THE WEIL PAIRING ON COHOMOLOGY

JACOB SWENBERG

1. Introduction

Motivated by work of Sharifi, we explore the pairing on Galois cohomology

$$H^1(G_{F,S}, E[n]) \times H^1(G_{F,S}, E[n]) \to H^2(G_{F,S}, \mu_n)$$

coming from the cup product and the Weil pairing, where:

- F is a number field;
- n is an odd positive integer;
- S is a set of places of F including the places above primes dividing n but not including any places above 2;
- E is an elliptic curve defined over F with good reduction outside S;
- $G_{F,S}$ is the Galois group of the maximal S-ramified extension F_S over F.

The *Kummer map* is an injection

$$\kappa_n : E(F)/nE(F) \to H^1(G_{F,S}, E[n]).$$

This gives us a pairing

$$E(F) \times E(F) \to H^2(G_{F,S}, \mu_n).$$

2. Kummer Theory and the Weil Pairing

We keep the notation of the introduction. For a matrix M, we denote by M^t its transpose. We denote by $\chi_n : G_{F,S} \to (\mathbb{Z}/n)^\times$ the character giving the action of $G_{F,S}$ on μ_n. For ρ a continuous homomorphism of G_F into another group, we denote by $F(\rho)$ the fixed field of its kernel.

2.1. Let $O_{F,S}$ denote the ring of S-integers of F. This Dedekind ring has class group isomorphic to $\mathrm{Cl}_{F,S}$, the S-class group of F. Let O_S be the ring of S-integers of F_S. Then we have an exact sequence

$$1 \to \mu_n \to O_S^\times \to O_S^\times \to 1$$

and an isomorphism

$$H^1(G_{F,S}, O_S^\times) \cong \mathrm{Cl}_{F,S}.$$

Taking a long exact sequence on cohomology, we have an exact sequence

$$0 \to \mathrm{Cl}_{F,S}/n\,\mathrm{Cl}_{F,S} \to H^2(G_{F,S}, \mu_n) \xrightarrow{\mathrm{inv}} \bigoplus_{v \in S} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0. \tag{2.1.1}$$

See [NSW08, Prop 8.3.11] for more details. *Actually maybe this isn't quite right...*

2.2. By applying the Kummer map, cupping, and taking the Weil pairing, we have a pairing

$$E(F) \times E(F) \to H^2(G_{F,S}, \mu_n),$$
$$(x, y) \longmapsto \langle x, y\rangle_{F,S,n} := e_n([\kappa_n x] \cup [\kappa_n y]),$$

where $e_n : E[n] \times E[n] \to \mu_n$ is the Weil pairing.

Lemma 2.1. *The image of $\langle \cdot, \cdot\rangle_{F,S,n}$ lies in $\mathrm{Cl}_{F,S} / n\, \mathrm{Cl}_{F,S}$.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccccc} E(F) & \times & E(F) & & \\ \downarrow & & \downarrow & & \\ H^1(G_{F,S}, E[n]) & \times & H^1(G_{F,S}, E[n]) & \longrightarrow & H^2(G_{F,S}, \mu_n) \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow \\ \bigoplus_{v\in S} H^1(F_v, E[n]) & \times & \bigoplus_{v\in S} H^1(F_v, E[n]) & \longrightarrow & \bigoplus_{v\in S} \mathbb{Q}/\mathbb{Z} \end{array} \cdot$$

The bottom (local) pairings are perfect by local Tate duality and perfectness of the Weil pairing. By Equation 2.1.1, it suffices to show that for all $v \in S$, the image of the local Kummer map

$$\kappa_{n,v} : E(F_v) \to H^1(F_v, E[n])$$

is self annihilating under the local pairing. □

2.3. Let $x, y \in E(F)$, let $\widetilde{x}, \widetilde{y} \in E$ be such that $n\widetilde{x} = x$ and $n\widetilde{y} = y$. Let $\alpha, \beta : G_F \to E[n]$ be the cocycles defined by $\alpha(\sigma) = \sigma\widetilde{x} - \widetilde{x}$ and $\beta(\sigma) = \sigma\widetilde{y} - \widetilde{y}$. These cocycles are unramified outside of S, and

$$\kappa_n(x) = [\alpha], \qquad \kappa_n(y) = [\beta].$$

2.4. We fix a $(\mathbb{Z}/n)$-basis $v_1, v_2 \in E[n]$. After choosing this basis, we identify $E[n] \cong (\mathbb{Z}/n)^2$ as column vectors. For instance, we will abuse notation and let $\alpha(\sigma)$ and $\beta(\sigma)$ denote column vectors for all $\sigma \in G_{F,S}$:

$$\alpha(\sigma) = \begin{bmatrix} \alpha_1(\sigma) \\ \alpha_2(\sigma) \end{bmatrix}, \qquad \beta(\sigma) = \begin{bmatrix} \beta_1(\sigma) \\ \beta_2(\sigma) \end{bmatrix},$$

where $\alpha_i(\sigma), \beta_i(\sigma) \in \mathbb{Z}/n$ are such that

$$\alpha(\sigma) = \alpha_1(\sigma)v_1 + \alpha_2(\sigma)v_2,$$
$$\beta(\sigma) = \beta_1(\sigma)v_1 + \beta_2(\sigma)v_2.$$

2.5. Since the Weil pairing is skew-symmetric and non-degenerate, we have that $e_n(v_i, v_i) = 0$ for $i = 1, 2$, and $\zeta := e_n(v_1, v_2)$ is a primitive nth root of unity. With this designated root of unity, we may identify $\mu_n \cong (\mathbb{Z}/n)(1)$. Then for $v, w \in E[n]$, we have

$$e_n(v, w) = \zeta^{v^t Jw}, \qquad J := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

2.6. With the chosen basis v_1, v_2 of $E[n]$, we obtain a matrix representation $\rho_{E,n}$ of the Galois action on n-torsion:

$$\rho_{E,n} : G_{F,S} \to \mathrm{GL}_2(\mathbb{Z}/n).$$

In particular, the cocycle condition on α can be written as

$$\alpha(\sigma\tau) = \alpha(\sigma) + \rho_{E,n}(\sigma)\alpha(\tau)$$

and similarly for β. By a simple matrix computation, we note that

$$\rho_{E,n}(\sigma)^t J \rho_{E,n}(\sigma) = \det(\rho_{E,n}(\sigma))J.$$

On the other hand, Galois equivariance of the Weil pairing gives, for all $v, w \in E[n]$,

$$v^t \rho_{E,n}(\sigma)^t J \rho_{E,n}(\sigma) w = \chi_n(\sigma) v^t J w.$$

From this, we obtain the well-known identities

$$\det(\rho_{E,n}(\sigma)) = \chi_n(\sigma) \qquad \rho_{E,n}^t(\sigma) J = \chi_n(\sigma) J \rho_{E,n}(\sigma)^{-1}.$$

Since $\ker \rho_{E,n} \subseteq \ker \chi_n$, we have in particular that

$$\mu_n \subseteq F(\rho_{E,n}) = F(E[n]).$$

3. An Embedding Problem

In this section, we show how the triviality of the pairing given in the introduction is related to a Galois embedding problem.

3.1. Consider the group of block upper-triangular matrices of the form

$$\mathcal{B} := \begin{bmatrix} (\mathbb{Z}/n)^\times & * & * \\ & \mathrm{GL}_2(\mathbb{Z}/n) & * \\ & & 1 \end{bmatrix} \subset \mathrm{GL}_4(\mathbb{Z}/n).$$

The matrix

$$C := \begin{bmatrix} 1 & & & 1 \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

generates a normal (but not central) cyclic subgroup $\langle C \rangle \subset \mathcal{B}$ of order n, and the quotient $\mathcal{B}/\langle C \rangle$ can be thought of as "matrices modulo the upper right corner." More precisely, two matrices in $\mathcal{B}$ become identified in the quotient $\mathcal{B}/\langle C \rangle$ if and only if they are equal outside of the upper right corner.

3.2. For $\sigma \in G_{F,S}$, we denote a column vector

$$\widetilde{\alpha}(\sigma) = \chi_n(\sigma)\alpha(\sigma^{-1})^t J.$$

By the cocycle condition on α, we see that $\widetilde{\alpha}$ satisfies

$$\begin{aligned}
\widetilde{\alpha}(\sigma\tau) &= \chi_n(\sigma\tau)\alpha(\tau^{-1}\sigma^{-1})^t J \\
&= \chi_n(\sigma\tau)(\alpha(\tau^{-1})^t + \alpha(\sigma^{-1})^t \rho_{E,n}(\tau^{-1})^t)J \\
&= \chi_n(\sigma)\widetilde{\alpha}(\tau) + \chi_n(\sigma\tau)\alpha(\sigma^{-1})^t(\chi_n(\tau^{-1})J\rho_{E,n}(\tau)) \\
&= \chi_n(\sigma)\widetilde{\alpha}(\tau) + \chi_n(\sigma)\alpha(\sigma^{-1})^t J\rho_{E,n}(\tau) \\
&= \chi_n(\sigma)\widetilde{\alpha}(\tau) + \widetilde{\alpha}(\sigma)\rho_{E,n}(\tau).
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\zeta^{\widetilde{\alpha}(\sigma)\beta(\tau)} &= \zeta^{\chi_n(\sigma)\alpha(\sigma^{-1})^t J\beta(\tau)} \\
&= \sigma(e_n(\alpha(\sigma^{-1}), \beta(\tau))) \\
&= e_n(\sigma\alpha(\sigma^{-1}), \sigma\beta(\tau)) \\
&= e_n(\alpha(\sigma), \sigma\beta(\tau))^{-1} \\
&= -e_n(\alpha \cup \beta)(\sigma, \tau).
\end{aligned}$$

In other words, $(\sigma, \tau) \mapsto \zeta^{\widetilde{\alpha}(\sigma)\beta(\tau)}$ is a 2-cocycle representing $-e_n([\alpha] \cup [\beta]) \in H^2(G_{F,S}, \mu_n)$.

3.3. We now define a continuous function (written in block matrix form)

$$B_{\alpha,\beta} : G_{F,S} \to \mathcal{B}, \qquad B_{\alpha,\beta}(\sigma) = \begin{bmatrix} \chi_n(\sigma) & \widetilde{\alpha}(\sigma) & \\ & \rho_{E,n}(\sigma) & \beta(\sigma) \\ & & 1 \end{bmatrix}.$$

We verify that the composition $\overline{B}_{\alpha,\beta} : G_{F,S} \to \mathcal{B}/\langle C \rangle$ is a homomorphism: by block matrix multiplication,

$$\begin{aligned}
\overline{B}_{\alpha,\beta}(\sigma\tau) &= \begin{bmatrix} \chi_n(\sigma\tau) & \widetilde{\alpha}(\sigma\tau) & * \\ & \rho_{E,n}(\sigma\tau) & \beta(\sigma\tau) \\ & & 1 \end{bmatrix} \\
&= \begin{bmatrix} \chi_n(\sigma)\chi_n(\tau) & \chi_n(\sigma)\widetilde{\alpha}(\tau) + \widetilde{\alpha}(\sigma)\rho_{E,n}(\tau) & * \\ & \rho_{E,n}(\sigma)\rho_{E,n}(\tau) & \beta(\sigma) + \rho_{E,n}(\sigma)\beta(\tau) \\ & & 1 \end{bmatrix} \\
&= \begin{bmatrix} \chi_n(\sigma) & \widetilde{\alpha}(\sigma) & * \\ & \rho_{E,n}(\sigma) & \beta(\sigma) \\ & & 1 \end{bmatrix} \begin{bmatrix} \chi_n(\tau) & \widetilde{\alpha}(\tau) & * \\ & \rho_{E,n}(\tau) & \beta(\tau) \\ & & 1 \end{bmatrix} \\
&= \overline{B}_{\alpha,\beta}(\sigma)\overline{B}_{\alpha,\beta}(\tau) \in \mathcal{B}/\langle C \rangle.
\end{aligned}$$

3.4. However, there is a potential obstruction to lifting $\overline{B}_{\alpha,\beta}$ to a homomorphism $G_{F,S} \to \mathcal{B}$. Let $\gamma : G_{F,S} \to \mathbb{Z}/n$ be a continuous map, and let

$$B^{\gamma}_{\alpha,\beta} : G_{F,S} \to \mathcal{B}, \qquad B^{\gamma}_{\alpha,\beta}(\sigma) = \begin{bmatrix} \chi_n(\sigma) & \widetilde{\alpha}(\sigma) & \gamma(\sigma) \\ & \rho_{E,n}(\sigma) & \beta(\sigma) \\ & & 1 \end{bmatrix} \in \mathcal{B}.$$

We let a cochain $\zeta^\gamma : G_{F,S} \to \mu_n$ be defined by $\zeta^\gamma(\sigma) = \zeta^{\gamma(\sigma)}$. One checks $B^\gamma_{\alpha,\beta}$ is a homomorphism if and only if

$$\gamma(\sigma\tau) = \chi(\sigma)\gamma(\tau) + \widetilde{\alpha}(\sigma)\beta(\tau) + \gamma(\sigma),$$

if and only if

$$d(\zeta^\gamma)(\sigma,\tau) = e_n(\alpha \cup \beta).$$

This shows that $\overline{B}_{\alpha,\beta}$ lifts to a homomorphism $G_{F,S} \to \mathcal{B}$ if and only if $e_n(\alpha \cup \beta) \in Z^2(G_{F,S}, \mu_n)$ is a coboundary, if and only if $\langle [\alpha], [\beta] \rangle_{F,S,n} = 0$.

3.5. We make a few useful calculations. First, let $B^0_{\alpha,\beta} = B_{\alpha,\beta} : G_{F,S} \to \mathcal{B}$ be the function defined above. Then

$$B_{\alpha,\beta}(\sigma)B_{\alpha,\beta}(\tau) = C^{\widetilde{\alpha}(\sigma)\beta(\tau)}B_{\alpha,\beta}(\sigma\tau).$$

Also,

$$C^{\chi_n(\sigma)}B_{\alpha,\beta}(\sigma) = B_{\alpha,\beta}(\sigma)C,$$

so

$$B_{\alpha,\beta}(\sigma)CB_{\alpha,\beta}(\sigma)^{-1} = C^{\chi_n(\sigma)}.$$

3.6. **Matrix calculations.** Let $E_{i,j}$ be the matrix with a 1 in the (i,j) entry and zeros elsewhere. For $i = 1,2$, let $X_i = I + E_{1,i}$ and let $Y_i = I + E_{i,4}$. Then

$$[X_i, Y_j] = \begin{cases} C, & i = j, \\ 0, & i \neq j. \end{cases}$$

We define a subgroup

$$\mathcal{G} := \begin{bmatrix} 1 & * & * \\ & I & * \\ & & 1 \end{bmatrix} \subset \mathcal{B}.$$

The normal subgroup $\mathcal{N} \subset \mathcal{G}$ generated by $\{Y_1, Y_2\}$ is generated by $\{Y_1, Y_2, C\}$ and we have $\mathcal{N} \cong (\mathbb{Z}/n)^3$ as groups. Let $G \subset \mathcal{G}$ be the subgroup generated by $\{X_1, X_2\}$. Then $G \cong (\mathbb{Z}/n)^2$, and

$$\mathcal{G} \cong \mathcal{N} \rtimes G.$$

We consider $\mathcal{N}$ as a $(\mathbb{Z}/n)[G]$-module. Let G_i be the direct factor of G generated by X_i. We write the generator of G_i as g_i instead of X_i. Then we have an isomorphism of $(\mathbb{Z}/n)[G]$-modules

$$\mathcal{N} \cong \frac{(\mathbb{Z}/n)[G_1]m_1 \oplus (\mathbb{Z}/n)[G_2]m_2}{((g_1-1)m_1 - (g_2-1)m_2)}.$$

4. More on the Weil Pairing

We recall the definition of the Weil pairing as given in [Sil09].

We assume that $K(E[n]) = K$. Recall that we have chosen a $(\mathbb{Z}/n)$-basis $v_1, v_2 \in E[n]$ such that $e_n(v_1, v_2) = \zeta$ is a fixed primitive nth root of unity. Let $w_i \in E$ be such that $nw_i = v_i$. For $i \in \{1,2\}$, choose rational functions $f_i, g_i \in \overline{K}(E)^\times$ such that

$$\mathrm{div}(f_i) = n[v_i] - n[0], \qquad \mathrm{div}(g_i) = \sum_{z \in E[n]} [w_i + z] - [z].$$

We can choose $f_i, g_i \in K(E)^\times$ since their divisors are Galois invariant. One sees that $\mathrm{div}(g_i^n) = \mathrm{div}(f_i \circ [n])$, so we can rescale f so that

$$g_i^n = f_i \circ [n].$$

Note that since g_i is defined up to multiplication by $K^\times$, we have f_i is well-defined up to multiplication by $K^{\times n}$. Then by definition of the Weil pairing, we have

$$e_n(\alpha(\sigma), v_i) = e_n(\sigma\widetilde{x} - \widetilde{x}, v_i) = g_i(\sigma\widetilde{x})/g_i(\widetilde{x}) = \sigma(g_i(\widetilde{x}))/g_i(\widetilde{x}),$$

whenever $\widetilde{x}$ is not in the support of $\mathrm{div}(g_i)$. If $\widetilde{x} \in \mathrm{Supp}(\mathrm{div}(g_i))$, then either $\widetilde{x} \in E[n]$ or $\widetilde{x} - w_i \in E[n]$. In the former case, we have $x = n\widetilde{x} = 0$, and in the latter case, $x = n\widetilde{x} = nw_i = v_i$. So we assume that $x \notin \{0, v_1, v_2\}$, and similarly for y.

Now, we have

$$\begin{aligned}
\sigma(g_1(\widetilde{x}))/g_1(\widetilde{x}) &= e_n(\alpha(\sigma), v_1) \\
&= e_n(\alpha_1(\sigma)v_1 + \alpha_2(\sigma)v_2, v_1) \\
&= \zeta^{-\alpha_2(\sigma)}, \\
\sigma(g_2(\widetilde{x}))/g_2(\widetilde{x}) &= e_n(\alpha(\sigma), v_2) \\
&= e_n(\alpha_1(\sigma)v_1 + \alpha_2(\sigma)v_2, v_2) \\
&= \zeta^{\alpha_1(\sigma)}.
\end{aligned}$$

So α_1 is the Kummer character associated to $g_2(\widetilde{x})^n = f_2(x)$, and α_2 is the Kummer character associated to $-f_1(x)$. A similar computation works for y. Then

$$\begin{aligned}
e_n^*(\alpha \cup \beta)(\sigma, \tau) \otimes \zeta &= e_n(\alpha(\sigma), \beta(\tau)) \otimes \zeta \\
&= \zeta^{\alpha_1(\sigma)\beta_2(\tau) - \alpha_2(\sigma)\beta_1(\tau)} \otimes \zeta \\
&= (\zeta^{\alpha_1(\sigma)} \otimes \zeta^{\beta_2(\tau)})(\zeta^{\alpha_2(\sigma)} \otimes \zeta^{\beta_1(\tau)})^{-1} \\
\langle x, y\rangle &= (f_2(x), f_1(y))_S^{-1}(f_1(x), f_2(y))_S \\
&= (f_1(x), f_2(y))_S(f_1(y), f_2(x))_S,
\end{aligned}$$

where $(\cdot,\cdot)_S$ is the pairing of Sharifi–McCallum:

$$(K^\times \cap K_S^{\times n}) \times (K^\times \cap K_S^{\times n}) \to H^2(G_{K,S}, \mu_n^{\otimes 2}).$$

We have thus shown the following theorem:

Theorem 4.1. *There exists K-rational maps $f_1, f_2 : E \to \mathbb{P}^1$ with*

$$\mathrm{div}(f_i) = n[v_i] - n[0]$$

such that $f_i \circ [n] \in K(E)^{\times n}$ and for $x, y \neq 0, v_1, v_2$, we have

$$\langle x, y\rangle = (f_1(x), f_2(y))_S(f_1(y), f_2(x))_S.$$

Example 4.2. Consider the Legendre family of elliptic curves

$$E_t := \{y^2 = x(x-1)(x-t)\}, \qquad t \neq 0, 1.$$

We let $n = 2$. Let S be a set of primes containing those dividing $2t(1-t)$. We can choose $v_1 = (0,0)$, $v_2 = (1,0)$. Recall that the doubling map on x-coordinates is

$$x \mapsto \frac{(x^2-t)^2}{4y^2}.$$

Then we may take $f_1 = x$ and $f_2 = x - 1$, and

$$g_1 = \frac{x^2 - t}{2y}, \qquad g_2 = \frac{x^2 - 2x + t}{2y}.$$

Our pairing then takes

$$\langle (x_1, y_1), (x_2, y_2) \rangle = (x_1, x_2 - 1)_S (x_1 - 1, x_2)_S$$

However, the identity $(x, y - 1)_S + (x - 1, y)_S = 0$ does not hold for all $x, y \in K^\times$ (one can see this with Hilbert symbols). In fact, this identity does not even hold for the local pairings. We denote by $(\cdot, \cdot)_v$ the local pairings.

We do, however, have the following condition:

Lemma 4.3. *Let $(x_1, y_1), (x_2, y_2) \in E_t(K)$ such that $x_1, x_2 \neq 0, 1$. Then*

$$\langle (x_1, y_1), (x_2, y_2) \rangle_v = 1$$

for all places v of K.

Proof. We have

$$\langle (x_1, y_1), (x_2, y_2) \rangle_v = (x_1, x_2 - 1)_v (x_2, x_1 - 1)_v$$

where $(\cdot, \cdot)_v$ denotes the Hilbert symbol. Recall that the quadratic Hilbert symbol is bilinear and symmetric and satisfies, for $a, b \in K^\times - 1$,

$$(a, 1 - a)_v = 1, \qquad (a^2, b)_v = 1.$$

We verify several identities from these. For instance, for $a \neq b$,

$$\begin{aligned}
(a, -a)_v &= (1/a, -1/a)_v \\
&= (1/a, -1/a)_v (a, 1 - a)_v \\
&= (1/a, -1/a)_v (1/a, 1 - a)_v \\
&= (1/a, 1 - 1/a)_v \\
&= 1, \\
(a, b - a)_v (b, a - b)_v (a, b)_v &= (a, b - a)_v (b, a - b)_v (a, b)_v (a - b, b - a)_v \\
&= (a(a - b), b(b - a))_v \\
&= \left(\frac{a}{a - b}, \frac{-b}{a - b} \right)_v \\
&= \left(\frac{a}{a - b}, 1 - \frac{a}{a - b} \right)_v \\
&= 1.
\end{aligned}$$

In our setting, we have

$$\begin{aligned}
y_1^2 &= x_1(x_1 - 1)(x_1 - t) = x_1^2(x_1 - 1) - x_1(x_1 - 1)t, \\
y_2^2 &= x_2(x_2 - 1)(x_2 - t) = x_2^2(x_2 - 1) - x_2(x_2 - 1)t.
\end{aligned}$$

Taking a linear combination of these equations yields

$$x_2(x_2 - 1)y_1^2 - x_1(x_1 - 1)y_2^2 = x_1 x_2 (x_1 - x_2)(x_1 - 1)(x_2 - 1).$$

Letting $Y_i = (x_1x_2(x_1-1)(x_2-1)(x_1-x_2))^2$ for $i = 1, 2$, we have

$$x_1(x_1-1)(x_1-x_2)Y_1^2 + x_2(x_2-1)(x_2-x_1)Y_2^2 = 1.$$

This implies that

$$\begin{aligned}
1 &= (x_1(x_1-1)(x_1-x_2), x_2(x_2-1)(x_2-x_1))_v \\
&= (x_1,x_2)_v(x_1,x_2-1)_v(x_1,x_2-x_1)_v \\
&\quad \cdot (x_1-1,x_2)_v(x_1-1,x_2-1)_v(x_1-1,x_2-x_1)_v \\
&\quad \cdot (x_1-x_2,x_2)_v(x_1-x_2,x_2-1)_v(x_1-x_2,x_2-x_1)_v \\
&= (x_1,x_2-1)_v(x_2,x_1-1)_v(x_1-x_2,x_2-x_1)_v \\
&\quad \cdot (x_1,x_2)_v(x_1,x_2-x_1)_v(x_2,x_1-x_2)_v \\
&\quad \cdot (x_1-1,x_2-x_1)_v(x_2-1,x_1-x_2)_v(x_1-1,x_2-1)_v \\
&= (x_1,x_2-1)_v(x_2,x_1-1)_v \cdot 1 \cdot 1 \cdot 1 \\
&= \langle (x_1,y_1),(x_2,y_2)\rangle_v.
\end{aligned}$$

□

We also wish to $\langle v_1, v_2\rangle$, so we derive an alternate formula in this particular case. Let $f_3, g_3 \in K(E)^\times$ correspond to v_1+v_2 as above. Then

$$\sigma(g_3(\widetilde{x}))/g_3(\widetilde{x}) = e_n(\alpha(\sigma), v_1+v_2) = \zeta^{\alpha_1(\sigma)-\alpha_2(\sigma)}.$$

This formula applies for $x \neq 0, v_1+v_2$. For $x \neq v_2$, we have

$$\sigma(g_2(\widetilde{x}))/g_2(\widetilde{x}) = e_n(\alpha(\sigma), v_2) = \zeta^{\alpha_1(\sigma)}.$$

So ζ^{α_1} is the Kummer character associated to $f_2(x)$.

$$\zeta^{\alpha_2(\sigma)} = \zeta^{\alpha_1(\sigma)}\zeta^{\alpha_2(\sigma)-\alpha_1(\sigma)} = \frac{\sigma(g_2(\widetilde{x}))}{g_2(\widetilde{x})} \cdot \frac{g_3(\widetilde{x})}{\sigma(g_3(\widetilde{x}))}.$$

So ζ^{α_2} is the Kummer character associated to $f_2(x)/f_3(x)$. For $y \neq v_1$, we have

$$\tau(g_1(\widetilde{y}))/g_1(\widetilde{y}) = e_n(\beta(\tau), v_1) = \zeta^{-\beta_2(\tau)}.$$

So ζ^{β_2} is the Kummer character associated to $1/f_1(y)$. Furthermore,

$$\zeta^{\beta_1(\tau)} = \zeta^{\beta_1(\tau)-\beta_2(\tau)}\zeta^{\beta_2(\tau)} = \frac{\tau(g_3(\widetilde{y}))}{g_3(\widetilde{y})}\frac{g_1(\widetilde{y}))}{\tau(g_1(\widetilde{y}))}.$$

So ζ^{β_1} is the Kummer character associated to $f_3(y)/f_1(y)$. So for $x = v_1$ and $y = v_2$, we have

$$\begin{aligned}
e_n^*(\alpha \cup \beta)(\sigma,\tau) \otimes \zeta &= (\zeta^{\alpha_1(\sigma)} \otimes \zeta^{\beta_2(\tau)})(\zeta^{\alpha_2(\sigma)} \otimes \zeta^{\beta_1(\tau)})^{-1}, \\
\langle v_1, v_2\rangle \otimes \zeta &= (f_2(v_1), f_1(v_2)^{-1})_S(f_2(v_1)f_3(v_1)^{-1}, f_3(v_2)f_1(v_2)^{-1})_S^{-1} \\
&= (f_2(v_1), f_1(v_2)^{-1})_S(f_2(v_1)f_3(v_1)^{-1}, f_1(v_2)f_3(v_2)^{-1})_S \\
&= (f_3(v_1), f_3(v_2))_S(f_1(v_2), f_3(v_1))_S(f_2(v_1), f_3(v_2))_S^{-1}.
\end{aligned}$$

In the Legendre elliptic curve case, this says

$$\langle (0,0),(1,0)\rangle = (-t, 1-t)_S(1,-t)_S(-1,1-t)_S = (t,1-t)_S = 0$$

since the primes dividing $t(1-t)$ are contained in S.

5. Local Vanishing

In this section, we prove that the pairing

$$E(K) \times E(K) \to H^2(G_{K,S}, \mu_n)$$

always has image in the image of

$$\mathrm{Cl}_{K,S} / n \,\mathrm{Cl}_{K,S} \to H^2(G_{K,S}, \mu_n).$$

Recall the exact sequence

$$0 \to \mathrm{Cl}_{K,S} / n \,\mathrm{Cl}_{K,S} \to H^2(G_{K,S}, \mu_n) \to \mathrm{Br}_S(K)[n] \to 0.$$

For $a, b \in K^\times / K^{\times n}$, we recall that the Kummer map followed by the cup product gives us the element $(a, b)_S \in H^2(G_{K,S}, \mu_n)$. We denote its image in $\mathrm{Br}_S(K)$ by $(a, b)_K$. This is the *norm-residue symbol*.

Recall also that we have maps

$$f_1, f_2 : E(K) \to (K^\times \cap K_S^{\times n})/K^{\times n}$$

such that for $P, Q \in E(K)$,

$$\langle P, Q \rangle = (f_1(P), f_2(Q))_S (f_1(Q), f_2(P))_S.$$

The *period-index obstruction* is a map

$$\Delta : H^1(G_K, E[n]) \to \mathrm{Br}(K)$$

that vanishes on the image of the Kummer map by [CS10, §2.2]. We have an isomorphism $H^1(G_K, E[n]) \cong (K^\times / K^{\times n})^2$ such that the Kummer map $\kappa : E(K)/n \to H^1(G_K, E[n])$ becomes identified with the map $P \mapsto (f_1(P), f_2(P))$.

Proposition 5.1. *There exists $C_1, C_2 \in K^\times / K^{\times n}$ such that for all $a, b \in K^\times / K^{\times n}$,*

$$\Delta(a, b) = (C_1 a, C_2 b)_K - (C_1, C_2)_K.$$

Proof. See [Cla05, Thm 6]. □

Combined with the vanishing of Δ on the image of the Kummer map, we have the following:

Proposition 5.2. *For all $P, Q \in E(K)$, we have*

$$\langle P, Q \rangle \in \mathrm{Cl}_{K,S} / n.$$

Proof. It suffices to show that

$$(f_1(P), f_2(Q))_K + (f_1(Q), f_2(P))_K = 0.$$

From Proposition 5.1 and vanishing of Δ on the image of κ, we have

$$\begin{aligned}(f_1(P), f_2(P))_K &= (C_1 f_1(P), C_2 f_2(P))_K - (C_1, C_2)_K - (C_1, f_2(P))_K - (f_1(P), C_2)_K \\ &= \Delta(\kappa(P)) + (f_2(P), C_1)_K + (C_2, f_1(P))_K \\ &= 0 + (f_2(P), C_1)_K + (C_2, f_1(P))_K.\end{aligned}$$

We have

$$\begin{aligned}
(f_1(P), f_2(Q))_K + (f_1(Q), f_2(P))_K &= (f_1(P)f_1(Q), f_2(P)f_2(Q))_K - (f_1(P), f_2(P))_K \\
&\quad - (f_1(Q), f_2(Q))_K \\
&= (f_1(P+Q), f_2(P+Q))_K - (f_1(P), f_2(P))_K \\
&\quad - (f_1(Q), f_2(Q))_K \\
&= (f_2(P+Q), C_1)_K + (C_2, f_1(P+Q))_K \\
&\quad - (f_2(P), C_1)_K + (C_2, f_1(P))_K \\
&\quad - (f_2(Q), C_1)_K + (C_2, f_1(Q))_K \\
&= 0.
\end{aligned}$$

□

6. A formula in the Legendre case

As above, let $E = \{y^2 = x(x-1)(x-t)\}$ be a Legendre elliptic curve. Let $(x_1, y_1), (x_2, y_2) \in E(K)$. Sharifi notes that

$$\begin{aligned}
(x_1, x_2 - 1)_S + (x_2, x_1 - 1)_S &= \left(x_1, \frac{x_2 - 1}{1 - x_1}\right)_S + \left(x_2, \frac{x_1 - 1}{1 - x_2}\right)_S + (x_1, 1 - x_1)_S + (x_2, 1 - x_2)_S \\
&= \left(\frac{x_1}{x_2}, \frac{x_2 - 1}{1 - x_1}\right)_S + (x_1, 1 - x_1)_S + (x_2, 1 - x_2)_S.
\end{aligned}$$

The latter two terms vanish locally, so the first term must also vanish locally. We can then apply the Sharifi–McCallum formula.

Lemma 6.1. *There is an isomorphism*

$$\Phi_K := \Phi_{K,S} := \Phi_{K,S,n} : (K^\times \cap K_S^{\times n})/O_{K,S}^\times K^{\times n} \to \mathrm{Cl}_{K,S}[n]$$

such that if $I \subset O_{K,S}$ is an ideal with $I^n = aO_{K,S}$, then

$$\Phi_{K,S}(a) = [I].$$

Proof. The Kummer sequence

$$1 \to \mu_n \to O_S^\times \xrightarrow{n} O_S^\times \to 1$$

gives an exact sequence

$$1 \to O_{K,S}^\times/O_{K,S}^{\times n} \to H^1(G_{K,S}, \mu_n) \to \mathrm{Cl}_{K,S}[n] \to 0.$$

We have a commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & O_{K,S}^\times/O_{K,S}^{\times n} \arrow[r] \arrow[d] & H^1(G_{K,S}, \mu_n) \arrow[r] \arrow[d, "="] & \mathrm{Cl}_{K,S}[n] \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & (K^\times \cap K_S^{\times n})/K^{\times n} \arrow[r] & H^1(G_{K,S}, \mu_n) \arrow[r] & 0 &
\end{tikzcd}$$

Applying the snake lemma will give the desired isomorphism $\Phi_{K,S}$. Given $[I] \in \mathrm{Cl}_{K,S}[n]$, recall that we lift to $H^1(G_{K,S}, \mu_n)$ as follows: we write $IO_S = \alpha O_S$ for some $\alpha \in O_S$. The cocycle $G_{K,S} \to O_S^\times$ given by $\sigma \mapsto \sigma\alpha/\alpha$ has class in $H^1(G_{K,S}, O_S^\times)[n]$ corresponding to

$[I] \in \mathrm{Cl}_{K,S}$. In particular, if we write $I^n = aO_{K,S}$, then $\alpha^n O_S = aO_S$, so there exists $\epsilon_0 \in O_S^\times$ such that $\alpha^n = a\epsilon_0$. Then for $\sigma \in G_{K,S}$, we have

$$(\sigma\alpha/\alpha)^n = \sigma\alpha^n/\alpha^n = \sigma\epsilon_0/\epsilon_0.$$

Since the nth power map $O_S^\times \xrightarrow{n} O_S^\times$ is surjective, we may find $\epsilon \in O_S^\times$ such that $\epsilon^n = \epsilon_0$. Then $\sqrt[n]{a} := \alpha/\epsilon \in K_S^\times$ is an nth root of a, and the cocycle $\sigma \mapsto \sigma\alpha/\alpha$ is cohomologous with $\sigma \mapsto \sigma \sqrt[n]{a}/\sqrt[n]{a}$, which is the image of a in $H^1(G_{K,S}, \mu_n)$. It follows that $\Phi_{K,S}(a) = [I]$. □

Lemma 6.2. *Let L/K be a finite Galois extension. Then Φ_L is Galois equivariant.*

Proof. Let $\sigma \in G_{L/K}$, let $[I] \in \mathrm{Cl}_{L,S}$, and let $b \in L^\times \cap L_S^{\times n}$ be such that $I^n = bO_{L,S}$. Then $\Phi_L(b) = [I]$. Note also that

$$(I^\sigma)^n = \sigma(I^n) = \sigma b O_{L,S},$$

so

$$\Phi_L(\sigma b) = \sigma[I] = \sigma\Phi_L(b).$$ □

We return to the case $n = 2$.

Proposition 6.3. *Let $a, 1-a \in K^\times \cap K_S^{\times 2}$. Then*

$$(a, 1-a)_S = [\mathfrak{a}] \in \mathrm{Cl}_{K,S}/2$$

where $\mathfrak{a}^2$ is the fractional ideal $(1, a)O_{K,S}$.

Proof. Let $L = K(\sqrt{a})$, and let $\gamma = 1 - \sqrt{a} \in L$. Let $\mathfrak{b} \subset K$ be a fractional ideal such that

$$(1-a)O_{K,S} = \mathfrak{b}^2,$$

and let $\mathfrak{c}$ be a fractional ideal of L such that

$$\gamma O_{L,S} = \mathfrak{b}\mathfrak{c}^{1-\sigma}.$$

By the formula of McCallum–Sharifi, we have

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

Now let $\mathfrak{p}$ be a prime of K not in S and $\mathfrak{P} \subset L$ a prime above $\mathfrak{p}$. In particular, $\mathfrak{p}$ is unramified in L and does not divide 2. Then

$$v_\mathfrak{p}(\mathfrak{b}\mathfrak{c}^{1+\sigma}) = v_\mathfrak{P}(\mathfrak{b}\mathfrak{c}^{1+\sigma}) \equiv v_\mathfrak{P}(\mathfrak{b}\mathfrak{c}^{1-\sigma}) = v_\mathfrak{P}(\gamma) \pmod 2.$$

Note that this implies that

$$v_\mathfrak{P}(\gamma) \equiv v_\mathfrak{P}(\gamma^\sigma) \pmod 2.$$

The minimal polynomial of γ over K is $x^2 - 2x + 1 - a$. Let $\mathfrak{a}$ be the fractional ideal such that $\mathfrak{a}^2 = (1, a)O_{K,S} = (1, 1-a)O_{K,S}$. Then by considering the Newton polygon of $x^2 - 2x + 1 - a$ at $\mathfrak{P}$.

$$\begin{aligned} v_\mathfrak{P}(\gamma) &\equiv \min\{v_\mathfrak{P}(\gamma), v_\mathfrak{P}(\gamma^\sigma)\} \pmod 2 \\ &= \min\left\{v_\mathfrak{P}(2), \frac{1}{2}v_\mathfrak{P}(1-a)\right\} \\ &= \frac{1}{2}\min\{0, v_\mathfrak{p}(1-a)\} \\ &= \frac{1}{2}v_\mathfrak{p}((1, 1-a)) \\ &= v_\mathfrak{p}(\mathfrak{a}). \end{aligned}$$

So as elements of $\mathrm{Cl}_{K,S}/2$, we have $[\mathfrak{b}\mathfrak{c}^{1+\sigma}] = [\mathfrak{a}]$. $\square$

The more general proposition is as follows:

Proposition 6.4. *Let $n \geq 2$. Let $a, 1-a \in K^\times \cap K_S^{\times n}$. If n is odd, then $(a, 1-a)_S = 0$. If n is even, then $(a, 1-a)_S = [\mathfrak{a}]$, where $\mathfrak{a}^2 = (a, 1-a)O_{K,S}$ as fractional ideals.*

Proof. Let $d = [L : K]$. Let σ be a generator for $G_{L/K}$, and let ζ be a primitive nth root of unity such that $\sigma \sqrt[n]{a} = \zeta^{n/d} \sqrt[n]{a}$. We note that

$$1 - a = \prod_{i=0}^{n-1}(1 - \zeta^i \sqrt[n]{a}) = \prod_{i=0}^{d-1} \prod_{j=0}^{n/d-1} (1 - \zeta^{j+(n/d)i} \sqrt[n]{a}) = N_{L/K}\left(\prod_{j=0}^{n/d-1} (1 - \zeta^j \sqrt[n]{a})\right).$$

Accordingly, we let $\gamma = \prod_{j=0}^{n/d-1}(1 - \zeta^j \sqrt[n]{a})$.

Let $\mathfrak{c} \subset L$ be a fractional $O_{L,S}$ ideal such that

$$\gamma O_{L,S} = \mathfrak{c}^{1-\sigma}\mathfrak{b}^{n/d}.$$

We have

$$\mathfrak{c}^\sigma = \mathfrak{c}\mathfrak{b}^{n/d}\gamma^{-1}.$$

Inductively, this implies that

$$\mathfrak{c}^{\sigma^i} = \mathfrak{c}\mathfrak{b}^{ni/d} \prod_{j=1}^{i} \gamma^{-\sigma^{j-1}}$$

Now suppose that n is odd. Then $(a, 1-a)_S = [N_{L/K}\mathfrak{c}] \otimes \zeta^{n/d}$. Let $\mathfrak{P}$ be a prime of L over a prime $\mathfrak{p}$ of K not in S. In particular, $\mathfrak{p}$ does not divide n and $\mathfrak{P}$ is unramified over $\mathfrak{p}$. Then

$$\begin{aligned}
v_\mathfrak{p}(N_{L/K}\mathfrak{c}) &= v_\mathfrak{P}(N_{L/K}\mathfrak{c}) \\
&= \sum_{i=1}^{d} v_\mathfrak{P}(\mathfrak{c}^{\sigma^i}) \\
&= d v_\mathfrak{P}(\mathfrak{c}) + \sum_{i=1}^{d} \frac{ni}{d} v_\mathfrak{P}(\mathfrak{b}) - \sum_{i=1}^{d}\sum_{j=1}^{i} v_\mathfrak{P}(\gamma^{\sigma^{j-1}}) \\
&= d v_\mathfrak{P}(\mathfrak{c}) + \frac{n(d+1)}{2} v_\mathfrak{P}(\mathfrak{b}) - \sum_{j=1}^{d}\sum_{i=j}^{d} v_\mathfrak{P}(\gamma^{\sigma^{j-1}}) \\
&\equiv d v_\mathfrak{P}(\mathfrak{c}) + \sum_{j=1}^{d} j v_\mathfrak{P}(\gamma^{\sigma^{j-1}}) - (d+1)\sum_{j=1}^{d} v_\mathfrak{P}(\gamma^{\sigma^{j-1}}) \pmod{n} \\
&\equiv d v_\mathfrak{P}(\mathfrak{c}) + \sum_{i=1}^{d} i \sum_{j=0}^{n/d-1} v_\mathfrak{P}(1 - \zeta^{j+(n/d)(i-1)} \sqrt[n]{a}).
\end{aligned}$$

Suppose further that $v_\mathfrak{p}(1-a) \leq 0$. By considering the Newton polygon of $(1-x)^n - a$, we have that

$$v_\mathfrak{P}(1 - \zeta^{j+(n/d)(i-1)} \sqrt[n]{a}) = \frac{1}{n} v_\mathfrak{p}(1-a).$$

Then

$$v_{\mathfrak{p}}(N_{L/K}\mathfrak{c}) \equiv d v_{\mathfrak{P}}(\mathfrak{c}) + \frac{(d+1)}{2} v_{\mathfrak{p}}(1-a) \equiv 0 \pmod{d}.$$

If $v_{\mathfrak{p}}(1-a) > 0$, then similar Newton polygon considerations show that $v_{\mathfrak{P}}(1-\zeta^k \sqrt[n]{a})$ is divisible by d for all k. So

$$(a, 1-a)_S = [N_{L/K}\mathfrak{c}] \otimes \zeta^{n/d} = 0.$$

Now suppose that n is even. Then

$$(a, 1-a) = ([N_{L/K}\mathfrak{c}] + \frac{n}{2}[\mathfrak{b}]) \otimes \zeta^{n/d}.$$

A similar calculation to the above yields

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{b}^{n/2} N_{L/K}\mathfrak{c}) &= v_{\mathfrak{P}}(\mathfrak{b}^{n/2} N_{L/K}\mathfrak{c}) \\ &\equiv \frac{n}{2} v_{\mathfrak{P}}(\mathfrak{b}) + \frac{n(d+1)}{2} v_{\mathfrak{P}}(\mathfrak{b}) + \sum_{i=1}^{d} i \sum_{j=0}^{n/d-1} v_{\mathfrak{P}}(1-\zeta^{j+(n/d)(i-1)} \sqrt[n]{a}) \pmod{d} \\ &= \frac{d+2}{2} v_{\mathfrak{p}}(1-a) + \sum_{i=1}^{d} i \sum_{j=0}^{n/d-1} v_{\mathfrak{P}}(1-\zeta^{j+(n/d)(i-1)} \sqrt[n]{a}) \pmod{d}. \end{aligned}$$

If $v_{\mathfrak{p}}(1-a) < 0$, then

$$v_{\mathfrak{p}}(\mathfrak{b}^{n/2} N_{L/K}\mathfrak{c}) \equiv \frac{d+2}{2} v_{\mathfrak{p}}(1-a) + \frac{d+1}{2} v_{\mathfrak{p}}(1-a) \equiv \frac{1}{2} v_{\mathfrak{p}}(1-a) \pmod{d}.$$

Otherwise,

$$v_{\mathfrak{p}}(\mathfrak{b}^{n/2} N_{L/K}\mathfrak{c}) \equiv (d+2)\frac{v_{\mathfrak{p}}(1-a)}{2} \equiv v_{\mathfrak{p}}(1-a) \equiv 0 \pmod{d}.$$

So

$$v_{\mathfrak{p}}(\mathfrak{b}^{n/2} N_{L/K}\mathfrak{c}) \equiv \frac{1}{2} \min\{0, v_{\mathfrak{p}}(1-a)\} = v_{\mathfrak{p}}(\mathfrak{a}) \pmod{d}.$$

□

References

[Cla05] Pete L. Clark. The period-index problem in WC-groups. I. Elliptic curves. *J. Number Theory*, 114(1):193–208, 2005.

[CS10] Pete L. Clark and Shahed Sharif. Period, index and potential. III. *Algebra Number Theory*, 4(2):151–174, 2010.

[MS03] William G. McCallum and Romyar T. Sharifi. A cup product in the Galois cohomology of number fields. *Duke Math. J.*, 120(2):269–310, 2003.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.