On Tate Local Duality

Mihran Papikian

1 Tate local duality

I will try to explain and prove all the statements in Section 7 of B. Gross "Kolyvagin's work on modular elliptic curves"

Let $\mathbf{F}_q$ be a finite field, and let g be its absolute Galois group. Hence $g \cong \widehat{\mathbf{Z}}$, topologically generated by the Frobenius automorphism. Let A be a topological $g-$module, i.e. for each $a \in A$ there is a positive integer n such that $Frob^n\ a = a$ (for us A will be either an elliptic curve or some torsion group). Thus the group A is the union of its subgroups A^{g_n}, the latter being g/g_n-module, where $g_n = n\widehat{\mathbf{Z}}$ is an open subgroup of index n. The cohomology groups of g with values in A are defined by the formula

$$H^s(g, A) = \varinjlim H^s(g/g_n, A^{g_n})$$

Theorem 1.1 *If A is a torsion group or a divisible group such that A^g is torsion, then*

$$H^s(g,A) = \begin{cases} A^g & s = 0, \\ A/(Frob - 1)A, & \textit{the largest quotient on which } g \textit{ acts trivially}, \\ 0 & s \geq 2. \end{cases}$$

Proof. Suppose first A is finite. Denote by $D := Frob - 1$ and $N_n := 1 + Frob + Frob^2 + \cdots + Frob^{n-1}$. Then a standart fact from homological algebra implies, since g/g_n is a cyclic group, that the following complex computes the cohomology groups of A^{g_n} as a g/g_n-module

$$0 \longrightarrow A^{g_n} \xrightarrow{D} A^{g_n} \xrightarrow{N_n} A^{g_n} \xrightarrow{D} A^{g_n} \xrightarrow{N_n} A^{g_n} \xrightarrow{D} A^{g_n} \xrightarrow{N_n} \cdots$$

More precisely, $H^0(g/g_n, A^{g_n}) = A^g$, $H^{2m}(g/g_n, A^{g_n}) = \ker\ (DA^{g_n})/N_nA^{g_n} = A^g/N_nA^{g_n}$, and $H^{2m-1}(g/g_n, A^{g_n}) = \ker\ (N_nA^{g_n})/DA^{g_n}$, where $m \geq 1$.

To compute $H^s(g, A)$ one has to know the connecting homomorphisms between $H^s(g/g_n, A^{g_n})$ and $H^s(g/g_{nm}, A^{g_{nm}})$ for an arbitrary m, which appear in the directed system $\varinjlim H^s(g/g_n, A^{g_n})$.

The connecting homomorphisms should make the following diagram commutative

$$\begin{array}{ccccccccccccccc} 0 & \longrightarrow & A^{g_n} & \xrightarrow{D} & A^{g_n} & \xrightarrow{N_n} & A^{g_n} & \xrightarrow{D} & A^{g_n} & \xrightarrow{N_n} & A^{g_n} & \xrightarrow{D} & A^{g_n} & \xrightarrow{N_n} & \cdots \\ & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m^2} & & \downarrow{\scriptstyle m^2} & & \\ 0 & \longrightarrow & A^{g_{nm}} & \xrightarrow{D} & A^{g_{nm}} & \xrightarrow{N_{nm}} & A^{g_{nm}} & \xrightarrow{D} & A^{g_{nm}} & \xrightarrow{N_{nm}} & A^{g_{nm}} & \xrightarrow{D} & A^{g_{nm}} & \xrightarrow{N_{nm}} & \cdots \end{array}$$

and it is easy to see that the first map on the left is isomorphism as $H^0(g/g_n, A^{g_n}) = A^g$ independent of n. For the diagram to commute the rest of the connecting homomorphisms should be multiplications by an appropriate power of m as marked, since for any $a \in A^{g_n} \quad N_{nm}a = m \cdot N_n a$. But then if m is a multiple of the order of A, these homomorphisms are zero, hence $\varinjlim H^s(g/g_n, A^{g_n}) = 0$ for $s \geq 2$.

If A is a torsion group, then $A = \varinjlim A_\alpha$, where A_α are finite and stable under g, whence $H^s(g, A) = \varinjlim H^s(g, A_\alpha) = 0$.

Finally, suppose A is divisible. If $n \geq 1$, denote by A_n the kernel of multiplication by n on A. The exact sequence (here we use divisibility)

$$0 \longrightarrow A_n \longrightarrow A \xrightarrow{n} A \longrightarrow 0$$

induces a long exact sequence of cohomology groups

$$\cdots \longrightarrow H^s(g, A_n) \longrightarrow H^s(g, A) \xrightarrow{n} H^s(g, A) \longrightarrow H^{s+1}(g, A_n) \longrightarrow \cdots$$

By the preceding argument $H^s(g, A_n) = H^{s+1}(g, A_n) = 0$. Hence multiplication by n is an isomorphism on $H^s(g, A)$ for any $n \geq 1$. But this is a torsion group, since it is a direct limit of torsion groups, so it must be zero.

Now to complete the proof of the proposition it remains to show that when A^g is torsion then any element of A is in the kernel of N_n for some n. Indeed, since A is a topological $g-$module for any $a \in A$, there is a positive integer n such that $Frob^n a = a$. This implies that $N_n a \in A^g$. Let m be the order of $N_n a$. Then $N_{nm}a = m \cdot N_n a = 0$.

It is also clear from the last argument that the condition of A^g being torsion is necessary for the first cohomology to have the given form, as if there is an element b in A^g of infinite order then $N_n b = n \cdot b$ is non-zero for any n. Ref. Serre - Local Fields, Ch XIII, 1, 2. □

From here on K is a local field, with ring of integers $\mathcal{O}$, maximal ideal π and finite residue field F of characteristic ℓ. Denote by G_K its absolute Galois group. We let E be an elliptic curve over K with good reduction over $\mathcal{O}$.

Let p be a prime, with $p \neq \ell$. Then E_p is a finite etale group scheme of rank p^2 over $\mathcal{O}$. We also will be denoting by $g = Gal(K^{un}/K)$ the Galois group of the maximal unramified extension of K, which is isomorphic to $Gal(F^{ab}/F)$. Let $\widetilde{E}(F)$ be the reduction of E then there is an exact sequence

$$0 \longrightarrow E^1(K) \longrightarrow E(K) \longrightarrow \widetilde{E}(F) \longrightarrow 0$$

where $E^1(K)$ can be expressed as the π-values of a certain formal group, it is pro-ℓ and multiplication by p is an isomorphism.

Apply snake lemma to the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E^1(K) & \longrightarrow & E(K) & \longrightarrow & \widetilde{E}(F) & \longrightarrow & 0 \\ & & \downarrow p & & \downarrow p & & \downarrow p & & \\ 0 & \longrightarrow & E^1(K) & \longrightarrow & E(K) & \longrightarrow & \widetilde{E}(F) & \longrightarrow & 0 \end{array}$$

Since the cokernel of the left map is 0 we have

$$E(K)/pE(K) \cong \widetilde{E}(F)/p\widetilde{E}(F) \tag{1}$$

From Kummer sequence

$$0 \longrightarrow \widetilde{E}_p \longrightarrow \widetilde{E}(F) \stackrel{p}{\longrightarrow} \widetilde{E}(F) \longrightarrow 0$$

get

$$0 \longrightarrow \widetilde{E}(F)/p\widetilde{E}(F) \longrightarrow H^1(g, \widetilde{E}_p) \longrightarrow H^1(g, \widetilde{E}) = \widetilde{E}/(Frob-1)\widetilde{E}$$

The last equality comes from (1.1).

$(Frob-1)$ has finite fibres and has Zariski-closed image (because $\widetilde{E}$ is complete) of dimension one (because fibres have dimension 0). Hence it is surjective as a morphism of algebraic varieties [1]. This implies that the last cohomology group vanishes (special case of Lang's theorem) and we obtain

$$E(K)/pE(K) \cong \widetilde{E}(F)/p\widetilde{E}(F) \cong H^1(g, \widetilde{E}_p) \cong H^1(g, E_p)$$

since p-torsion injects into $\widetilde{E}$.

Theorem 1.2 (Tate Local Duality) *For all i, $H^i(G_K, E_p)$ is finite, and there are alternating, non-degenerate pairings*

$$< \, , \, > \qquad H^i(G_K, E_p) \otimes H^{2-i}(G_K, E_p) \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

induced by cup product, Weil pairing and the invariant map of the Class Field Theory.

[1] This argument appears in the email of Peter Clark, as well as in a proof of the exactness of Kummer sequence for elliptic curves.

Remark $H^2(G_K, \mu_p) = \mathbf{Z}/p\mathbf{Z}$ from Kummer sequence

$$0 \longrightarrow \mu_p \longrightarrow (K^{al})^{\times} \xrightarrow{p} (K^{al})^{\times} \longrightarrow 0$$

by applying Hilbert 90, and that $H^2(G_K, (K^{al})^{\times}) = \mathbf{Q}/\mathbf{Z}$.

It is interesting to observe that Weil pairing is also a duality statement in disguise. Believe for a moment in the existence of cohomology theory for algebraic varieties which behaives like the singular cohomology in topology. Then the topological Poincare duality for a torus (our case) gives a perfect pairing of

$$H^1(E(\mathbf{C}), \mathbf{Z}/p\mathbf{Z}) \otimes H^1(E(\mathbf{C}), \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2(E(\mathbf{C}), \mathbf{Z}/p\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$$

and the same statement for etale cohomology (now E is a proper algebraic curve over algebraicaly closed field such as K^{al} and $\mathbf{Z}/p\mathbf{Z}$ is a locally constant sheaf on it) is

$$H^1_{et}(E, \mathbf{Z}/p\mathbf{Z}) \otimes H^1_{et}(E, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2_{et}(E, \mathbf{Z}/p\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$$

(the last equality follows e.g. from the comparison theorem: $H^i_{et}(E, \mathbf{Z}/p\mathbf{Z}) = H^i(E(\mathbf{C}), \mathbf{Z}/p\mathbf{Z})$). Yet another (non-trivial) theorem states that $H^1_{et}(E, \mathbf{Z}/p\mathbf{Z}) \cong Jac(E)_p = E_p$. Putting all together we have a non-degenerate, alternaiting pairing $E_p \times E_p \longrightarrow \mathbf{Z}/p\mathbf{Z}$. Unscrewing the map which goes into the algebraic version of Poincare duality, one essentially obtains the proof in Silverman, Ch III.

Proposition 1.3 *Under the Tate pairing $H^1(g, E_p)$ and $H^1(g, E_p)$ are orthogonal, i.e. the subspace $E(K)/pE(K) \cong H^1(g, E_p)$ is isotropic for the pairing $< \cdot\ ,\ \cdot >$.*

Proof. We have a commutative diagram

$$\begin{array}{ccc}
H^1(g, E_p) \otimes H^1(g, E_p) & \xrightarrow{inf \otimes inf} & H^1(G_K, E_p) \otimes H^1(G_K, E_p) \\
\downarrow & & \downarrow \\
H^2(g, E_p \otimes E_p) & & H^2(G_K, E_p \otimes E_p) \\
\downarrow & & \downarrow \\
H^2(g, \mathbf{Z}/p\mathbf{Z}) & \xrightarrow{inf} & H^2(G_K, \mathbf{Z}/p\mathbf{Z}) \\
 & & \downarrow \\
 & & \mathbf{Z}/p\mathbf{Z}
\end{array}$$

But $H^2(g, \mathbf{Z}/p\mathbf{Z}) = 0$ by (1.1), thus the claim. □

Theorem 1.4 (Restricted Tate Local Duality) *The pairing $< \cdot\,,\,\cdot >$ induces a non-degenerate pairing of $\mathbf{Z}/p\mathbf{Z}$-vector spaces (of dimension ≤ 2)*

$$< \cdot\,,\,\cdot > : \quad E(K)/pE(K) \otimes H^1(G_K, E)_p \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

Proof. The absolute Galois group G_K surjects onto g and we have a natural exact sequence

$$0 \longrightarrow \mathcal{I} \longrightarrow G_K \longrightarrow g \longrightarrow 0$$

where $\mathcal{I}$ is the inertia subgroup.

Take the Inf-Res of the above sequence

$$0 \longrightarrow H^1(g, E_p^{\mathcal{I}}) \longrightarrow H^1(G_K, E_p) \longrightarrow H^1(\mathcal{I}, E_p)^g \longrightarrow H^2(g, E_p^{\mathcal{I}})$$

The last group is zero by (1.1) and E_p is stable under $\mathcal{I}$ as E has a good reduction. So

$$0 \longrightarrow H^1(g, E_p) \longrightarrow H^1(G_K, E_p) \longrightarrow H^1(\mathcal{I}, E_p)^g \longrightarrow 0$$

Kummer sequence yields

$$0 \longrightarrow E(K)/pE(K) \longrightarrow H^1(G_K, E_p) \longrightarrow H^1(G_K, E)_p \longrightarrow 0\ .$$

In particular,

$$H^1(\mathcal{I}, E_p)^g \cong H^1(G_K, E)_p.$$

We want to analize $H^1(\mathcal{I}, E_p)$ to see which portion of it is non-trivial.

Let Δ be the image of $\mathcal{I}$ in the tamely ramified part of G_K, i.e.

$$0 \longrightarrow \mathcal{P} \longrightarrow \mathcal{I} \longrightarrow \Delta \longrightarrow 0$$

where $\mathcal{P}$ is the wild-ramification group which is a rather complicated group. On the other hand it is well-known that $\Delta \cong \prod_{s\neq\ell} \mathbf{Z}_s(1)$.

The Inf-Res of the last sequence gives

$$0 \longrightarrow H^1(\Delta, E_p) \longrightarrow H^1(\mathcal{I}, E_p) \longrightarrow H^1(\mathcal{P}, E_p)^{\Delta}\ .$$

But $\mathcal{P}$ is pro-ℓ, hence

$$H^1(\mathcal{P}, E_p) = \text{Hom }(\mathcal{P}, E_p) = 0.$$

Finally,

$$H^1(\mathcal{I}, E_p)^g = H^1(\Delta, E_p)^g = \text{Hom }(\Delta, E_p)^g = \text{Hom }(\prod_{s\neq\ell} \mathbf{Z}_s(1), E_p)^g =$$

$$= \text{Hom }(\mathbf{Z}_p(1), E_p)^g = \text{Hom }(\varprojlim \mu_{p^n}, E_p)^g = \text{Hom }(\mu_p, E_p)^g.$$

Weil pairing is non-degenerate and Galois invariant, so the last group has the same dimension as $E(K)_p$.

From (1.1) $H^1(g, E_p) = E_p/(Frob - 1)E_p = \widetilde{E}(F)_p = E(K)_p$. On the other hand $H^1(g, E_p) = E(K)/pE(K)$. Together

$$E(K)/pE(K) = E(K)_p.$$

(If the last statement seems bizarre to you keep in mind that we are working over complete field).

Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (H^1(G_K, E)_p)^* & \longrightarrow & (H^1(G_K, E_p))^* & \longrightarrow & (E(K)/pE(K))^* & \longrightarrow & 0 \\ & & \uparrow & & \uparrow \cong & & \uparrow & & \\ 0 & \longrightarrow & E(K)/pE(K) & \longrightarrow & H^1(G_K, E_p) & \longrightarrow & H^1(G_K, E)_p & \longrightarrow & 0 \end{array}$$

Where the upper row is the Cartier dual of the lower row, and the middle map is an isomorphism as Tate Local Duality is a perfect pairing.

Left map is injective since $E(K)/pE(K)$ is isotropic. But we saw that $\dim(E(K)/pE(K)) = \dim(E(K)_p) = \dim H^1(\mathcal{I}, E_p)^g = \dim H^1(G_K, E)_p$. Hence it is an isomorphism. Similarly, for the right map.

Finally,

$$E(K)/pE(K) \otimes H^1(G_K, E)_p \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

is a non-degenerate pairing. □

2 Hilbert symbols and Kolyvagin's formula

We are still assuming that K is a local field with uniformizer π, and residue field F of characteristic ℓ. Let U_K be the group of units in $K^\times$, i.e.

$$U_K = \{x \in K^\times \mid \text{val }(x) = 0\}.$$

Then $K^\times = U_K \times \pi^{\mathbf{Z}}$. Fix ξ, primitive (|F| - 1) - st root of unity in K (which exists e.g. by Hensels lemma), and $\zeta = \xi^{(|F|-1)/p}$, primitive p^{th} root of 1. Recall the main theorems of local class field theory

Theorem 2.1 (Local class field theory) *For any nonarchimedean local field, there is a unique homomorphism, the* **local Artin map***,*

$$\theta_K \;:\; K^\times \longrightarrow Gal(K^{ab}/K)$$

with the following properties:

(a) *For any prime element* π *of* K *and any finite unramified extension* L *of* K, $\theta_K(\pi) \mid L = Frob_{L/K}$

(b) *For any finite abelian extension* L *of* K, $Nm_{L/K}(L^\times)$ *is contained in the kernel of* $a \to \theta_K(a) \mid L$, *and* θ_K *induces an isomorphism*

$$\theta_{L/K} \; : \; K^\times / Nm_{L/K}(L^\times) \longrightarrow Gal(L/K)$$

Moreover

(c) *A subgroup* N *of* $K^\times$ *is of the form* $Nm_{L/K}(L^\times)$ *for some finite abelian extension* L *of* K *iff it is of finite index and open.*

From this theorem it is easy to see that for any unramified extension U_K is in the image of the norm map ($u\pi$ and π are both uniformizers $\Longrightarrow \theta(u) = \theta(u\pi) \cdot \theta(\pi^{-1}) = Frob \cdot Frob^{-1} = 1$), and for totally ramified extensions π is in the image of norm.

From now on we assume that E_p is rational over K, which by Weil pairing implies that K contains p^{th} root ζ of 1.

Taking cohomology of the Kummer sequence yields

$$H^1(G_K, \mu_p) \cong K^\times / K^{\times p}$$

$$H^2(G_K, \mu_p) \cong \mathbf{Z}/p\mathbf{Z}$$

The cup-product pairing

$$H^2(G_K, \mu_p) \otimes H^0(G_K, \mu_p) \longrightarrow H^2(G_K, \mu_p \otimes \mu_p)$$

defines an isomorphism

$$H^2(G_K, \mu_p) \otimes \mu_p \longrightarrow H^2(G_K, \mu_p \otimes \mu_p)$$

Hence

$$H^2(G_K, \mu_p \otimes \mu_p) \cong (\mathbf{Z}/p\mathbf{Z}) \otimes \mu_p \cong \mu_p$$

The cup-product for

$$H^1(G_K, \mu_p) \otimes H^1(G_K, \mu_p) \longrightarrow H^2(G_K, \mu_p \otimes \mu_p)$$

becomes a pairing

$$a, b \longrightarrow (a, b) : K^\times / K^{\times p} \times K^\times / K^{\times p} \longrightarrow \mu_p$$

This pairing is called the **Hilbert symbol**.

The first step in proving Kolyvagin's formula for Tate's pairing (see below) is to understand the Hilbert symbol.

Theorem 2.2 *The Hilbert symbol has the following properties*

(a) It is bi-multiplicative, i.e.

$$(aa', b) = (a, b)\ (a', b)$$

$$(a, bb') = (a, b)\ (a, b')$$

(b) It is skew-symmetric, i.e.

$$(b, a) = (a, b)^{-1}$$

(c) It is nondegenerate, i.e.

$$(a, b) = 1 \textit{ for all } b \in K^{\times}/K^{\times p} \Longrightarrow a \in K^{\times p}$$

$$(a, b) = 1 \textit{ for all } a \in K^{\times}/K^{\times p} \Longrightarrow b \in K^{\times p}$$

(d) (a, b) = 1 if and only if b is a norm from $K[a^{1/p}]$

Remark (a) and (b) follow from definition of cup-product, and (c) is a form of Tate local duality, (d) is harder.

Theorem 2.3 *The Hilbert symbol is related to the local Artin map by the formula*

$$\theta(b)(a^{1/p}) = (a, b)a^{1/p}$$

Note that Galois theory tells us that, for any $\tau \in Gal(K[a^{1/p}]/K)$, $\tau a^{1/p} = \zeta' a^{1/p}$ for some p^{th} root of one ζ', and so the point of the formula is that roots of 1 are the same.

Let G_p be the Galois group of the largest abelian extension of K of exponent p. Then one of the consequences of local class field theory is that

$$\theta : G_p \cong K^{\times}/K^{\times p}$$

(this statement is also known as Kummer theory).

If $b \in K^{\times}$, define $\phi_b \in$ Hom (G_p, μ_p) by

$$\phi_b(g) = \frac{g(b^{1/p})}{b^{1/p}}$$

Then we can rewrite (2.3) as

$$(a,b) = \phi_b(\theta(a)) \tag{2}$$

Define homomorphisms $\overline{\phi}_a, \overline{\phi}_b \ : \quad G_p \longrightarrow \mathbf{Z}/p\mathbf{Z}$ such that

$$\zeta^{\overline{\phi}_a(g)} = \phi_a(g) \quad , \quad \zeta^{\overline{\phi}_b(g)} = \phi_b(g).$$

Define an element of $H^2(G_p, \mu_p)$ by the bilinear form

$$B_{a,b}(g_1, g_2) = \zeta^{\overline{\phi}_a(g)\ \overline{\phi}_b(g)}.$$

To see that this is a 2-cocycle one has to check that

$$B_{a,b}(g_1, g_2) \cdot B_{a,b}(g_1\ g_2, g_3) = (g_1 \cdot B_{a,b}(g_2, g_3)) \cdot B_{a,b}(g_1, g_2\ g_3)$$

and since the action of G_p on μ_p is trivial the equality becomes

$$B_{a,b}(g_1, g_2) \cdot B_{a,b}(g_1\ g_2, g_3) = B_{a,b}(g_2, g_3) \cdot B_{a,b}(g_1, g_2\ g_3).$$

To check this is straightforward using the fact that $\overline{\phi}$ is a homomorphism.

Theorem 2.4

$$(a,b) = \zeta^{inv\ B_{a,b}} \tag{3}$$

Proof. This follows from a general theorem of computing cup-products (here we regard ϕ_a and ϕ_b as elements in $H^1(G_p, \mu_p)$), which in our case states

$$\phi_b(\theta(a)) = \zeta^{inv\ (B_{a,b})}$$

(Ref. Serre, Local fields, Ch XI + Appendix).

Here *inv* is the invariant map

$$H^2(G_K, \mu_p) \cong H^2(G_K, K^{al\ \times})[p] \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

To get the theorem use (2.3). I have to remark that to prove (2.3) one needs the above relation. □

Now we calculate one specific $B_{a,b}$.

First we compute

$$(\pi, \xi) = \frac{\theta(\pi)(\xi^{1/p})}{\xi^{1/p}} = \frac{(\xi^{1/p})^{|F|}}{\xi^{1/p}} = \xi^{(|F|-1)/p} = \zeta$$

Then $(\xi,\pi)=\zeta^{-1}$, and $(\pi,\pi)=1$, $(\xi,\xi)=1$. The last two follow, for example, from the fact that a is a norm from $K[a^{1/p}]$.

For any fixed a,b, $B_{a,b}$ as a quadratic form is uniquely determined by its values on four 2-tuples (ξ,ξ), (π,ξ), (ξ,π), (π,π), since

$$G_p \cong K^\times/K^{\times p} \cong \pi^{\mathbf{Z}/p\mathbf{Z}}\ \xi^{\mathbf{Z}/p\mathbf{Z}}$$

(for the last isomorphism it is important that $p \neq \ell$). The maximal abelian extension of K of exponent p lies in the tamely ramified part of K^{al}/K (because of p). One may think of it as consisting of the union of totally tamely ramified part, when we attach p^{th} root of π, and unramified part, when we attach p^{th} root of unity, e.g. $\xi^{1/p}$, which corresponds to the unique degree p extension of the residue field. After identifying $K^\times/K^{\times p}$ and G_p via θ (i.e. denote the image $\theta(a)$ in G_p also by a) we can treat π as the generator of the unramified part of G_p (since $\theta(\pi)=Frob$), and ξ as the generator of the totally ramified part, for a similar reason. Then what the above calculations of Hilbert symbols show is that

$$B_{\xi,\pi}(\pi,\pi)=\zeta^{\overline{\phi}_\xi(\pi)\ \overline{\phi}_\pi(\pi)}=\phi_\pi(\pi)^{\overline{\phi}_\xi(\pi)}=(\pi,\pi)^{\overline{\phi}_\xi(\pi)}=1$$

Similarly, one obtains

$$B_{\xi,\pi}(\xi,\pi)=1 \quad , \quad B_{\xi,\pi}(\xi,\xi)=1$$

And finally,

$$B_{\xi,\pi}(\pi,\xi)=\zeta^{\overline{\phi}_\xi(\pi)\ \overline{\phi}_\pi(\xi)}=\phi_\pi(\xi)^{\overline{\phi}_\xi(\pi)}=\left(\zeta^{-1}\right)^{\overline{\phi}_\xi(\pi)}=\left(\zeta^{\overline{\phi}_\xi(\pi)}\right)^{-1}=(\phi_\xi(\pi))^{-1}=\zeta^{-1}$$

Let $<\,,\,>$ be the pairing in the restricted Tate local duality theorem.

$$E(K)/pE(K)\cong H^1(g,E_p)=\mathrm{Hom}(g,E_p)\cong \mathrm{Hom}(\prod_s \mathbf{Z}_s(1),E_p)\cong$$

$$\mathrm{Hom}(\mathbf{Z}_p(1),E_p)\cong \mathrm{Hom}(\varprojlim \mu_{p^n},E_p)=\mathrm{Hom}(\mu_p,E_p)$$

So to $c_1\in E(K)/pE(K)$ we associate the corresponding homomorphism

$$\varphi_1\ :\ \mu_p \longrightarrow E_p(K)$$

Similarly, to $c_2 \in H^1(G_k,E)_p \cong H^1(\mathcal{I},E_p)^g \cong \mathrm{Hom}\,(\mu_p,E_p)^g \cong \mathrm{Hom}\,(\mu_p,E_p)$ associate the corresponding homomorphism

$$\varphi_2\ :\ \mu_p \longrightarrow E_p(K)$$

Let ζ be as above, and $\varphi_1(\pi)=e_1$, $\varphi_2(\xi)=e_2$ in E_p. Then

Theorem 2.5 (Kolyvagin)

$$\zeta^{<c_1,\ c_2>} = \{e_1,\ e_2\}$$

where $\{\ ,\ \}$ *is the Weil pairing on* E_p.

Proof. First extend φ_1 and φ_2 to a map $K^\times/K^{\times p} \longrightarrow E_p$ in an obvious way

$$\varphi_1(\pi) = e_1 \quad , \quad \varphi_1(\xi) = 0$$

$$\varphi_2(\pi) = 0 \quad , \quad \varphi_2(\xi) = e_2$$

Now the cup-product $\varphi_1 \cup \varphi_2 \in H^2(G_p, \mu_p)$, which is used to evaluate the Tate pairing, is described by the bilinear form

$$B_1 \ : \quad K^\times/K^{\times p} \otimes K^\times/K^{\times p} \longrightarrow \mu_p$$

satisfying $B_1(a,\ b) = \{\varphi_1(a),\ \varphi_2(b)\}$, so

$$B_1(\pi,\pi) = 1, \quad B_1(\pi,\xi) = \{e_1, e_2\}, \quad B_1(\xi,\pi) = 1, \quad B_1(\xi,\xi) = 1.$$

We first applied the cup-product, then Weil pairing, finally to get the Tate pairing we have to take the invariant map $H^2(G_p, \mu_p) \longrightarrow \mathbf{Z}/p\mathbf{Z}$. So

$$< \cdot, \cdot >= inv B_1(\cdot, \cdot)$$

Let $\{e_1, e_2\} = \zeta^x$.

Compairing B_1 and $B_{\xi,\pi}$, we have $B_1 = B_{\xi,\pi}^{-x}$ hence

$$inv\ B_1 = (-x) inv\ B_{\xi,\pi}$$

Since

$$\zeta^{inv\ B_{\xi,\pi}} = (\xi, \pi) = \zeta^{-1}$$

we have $inv\ B_1 = x$. Finally

$$\zeta^{<c_1,\ c_2>} = \{e_1,\ e_2\}$$

□

Remark This theorem gives a proof of the non-degeneracy of $< \cdot, \cdot >$ modulo the proofs of the statements from local class field theory we have skipped.

References

[1] P. Clark, *Personal communication*

[2] B. Gross, *Kolyvagin's work on modular elliptic curves*, London Math. Soc. Lecture Note Ser. **153** (1991), 235-256.

[3] J. Milne, *Lectures on etale cohomology*, available at www.jmilne.org

[4] J. Milne, *Class field theory*, available at www.jmilne.org

[5] J. Milne, *Arithmetic duality theorems*

[6] J-P. Serre, *Local fields*

[7] J. Silverman, *The arithmetic of elliptic curves*

[8] L. Washington, *Number fields and elliptic curves*, in Number Theory and Applications, R.A. Mollin ed. (1989), 245 - 278.

[9] T. Weston, *Notes of Mazur's course*