed normal subgroup $I \triangleleft G$ of a profinite group, put $\Gamma = G/I$. Restriction and pullback along $G \to \Gamma$ give*

$$0 \to H^1(\Gamma, A^I) \xrightarrow{\inf} H^1(G,A) \xrightarrow{\mathrm{res}} H^1(I,A)^\Gamma \to H^2(\Gamma, A^I).$$

Definition 1.3.4 (Unramified classes and cup products)**.** The unramified subgroup is

$$H^1_{\mathrm{ur}}(K,A) = \ker\Big(H^1(K,A) \to H^1(I_K,A)\Big) \simeq H^1(G_k, A^{I_K}).$$

For finite A with trivial inertia action, $H^1_{\mathrm{ur}}(K,A) \simeq A/(\mathrm{Frob}_q - 1)A$; for trivial G_K-action, this is $\mathrm{Hom}_{\mathrm{cont}}(G_k, A)$.

A Galois-equivariant bilinear map $b : A_1 \times A_2 \to C$ induces

$$H^1(K,A_1) \times H^1(K,A_2) \xrightarrow{\cup_b} H^2(K,C), \qquad (c \cup_b d)(\sigma,\tau) = b(c_\sigma, \sigma d_\tau).$$

The resulting class is independent of the cocycle representatives.

1.4 Local Class Field Theory and the Hilbert Symbol

Theorem 1.4.1 (Hilbert 90 and the local Brauer invariant)**.** *One has*

$$H^1(K,\overline{K}^\times)=0,\qquad \mathrm{Br}(K)\simeq H^2(K,\overline{K}^\times),\qquad \mathrm{inv}_K:\mathrm{Br}(K)\xrightarrow{\sim}\mathbb{Q}/\mathbb{Z}.$$

The map inv_K *identifies* $\mathrm{Br}(K)[n]=\ker(n:\mathrm{Br}(K)\to\mathrm{Br}(K))$ *with* $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Here $\mathrm{Br}(K)$ is the group of Brauer-equivalence classes of central simple K-algebras, with tensor product as its operation. We use its cohomological description. On $H^2(K,\mu_2)$, the notation inv_K denotes

$$H^2(K,\mu_2)\longrightarrow H^2(K,\overline{K}^\times)\xrightarrow{\mathrm{inv}_K}\mathbb{Q}/\mathbb{Z},$$

induced by $\mu_2\hookrightarrow\overline{K}^\times$; its image lies in D.

Theorem 1.4.2 (Local reciprocity)**.** *There is a continuous homomorphism with dense image*

$$\mathrm{rec}_K:K^\times\longrightarrow G_K^{\mathrm{ab}}=\mathrm{Gal}(K^{\mathrm{ab}}/K),$$

normalized so that a uniformizer maps to arithmetic Frobenius in the unramified quotient. For every finite abelian extension L/K*,*

$$K^\times/N_{L/K}(L^\times)\xrightarrow{\sim}\mathrm{Gal}(L/K).$$

Definition 1.4.3 (Quadratic Hilbert symbol)**.** For $a,b\in K^\times$, set

$$(a,b)_K=\frac{\mathrm{rec}_K(b)(\sqrt{a})}{\sqrt{a}}\in\mu_2,\qquad h_K(a,b)=\begin{cases}0, & (a,b)_K=1,\\ \frac{1}{2}, & (a,b)_K=-1.\end{cases}$$

The action is restricted to $K(\sqrt{a})$. The symbol is independent of the square-root choice and depends only on square classes.

Theorem 1.4.4 (Hilbert-symbol properties)**.** *The pairing* $h_K:S_K\times S_K\to D$ *is bilinear, symmetric, and nondegenerate. In multiplicative notation,*

$$(aa',b)_K=(a,b)_K(a',b)_K,\qquad (a,bb')_K=(a,b)_K(a,b')_K,$$
$$(a,b)_K=(b,a)_K,\qquad (a,b)_K=1\ \forall b\implies a\in K^{\times 2}.$$

The norm criterion is

$$(a,b)_K=1\quad\Longleftrightarrow\quad b\in N_{K(\sqrt{a})/K}\big(K(\sqrt{a})^\times\big).$$

Symmetry need not imply $h_K(a,a)=0$. The identification of the isogeny kernel cup product with h_K, and the calculation of $U^\perp$, are reserved for the main text.

1.5 Good Reduction and Formal Groups

Definition 1.5.1. An integral Weierstrass equation has coefficients in $\mathcal{O}_K$. The curve E/K has **good reduction** if such an equation exists with $\Delta \in \mathcal{O}_K^\times$; its smooth reduction is $\widetilde{E}/k$. Set $E_1(K) = \ker(\mathrm{red} : E(K) \to \widetilde{E}(k))$.

Theorem 1.5.2 (Reduction exact sequence)**.** *For good reduction, reduction is a surjective group homomorphism:*

$$0 \longrightarrow E_1(K) \longrightarrow E(K) \xrightarrow{\mathrm{red}} \widetilde{E}(k) \longrightarrow 0.$$

To reduce any point, scale projective coordinates to be integral with at least one unit. Surjectivity follows from smoothness and Hensel lifting.

Definition 1.5.3 (Formal group and homomorphism)**.** A one-dimensional commutative formal group over $\mathcal{O}_K$ is $F(X,Y) = X + Y +$ terms of degree ≥ 2 satisfying

$$F(X,0) = X, \quad F(0,Y) = Y, \quad F(X,Y) = F(Y,X),$$
$$F(F(X,Y),Z) = F(X,F(Y,Z)).$$

Its inverse series $\iota_F(T) = -T + \cdots$ satisfies $F(T, \iota_F(T)) = 0$. A homomorphism $f : F \to G$ is an element of $T\mathcal{O}_K[[T]]$ with $f(F(X,Y)) = G(f(X), f(Y))$.

Theorem 1.5.4 (Formal group at the identity)**.** *The parameter $t = -x/y$, extended by $t(O) = 0$, identifies*

$$E_1(K) \xrightarrow{\sim} (\mathfrak{m}_K, F_E), \qquad t(P+Q) = F_E(t(P), t(Q)).$$

The series converge on $\mathfrak{m}_K$, and $[n]_F(T) = nT + \cdots$. If $f(T) = a_1 T + \cdots$ has $a_1 \in \mathcal{O}_K^\times$, it has a unique compositional inverse $g(T) \in T\mathcal{O}_K[[T]]$.

Theorem 1.5.5 (Prime-to-p isogenies and unramified models)**.** *If E, E' have good reduction and $p \nmid \deg \psi$, a K-isogeny $\psi : E \to E'$ extends uniquely to a finite étale isogeny of their smooth proper group models. Its reduction $\widetilde{\psi}$ is separable and $\deg \widetilde{\psi} = \deg \psi$. Finite étale $\mathcal{O}_K$-algebras are precisely finite products of integer rings of finite unramified extensions of K.*

Definition 1.5.6 (Frobenius endomorphism)**.** For $\widetilde{E}/\mathbb{F}_q$, let $\pi_{\widetilde{E}}$ raise coordinates to their qth powers. It is purely inseparable of degree q, with zero differential, and

$$\widetilde{E}(k) = \ker(\pi_{\widetilde{E}} - 1)(\overline{k}), \qquad \pi_{\widetilde{E}'} \widetilde{\psi} = \widetilde{\psi} \pi_{\widetilde{E}}$$

for every k-isogeny $\widetilde{\psi}$.

1.6 Finite Pairings and Torsors

Definition 1.6.1 (Perfect pairing and orthogonal complement)**.** Let V, W be finite groups killed by two and $B : V \times W \to D$ be bilinear. It is perfect if the induced maps

$$V \longrightarrow \mathrm{Hom}(W, D), \quad v \longmapsto B(v, -), \qquad W \longrightarrow \mathrm{Hom}(V, D), \quad w \longmapsto B(-, w)$$

are isomorphisms; equivalently, both maps are injective. For $L \subset V$,

$$L^{\perp} = \{w \in W : B(\ell, w) = 0 \text{ for all } \ell \in L\}.$$

The orthogonal complement belongs to the opposite side of the pairing.

Definition 1.6.2 (Torsor)**.** An E-torsor over K is a nonempty K-variety X with a K-defined action $E \times X \to X$ that becomes equivariantly isomorphic over $\overline{K}$ to $E_{\overline{K}}$ acting on itself by translations. Thus any $x, y \in X(\overline{K})$ have a unique difference $P \in E(\overline{K})$ with $y = x + P$. It is trivial if the equivariant isomorphism exists over K.

Theorem 1.6.3 (Torsors and first cohomology)**.** *One has*

$$X \text{ trivial} \iff X(K) \neq \varnothing, \qquad \{E\text{-torsors over } K\}/\simeq \xrightarrow{\sim} H^1(K, E(\overline{K})).$$

The trivial torsor corresponds to zero. For $x_0 \in X(\overline{K})$, its class is represented by the cocycle determined by

$$\sigma x_0 = x_0 + c_\sigma, \qquad c_{\sigma\tau} = c_\sigma + \sigma c_\tau.$$

Replacing x_0 by $x_0 + P$ changes c_σ to $c_\sigma + \sigma P - P$, hence leaves the class unchanged.

Definition 1.6.4 (Weil–Châtelet group and isogeny kernels)**.** Write $H^1(K, E) = H^1(K, E(\overline{K}))$ for the Weil–Châtelet group. A K-isogeny $\psi : E_1 \to E_2$ induces

$$\psi_*[c_\sigma] = [\psi(c_\sigma)], \qquad H^1(K, E_1)[\psi] = \ker\Big(H^1(K, E_1) \xrightarrow{\psi_*} H^1(K, E_2)\Big).$$

In particular, $H^1(K, E)[\varphi]$ and $H^1(K, E')[\widehat{\varphi}]$ refer to the two different isogeny-induced maps.

2 Divisor Classes and Dual Isogenies

The central question in this section is: given a degree-two isogeny

$$\varphi : E \longrightarrow E',$$

how can one construct the dual isogeny $\widehat{\varphi} : E' \to E$ in the opposite direction, and why does it correspond to pullback on divisor classes of degree zero?

We retain the standing assumptions: $K/\mathbb{Q}_p$ is a finite extension with $p \neq 2$, and $\varphi : E \to E'$ is a K-isogeny of degree two.

All divisors below are considered over $\overline{K}$. We write (P) for the point divisor associated with P and $[\mathcal{D}]$ for the linear equivalence class of a divisor $\mathcal{D}$. Put

$$\mathrm{Pic}^0(E_{\overline{K}}) = \mathrm{Div}^0(E_{\overline{K}})/\,\mathrm{Prin}(E_{\overline{K}}),$$

the group of divisors of degree zero modulo principal divisors.

2.1 Points and Divisor Classes of Degree Zero

The identity O gives a natural map

$$\alpha_E : E(\overline{K}) \longrightarrow \mathrm{Pic}^0(E_{\overline{K}}), \qquad P \longmapsto [(P) - (O)].$$

This map allows calculations with divisor classes to be translated into calculations in the elliptic-curve group.

Proposition 2.1.1 (The Abel–Jacobi isomorphism)**.** The map α_E is a G_K-equivariant group isomorphism. For a divisor of degree zero $\mathcal{D} = \sum_P n_P(P)$, its inverse is given by

$$\alpha_E^{-1}([\mathcal{D}]) = \sum_P n_P P, \tag{2.1}$$

where the sum on the right is taken in the elliptic-curve group.

In particular, a divisor $\mathcal{D} = \sum_P n_P(P)$ of degree zero satisfies the principal-divisor criterion

$$\mathcal{D} \text{ is principal} \quad \Longleftrightarrow \quad \sum_P n_P P = O. \tag{2.2}$$

The pullback calculation below will use this criterion directly.

2.2 Constructing the Dual Isogeny

Since φ is a degree-two isogeny in characteristic zero, it is separable and

$$M = \ker \varphi = \{O, T\}, \qquad 2T = O.$$

By the preliminaries, the unique nonzero kernel point T belongs to $E(K)$.

The key observation is that multiplication by two vanishes on M, and hence factors through the quotient curve E/M.

Theorem 2.2.1 (Existence and uniqueness of the dual isogeny)**.** *There is a unique K-isogeny*

$$\widehat{\varphi} : E' \longrightarrow E$$

satisfying

$$\widehat{\varphi} \circ \varphi = [2]_E. \tag{2.3}$$

It has degree two and satisfies

$$\varphi \circ \widehat{\varphi} = [2]_{E'}. \tag{2.4}$$

The isogeny $\widehat{\varphi}$ is called the dual isogeny *of φ.*

Proof. By the existence theorem for quotient curves, there is a quotient isogeny over K,

$$q : E \longrightarrow E/M.$$

Since φ vanishes on M, the universal property of the quotient gives a K-homomorphism

$$\iota : E/M \longrightarrow E', \qquad \varphi = \iota \circ q.$$

Both φ and q have degree two, so multiplicativity of degrees gives $\deg \iota = 1$. A finite morphism of degree one between smooth projective curves is an isomorphism. Thus

$$\iota : E/M \xrightarrow{\sim} E'$$

is a K-isomorphism.

The map $[2]_E$ also vanishes on M. Applying the universal property again gives a unique K-homomorphism

$$h : E/M \longrightarrow E, \qquad h \circ q = [2]_E.$$

Define

$$\widehat{\varphi} = h \circ \iota^{-1}.$$

Then

$$\widehat{\varphi} \circ \varphi = h \circ \iota^{-1} \circ \iota \circ q = [2]_E.$$

Since $[2]_E$ is nonconstant, $\widehat{\varphi}$ is nonconstant and hence is an isogeny. Every map in the construction is defined over K, so $\widehat{\varphi}$ is a K-isogeny.

If another isogeny $\psi : E' \to E$ satisfies $\psi \circ \varphi = [2]_E$, then

$$\psi \circ \varphi = \widehat{\varphi} \circ \varphi.$$

Surjectivity of φ on geometric points gives $\psi = \widehat{\varphi}$, proving uniqueness.

Multiplicativity of degrees gives

$$4 = \deg[2]_E = \deg \widehat{\varphi} \cdot \deg \varphi = 2 \deg \widehat{\varphi},$$

so $\deg \widehat{\varphi} = 2$. Finally, since φ respects the group law,

$$\begin{aligned}(\varphi \circ \widehat{\varphi}) \circ \varphi &= \varphi \circ [2]_E \\ &= [2]_{E'} \circ \varphi.\end{aligned}$$

Surjectivity of φ again gives (2.4). Here we use surjectivity of $E(\overline{K}) \to E'(\overline{K})$, not surjectivity on K-rational points. □

The construction gives a direct description on points. For any $P' \in E'(\overline{K})$, choose a preimage P. Then

$$\widehat{\varphi}(P') = 2P. \tag{2.5}$$

The other preimage is $P + T$, and $2(P + T) = 2P$, so this expression is independent of the chosen preimage. The quotient-curve construction ensures that it comes from an algebraic morphism.

2.3 Interpreting the Dual Isogeny as Pullback

The isogeny φ also induces pullback in the opposite direction,

$$\varphi^* : \mathrm{Div}(E'_{\overline{K}}) \longrightarrow \mathrm{Div}(E_{\overline{K}}).$$

If $P' \in E'(\overline{K})$ and $\varphi(P) = P'$, then

$$\varphi^{-1}(P') = \{P, P+T\}.$$

These points are distinct, and the total multiplicity of the fiber is two, so each has multiplicity one. Thus

$$\varphi^*((P')) = (P) + (P+T), \qquad \varphi^*((O')) = (O) + (T). \tag{2.6}$$

Pullback satisfies

$$\deg(\varphi^*\mathcal{D}') = 2\deg \mathcal{D}', \qquad \mathrm{div}(f \circ \varphi) = \varphi^*(\mathrm{div}(f)).$$

It therefore preserves divisors of degree zero and takes principal divisors to principal divisors, inducing

$$\varphi^* : \mathrm{Pic}^0(E'_{\overline{K}}) \longrightarrow \mathrm{Pic}^0(E_{\overline{K}}).$$

Theorem 2.3.1. *Under the Abel–Jacobi isomorphisms,*

$$\widehat{\varphi} = \alpha_E^{-1} \circ \varphi^* \circ \alpha_{E'}. \tag{2.7}$$

Proof. Let $P' \in E'(\overline{K})$ and choose $P \in E(\overline{K})$ with $\varphi(P) = P'$. By (2.6),

$$\varphi^*\Big((P') - (O')\Big) = (P) + (P+T) - (O) - (T).$$

By Proposition 2.1.1, the point corresponding to the divisor class on the right is

$$P + (P+T) - O - T = 2P.$$

Therefore

$$\alpha_E^{-1}\Big(\varphi^*\Big(\alpha_{E'}(P')\Big)\Big) = 2P.$$

On the other hand, the defining identity for the dual isogeny gives

$$\widehat{\varphi}(P') = \widehat{\varphi}(\varphi(P)) = 2P.$$

These equalities hold for every P', proving (2.7). □

This identity explains the reversal of direction: φ sends points of E to points of E', whereas pullback sends divisor classes on E' to divisor classes on E. After identifying each curve with its group of divisor classes of degree zero, this reverse map is precisely the dual isogeny.

The decisive calculation is

$$(P) + (P+T) - (O) - (T) \quad \longmapsto \quad P + (P+T) - O - T = 2P.$$

In the difference of the two fibers, the contributions of the kernel point T cancel. The remaining double agrees with the identity $\widehat{\varphi} \circ \varphi = [2]_E$.

2.4 The Dual Kernel and Functions for the Pairing

Put

$$M = E[\varphi], \qquad N = E'[\widehat{\varphi}].$$

We record two consequences that will be used directly in the subsequent sections.

Corollary 2.4.1. There is a short exact sequence of G_K-modules

$$0 \longrightarrow M \longrightarrow E[2] \xrightarrow{\varphi} N \longrightarrow 0. \tag{2.8}$$

Both M and N are groups of order two with trivial Galois action.

Proof sketch. The identity $\widehat{\varphi} \circ \varphi = [2]_E$ gives $\varphi(E[2]) \subseteq N$. Conversely, if $S' \in N$, choose a preimage P. Then $2P = \widehat{\varphi}(S') = O$, so $P \in E[2]$ and $N = \varphi(E[2])$. The kernel of the restricted map is M, proving exactness. The maps are defined over K and hence are Galois-equivariant.

Since $|E[2]| = 4$ and $|M| = 2$, we have $|N| = 2$. The Galois action must fix the unique nonzero point of each kernel, so both actions are trivial. □

Corollary 2.4.2. For every $S' \in E'(\overline{K})$,

$$S' \in N \quad \Longleftrightarrow \quad \varphi^*\Big((S') - (O')\Big) \text{ is principal.} \tag{2.9}$$

Proof sketch. Theorem 2.3.1 gives

$$\Big[\varphi^*\Big((S') - (O')\Big)\Big] = \alpha_E(\widehat{\varphi}(S')).$$

Since α_E is a group isomorphism, the left-hand side is zero if and only if $\widehat{\varphi}(S') = O$, or equivalently $S' \in N$. □

Thus, for every $S' \in N$, one can choose $g_{S'} \in \overline{K}(E)^\times$ such that

$$\operatorname{div}(g_{S'}) = \varphi^*\Big((S') - (O')\Big). \tag{2.10}$$

The function is unique up to multiplication by a nonzero constant: the quotient of two functions with the same divisor has no poles and is therefore constant on the smooth projective curve.

Equation (2.10) is the starting point for the kernel pairing. We will compute $g_{S'}$ for an explicit degree-two isogeny and then study how translation by a kernel point acts on it, obtaining

$$e_\varphi : M \times N \longrightarrow \mu_2.$$

In this way, the geometric duality described by divisor pullback enters Galois cohomology and can be connected with the Hilbert symbol.

3 Degree-Two Isogenies and the Kernel Pairing

In the preceding section, we interpreted the dual isogeny in terms of pullback on divisor classes and proved that, for every

$$S' \in N = E'[\widehat{\varphi}],$$

the divisor

$$\varphi^*\Big((S') - (O')\Big)$$

is principal.

Starting from this observation, we construct a Galois-equivariant perfect pairing

$$e_\varphi : M \times N \longrightarrow \mu_2, \qquad M = E[\varphi], \quad N = E'[\widehat{\varphi}].$$

We first give an explicit pair of degree-two isogenies, then establish the properties of the kernel pairing in general, and finally return to the example for an explicit computation. No good reduction assumption is needed in this section.

3.1 An Explicit Pair of Degree-Two Isogenies

Consider the elliptic curves

$$E : y^2 = x^3 - x, \qquad E' : v^2 = u^3 + 4u,$$

and write

$$T = (0,0) \in E(K), \qquad T' = (0,0) \in E'(K).$$

Their discriminants are

$$\Delta_E = 64, \qquad \Delta_{E'} = -4096,$$

so both curves are nonsingular over a field of characteristic zero.

Proposition 3.1.1. The rational formulas

$$\varphi(x,y) = \left(x - \frac{1}{x},\ y\left(1 + \frac{1}{x^2}\right)\right)$$

and

$$\widehat{\varphi}(u,v) = \left(\frac{u^2+4}{4u},\ \frac{v(u^2-4)}{8u^2}\right)$$

extend to degree-two isogenies defined over K,

$$\varphi : E \longrightarrow E', \qquad \widehat{\varphi} : E' \longrightarrow E.$$

Their kernels are

$$\ker\varphi = \{O, T\}, \qquad \ker\widehat{\varphi} = \{O', T'\},$$

and they are dual to each other.

Proof. We first verify that the first formula takes values on E'. Put

$$u = \frac{x^2-1}{x}, \qquad v = \frac{y(x^2+1)}{x^2}.$$

Using $y^2 = x(x^2-1)$, we obtain

$$v^2 = \frac{(x^2-1)(x^2+1)^2}{x^3}.$$

On the other hand,

$$u^3 + 4u = \frac{(x^2-1)^3 + 4x^2(x^2-1)}{x^3} = \frac{(x^2-1)(x^2+1)^2}{x^3}.$$

Thus the first formula defines a nonconstant rational map from E to E'.

For the second formula, put

$$X = \frac{u^2+4}{4u}, \qquad Y = \frac{v(u^2-4)}{8u^2}.$$

Since $v^2 = u(u^2+4)$, we have

$$Y^2 = \frac{(u^2+4)(u^2-4)^2}{64u^3}.$$

Moreover,

$$X^3 - X = \frac{(u^2+4)\Big((u^2+4)^2 - 16u^2\Big)}{64u^3} = \frac{(u^2+4)(u^2-4)^2}{64u^3}.$$

Hence the second formula also defines a nonconstant rational map, this time from E' to E.

Because the source curves are smooth and the target curves are projective, both rational maps extend uniquely to morphisms on the entire curves. We now determine their values at the identities and at the points where the displayed denominators vanish.

On E, the function x has a pole of order two at O and a zero of order two at T. Consequently,

$$u \circ \varphi = x - \frac{1}{x}$$

has poles precisely at O and T. Since the only pole of u on E' is O', we obtain

$$\varphi(O) = \varphi(T) = O'.$$

Every other affine point has an image with finite coordinates, so

$$\varphi^{-1}(O') = \{O, T\}.$$

In particular, φ preserves the identity and is therefore an isogeny. In characteristic zero, an isogeny is separable and its degree equals the order of its geometric kernel. Thus

$$\deg \varphi = 2.$$

For $\widehat{\varphi}$, the function

$$x \circ \widehat{\varphi} = \frac{1}{4}\left(u + \frac{4}{u}\right)$$

has poles precisely at O' and T'. The same argument gives

$$\widehat{\varphi}(O') = \widehat{\varphi}(T') = O,$$

and

$$\ker \widehat{\varphi} = \{O', T'\}, \qquad \deg \widehat{\varphi} = 2.$$

It remains to verify the duality relation. On E, the slope in the duplication formula is

$$\lambda = \frac{3x^2 - 1}{2y}.$$

Substituting this into the group-law formulas and simplifying yields

$$[2]_E(x,y) = \left(\frac{(x^2+1)^2}{4y^2},\ \frac{(x^2+1)(x^4-6x^2+1)}{8y^3} \right).$$

Substituting the coordinates of φ into $\widehat{\varphi}$ gives the same expression. Therefore

$$\widehat{\varphi} \circ \varphi = [2]_E$$

on a dense open subset, and hence as morphisms on the entire curve.

By the uniqueness of the dual isogeny established in the preceding section, this $\widehat{\varphi}$ is the dual of φ, and

$$\varphi \circ \widehat{\varphi} = [2]_{E'}.$$

□

3.2 Constructing the Kernel Pairing by Divisor Pullback

We now return to a general degree-two isogeny

$$\varphi : E \longrightarrow E'.$$

Write

$$M = \{O, T\}, \qquad N = \{O', T'\}.$$

Each kernel has a unique nonzero point and is stable under the Galois action. Consequently,

$$T \in E(K), \qquad T' \in E'(K).$$

For $S' \in N$, put

$$D_{S'} = (S') - (O').$$

By the result of the preceding section, we may choose

$$g_{S'} \in \overline{K}(E)^\times$$

such that

$$\mathrm{Div}(g_{S'}) = \varphi^* D_{S'}.$$

For $S' = O'$, take $g_{O'} = 1$.

Let $S \in M$. Since $\varphi(S) = O'$, translation by S satisfies

$$\varphi \circ \tau_S = \varphi, \qquad \tau_S(P) = P + S.$$

It follows that

$$\begin{aligned} \mathrm{Div}(g_{S'} \circ \tau_S) &= \tau_S^* \,\mathrm{Div}(g_{S'}) \\ &= \tau_S^* \varphi^* D_{S'} \\ &= \varphi^* D_{S'}. \end{aligned}$$

Thus $g_{S'} \circ \tau_S$ and $g_{S'}$ have the same divisor, so their quotient is a nonzero constant.

We therefore define

$$e_\varphi(S, S') = \frac{g_{S'} \circ \tau_S}{g_{S'}}.$$

The right-hand side denotes the constant determined by this quotient of rational functions. At any point P avoiding the relevant zeros and poles, it may be evaluated as

$$e_\varphi(S, S') = \frac{g_{S'}(P+S)}{g_{S'}(P)}.$$

Proposition 3.2.1. This construction gives a Galois-equivariant bilinear pairing

$$e_\varphi : M \times N \longrightarrow \mu_2$$

that is independent of the choice of the auxiliary functions.

Proof. We first prove independence of the auxiliary function. If $\widetilde{g}_{S'}$ has the same divisor as $g_{S'}$, then

$$\widetilde{g}_{S'} = c\, g_{S'} \qquad (c \in \overline{K}^\times).$$

Hence

$$\frac{\widetilde{g}_{S'} \circ \tau_S}{\widetilde{g}_{S'}} = \frac{g_{S'} \circ \tau_S}{g_{S'}}.$$

Next, write $e_\varphi(S, S') = c$. By definition,

$$g_{S'} \circ \tau_S = c\, g_{S'}.$$

Since $2S = O$, translating once more gives

$$g_{S'} = c^2 g_{S'}.$$

Therefore $c^2 = 1$, so the pairing takes values in μ_2.

For the first variable, evaluation at a general point P gives

$$\begin{aligned} e_\varphi(S_1 + S_2, S') &= \frac{g_{S'}(P + S_1 + S_2)}{g_{S'}(P)} \\ &= \frac{g_{S'}(P + S_1 + S_2)}{g_{S'}(P + S_2)} \frac{g_{S'}(P + S_2)}{g_{S'}(P)} \\ &= e_\varphi(S_1, S') e_\varphi(S_2, S'). \end{aligned}$$

For the second variable, let $A', B' \in N$. Since the Abel–Jacobi map is a group homomorphism, the divisor

$$D_{A'} + D_{B'} - D_{A'+B'}$$

is principal. Choose $f \in \overline{K}(E')^\times$ such that

$$\mathrm{Div}(f) = D_{A'} + D_{B'} - D_{A'+B'}.$$

Comparing divisors shows that, for some nonzero constant c,

$$g_{A'} g_{B'} = c\, g_{A'+B'}(f \circ \varphi).$$

Compose both sides with τ_S and divide by the original identity. Since

$$f \circ \varphi \circ \tau_S = f \circ \varphi,$$

we obtain

$$e_\varphi(S, A') e_\varphi(S, B') = e_\varphi(S, A' + B').$$

This proves linearity in the second variable.

Finally, let $\sigma \in G_K$. Because φ is defined over K,

$$\mathrm{Div}(\sigma g_{S'}) = \varphi^* D_{\sigma S'}.$$

Thus $\sigma g_{S'}$ is a valid auxiliary function for the second argument $\sigma S'$. Independence of the choice of auxiliary function now gives

$$e_\varphi(\sigma S, \sigma S') = \sigma\Big(e_\varphi(S, S')\Big),$$

which is the required Galois equivariance. □

3.3 Nondegeneracy of the Kernel Pairing

Theorem 3.3.1. *The pairing*

$$e_\varphi : M \times N \longrightarrow \mu_2$$

is perfect, and

$$e_\varphi(T, T') = -1.$$

Proof. Both groups have order two, so it is enough to prove that

$$e_\varphi(T, T') \neq 1.$$

Suppose instead that $e_\varphi(T, T') = 1$. Then

$$g_{T'} \circ \tau_T = g_{T'},$$

so $g_{T'}$ is invariant under translation by the kernel.

Put

$$F = \overline{K}(E), \qquad F_0 = \varphi^* \overline{K}(E').$$

Since $\deg \varphi = 2$, we have $[F : F_0] = 2$. Translation by T induces a nontrivial F_0-automorphism of F, and therefore

$$F^{\langle \tau_T^* \rangle} = F_0.$$

Consequently, there exists $f \in \overline{K}(E')^\times$ such that

$$g_{T'} = f \circ \varphi.$$

Taking divisors yields

$$\varphi^*(\operatorname{Div} f) = \operatorname{Div}(g_{T'}) = \varphi^*\Big((T') - (O')\Big).$$

Pullback by a finite surjective morphism is injective on divisor groups. Indeed, the coefficient of a point is multiplied by a positive ramification index at each point above it, so a nonzero coefficient cannot disappear under pullback. Thus

$$\operatorname{Div} f = (T') - (O').$$

By the principal-divisor criterion from the preceding section, this would imply $T' = O'$, contrary to the choice of T' as the nonzero kernel point.

Hence

$$e_\varphi(T, T') = -1.$$

Together with bilinearity, this determines the entire pairing:

$$e_\varphi(iT, jT') = (-1)^{ij}, \qquad i, j \in \{0, 1\}.$$

The nonzero element on either side pairs to -1 with the nonzero element on the other side. The pairing is therefore nondegenerate on both sides, and it is perfect because both groups are finite. □

We obtain Galois-equivariant isomorphisms

$$N \xrightarrow{\sim} \operatorname{Hom}(M, \mu_2), \qquad S' \longmapsto \Big(S \mapsto e_\varphi(S, S')\Big),$$

and

$$M \xrightarrow{\sim} \operatorname{Hom}(N, \mu_2).$$

Thus the kernels of an isogeny and its dual are naturally dual through this pairing.

3.4 An Explicit Computation in the Running Example

Return to

$$E : y^2 = x^3 - x, \qquad E' : v^2 = u^3 + 4u.$$

Put

$$P_+ = (1, 0), \qquad P_- = (-1, 0).$$

The isogeny formulas give

$$\varphi^{-1}(T') = \{P_+, P_-\}, \qquad \varphi^{-1}(O') = \{O, T\}.$$

Each point in these fibers occurs with multiplicity one. Hence

$$\varphi^*\Big((T') - (O')\Big) = (P_+) + (P_-) - (O) - (T).$$

On the other hand,

$$\mathrm{Div}(x) = 2(T) - 2(O),$$

and

$$\mathrm{Div}(y) = (T) + (P_+) + (P_-) - 3(O).$$

Therefore

$$\mathrm{Div}\left(\frac{y}{x}\right) = (P_+) + (P_-) - (T) - (O).$$

We may consequently take

$$g_{T'} = \frac{y}{x}$$

in the construction of the kernel pairing.

We next compute τ_T. The line through (x, y) and $T = (0, 0)$ has slope y/x, so the addition formulas give

$$x(P + T) = \frac{y^2}{x^2} - x = -\frac{1}{x}$$

and

$$y(P + T) = \frac{y}{x}\left(x + \frac{1}{x}\right) - y = \frac{y}{x^2}.$$

Thus

$$\tau_T(x, y) = \left(-\frac{1}{x}, \frac{y}{x^2}\right).$$

It follows that

$$g_{T'} \circ \tau_T = \frac{y/x^2}{-1/x} = -\frac{y}{x},$$

and hence

$$e_\varphi(T, T') = \frac{g_{T'} \circ \tau_T}{g_{T'}} = -1.$$

This calculation shows that the nontrivial kernel translation preserves the divisor of the function while multiplying the function itself by -1. The kernel pairing records precisely this change.

Finally, we record two identities for later use:

$$\left(\frac{y}{x}\right)^2 = \frac{x^3 - x}{x^2} = x - \frac{1}{x} = u \circ \varphi,$$

and

$$\left(\frac{v}{2u}\right)^2 = \frac{u^3 + 4u}{4u^2} = \frac{u^2 + 4}{4u} = x \circ \widehat{\varphi}.$$

The function y/x used to construct the kernel pairing is also a square root of the pullback of the coordinate function u. In the later derivation of the Kummer maps, this relation will translate the Galois action on division points into sign changes of square roots.

4 Hilbert Symbols and the Cohomological Pairing on the Kernels

The preceding section constructed a Galois-equivariant perfect pairing

$$e_\varphi : M \times N \longrightarrow \mu_2.$$

By the cup product, it induces a pairing

$$H^1(K, M) \times H^1(K, N) \longrightarrow H^2(K, \mu_2).$$

Composing with the local invariant map gives a pairing with values in

$$D = \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

We will show that, in square-class coordinates, this pairing is the quadratic Hilbert symbol defined in the preliminaries using local reciprocity. We will then prove

$$U^\perp = U.$$

4.1 Kummer Theory for the Multiplicative Group and Square-Class Coordinates

Consider the short exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow \overline{K}^\times \xrightarrow{z \mapsto z^2} \overline{K}^\times \longrightarrow 1.$$

Hilbert's Theorem 90 gives

$$H^1(K, \overline{K}^\times) = 0.$$

The associated long exact sequence in cohomology therefore yields an isomorphism

$$\kappa : S_K = K^\times / K^{\times 2} \xrightarrow{\sim} H^1(K, \mu_2).$$

Explicitly, for $a \in K^\times$, choose $\alpha \in \overline{K}$ with $\alpha^2 = a$. Then

$$\kappa([a]) = \left[\sigma \longmapsto \frac{\sigma\alpha}{\alpha}\right].$$

Changing the choice of square root does not change this cocycle. Multiplying a by a square in K likewise leaves its cohomology class unchanged.

The same long exact sequence gives

$$H^2(K, \mu_2) \xrightarrow{\sim} \mathrm{Br}(K)[2].$$

Together with the local invariant map, this yields

$$H^2(K, \mu_2) \xrightarrow{\sim} D.$$

Since M and N are groups of order two with trivial Galois action, we have isomorphisms

$$\iota_M : M \xrightarrow{\sim} \mu_2, \qquad O \mapsto 1, \quad T \mapsto -1,$$

and

$$\iota_N : N \xrightarrow{\sim} \mu_2, \qquad O' \mapsto 1, \quad T' \mapsto -1.$$

We thus obtain isomorphisms

$$\kappa_M : S_K \xrightarrow{\sim} H^1(K, M), \qquad \kappa_N : S_K \xrightarrow{\sim} H^1(K, N).$$

For $a \in K^\times$, define the quadratic character

$$\chi_a : G_K \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

by

$$\frac{\sigma(\sqrt{a})}{\sqrt{a}} = (-1)^{\chi_a(\sigma)}.$$

The two isomorphisms above can then be written as

$$\kappa_M([a]) = \Big[\sigma \mapsto \chi_a(\sigma)T\Big]$$

and

$$\kappa_N([a]) = \Big[\sigma \mapsto \chi_a(\sigma)T'\Big].$$

Since

$$e_\varphi(iT, jT') = (-1)^{ij},$$

these identifications carry the kernel pairing to the bilinear map

$$\mu_2 \times \mu_2 \longrightarrow \mu_2, \qquad \Big((-1)^i, (-1)^j\Big) \longmapsto (-1)^{ij}.$$

4.2 Constructing the Cohomological Pairing

Define

$$B_\varphi : H^1(K, M) \times H^1(K, N) \longrightarrow D, \qquad B_\varphi(\xi, \eta) = \mathrm{inv}_K(\xi \cup_{e_\varphi} \eta).$$

The cup product is well-defined on cohomology classes, and the kernel pairing is bilinear. Thus B_φ is also bilinear.

If c and d represent ξ and η, respectively, their cup product is represented by the 2-cocycle

$$(c \cup_{e_\varphi} d)(\sigma, \tau) = e_\varphi(c_\sigma, \sigma d_\tau).$$

In particular, take

$$\xi = \kappa_M([a]), \qquad \eta = \kappa_N([b]).$$

The Galois action on N is trivial, so

$$(c \cup_{e_\varphi} d)(\sigma, \tau) = (-1)^{\chi_a(\sigma)\chi_b(\tau)}.$$

Writing

$$z_{a,b}(\sigma, \tau) = (-1)^{\chi_a(\sigma)\chi_b(\tau)},$$

we therefore have

$$B_\varphi\Big(\kappa_M([a]), \kappa_N([b])\Big) = \mathrm{inv}_K([z_{a,b}]).$$

We now show that this invariant is precisely $h_K(a, b)$.

Theorem 4.2.1. *For all $a, b \in K^\times$,*

$$B_\varphi\Big(\kappa_M([a]), \kappa_N([b])\Big) = h_K(a, b).$$

Proof. We use the compatibility between local reciprocity and cup products. Let

$$\psi : G_K \longrightarrow \mathbb{Q}/\mathbb{Z}$$

be a continuous character of finite order, and let

$$\partial\psi \in H^2(K, \mathbb{Z})$$

be its image under the connecting homomorphism associated with

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Then

$$\mathrm{inv}_K(b \cup \partial\psi) = \psi(\mathrm{rec}_K(b)), \qquad b \in K^\times.$$

Here the coefficient pairing is $(b, m) \mapsto b^m$.

We relate $z_{a,b}$ to this formula by an explicit cochain calculation.

Choose the integer representatives

$$A_\sigma, B_\sigma \in \{0, 1\}$$

of $\chi_a(\sigma)$ and $\chi_b(\sigma)$, respectively, and define

$$\psi_a(\sigma) = \frac{A_\sigma}{2} \pmod{\mathbb{Z}}.$$

Since

$$A_{\sigma\tau} = A_\sigma + A_\tau - 2A_\sigma A_\tau,$$

the rational lift $A_\sigma/2$ shows that $\partial\psi_a$ is represented by the integer-valued 2-cocycle

$$\frac{A_\sigma + A_\tau - A_{\sigma\tau}}{2} = A_\sigma A_\tau.$$

Hence $b \cup \partial\psi_a$ is represented by

$$f_{a,b}(\sigma, \tau) = b^{A_\sigma A_\tau}.$$

Choose $\beta \in \overline{K}^\times$ with $\beta^2 = b$, and define a 1-cochain

$$r_\sigma = (\sigma\beta)^{-A_\sigma}.$$

Using

$$\frac{\sigma\tau\beta}{\sigma\beta} = (-1)^{B_\tau},$$

we compute

$$\begin{aligned}
(dr)(\sigma, \tau) &= \frac{r_\sigma \, \sigma(r_\tau)}{r_{\sigma\tau}} \\
&= \left(\frac{\sigma\tau\beta}{\sigma\beta}\right)^{A_\sigma} (\sigma\tau\beta)^{-2A_\sigma A_\tau} \\
&= (-1)^{A_\sigma B_\tau} b^{-A_\sigma A_\tau} \\
&= z_{a,b}(\sigma, \tau) f_{a,b}(\sigma, \tau)^{-1}.
\end{aligned}$$

Thus $z_{a,b}$ and $f_{a,b}$ represent the same class in

$$H^2(K, \overline{K}^\times).$$

Applying the compatibility formula from local class field theory gives

$$\begin{aligned}
B_\varphi\Big(\kappa_M([a]), \kappa_N([b])\Big) &= \mathrm{inv}_K([z_{a,b}]) \\
&= \mathrm{inv}_K([f_{a,b}]) \\
&= \psi_a(\mathrm{rec}_K(b)).
\end{aligned}$$

By the definition of ψ_a, the last expression is

$$\begin{cases} 0, & \mathrm{rec}_K(b)(\sqrt{a}) = \sqrt{a}, \\ \dfrac{1}{2}, & \mathrm{rec}_K(b)(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

The definition in the preliminaries is

$$(a,b)_K = \frac{\mathrm{rec}_K(b)(\sqrt{a})}{\sqrt{a}}.$$

It follows that

$$\psi_a(\mathrm{rec}_K(b)) = h_K(a,b),$$

as required. □

This theorem makes the connection between the kernel pairing and the Hilbert symbol visible at the cocycle level. The value

$$e_\varphi(T,T') = -1$$

produces the 2-cocycle

$$(-1)^{\chi_a(\sigma)\chi_b(\tau)},$$

and the local invariant converts its cohomology class into the sign with which the reciprocity map acts on a square root.

Corollary 4.2.2. The pairing

$$B_\varphi : H^1(K,M) \times H^1(K,N) \longrightarrow D$$

is perfect.

Proof. Kummer theory identifies both sides with S_K. Suppose

$$\xi = \kappa_M([a])$$

pairs trivially with every element on the right. The preceding theorem implies

$$h_K(a,b) = 0 \qquad \text{for every } b \in K^\times.$$

Nondegeneracy of the Hilbert symbol gives $a \in K^{\times 2}$, hence $\xi = 0$. The same argument on the other side shows that the right kernel is also zero.

Thus B_φ is nondegenerate on both sides. Since

$$|H^1(K,M)| = |H^1(K,N)| = |S_K| = 4,$$

it is a perfect pairing of finite groups. □

4.3 The Orthogonal Complement of the Unit Square Classes

Recall that

$$U = \mathrm{im}\Big(\mathcal{O}_K^\times \longrightarrow S_K\Big).$$

Because the residue characteristic is not two, the preliminaries give

$$|S_K| = 4, \qquad |U| = 2.$$

Lemma 4.3.1. For all $u, v \in \mathcal{O}_K^\times$,

$$h_K(u,v) = 0.$$

Proof. If $u \in K^{\times 2}$, the assertion is immediate.

Suppose $u \notin K^{\times 2}$. By Hensel's lemma, its residue class is also a nonsquare. Consequently,

$$L = K(\sqrt{u})$$

is the unramified quadratic extension of K.

The norm map on units of an unramified extension is surjective, so

$$v \in N_{L/K}(\mathcal{O}_L^\times) \subseteq N_{L/K}(L^\times).$$

The norm criterion for the Hilbert symbol gives

$$(u, v)_K = 1,$$

or equivalently $h_K(u, v) = 0$. □

Theorem 4.3.2. *With respect to the Hilbert-symbol pairing, the unit square-class subgroup satisfies*

$$U^\perp = U.$$

Proof. The preceding lemma shows that the pairing vanishes on every pair of unit square classes. Therefore

$$U \subseteq U^\perp.$$

Choose a unit $\varepsilon \in \mathcal{O}_K^\times$ whose residue class is a nonsquare. Then

$$U = \{1, [\varepsilon]\}.$$

Consider the homomorphism

$$S_K \longrightarrow D, \qquad [b] \longmapsto h_K(\varepsilon, b).$$

Since $[\varepsilon] \neq 1$, nondegeneracy of the Hilbert symbol shows that this homomorphism is nonzero. As $|S_K| = 4$ and $|D| = 2$, its kernel has exactly two elements.

On the other hand, U is generated by $[\varepsilon]$, so

$$U^\perp = \{[b] \in S_K : h_K(\varepsilon, b) = 0\}.$$

Thus $|U^\perp| = 2$. Combining this with $U \subseteq U^\perp$ and $|U| = 2$ yields

$$U^\perp = U.$$

□

There is also a direct valuation-theoretic interpretation. Put

$$L = K(\sqrt{\varepsilon}).$$

Since L/K is unramified of degree two,

$$v_K(N_{L/K} z) = 2v_L(z).$$

Every norm therefore has even valuation. Conversely, the norm map on units is surjective, and

$$N_{L/K}(\varpi) = \varpi^2.$$

Hence

$$N_{L/K}(L^\times) = \varpi^{2\mathbb{Z}} \mathcal{O}_K^\times.$$

The norm criterion now gives

$$h_K(\varepsilon, b) = 0 \quad \Longleftrightarrow \quad v_K(b) \equiv 0 \pmod 2.$$

A square class has even valuation if and only if it can be represented by a unit. Thus this kernel is precisely U. In particular,

$$h_K(\varepsilon, \varpi) = \frac{1}{2}.$$

Under the identification of the cohomological pairing with the Hilbert symbol, the orthogonal-complement identity becomes

$$\Big(\kappa_M(U)\Big)^{\perp} = \kappa_N(U).$$

Here $\kappa_M(U)$ is a subgroup of $H^1(K, M)$, and its orthogonal complement lies in $H^1(K, N)$.

In the following sections, we will construct the Kummer maps for the isogeny and its dual. Under the good reduction hypothesis, we can prove that their images are exactly $\kappa_M(U)$ and $\kappa_N(U)$, respectively. The orthogonal-complement identity obtained in this section from unramified extensions, norms, and Hilbert symbols will then give the local duality relation between the two Kummer images.

5 Kummer Exact Sequences and Coordinate Formulas

The preceding section constructed a perfect pairing

$$B_\varphi : H^1(K, M) \times H^1(K, N) \longrightarrow D, \qquad D = \tfrac{1}{2}\mathbb{Z}/\mathbb{Z},$$

and proved that, in square-class coordinates,

$$B_\varphi\Big(\kappa_M([a]), \kappa_N([b])\Big) = h_K(a, b).$$

We now relate the rational points of the elliptic curves to these cohomology groups. The connecting homomorphisms associated with the isogeny and its dual provide this relation. We first construct the resulting Kummer exact sequences, then use the rational functions from the preceding sections to derive explicit coordinate formulas in the running example.

We retain the standing assumptions: $K/\mathbb{Q}_p$ is a finite extension with $p \neq 2$, and $\varphi : E \to E'$ is a degree-two K-isogeny with dual $\widehat{\varphi} : E' \to E$. Put

$$M = E[\varphi] = \{O, T\}, \qquad N = E'[\widehat{\varphi}] = \{O', T'\}.$$

No good reduction assumption is needed in this section.

5.1 The Two Kummer Exact Sequences

An isogeny is surjective on geometric points. Since the kernel of φ is M, there is a short exact sequence of discrete continuous G_K-modules

$$0 \longrightarrow M \longrightarrow E(\overline{K}) \xrightarrow{\varphi} E'(\overline{K}) \longrightarrow 0.$$

The associated long exact sequence in Galois cohomology contains

$$E(K) \xrightarrow{\varphi} E'(K) \xrightarrow{\delta_\varphi} H^1(K, M) \longrightarrow H^1(K, E) \xrightarrow{\varphi_*} H^1(K, E').$$

As in the preliminaries, write

$$H^1(K, E)[\varphi] = \ker\Big(H^1(K, E) \xrightarrow{\varphi_*} H^1(K, E')\Big).$$

Exactness gives the following statement.

Proposition 5.1.1 (Kummer exact sequences)**.** There are natural short exact sequences

$$\begin{aligned} 0 \longrightarrow E'(K)/\varphi E(K) &\xrightarrow{\delta_\varphi} H^1(K, M) \\ &\xrightarrow{\rho_\varphi} H^1(K, E)[\varphi] \longrightarrow 0, \end{aligned}$$

and

$$\begin{aligned} 0 \longrightarrow E(K)/\widehat{\varphi}E'(K) &\xrightarrow{\delta_{\widehat{\varphi}}} H^1(K, N) \\ &\xrightarrow{\rho_{\widehat{\varphi}}} H^1(K, E')[\widehat{\varphi}] \longrightarrow 0. \end{aligned}$$

The maps ρ_φ and $\rho_{\widehat{\varphi}}$ are induced by the inclusions $M \hookrightarrow E(\overline{K})$ and $N \hookrightarrow E'(\overline{K})$, respectively.

The connecting homomorphisms can be described explicitly. Given $P' \in E'(K)$, choose $Q \in E(\overline{K})$ such that $\varphi(Q) = P'$. For every $\sigma \in G_K$,

$$\varphi(\sigma Q - Q) = \sigma P' - P' = O',$$

so

$$c_\sigma = \sigma Q - Q \in M.$$

Moreover,

$$\begin{aligned} c_{\sigma\tau} &= \sigma\tau Q - Q \\ &= \sigma(\tau Q - Q) + (\sigma Q - Q) \\ &= \sigma c_\tau + c_\sigma. \end{aligned}$$

Thus c is a continuous 1-cocycle, and

$$\delta_\varphi(P') = \Big[\sigma \longmapsto \sigma Q - Q\Big].$$

We use the same notation for the connecting map on $E'(K)$ and the induced injection on $E'(K)/\varphi E(K)$.

If Q is replaced by $Q + S$, where $S \in M$, the resulting cocycle is

$$c_\sigma + \sigma S - S.$$

It differs from the original cocycle by a coboundary, so its cohomology class is independent of the chosen preimage. Likewise, for $P \in E(K)$ and $Q' \in E'(\overline{K})$ satisfying $\widehat{\varphi}(Q') = P$,

$$\delta_{\widehat{\varphi}}(P) = \Big[\sigma \longmapsto \sigma Q' - Q'\Big].$$

This description also explains the kernel of the connecting map. If $P' = \varphi(R)$ for some $R \in E(K)$, we may take $Q = R$, giving the zero cocycle. Conversely, if $\delta_\varphi(P') = 0$, there is an $S \in M$ such that

$$\sigma Q - Q = \sigma S - S \qquad \text{for every } \sigma \in G_K.$$

It follows that $Q - S \in E(K)$ and

$$\varphi(Q - S) = P'.$$

Consequently,

$$\ker \delta_\varphi = \varphi E(K).$$

The class $\delta_\varphi(P')$ therefore measures the obstruction to choosing a preimage of P' over K. The dual connecting map has the same interpretation.

5.2 Kummer Coordinates for the Isogeny in the Running Example

Return to the curves

$$E : y^2 = x^3 - x, \qquad E' : v^2 = u^3 + 4u,$$

and the isogeny

$$\varphi(x, y) = \left(x - \frac{1}{x},\ y\left(1 + \frac{1}{x^2}\right)\right).$$

Here

$$T = (0, 0) \in E(K), \qquad T' = (0, 0) \in E'(K).$$

To distinguish cohomology classes from square classes, define

$$\Delta_\varphi = \kappa_M^{-1} \circ \delta_\varphi : E'(K) \longrightarrow S_K$$

and

$$\Delta_{\widehat{\varphi}} = \kappa_N^{-1} \circ \delta_{\widehat{\varphi}} : E(K) \longrightarrow S_K.$$

These are the square-class coordinates of the two Kummer maps. The zero cohomology class corresponds to the multiplicative identity $1 \in S_K$.

Proposition 5.2.1. If $P' = (u_0, v_0) \in E'(K)$ and $u_0 \neq 0$, then

$$\Delta_\varphi(P') = [u_0].$$

Proof. In the construction of the kernel pairing, we used

$$g = \frac{y}{x}$$

and proved the identities

$$g^2 = u \circ \varphi, \qquad g \circ \tau_T = -g.$$

Choose $Q \in E(\overline{K})$ with $\varphi(Q) = P'$. Since $u_0 \neq 0$, the value $g(Q)$ is defined and nonzero, and

$$g(Q)^2 = u_0.$$

Write

$$\sigma Q - Q = i_\sigma T, \qquad i_\sigma \in \{0, 1\}.$$

The function g is defined over K, so

$$\sigma(g(Q)) = g(\sigma Q) = g(Q + i_\sigma T) = (-1)^{i_\sigma} g(Q).$$

Hence

$$\frac{\sigma(g(Q))}{g(Q)} = (-1)^{i_\sigma}.$$

The left-hand side is the multiplicative Kummer cocycle associated with $[u_0]$. The right-hand side is the image of the elliptic-curve Kummer cocycle under

$$M \xrightarrow{\sim} \mu_2, \qquad T \longmapsto -1.$$

Therefore

$$\delta_\varphi(P') = \kappa_M([u_0]),$$

which proves the assertion. □

The points O' and T' must be treated separately. Taking O as a preimage of O' gives

$$\Delta_\varphi(O') = 1.$$

For T', the calculation in the preceding sections gives

$$\varphi^{-1}(T') = \{(1, 0), (-1, 0)\}.$$

Both points are defined over K, so $T' \in \varphi E(K)$ and

$$\Delta_\varphi(T') = 1.$$

The complete formula is thus

$$\Delta_\varphi(P') = \begin{cases} 1, & P' = O', \\ 1, & P' = T', \\ [u(P')], & P' \notin \{O', T'\}. \end{cases}$$

The value at T' may also be written as $[4]$, since 4 is a square. It cannot be obtained by substituting $u(T') = 0$ into the formula for the other affine points: zero does not define an element of S_K.

5.3 Kummer Coordinates for the Dual Isogeny

The dual isogeny is

$$\widehat{\varphi}(u,v) = \left(\frac{u^2+4}{4u},\ \frac{v(u^2-4)}{8u^2} \right).$$

We have already recorded the identity

$$\left(\frac{v}{2u}\right)^2 = x \circ \widehat{\varphi}.$$

Put

$$h = \frac{v}{2u}.$$

To apply the argument used for φ, we first compute the effect of translation by T' on h. The line through (u,v) and $T' = (0,0)$ has slope v/u. The addition formulas give

$$u(P'+T') = \frac{v^2}{u^2} - u = \frac{4}{u}$$

and

$$v(P'+T') = \frac{v}{u}\left(u - \frac{4}{u}\right) - v = -\frac{4v}{u^2}.$$

Thus

$$\tau_{T'}(u,v) = \left(\frac{4}{u}, -\frac{4v}{u^2}\right),$$

and consequently

$$h \circ \tau_{T'} = \frac{-4v/u^2}{2(4/u)} = -\frac{v}{2u} = -h.$$

Proposition 5.3.1. If $P = (x_0, y_0) \in E(K)$ and $x_0 \neq 0$, then

$$\Delta_{\widehat{\varphi}}(P) = [x_0].$$

Proof. Choose $Q' \in E'(\overline{K})$ such that $\widehat{\varphi}(Q') = P$. The function identity gives

$$h(Q')^2 = x_0.$$

If

$$\sigma Q' - Q' = j_\sigma T', \qquad j_\sigma \in \{0,1\},$$

then

$$\frac{\sigma(h(Q'))}{h(Q')} = \frac{h(Q'+j_\sigma T')}{h(Q')} = (-1)^{j_\sigma}.$$

Under $N \simeq \mu_2$, the connecting cocycle is therefore the Kummer cocycle of $[x_0]$. Hence

$$\delta_{\widehat{\varphi}}(P) = \kappa_N([x_0]).$$

□

At the identity,

$$\Delta_{\widehat{\varphi}}(O) = 1.$$

To compute the value at $T = (0,0)$, choose $i \in \overline{K}$ with $i^2 = -1$ and put

$$R' = (2i, 0).$$

Since

$$(2i)^3 + 4(2i) = 0,$$

we have $R' \in E'(\overline{K})$, and direct substitution gives

$$\widehat{\varphi}(R') = T.$$

If $\sigma(i) = i$, then $\sigma R' = R'$. If $\sigma(i) = -i$, then

$$\sigma R' = (-2i, 0) = R' + T'.$$

The connecting cocycle thus gives exactly the quadratic character associated with $[-1]$, including the trivial character when -1 is a square in K. Therefore

$$\Delta_{\widehat{\varphi}}(T) = [-1].$$

The complete formula is

$$\Delta_{\widehat{\varphi}}(P) = \begin{cases} 1, & P = O, \\ [-1], & P = T, \\ [x(P)], & P \notin \{O, T\}. \end{cases}$$

Both coordinate formulas arise from the same construction. A rational function has square equal to the pullback of a coordinate function on the target curve, and translation by the nonzero kernel point changes its sign. The Galois action on a preimage is thereby expressed as the Galois action on a square root.

5.4 The Local Kummer Images

Return to a general degree-two isogeny. Define

$$L_{\varphi} = \operatorname{im}\Big(\delta_{\varphi} : E'(K) \longrightarrow H^1(K, M)\Big)$$

and

$$L_{\widehat{\varphi}} = \operatorname{im}\Big(\delta_{\widehat{\varphi}} : E(K) \longrightarrow H^1(K, N)\Big).$$

The Kummer exact sequences identify these groups as

$$L_{\varphi} \simeq E'(K)/\varphi E(K), \qquad L_{\widehat{\varphi}} \simeq E(K)/\widehat{\varphi} E'(K).$$

They also give

$$H^1(K, M)/L_{\varphi} \simeq H^1(K, E)[\varphi]$$

and

$$H^1(K, N)/L_{\widehat{\varphi}} \simeq H^1(K, E')[\widehat{\varphi}].$$

To pass from the pairing on the kernel cohomology groups to a pairing involving rational points and the Weil–Châtelet groups, we must determine the orthogonal complements of these two subgroups. Under good reduction, the next section will prove

$$L_{\varphi} = \kappa_M(U), \qquad L_{\widehat{\varphi}} = \kappa_N(U).$$

The orthogonal-complement identity for unit square classes will then give

$$L_{\varphi}^{\perp} = L_{\widehat{\varphi}}.$$

6 Local Duality under Good Reduction

In this section we impose the additional assumption that E and E' both have good reduction over K. We continue to assume

$$K/\mathbb{Q}_p \text{ is finite}, \qquad p \neq 2, \qquad \deg \varphi = 2.$$

Write the reductions of the curves as $\widetilde{E}$ and $\widetilde{E}'$, and the reductions of the two isogenies as

$$\widetilde{\varphi} : \widetilde{E} \longrightarrow \widetilde{E}', \qquad \widetilde{\widehat{\varphi}} : \widetilde{E}' \longrightarrow \widetilde{E}.$$

The proof has three steps. We first use formal groups to control the kernels of reduction. We then show that the Kummer images are exactly the unramified cohomology subgroups. Finally, the Hilbert-symbol calculation yields the orthogonal-complement theorem and the resulting perfect pairings.

6.1 The Isogenies on the Kernels of Reduction

For a finite extension L/K, with residue field k_L, put

$$E_1(L) = \ker\Big(E(L) \longrightarrow \widetilde{E}(k_L)\Big),$$

and use the analogous notation for E'. Good reduction is preserved under finite extension. By the extension theorem for prime-to-p isogenies in the preliminaries, the isogenies extend to the good models and commute with reduction. In particular,

$$\varphi(E_1(L)) \subseteq E_1'(L), \qquad \widehat{\varphi}(E_1'(L)) \subseteq E_1(L).$$

Lemma 6.1.1. For every finite extension L/K, the restrictions

$$\varphi : E_1(L) \longrightarrow E_1'(L)$$

and

$$\widehat{\varphi} : E_1'(L) \longrightarrow E_1(L)$$

are isomorphisms.

Proof. In the formal group at the identity, multiplication by two has the form

$$[2]_{\mathcal{F}}(t) = 2t + \text{terms of degree at least two.}$$

Since $p \neq 2$, the linear coefficient is a unit in $\mathcal{O}_L$. The existence of a formal inverse therefore shows that

$$[2] : E_1(L) \longrightarrow E_1(L)$$

is an isomorphism. The same statement holds for $E_1'(L)$.

Suppose $Q \in E_1(L)$ and $\varphi(Q) = O'$. Then

$$[2]Q = \widehat{\varphi}(\varphi(Q)) = O.$$

Injectivity of $[2]$ on $E_1(L)$ gives $Q = O$, proving injectivity of φ on this subgroup.

For surjectivity, take $R' \in E_1'(L)$. There is an $S' \in E_1'(L)$ such that $[2]S' = R'$. Hence

$$\varphi\Big(\widehat{\varphi}(S')\Big) = [2]S' = R',$$

and $\widehat{\varphi}(S') \in E_1(L)$. Thus φ is surjective. Interchanging the isogenies proves the second assertion. □

Proposition 6.1.2. Reduction induces natural isomorphisms

$$E'(K)/\varphi E(K) \simeq \widetilde{E}'(k)/\widetilde{\varphi}\,\widetilde{E}(k)$$

and

$$E(K)/\widehat{\varphi}E'(K) \simeq \widetilde{E}(k)/\widetilde{\widehat{\varphi}}\,\widetilde{E}'(k).$$

Proof. Compatibility of reduction with the isogeny shows that $P' \mapsto \widetilde{P}'$ induces the first homomorphism of quotient groups. It is surjective because $E'(K) \to \widetilde{E}'(k)$ is surjective.

To prove injectivity, suppose

$$\widetilde{P}' \in \widetilde{\varphi}\,\widetilde{E}(k).$$

Choose $\widetilde{Q} \in \widetilde{E}(k)$ such that

$$\widetilde{\varphi}(\widetilde{Q}) = \widetilde{P}',$$

and lift $\widetilde{Q}$ to $Q \in E(K)$. Then

$$P' - \varphi(Q) \in E_1'(K).$$

By the preceding lemma, there is an $R \in E_1(K)$ with

$$\varphi(R) = P' - \varphi(Q).$$

It follows that $P' = \varphi(Q + R)$, so the class of P' in $E'(K)/\varphi E(K)$ is zero. This proves injectivity. The proof for the dual isogeny is identical. □

6.2 The Kummer Images Are Unramified

Recall that

$$H^1_{\mathrm{ur}}(K, M) = \ker\Big(H^1(K, M) \longrightarrow H^1(I_K, M)\Big).$$

Proposition 6.2.1. Under the good reduction assumption,

$$L_\varphi \subseteq H^1_{\mathrm{ur}}(K, M), \qquad L_{\widehat{\varphi}} \subseteq H^1_{\mathrm{ur}}(K, N).$$

Proof. Let $P' \in E'(K)$. We show that $P' \in \varphi E(L)$ for some finite unramified extension L/K.

The reduction $\widetilde{\varphi}$ is an isogeny and is therefore surjective on geometric points. Choose

$$\widetilde{Q} \in \widetilde{E}(\overline{k}) \qquad \text{with} \qquad \widetilde{\varphi}(\widetilde{Q}) = \widetilde{P}'.$$

The point $\widetilde{Q}$ is defined over some finite extension k'/k. Let L/K be the corresponding finite unramified extension, with residue field k'.

Smoothness and Hensel lifting give a point $Q_0 \in E(L)$ reducing to $\widetilde{Q}$. Thus

$$D' = P' - \varphi(Q_0) \in E_1'(L).$$

By Lemma 6.1.1, there is an $R \in E_1(L)$ such that $\varphi(R) = D'$. Putting $Q = Q_0 + R$, we obtain

$$Q \in E(L), \qquad \varphi(Q) = P'.$$

Use this preimage to represent the connecting class by

$$c_\sigma = \sigma Q - Q.$$

Because L/K is unramified, it is contained in K^{ur} and is fixed by I_K. Hence

$$c_\sigma = 0 \qquad \text{for every } \sigma \in I_K.$$

Therefore $\delta_\varphi(P')$ is unramified. Applying the same argument to $\widehat{\varphi}$ proves the other inclusion. □

The proof also shows that every K-rational point on the target has an isogeny preimage over a finite unramified extension.

6.3 The Orders of the Kummer Images

To turn the inclusions just proved into equalities, we determine the orders of the Kummer images. Proposition 6.1.2 reduces this to a computation with point groups over the finite field k.

Lemma 6.3.1. If two elliptic curves C and C' are isogenous over $k = \mathbb{F}_q$, then

$$\#C(k) = \#C'(k).$$

Proof. Let $\psi : C \to C'$ be a k-isogeny, and let π and π' denote the q-power Frobenius endomorphisms. Since ψ is defined over k,

$$\pi' \circ \psi = \psi \circ \pi,$$

and consequently

$$(\pi' - [1]) \circ \psi = \psi \circ (\pi - [1]).$$

The differential of Frobenius is zero, so

$$d(\pi - [1]) = -1.$$

Thus $\pi - [1]$ is a separable isogeny. Its geometric kernel is exactly $C(k)$, giving

$$\deg(\pi - [1]) = \#C(k).$$

Similarly,

$$\deg(\pi' - [1]) = \#C'(k).$$

Taking degrees in the composition identity yields

$$\deg(\pi' - [1]) \deg \psi = \deg \psi \deg(\pi - [1]).$$

Canceling $\deg \psi$ proves the assertion. □

Proposition 6.3.2. Each local Kummer image has exactly two elements:

$$|L_\varphi| = |L_{\widehat{\varphi}}| = 2.$$

Proof. First consider φ. Its nonzero kernel point $T \in E(K)$ cannot reduce to the identity. Otherwise $T \in E_1(K)$ and $[2]T = O$, contradicting injectivity of $[2]$ on $E_1(K)$. Hence

$$\widetilde{T} \neq \widetilde{O}.$$

The reduced isogeny $\widetilde{\varphi}$ is separable of degree two, so its geometric kernel has two elements. They are $\widetilde{O}$ and $\widetilde{T}$, both of which are k-rational. Consequently,

$$\left|\ker\left(\widetilde{\varphi} : \widetilde{E}(k) \longrightarrow \widetilde{E}'(k)\right)\right| = 2.$$

The order formula for a homomorphism of finite groups gives

$$\left|\widetilde{\varphi}\,\widetilde{E}(k)\right| = \frac{\#\widetilde{E}(k)}{2}.$$

The preceding lemma therefore implies

$$\left|\widetilde{E}'(k)/\widetilde{\varphi}\,\widetilde{E}(k)\right| = \frac{\#\widetilde{E}'(k)}{\#\widetilde{E}(k)/2} = 2.$$

By Proposition 6.1.2 and injectivity of the Kummer map on the quotient,

$$|L_\varphi| = |E'(K)/\varphi E(K)| = 2.$$

The same argument for $\widehat{\varphi}$ gives $|L_{\widehat{\varphi}}| = 2$. □

On the other hand, the Galois action on M is trivial. Inflation–restriction gives

$$H^1_{\mathrm{ur}}(K, M) \simeq H^1(G_k, M) = \mathrm{Hom}_{\mathrm{cont}}(G_k, M).$$

Since

$$G_k \simeq \widehat{\mathbb{Z}}, \qquad M \simeq \mathbb{Z}/2\mathbb{Z},$$

a continuous homomorphism is uniquely determined by the image of arithmetic Frobenius, and either element of M can occur as its image. Thus

$$|H^1_{\mathrm{ur}}(K, M)| = 2.$$

The same holds for N. Combining this with Propositions 6.2.1 and 6.3.2 proves

$$L_\varphi = H^1_{\mathrm{ur}}(K, M), \qquad L_{\widehat{\varphi}} = H^1_{\mathrm{ur}}(K, N).$$

6.4 Unit Square Classes and the Orthogonal-Complement Theorem

We now express the unramified cohomology subgroups in square-class coordinates.

Lemma 6.4.1. Under the Kummer identifications fixed in the preceding section,

$$H^1_{\mathrm{ur}}(K, M) = \kappa_M(U), \qquad H^1_{\mathrm{ur}}(K, N) = \kappa_N(U).$$

Proof. Choose $\varepsilon \in \mathcal{O}_K^\times$ with nonsquare residue. By the preliminaries,

$$U = \{1, [\varepsilon]\},$$

and $K(\sqrt{\varepsilon})/K$ is the unramified quadratic extension. The square class $[\varepsilon]$ corresponds to the cocycle

$$\sigma \longmapsto \chi_\varepsilon(\sigma)T.$$

Inertia fixes $\sqrt{\varepsilon}$, so this cocycle restricts to zero on I_K. Therefore

$$\kappa_M(U) \subseteq H^1_{\mathrm{ur}}(K, M).$$

Both sides have two elements, so they are equal. The argument for N is identical. □

We can now prove the central result of the report.

Theorem 6.4.2 (Orthogonality of the local Kummer images)**.** *Let $K/\mathbb{Q}_p$ be a finite extension with $p \neq 2$, and let $\varphi : E \to E'$ be a degree-two K-isogeny. Suppose that both curves have good reduction. With respect to*

$$B_\varphi : H^1(K, M) \times H^1(K, N) \longrightarrow D,$$

the local Kummer images satisfy

$$L_\varphi^\perp = L_{\widehat{\varphi}}.$$

In the opposite direction,

$$L_{\widehat{\varphi}}^{\perp} = L_{\varphi},$$

where this second orthogonal complement is taken in $H^1(K, M)$.

Proof. The results above give

$$L_{\varphi} = \kappa_M(U), \qquad L_{\widehat{\varphi}} = \kappa_N(U).$$

The preceding section proved both

$$B_{\varphi}\Big(\kappa_M([a]), \kappa_N([b])\Big) = h_K(a, b)$$

and

$$U^{\perp} = U.$$

For any $[b] \in S_K$, it follows that

$$\begin{aligned} \kappa_N([b]) \in L_{\varphi}^{\perp} &\iff h_K(u, b) = 0 \quad \text{for every } [u] \in U \\ &\iff [b] \in U^{\perp} \\ &\iff [b] \in U \\ &\iff \kappa_N([b]) \in L_{\widehat{\varphi}}. \end{aligned}$$

This proves the first equality. Interchanging the two sides and using the symmetry of the Hilbert symbol proves the second. □

The two Kummer images belong to different cohomology groups. Each corresponds to U in square-class coordinates, and the kernel pairing identifies them as the exact annihilators of one another.

6.5 From Orthogonal Complements to Finite-Level Local Duality

Put

$$V = H^1(K, M), \qquad W = H^1(K, N).$$

We have a perfect pairing $B_{\varphi} : V \times W \to D$ and an equality

$$L_{\varphi}^{\perp} = L_{\widehat{\varphi}}.$$

Restricting the first variable therefore gives a pairing on

$$L_{\varphi} \times W/L_{\widehat{\varphi}}.$$

The Kummer exact sequences identify these groups with a quotient of the rational point group and a subgroup of the Weil–Châtelet group, respectively.

Theorem 6.5.1 (Local duality for a degree-two isogeny with good reduction)**.** *Under the assumptions of Theorem 6.4.2, there are natural perfect pairings*

$$E'(K)/\varphi E(K) \times H^1(K, E')[\widehat{\varphi}] \longrightarrow D$$

and

$$E(K)/\widehat{\varphi}E'(K) \times H^1(K, E)[\varphi] \longrightarrow D.$$

Proof. We first construct the first pairing. Let

$$\overline{P'} \in E'(K)/\varphi E(K), \qquad \eta \in H^1(K, E')[\widehat{\varphi}].$$

By the second Kummer exact sequence, choose $w \in H^1(K, N)$ such that

$$\rho_{\widehat{\varphi}}(w) = \eta.$$

Define

$$\langle \overline{P'}, \eta \rangle_\varphi = B_\varphi\Big(\delta_\varphi(P'), w\Big).$$

We first check independence of the choices. Replacing P' by another representative of the same quotient class does not change $\delta_\varphi(P')$. If w' is another lift of η, exactness gives

$$w' - w \in L_{\widehat{\varphi}}.$$

Since $L_{\widehat{\varphi}} = L_\varphi^\perp$,

$$B_\varphi\Big(\delta_\varphi(P'), w' - w\Big) = 0.$$

Thus the value is also independent of the chosen lift. Bilinearity follows from bilinearity of B_φ.

For left nondegeneracy, suppose that $\overline{P'}$ pairs trivially with every element on the right. For any $w \in W$, take $\eta = \rho_{\widehat{\varphi}}(w)$. Then

$$B_\varphi\Big(\delta_\varphi(P'), w\Big) = 0.$$

Nondegeneracy of B_φ gives $\delta_\varphi(P') = 0$, and the Kummer exact sequence implies $\overline{P'} = 0$.

For right nondegeneracy, suppose that η pairs trivially with every $\overline{P'}$. Choose a lift $w \in W$. Then

$$B_\varphi(\ell, w) = 0 \qquad \text{for every } \ell \in L_\varphi.$$

Hence

$$w \in L_\varphi^\perp = L_{\widehat{\varphi}},$$

and exactness gives $\eta = \rho_{\widehat{\varphi}}(w) = 0$. The groups are finite, so nondegeneracy on both sides proves that the pairing is perfect.

For the second pairing, take

$$\overline{P} \in E(K)/\widehat{\varphi}E'(K), \qquad \xi \in H^1(K, E)[\varphi],$$

choose $v \in V$ with $\rho_\varphi(v) = \xi$, and define

$$\langle \overline{P}, \xi \rangle_{\widehat{\varphi}} = B_\varphi\Big(v, \delta_{\widehat{\varphi}}(P)\Big).$$

Using $L_{\widehat{\varphi}}^\perp = L_\varphi$, the same argument proves that this pairing is well-defined and perfect. $\square$

In square-class coordinates, the first pairing has a direct formula. If

$$\delta_\varphi(P') = \kappa_M([a]), \qquad \eta = \rho_{\widehat{\varphi}}\Big(\kappa_N([b])\Big),$$

then

$$\langle \overline{P'}, \eta \rangle_\varphi = h_K(a, b).$$

Here $[a] \in U$, while $[b]$ is determined only up to multiplication by an element of U. Since the Hilbert symbol vanishes on $U \times U$, the right-hand side does not depend on this choice.

One can also exhibit a nonzero value of the pairing. Choose a nonsquare unit ε and a uniformizer ϖ. Since $L_\varphi = \kappa_M(U)$, there is a $P' \in E'(K)$ such that

$$\delta_\varphi(P') = \kappa_M([\varepsilon]).$$

Put

$$\eta_\varpi = \rho_{\widehat{\varphi}}\Big(\kappa_N([\varpi])\Big).$$

Because $[\varpi] \notin U$, we have $\eta_\varpi \neq 0$. The norm calculation in the preceding section gives

$$\langle \overline{P'}, \eta_\varpi \rangle_\varphi = h_K(\varepsilon, \varpi) = \tfrac{1}{2}.$$

Indeed,

$$|E'(K)/\varphi E(K)| = 2$$

and

$$|H^1(K, E')[\widehat{\varphi}]| = \frac{|H^1(K, N)|}{|L_{\widehat{\varphi}}|} = \frac{4}{2} = 2.$$

Thus this calculation gives the pairing of the unique nonzero elements.

Finally, we relate the construction to the usual local Tate pairing. Its standard compatibility with the connecting homomorphisms gives

$$\langle P', \rho_{\widehat{\varphi}}(w) \rangle_{\mathrm{Tate},E'} = B_\varphi\Big(\delta_\varphi(P'), w\Big).$$

Accordingly, the pairing constructed above is the local Tate pairing at the finite level determined by the isogeny.

The perfectness at this finite level has been proved directly from good reduction, Kummer theory, and the Hilbert symbol. The next section will apply these results to the running example over $\mathbb{Q}_5$, making both Kummer images and a nonzero local pairing value explicit.

7 An Explicit Computation over $\mathbb{Q}_5$

7.1 The Curves and the Square-Class Group

Take

$$K = \mathbb{Q}_5, \qquad E : y^2 = x^3 - x, \qquad E' : v^2 = u^3 + 4u.$$

The degree-two isogeny and its dual constructed in Section 3 are

$$\varphi(x, y) = \left(x - \frac{1}{x},\, y\left(1 + \frac{1}{x^2}\right)\right)$$

and

$$\widehat{\varphi}(u, v) = \left(\frac{u^2 + 4}{4u},\, \frac{v(u^2 - 4)}{8u^2}\right).$$

Their kernels are

$$M = \{O, T\}, \qquad N = \{O', T'\},$$

where $T = (0, 0) \in E(K)$ and $T' = (0, 0) \in E'(K)$.

The displayed integral Weierstrass equations have discriminants

$$\Delta_E = 64, \qquad \Delta_{E'} = -4096.$$

Both are units in $\mathbb{Z}_5$. Thus both curves have good reduction, and the results of Section 6 apply.

The nonzero squares in $\mathbb{F}_5$ are 1 and 4, so 2 is a nonsquare unit in K. Taking 5 as a uniformizer gives

$$S_K = K^\times / K^{\times 2} = \{1, [2], [5], [10]\}, \qquad U = \{1, [2]\}.$$

The class [2] generates the unit square-class subgroup, while the exponent of [5] records the parity of the valuation.

7.2 Explicit Generators of the Kummer Images

Recall the square-class coordinates introduced in Section 5:

$$\Delta_\varphi = \kappa_M^{-1} \circ \delta_\varphi, \qquad \Delta_{\widehat{\varphi}} = \kappa_N^{-1} \circ \delta_{\widehat{\varphi}}.$$

For affine points with nonzero first coordinate, they satisfy

$$\Delta_\varphi(u, v) = [u], \qquad \Delta_{\widehat{\varphi}}(x, y) = [x].$$

First take

$$P' = (2, 4) \in E'(K).$$

Indeed, $4^2 = 2^3 + 4 \cdot 2$. The coordinate formula gives

$$\Delta_\varphi(P') = [2], \qquad \delta_\varphi(P') = \kappa_M([2]) \neq 0.$$

Consequently, $P' \notin \varphi E(K)$.

For the other curve, apply Hensel's lemma to $F(Y) = Y^2 - 6$ at $Y = 1$. Since

$$F(1) \equiv 0 \pmod 5, \qquad F'(1) \not\equiv 0 \pmod 5,$$

there is an $s \in \mathbb{Z}_5$ with $s^2 = 6$ and $s \equiv 1 \pmod 5$. Hence

$$P = (2, s) \in E(K), \qquad \Delta_{\widehat{\varphi}}(P) = [2].$$

It follows that

$$\delta_{\widehat{\varphi}}(P) = \kappa_N([2]) \neq 0,$$

so $P \notin \widehat{\varphi}E'(K)$.

The good reduction argument in Section 6 identifies the two Kummer images with $\kappa_M(U)$ and $\kappa_N(U)$, respectively. Thus

$$L_\varphi = \{0, \kappa_M([2])\}, \qquad L_{\widehat{\varphi}} = \{0, \kappa_N([2])\}.$$

In particular,

$$E'(K)/\varphi E(K) = \{0, \overline{P'}\}, \qquad E(K)/\widehat{\varphi}E'(K) = \{0, \overline{P}\},$$

where the bars denote classes in the respective quotient groups.

The nonsquare coordinate of P' therefore gives an explicit obstruction to choosing a K-rational preimage under φ. The point P has the same interpretation for the dual isogeny.

7.3 The Quadratic Hilbert Symbol

The result for units in Section 4 gives

$$h_5(2, 2) = 0.$$

To compute $h_5(2, 5)$, consider

$$L = \mathbb{Q}_5(\sqrt{2}).$$

Since 2 has nonsquare residue, L/K is the unramified quadratic extension. For the normalized valuations,

$$v_5(N_{L/K}z) = 2v_L(z).$$

Every norm has even valuation, whereas $v_5(5) = 1$. The norm criterion for the Hilbert symbol therefore gives

$$(2, 5)_5 = -1, \qquad h_5(2, 5) = \frac{1}{2}.$$

This value can also be read directly from local reciprocity. With the normalization fixed in the preliminaries, $\mathrm{rec}_K(5)$ acts as arithmetic Frobenius on unramified extensions. If α is the residue of $\sqrt{2}$ in $\mathbb{F}_{25}$, then

$$\alpha^5 = \alpha(\alpha^2)^2 = 4\alpha = -\alpha.$$

Thus Frobenius is the nontrivial automorphism of L/K, and its action on $\sqrt{2}$ changes the sign.

For completeness, we also compute $h_5(5, 5)$. Hensel's lemma applied to $X^2 + 1$ at $X = 2$ shows that -1 is a square in K. Choose $i \in K$ with $i^2 = -1$. In the quadratic extension $K(\sqrt{5})/K$,

$$N_{K(\sqrt{5})/K}(i\sqrt{5}) = (i\sqrt{5})(-i\sqrt{5}) = 5.$$

The norm criterion now gives

$$h_5(5, 5) = 0.$$

Since [2] and [5] generate S_K, bilinearity and symmetry determine the entire pairing:

$h_5(a,b)$	1	2	5	10
1	0	0	0	0
2	0	0	$\frac{1}{2}$	$\frac{1}{2}$
5	0	$\frac{1}{2}$	0	$\frac{1}{2}$
10	0	$\frac{1}{2}$	$\frac{1}{2}$	0

The row and column labels denote square classes. The elements pairing trivially with [2] are exactly 1 and [2]. Hence

$$U^{\perp} = U.$$

Through κ_M and κ_N, this explicitly realizes the identity

$$L_{\varphi}^{\perp} = L_{\widehat{\varphi}}.$$

7.4 A Nonzero Value of the Local Tate Pairing

The second Kummer exact sequence gives

$$H^1(K,E')[\widehat{\varphi}] \simeq H^1(K,N)/L_{\widehat{\varphi}} \simeq S_K/U.$$

The last quotient has two elements, represented by the cosets

$$U = \{1,[2]\}, \qquad [5]U = \{[5],[10]\}.$$

Put

$$\eta = \rho_{\widehat{\varphi}}\Big(\kappa_N([5])\Big) \in H^1(K,E')[\widehat{\varphi}].$$

Since $[5] \notin U$, we have $\eta \neq 0$, and

$$H^1(K,E')[\widehat{\varphi}] = \{0,\eta\}.$$

By the definition of the pairing in Theorem 6.5.1,

$$\begin{aligned}\langle \overline{P'}, \eta \rangle_{\varphi} &= B_{\varphi}\Big(\delta_{\varphi}(P'), \kappa_N([5])\Big) \\ &= B_{\varphi}\Big(\kappa_M([2]), \kappa_N([5])\Big) \\ &= h_5(2,5) = \frac{1}{2}.\end{aligned}$$

Replacing [5] by [10] gives the same Weil–Châtelet class, because the two classes differ by the unit square class [2]. The pairing value is likewise unchanged:

$$h_5(2,10) = h_5(2,2) + h_5(2,5) = \frac{1}{2}.$$

This directly verifies independence of the chosen lift in this example.

Both groups have order two, so the complete pairing is

$\langle\ ,\ \rangle_{\varphi}$	0	η
0	0	0
$\overline{P'}$	0	$\frac{1}{2}$

The unique nonzero elements pair nontrivially. The pairing is therefore perfect.

For the other pairing, put

$$\xi = \rho_{\varphi}\Big(\kappa_M([5])\Big) \in H^1(K,E)[\varphi].$$

The same argument gives

$$H^1(K,E)[\varphi] = \{0,\xi\}, \qquad \langle \overline{P},\xi\rangle_{\widehat{\varphi}} = h_5(5,2) = \frac{1}{2}.$$

In terms of torsors, η represents a nontrivial E'-torsor with no K-rational point. The nonzero pairing value detects its nontriviality. The condition $\widehat{\varphi}_*\eta = 0$ says that extension of the structure group along $\widehat{\varphi}$ gives a trivial E-torsor.