Fields Institute Communications
Volume **56**, 2009

Local Galois Symbols on $E \times E$

Jacob Murre
Department of Mathematics
University of Leiden
2300 RA Leiden
Leiden, Netherlands
`murre@math.leidenuniv.nl`

Dinakar Ramakrishnan
Department of Mathematics
California Institute of Technology
Pasadena, CA 91125 USA
`dinakar@caltech.edu`

To Spencer Bloch, with admiration

Abstract. This article studies the Albanese kernel $T_F(E \times E)$, for an elliptic curve E over a p-adic field F. The main result furnishes information, for any odd prime p, about the kernel and image of the Galois symbol map from $T_F(E \times E)/p$ to the Galois cohomology group $H^2(F, E[p] \otimes E[p])$, for E/F ordinary, without requiring that the p-torsion points are F-rational, or even that the Galois module $E[p]$ is semisimple. A key step is to show that the image is zero when the finite Galois module $E[p]$ is acted on non-trivially by the pro-p-inertia group I_p. Non-trivial classes in the image are also constructed when $E[p]$ is suitably unramified. A forthcoming sequel will deal with global questions.

Introduction

Let E be an elliptic curve over a field F, $\overline{F}$ a separable algebraic closure of F, and ℓ a prime different from the characteristic of F. Denote by $E[\ell]$ the group of ℓ-division points of E in $E(\overline{F})$. To any F-rational point P in $E(F)$ one associates by Kummer theory a class $[P]_\ell$ in the Galois cohomology group $H^1(F, E[\ell])$,

---

2000 *Mathematics Subject Classification.* Primary 11G07, 14C25, 11G10; Secondary 11S25.
Partially supported by the NSF.

represented by the 1-cocycle

$$\beta_\ell : \mathrm{Gal}(\overline{F}/F) \to E[\ell],\ \sigma \mapsto \sigma\left(\frac{P}{\ell}\right) - \frac{P}{\ell}.$$

Here $\frac{P}{\ell}$ denotes any point in $E(\overline{F})$ with $\ell\left(\frac{P}{\ell}\right) = P$. Given a pair (P, Q) of F-rational points, one then has the cup product class

$$[P, Q]_\ell := [P]_\ell \cup [Q]_\ell \in H^2(F, E[\ell]^{\otimes 2}).$$

Any such pair (P, Q) also defines a F-rational algebraic cycle on the surface $E \times E$ given by

$$\langle P, Q\rangle := [(P, Q) - (P, 0) - (0, Q) + (0, 0)],$$

where $[\cdots]$ denotes the class taken modulo *rational equivalence*. It is clear that this *zero cycle of degree zero* defines, by the parallelogram law, the trivial class in the Albanese variety $Alb(E \times E)$. So $\langle P, Q\rangle$ lies in the *Albanese kernel* $T_F(E \times E)$. It is a known, but non-obvious, fact that the association $(P, Q) \to [P, Q]_\ell$ depends only on $\langle P, Q\rangle$, and thus results in the *Galois symbol map*

$$s_\ell : T_F(E \times E)/\ell \to H^2(F, E[\ell]^{\otimes 2}).$$

For the precise technical definition of s_ℓ we refer to Definition 2.5.3. In essence, s_ℓ is the restriction to the Albanese kernel $T_F(E \times E)$ of the cycle map over F with target the continuous cohomology (in the sense of Jannsen [J]) with $\mathbb{Z}/\ell$-coefficients. Due to the availability of the norm map for finite extensions (see Section 1.7), it suffices to study this map s_ℓ on the subgroup $ST_F(E \times E)$ of $T_F(E \times E)$ generated by symbols, whence the christening of s_ℓ as the *Galois symbol map*. Moreover, it is possible to study this map via a Kummer sequence (see Sections 2.2 and 2.3).

It is a conjecture of Somekawa and Kato that this map is always injective ([So]). It is easy to verify this when F is $\mathbb{C}$ or $\mathbb{R}$. In the latter case, the image of s_ℓ is non-trivial iff $\ell = 2$ and all the 2-torsion points are $\mathbb{R}$-rational, which can be used to exhibit a non-trivial global 2-torsion class in $T_{\mathbb{Q}}(E \times E)$, whenever E is defined by $y^2 = (x-a)(x-b)(x-c)$ with $a, b, c \in \mathbb{Q}$. It should also be noted that injectivity of the analog of s_ℓ fails for certain surfaces occurring as quadric fibrations (cf. [ParS]). However, the general expectation is that such pathologies do not occur for *abelian* surfaces.

Let F denote a non-archimedean local field, with ring of integers $\mathcal{O}_F$ and residual characteristic p. Let E be a semistable elliptic curve over F, and $\mathcal{E}[\ell]$ the kernel of multiplication by ℓ on $\mathcal{E}$, which defines a finite flat groupscheme $\mathcal{E}[\ell]$ over $S = \mathrm{Spec}(\mathcal{O}_F)$. Let $F(E[\ell])$ denotes the smallest Galois extension of F over which all the ℓ-division points of E are rational. It is easy to see that the image of s_ℓ is zero if (i) E has good reduction *and* (ii) $\ell \neq p$, the reason being that the absolute Galois group G_F acts via its maximal unramified quotient $\mathrm{Gal}(F_{nr}/F) \simeq \hat{\mathbb{Z}}$, which has cohomological dimension 1. So we will concentrate on the more subtle $\ell = p$ case.

Theorem A *Let F be a non-archimedean local field of characteristic zero with residue field $\mathbb{F}_q$, $q = p^r$, p odd. Suppose E/F is an elliptic curve over F, which has good, ordinary reduction. Then the following hold:*

(a) *s_p is injective, with image of $\mathbb{F}_p$-dimension ≤ 1.*

(b) *The following are equivalent:*

(bi) *$dim\, Im(s_p) = 1$*

(bii) *$F(E[p])$ is unramified over F, with the prime-to-p part of $[F(E[p]) : F]$ being ≤ 2, and $\mu_p \subset F$.*

(c) *If $E[p] \subset F$, then $T_F(E \times E)/p \simeq \mathbb{Z}/p$ consists of symbols $\langle P, Q\rangle$ with P, Q in $E(F)/p$.*

Note that $[F(E[p]) : F]$ is prime to p iff the $\mathrm{Gal}(\overline{F}/F)$-representation ρ_p on $E[p]$ is semisimple. We obtain:

Corollary B *$T_F(E \times E)$ is p-divisible when $E[p]$ is non-semisimple and wildly ramified.*

When all the p-division points of E are F-rational, the injectivity part of part (a) has already been asserted, without proof, in [R-S], where the authors show the interesting result that $T_F(E \times E)/p$ is a quotient of $K_2(F)/p$. Our techniques are completely disjoint from theirs, and besides, the delicate part of our proof of injectivity is exactly when $[F(E[p]) : F]$ is divisible by p, which is equivalent to the Galois module $E[p]$ being non-semisimple. Our results prove in fact that when $T_F(A)/p$ is non-zero, i.e., when $F(E[p])/F$ is unramified of degree ≤ 2, it is isomorphic to the p-part $\mathrm{Br}_F[p]$ of the Brauer group of F, which is known ([Ta1]) to be isomorphic to $K_2(F)/p$.

A completely analogous result concerning s_ℓ holds when E/F has multiplicative reduction, for both $\ell = p$ and $\ell \neq p$, and this can be proved by arguments similar to the ones we use in the ordinary case. However, there is already an elegant paper of Yamazaki ([Y]) giving the analogous result (in the multiplicative case) by a different method, and we content ourselves to a very brief discussion in section 7 on how to deduce this analogue from [Y].

The relevant preliminary material for the paper is assembled in the first two sections and in the Appendix. We have, primarily (but not totally) for the convenience of the reader, supplied proofs of various statements for which we could not find published references, even if they are apparently known to experts or in the *folklore*. After this the proof of Theorem A is achieved in the following sections via a number of Propositions. In section 3, we first prove, via the key Proposition C, that the image of s_p is at most one and establish part of the implication $(bi) \implies (bii)$; the remaining part of this implication is proved in section 4 via Proposition D. The converse implication $(bii) \implies (bi)$ and part (c) are proved in section 5. Finally, part (a), giving the injectivity of s_p, is proved in section 6.

In a sequel we will use these results in conjunction with others (including a treatment of the case of supersingular reduction, p-adic approximation, and a local-global lemma) and prove two global theorems about the Galois symbols on $E \times E$ modulo p, for any odd prime p.

The second author would like to acknowledge support from the National Science Foundation through the grants DMS-0402044 and DMS-0701089, as well as the hospitality of the *DePrima Mathematics House* at Sea Ranch, CA. The first author would like to thank Caltech for the invitation to visit Pasadena, CA, for several visits during the past eight years. This paper was finalized in May 2008. We are grateful to various mathematicians who pointed out errors in a previous version, which we have fixed. Finally, it is a pleasure to thank the referee of this paper, and also Yamazaki, for their thorough reading and for pointing out the need for further

explanations; one such comment led to our noticing a small gap, which we have luckily been able to take care of with a modified argument.

It gives us great pleasure to dedicate this article to Spencer Bloch, whose work has inspired us over the years, as it has so many others. The first author (J.M.) has been a friend and a fellow *cyclist* of Bloch for many years, while the second author (D.R.) was Spencer's post-doctoral mentee at the University of Chicago during 1980-82, a period which he remembers with pleasure.

1 Preliminaries on Symbols

1.1 Cycles

Let F be a field and X a smooth projective variety of dimension d and defined over F. Let $0 \le i \le d$ and $\mathcal{Z}_i(X)$ be the group of algebraic cycles on X defined over F and of dimension i, i.e. the free group generated by the subvarieties of X of dimension i and defined over F (see [F], section 1.2). A cycle of dimension i is called rationally equivalent to zero over F if there exists $T \in \mathcal{Z}_{i+1}(\mathbb{P}^1 \times X)$ and two points P and Q on $\mathbb{P}^1$, each rational over F, such that $T(P) = Z$ and $T(Q) = 0$, where for $R \in \mathbb{P}^1$ we put $T(R) = \mathrm{pr}_2(T.(R \times X))$ in the usual sense of calculation with cycles (see [F]). Let $\mathcal{Z}_i^{\mathrm{rat}}(X)$ be the subgroup of $Z_i(X)$ generated by the cycles rationally equivalent to zero and $\mathrm{CH}_i(X) = \mathcal{Z}_i(X)/\mathcal{Z}_i^{\mathrm{rat}}(X)$ the Chow group of rational equivalence classes of i-dimensional cycles on X defined on F.

If $K \supset F$ is an extension then we write $X_K = X \times_F K$, $Z_i(X_K)$ and $\mathrm{CH}_i(X_K)$ for the corresponding groups defined over K and if $\bar{F}$ is the algebraic closure of F then we write $\bar{X} = X_{\bar{F}}$, $\mathcal{Z}_i(\bar{X})$ and $\mathrm{CH}_i(\bar{X})$.

1.2 The Albanese kernel

In this paper we are only concerned with the case when X is of dimension 2, i.e. X is a *surface* (and in fact we shall only consider very special ones, see below) and with groups of 0-dimensional cycles contained in $\mathrm{CH}_0(X)$. In that case note that if $Z \in \mathcal{Z}_0(X)$ then we can write $Z = \sum n_i P_i$ when $P_i \in X(\bar{F})$, i.e. the P_i are points on X – but themselves only defined (in general) over an extension field K of F. Put $A_0(X) = \mathrm{Ker}(\mathrm{CH}_0(X) \xrightarrow{\deg} \mathbb{Z})$ where $\deg(Z) = \sum n_i \deg(P_i)$, i.e. $A_0(X)$ are the cycle classes of degree zero and put further $T(X) := \mathrm{Ker}(A_0(X) \to \mathrm{Alb}(X))$, where $\mathrm{Alb}(X)$ is the Albanese variety of X (see [Bl]). Again if $K \supset F$, write $A_0(X_K)$, $T(X_K)$ or also $T_K(X)$ for the corresponding groups over K.

It is known that both $A_0(\bar{X})$ and $T(\bar{X})$ are *divisible* groups ([Bl]). Moreover if the group of transcendental cycles $H^2(\bar{X})_{\mathrm{trans}}$ is non-zero, and if $\bar{F}$ is a universal domain (ex. $\bar{F} = \mathbb{C}$), the group $T(\bar{X})$ is "huge" (infinite dimensional) by Mumford (in characteristic zero) and Bloch (in general) ([Bl], 1.22).

1.3 Symbols

We shall only be concerned with surfaces X which are abelian, even of the form $A = E \times E$, where E is an *elliptic curve* defined over F. If $P, Q \in E(F)$, put

$$\langle P, Q \rangle := (P, Q) - (P, O) - (O, Q) + (O, O)$$

where O is the origin on E, and the addition is the *addition of cycles* (or better: cycle classes). Clearly $\langle P, Q \rangle \in T_F(A)$ and $\langle P, Q \rangle$ is called the *symbol* of P and Q.

Definition $ST_F(A)$ denotes the subgroup of $T_F(A)$ generated by symbols $\langle P, Q\rangle$ with $P \in E(F)$, $Q \in E(F)$. It is called the *symbol group* of $A = E \times E$.

1.4 Properties and remarks

1. The symbol is *bilinear* in P and Q. For instance
$$\langle P_1 + P_2, Q\rangle = \langle P_1, Q\rangle + \langle P_2, Q\rangle$$
(where now the first + sign is addition on E!).
2. The symbol is the Pontryagin product
$$\langle P, Q\rangle = \{(P, 0) - (0, 0)\} * \{(0, Q) - (0, 0)\}$$
3. If F is finitely generated over the prime field, then it follows from the theorem of Mordell-Weil that $ST_F(A)$ is finitely generated.
4. Note the similarity with the group $K_2(F)$ of a field. Also the symbol group $ST_F(A)$ is related to, but different from, the group $K_2(E \times E)$ defined by Somekawa ([So]); compare also with [R-S].

1.5 Restriction and norm/corestriction

Let $K \supset F$. Consider the morphism $\varphi_{K/F}\colon A_K \to A_F$.

a. This induces homomorphisms, called the *restriction* homomorphisms:
$$\mathrm{res}_{K/F} = \varphi^*_{K/F}\colon \mathrm{CH}_i(A_F) \to \mathrm{CH}_i(A_K), T_F(A) \to T_K(A)$$
and $ST_F(A) \to ST_K(A)$ (see [F], section 1.7).

b. Also, when $[K : F] < \infty$, we have the *norm* or *corestriction* homomorphisms
$$N_{K/F} = (\varphi_{K/F})_*\colon CH_i(A_K) \to CH_i(A_F) \text{ and } T(A_K) \to T_F(A)$$
(see [F], section 1.4, page 11 and 12).

Remarks 1. If $[K\colon F] = n$ we have $\varphi_* \circ \varphi^* = n$

2. It is *not* clear if $N_{K/F} = \varphi_*$ induces a homomorphism on the *symbol groups themselves*. Note however that there is such norm map for cohomology ([Se2], p. 127) and for K_2-theory ([M], p. 137).

1.6 Some preliminary lemmas

Lemma 1.6.1 *Let $Z \in T_F(A)$. Suppose we can write $Z = \sum_{i=1}^{N}(P_i, Q_i) - \sum_{i=1}^{N}(P'_i, Q'_i)$ with P_i, P'_i, Q_i and Q'_i all in $E(F)$ for $i = 1, \ldots, N$. Then $Z \in ST_F(A)$.*

Proof Since $Z \in T_F(A)$ we have that $\sum_{i=0}^{N} P_i = \sum_{i=0}^{N} P'_i$ and $\sum_{i=1}^{N} Q_i = \sum_{i=1}^{N} Q'_i$ as *sum of points on E*. From this it follows immediately that we can rewrite $Z = \sum_{i=1}^{N}\{(P_i, Q_i) - (P_i, 0) - (0, Q_i) + (0, 0)\} - \sum_{i=1}^{N}\{(P'_i, Q'_i) - (P'_i, 0) - (0, Q'_i) + (0, 0)\} = \sum_{i=1}^{N}\langle P_i, Q_i\rangle - \sum_{i=1}^{N}\langle P'_i, Q'_i\rangle$; hence $Z \in ST_F(A)$. □

Corollary 1.6.2 *Over the algebraic closure we have*
$$T(\bar{A}) = \varinjlim_{K} \{\mathrm{res}_{\bar{F}/K} ST_K(A)\}$$
where the limit is over all finite extensions $K \supset F$.

Proof Immediate from Lemma 1.6.1. □

1.7 Norms of symbols

Next we turn our attention again to $T(A) = T_F(A)$ itself. If $K \supset F$ is a finite extension and $P, Q \in E(K)$ then consider $N_{K/F}(\langle P, Q\rangle) \in T_F(A)$. Let $ST_{K/F}(A) \subset T_F(A)$ be the subgroup of $T_F(A)$ generated by such elements (i.e., coming as norms of the symbols from finite field extensions $K \supset F$). Note that clearly $ST_{F/F}(A) = ST_F(A)$ and also that $ST_{K/F}(A)$ consists of the norms of elements of $ST_K(A)$.

Lemma 1.7.1 *With the above notations let $T'_F(A)$ be the subgroup of $T_F(A)$ generated by all the subgroups of type $ST_{K/F}(A)$ of $T_F(A)$ for $K \supset F$ finite (with $K \subset \bar{F}$). Then $T'_F(A) = T_F(A)$.*

Proof For simplicity we shall (first) assume $\mathrm{char}(F) = 0$. If $\mathrm{cl}(Z) \in T_F(A)$, then $\mathrm{cl}(Z)$ is the (rational equivalence) class of a cycle $Z \in \mathcal{Z}_0(A_F)$ and moreover $Z = Z' - Z''$ with Z' and Z'' positive (i.e. "effective"), of the same degree and both $Z' \in \mathcal{Z}_0(A_F)$ and $Z'' \in \mathcal{Z}_0(A_F)$. Fixing our attention on $Z' \in \mathcal{Z}_0(A_F)$ we can, by definition, write $Z' = \sum_\alpha Z'_\alpha$ where the Z'_α are (0-dimensional) subvarieties of A and *irreducible* over F (Remark: in the terminology of Weil's Foundations [W] the Z' is a "rational chain" over F and the Z'_α are the "prime rational" parts of it, see [W], p. 207). For each α we have $Z'_\alpha = \sum_{i=1}^{n_\alpha}(P'_{\alpha i}, Q'_{\alpha i})$ where the $(P'_{\alpha i}, Q'_{\alpha i}) \in A(\bar{F})$ is a set of points which form a *complete set of conjugates over* F (see [W], 207). Note that also $\sum_{i=1}^{n_\alpha}(P'_{\alpha i}, 0) \in \mathcal{Z}_0(A_F)$ and similarly $\sum_{i=1}^{n_\alpha}(0, Q'_{\alpha i}) \in \mathcal{Z}_0(A_F)$ (Note: these cycles are rational, but not necessarily prime rational.) For each α fix an arbitrary $i(\alpha)$ and put $K_{\alpha i(\alpha)} = F(P'_{\alpha i(\alpha)}, Q'_{\alpha i(\alpha)})$ and consider now the *cycle* $(P'_{\alpha i(\alpha)}, Q'_{\alpha i(\alpha)}) \in \mathcal{Z}_0(A_{K_{\alpha i(\alpha)}})$. We have by definition (see [F], section 1.4, p. 11), $Z'_\alpha = N_{K_{\alpha i(\alpha)}/F}(P'_{\alpha i(\alpha)}, Q'_{\alpha i(\alpha)})$. Furthermore if we put

$$Z^*_{\alpha i(\alpha)} = \left\langle P'_{\alpha i(\alpha)}, Q'_{\alpha i(\alpha)}\right\rangle \in ST_{K_{\alpha i(\alpha)}}(A)$$

then in $T_F(A)$ we have

$$N_{K_{\alpha i(\alpha)}/F}(Z^*_{\alpha i(\alpha)}) = \sum_{i=1}^{n_\alpha}\langle P'_{\alpha i}, Q'_{\alpha i}\rangle$$

(again by the definition of the $N_{-/F}$) and clearly the cycle is in $ST_{K_{\alpha i(\alpha)}/F}(A)$, i.e. in $T'_F(A)$. Now doing this for every α and treating similarly $Z'' = \sum_\beta Z''_\beta$, we have, since $Z \in T_F(A)$, that

$$Z = Z' - Z'' = \sum_\alpha Z'_\alpha - \sum_\beta Z'_\beta = \sum_\alpha \sum_i \langle P'_{\alpha i}, Q'_{\alpha i}\rangle - \sum_\beta \sum_j \left\langle P''_{\beta j}, Q''_{\beta j}\right\rangle.$$

Hence $Z \in T'_F(A)$, which completes the proof (in char 0). □

Remark If $\mathrm{char}(F) = p > 0$, then we have that $Z'_\alpha = p^{m_\alpha} \sum_i (P'_{\alpha i}, Q'_{\alpha i})$ where the p^{m_α} is the degree of inseparability of the field extension $K_{\alpha i(\alpha)}$ over F (see again [W], p. 207). Note that p^{m_α} does not depend on the choice of the index

$i(\alpha)$, because the field $K_{\alpha i(\alpha)}$ is determined by α up to *conjugation* over F. From that point onwards the proof is the same (note in particular that we shall have $Z'_\alpha = N_{K_{\alpha i(\alpha)}/F}(P'_{\alpha i}, Q'_{\alpha i})$).

Lemma 1.7.2 *For $P, Q \in E(F)$ we have $\langle Q, P\rangle = -\langle P, Q\rangle$, i.e., the symbol is skew-symmetric.*

Proof Since the symbol is bilinear we have a well-defined homomorphism

$$\lambda\colon\ E(F) \otimes_{\mathbb{Z}} E(F) \to ST_F(A) \text{ with } \lambda(P \otimes Q) = \langle P, Q\rangle\,.$$

Then $\lambda((P+Q) \otimes (P+Q)) = (P+Q, P+Q) - (P+Q, 0) - (0, P+Q) + (0,0)$. On the other hand by the bilinearity, it also equals $\langle P, P\rangle + \langle P, Q\rangle + \langle Q, P\rangle + \langle Q, Q\rangle$. On the diagonal we have $(P+Q, P+Q) + (0,0) = (P,P) + (Q,Q)$, on $E \times 0$ we have $(P+Q, 0) + (0,0) = (P,0) + (Q,0)$, and on $0 \times E$ we have $(0, P+Q) + (0,0) = (0,P) + (0,Q)$. Putting these facts together we get $\langle P, Q\rangle + \langle Q, P\rangle = 0$. $\square$

1.8 A useful lemma

We will often have occasion to use the following simple observation:

Lemma 1.8.1 *Let F be any field and ℓ a prime. Let P, Q be points in $E(F)$, $Q' \in E(\bar{F})$ s.t. $\ell Q' = Q$, and put $K = F(Q')$. Consider the statements*

(a) $P \in N_{K/F} E(K) \bmod \ell\, E(F)$

(b) $\langle P, Q\rangle \in \ell\, T_F(A)$

Then (a) implies (b).

Proof Let $P = N_{K/F}(P') + \ell P_1$, with $P' \in E(K)$, $P_1 \in E(F)$. Then $\langle P, Q\rangle - \ell\,\langle P_1, Q\rangle = \left\langle N_{K/F}(P'), Q\right\rangle$, which equals, by the projection formula,

$$N_{K/F}(\left\langle P', \mathrm{Res}_{K/F} Q\right\rangle) = N_{K/F}(\langle P', \ell Q'\rangle) = \ell N_{K/F}(\langle P', Q'\rangle) \in \ell T_F(A).$$

$\square$

2 Symbols, cup products, and $H^2_s(F, E^{\otimes 2})$

2.1 Degeneration of the spectral sequence

Notations and assumption are as before. Let ℓ be a prime number with $\ell \neq \mathrm{char}(F)$. We work here with $\mathbb{Z}_\ell$ coefficients, but the results are also true for $\mathbb{Z}/\ell^s$ coefficients (any $s \geq 1$) and $\mathbb{Q}_\ell$-coefficients.

Lemma 2.1.1 *The Hochschild-Serre spectral sequence*

$$E_2^{pq} = H^p(F, H^q_{\mathrm{et}}(\bar{A}, \mathbb{Z}_\ell(s)) \Longrightarrow H^{p+q}_{\mathrm{et}}(A, \mathbb{Z}_\ell(s))$$

degenerates at d_2-level (and at all d_t-levels, $t \geq 2$) for all r.

Remark We could take here any abelian variety A instead of $E \times E$.

Proof This follows from "weight" considerations. Consider on A multiplication by n, i.e. $n\colon A \to A$ is the map $x \to nx$. Then we have a commutative diagram

$$\begin{array}{ccc}
H^p(F, H^q_{\mathrm{et}}(\bar{A}, -)) & \xrightarrow{d_2} & H^{p+2}(F, H^{q-1}_{\mathrm{et}}(\bar{A}, -)) \\
{\scriptstyle n^*}\big\downarrow & & {\scriptstyle n^*}\big\downarrow \\
H^p(F, H^q_{\mathrm{et}}(\bar{A}, -)) & \xrightarrow{d_2} & H^{p+2}(F, H^{q-1}_{\mathrm{et}}(\bar{A}, -))
\end{array}$$

On the left we have multiplication by n^q, on the right by n^{q-1}. this being true for any $n > 0$, we must have $d_2 = 0$. $\square$

2.2 Kummer sequence (and some notations)

If E is an elliptic curve defined over F, we write (by abuse of notation)

$$E[\ell^n] := \ker\{E(\bar{F}) \xrightarrow{\ell^n} E(\bar{F})\},$$

and we have the (elliptic) Kummer sequence

$$0 \longrightarrow E[\ell^n] \longrightarrow E(\bar{F}) \xrightarrow{\ell^n} E(\bar{F}) \longrightarrow 0.$$

This is an exact sequence of $\mathrm{Gal}(\bar{F}/F)$-modules and gives us a short exact sequence of (cohomology) groups

$$0 \longrightarrow E(F)/\ell^n \longrightarrow H^1(F, E[\ell^n]) \longrightarrow H^1(F, \bar{E})[\ell^n] \longrightarrow 0$$

Taking the limit over n, one gets the homomorphism

$$\delta_\ell^{(1)} \colon\ E(F) \longrightarrow H^1(F, T_\ell(E))$$

where $T_\ell(E) = \varprojlim_n E[\ell^n]$ is the Tate group.

This allows us to define

$$[\cdot,\cdot]_\ell \colon\ E(F) \otimes E(F) \longrightarrow H^2(F, T_\ell(E)^{\otimes 2})$$

by

$$[P, Q]_\ell = \delta_\ell^{(1)}(P) \cup \delta_\ell^{(1)}(Q)$$

We have similar maps (and we use the same notations) if we take $E(F)/\ell^n$ and $E[\ell^n]^{\otimes 2}$.

Explicitly the map $\delta_\ell^{(1)}$ is given by the following: For $P \in E(F)$ the cohomology class $\delta_\ell^1(P)$ is represented by the 1-cocycle

$$\mathrm{Gal}(\bar{F}/F) \rightarrow T_\ell(E),$$

$$\sigma \mapsto \left(\sigma\left(\frac{1}{\ell}P\right) - \frac{1}{\ell}P,\ \sigma\left(\frac{1}{\ell^2}P\right) - \frac{1}{\ell^2}P,\ \ldots\ldots\right).$$

2.3 Comparison with the usual cycle class map

For every smooth projective variety X defined over F there is the cycle class map to continuous cohomology as defined by Jannsen ([J], lemma 6.14)

$$\mathrm{cl}_\ell^{(i)} \colon\ \mathrm{CH}^i(X) \longrightarrow H^{2i}_{\mathrm{cont}}(X, \mathbb{Z}_\ell(i))$$

Taking now $X = E$, resp. $X = A$, and using the degeneration of the Hochschild-Serre spectral sequence we get

$$\mathrm{cl}_\ell^{(1)} \colon\ CH^1_{(0)}(E) \longrightarrow H^1(F, H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1)))$$

where $\mathrm{CH}^1_{(0)}(E)$ is the Chow group of 0-cycles on E of degree 0, resp.

$$\mathrm{cl}_\ell^{(2)} \colon\ T_F(A) \longrightarrow H^2(F, H^2_{\mathrm{et}}(\bar{A}, \mathbb{Z}_\ell(2))).$$

Lemma 2.3.1 *There is a commutative diagram*

$$\begin{array}{ccc} E(F) & \xrightarrow{\delta_\ell^{(1)}} & H^1(F, T_\ell(E)) \\ \downarrow & & \downarrow \cong \\ \mathrm{CH}^1_{(0)}(E) & \xrightarrow{cl_\ell^{(1)}} & H^1(F, H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1))) \end{array}$$

where the vertical map on the left is $P \mapsto (P) - (0)$ and the one on the right comes from the well-known isomorphism $T_\ell(E) \xrightarrow{\sim} H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1))$.

Proof See [R], proof of the lemma in the appendix. $\square$

2.4 The symbolic part of cohomology

Let K/F be any finite extension. Given a pair of points $P, Q \in E(K)/\ell$, with associated classes $\delta_\ell^{(1)}(P), \delta_\ell^{(1)}(Q)$ in $H^1(K, E[\ell])$. We have seen in section 2.2 that by taking cup product in Galois cohomology, we get a class $[P, Q]_\ell$ in $H^2(K, E[\ell]^{\otimes 2})$. By taking the norm (corestriction) from $H^2(K, E[\ell]^{\otimes 2})$ to $H^2(F, E[\ell]^{\otimes 2})$, we then get a class

$$N_{K/F}([P, Q]_\ell) \in H^2(F, E[\ell]^{\otimes 2}).$$

We define the *symbolic part* $H^2_s(F, E[\ell]^{\otimes 2})$ of $H^2(F, E[\ell]^{\otimes 2})$ to be the $\mathbb{F}_\ell$-subspace generated by such *norms of symbols* $N_{K/F}([P, Q]_\ell)$, where K runs over all possible finite extensions of F and P, Q run over all pairs of points in $E(K)/\ell$.

Note the similarity of this definition with the description of $T_F(E \times E)/\ell$ via Lemma 1.7.1.

2.5 Summary

The remarks and maps of the previous sections can be subsumed in the following:

Proposition 2.5.1 *There exist maps and a commutative diagram*

$$
\begin{tikzcd}
E(F)^{\otimes 2} \arrow[r, "\delta_\ell^{(1)}\otimes\delta_\ell^{(1)}"] \arrow[d] \arrow[ddddd, bend right=60, "\langle\ ,\ \rangle"'] & H^1(F, T_\ell(E))^{\otimes 2} \arrow[d, "\cong"] \\
\mathrm{CH}^1_{(0)}(E)^{\otimes 2} \arrow[r, "\mathrm{cl}_\ell^{(1)}\otimes\mathrm{cl}_\ell^{(1)}"] \arrow[dd, "p_1^*\otimes p_2^*"] & H^1(F, H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1)))^{\otimes 2} \arrow[d, hook] \arrow[ddddd, bend left=60] \\
 & H^2_{\mathrm{cont}}(E, \mathbb{Z}_\ell(1))^{\otimes 2} \arrow[d, "p_1^*\otimes p_2^*"] \\
\mathrm{CH}^1(A)^{\otimes 2} \arrow[r, "\mathrm{cl}_\ell^{(1)}\otimes\mathrm{cl}_\ell^{(1)}"] \arrow[d, "\cap"] & H^2_{\mathrm{cont}}(A, \mathbb{Z}_\ell(1))^{\otimes 2} \arrow[d, "\cup"] \\
\mathrm{CH}^2(A) \arrow[r, "\mathrm{cl}_\ell^{(2)}"] & H^4_{\mathrm{cont}}(A, \mathbb{Z}_\ell(2)) \\
T_F(A) \arrow[u, hook] \arrow[r, "\mathrm{cl}_\ell^{(2)}"] \arrow[dr, "c_\ell"'] & H^2(F, H^2_{\mathrm{et}}(\bar{A}, \mathbb{Z}_\ell(2))) \arrow[u, hook] \\
 & H^2(F, H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1))^{\otimes 2}) \arrow[u, hook]
\end{tikzcd}
$$

where c_ℓ is defined via the Künneth formula $H^2_{\mathrm{et}}(\bar{A}, \mathbb{Z}_\ell(2)) = H^2_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(2)) \oplus H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1))^{\otimes 2} \oplus H^2_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(2))$ and the injection on the relevant (= middle) term. In particular $[P,Q]_\ell := \delta_\ell^{(1)}(P) \cup \delta_\ell^{(1)}(Q) = c_\ell(\langle P, Q\rangle)$ for $P, Q \in E(F)$. Moreover the same holds for $\mathbb{Z}/\ell^n$-coefficients (instead of $\mathbb{Z}_\ell$) and also for $\mathbb{Q}_\ell$-coefficients.

Remark Note that the map $\langle , \rangle$ on the left from $E(F)^{\otimes 2}$ to $T_F(A)$ is the symbol map, and that the map from $H^1(F, H^1_{\mathrm{et}}(\overline{E}, \mathbb{Z}_\ell(1)))^{\otimes 2}$ to $H^2(F, H^1_{\mathrm{et}}(\overline{E}, \mathbb{Z}_\ell(1))^{\otimes 2})$ on the right is the one given by taking the cup product in group cohomology.

Proof and further explanation of the maps The map $p_1^* \otimes p_2^*$ is induced by the projections $p_i\colon A = E \times E \to E$. The commutativity in upper rectangle comes from Lemma 2.3.1. The other rectangles are all "natural". □

Corollary 2.5.2 *With respect to the decomposition*

$$H^1_{\mathrm{et}}(\bar{E}, \mathbb{Z}_\ell(1))^{\otimes 2} = T_\ell(E)^{\otimes 2} \simeq \mathrm{Sym}^2 T_\ell(E) \oplus \Lambda^2 T_\ell(E)$$

we have that $[P,Q]_\ell = c_\ell(\langle P, Q\rangle) \in H^2(F, \mathrm{Sym}^2 T_\ell(E))$ if $\ell \neq 2$ (and similarly for $\mathbb{Z}/\ell^s$-coefficients).

Proof Step 1. For the sake of clarity of the proof we shall first take two different elliptic curves E_1 and E_2 (or, if one prefers, two "different copies" E_1 and E_2 of E). Put $A_{12} = E_1 \times E_2$. There exist obvious analogs of the maps and the commutation diagram of Proposition 2.5.1; only – of course – one should now write $E_1(F) \times E_2(F)$, etc. In particular we have again the cup product on the right:

$$H^1(F, T_\ell(E_1)) \otimes H^1(F, T_\ell(E_2)) \xrightarrow{\cup} H^2(F, T_\ell(E_1) \otimes T_\ell(E_2))$$

where we write $T_\ell(E_1) = H^1_{\mathrm{et}}(\bar{E}_i, \mathbb{Z}_\ell(1))$, $i = 1, 2$. We get $c_\ell(\langle P, Q\rangle) = \delta_\ell^{(1)}(P) \cup \delta_\ell^{(1)}(Q)$. Now consider also $A_{21} = E_2 \times E_1$ and the corresponding diagram for A_{21}. Consider the natural isomorphism $t\colon A_{12} \to A_{21}$ given by $t(x, y) = (y, x)$ for $x \in E_1$ and $y \in E_2$ and also the corresponding isomorphism

$$t_*\colon H^1(\bar{E}_1) \otimes H^1(\bar{E}_2) \longrightarrow H^1(\bar{E}_2) \otimes H^1(\bar{E}_1).$$

□

Claim. *If $P \in E_1(F)$ and $Q \in E_2(F)$ then*

$$c_{\ell, A_{21}}(\langle Q, P\rangle) = -t_*(\delta_\ell^{(1)}(P) \cup \delta_\ell^{(1)}(Q)).$$

Here we have written – in order to avoid confusion – $c_{\ell,A_{21}}$ for c_ℓ in the diagram relative to A_{21}.

Proof of the claim

$$c_{\ell, A_{21}}(\langle Q, P\rangle) = \delta_\ell^{(1)}(Q) \cup \delta_\ell^{(1)}(P) = -t_* \left(\delta_\ell^{(1)}(P) \cup \delta_\ell^{(1)}(Q)\right)$$

where the first equality is from the diagram (for A_{21}) in Proposition 2.5.1 and the second equality is a well-known property in cohomology (see for instance [Br], p. 111, (3.6), or [Sp], chap.5, §6, p. 250).

Step 2. Returning to the case $E_1 = E_2 = E$, we have $\langle Q, P\rangle = -\langle P, Q\rangle$ in $T_F(A)$ by Lemma 1.7.2.

Step 3. Let us write $c_\ell(\langle P, Q\rangle) = \alpha + \beta$, with α in $H^2(F, \mathrm{Sym}^2 T_\ell(E))$ and β in $H^2(F, \Lambda^2 T_\ell(E))$. We get $c_\ell(\langle P, Q\rangle) = -c_\ell\,\langle Q, P\rangle)$ from Step 2, and next from Claim in Step 1 we have $-c_\ell(\langle Q, P\rangle) = t_*(\delta_\ell^{(1)}(P) \cup \delta_\ell^{(1)}(Q))$, hence $\alpha + \beta = t_*(\alpha + \beta) = \alpha - \beta$, hence $\beta = 0$ if $\ell \neq 2$. □

Definition 2.5.3 *Let*

$$s_\ell : T_F(E \times E)/\ell \;\to\; H^2(F, E[\ell]^{\otimes 2})$$

be the homomorphism induced by the reduction of c_ℓ modulo ℓ and by using the isomorphism of $H^1(E_{\overline{F}}, \mathbb{Z}_\ell(1))$ with the ℓ-adic Tate module of E, which is the inverse limit of $E[\ell^n]$ over n.

Thanks to the discussion above, as well as the definition of the symbolic part of $H^2(F, E[\ell]^{\otimes 2})$ in section 2.4, and Lemma 1.7.1, we obtain the following:

Proposition 2.5.4 *The image of $T_F(E \times E)/\ell$ under s_ℓ is $H^2_s(F, E[\ell]^{\otimes 2})$.*

3 A key Proposition

Let E/F be an elliptic curve over a local field F as in Theorem A, i.e., non archimedean and with finite residue field of characteristic $p > 2$, and with E having good, ordinary reduction. We will henceforth take $\ell = p$.

A basic fact is that the representation ρ_p of G_F on $E[p]$ is reducible, so the matrix of this representation is triangular. Since the determinant is the mod p cyclotomic character χ_p, we may write

$$\rho_p \;=\; \begin{pmatrix} \chi_p \nu^{-1} & * \\ 0 & \nu \end{pmatrix}, \tag{3.1}$$

where ν is an unramified character of finite order, such that $E[p]$ is semisimple (as a G_F-module) iff $* = 0$. Note that ν is necessarily of order at most 2 when E has multiplicative reduction, with $\nu = 1$ iff E has *split* multiplicative reduction. On the other hand, ν can have arbitrary order (dividing $p-1$) when E has good, ordinary reduction. In any case, there is a natural G_F-submodule C_F of $E[p]$ of dimension 1, such that we have a short exact sequence of G_F-modules:

$$0 \to C_F \to E[p] \to C'_F \to 0, \tag{3.2}$$

with G_F acting on C_F by $\chi_p\nu^{-1}$ and on C'_F by ν. Clearly, $E[p]$ is semisimple iff the sequence (3.2) splits.

The natural G_F-map $C_F^{\otimes 2} \to E[p]^{\otimes 2}$ induces a homomorphism

$$\gamma_F : H^2(F, C_F^{\otimes 2}) \to H^2F, E[p]^{\otimes 2}). \tag{3.3}$$

The key result we prove in this section is the following:

Proposition C *Let F be a non-archimedean local field with odd residual characteristic p, and E an elliptic curve over F with good, ordinary reduction. Denote by $Im(s_p)$ the image of $T_F(E \times E)/p$ under the Galois symbol map s_p into $H^2F, E[p]^{\otimes 2})$. Then we have*

(a) $\mathrm{Im}(s_p) \subset \mathrm{Im}(\gamma_F)$.

(b) *The dimension of* $\mathrm{Im}(s_p)$ *is at most* 1*, and it is zero dimensional if either* $\mu_p \not\subset F$ *or* $\nu^2 \neq 1$.

Remark If E/F has multiplicative reduction, with ℓ an arbitrary odd prime (possibly equal to p), then again the Galois representation ρ_ℓ on $E[\ell]$ has a similar shape, and in fact, ν is at most quadratic, reflecting the fact that E attains split multiplicative reduction over at least a quadratic extension of F, over which the two tangent directions at the node are rational. An analogue of Proposition C holds in that case, thanks to a key result of W.McCallum ([Mac], Prop.3.1), once we assume that ℓ does not divide the order of the component group of the special fibre $\mathcal{E}_s$ of the Néron model $\mathcal{E}$. For the sake of brevity, we are not treating this case here.

The bulk of this section will be involved in proving the following result, which at first seems weaker than Proposition C:

Proposition 3.4 *Let F, E, p be as in Proposition C. Then, for all points P, Q in $E(F)/p$, we have*

$$s_p(\langle P, Q\rangle) \in \mathrm{Im}(\gamma_F).$$

Claim 3.5 *Proposition 3.4 $\implies$ Part (a) of Proposition C*:

Proof of this claim goes via some lemmas.

Lemma 3.6 (Behavior of γ under finite extensions) *Let K/F be finite. We then have two commutative diagrams, one for the norm map $N = N_{K/F}$ and the other for the restriction map Res=Res$_{K/F}$:*

$$\begin{array}{ccc}
H^2(K, C_K^{\otimes 2}) & \xrightarrow{\gamma_K} & H^2(K, E[p]^{\otimes 2}) \\
{\scriptstyle N}\Big\downarrow \uparrow Res & & {\scriptstyle N}\Big\downarrow \uparrow Res \\
H^2(F, C_F^{\otimes 2}) & \xrightarrow[\gamma_F]{} & H^2(F, E[p]^{\otimes 2})
\end{array}$$

This Lemma follows from the compatibility of the exact sequence (3.2) (of Galois modules) with base extension.

Lemma 3.7 *In order to prove that $Im(s_p) \subset \mathrm{Im}(\gamma_F)$, it suffices to prove it for the image of symbols, i.e., that*

$$\mathrm{Im}\,(s_p(ST_{F,p}(A))) \subset \mathrm{Im}(\gamma_F),$$

where

$$ST_{F,p}(A) := \mathrm{Im}\,(ST_F(A) \to T_F(A)/p)\,.$$

Proof Use the commutativity of the diagram in Lemma 3.6 for the norm. □

This proves *Claim 3.5.* □

Lemma 3.8 *In order to prove that $Im(s_p) \subset \mathrm{Im}(\gamma_F)$, we may assume that $\mu_p \subset F$ and that $\nu = 1$, i.e., that we have the following exact sequence for groupschemes over S:*

$$0 \to \mu_{p,S} \to \mathcal{E}[p] \to (\mathbb{Z}/p)_S \to 0. \tag{$*$}$$

Proof There is a finite extension K/F such that $(*)$ holds over K, with $p \nmid [K : F]$. Now use the diagram(s) in Lemma 3.6 as follows: Let $P, Q \in E(F) \subset E(K)$, then $\mathrm{Res}(P) = P$, $\mathrm{Res}(Q) = Q$, and we have

$$[K : F]s_{F,p}(\langle P, Q\rangle) = N\{\mathrm{Res}(s_{F,p}(\langle P, Q\rangle\},$$

which equals

$$N\{s_{K,p}\,(\langle \mathrm{Res}(P), \mathrm{Res}(Q)\rangle)\} = N\{s_{K,p}(\langle P, Q\rangle)\}.$$

Therefore, if $s_{K,p}(\langle P, Q\rangle) \subset \mathrm{Im}(\gamma_K)$, then (again by using Lemma 3.6 for norm) we see that $N\{s_{K,p}(\langle P, Q\rangle)\}$ is contained in $\mathrm{Im}(\gamma_F)$. Hence $[K : F]s_{F,p}(\langle P, Q\rangle)$ lies in $\mathrm{Im}(\gamma_F)$. Finally, since $p \nmid [K : F]$, $s_{F,p}(\langle P, Q\rangle)$ itself belongs to $\mathrm{Im}(\gamma_F)$. □

3.9 Proof of Proposition 3.4. Since we may take $\mu_p \subset F$ and $\nu = 1$, the exact sequence $(*)$ in Lemma 3.8 holds, compatibly with the corresponding one over F of $\mathrm{Gal}(\overline{F}/F)$-modules. Taking cohomology, we get a commutative diagram of $\mathbb{F}_p$-vector spaces with exact rows:

$$\begin{array}{ccccccc}
\mathcal{O}_F^*/p & \to & E(F)/p & \to & \mathbb{Z}/p & & \\
\downarrow & & \downarrow & & \downarrow & & \\
\overline{H}^1(F, \mu_p) & \to & \overline{H}^1(F, E[p]) & \to & \overline{H}^1(F, \mathbb{Z}/p) & \to & 0
\end{array}$$

Here the vertical maps are isomorphisms (see the Appendix), which induce the horizontal maps on the top row.

Definition 3.10 *Put*

$$U_F := \mathrm{Im}\,(\mathcal{O}_F^*/p \to E(F)/p)\,,$$

and choose a non-canonical decomposition

$$E(F)/p \simeq U_F \oplus W_F, \quad \text{with} \quad W_F \simeq \mathbb{Z}/p.$$

Notation 3.11 If S_1, S_2 are subsets of $E(F)/p$, we denotes by $\langle S_1, S_2\rangle$ the subgroup of $ST_{F,p}(A)$ generated by the symbols $\langle s_1, s_2\rangle$, with $s_1 \in S_1$ and $s_2 \in S_2$.

Lemma 3.12 *$ST_{F,p}(A)$ is generated by the two vector subspaces*

$$\Sigma_1 := \langle U_F, E(F)/p\rangle \quad \text{and} \quad \Sigma_2 := \langle E(F)/p, U_F\rangle.$$

Proof $ST_{F,p}(A)$ is clearly generated by Σ_1, Σ_2 and by $\langle W_F, W_F\rangle$. However, W_F is one-dimensional and the pairing $\langle \cdot, \cdot \rangle$ is skew-symmetric, so $\langle W_F, W_F\rangle = 0$. $\square$

Now we have a commutative diagram
(3.13-i)

$$\begin{array}{ccc} \mathcal{O}_F^*/p \otimes E(F)/p & \xrightarrow{\alpha_1} & E(F)/p \otimes E(F)/p \\ \Big\downarrow{\scriptstyle \sigma_1} & & \Big\downarrow{\scriptstyle s_p} \\ H^2(F, \mu_p \otimes E[p]) & \xrightarrow{\beta_1} & H^2(F, E[p]^{\otimes 2}), \end{array}$$

where the top map α_1 factors as

$$\mathcal{O}_F^*/p \otimes E(F)/p \to U_F \otimes E(F)/p \to E(F)/p \otimes E(F)/p.$$

We also get a similar diagram (3.13-ii) by replacing $\mathcal{O}_F^*/p \otimes (E(F)/p)$ (resp. $U_F \otimes (E(F)/p)$) by $(E(F)/p) \otimes \mathcal{O}_F^*/p$ (resp. $(E(F)/p) \otimes U_F$). The maps α_j and their factoring are obvious, s_p is the map constructed in section 2, and the vertical maps σ_j are defined entirely analogously.

Lemma 3.14 *The image of* $s_p : ST_{F,p}(A) \to H^2(F, E[p]^{\otimes 2})$ *is generated by* $\beta_1(Im(\sigma_1))$ *and* $\beta_2(Im(\sigma_2))$.

Proof Immediate by Lemma 3.12 together with the commutative diagrams (3.13-i) and (3.13-ii). $\square$

Tensoring the exact sequence

$$0 \to \mu_p \to E[p] \to \mathbb{Z}/p \to 0 \tag{3.15}$$

with μ_p from the left and the right, and taking Galois cohomology, we get two natural homomorphisms

$$\gamma_1 : H^2(F, \mu_p^{\otimes 2}) \to H^2(F, \mu_p \otimes E[p]) \tag{3.16-i}$$

and

$$\gamma_2 : H^2(F, \mu_p^{\otimes 2}) \to H^2(F, E[p] \otimes \mu_p). \tag{3.16-ii}$$

Lemma 3.17 $\mathrm{Im}(\sigma_j) \subset \mathrm{Im}(\gamma_j)$, *for* $j = 1, 2$.

Proof of Lemma 3.17 We give a proof for $j = 1$ and leave the other (entirely similar) case to the reader. By tensoring (3.15) by μ_p, we obtain the following exact sequence of G_F-modules:

$$0 \to \mu_p^{\otimes 2} \to \mu_p \otimes E[p] \to \mu_p \to 0 \tag{3.18}$$

Consider now the following commutative diagram, in which the bottom row is exact:
(3.19)

$$\begin{array}{ccccc} & & U_F \otimes E(F)/p & & \\ & & \Big\downarrow{\scriptstyle \tilde{\sigma}_1} & & \\ & & \overline{H}^2(F, \mu_p \otimes E[p]) & \xrightarrow{\varepsilon_0} & \overline{H}^2(F, \mu_p) \\ & & \Big\downarrow{\scriptstyle i_1} & & \Big\downarrow \\ H^2(F, \mu_p^{\otimes 2}) & \xrightarrow{\gamma_1} & H^2(F, \mu_p \otimes E[p]) & \xrightarrow{\varepsilon} & H^2(F, \mu_p) \end{array}$$

where $\sigma_1 = i_1 \circ \tilde{\sigma}_1$ is the map from (3.13-i).

To begin, the exactness of the bottom row follows immediately from the exact sequence (3.18). The factorization of σ_1 is the crucial point, and this holds because U_F comes from $\mathcal{O}_F^*/p$ and is mapped to $H^1(F, \mu_p)$ via $\overline{H}^1(F, \mu_p)$, which is the image of $H^1_{\mathrm{fl}}(S, \mu_p)$ (see Lemma A.3.1 in the Appendix). Similarly, $E(F)/p \simeq \mathcal{E}(S)/p$ maps into $\overline{H}^1(F, E[p])$, the image of $H^1_{\mathrm{fl}}(S, \mathcal{E}[p])$; therefore the tensor product maps into $\overline{H}^2(F, \mu_p \otimes E[p])$, the image of $H^2_{\mathrm{fl}}(S, \mu_p \otimes \mathcal{E}[p])$.

To prove Lemma 3.17, it suffices, by the exactness of the bottom row, to see that $\mathrm{Im}(\sigma_1)$ is contained in $\mathrm{Ker}(\varepsilon)$, i.e., to see that $\varepsilon \circ \sigma_1 = 0$. Luckily for us, this composite map factors through $\varepsilon_0 \circ \tilde{\sigma}_1$, which vanishes because $H^2_{\mathrm{fl}}(S, \mu_{p,S})$, and hence $\overline{H}^2(F, \mu_p)$, is zero by [Mi2], part III, Lemma 1.1. □

Putting these Lemmas together, we get the truth of Proposition 3.4.

3.20 Proof of Proposition C. As we saw earlier, Proposition 3.4, which has now been proved, implies (by Claim 3.5) part (a) of Proposition C. So we need to prove only part (b).

By part (a) of Prop. C, the dimension of the image of s_p is at most that of $H^2(F, C^{\otimes 2})$. Since $E[p]$ is selfdual, the short exact sequence (3.2) shows that the Cartier dual of C is C'. It follows easily that $(C^{\otimes 2})^D$ is $C'^{\otimes 2}(-1)$. By the local duality, we then get

$$H^2(F, C^{\otimes 2}) \simeq H^0(F, C'^{\otimes 2}(-1))^\vee,$$

As C' is a line over $\mathbb{F}_p$ with G_F-action, the dimension of the group on the right is less than or equal to 1, with equality holding iff $C'^{\otimes 2} \simeq \mu_p$.

Since G_F acts on C' by an unramified character ν, for $C'^{\otimes 2}$ to be μ_p as a G_F-module, it is necessary that $\mu_p \subset F$. So

$$\mu_p \not\subset F \implies \mathrm{Im}(s_p) = 0.$$

Now suppose $\mu_p \subset F$. Then for $\mathrm{Im}(s_p)$ to be non-zero, it is necessary that $C'^{\otimes 2} \simeq \mathbb{Z}/p$, implying that $\nu^2 = 1$. □

4 Vanishing of s_p in the wild case

We start with a simple Lemma, doubtless known to experts.

Lemma 4.0 *Let E/F be ordinary. Then the Galois representation on $E[p]$ is one of the following (disjoint) types:*

(i) *The wild inertia group I_p acts non-trivially, making $E[p]$ non-semisimple;*
(ii) *$E[p]$ is semisimple, in which case $p \nmid F(E[p]) : F]$;*
(iii) *$E[p]$ is unramified and non-semisimple, in which case $[F(E[p]) : F] = p$.*

In case (i), we will say that we are in the *wild case*.

Proof Clearly, when I_p acts non-trivially, the triangular nature of the representation on $E[p]$ makes $E[p]$ non-semisimple. Suppose from here on that I_p acts trivially. If $E[p]$ is semisimple, $F(E[p])/F$ is necessarily a prime-to-p extension, again because the representation is solvable in the ordinary case. This leaves the final possibility when $E[p]$ is non-semisimple, but I_p acts trivially. We claim that the tame inertia group I_t also acts trivially. Since $I_t \simeq \lim_m \mathbb{F}_{p^m}^*$, its image in $\mathrm{GL}_2(\mathbb{F}_p)$ ($\simeq \mathrm{Aut}(E[p])$) will have prime-to-$p$ order, and so must be (conjugate to) a subgroup H of the diagonal group $D \simeq (\mathbb{F}_p^*)^2$. H cannot be central, as the semisimplification is a direct sum of two characters, at most one of which is ramified, and for the same reason, H cannot be all of D. It follows that, when I_t acts non-trivially, H must be conjugate to

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in C \subset \mathbb{F}_p^* \right\},$$

for a subgroup $C \neq \{1\}$ of $\mathbb{F}_p^*$. An explicit calculation shows that any element of $\mathrm{GL}_2(\mathbb{F}_p)$ normalizing H must be contained in the group generated by D and the Weyl element $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Again, since the representation is triangular, w cannot be in the image. Consequently, if I_t acts non-trivially, the image of $\mathcal{G}_k$ must also be in D, implying that $E[p]$ is semisimple, whence the claim. Thus in the third (and last) case, $E[p]$ must be unramified and non-semisimple. As $\mathcal{G}_k$ is pro-cyclic, the only way this can happen is for the image to be unipotent of order p. $\square$

Remark An example of Rubin shows that for a suitable, ordinary elliptic curve E over a p-adic field, we can be in case (iii). To see this, start with an example E/F in case (i), with E[p] unipotent and non-trivial, which is easy to produce. Let L be the ramified extension of F of degree p obtained by trivializing $E[p]$. Let K be the unique unramified extension of F of degree p, and let M be an extension of F of degree p inside the compositum LK, different from both L and K. Then over M, $E[p]$ has the form we want. Since M does not contain L, $E[p]$ is a non-trivial $\mathcal{G}_M$-module. On the other hand, this representation (of $\mathcal{G}_M$) is unramified because all the p-torsion is defined over the unramified extension MK of M, which contains L.

The object of this section is to prove the following:

Proposition D *Suppose E/F is an elliptic curve (with good ordinary reduction) over a non-archimedean local field F of odd residual characteristic p. Assume that we are in the wild case. Then we have*

$$s_p(T_F(E \times E)/p) \,=\, 0.$$

Combining this with Proposition C, we get the following

Corollary 4.1 *Let F be a non-archimedean local field with residual characteristic $p > 2$, and E an elliptic curve over F with good, ordinary reduction. If $Im(s_p)$ is non-zero, then either $[F(E[p]) : F] \leq 2$ or $F(E[p])$ is an unramified p-extension.*

Indeed, if $\mathrm{Im}(s_p)$ is non-zero, Proposition D says that I_p acts trivially on $E[p]$. If the $\mathrm{Gal}(\overline{F}/F)$- action on $E[p]$ is semisimple, then by Proposition C, $[F(E[p]) : F] \leq 2$. Since the tame inertia group has order prime to p, the only other possibility, thanks to Lemma 4.0, is for $E[p]$ to be non-semisimple and unramified. As the residual Galois group is cyclic, this also forces $[F(E[p]) : F] = p$. Hence the Corollary (assuming the truth of Proposition D).

Proof of Proposition D Let us first note a few basic things concerning base change to a finite extension K/F of degree m prime to p. To begin, since E/F has ordinary reduction, the Galois representation ρ_F on $E[p]$ is triangular, and it is semisimple iff the image does not contain any element of order p. It follows that ρ_K is semisimple iff ρ_F is semisimple. Moreover, the functoriality of the Galois symbol map relative to the respective norm and restriction homomorphisms, together with the fact that the composition of restriction with norm is multiplication by m, implies, as $p \nmid m$, that for any $\theta \in T_F(E \times E)/p$, we have

$$s_{p,K}(\mathrm{res}_{K/F}(\theta)) = 0 \implies s_p(\theta) = 0.$$

So it suffices to prove Proposition D, after possibly replacing F by a finite prime-to-p extension, under the assumption that F contains μ_p *and* $\nu = 1$, still with $E[p]$ non-semisimple and wild. Thus we have a non-split, short exact sequence of finite flat groupschemes over S:

$$0 \to \mu_{p,S} \to \mathcal{E}[p] \to (\mathbb{Z}/p)_S \to 0, \tag{4.2}$$

with the representation ρ_F of $G = \mathrm{Gal}(\overline{F}/F)$ on $E[p]$ having the form:

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \tag{4.3}$$

relative to a suitable basis. Here $\alpha : G \to \mathbb{Z}/p$ is a non-zero homomorphism, and $F(\alpha)$, the smallest extension of F over which α becomes trivial, is a ramified p-extension.

Using the exact sequence (4.2), both over S and over F, we get the following commutative diagram:

$$\begin{array}{ccccccccc}
\mathcal{E}[p](S) & \xrightarrow{0} & \mathbb{Z}/p & \to & H^1_{\mathrm{fl}}(S,\mu_p) & \xrightarrow{\psi_S} & H^1_{\mathrm{fl}}(S,\mathcal{E}[p]) & \twoheadrightarrow & H^1_{\mathrm{fl}}(S,\mathbb{Z}/p) \\
\| & & \| & & \downarrow & & \downarrow & & \downarrow \\
E[p](F) & \xrightarrow{0} & \mathbb{Z}/p & \to & H^1(F,\mu_p) & \xrightarrow{\psi} & H^1(F,E[p]) & \to & H^1(F,\mathbb{Z}/p) \\
 & & & & \| & & \cap & & \\
 & & & & X+Y & & Z=\psi(Y) & &
\end{array} \tag{4.4}$$

where $X \subset \overline{H}^1(F,\mu_p) \subset H^1(F,\mu_p)$ is the subspace given by the image of $\mathbb{Z}/p$. Since μ_p is in F, we can identify $H^2(F,\mu_p^{\otimes 2})$ with $\mathrm{Br}_F[p] \simeq \mathbb{Z}/p$. By our assumption, $X \neq 0$ as the sequence (4.2) does *not* split. Now take $e \in X$, with $e \neq 0$. Then

$$e \in \mathcal{O}_F^*/p \subset F^*/F^{*p} = H^1(F,\mu_p).$$

Since $K = F(e^{1/p})$ is clearly the smallest extension of F over which (4.2) splits, K is also $F(\alpha)$ and hence a ramified p-extension of F, since the Galois representation on $E[p]$ is wild. Then, applying [Se2], Prop.5 (iii), we get a $v \in \overline{H}^1(F,\mu_p)$ which is not a norm from K, and so the cup product $\{e,v\}$ is non-zero in $\mathrm{Br}_F[p]$ (cf. [Ta1], Prop.4.3).

Now consider the commutative diagram

$$\begin{array}{ccc}
H^1(F,\mu_p)^{\otimes 2} & \xrightarrow{\cup} & H^2(F,\mu_p^{\otimes 2}) \\
{\scriptstyle\psi^{\otimes 2}}\downarrow & & \downarrow{\scriptstyle\gamma} \\
H^1(F,E[p])^{\otimes 2} & \xrightarrow{\cup} & H^2(F,E[p]^{\otimes 2})
\end{array} \tag{4.5}$$

where ψ is the map defined in the previous diagram, and $\gamma = \gamma_F$ is the map defined in section 3 with $C_F = \mu_p$ and $C'_F = \mathbb{Z}/p$. By Proposition C, the image of s_p is contained in that of γ. On the other hand, $\psi(e) \cup \psi(v) = 0$ because $\psi(e) = 0$. Hence $\gamma(\{e, v\}) = 0$, and the image of s_p is zero as asserted. $\square$

5 Non-trivial classes in Im(s_p) in the non-wild case with $[F(E[p]) : F]' \leq 2$

For any finite extension K/F, we will write $[K : F]'$ for the prime-to-p degree of K/F.

Proposition E *Let E be an elliptic curve over a non-archimedean local field F of residual characteristic $p \neq 2$. Assume that E has good ordinary reduction, with trivial action on I_p on $E[p]$, such that*

(a) $[F(E[p]) : F]' \leq 2$;
(b) $\mu_p \subset F$.

Then Im$(s_p) \neq 0$. Moreover, if $F(E[p]) = F$, i.e., if all the p-division points are rational over F, then there exist points P, Q of $E(F)/p$ such that

$$s_p(\langle P, Q\rangle) \neq 0.$$

In this case, up to replacing F by a finite unramified extension, we may choose P to be a p-power torsion point.

Proof First consider the case when $E[p]$ is semisimple, so that $[K : F]' = [K : F] \leq 2$, where $K := F(E[p])$.

Suppose K is quadratic over F. Recall that over F, C_F (resp. C'_F) is given by the character $\chi\nu^{-1}$ (resp. ν), and since $\mu_p \subset F$ and ν quadratic, we have

$$H^2(F, C_F^{\otimes 2}) \simeq H^2(F, \mu_p) = Br_F[p] \simeq \mathbb{Z}/p.$$

Suppose we have proved the existence of a class θ_K in $T_K(E \times E)/p$ such that $s_{p,K}(\theta_K)$ is non-zero, and this image must be, thanks to Proposition C, in the image of a class t_K in $Br_K[p]$. Put $\theta := N_{K/F}(\theta_K) \in T_F(E \times E)/p$. Then $s_p(\theta)$ equals $N_{K/F}(s_{p,K}(\theta_K))$, which is in the image of $t := N_{K/F}(t_K) \in Br_F[p]$, which is non-zero because the norm map on the Brauer group is an isomorphism.

So we may, and we will, assume henceforth in the proof of this Proposition that $E[p]) \subset F$, i.e., $K = F$.

Now let us look at the basic setup carefully. Since E has good reduction, the Néron model is an elliptic curve over S. Moreover, since E has ordinary reduction with $E[p] \subset F$, we also have

$$\mathcal{E}[p] = (\mu_p)_S \oplus \mathbb{Z}/p$$

as group schemes over S (and as sheaves in S_{flat}). By the Appendix A.3.2,

$$E(F)/p \simeq \mathcal{E}(S)/p \xrightarrow{\partial_F} H^1_{\text{fl}}(S, \mathcal{E}[p]) = H^1_{\text{fl}}(S, \mu_p) \oplus H^1_{\text{fl}}(S, \mathbb{Z}/p), \tag{5.1}$$

where the boundary map ∂_F is an isomorphism. Moreover, the direct sum on the right of (5.1) is isomorphic to

$$H^1_{\text{fl}}(S, \mu_p) \oplus H^1_{\text{et}}(k, \mathbb{Z}/p) \simeq \mathcal{O}_F^*/p \oplus \mathbb{Z}/p,$$

thanks to the isomorphism $H^1_{\text{fl}}(S, \mu_p) \simeq \mathcal{O}_F^*/p$ and the identification of $H^1_{\text{fl}}(S, \mathbb{Z}/p)$ with $H^1_{\text{et}}(k, \mathbb{Z}/p) \simeq \mathbb{Z}/p$ ([Mi1], p. 114, Thm. 3.9). Therefore we have a 1-1 correspondence

$$\bar{P} \longleftrightarrow (\bar{u}_p, \bar{n}_p) \tag{5.2}$$

with $\bar{P} \in E(F)/p$, $\bar{u}_p \in \mathcal{O}_F^*/p$, $\bar{n}_p \in \mathbb{Z}/p$. The ordered pair on the right of (5.2) can be viewed as an element of $H^1_{\mathrm{fl}}(S, \mathcal{E}[p])$ or of its (isomorphic) image $\overline{H}^1(F, E[p])$ in $H^1(F, E[p])$.

In Galois cohomology, we have the decomposition

$$H^2(F, E[p]^{\otimes 2}) \simeq H^2(F, \mu_p^{\otimes 2}) \oplus H^2(F, \mu_p)^{\oplus 2} \oplus H^2(F, \mathbb{Z}/p). \tag{5.3}$$

We have a similar one for $H^2_{\mathrm{fl}}(S, \mathcal{E}[p]^{\otimes 2})$.

It is essential to note that by Proposition C,

$$Im(s_p) \hookrightarrow H^2(F, \mu_p^{\otimes 2}) \subset H^2(F, E[p]^{\otimes 2}), \tag{5.4 - i}$$

and in addition,

$$H^2(F, \mu_p^{\otimes 2}) \simeq H^2(F, \mu_p) = \mathrm{Br}_F[p] \simeq \mathbb{Z}/p, \tag{5.4 - ii}$$

which is implied by the fact that $\mu_p \subset F$ (since it is the determinant of $E[p]$)).

In terms of the decomposition (5.2) from above, we get, for all $P, Q \in E(F)$,

$$s_p(\langle P, Q\rangle) = \bar{u}_P \cup \bar{u}_Q \in Br_F[p] \simeq \mathbb{Z}/p. \tag{5.5}$$

$\square$

One knows that (cf. [L2], chapter II, sec. 3, Prop.6)

$$|\mathcal{O}_F^*/p| = |\mu_p(F)| p^{[F:\mathbb{Q}_p]}. \tag{5.6}$$

Since we have assumed that F contains all the p-th roots of unity, the order of $\mathcal{O}_F^*/p|$ is at least p^2.

Claim 5.7 *Let u, v be units in $\mathcal{O}_F$ which are linearly independent in the $\mathbb{F}_p$-vector space $V := \mathcal{O}_F^*/(\mathcal{O}_F^*)^p$. Then $F[u^{1/p}]$ and $F[v^{1/p}]$ are disjoint p-extensions of F.*

This is well known, but we give an argument for completeness. Pick p-th roots α, β of u, v respectively. If the extensions are not disjoint, we must have $\alpha = \sum_{j=0}^{p-1} c_j \beta^j$ in $K = F[v^{1/p}]$, with $\{c_j\} \subset F$. A generator σ of Gal$(K/F$ must send β to $w\beta$ for some p-th root of unity $w \neq 1$ (assuming, as we can, that v is not a p-th power in F), and moreover, σ will send α to $w^i \alpha$ for some i. Thus α^σ can be computed in two different ways, resulting in the identity $\sum_j c_j w^i \beta^j = \sum_j c_j w^j \beta^j$, from which the Claim follows.

Consequently, since the dimension of V is at least 2 and since F has a unique unramified p-extension, we can find $u \in \mathcal{O}_F^*$ such that $K := F[u^{1/p}]$ is a ramified p-extension. Fix such a u and let $Q \in E(F)$ be given by $(\bar{u}, 0)$. By [Se2], Prop. 5 (iii) on page 72 (see also the Remark on page 95), there exists $v \in \mathcal{O}_F^*$ s.t. $v \notin N_{K/F}(\mathcal{O}_K^*)$. Then by [Ta1], Prop. 4.3, page 266, $\{v, u\} \neq 0$ in $\mathrm{Br}_F[p]$. Take $P \in E(F)$ such that $\bar{P} \leftrightarrow (\bar{v}, 0)$ then $s_p(\langle P, Q\rangle) = \{v, u\} \in H^2(F, E[p]^{\otimes 2}) \subset \mathrm{Br}_F[p]$ and $\{v, u\} \neq 0$.

It remains to show that we may choose P to be a p-power torsion point after possibly replacing F by a finite unramified extension. Since $E[p]$ is in F, μ_p is in F; recall that $\mu_p(F) \subset E[p](F)$. So we may pick a non-trivial p-th root of unity ζ in F. Let m be the largest integer such that $\zeta := w^{p^{m-1}}$ for some $w \in F^*$; in this case w is in $F^* - F^{*p}$. Let F'/F be the unramified extension of F such that over the corresponding residual extension, all the p^m-torsion points of $\mathcal{E}_s$ are rational; note however that $\mathcal{E}[p^m]$ need not be in F. This results in the following short exact sequence:

$$0 \to \mu_{p^m} \to \mathcal{E}[p^m] \to \mathbb{Z}/p^m \to 0,$$

leading to the inclusion

$$\mu_{p^m}(F') \subset E[p^m](F').$$

Since F'/F is unramified, w cannot belong to ${F'}^{*p}$, and the corresponding point P, say, in $E[p^m](F')$ is not in $pE(F')$. Put

$$L = F'(\frac{1}{p}P) = F'(w^{1/p}),$$

which is a ramified p-extension. So there exists a unit u in $\mathcal{O}_{F'}$ such that $\{w, u\}$ is not trivial in $\mathrm{Br}_{F'}[p]$. Now let Q be a point in $E(F')$ such that its class in $E(F')/p$ is given by $(\overline{u}, 0) \in \mathcal{O}_{F'}/p \oplus \mathbb{Z}/p$. It is clear that $\langle P, Q\rangle$ is non-zero in $T_{F'}(A)/p$.

Now suppose $E[p]$ is not semisimple. Since we are not in the wild case, we know by Lemma 4.0 that $K := F(E[p])$ is an unramified p-extension of F. By the discussion above, there are points $P, Q \in E(K)/p$ such that $s_{p,K}(\langle P, Q\rangle_K) \neq 0$. Put

$$\theta := N_{K/F}(\langle P, Q\rangle_K) \in T_F(A)/p.$$

Claim: $s_p(\theta)$ is non-zero.

Since we have

$$s_p(\theta) = N_{K/F}\left(s_{p,K}(\langle P, Q\rangle_K)\right),$$

the Claim is a consequence of the following Lemma, well known to experts.

Lemma 5.8 *If $K \supset F$ is any finite extension of p-adic fields, then $N_{K/F}\colon \mathrm{Br}_K \to \mathrm{Br}_F$ is an isomorphism.*

For completeness we give a

Proof The *invariant map* $inv_F : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$ is an isomorphism and moreover (cf. [Se2], chap.XIII, Prop.7), if $n = [K : F]$, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Br}_F & \xrightarrow{\mathrm{Res}_{K/F}} & \mathrm{Br}_K \\ {\scriptstyle \mathrm{inv}_F}\downarrow & & \downarrow{\scriptstyle \mathrm{inv}_K} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

As $\mathbb{Q}/\mathbb{Z}$ is divisible, every element in Br_K is the restriction of an element in Br_F. Now since $\mathrm{Res}_{K/F}\colon \mathrm{Br}(F) \to \mathrm{Br}(K)$ is already multiplication by n in $\mathbb{Q}/\mathbb{Z}$, the projection formula $N_{K/F} \circ \mathrm{Res}_{K/F} = [K : F]\mathrm{Id} = n\mathrm{Id}$ implies that the norm $N_{K/F}$ on Br_K must correspond to the identity on $\mathbb{Q}/\mathbb{Z}$.

We are now done with the proof of Proposition E.

□

6 Injectivity of s_p

Proposition F *Let E be an elliptic curve over a non-archimedean local field F of odd residual characteristic p, such that E has good, ordinary reduction. Then s_p is injective on $T_F(E \times E)/p$.*

In view of Proposition E, we have the following

Corollary 6.1 *Let F, E, p be as in Proposition E. Then $T_F(E \times E)/p$ is a cyclic group of order p. Moreover, if $E[p] \subset F$, it even consists of symbols $\langle P, Q\rangle$, with $P, Q \in E(F)/p$.*

To prove Proposition F, we will need to consider separately the cases when $E[p]$ is semisimple and non-semisimple, the latter case being split further into the wild and unramified subcases.

Proof of Proposition F in the semisimple case. Again, to prove injectivity, we may replace F by any finite extension of prime-to-p degree. Since p does not divide $[F(E[p]) : F]$ when $E[p]$ is semisimple, we may assume (in this case) that all the p-torsion points of E are rational over F.

Remark The injectivity of s_p when $E[p] \subset F$ has been announced without proof, and in fact for a more general situation, by Raskind and Spiess [R-S], but the method of their paper is completely different from ours.

There are three steps in our proof of injectivity when $E[p] \subset F$:

Step I: Injectivity of s_p on symbols

Pick any pair of points P, Q in $E(F)$. We have to show that if $s_p(< P, Q >) = 0$, then the symbol $< P, Q >$ lies in $pT_F(A)$.

To achieve Step I, it suffices to prove that the condition (a) of lemma 1.8.1 holds.

In the correspondence (5.2), let $\bar{P} \leftrightarrow (\bar{u}_P, \bar{n}_P)$ and $\bar{Q} \leftrightarrow (\bar{u}_Q, \bar{n}_Q)$. Put $K_1 = F(\sqrt[p]{u_Q})$ and take K_2 to be the unique unramified extension of F of degree p if $\bar{n}_Q \neq 0$; otherwise take $K_2 = F$. Consider the compositum K_1K_2 of K_1, K_2, and $K := F\left(\frac{1}{p}Q\right)$, all the fields being viewed as subfields of $\bar{F}$.

From (5.1) we get the following commutative diagram:

$$\begin{array}{ccccccc}
\mathcal{E}(\mathcal{O}_K)/p & \xrightarrow{\sim} & H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{E}[p]) & \simeq & \mathcal{O}_K^*/(\mathcal{O}_K^*)^p & \oplus & \mathbb{Z}/p \\
{\scriptstyle N_{K/F}}\big\downarrow \ \uparrow Res & & \uparrow Res & & {\scriptstyle N_{K/F}}\big\downarrow \ \uparrow Res & & \big\downarrow{\scriptstyle N_{K/F}=\mathrm{id}} \\
\mathcal{E}(\mathcal{O}_F)/p & \xrightarrow{\sim} & H^1_{\mathrm{fl}}(\mathcal{O}_F, \mathcal{E}[p]) & \simeq & \mathcal{O}_F^*/(\mathcal{O}_F^*)^p & \oplus & \mathbb{Z}/p.
\end{array} \tag{6.2}$$

Here the map *Res*$=$ $Res_{K/F}$ on $\mathcal{E}(\mathcal{O}_F)/p$ and $\mathcal{O}_F^*/p$ induced by the inclusion $F \hookrightarrow K$ is the obvious restriction map. However, on $\mathbb{Z}/p$, *Res* comes from the residue fields $\mathbb{F}$ of F and $\mathbb{F}'$ of K via the identifications

$$H^1_{\mathrm{fl}}(S, \mathbb{Z}/p) \simeq H^1(\mathbb{F}, \mathbb{Z}/p) \simeq \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}), \mathbb{Z}/p) \simeq \mathbb{Z}/p \tag{6.3}$$

and the corresponding one for K and $\mathbb{F}'$. As $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) = \hat{\mathbb{Z}}$, we see by taking $\mathbb{F} \subset \mathbb{F}' \subset \overline{\mathbb{F}}$ with $[\mathbb{F}' : \mathbb{F}] = d$ dividing p, that $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}')$ is the obvious subgroup of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ corresponding to $d\hat{\mathbb{Z}}$; consequently, the map *Res* on the $\mathbb{Z}/p$ summand is multiplication by d. Finally note that $N_{K/F} \circ Res_{K/F} = [K : F]\mathrm{id}$.

Lemma 6.4 *With K, K_1, K_2 as above, we have*

$$K \ = \ K_1K_2.$$

In other words we have the following diagram

$$\begin{tikzcd}
 & K = K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash, "p"'] & & K_2 \arrow[dl, dash, "p"] \\
 & F &
\end{tikzcd}$$

(If $\bar{u}_Q \neq 1$, $\bar{n}_Q \neq 0$)
$K_1 \supset F$ ramified
$K_2 \supset F$ unramified

Proof Put $L = K_1K_2$. Let ∂_L be the boundary map given by the sequence (5.1).
a) $\mathbf{K} \subset \mathbf{L}$: Apply the diagram (6.2) with L instead of K. We claim that $\partial_L(Res(Q)) = 0$ and hence $K \subset L$. If $\overline{n}_Q = 0$, so that $L = K_1$, we get $\partial_L(Res(Q)) = (Res(\overline{u}_Q), 0) = 0$. On the other hand, if $\overline{n}_Q \neq 0$, then K_2 is the unique unramified p-extension of F and the restriction map on $\mathbb{Z}/p$ is, by the remarks above, given by multiplication by p. So we still have $\partial_L(Res(Q)) = 0$, as claimed.
b) $\mathbf{K} \supset \mathbf{L}$: In this case we have $\partial_K(Res(Q)) = 0$. On the other hand,

$$\partial_K(Res(Q)) = (Res(\overline{u}_Q), Res(\overline{n}_Q)) = (0, 0).$$

Hence $K \supset K_1$. If $\overline{n}_Q = 0$, $K_2 = F$ and we are done. So suppose $\overline{n}_Q \neq 0$. Then, since $Res(\overline{n}_Q)$ is zero, we see that the residual extension of K/F must be non-trivial and so must contain the unique unramified p-extension K_2 of F. Hence K contains $L = K_1K_2$. □

Lemma 6.5 *Let P, Q be in $E(F)/p$ with coordinates in the sense of (5.2), namely $P = (\overline{u}_P, \overline{n}_P)$ and $Q = (\overline{u}_Q, \overline{n}_Q)$. Let P_0, Q_0 be the points in $E(F)/p$ with coordinates $(\overline{u}_P, 0)$, $(\overline{u}_Q, 0)$ respectively. Then*

$$\langle P, Q\rangle \;=\; \langle P_0, Q_0\rangle \;\in T_F(A)/p.$$

Proof of Lemma 6.5 Put $P_1 = (0, \overline{n}_P)$ and $Q_1 = (0, \overline{n}_Q)$. Then by linearity,

$$\langle P, Q\rangle \;=\; \langle P_0, Q_0\rangle + \langle P_1, Q_0\rangle + \langle P_0, Q_1\rangle + \langle P_1, Q_1\rangle.$$

First note that linearity,

$$\langle P_1, Q_1\rangle \;=\; \overline{n}_P\overline{n}_Q\langle (0,1), (0,1)\rangle.$$

It is immediate, since $p \neq 2$, to see that $\langle (0,1), (0,1)\rangle$ is zero by the skew-symmetry of $\langle ., .\rangle$. Thus we have, by bi-additivity,

$$\langle P_1, Q_1\rangle \;=\; 0.$$

Next we show that in $T_F(A)/p$,

$$\langle P_0, Q_1\rangle \;= 0 \;=\; \langle P_1, Q_0\rangle.$$

We will prove the triviality of $\langle P_0, Q_1\rangle$; the triviality of $\langle P_1, Q_0\rangle$ will then follow by the symmetry of the argument. There is nothing to prove if $\overline{n}_Q = 0$, so we may (and we will) assume that $\overline{n}_Q \neq 0$. Then it corresponds to the unramified p-extension $M = F\left(\frac{1}{p}Q_1\right)$ of F. It is known that every unit in F^* is the norm of a unit in M^*/p. This proves that the point P_0 in $E(F)/p$ is a norm from M. Thus $\langle P_0, Q_1\rangle$ is zero by Lemma 1.8.1. Putting everything together, we get

$$\langle P, Q\rangle \;=\; \langle P_0, Q_0\rangle$$

as asserted in the Lemma. □

Proof of Step I Let $P, Q \in E(F)/p$ be such that $s_p(\langle P, Q\rangle) = 0$. We have to show that $\langle P, Q\rangle = 0$ in $T_F(A)/p$. By Lemma 6.5 we may assume that $\overline{n}_P = \overline{n}_Q = 0$. So it follows that the element $\{\bar{u}_P, \bar{u}_Q\} := \bar{u}_P \cup \bar{u}_Q$ is zero in the Brauer group $\mathrm{Br}_F[p]$. Then putting $K_1 = K\left(u_Q^{1/p}\right)$, we have by [Ta1], Prop. 4.3, we have $u_P = N_{K_1/F}(u_1')$ with $u_1' \in K_1^*$ and where $u_P \in \mathcal{O}_F^*$ with image $\bar{u}_P$. It follows that u_1' must also be a unit in $\mathcal{O}_{K_1}$. Now with the notations introduced at the beginning of *Step I* we have, since $\overline{n}_Q = 0$, that $K = K_1$ and so $[K : F] = p$. In the diagram

(6.2), take in the upper right corner the element $(\overline{u'}, 0)$. Then we get an element $\overline{P'} \in E(K)/p$ such that $N_{K/F}\overline{P'} \equiv P \pmod{p}$. Hence condition (a) of Lemma 1.8.1 holds, yielding Step I. □

Step II:

Put

$$\mathrm{ST}_{F,p}(A) \;=\; \mathrm{Im}\,(\mathrm{ST}_F(A) \;\to\; T_F(A)/p)$$

Lemma 6.6 *s_p is injective on $\mathrm{ST}_{F,p}(A)$.*

Proof This follows from

Claim: If V is an $\mathbb{F}_p$-vector space with an alternating bilinear form $[\quad,\quad]\colon V \times V \to W$, with W a 1-dimensional $\mathbb{F}_p$-vector space, then the conditions (i) and (ii) of [Ta1], p. 266, are satisfied, which in our present setting read as follows :

(i) Given a, b, c, d in V such that $[a, b] = [c, d]$, then there exist elements x and y in V such that

$$[a, b] = [x, b] = [x, y] = [c, y] = [c, d].$$

(ii) Given a_1, a_2, b_1, b_2 in V, there exist c_1, c_2 and d in V such that

$$[a_1, b_1] = [c_1, d], \text{ and } [a_2, b_2] = [c_2, d].$$

□

Proof Recall that we are assuming in this paper that p is odd. The Claim is just Proposition 4.5 of [Ta1], p. 267. The proof goes through verbatim. In our case we apply this to $V = E(F)/p, W = \mathrm{Br}_F[p]$ and $[\bar{P}, \bar{Q}] = s_p(\langle P, Q\rangle) = \bar{u}_P \cup \bar{u}_Q$. By ([Ta1], Corollary on p. 266), the s_p is injective on $\mathrm{ST}_{F,p}(A)$. □

Step III: Injectivity of s_p in the general case (but still assuming $E[p] \subset F$).

For this we shall appeal to Lemma 5.8.

Proof of Step III By Step II, we see from Lemma 1.7.1 that it suffices to prove the following result, which may be of independent interest.

Proposition 6.7 *Let $K \supset F$ be a finite extension, and $E[p] \subset F$. Then $N_{K/F}(\mathrm{ST}_{K,p}(A))$ is a subset of $\mathrm{ST}_{F,p}(A)$ and hence*

$$\mathrm{ST}_{F,p}(A) \;=\; T_F(A)/p.$$

In other words, $T_F(A)$ is generated by symbols modulo $pT_F(A)$.

It is an open question as to whether $T_F(A)$ is different from $\mathrm{ST}_F(A)$, though many expect it to be so.

Proof of Proposition 6.7 We have to prove that if $P', Q' \in E(K)$, then the norm to F of $\langle P', Q'\rangle$ is mapped into $\mathrm{ST}_{F,p}(A)$. Since we have

$$\mathrm{Im} s_p(\mathrm{ST}_F(A)) \;=\; \mathrm{Im} s_p(T_F(A)/p \;\simeq\; \mathbb{Z}/p,$$

the assertion is a consequence of the following

Lemma 6.8 *If $[K\colon F] = n$ and $P', Q' \in E(K)$, $P, Q \in E(F)$ are such that*

$$s_{p,F}(N_{K/F}\,\langle P', Q'\rangle) \;=\; s_{p,F}(\langle P, Q\rangle),$$

then, assuming that all the p-torsion in $E(\overline{F})$ is F-rational,

$$N_{K/F}(\langle P', Q'\rangle) \equiv \langle P, Q\rangle \ (\mathrm{mod}\, p\, T_F(A))$$

.

Proof of Lemma 6.8. We start with a few simple sublemmas.

Sublemma 6.9 *If K/F is unramified, then Lemma 6.8 is true.*

Proof Indeed, in this case, every point in $E(F)$ is the norm of a point in $E(K)$ (cf. [Ma], Corollary 4.4). So we can write $P \equiv N_{K/F}(P_1)(\mathrm{mod} pE(K))$ with $P_1 \in E(K)$, from which it follows that

$$N_{K/F}(\langle P_1, Q\rangle) \equiv \langle P, Q\rangle\, (\mathrm{mod} pT_F(A)).$$

On the other hand, by the remark above (in the beginning of Step III) about the norm map on the Brauer group, we have

$$s_{p,K}(\langle P_1, Q\rangle) = s_{p,K}(\langle P', Q'\rangle)$$

and applying Step II to $\langle P_1, Q\rangle$ and $\langle P', Q'\rangle$ for K, we are done. □

Subemma 6.10 *If $K/F = n$ with $p \nmid n$, then Lemma 6.8 is true.*

Proof Indeed, as the cokernel of $N_{K/F}$ is annihilated by n which is prime to p, the norm map on $E(K)/p$ is surjective onto $E(F)/p$. Let $P_1 \in E(K)$ satisfy $P \equiv N_{K/F}(P_1)(\mathrm{mod} pE(F))$. Then by the projection formula,

$$\langle P, Q\rangle \equiv N_{K/F}(\langle P_1, Q\rangle)\, (\mathrm{mod} pT_F(A)). \qquad (*)$$

Since $s_{p,F} \circ N_{K/F} = N_{K/F} \circ s_{p,K}$ and since $N_{K/F}$ is non-trivial, and hence an isomorphism, on the one-dimensional $\mathbb{F}_p$-space $\mathrm{Br}_K[p]$, we see that

$$s_{p,K}(\langle P', Q'\rangle) = s_{p,K}(\langle P_1, Q\rangle).$$

Applying Lemma 6.6 for K we see that $\langle P', Q'\rangle)$ equals $\langle P_1, Q\rangle$ in $T_K(A)/p$. Now we are done by $(*)$. □

Sublemma 6.11 *If $K \supset F_1 \supset F$ and if 6.8 is true for both the pairs K/F_1 and F_1/F, then it is true for K/F.*

Proof Let $P, Q \in E(F)$ and $P', Q' \in E(K)$ be such that

$$s_{p,F}(N_{K/F}\, \langle P', Q'\rangle) = s_{p,F}(\langle P, Q\rangle). \qquad (a)$$

Applying Proposition E with F_1 in the place of F, we get points P_1, Q_1 in $E(F_1)$ such that

$$s_{p,F_1}(\langle P_1, Q_1\rangle) = N_{K/F_1}(s_{p,K}(\langle P', Q'\rangle)). \qquad (b)$$

Since the right hand side is the same as $s_{p,F_1}(N_{K/F_1}(\langle P', Q'\rangle))$, we may apply 6.8 to the pair K/F_1 to conclude that

$$\langle P_1, Q_1\rangle = N_{K/F_1}(\langle P', Q'\rangle). \qquad (c)$$

Applying $N_{F_1/F}$ to both sides of (b), using the facts that the norm map commutes withs_p and that $N_{K/F} = N_{K/F_1} \circ N_{F_1/F}$, and appealing to (a), we get

$$s_{p,F}(N_{F_1/F}\, \langle P_1, Q_1\rangle) = s_{p,F}(\langle P, Q\rangle). \qquad (d)$$

Applying (6.8) to F_1/F, we then get

$$\langle P, Q\rangle = N_{F_1/F}(\langle P_1, Q_1\rangle). \qquad (e)$$

The assertion of the Sublemma now follows by combining (c) and (e). $\square$

Sublemma 6.12 *It suffices to prove 6.8 for all finite Galois extensions K'/F' with $E[p] \subset F'$ and $[F' : \mathbb{Q}_p] < \infty$.*

Proof Assume 6.8 for all finite Galois extensions K'/F' as above. Let K/F be a finite, non-normal extension with Galois closure L, and let $E[p] \subset F$. Suppose $P, Q \in E(F)$ and $P', Q' \in E(K$ satisfy the hypothesis of 6.8. We may use the surjectivity of $N_{L/K} : \mathrm{Br}_L \to \mathrm{Br}_K$ and Proposition E (over L) to deduce the existence of points $P'', Q'' \in E(L)$ such that

$$s_{p,K}(N_{L/K} \langle P'', Q'' \rangle) = s_{p,K}(\langle P', Q' \rangle).$$

As L/K is Galois, we have by hypothesis,

$$N_{L/K}(\langle P'', Q'' \rangle) = \langle P', Q' \rangle \,. \tag{i}$$

By construction, we also have

$$s_{p,F}(N_{L/F} \langle P'', Q'' \rangle) = s_{p,F}(\langle P, Q \rangle).$$

As L/F is Galois, we have

$$N_{L/F}(\langle P'', Q'' \rangle) = \langle P, Q \rangle \,. \tag{ii}$$

The assertion now follows by applying $N_{K/F}$ to both sides of (i) and comparing with (ii). $\square$

Thanks to this last sublemma, we may assume that K/F is Galois. Appealing to the previous three sublemmas, we may assume that we are in the following **key case**:

($\mathcal{K}$) *K/F is a totally ramified, cyclic extension of degree p, with $E[p] \subset F$*

So it suffices to prove the following

Lemma 6.13 *6.8 holds in the key case ($\mathcal{K}$).*

Proof Suppose K/F is a cyclic, ramified p-extension with $E[p] \subset F$, and let $P, Q \in E(F)$, $P', Q' \in E(K)$ satisfy the hypothesis of 6.8. Since $\mu_p = \det(E[p])$, the p-th roots of unity are in F and so

$$W := F^*/p = H^1(F, \mu_p) \simeq H^1(F, \mathbb{Z}/p) = \mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), \mathbb{Z}/p).$$

In other words, lines in W correspond to cyclic p-extensions of F, and we can write $K = F\left(u^{1/p}\right)$ for some $u \in \mathcal{O}_F^*$. For every $w \in \mathcal{O}_F^*$, let $\overline{w}$ denote its image in W. Put $m = \dim_{\mathbb{F}_p} W$. Then $m \geq 3$ by [L2], chapter II, sec. 3, Proposition 6. Let W_1 denote the line spanned in W by the unique unramified p-extension of F. Since $m > 2$, we can find some $v \in \mathcal{O}_F^*$ such that $\overline{v}$ is not in the linear span of W_1 and $\overline{u}$. Using the *Claim* stated in the proof of Proposition E, we see that $L := F\left(v^{1/p}\right)$ is linearly disjoint from K over F. Both K and L are totally ramified p-extensions of F, and so is the (p,p)-extension KL. Then KL/K is a cyclic, ramified p-extension, and by local class field theory ([Se2], chap. V, sec 3), there exists $y \in \mathcal{O}_K^*$ not lying in $N_{KL/K}((KL)^*)$. Hence $\overline{v} \cup \overline{y}$ is non-zero in $\mathrm{Br}_K[p]$ (see [Ta1], Prop.4.3, p.266, for example). Let $P_1 \in E(F)$ and $Q_1 \in E(K)$ be such that in the sense of (5.2) we have

$$\overline{P}_1 \leftrightarrow (\overline{v}, 0), \ \overline{Q}_1 \leftrightarrow (\overline{y}, 0).$$

Then

$$s_{p,K}(\langle P_1, Q_1\rangle) = \overline{v} \cup \overline{y} \neq 0.$$

Since $\mathrm{Br}_K[p]$ is one-dimensional (over $\mathbb{F}_p$), we may replace Q_1 by a multiple and assume that

$$s_{p,K}(\langle P_1, Q_1\rangle) = s_{p,K}(\langle P', Q'\rangle).$$

Hence

$$\langle P_1, Q_1\rangle \equiv \langle P', Q'\rangle \mod pT_K(A)$$

by *Step II* for K. So we get by the hypothesis,

$$s_{p,F}(N_{K/F}\langle P_1, Q_1\rangle) = s_{p,F}(\langle P, Q\rangle).$$

But P_1 is by construction in $E(F)$, and so the projection formula says that

$$N_{K/F}\langle P_1, Q_1\rangle = \langle P_1, N_{K/F}(Q_1)\rangle.$$

Now we are done by applying *Step II* to F. □

Now we have completed the proof of Proposition F when $E[p]$ is semisimple.

Proof of Proposition F in the non-semisimple, unramified case. In this case $K := F(E[p])$ is an unramified p-extension of F. By Mazur ([Ma]), we know that as E/F is ordinary, the norm map from $E(K)$ to $E(F)$ is surjective. This shows the injectivity on symbols, giving Step I in this case. Indeed, if $s_p(\langle P, Q\rangle) = 0$ for some $P, Q \in E(F)/p$, we may pick an $R \in E(K)$ with norm Q and obtain

$$N_{K/F}(s_p(\langle P, R\rangle_K)) = s_p(\langle P, N_{K/F}(R)\rangle) = 0.$$

On the other hand, the norm map on the Brauer group is injective (cf. Lemma 5.8). This forces $s_p(\langle P, R\rangle_K)$ to be non-zero. As $E[p]$ is trivial over K, the injectivity in the semisimple situation gives the triviality of $\langle P, R\rangle_K = 0$.

The proof of injectivity on $ST_{F,p}(A)$ (Step II) is the same as in the semisimple case.

The proof of injectivity on $T_F(A)/p$ (Step III) is an immediate consequence of the following Lemma (and the proof in the semisimple case).

Lemma 6.14 *Let $\theta \in T_F(A)/p$. Then $\exists\, \tilde{\theta} \in T_K(A)/p$ such that $\theta = N_{K/F}(\tilde{\theta})$.*

Proof of Lemma In view of Lemma 1.7.1, it suffices to show, for any finite extension L/F and points $P, Q \in E(L)/p$, that $\beta := N_{L/F}(\langle P, Q\rangle_L)$ is a norm from K. This is obvious if L contains K. So let L not contain K, and hence is linearly disjoint from K over F (as K/F has prime degree). Consider the compositum $M = LK$, which is an unramified p-extension of L. By Mazur ([Ma]), we can write $Q = N_{M/L}(R)$, for some $R \in E(M)/p$. Put

$$\tilde{\beta} := N_{M/K}(\langle P, R\rangle_M) \in T_K(A)/p.$$

Then, using $N_{L/F} \circ N_{M/L} = N_{M/F} = N_{K/F} \circ N_{M/K}$, we obtain the desired conclusion

$$\beta = N_{L/F}\left(\langle P, N_{M/L}(R)\rangle_L\right) = N_{M/F}\left(\langle P, R\rangle_M\right) = N_{K/F}(\tilde{\theta}).$$

□

This finishes the proof when $E[p]$ is non-semisimple and unramified.

Proof of Proposition F in the non-semisimple, wild case. Here K/F is a wildly ramified extension, so we cannot reduce to the case $E[p] \subset F$. Still, we may, as in section 4, assume that $\mu_p \subset F$ and that $\nu = 1$, which implies that the p-torsion points of the special fibre $\mathcal{E}_s$ are rational over the residue field $\mathbb{F}_q$ of F. We have in effect (4.2) through (4.4).

Consider the commutative diagram (4.4). We can write

$$\mathcal{O}_F^*/p \;=\; H^1_{\mathrm{fl}}(S, \mu_p) \;\simeq\; \overline{H}^1(F, \mu_p) \;=\; X + Y_S,$$

with $X \simeq \mathbb{Z}/p$ and Y_S some complement. Furthermore, we have (cf. [Mi1], Theorem 3.9, p.114)

$$H^1_{\mathrm{fl}}(S, \mathbb{Z}/p) \;\simeq\; H^1_{\mathrm{et}}(k, \mathbb{Z}/p) \;=\; \mathbb{Z}/p.$$

Hence

$$H^1_{\mathrm{fl}}(S, \mathcal{E}[p]) \;=\; Z_S \oplus \mathbb{Z}/p, \quad \text{where} Z_S = \psi_S(Y_S). \tag{6.15}$$

(Note that the surjectivity of the right map on the top row of the diagram (4.4) comes from the fact that $H^2_{\mathrm{fl}}(S, \mu_p)$ is 0 ([Mi2], chapter III, Lemma 1.1). Recall (cf. (6.2)) that $E(F)/p$ is isomorphic to $H^1_{\mathrm{fl}}(S, \mathcal{E}[p])$. So by (6.15), we have a bijective correspondence

$$P \;\longleftrightarrow\; (\tilde{u}_P, \overline{n}_P) \tag{6.16}$$

where P runs over points in $E(F)/p$. Compare this with (5.2).

Lemma 6.17 *Fix any odd prime p. Let K be an arbitrary finite extension of F where $E[p]$ remains non-semisimple as a G_K-module. Suppose $\langle (u', 0), (u'', 0)\rangle \;=\; 0$ in $T_K(A)/p$ for all $u', u'' \in \mathcal{O}_K^*/p$. Then $\langle P, Q\rangle \;=\; 0$ for all $P, Q \in E(F)/p$.*

Proof of Lemma. Let $P = (u_P, n_P), Q = (u_Q, n_Q)$ be in $E(F)/p$. Then by the bilinearity and skew-symmetry of $\langle .,.\rangle$, the fact that $\langle 1, 1\rangle = 0$, and also the hypothesis of the Lemma (applied to $K = F$), it suffices to show that

$$\langle (u_P, 0), (0, n_Q)\rangle \;=\; \langle (u_Q, 0), (0, n_P)\rangle \;=\; 0.$$

It suffices to prove the triviality of the first one, as the argument is identical for the second. Let L denote the unique unramified p-extension of F. Then there exists $u' \in \mathcal{O}_L^*/p$ such that $u_P = N_{L/F}(u')$. Since $\langle (u_P, 0), (0, n_Q)\rangle$ equals $N_{L/F}(\langle (u_P, 0), \mathrm{Res}_{L/F}((0, n_Q))\rangle)$ by the projection formula, it suffices to show that

$$\langle (u', 0), \mathrm{Res}_{L/F}((0, n_Q))\rangle \;=\; 0.$$

Now recall (cf. the discussion around (6.3)) that the restriction map $H^1(\mathcal{O}_F, \mathbb{Z}/p) \to H^1(\mathcal{O}_L, \mathbb{Z}/p)$ is zero. This implies that $\mathrm{Res}_{L/F}((0, n_Q)) = (u'', 0)$ for some $u'' \in \mathcal{O}_L^*/p$. (We cannot claim that this restriction is $(0, 0)$ in $E(L)/p$ because the splitting of the surjection $H^1(\mathcal{O}_K, \mathcal{E}[p]) \to H^1(\mathcal{O}_K, \mathbb{Z}/p)$ is not canonical when $E[p]$ is non-semisimple over K. This point is what makes this Lemma delicate.) Thus we have only to check that $\langle (u', 0), (u'', 0)\rangle \;=\; 0$ in $T_L(A)/p$. This is a consequence of the hypothesis of the Lemma, which we can apply to $K = L$ because $E[p]$ remains non-semisimple over any unramified extension of F. Done.

As in the semisimple case, there are three steps in the proof.

Step I Injectivity on symbols:

We shall use the following terminology. For $u \in \mathcal{O}_F^*$, write $\overline{u}$ and $\tilde{u}$ for its respective images in $\mathcal{O}_F^*/p$ and Y, seen as a quotient of $H^1_{\mathrm{fl}}(S, \mu_p)/X$. We will also denote by $\tilde{u}$ the corresponding element in $Z = \psi_S(Y_S) \subset H^1_{\mathrm{fl}}(S, \mathcal{E}[p])$, which should not cause any confusion as Y is isomorphic to Z. We use similar notation in

$\overline{H}^1(F,-)$. For $\overline{u}$ in $\mathcal{O}_F^*/p$, we denote by $P_{\overline{u}}$ the element in $E(F)/p$ corresponding to the pair $(\tilde{u},0)$ given by (6.16).

As in the proof of Proposition D under the diagram (4.4), pick a non-zero element $e \in X \subset \mathcal{O}_F^*/p$. By definition, $\tilde{e}=0$, so that $P_e=(\tilde{e},0)$ is the zero element of $E(F)/p$. As we have seen in the proof of Proposition D, there exists a v in $\mathcal{O}_F^*/p$ such that $[\overline{e},\overline{v}] := \overline{e}\cup\overline{v}$ is non-zero in $\mathrm{Br}_F[p]$.

Now let $\overline{x},\overline{y} \in \mathcal{O}_F^*/p$ be such that $s_p(\langle P_{\overline{x}},P_{\overline{y}}\rangle) = 0$. We have to show that

$$\langle P_{\overline{x}},P_{\overline{y}}\rangle \;=\; 0 \;\in T_F(A)/p. \tag{6.18}$$

There are two cases to consider.

Case (a) $[\overline{x},\overline{y}]=0\in \mathrm{Br}_F[p]$:

Then $\overline{x}$ is a norm from $K=F(y^{1/p})$. This implies, as in the proof in the semisimple case, that $P_{\overline{x}}$ is a norm from $E(K)/p$, and by Lemma 1.8.1, we then have (6.18).

Case (b) $[\overline{x},\overline{y}]\neq 0$:

Since $\mathrm{Br}_F[p]\simeq \mathbb{Z}/p$, we may, after modifying by a scalar, assume that $[\overline{x},\overline{y}] = [\overline{e},\overline{v}]$ in $\mathrm{Br}_F[p]$. Then by Tate ([Ta1], page 266, conditions (i), (ii)), there are elements $\overline{a},\overline{b}\in\mathcal{O}_F^*/p$ such that

$$[\overline{x},\overline{y}] = [\overline{x},\overline{b}] = [\overline{a},\overline{b}] = [\overline{a},\overline{v}] = [\overline{e},\overline{v}].$$

Claim 6.19 *For each pair of neighbors in this sequence, the corresponding symbols are equal in $T_F(A)/p$.*

Proof of Claim 6.19 From $[\overline{x},\overline{y}]=[\overline{x},\overline{b}]$ we have, by linearity, that $[\overline{x},\overline{y}\overline{b}^{-1}] = 0$, hence x is a norm from $L:=F((yb^{-1})^{1/p})$. Hence $P_{\overline{x}}$ is a norm from from $E(L)/p$, and so we get $\langle P_{\overline{x}},P_{\overline{yb^{-1}}}\rangle = 0$ in $T_F(A)/p$. Consequently, now by the linearity of $\langle\cdot,\cdot\rangle$, $\langle P_{\overline{x}},P_{\overline{y}}\rangle \;=\; \langle P_{\overline{x}},P_{\overline{b}}\rangle$. The remaining assertions of the Claim are proved in exactly the same way. $\square$

This Claim finishes the proof of Step I since $\langle P_{\overline{e}},P_{\overline{v}}\rangle \;=\; 0$, which holds because $P_{\overline{e}}=0$ in $E(F)/p$. $\square$

Step II Injectivity on $\mathbf{ST_{F,p}(A)\subset T_F(A)/p}$:

Proof We have just seen in Step I that each of the symbol in $T_F(A)/p$ is zero. Since $ST_{F,p}(A)$ is generated by such symbols, it is identically zero. Done in this case.

Step III Injectivity on $\mathbf{T_F(A)/p}$:

Proof Since $T_F(A)$ is generated by norms of symbols from finite extensions of F, it suffices to show the following for *every finite extension L/F and points $P,Q\in E(L)$*:

$$N_{L/F}(\langle P,Q\rangle \;=\; 0 \;\in T_F(A)/p. \tag{6.20}$$

Fix an arbitrary finite extension L/F and put

$$F_1 \;=\; F(E[p]).$$

There are again two cases.

Case (a) $L\supset F_1$:

Here we are in the situation where $E[p]\subset L$. In particular, $s_{p,L}$ is injective.

In the correspondence of (5.2), let $P, Q \in E(L)/p$ correspond to $\overline{u}_P, \overline{u}_Q \in \mathcal{O}_L^*/p$ respectively. Put

$$t := s_{p,L}(\langle P, Q\rangle) = [\overline{u}_P, \overline{u}_Q] \in \mathrm{Br}_F[p].$$

If $t = 0$, we have $\langle P, Q\rangle = 0$ in $T_L(A)/p$ (as $E[p] \subset L$), and we are done.

So let $t \neq 0$. Now let e, as before, be the $\mathbb{F}_p$-generator of $X \subset \mathcal{O}_F^*/p$, where X is the image of $\mathbb{Z}/p$ encountered in the proof of Proposition D. The diagram (4.4) shows that $F_1 = F(e^{1/p})$. In particular, F_1/F is a ramified p-extension. Since $p \neq 2$, $\mathcal{O}_F^*/p$ has dimension at least 3, and so we can take $v \in \mathcal{O}_F^*/p$ such that the space spanned by $\overline{e}$ and $\overline{v}$ in $\mathcal{O}_F^*/p$ has dimension 2 and does not contain the line corresponding to the unique unramified p-extension $M$of F. Put

$$F_2 = F(v^{1/p}) \quad \text{and} \quad K = F_1F_2 \subset \overline{F}.$$

Then K/F is totally ramified with $[K : F] = p^2$. Hence K/F_1 is still a ramified p-extension. By the local class field theory ([Se2], chapter V, section 3), we can choose $y \in \mathcal{O}_{F_1}^*/p$ such that $y \notin N_{K/F_1}(K^*)$, so that $[\overline{v}, \overline{y}] \neq 0$ in $\mathrm{Br}_F[p]$. By linearity, we can replace y by a power such that $[\overline{v}, \overline{y}] = t = [\overline{u}_P, \overline{u}_Q]$. Now we have

$$\langle P_{\overline{v}}, P_{\overline{y}}\rangle_L = \langle P, Q\rangle_L \in T_L(A)/p, \tag{6.21}$$

where $\langle\cdot,\cdot\rangle_L$ denotes the pairing over L. (This makes sense here because of the hypothesis $F_1 \subset L$.) Applying the projection formula to L/F_1 and F_1/F, using the facts that $P_{\overline{v}} \in E(F)/p$ and $P_{\overline{y}} \in E(F_1)/p$,

$$N_{L/F_1}(\langle P_{\overline{v}}, P_{\overline{y}}\rangle_L) = [L : F_1]\langle P_{\overline{v}}, P_{\overline{y}}\rangle_{F_1} \tag{6.22}$$

and

$$N_{F_1/F}(\langle P_{\overline{v}}, P_{\overline{y}}\rangle_{F_1}) = \langle P_{\overline{v}}, N_{F_1/F}(P_{\overline{y}})\rangle.$$

Now since $N_{L/F} = N_{L/F_1} \circ N_{F_1/F}$ and since we have shown that the symbols in $T_F(A)/p$ are all trivial, we get the triviality of $N_{L/F}(\langle P, Q\rangle)$ by combining (6.21) and (6.22).

Case (b) $L \not\supset F_1$:

In this case $E[p]$ is not semisimple over L. Hence by Step II, we have $\langle P, Q\rangle_L = 0$ in $T_L(A)/p$. So (6.20) holds. Done.

This finishes the proof of Step III, and hence of Proposition F. □

7 Remarks on the case of multiplicative reduction

Here one has the following version of Theorem A, which we will need in the sequel giving certain global applications:

Theorem G *Let F be a non-archimedean local field of characteristic zero with residue field $\mathbb{F}_q$, $q = p^r$. Suppose E/F is an elliptic curve over F, which has multiplicative reduction. Then for any prime $\ell \neq 2$, possibly with $\ell = p$, the following hold:*

(a) *s_ℓ is injective, with image of $\mathbb{F}_\ell$-dimension ≤ 1.*

(b) *$Im(s_\ell) = 0$ if $\mu_\ell \not\subset F$.*

This theorem may be proved by the methods of the previous sections, but in the interest of brevity, we will just show how it can be derived, in effect, from the results of T. Yamazaki ([Y]).

The Galois representation ρ_F on $E[\ell]$ is reducible as in the ordinary case, giving the short exact sequence (cf. [Se1], Appendix)

$$0 \to C_F \to E[\ell] \to C'_F \to 0, \tag{7.1}$$

where C'_F is given by an unramified character ν of order dividing 2; E is split multiplicative iff $\nu = 1$. And C_F is given by $\chi\nu$ ($= \chi\nu^{-1}$ as $\nu^2 = 1$), where χ is the mod ℓ cyclotomic character given by the Galois action on μ_ℓ.

Using (7.1), we get a homomorphism (as in the ordinary case)

$$\gamma_F : \, H^2(F, C_F^{\otimes 2}) \, \to \, H^2(F, E[\ell]^{\otimes 2}). \tag{7.2}$$

Here is the analogue of Proposition C:

Proposition 7.3 *We have*

$$Im(s_\ell) \, \subset \, Im(\gamma_F).$$

Furthermore, the image of s_ℓ is at most one-dimensional as asserted in Theorem G.

Proof of Proposition 7.3 As $\nu^2 = 1$ and $\ell \neq 2$, we may replace F by the (at most quadratic) extension $F(\nu)$ and assume that $\nu = 1$, which implies that $C_F = \mu_\ell$ and $C'_F = \mathbb{Z}/\ell$. We get the injective maps

$$\psi : H^1(F, \mu_\ell) \to H^1(F, E[\ell])$$

and

$$\delta : E(F)/\ell \to H^1(F, E[\ell]).$$

Claim 7.4 *$Im(\delta) \subset Im(\psi)$.*

Indeed, since $E(F)$ is the Tate curve $F^*/q^{\mathbb{Z}}$ for some $q \in F^*$ (cf. [Se1], Appendix), we have the uniformizing map

$$\varphi : F^* \to E(F).$$

Given $P \in E(F)$, pick an $x \in F^*$ such that $P = \varphi(x)$. Now $\delta(P)$ is represented by the 1-cocycle $\sigma \to \sigma(\frac{1}{\ell}P) - \frac{1}{\ell}P$, for all $\sigma \in G_F$. Let $y \in \overline{F}^*$ be such that $y^\ell = x$. Put $K = F(y)$. One knows that there is a natural uniformization map (over K) $\varphi_K : K^* \to E(K)$, which agrees with φ on F^*. Then we may take $\varphi_K(y)$ to be $\frac{1}{\ell}P$. It follows that the 1-cocycle above sends σ to $\frac{y^\sigma}{y} = \zeta_\sigma$, for an ℓ-th root of unity ζ_σ. In other words, the class of this cocycle is in the image of ψ in the long exact sequence in cohomology:

$$0 \to \mu_\ell(F) \to E[\ell](F) \to \mathbb{Z}/\ell \to H^1(F, \mu_\ell) \xrightarrow{\psi} H^1(F, E[\ell]) \to \mathbb{Z}/\ell \to \dots,$$

namely $\psi((\zeta_\sigma)) = \delta(P)(\sigma)$, with $(\zeta_\sigma) \in H^1(F, \mu_\ell)$. Hence the Claim.

Thanks to the Claim, the first part of the Proposition follows because $\mathrm{Im}(s_\ell)$ is obtained via the cup product of classes in $\mathrm{Im}(\delta)$, and $\mathrm{Im}(\gamma_F)$ is obtained via the cup product of classes in $\mathrm{Im}(\psi)$.

The second part also follows because $H^2(F, \mu_\ell^{\otimes 2})$ is isomorphic to (the dual of) $H^0(F, \mathbb{Z}/\ell(-1))$, which is at most one-dimensional. $\square$

The injectivity of s_ℓ has been proved in Theorem 4.3 of [Y] in the split multiplicative case, and this saves a long argument we can give analogous to our proof in the ordinary situation. Injectivity also follows for the general case because we can, since $\ell \neq 2$, make a quadratic base change to $F(\nu)$ when $\nu \neq 1$. When combined with Proposition 7.3, we get part (a) of Theorem G.

To prove part (b) of Theorem G, just observe that, thanks to Proposition 7.3, it suffices to prove that when $\mu_\ell \notin F$, we have $H^2(F, \mu_\ell^{\otimes 2}) = 0$. This is clear because the one-dimensional Galois module $\mathbb{Z}/\ell(-1)$, which is the dual of $\mu_\ell^{\otimes 2}$, has G_F-invariants iff $\mathbb{Z}/\ell \simeq \mu_\ell$, i.e., iff $\mu_\ell \subset F$. Now we are done.

Appendix

In this Appendix, we will collect certain facts and results we use concerning the flat topology, locally of finite type (cf. [Mi1], chapter II).

A1. The setup

As in the main body of the paper, we assume that F is a non-archimedean *local field* of *characteristic zero*, with *residue field* $k = F_q$ of *characteristic* $p > 0$. Let $S = \operatorname{Spec} \mathcal{O}_F$, $j\colon U = \operatorname{Spec} F \to S$ and $i\colon s = \operatorname{Spec} k \to S$ where s is the closed point.

Let E be an *elliptic curve* defined on F, and let $A = E \times E$. Let $\mathcal{E}$ be the Néron model of E over S, so we have in particular $E(F) = \mathcal{E}(S)$ where $E(F)$ denotes the F-rational points of E and $\mathcal{E}(S)$ are the sections of $\mathcal{E}$ over S. We have $E = j^*\mathcal{E}$ and $i^*\mathcal{E}$ as pullbacks, and $i^*\mathcal{E}$ is the reduction of E. For any $n \geq 1$, let $\mathcal{E}[n]$ denote the kernel of multiplication by n on $\mathcal{E}$.

Let ℓ be a prime number > 2, possibly equal to p. Under these assumptions we can apply Proposition 2.5.1 and Corollary 2.5.2 to E and $A = E \times E$. Since $H^1_{\text{et}}(\bar{E}, \mathbb{Z}_\ell(1))$ is the Tate module $\mathcal{T}_\ell(E)$, we have the homomorphism $c_\ell\colon T_F(A) \to H^2(F, \mathcal{T}_\ell(E)^{\otimes 2})$. Reducing modulo ℓ, we obtain now a homomorphism

$$s_\ell\colon T_F(A)/\ell \longrightarrow H^2(F, E[\ell]^{\otimes 2}).$$

A2. Flat topology and the integral part

We shall need flat topology, or to be precise, *flat topology, locally of finite type* (cf. [Mi1]).

Let $\mathcal{F}$ be a sheaf on the *big flat site* S_{fl}. Consider the restriction $\mathcal{F}_{|U} = \mathcal{F}_U := j^*\mathcal{F}$ to U. Now assume that $\mathcal{F}_U$ is the pull back $\pi_U^*(\mathcal{G})$ of a sheaf $\mathcal{G}$ on the *étale site* U_{et} under the morphism of sites $\pi_U : U_{\text{fl}} \to U_{\text{et}}$. Then we have, in each degree i, a homomorphism

$$\pi_U^* : H^i_{\text{et}}(F, \mathcal{G}|_U) \to H^i_{\text{fl}}(F, \mathcal{F}|_U). \tag{A.2.1}$$

We will need the following well known fact (cf. [Mi1], Remark 3.11(b), pp. 116–117):

Lemma A.2.2 *This is an isomorphism when $\mathcal{G}$ is a locally constructible sheaf on U_{et}.*

Now let $\mathcal{F}$ and $\mathcal{G}$ be as above, with $\mathcal{G}$ locally constructible. Composing the natural map $H^i_{\text{fl}}(S, \mathcal{F}) \to H^i_{\text{fl}}(U, \mathcal{F})$ with the inverse of the isomorphism of Lemma A.2.2, we get a homomorphism

$$\beta :\ H^i(_{\text{fl}}(S, \mathcal{F}) \to H^i(F, \mathcal{G}_F),$$

where the group on the right is Galois cohomology in degree i of F, i.e., of $\mathrm{Gal}(\overline{F}/F)$, with coefficients in the Galois module $\mathcal{G}_F$ associated to the sheaf $\mathcal{G}$ on U_{et}.

Definition A.2.3 *In the above setup, define the integral part of $H^i(F, \mathcal{G}_F)$ to be*

$$\overline{H}^i(F, \mathcal{G}_F) := Im(\beta).$$

The sheaves of interest to us below will be even constructible, and in many cases, $\mathcal{G}$ will itself be the restriction to U of a sheaf on S_{et}. A key case will be when there is a finite, flat groupscheme C on S and $\mathcal{G} = C_U$, where C_U is the sheaf on U_{et} defined by $C_{|_U}$. We will, by abuse of notation, use the same letter $\tilde{C}$ to indicate the corresponding sheaf on S_{fl} or S_{et} as long as the context is clear.

More generally, let $C_1, C_2, \ldots, C_r$ denote a collection of smooth, commutative, finite flat groupschemes over S, which are étale over U. (They need not be étale over S itself, and possibly, $C_i = C_j$ for $i \neq j$.) Let $\mathcal{F}_{\mathrm{et}}$, resp. $\mathcal{F}_{\mathrm{fl}}$, denote the sheaf for S_{et}, resp. S_{fl}, defined by the tensor product $\otimes_{j=1}^r \tilde{C}_j$. Since each $\mathcal{G}_i$ is étale over U, we have, for the restrictions to U via $\pi_U : U_{\mathrm{fl}} \to U_{\mathrm{et}}$, an isomorphism

$$\mathcal{F}_{\mathrm{fl}}|_U \simeq \mathcal{F}_{\mathrm{et}}|_U. \tag{A.2.4}$$

This puts us in the situation above with $\mathcal{F} = \mathcal{F}_{\mathrm{fl}}$ and $\mathcal{G} = \mathcal{F}_{\mathrm{fl}}|_U$.

In fact, for the $\tilde{C}_i$ themselves, (A.2.4) follows from [Mi1], p. 69, while for their tensor products, one proceeds via the tensor product of sections of presheaves. Note also that $j^*(\mathcal{F}_{\mathrm{et}})$ is constructible in U_{et} since it is locally constant. Ditto for the kernels and cokernels of homomorphisms between such sheaves on U_{et}.

A3. Application: The image of symbols

We begin with a basic result:

Lemma A.3.1 *We have for any prime ℓ (possibly p),*

$$\mathcal{O}_F^*/\ell \xrightarrow{\sim} H^1_{\mathrm{fl}}(S, \mu_\ell) \xrightarrow{\sim} \overline{H}^1(F, \mu_\ell) \hookrightarrow H^1_{\mathrm{et}}(F, \mu_\ell) \xleftarrow{\sim} F^*/\ell$$

(with the natural inclusion).

Proof: The first isomorphism follows from the exact sequence on S_{fl}

$$1 \longrightarrow \mu_\ell \longrightarrow \mathcal{G}_m \xrightarrow{\ell} \mathcal{G}_m \longrightarrow 1$$

and the fact that $H^1_{\mathrm{fl}}(S, \mathcal{G}_m) = \mathrm{Pic}(S) = 0$. (Of course, when $\ell \neq p$, this sequence is also exact over S_{et}. The second isomorphism then follows from the inclusion $\mathcal{O}_F^*/\ell \hookrightarrow F^*/\ell$. The last two statements follow from the definition or are well known.

Proposition A.3.2 *Let F be a local field of characteristic 0 with finite residue field k of characteristic p, E/F an elliptic curve with good reduction, and $\mathcal{E}$ the Néron model. Then for any odd prime ℓ, possibly equal to p, there is a short exact sequence*

$$0 \to E(F)/\ell \to H^1_{\mathrm{fl}}(S, \mathcal{E}[\ell]) \to H^1(k, \pi_0(\mathcal{E}_s))[\ell] \to 0. \tag{i}$$

In particular, since E has good reduction, we have isomorphisms

$$E(F)/\ell \simeq \mathcal{E}(S)/\ell \xrightarrow{\sim} H^1_{\mathrm{fl}}(S, \mathcal{E}[\ell]) \xrightarrow{\sim} \overline{H}^1(F, E[\ell])$$

Proof Over $\mathcal{S}_{\mathrm{fl}}$ we have the following *exact sequence of sheaves* associated to the group schemes (see [Mi2], p. 400, Corollary C9):

$$0 \longrightarrow \mathcal{E}[\ell] \longrightarrow \mathcal{E} \xrightarrow{\ell} \mathcal{E},$$

where the arrow on the right is surjective when E has good reduction. In any case, taking flat cohomology, we get an exact sequence

$$0 \to \mathcal{E}(S)/\ell = E(F)/\ell \to H^1_{\mathrm{fl}}(S, \mathcal{E}[\ell]) \to H^1_{\mathrm{fl}}(S, \mathcal{E})[\ell].$$

There is an isomorphism

$$H^1_{\mathrm{fl}}(S, \mathcal{E}) \simeq H^1(k, \pi_0(\mathcal{E}_s)). \tag{A.3.3}$$

Since E has good reduction, this is proved as follows: The natural map

$$H^1_{\mathrm{fl}}(S, \mathcal{E}) \to H^1(s, \mathcal{E}_s), \ s = \mathrm{spec} k,$$

is an isomorphism when $\mathcal{E}$ is smooth over S (see [Mi1], p. 116, Remark 3.11), and $H^1(s, \mathcal{E}_s)$ vanishes in this case by a theorem of Lang ([L1].

Clearly, we now have the exact sequence (i). □

Proposition A.3.4 *Let E be an elliptic curve over F with good reduction, and let ℓ be an odd prime, possibly the residual characteristic p of F. Then the restriction s_ℓ^{symb} of s_ℓ to the symbol group $ST_{F,\ell}(A)$ factors as follows:*

$$s_\ell^{\mathrm{symb}} : ST_{F,\ell}(A) \to \overline{H}^2(F, E[\ell]^{\otimes 2}) \hookrightarrow H^2(F, E[\ell]^{\otimes 2}).$$

Proof Thanks to Proposition A.3.2 and the definitions, this is a consequence of the following commutative diagram:

$$\begin{array}{ccccc}
E(F)/\ell \times E(F)/\ell & \to & H^1_{\mathrm{fl}}(S, \mathcal{E}[\ell]) \times H^1_{\mathrm{fl}}(S, \mathcal{E}[\ell]) & & \\
\downarrow & & \downarrow & & \\
ST_{F,\ell}(A) & \longrightarrow & H^2_{\mathrm{fl}}(S, \mathcal{E}[\ell]^{\otimes 2}) & \longrightarrow & \overline{H}^2(F, E[\ell]^{\otimes 2}) \hookrightarrow H^2(F, E[\ell]^{\otimes 2})
\end{array}$$

□

A4. A lemma in the case of good ordinary reduction

Let E be an elliptic curve over a non-archimedean local field F of characteristic zero, whose residue field k has characteristic $p > 0$.

Lemma A.4.1 *Assume that E has good ordinary reduction, with Néron model $\mathcal{E}$ over $S = \mathrm{Spec}(\mathcal{O}_F)$. Then the following hold:*

(a) *There exists an exact sequence of group schemes, finite and flat over S, and a corresponding exact sequence of sheaves on S_{fl}, both compatible with finite field extensions K/F:*

$$0 \longrightarrow C \longrightarrow \mathcal{E}[p] \longrightarrow C' \longrightarrow 0, \tag{A.4.2}$$

where $C = \mathcal{E}[p]^{\mathrm{loc}}$ and $C' = \mathcal{E}[p]^{\mathrm{et}}$.

(b) *If the points of $E_s^{\mathrm{et}}[p]$ are all rational over k then the above exact sequence becomes*

$$0 \longrightarrow \mu_{p,S} \longrightarrow \mathcal{E}[p]_S \longrightarrow (\mathbb{Z}/p)_S \longrightarrow 0. \tag{A.4.3}$$

(c) *If $E[p]$ is in addition semisimple as a $Gal(\overline{F}/F)$-module, the exact sequence (A.4.3) splits as groupschemes (and à fortiori as sheaves on S_{fl}), i.e.,*

$$\mathcal{E}[p] \simeq \mu_{p,S} \oplus (\mathbb{Z}/p)_S. \tag{A.4.4}$$

Proof (a) This sequence of finite, flat groupschemes is well known (see [Ta2], Thm. 3.4). The exactness of the sequence in S_{fl}, which is clear except on the right, follows from the fact that $\mathcal{E}[p] \to \mathcal{E}[p]^{\mathrm{et}}$ is itself flat (cf. [Ray], pp. 78–85). Moreover, the naturality of the construction furnishes compatibility with finite base change.

(b) Since C' is $\mathcal{E}[p]^{\mathrm{et}}$, it becomes $(\mathbb{Z}/p)_S$ when all the p-torsion points of $\mathcal{E}_s^{\mathrm{et}}$ become rational over k. On the other hand, since $\mathcal{E}[p]$ is selfdual, C is the Cartier dual of C', and so when the latter is $(\mathbb{Z}/p)_S$, the former has to be $\mu_{p,S}$.

(c) When $E[p]$ is semisimple, it splits as a direct sum $C_F \oplus C'_F$. In other words, the groupscheme $\mathcal{E}[p]$ splits over the generic point, and since we are in the Néron model, any section over the generic point furnishes a section over S. This leads to a decomposition $C \oplus C'$ over S as well. When we are in the situation of (b), the semisimplicity assumption yields (A.4.4). □

References

[Bl] S. Bloch, *Lectures on Algebraic Cycles*, Duke University Press (1980).

[Br] K. Brown, *Cohomology of groups*, Graduate Texts in Mathematics **87**, Springer-Verlag (1994).

[F] W. Fulton, *Intersection theory* (second edition), Springer-Verlag (1998).

[J] U. Jannsen, *Continuous étale cohomology*, Math. Annalen **280** (1988), no. 2, 207–245.

[L1] S. Lang, Algebraic groups over finite fields. Amer. J. Math. **78** (1956), 555–563. (1956), 555–563.

[L2] S. Lang, *Algebraic Number Theory*, Addison-Wesley (1970).

[Ma] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Inventiones Math. **18** (1972), 183–266.

[Mac] W. McCallum, Duality theorems for Néron models, Duke Math. Journal **53** (1986), 1093–1124.

[Mi1] J.S. Milne, *Étale cohomology*, Princeton University Press (1980), Princeton, NJ.

[Mi2] J.S. Milne, *Arithmetic duality theorems*, Perspectives in Math. **1**, Academic Press (1986).

[M] J. Milnor, *Algebraic K-theory*, Annals of Math. Studies **72**, Princeton University Press (1971).

[ParS] R. Parimala and V. Suresh, Zero cycles on quadric fibrations: Finiteness theorems and the cycle map, Inventiones Math. **122** (1995), 83–117.

[R] W. Raskind, Higher l-adic Abel-Jacobi mappings and filtrations on Chow groups. Duke Math. Journal **78** (1995), no. 1, 33–57.

[R-S] W. Raskind and M. Spiess, Milnor K-groups and zero-cycles on products of curves over p-adic fields, Compositio Math. **121** (2000), no. 1, 1–33.

[Ray] M. Raynaud, Passage au quotient par une rélation déquivalence plate, in *Proceedings of Local Fields*, Driebergen 1966, 78–85, Springer-Verlag.

[Se1] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves* (second edition), Addison-Wesley (1989).

[Se2] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer-Verlag (1979).

[So] M. Somekawa, On Milnor K-groups attached to semi-abelian varieties, K-Theory **4** (1990), no. 2, 105–119.

[Sp] E.H. Spanier, *Algebraic Topology*, McGraw-Hill (1966).

[Ta1] J. Tate, K_2 and Galois cohomology, Inventiones Math. **36** (1976), 257–274.

[Ta2] J. Tate, Finite flat group schemes, in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), 121–154, Springer, NY (1997).

[W] A. Weil, *Foundations of algebraic geometry* (second edition), American Mathematical Society, Providence, R.I. (1962).

[Y] T. Yamazaki, On Chow and Brauer groups of a product of Mumford curves, Mathematische Annalen **333**, 549–567 (2007).