Local computations on the Cassels–Tate pairing on an elliptic curve

Hendrik D. Visse

Master thesis
defended on March 4th, 2014

official supervision by
Dr. R.M. van Luijk

daily supervision by
Dr. D.S.T. Holmes
Dr. R.D. Newton

Mathematisch Instituut
Universiteit Leiden

Not marble nor the gilded monuments
Of princes shall outlive this powerful rhyme,
But you shall shine more bright in these contents
Than unswept stone besmeared with sluttish time.
When wasteful war shall statues overturn,
And broils root out the work of masonry,
Nor Mars his sword nor wars quick fire shall burn
The living record of your memory.
Gainst death and all-oblivious enmity
Shall you pace forth; your praise shall still find room
Even in the eyes of all posterity
That wear this world out to the ending doom.
So, till the Judgement that yourself arise,
You live in this, and dwell in lovers eyes.
William Shakespeare
Sonnet 55

Abstract

We describe a method of bounding the Mordell–Weil rank of an elliptic curve E over a number field k. The result of this method may improve upon an upper bound from the p-Selmer group for some odd prime number p and involves an expression for the Cassels–Tate pairing on $Ш(E/k)$ in terms of certain local pairings, one for each place v of k, which we call Tate local pairings. For each odd prime number p we give explicit formulas for the Tate local pairings both in the case where all p-torsion of E is locally defined over the base field and for the more general case. We prove that in the case where all p-torsion is rational the formula for the general case also suffices. This means that the elements in the two formulas differ by the norm of some element. We conjecture which element this should be and prove our conjecture for small primes.

Acknowledgements

There are several people that I want to thank for their contribution to my study in mathematics so far, however great or small.

I am grateful to Rachel Newton and David Holmes for their daily guidance.
To Rachel: I am glad you suggested this topic to me and I particularly want to mention your enthusiasm and your encouraging words.
To David: thanks for learning with me. Your advice beyond just the contents of this thesis is very much appreciated.

I thank Ronald van Luijk for being my official supervisor, even though he was only added late to the 'team' and furthermore for teaching the coolest course that I have taken.

I thank Hendrik Lenstra for being on the reading committee.

I cannot write a thesis without mentioning the genuine interest in my academic pursuits shown by Jan Goezinne. His giving me 'The World of Mathematics' series by James Newman at my graduation from secondary school shows that he knew that I would like mathematics better than physics years before I realised it myself.

To my parents and sisters: thanks for your love and support.

Finally, I want to thank my friends for basically existing unconditionally.

Table of Contents

1 | Introduction

The results of this thesis require a larger background in the subjects of principal homogeneous spaces and central simple algebras than I assume the reader to have, mostly since I had to learn these topics myself during the preparation of this thesis. Instead of giving this background at the start, I have chosen to put the necessary results in two appendices at the end. The advantage is that the interesting results of this thesis occur earlier, the disadvantage of course is that in doing this, it is necessary to refer forwards into the document and often state facts about objects that are not defined yet when reading the thesis from front to back. Any other choice in structure however also carries both advantages and disadvantages and I believe that the chosen structure finds the right balance between the presented order of the statements and not breaking the narrative.

1.1 Bounding the rank of $E(k)$

Let k be a number field and $(E, \mathcal{O})$ an elliptic curve over k. We recall the definitions of the Selmer and Tate–Shafarevich groups. Let M_k denote the set of places of k.

Definition 1.1. The n-Selmer group is

$$S^{(n)}(E/k) = \ker\Big(H^1(k, E[n]) \to \prod_{v \in M_k} H^1(k_v, E)[n]\Big)$$

and the Tate–Shafarevich group is

$$\text{Ш}(E/k) = \ker\Big(H^1(k, E) \to \prod_{v \in M_k} H^1(k_v, E)\Big).$$

The Mordell–Weil theorem states that $E(k)$ is a finitely generated abelian group. For each $n \geq 2$ there is an exact sequence

$$0 \longrightarrow E(k)/nE(k) \longrightarrow S^{(n)}(E/k) \longrightarrow \text{Ш}(E/k)[n] \longrightarrow 0. \tag{1.1}$$

From the inclusion $E(k)/nE(k) \subset S^{(n)}(E/k)$ one finds an upper bound for the Mordell–Weil rank $\operatorname{rk}(E(k))$ depending on n.

Lemma 1.2. *We have* $\#(E[n](k)) \cdot n^{\operatorname{rk}(E(k))} = \#\left(E(k)/nE(k)\right)$.

Proof. Since $E(k)$ is a finitely generated abelian group, we have

$$E(k) \cong E(k)_{\text{tors}} \times \mathbb{Z}^{\text{rk}(E/k)},$$

where the index 'tors' indicates the torsion part. We have

$$\#\left(E(k)/nE(k)\right) = \#\left(E(k)_{\text{tors}}/nE(k)_{\text{tors}}\right) \cdot n^{\text{rk}(E/k)}.$$

For every abelian group A the sequence

$$0 \longrightarrow A[n] \longrightarrow A \xrightarrow{\times n} A \longrightarrow A/nA \longrightarrow 0$$

is exact. Since $\#$ is multiplicative, we find $\#A[n] \cdot \#A = \#A \cdot \#\left(A/nA\right)$. Since $E(k)_{\text{tors}}$ is finite, we conclude that $\#\left(E(k)_{\text{tors}}/nE(k)_{\text{tors}}\right) = \#E(k)[n] = \#E[n](k)$ holds. This proves the proposition. □

Proposition 1.3. *For each integer $n \geq 2$, one has*

$$\#(E[n](k)) \cdot n^{\text{rk}(E(k))} \leq \#\left(S^{(n)}(E/k)\right).$$

Proof. From the exact sequence (1.1) we find the inequality

$$\#\left(E(k)/nE(k)\right) \leq \#\left(S^{(n)}(E/k)\right).$$

We conclude the proof by application of Lemma 1.2. □

By calculating Selmer groups for higher n, we may hope to find better bounds for $\text{rk}(E(k))$. We may however also hope to achieve a better upper bound by using the inclusions

$$E(k)/nE(k) \subset \text{im}(\varphi_n) \subset S^{(n)}(E/k)$$

where $\varphi_n : S^{(n^2)}(E/k) \to S^{(n)}(E/k)$ is induced by multiplication by n as in the commutative diagram below.

$$\begin{tikzcd}
E(k) \arrow[r, "\times n^2"] \arrow[d, "\times n"'] & E(k) \arrow[r] \arrow[d, equal] & S^{(n^2)}(E/k) \arrow[r] \arrow[d, "\varphi_n"'] & Ш(E/k)[n^2] \arrow[r] \arrow[d, "\times n"'] & 0 \\
E(k) \arrow[r, "\times n"] & E(k) \arrow[r] & S^{(n)}(E/k) \arrow[r] & Ш(E/k)[n] \arrow[r] & 0
\end{tikzcd}$$

Proposition 1.4. *For each integer $n \geq 2$, one has*

$$\#(E[n](k)) \cdot n^{\text{rk}(E(k))} \leq \#\,\text{im}(\varphi_n).$$

Proof. By Lemma 1.2 and the inclusion $E(k)/nE(k) \subset \text{im}(\varphi_n)$. □

1.2 The Cassels–Tate pairing

To find $\mathrm{im}(\varphi_n)$ it is useful to consider the Cassels–Tate pairing

$$\langle\ ,\ \rangle_{\mathrm{CT}} : S^{(n)}(E/k) \times S^{(n)}(E/k) \to \mathbb{Q}/\mathbb{Z} \tag{1.2}$$

as Cassels showed that $\mathrm{im}(\varphi_n)$ is its kernel [Cas59]. This method of finding a bound on $\mathrm{rk}(E(k))$ is useful if $\mathrm{im}(\varphi_n) \subsetneq S^{(n)}(E/k)$ or equivalently if the pairing (1.2) is non-trivial. Incidentally, this is exactly the case where $\text{Ш}(E/k)[n]$ is non-trivial.

Remark 1.5. We restrict the discussion in this thesis to the case where n is an odd prime number. A lot of the computational statements that will occur in this thesis can actually be stated for composite n. We chose to sacrifice the highest generality possible to achieve a clear overall presentation. We will use the letter p throughout the thesis for the odd prime number that we use in the place of n above and which we fix at this point. Most of our definitions and results depend on the fact that p is odd. We will however often not refer to p in our notation.

Cassels showed how to calculate the Cassels–Tate pairing on the 2-Selmer group, by writing the pairing as a certain sum of local invariants, one for each place v of k [Cas98]. Work by Tom Fisher and Rachel Newton [FN13] has shown a method for $p = 3$. Their method for the local part of the calculation suggests a generalization for each odd prime.

To implement our method of possibly enhancing the bound on $\mathrm{rk}(E(k))$ it is still necessary to find the p-Selmer group via some method. It is natural to ask why not find the p^2-Selmer group via possibly the same method and not bother with the calculations outlined in this thesis. One good reason might be that it is computationally infeasible to calculate large Selmer groups, whereas our method might be quicker. In this thesis however, we do not discuss these issues since it is not yet clear how to compute all the necessary ingredients for the ‘global’ part of the method studied in this thesis. In particular we are not in a position to say anything on the effectiveness of such computations. We hope to be able to work on this in later research. In any case, even if our method would not be usable to bound ranks of elliptic curves in practice, it is still of theoretical interest as it allows us to calculate the local pairings of the form (1.3) below.

The aim of the remainder of this chapter is to give the reader a general view on what will be discussed in this thesis.

Following [FN13], we define a local pairing for each place $v \in M_k$ in terms of which the Cassels–Tate pairing will be written.

Definition 1.6. Let v be a place of k. We define a local pairing

$$(\ ,\ )_v : H^1(k_v, E[p]) \times H^1(k_v, E[p]) \overset{\cup}{\to} H^2(k_v, E[p] \otimes E[p]) \overset{e_p}{\to} H^2(k_v, \mu_p) \overset{\mathrm{inv}_{k_v}}{\to} \tfrac{1}{p}\mathbb{Z}/\mathbb{Z} \tag{1.3}$$

composed of the cup product $\cup$ (which lies outside the scope of this thesis, see [GS06] section 3.4), the Weil pairing e_p (see Definition 2.3) and the Hasse invariant inv_{k_v} (see Definition B.38).

For a finite extension $k_v \subset K$ we define $(\ ,\ )_K$ by replacing all instances of k_v by K.

For a finite extension $k_v \subset K$, consider the inflation-restriction exact sequence

$$\begin{aligned} 0 \to & H^1\big(\mathrm{Gal}(K/k_v), E[p]^{G_K}\big) \overset{Inf}{\to} H^1(G_{k_v}, E[p]) \overset{res}{\to} \big(H^1(G_K, E[p])\big)^{\mathrm{Gal}(K/k_v)} \to \\ & \to H^2\big(\mathrm{Gal}(K/k_v), E[p]^{G_K}\big) \overset{Inf}{\to} H^2(G_{k_v}, E[p]) \end{aligned}$$

where we have written the groups in full for clarity.

For $i = 1, 2$, the group $H^i\big(\mathrm{Gal}(K/k_v), E[p]^{G_K}\big)$ is annihilated by $[K : k_v]$ since $[K : k_v]$ is the order of $\mathrm{Gal}(K/k_v)$, and by p since $E[p]^{G_K}$ is. If $[K : k_v]$ is not divisible by p, then $H^i\big(\mathrm{Gal}(K/k_v), E[p]^{G_K}\big)$ is annihilated by 1 and therefore trivial. Then the restriction map gives an isomorphism

$$H^1(k_v, E[p]) \cong \big(H^1(G_K, E[p])\big)^{\mathrm{Gal}(K/k_v)} \subset H^1(G_K, E[p]).$$

Proposition 1.7. *The pairings from Definition 1.6 fit into the following commutative diagram if $[K : k_v]$ is not divisible by p.*

$$\begin{tikzcd} H^1(k_v, E[p]) \times H^1(k_v, E[p]) \arrow[r, "\cup"] \arrow[d, "\mathrm{res}"'] & H^2(k_v, E[p] \otimes E[p]) \arrow[r, "e_p"] \arrow[d, "\mathrm{res}"'] & H^2(k_v, \mu_p) \arrow[r, "\mathrm{inv}_{k_v}"] \arrow[d, "\mathrm{res}"'] & \frac{1}{p}\mathbb{Z}/\mathbb{Z} \arrow[d, "\times[K:k_v]"'] \\ H^1(K, E[p]) \times H^1(K, E[p]) \arrow[r, "\cup"] & H^2(K, E[p] \otimes E[p]) \arrow[r, "e_p"] & H^2(K, \mu_p) \arrow[r, "\mathrm{inv}_K"] & \frac{1}{p}\mathbb{Z}/\mathbb{Z} \end{tikzcd} \tag{1.4}$$

Proof. See [GS06] Proposition 3.4.10 for the first square and Lemma B.40 of this thesis for the third square. The middle square is trivial. □

For every field K the cohomology group $H^2(K, \mu_p)$ injects into $H^2(K, \overline{K}^\times)$ and the latter is isomorphic to the Brauer group $\mathrm{Br}(K)$ of K. The Brauer group (discussed in Appendix B) consists of equivalence classes of central simple algebras with a certain group operation. For K a finite extension of some k_v, the Hasse invariant inv_K is an isomorphism between $\mathrm{Br}(K)$ and $\mathbb{Q}/\mathbb{Z}$. Since $H^2(K, \mu_p)$ corresponds to $\mathrm{Br}(K)[p]$ under the isomorphism $H^2(K, \overline{K}^\times) \cong \mathrm{Br}(K)$, the Hasse invariant induces an isomorphism $H^2(K, \mu_p) \cong \frac{1}{p}\mathbb{Z}/\mathbb{Z}$.

Theorem 3.6 shows that for odd primes p, the Cassels–Tate pairing can be written as a certain sum of Tate local pairings. The Tate local pairings come from the local pairings as given in Definition 1.6 and are themselves defined below in Definition 1.13. In this thesis we give explicit formulas for the Tate local pairings in terms of the Hasse invariant of certain central simple algebras over non-Archimedean local fields of characteristic zero or in fact their associated Hilbert norm residue symbol. We call the determination of the central simple algebras the global problem and calculating the local pairings involved the local problem. We only study the local problem where we assume that the central simple algebra is given.

Lemma 1.8. *For each place $v \in M_k$ and finite extension $k_v \subset K$ the pairing $(\ ,\ )_K$ is symmetric. (This uses that p is odd.)*

Proof. By Proposition 1.38 from [Mil13] a cup-product

$$\cup : H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, A \otimes B)$$

satisfies $a \cup b = (-1)^{ij} b \cup a$ so the cup-product here is antisymmetric. The Weil pairing is also antisymmetric since it is alternating and the order of its codomain is odd. Therefore $(\, , \,)_K$ is symmetric. □

Definition 1.9. Let K be a field. For maps (of sets) $f : E[p](\overline{K}) \to \overline{K}$, where K is a field, we define a Galois action as follows. For $\sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$ and $P \in E[p](\overline{K})$ define $(\sigma f)(P) = \sigma(f(\sigma^{-1}P))$. We call

$$R = \mathrm{Map}_K(E[p](\overline{K}), \overline{K})$$

the étale algebra of $E[p](\overline{K})$ over K. Here the subscript K is used to denote G_K-invariant maps.

Remark 1.10. Since for every integer n that is not divisible by $\mathrm{char}(\overline{K})$ we know that $E[n](\overline{K})$ has n^2 elements, $E[n](\overline{K})$ consists of a finite number of Galois orbits. Let $\{P_1, \ldots, P_m\} \subset E[n](\overline{K})$ be a minimal set of points such that the orbits of these points cover $E[n](\overline{K})$ and denote by $K(P_i)$ the smallest field extension of K such that $P_i \in E[n](K(P_i))$ holds. Then there is an isomorphism $R \cong K(P_1) \times \cdots \times K(P_m)$ given by $f \mapsto (f(P_1), f(P_2), \ldots, f(P_m))$. This expains the name étale algebra over K.

We let R be the étale algebra of $E[p](k)$ over k and for a finite place $v \in M_k$ and a finite field extension $k_v \subset K$ we write R_K for the étale algebra of $E[p](\overline{K})$ over K. The underlying additive groups of these R_K's will be given the structure of a central simple algebra and it is this structure that will be instrumental in solving the local problem.

In Chapter 2 we will define an injective map

$$w_{1,k} : \mathrm{H}^1(k, E[p]) \to R^\times/(R^\times)^p$$

and for each finite place $v \in M_k$ and finite extension K of k_v we will define injective maps

$$w_{1,K} : \mathrm{H}^1(K, E[p]) \to R_K^\times/(R_K^\times)^p$$

that will fit into commutative diagrams

$$\begin{tikzcd}
\mathrm{H}^1(k, E[p]) \arrow[r, "w_{1,k}"] \arrow[d, "\mathrm{res}"'] & R^\times/(R^\times)^p \arrow[d] \\
\mathrm{H}^1(k_v, E[p]) \arrow[r, "w_{1,k_v}"] \arrow[d, "\mathrm{res}"'] & R_{k_v}^\times/(R_{k_v}^\times)^p \arrow[d] \\
\mathrm{H}^1(K, E[p]) \arrow[r, "w_{1,K}"] & R_K^\times/(R_K^\times)^p.
\end{tikzcd} \tag{1.5}$$

Definition 1.11. The pairing $(\, , \,)_K$ induces a pairing $[\, , \,]_K$ on the image of $w_{1,K}$. We call this latter pairing the Tate local pairing for K.

Remark 1.12. By the diagram 1.5, it also makes sense to speak of $[a, b]_K$ where a and/or b lies in $w_{1,k}(H^1(k, E[p]))$ instead of $w_{1,K}(H^1(K, E[p]))$.

As for every symmetric bilinear form of which the codomain is not of characteristic 2, we may associate a quadratic form to the Tate local pairing. Calculating the Tate local pairing is then equivalent to calculating its associated quadratic form. Where such a quadratic form is usually defined with a factor $\frac{1}{2}$ in front, we take this factor into the definition.

Definition 1.13. Let $[\ ,\ ]_K$ be the Tate local pairing for a non-Archimedean local field of characteristc zero K. Then we write q_K for the quadratic form that satisfies $[a, b]_K = q_K(ab) - q_K(a) - q_K(b)$ for all $a, b \in \mathrm{im}(w_{1,K})$, i.e. $q_K(a) = \frac{1}{2}[a, a]_K$ for all $a \in \mathrm{im}(w_{1,K})$.

The quadratic forms q_K for non-Archimedean local fields of characteristic zero behave well under field extensions.

Proposition 1.14. *Let K be a non-Archimedean local field of characteristic zero and L/K a finite extension. Then we have*

$$q_L = [L : K]q_K.$$

Proof. This is the analogue of Proposition B.40 on a similar equation for the Hasse invariants inv_K and inv_L. □

Remark 1.15. Since q_K maps to $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$, Proposition 1.14 allows us to extend K by a field L of degree $[L : K]$ coprime to p and do our calculations over L. Such field extensions will enable us to assume certain properties of our local base field that allow us to give nice expressions for q_K.

In Theorems 4.7 and 4.22 we will see that we can calculate these quadratic forms q_K by switching to the calculation of a Hilbert norm residue symbol on K. It is in these final forms that our explicit expression is stated.

Remark 1.16. From now on, whenever we mean 'non-Archimedean local field of characteristic zero' we will just say 'local field' for brevity, i.e. we don't consider $\mathbb{R}$ and $\mathbb{C}$ and all our local fields are completions of a number field with respect to a discrete valuation. The quadratic forms $q_{\mathbb{R}}$ and $q_{\mathbb{C}}$ are trivial on the image of $w_{1,\mathbb{R}}$ and $w_{1,\mathbb{C}}$ respectively. (cf. Proposition B.13)

2 | Important definitions

Let R be the étale algebra of $E[p](\overline{K})$ over some field K. In this chapter we will see definitions of some functions that will play a vital role in giving the underlying K-vector space of R the structure of a central simple algebra in the case where K is a finite extension of k_v for some finite place $v \in M_k$ and therefore in calculating the Cassels–Tate pairing. The constructions given in this chapter are taken from [CFO⁺08]. We however give more details along the way.

2.1 The Weil pairing

Remark 2.1. Since we will deal with divisors on elliptic curves as well as on principal homogeneous spaces (cf. Appendix A), and some confusion between formal addition of divisors and addition of points may arise, we will use the notation (P) for the primitive divisor defined by a point P on either an elliptic curve or a principal homogeneous space.

Lemma 2.2. *Let E be an elliptic curve over a field K and let $D = \sum_{P\in E} n_P(P)$ be a divisor on E. Then D is a principal divisor if and only if both* $\deg(D) = 0$ *and $\sum_{P\in E}[n_P]P = \mathcal{O}$ hold.*

Proof. This proof comes from Silverman [Sil09] Corollary III.3.5. It is well known that a principal divisor on a smooth curve has degree 0. Let $D' \in \mathrm{Div}^0(E)$ be given. The Riemann-Roch space $\mathcal{L}(D' + (\mathcal{O}))$ is 1-dimensional over K by the Riemann-Roch theoreom, so there exists a point $Q \in E(\overline{K})$ such that D' is linearly equivalent to $(Q) - (\mathcal{O})$. Again by Riemann-Roch we find that two primitive divisors (i.e. divisors consisting of a single point) are linearly equivalent if and only if they are equal. Thus this point Q is uniquely determined by D'. We now define an injective map

$$\phi : \mathrm{Div}^0(E) \longrightarrow E(\overline{K})$$

that sends a divisor D' to its associated point Q such that $D' \sim (Q) - (\mathcal{O})$ holds. Since the group law on an elliptic curve may be defined in terms of divisors of the form $(Q) - (\mathcal{O})$ and therefore ϕ is a homomorphism, we arrive at the following equivalence for $D \in \mathrm{Div}^0(E)$:

$$D \sim 0 \Leftrightarrow \phi(D) = \mathcal{O} \Leftrightarrow \sum_{P\in E}[n_P]\phi\left((P) - (\mathcal{O})\right) = \mathcal{O} \Leftrightarrow \sum_{P\in E}[n_P]P = \mathcal{O}$$

which finishes our proof. □

For every positive integer $n \geq 2$ not divisible by $\operatorname{char}(K)$, we will need the Weil pairing $e_n : E(\overline{K}) \times E(\overline{K}) \to \mu_n(\overline{K})$, leaving out the reference n where no confusion is likely to arise. The Weil pairing can be defined as follows:

Definition 2.3. Let $T \in E[n](\overline{K})$ be a point. Then by Lemma 2.2 there is a function $f \in \overline{K}(E)$ with divisor $\operatorname{div}(f) = n(T) - n(\mathcal{O})$. Let $T' \in E(\overline{K})$ be a point with $[n]T' = T$. Such T' exists since its coordinates are solutions for polynomial equations. Further let $g \in \overline{K}(E)$ be a function with divisor

$$\operatorname{div}(g) = \sum_{R \in E[n](\overline{K})} (T' + R) - (R).$$

Then $f \circ [n]$ and g^n have the same divisor, so by scaling f by a suitable constant, we have $f \circ [n] = g^n$.
Let $S \in E[n](\overline{K})$. Then we define a map

$$\begin{aligned} \phi_{g,S} : E(\overline{K}) &\to \mathbb{P}^1(\overline{K}), \\ X &\mapsto g(X+S)/g(X). \end{aligned}$$

The image of $\phi_{g,S}$ is contained in $\mu_n \subset \overline{K} \subset \mathbb{P}^1(\overline{K})$. In particular, $\phi_{g,S}$ is not surjective and therefore constant. For any choice of X where both $g(X+S)$ and $g(X)$ are defined and non-zero we now define

$$e_n(S,T) = \frac{g(X+S)}{g(X)}.$$

Proposition 2.4. *The Weil pairings satisfy the following:*

1. *bilinearity*

$$\begin{aligned} e_n(S_1 + S_2, T) &= e_n(S_1, T)e_n(S_2, T) \\ e_n(S, T_1 + T_2) &= e_n(S, T_1)e_n(S, T_2) \end{aligned}$$

2. *alternating*

$$e_n(T,T) = 1$$

3. *nondegeneracy*

$$\textit{If } e_n(S,T) = 1 \textit{ for all } S \in E[n](\overline{K}), \textit{ then } T = \mathcal{O}.$$

4. *Galois equivariance*

$$\sigma(e_n(S,T)) = e_n(\sigma(S), \sigma(T)) \textit{ for all } \sigma \in G_K$$

5. *compatibility*

$$e_{nn'}(S,T) = e_n([n']S, T) \textit{ for all } S \in E[nn'](\overline{K}) \textit{ and } T \in E[n](\overline{K})$$

Proof. All of these properties are found by easy computations. Since they do take up a lot of space, we simply refer to [Sil09] Proposition III.8.1. □

Lemma 2.5. *The Weil pairing e_n satisfies the following rule:*

$$e_n(aS + bT, cS + dT) = e_n(S, T)^{ad-bc},$$

where a, b, c, d are integers.

Proof. Immediate from the bilinear and alternating properties in Proposition 2.4. □

2.2 Compatible representatives

We will consider the algebra $\overline{R} = R \otimes_K \overline{K} = \mathrm{Map}(E[p](\overline{K}), \overline{K})$, i.e. dropping the Galois invariance. The Weil pairing e_p induces an injection $w : E[p](\overline{K}) \to \overline{R}^\times$ by setting $w(S)(T) = e_p(S, T)$.

Proposition 2.6. *Let $\partial : \overline{R}^\times \to (\overline{R} \otimes_{\overline{K}} \overline{R})^\times$ be defined by $(\partial\alpha)(T_1, T_2) = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1+T_2)}$. The sequence*

$$0 \to E[p](\overline{K}) \xrightarrow{w} \overline{R}^\times \xrightarrow{\partial} (\overline{R} \otimes_{\overline{K}} \overline{R})^\times, \tag{2.1}$$

is exact.

Proof. By non-degeneracy of e_p, we find that $w(S) = 1 \in \overline{R}^\times$ implies $S = \mathcal{O}$. Thus the sequence is exact at $E[p](\overline{K})$. By bilinearity of e_p, we find that for each $S \in E[p](\overline{K})$ we have $w(S) \in \mathrm{Hom}(E[p](\overline{K}), \mu_p) \subset \overline{R}^\times$. Since both $E[p](\overline{K})$ and $\mathrm{Hom}(E[p](\overline{K}), \mu_p)$ have p^2 elements, and we have just shown w to be injective, we have $w(E[p](\overline{K})) = \mathrm{Hom}(E[p](\overline{K}), \mu_p)$. A quick calculation shows that $\mathrm{Hom}(E[p](\overline{K}), \mu_p) \subset \ker \partial$ holds. Conversely, let $f \in \ker \partial$. Then f is a group homomorphism to $\overline{K}^\times$. In particular for all $T \in E[p](\overline{K})$ we also have

$$f(T)^p = f(pT) = f(\mathcal{O}) = 1,$$

so we may conclude $f \in \mathrm{Hom}(E[p](\overline{K}), \mu_p)$. Therefore the sequence is also exact at $\overline{R}^\times$. □

Lemma 2.7 (generalised Hilbert 90). *We have $H^1(K, \overline{R}^\times) = 0$.*

Proof. Let L be the smallest field inside $\overline{K}$ such that $E[p](L) = E[p](\overline{K})$ holds. Set $G = G_K$ and for $x \in L$: $H_x = G_{K(x)}$. By Remark 1.10 we have

$$\overline{R}^\times \cong \bigoplus_{G_K-\text{orbits}} \left(\bigoplus_{E[p](L)-\text{points in orbit}} \overline{K}^\times \right),$$

which implies

$$\overline{R}^\times \cong \bigoplus_{\substack{G_K-\text{orbits of } K(x) \\ x \in L}} \mathrm{Hom}_{\mathbb{Z}[H_x]} \left(\mathbb{Z}[G], \overline{K}^\times \right).$$

Now Shapiro's lemma (see for example [Mil13] Proposition II.1.11) shows

$$H^1(G_K, \overline{R}^\times) = H^1(G_L, \overline{K}^\times)$$

which is trivial by the usual statement of Hilbert 90. □

We use this to define group homomorphisms

$$w_{1,K} : H^1(K, E[p]) \to R^\times/(R^\times)^p$$

and

$$w_{2,K} : H^1(K, E[p]) \to (R \otimes_K R)^\times/\partial R^\times.$$

Definition 2.8. Take any $[\xi] \in H^1(K, E[p])$. By Lemma 2.7 there exists a $\gamma \in \overline{R}^\times$ such that

$$w(\xi(\sigma)) = \sigma(\gamma)/\gamma$$

holds for all $\sigma \in G_K$. From this γ, define $\alpha = \gamma^p$ and $\rho = \partial\gamma$. Then the maps $w_{1,K}$ and $w_{2,K}$ are given by

$$w_{1,K}(\xi) = \alpha(R^\times)^p$$

and

$$w_{2,K}(\xi) = \rho\partial R^\times.$$

Remark 2.9. When we write $w_{1,F}$ or $w_{2,F}$ for a field F other than K, this is to be understood as the map given by Definition 2.8 above where we replace R by the étale algebra of $E[p](\overline{F})$ over F. We will also drop the index of the field when confusion is unlikely to arise.

Proposition 2.10. *The functions w_1 and w_2 above are well-defined.*

Proof. The proof consists of two parts: first that any choices made in the definition do not change the outcome and second that these α and ρ lie in $R^\times$ and $(R \otimes_K R)^\times$ respectively.

We may change ξ by a coboundary, say $\sigma(T) - T$ for some $T \in E[p](\overline{K})$. Then by the Galois equivariance of the Weil pairing, γ is multiplied by $w(T)$. Since $w(T)$ maps into the pth roots of unity, we get $w(T)^p = 1$ and by the bilinearity of the Weil pairing we get $\partial(w(T)) = 1$. Thus this alteration of ξ leaves α and ρ unchanged. Now there is only one other freedom in the choice for γ, and this is multiplication by an element of $R^\times$. However, this multiplies α and ρ by elements of $(R^\times)^p$ and $\partial R^\times$ respectively.

For the Galois invariance of α and ρ, we do two simple calculations where we let $\sigma \in G_K$. We have

$$\begin{aligned}
\sigma(\alpha)(T) &= \sigma(\alpha(\sigma^{-1}(T))) \\
&= \sigma(\gamma^p(\sigma^{-1}T)) \\
&= (\sigma(\gamma))^p\,(T) \\
&= (w(\xi(\sigma)) \cdot \gamma)^p\,(T) \\
&= \gamma^p(T) = \alpha(T)
\end{aligned}$$

since $w(\cdot)^p = 1$ holds, and

$$\begin{aligned}
\sigma(\rho)(T_1, T_2) &= \sigma(\partial\gamma)(\sigma^{-1}T_1, \sigma^{-1}T_2) \\
&= \sigma\left(\frac{\gamma(\sigma^{-1}T_1)\gamma(\sigma^{-1}T_2)}{\gamma(\sigma^{-1}(T_1+T_2))}\right) \\
&= \frac{\sigma(\gamma(\sigma^{-1}(T_1)))\sigma(\gamma(\sigma^{-1}T_2))}{\sigma(\gamma(\sigma^{-1}(T_1+T_2)))} \\
&= \partial(\sigma(\gamma))(T_1, T_2) \\
&= \partial(w(\xi(\sigma))\cdot\gamma)(T_1, T_2) \\
&= (\partial\gamma)(T_1, T_2) = \rho(T_1, T_2)
\end{aligned}$$

by the exactness of the sequence 2.1. □

Remark 2.11. The freedom we have in choosing γ will be used extensively. A choice we already make from the start (possible by multiplying by elements of $K^\times$), is

$$\gamma(\mathcal{O}) = 1.$$

In the case where all p-torsion is defined over the base field, we will exploit this freedom even further in Lemma 4.25.

Lemma 2.12. *For any field K, both $w_{1,K}$ and $w_{2,K}$ are injective.*

Proof. See [CFO+08] Lemmas 3.1 and 3.2. □

Remark 2.13. The injectivity of $w_{1,K}$ depends on the fact that we take p prime.

Remark 2.14. From the definition we may easily see that the maps $w_{1,k}$, w_{1,k_v} and $w_{1,K}$ indeed fit into the commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(k, E[p]) \arrow[r, "w_{1,k}"] \arrow[d, "\mathrm{res}"'] & R^\times/(R^\times)^p \arrow[d] \\
\mathrm{H}^1(k_v, E[p]) \arrow[r, "w_{1,k_v}"] \arrow[d, "\mathrm{res}"'] & R_{k_v}^\times/(R_{k_v}^\times)^p \arrow[d] \\
\mathrm{H}^1(K, E[p]) \arrow[r, "w_{1,K}"] & R_K^\times/(R_K^\times)^p
\end{tikzcd}$$

that was given before as equation (1.5). The right vertical arrows are given by inclusions.

Since we will want to refer to functions defined by the setting above in a convenient way, we introduce some language following [FN13].

Definition 2.15. Let $[\xi] \in H^1(K, E[p])$ be given. We call functions $\alpha \in R^\times$ and $\rho \in (R \otimes_K R)^\times$ compatible representatives for $[\xi]$ if there exists a $\gamma \in \overline{R}^\times$ such that the following hold:

1. for all $\sigma \in G_K$ and all $T \in E[p](\overline{K})$ we have $e_p(\xi(\sigma), T) = (\sigma\gamma/\gamma)(T)$,
2. $\gamma(\mathcal{O}) = 1$,

3. $\gamma^p = \alpha$, and
4. $\partial\gamma = \rho$.

2.3 The central simple algebra R_ρ

Definition 2.16. For $T \in E[p](\overline{K})$, the indicator function $\delta_T \in \overline{R}$ is defined as

$$\delta_T(S) = \begin{cases} 1 & \text{if } S = T, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 2.17. *The set $\{\delta_T : T \in E[p](\overline{K})\}$ of indicator functions forms a basis of $\overline{R}$ as a $\overline{K}$-vector space.*

Proof. This is nothing more than a basic fact from linear algebra. These indicator functions are clearly linearly independent and they span $\overline{R}$. □

Corollary 2.18. *The underlying vector space of $\overline{R}$ has dimension p^2 over $\overline{K}$ if* $\mathrm{char}(K)$ *does not divide p.*

Proof. By counting the number of points of $E[p](\overline{K}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

Remark 2.19. If all p-torsion is defined over K, the set $\{\delta_T : T \in E[p](K)\}$ forms a basis of R as a K-vector space.

Definition 2.20. For convenience in future calculations we introduce an altered Weil pairing $\varepsilon_n : E(\overline{K}) \times E(\overline{K}) \to \mu_n(\overline{K})$ for odd n by

$$\varepsilon_n(T_1, T_2) = e_n(T_1, T_2)^{1/2}$$

where we take the square root in the group of nth roots of unity. Where no confusion is likely to arise, we will again omit the subscript.

Using ε_p and $\rho \in (R \otimes_K R)^\times$, we define a peculiar multiplication on R, this procedure is taken from [CFO+08]. It will turn out that under this multiplication, R has the structure of a central simple algebra.

Remark 2.21. The slightly altered Weil pairing ε also satisfies the property of Lemma 2.5, namely $\varepsilon(aQ + bP, cQ + dP) = \varepsilon(Q, P)^{ad-bc}$ for all $P, Q \in E(\overline{K})$. The proof is the same.

Definition 2.22. Take $f, g \in R$ and define

$$(f *_\rho g)(T) = \sum_{\substack{T_1+T_2=T \\ T_1, T_2 \in E[p](\overline{K})}} \varepsilon(T_1, T_2)\rho(T_1, T_2)f(T_1)g(T_2).$$

We write R_ρ for $(R, +, *_\rho)$. The multiplication depends on ρ, but we will write $*$ for $*_\rho$ where no confusion is likely to arise.

Remark 2.23. This indeed makes R_ρ into a ring. The multiplicative unit is $\delta_\mathcal{O}$, the multiplication is associative and distributes over addition. It is not in general commutative. We identify K with $K \cdot \delta_\mathcal{O} \subset Z(R_\rho)$, where $Z(R_\rho)$ denotes the centre of R_ρ, which makes R_ρ into a K-algebra.

Lemma 2.24. *For two indicator functions we have*

$$\delta_T * \delta_S = \varepsilon(T,S)\rho(T,S)\delta_{T+S}.$$

Proof. We calculate $\delta_T * \delta_S$ directly:

$$\begin{aligned}(\delta_T * \delta_S)(A) &= \sum_{A_1+A_2=A} \varepsilon(A_1,A_2)\rho(A_1,A_2)\delta_T(A_1)\delta_S(A_2)\\ &= \begin{cases}\varepsilon(A_1,A_2)\rho(A_1,A_2) & \text{if } A_1 = T \text{ and } A_2 = S,\\ 0 & \text{else}\end{cases}\\ &= \varepsilon(T,S)\rho(T,S)\delta_{T+S}(A).\end{aligned}$$

□

Corollary 2.25. *We have*

$$\delta_T * \delta_S = \varepsilon(T,S)^2\delta_S * \delta_T = e(T,S)\delta_S * \delta_T.$$

Proof. This is immediate from Lemma 2.24. □

Corollary 2.26. *We have $\delta_T^{*p} = \alpha(T)\delta_\mathcal{O}$ and δ_T is invertible with inverse*

$$\delta_T^{-1} = \frac{1}{\gamma(T)\gamma(-T)}\delta_{-T}.$$

Proof. Using that $\delta_{nT} * \delta_T = \varepsilon(nT,T)\rho(nT,T)\delta_{(n+1)T} = \frac{\gamma(nT)\gamma(T)}{\gamma((n+1)T)}\delta_{(n+1)T}$ holds for every positive integer n, we find by repeatedly multiplying by δ_T from the right the equality

$$\begin{aligned}\delta_T^{*p} &= \prod_{n=1}^{p-1}\left(\frac{\gamma(nT)\gamma(T)}{\gamma((n+1)T)}\right)\delta_{pT}\\ &= \gamma(T)\gamma(T)^{p-1}\delta_\mathcal{O} = \alpha(T)\delta_\mathcal{O}.\end{aligned}$$

Since δ_T^{*p} is invertible in $K \subset R_\rho$, δ_T is invertible in R_ρ.

The last equality follows from Lemma 2.24, using $\rho(T,-T) = \gamma(T)\gamma(-T)$. □

Proposition 2.27. *The K-algebra R_ρ is a central simple algebra.*

Proof. This is part of Proposition 2.7 from [FN13] which combines several results from [CFO$^+$08]. Their proof is of an abstract nature and reaches further than the contents of this thesis. Therefore we give a more direct approach.

By Lemma B.9 it is sufficient to prove that $R_\rho \otimes_K \overline{K} = \overline{R}_\rho$ is central and simple over $\overline{K}$. We first prove that it is central.

Suppose there exists an $c \in \overline{R}_\rho$ such that $c \notin \overline{K}$ holds, but such that c lies in the centre of $\overline{R}_\rho$. Select such c and let $S \in E[p](\overline{K})$ be a point such that $c(S) \neq 0$ holds. Let $T \in E[p](\overline{K})$ be any point. We compute

$$\begin{aligned}(c * \delta_T)(S+T) = & \sum_{P_1+P_2=S+T} \varepsilon(P_1,P_2)\rho(P_1,P_2)c(P_1)\delta_T(P_2) \\ = & \varepsilon(S,T)\rho(S,T)c(S)\end{aligned}$$

and similarly

$$(\delta_T * c)(S+T) = \varepsilon(T,S)\rho(T,S)c(S).$$

By assumption these two expressions are equal and $c(S) \neq 0$ holds. Since ρ is symmetric, we conclude that $\varepsilon(S,T) = \varepsilon(T,S)$ holds and therefore $e(S,T) = 1$. Since this last equation holds for all $T \in E[p](\overline{K})$, by the non-degeneracy of the Weil pairing we conclude $S = \mathcal{O}$ and therefore $c = c(\mathcal{O})\delta_{\mathcal{O}} \in \overline{K}$ which contradicts our assumption. Thus $\overline{R}_\rho$ is central over $\overline{K}$.

Let $I \subset \overline{R}_\rho$ be a non-zero ideal. Let $a \in \overline{R}_\rho$ be any element. We can write a uniquely as $a = \sum_{T \in E[p](\overline{K})} a(T)\delta_T$. We define the length of a as the number of $T \in E[p](\overline{K})$ such that $a(T) \neq 0$ holds and we write $\ell(a)$ for this. Now let $m \in I$ be an element of minimal length among non-zero elements of I. Then

$$\ell(m) = \ell(m * \delta_T) = \ell(\delta_T * m)$$

holds for all $T \in E[p](\overline{K})$ and in particular we have $(m * \delta_T)(P) = 0$ if and only if $(\delta_T * m)(P) = 0$. Let $S \in E[p](\overline{K})$ be a point such that $m(S) \neq 0$ holds.

We have $(m * \delta_T)(S+T) = \varepsilon(S,T)\rho(S,T)m(S) = e(S,T)(\delta_T * m)(T+S)$. We write $r_T = m * \delta_T - e(S,T)\delta_T * m$. Since I is a two-sided ideal, we have $r_T \in I$ for all $T \in E[p](\overline{K})$. However we also have $\ell(r) < \ell(m)$ by $r_T(S+T) = 0$ and therefore $r_T = 0$ for all $T \in E[p](\overline{K})$.

From $r_S = 0$ we conclude that m commutes with δ_S and therefore $m(T) \neq 0$ holds only if T is a multiple of S. Then for T not a multiple of S (i.e. S and T generate $E[p](\overline{K})$), $r_T = 0$ implies $m = m(S)\delta_S$. Therefore we have $\delta_S \in I$ and then conclude $\delta_T \in I$ for all $T \in E[p](\overline{K})$ and thus $I = \overline{R}_\rho$. Therefore the only two-sided ideals are 0 and $\overline{R}_\rho$. □

The next Proposition relates the central simple algebra R_ρ to the Tate local pairing $[\ ,\ ]_K$ that plays a central role in the calculation of the Cassels–Tate pairing. The quadratic form q_K was first given in Definition 1.13.

Proposition 2.28. *Let K be a finite extension of k_v and let R be the étale algebra of $E[p](\overline{K})$ over K. Let $\alpha \in R^\times$ and $\rho \in (R \otimes_K R)^\times$ be compatible representatives for some $[\xi] \in H^1(K, E[p])$. Then we have*

$$q_K(\alpha) = \mathrm{inv}_K(R_\rho).$$

Proof. This is Proposition 2.7 from [FN13] which combines results from [CFO$^+$08]. The Hasse invariant inv_K is defined in Definition B.38. □

3 | Towards a local problem

Let R be the étale algebra of $E[p](\overline{k})$ over k.

Fact 3.1. The Cassels–Tate pairing $\langle\ ,\ \rangle_{CT} : S^{(p)}(E/k) \times S^{(p)}(E/k) \to \mathbb{Q}/\mathbb{Z}$ is actually induced by a pairing

$$\langle\ ,\ \rangle : Ш(E/k) \times Ш(E/k) \to \mathbb{Q}/\mathbb{Z}$$

that can be defined in several ways as in [PS99] section 3 or [Mil06] Proposition I.6.9. This pairing also will be referred to as the Cassels–Tate pairing. For our purposes it will suffice to only use the expression for the Cassels–Tate pairing found in Theorem 3.6 below. The proof of this theorem that can be found in [FN13] uses the definition that [PS99] and [Mil06] have in common.

Definition 3.2. Let C/k be a principal homogeneous space under E. Then we write $R(C) = \mathrm{Map}_k(E[p](\overline{k}), \overline{k}(C))$.

Remark 3.3. Appendix A will deal with principal homogeneous spaces under E. One of the facts that will be explained there is that points P_v as in Theorem 3.6 below are guaranteed to exist. See Proposition A.9 for this, combined with the alternative definition of the Tate–Shafarevich group given there.

Fact 3.4. For each $T \in E[p](\overline{K})$, there is a degree 0 divisor $\mathfrak{a}_T$ on C and rational functions $f_T \in \overline{k}(C)$ with $\mathrm{sum}(\mathfrak{a}_T) = T$ and $\mathrm{div}(f_T) = p\mathfrak{a}_T$. Furthermore, these f_T's may be scaled in such a way that the map $(T \mapsto f_T)$ is Galois equivariant. Please see Theorem A.15 for a proof of this fact. In particular we can take $\mathfrak{a}_{\mathcal{O}} = 0$ and $f_{\mathcal{O}} = 1$.

Lemma 3.5. *Let $f \in R(C)$ be given by $T \mapsto f_T$, where the f_T are as in Fact 3.4. Then after multiplying f by an element of $R^\times$, we may assume that for every place $v \in M_k$, the value of f at any point of $C(k_v)$ lies in the image of w_{1,k_v}.*

Proof. See [FN13] Lemmas 1.1 and 1.2. □

Theorem 3.6. *Let $x, y \in Ш(E/k)$ with $py = 0$. Let C/k be a principal homogeneous space under E representing x, and let $\eta \in S^{(p)}(E/k)$ be an element that maps to y. Let $f \in R(C)$ be scaled as in Lemma 3.5, and for each place v of k choose a point $P_v \in C(k_v)$, avoiding the zeroes and poles of the rational functions f_T. Then the Cassels–Tate pairing is given by*

$$\langle x, y\rangle = \sum_{v \in M_k} [f(P_v), w_1(\eta)]_v,$$

which is independent of choices of P_v.

Proof. See [FN13] Theorem 1.3. Their proof uses $\mathrm{Map}_k(E[p](\overline{k}) \setminus \{\mathcal{O}\}, \overline{k})$, whenever we use R. Since $f_{\mathcal{O}}$ is constant, it has no zeroes or poles. Therefore their proof also works in our case. □

4 | Calculations

Throughout this chapter, let K be a finite extension of k_v for some finite place v of k and let R be the étale algebra of $E[p](\overline{K})$ over K. Let $\alpha \in R^\times$ and $\rho \in (R \otimes_K R)^\times$ be compatible representatives for some $[\xi] \in H^1(K, E[p])$. The goal of this chapter is to give formulas for $q_K(\alpha)$ which may be used to calculate the Cassels–Tate pairing through Theorem 3.6.

Proposition 4.1. *There exists an extension F of K that has degree coprime to p such that we have exactly one of two cases:*

1. *$E[p](\overline{K}) = E[p](F)$, or*
2. *there exist points P and Q that generate $E[p](\overline{K})$ such that P is defined over F and Q is defined over a cyclic field extension $F \subset L$ of degree p and such that the Galois group $\mathrm{Gal}(L/F) = \langle \sigma \rangle$ acts on $E[p](\overline{K})$ by $\sigma(P) = P$ and $\sigma(Q) = Q + P$.*

Proof. By the action of G_K on $E[p](\overline{K})$ we get a homomorphism

$$G_K \to \mathrm{Aut}(E[p](\overline{K})) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

where we consider automorphisms of groups. The isomorphism is by choosing a basis. Let L be the fixed field of the kernel of this map. Then $E[p](L) = E[p](\overline{K})$ holds and we have maps

$$G_K \longrightarrow \mathrm{Gal}(L/K) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Let $C \subset \mathrm{Gal}(L/K)$ be a Sylow-p-subgroup and let $F = L^C$ be the field fixed by C. Then we have $K \subseteq F \subseteq L$ and since $\#\,\mathrm{GL}_2(\mathbb{F}_p) = p(p-1)(p^2-1)$ is divisible by only a single factor of p and C is (isomorphic to) a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, we have two cases: either C is trivial or C is cyclic of order p. In either case we have $p \nmid [F : K]$, so F is a candidate field for this proposition.

In the first case we have $F = L$. This yields case 1 above.

In the second case we have $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$. Since all Sylow-$p$-subgroups of a finite group are conjugates and we know that the subgroup

$$H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{F}_p)$$

is a Sylow-p-subgroup, by application of an automorphism of $\mathbb{F}_p^2$ and using the inclusiong $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$, we can identify C with H.

Let $P \in E[p](L)$ correspond to the vector $(1,0)^t$ and $Q \in E[p](L)$ to the vector $(0,1)^t$. Then the element $\sigma \in \mathrm{Gal}(L/F)$ that corresponds to the given generator of H yields $\sigma(P) = P$ and $\sigma(Q) = Q + P$. □

Since $[F : K]$ is coprime to p, by Proposition 1.14, we may replace K by F and do our calculations over the new base field which gives a nice structure for $E[p](F)$.

We will call case 1 from Proposition 4.1 'the rational case' and case 2 'the non-rational case'.

Proposition 4.2. *Suppose $\alpha(T) \in (K^\times)^p$ holds for some non-zero $T \in E[p](K)$, then the Hasse invariant $\mathrm{inv}_K(R_\rho) = 0$ holds and $q_K(\alpha) = 0$.*

Proof. In the polynomial ring $K[X,Y]$ we have $X^p - Y^p = (X-Y)\mathcal{P}(X,Y)$ for some polynomial $\mathcal{P} \in K[X,Y]$, so writing $\alpha(T) = \beta^p$ for some $\beta \in K$, we have

$$(\delta_T - \beta)\mathcal{P}(\delta_T, \beta) = \delta_T^{*p} - \beta^p \overset{\text{Prop.2.26}}{=} \alpha(T) - \alpha(T) = 0$$

since $\beta \in K$ commutes with δ_T. Since $T \neq \mathcal{O}$ holds, we have $\delta_T \notin K$ (and in particular $\delta_T \neq \beta$) and therefore $\delta_T - \beta$ is a zero-divisor in R_ρ.

The Artin–Wedderburn theorem implies that R_ρ is either a division algebra or isomorphic to a matrix ring with coefficients in a division algebra over K. In particular in the second case we have $R_\rho \cong \mathrm{Mat}_p(K)$ since both R_ρ and $\mathrm{Mat}_p(K)$ are of dimension p^2 over K. By having found a non-zero zero-divisor, the division ring case is excluded. So we have the matrix ring case and therefore have $\mathrm{inv}_K(R_\rho) = 0$. The result $q_K(\alpha) = 0$ follows from Proposition 2.28. □

For the remainder of this chapter fix a point $P \in E[p](K)$. If $\alpha(P) \in (K^\times)^p$, then by Proposition 4.2 we have $q_K(\alpha) = 0$ and we are done for the goal of this chapter.

4.1 The rational case

We first study case 1 from Proposition 4.1 and assume that all p-torsion points are defined over the base field which we again call K. This gives the existence of a group isomorphism $E[p](K) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proposition 4.3. *In the rational case the group of pth roots of unity lies in K.*

Proof. Let $Q \in E[p](K)$ be such that P and Q generate $E[p](K)$, then $e_p(Q,P)$ is a primitive pth root of unity by non-degeneracy of the Weil pairing. By equivariance of the Weil pairing we get for all $\tau \in G_K$:

$$\tau(e_p(Q,P)) = e_p(\tau(Q), \tau(P)) = e_p(Q,P)$$

and thus $e_p(Q,P) \in K$. □

Lemma 4.4. *For every $Q \in E[p](K)$ we have equalities*

$$\delta_Q * \delta_P * \delta_{-Q} = e(Q,P)\gamma(Q)\gamma(-Q)\delta_P$$

and

$$\delta_Q * \delta_P * \delta_Q^{-1} = e(Q,P)\delta_P.$$

Proof.

$$\begin{aligned}
\delta_Q * \delta_P * \delta_{-Q} &= \delta_Q * (\varepsilon(P,-Q)\rho(P,-Q)\delta_{P-Q}) \\
&= \varepsilon(P,-Q)\rho(P,-Q)\varepsilon(Q,P-Q)\rho(Q,P-Q)\delta_P \\
&= \varepsilon(P,-Q)\varepsilon(Q,P)\varepsilon(Q,-Q)\frac{\gamma(P)\gamma(-Q)}{\gamma(P-Q)}\frac{\gamma(Q)\gamma(P-Q)}{\gamma(P)}\delta_P \\
&= \varepsilon(P,-2Q)\gamma(Q)\gamma(-Q)\delta_P \\
&= e(Q,P)\gamma(Q)\gamma(-Q)\delta_P.
\end{aligned}$$

The second equality is found by using Lemma 2.26. □

Definition 4.5. If $\alpha(P) \notin (K^\times)^p$ holds, then there is a degree p field extension $K \subset K(\delta_P)$ inside R_ρ. Let σ be a generator for $\mathrm{Gal}(K(\delta_P)/K)$. Such σ multiplies δ_P by a primitive pth root of unity ζ and induces a K-algebra automorphism of R_ρ. By the Skolem–Noether Theorem B.21, there exists an element $r \in R_\rho$ such that $\sigma\delta_P = r * \delta_P * r^{-1}$ holds. We will call such an element r a Skolem–Noether element for ζ, not giving reference to the point P that this depends upon.

Remark 4.6. If the points P and Q generate $E[p](\overline{K})$ then $e(Q,P)$ is a primitive root of unity and Lemma 4.4 shows that δ_Q is a Skolem–Noether element for $e(Q,P)$.

Theorem 4.7. *Let $P,Q \in E[p](K)$ be points that together generate $E[p](\overline{K})$ as an abelian group. Let $\iota_{P,Q} : \mu_p \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ be the group isomorphism defined by $e(Q,P) \mapsto \frac{1}{p}$. Then we have*

$$q_K(\alpha) = \iota_{P,Q}\{\alpha(P),\alpha(Q)\}_K.$$

Proof. We will use Proposition 2.28 and the constructions from Appendix B.

If $\delta_P^{*p} = \alpha(P) \in (K^\times)^p$ holds, then by Proposition B.45 we have $\{\alpha(P),\alpha(Q)\}_K = 1$ and therefore $\iota_{P,Q}\{\alpha(P),\alpha(Q)\}_K = 0$ which is in accordance with Proposition 4.2. For the rest of the proof we assume $\alpha(P) \notin (K^\times)^p$ which gives us a cyclic extension $K(\delta_P)/K$.

We take $a = \delta_P^{*p}$ in Definition B.41. Then the character χ_a is given by

$$\begin{aligned}
\chi_a : G_K \longrightarrow \mathrm{Gal}(K(\delta_P)/K) &\longrightarrow \tfrac{1}{p}\mathbb{Z}/\mathbb{Z} \\
(\delta_P \mapsto e(Q,P)\delta_P) &\mapsto \frac{1}{p}.
\end{aligned}$$

We take $b = \delta_Q^{*p} = \alpha(Q)$. Since δ_Q is a Skolem–Noether element for $e(Q,P)$, the construction from Proposition B.28 shows that the symbol (χ_a, b) defines (the class in $\mathrm{Br}(K)$ of) R_ρ. For the Hilbert symbol $\{a,b\}_K$ we have

$$\{a,b\}_K = e(Q,P)^{p\cdot \mathrm{inv}_K(\chi_a,b)} = e(Q,P)^{p\cdot q_K(\alpha)}$$

by Proposition 2.28 and therefore

$$\iota_{P,Q}\left(\{a,b\}_K\right) = q_K(\alpha).$$

□

Remark 4.8. In the proof of Theorem 4.7 we have only made use of the fact that δ_Q is a Skolem–Noether element for $e(Q, P)$. In the non-rational case to be studied in the next section, we therefore only need to look for a Skolem–Noether element for some root of unity as we will still have the degree p field extension $K(\delta_P)/K$ inside R_ρ under the assumption $\alpha(P) \notin (K^\times)^p$.

4.2 The non-rational case

We have already studied the case where all p-torsion points are defined over the base field. This section will deal with what happens if not all p-torsion is rational, that is, when we are in the second case of Proposition 4.1. Let the new field of definition again be called K. For clarity we recall the setting we are given from Proposition 4.1. Let $P \in E[p](K)$ be a point such that $\alpha(P) \notin (K^\times)^p$ holds, let L/K be a cyclic field extension with $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ and $Q \in E[p](L)$ such that $\sigma(Q) = Q + P$ holds.

Proposition 4.9. *In the non-rational case the group of pth roots of unity also lies in K. (cf. Proposition 4.3)*

Proof. The proof is analogous to the proof of Proposition 4.3, where we now also need to use that the Weil pairing is alternating. We start by remarking that Proposition 4.3 immediately implies $\mu_p \subset L$.

We calculate for $\zeta = e(P, Q)$ and σ as above:

$$\sigma(\zeta) = e(\sigma(P), \sigma(Q)) = e(P, Q + P) = e(P, Q)e(P, P) = e(P, Q) = \zeta.$$

As σ generates $\mathrm{Gal}(L/K)$, we find $\zeta \in K$. □

Definition 4.10. We introduce the notation

$$\Delta_{P,Q} = \delta_Q + \delta_{Q+P} + \delta_{Q+2P} + \ldots + \delta_{Q+(p-1)P}$$

omitting the reference to the odd prime number p which is fixed throughout.

Remark 4.11. In the non-rational case we also have $\delta_P \in R$, but the element $\delta_Q \in \overline{R}$ does not lie in R as it is not Galois invariant. The element $\Delta_{P,Q}$ does lie in R as its terms are permuted by the Galois action.

Lemma 4.12. *We have $\Delta_{P,Q} * \delta_P = e(Q, P)\delta_P * \Delta_{P,Q}$.*

Proof. This follows immediately from Corollary 2.25 and Lemma 2.5. □

Remark 4.13. Lemma 4.12 shows that if $\Delta_{P,Q}$ is invertible, then it is a Skolem–Noether element for $e(Q, P)$.

Definition 4.14. Let $Q \in E[p](\overline{K})$ be such that P and Q generate $E[p](\overline{K})$. Then $\iota_{P,Q} : \mu_p \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ denotes the group homomorphism given by $e(Q, P) \mapsto \frac{1}{p}$.

Remark 4.15. We have already used the map denoted by $\iota_{P,Q}$ in Theorem 4.7 for a specific $Q \in E[p](\overline{K})$. Lemma 4.12 motivates us to introduce this notation for any suitable $Q \in E[p](\overline{K})$.

4.2.1 Motivating examples for $p = 3$

We devote some time to the special case $p = 3$ in order to give a 'feel' for the general odd prime case. The results of this section can also be found in [FN13].

Proposition 4.16. *We have the following identity in R_ρ:*

$$\Delta^{*3}_{P,Q} = \Big(\alpha(Q) + \alpha(Q+P) + \alpha(Q+2P) - 3\gamma(Q)\gamma(Q+P)\gamma(Q+2P)\Big)\delta_{\mathcal{O}}$$

and $\Delta^{*3}_{P,Q}$ lies in $K \subset R_\rho$.

Proof. The first part is proven by a direct (and slightly lengthy) calculation. By applying σ to this expression, we see that this lies in $K \subset R_\rho$. □

The following Proposition is the non-rational equivalent to Theorem 4.7 in the case $p = 3$.

Proposition 4.17. *We have*

$$q_K(\alpha) = \begin{cases} \iota_{P,Q}\{\alpha(P), \Delta^{*3}_{P,Q}\}_K & \textit{if } \Delta^{*3}_{P,Q} \neq 0, \\ 0 & \textit{else.} \end{cases}$$

Proof. If $\Delta^{*3}_{P,Q}$ is non-zero then it is a unit in K and therefore a unit in R_ρ. Then also $\Delta_{P,Q}$ itself is a unit in R_ρ. Then Lemma 4.12 shows that $\Delta_{P,Q}$ is a Skolem–Noether element for $e(Q,P)$ and we may proceed as in the proof of Theorem 4.7.

If $\Delta^{*3}_{P,Q}$ is zero, then the proof of Proposition 4.2 shows that $q_K(\alpha) = 0$ holds. □

4.3 The case for general p

Lemma 4.18. *For $\Delta_{P,Q} = \delta_Q + \delta_{Q+P} + \ldots + \delta_{Q+(p-1)P}$ one has for all $m \in \mathbb{Z}_{\geq 1}$:*

$$\Delta^{*m}_{P,Q} = \sum_{i_1,i_2,\ldots,i_m=0}^{p-1} \varepsilon(Q,P)^{\sum_{\ell=1}^m (2\ell-m-1)i_\ell} \frac{\prod_{\ell=1}^m \gamma(Q+i_\ell P)}{\gamma(mQ + (\sum_{\ell=1}^m i_\ell)P)} \delta_{mQ+(\sum_{\ell=1}^m i_\ell)P}$$

and in particular:

$$\Delta^{*p}_{P,Q} = \sum_{i_1,i_2,\ldots,i_p=0}^{p-1} \varepsilon(Q,P)^{\sum_{\ell=1}^p (2\ell-1)i_\ell} \frac{\prod_{\ell=1}^p \gamma(Q+i_\ell P)}{\gamma((\sum_{\ell=1}^p i_\ell)P)} \delta_{(\sum_{\ell=1}^p i_\ell)P}. \tag{4.1}$$

Proof. There exists a $\gamma \in \overline{R}^\times$ such that $\gamma(\mathcal{O}) = 1$ and $\rho = \partial\gamma$ hold as in Definition

2.15. We start by calculating the square of $\Delta_{P,Q}$ by using Lemma 2.24.

$$\begin{aligned}
\Delta_{P,Q}^{*2} &= \sum_{i_1,i_2=0}^{p-1} \delta_{Q+i_1P} * \delta_{Q+i_2P} \\
&= \sum_{i_1,i_2=0}^{p-1} \varepsilon(Q+i_1P, Q+i_2P)\rho(Q+i_1P, Q+i_2P)\delta_{2Q+(i_1+i_2)P} \\
&= \sum_{i_1,i_2=0}^{p-1} \varepsilon(Q,P)^{i_2-i_1} \frac{\gamma(Q+i_1P)\gamma(Q+i_2P)}{\gamma(2Q+(i_1+i_2)P)} \delta_{Q+(i_1+i_2)P}.
\end{aligned}$$

We proceed by induction, continually multiplying by $\Delta_{P,Q}$ from the right. We first focus on the power of $\varepsilon(Q,P)$. Starting from the expression for $\Delta_{P,Q}^{*m}$ we get the power of $\varepsilon(Q,P)$ in the expression for $\Delta_{P,Q}^{*(m+1)}$:

$$\begin{aligned}
\sum_{\ell=1}^{m}(2\ell-m-1)i_\ell + mi_{m+1} - (i_1+i_2+\ldots+i_m) &= \sum_{\ell=1}^{m}(2\ell-m-2)i_\ell + mi_{m+1} \\
&= \sum_{\ell=1}^{m+1}(2\ell-(m+1)-1)i_\ell
\end{aligned}$$

The part with ρ and γ is straightforward: writing $\rho(mQ+(i_1+\ldots+i_m)P, Q+i_{m+1}P)$ in terms of γ (using $\rho=\partial\gamma$), one sees that the first factor cancels with the denominator in the expression for $\Delta_{P,Q}^{*m}$.

The expression for $\Delta_{P,Q}^{*p}$ follows by recalling $\varepsilon(Q,P)^p = 1$ and $pQ = \mathcal{O}$. □

If, for $\sum_{\ell=1}^{p} i_\ell = j$ not divisible by p we prove that the δ_{jP}-terms cancel, then we have proven $\Delta_{P,Q}^{*p} \in K$. If $\Delta_{P,Q}^{*p}$ is non-zero, then it is a Skolem–Noether element for $e(Q,P)$ by Lemma 4.12.

Lemma 4.19. *In the expression for $\Delta_{P,Q}^{*p}$ given in equation (4.1), all $\delta_{\sum i_\ell P}$-terms for $\sum_{\ell=1}^{p} i_\ell$ not divisible by p cancel.*

Proof. Let $\{i_1, i_2, \ldots, i_p\}$ be a set of coefficients such that they do not sum to a multiple of p. Then in particular, they are not all equal and setting $i'_\ell = i_{\ell+1}$ we get a new set of coefficients since p is prime. The powers of $\varepsilon(Q,P)$ in the terms associated to the first and second set of coefficients differ by an amount

$$\sum_{\ell=1}^{p}(2\ell-1)i_\ell - \sum_{\ell=1}^{p}(2(\ell+1)-1)i_\ell = \sum_{\ell=1}^{p}(-2)i_\ell = -2\sum_{\ell=1}^{p} i_\ell,$$

which by assumption is not divisible by p. Thus by shifting a set of coefficients that do not sum to a multiple of p a p number of times, we get all pth roots of unity from the $\varepsilon(Q,P)$-part in our expression. As the γ-part is unchanged, and the sum of all pth roots of unity sum to zero, these terms cancel. □

Theorem 4.20. *We have*

$$\Delta^{*p}_{P,Q} = \sum_{\substack{i_1,i_2,\ldots,i_p=0\\ p\mid\sum_\ell i_\ell}}^{p-1} e(Q,P)^{\sum_{\ell=1}^p \ell\cdot i_\ell} \prod_{\ell=1}^{p} \gamma(Q+i_\ell P)\delta_{\mathcal{O}}.$$

Proof. This follows immediately from Lemmas 4.18 and 4.19, by application of $\varepsilon(Q,P)^2 = e(Q,P)$ and $\varepsilon(Q,P)^p = 1$. □

Remark 4.21. If one would not want to use γ but only α and ρ (which is a reasonable thing because given α and ρ there is still a choice involved for γ), then one would prefer an expression for $\Delta^{*p}_{P,Q}$ in terms of ρ instead of γ. Such an expression is easily found by going through the proof of Lemma 4.18. It is however not a very nice expression. We have

$$\Delta^{*p}_{P,Q} = \sum_{\substack{i_1,i_2,\ldots,i_p=0\\ p\mid\sum_\ell i_\ell}}^{p-1} e(Q,P)^{\sum_{\ell=1}^p \ell\cdot i_\ell} \left(\prod_{j=1}^{p-1} \rho\left(jQ+\sum_{\ell=1}^{j} i_\ell P, Q+i_{j+1}P\right)\right)\delta_{\mathcal{O}}.$$

Theorem 4.22. *Let $P \in E[p](K)$, let L/K be a cyclic extension with Galois group* $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ *and $Q \in E[p](L)$ be such that $\sigma(Q) = Q + P$ holds and such that P and Q generate $E[p](\overline{K})$ as an abelian group. Then we have*

$$q_K(\alpha) = \begin{cases} \iota_{P,Q}\{\alpha(P), \Delta^{*p}_{P,Q}\}_K & \textit{if } \Delta^{*p}_{P,Q} \neq 0, \\ 0 & \textit{else.} \end{cases}$$

Proof. We have already seen in Lemma 4.12 that $\Delta_{P,Q}$ is a Skolem–Noether element for $e(Q,P)$ if it is invertible. We may copy the proof of Theorem 4.7 and replace all instances of δ_Q by $\Delta_{P,Q}$. If however $\Delta^{*p}_{P,Q}$ is zero, then the proof of Proposition 4.2 shows that $q_K(\alpha) = 0$ holds. □

4.4 Combining the statements

Since in our study we have switched viewpoints several times, it is useful to collect the important results into a single statement.

Fact 4.23. Let K be a local field and let R be the étale algebra of $E[p](\overline{K})$ over K. Let α_1, α_2 be in the image of $w_{1,K}$. Let $\rho_1, \rho_2 \in (R \otimes_K R)^\times$ be such that α_i and ρ_i are compatible representatives for some classes in $H^1(K, E[p])$ for $i = 1, 2$. (Remark that this makes $\alpha_1\alpha_2$ and $\rho_1\rho_2$ into compatible representatives for some class too.) Let $K \subset F \subset L$ be field extensions such that $[F : K]$ is coprime to p, such that $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ is cyclic and such that there exist $P \in E[p](F)$ and $Q \in E[p](L)$ such that $\sigma(Q) = Q + P$ holds and such that P and Q generate $E[p](\overline{K})$ as an abelian group. Fix such P and Q. Then we have

$$\begin{aligned}[\alpha_1,\alpha_2]_K =& q_K(\alpha_1\alpha_2)-q_K(\alpha_1)-q_K(\alpha_2)\\ =&\frac{1}{[L:F]}\Big(q_F(\alpha_1\alpha_2)-q_F(\alpha_1)-q_F(\alpha_2)\Big)\\ =&\frac{1}{[F:K]}\left\{\begin{array}{ll}\iota_{P,Q}\{\alpha_1\alpha_2(P),\Delta^{*\rho_1\rho_2 p}_{P,Q}\}_K & \text{if } \Delta^{*\rho_1\rho_2 p}_{P,Q}\neq 0,\\ 0 & \text{else}\end{array}\right\}\\ &-\frac{1}{[F:K]}\left\{\begin{array}{ll}\iota_{P,Q}\{\alpha_1(P),\Delta^{*\rho_1 p}_{P,Q}\}_K & \text{if } \Delta^{*\rho_1 p}_{P,Q}\neq 0,\\ 0 & \text{else}\end{array}\right\}\\ &-\frac{1}{[F:K]}\left\{\begin{array}{ll}\iota_{P,Q}\{\alpha_2(P),\Delta^{*\rho_2 p}_{P,Q}\}_K & \text{if } \Delta^{*\rho_2 p}_{P,Q}\neq 0,\\ 0 & \text{else}\end{array}\right\}.\end{aligned}$$

4.5 Connection between rational and non-rational cases

Let $P \in E[p](K)$ be a point such that $\alpha(P) \notin (K^\times)^p$ holds. By $\gamma(P)^p = \alpha(P) \in K^\times$, there is a degree p field extension $M = K(\gamma(P))$ of K. The norm of the element $1+\gamma(P)+\cdots+\gamma^{p-1}(P)$ will be useful.

Lemma 4.24. *We have the identity* $N_{M/K}(1+\gamma(P)+\cdots+\gamma^{p-1}(P)) = (1-\alpha(P))^{p-1}$.

Proof. We have $\Big(1+\gamma(P)+\cdots+\gamma^{p-1}(P)\Big)(1-\gamma(P)) = 1-\gamma^p(P) = 1-\alpha(P)$ and since the norm is multiplicative:

$$N_{M/K}\Big(1+\gamma(P)+\cdots+\gamma^{p-1}(P)\Big) = \frac{N_{M/K}(1-\alpha(P))}{N_{M/K}(1-\gamma(P))}.$$

As $1-\alpha(P)$ is an element of K, its norm is just $(1-\alpha(P))^p$. The norm of $1-\gamma(P)$ is found by using the equality

$$(X-\gamma(P))(X-\zeta\gamma(P))\cdots(X-\zeta^{p-1}\gamma(P)) = X^p-\gamma^p(P) = X^p-\alpha(P)$$

where ζ is a primitive pth root of unity and by substituting $X=1$. □

As announced, when we are in the rational case, we may choose γ in Definition 2.8 such that it has the following nice property.

Lemma 4.25. *For all $Q \in E[p](K)$ such that P and Q generate $E[p](K)$, there exists a γ as in Definition 2.8 such that we have $\gamma(aQ+bP) = \gamma(Q)^a\gamma(P)^b$ for $0 \le a, b \le p-1$.*

Proof. Let P and Q be two p-torsion points that generate $E[p](K)$. The only constraint in choosing γ in Definition 2.8 is that for all $T \in E[p](K)$ and all $\sigma \in G_K$ the equality

$$e(\xi_\sigma, T) = \frac{\sigma(\gamma)(T)}{\gamma(T)} = \frac{\sigma(\gamma(\sigma^{-1}T))}{\gamma(T)}$$

must hold, where we write ξ_σ for $\xi(\sigma)$. We know that there exists a γ such that this relation holds for P and Q. We take such a γ and we will below use this one to define a new one on the other points of the form $aQ+bP$ for $0 \le a, b, \le p-1$.

We must satisfy the relation

$$\frac{\sigma(\gamma(aP+bQ))}{\gamma(aP+bQ)} = e(\xi_\sigma, aP+bQ).$$

For the right-hand side we have

$$\begin{aligned} e(\xi_\sigma, aP+bQ) &= e(\xi_\sigma, P)^a e(\xi_\sigma, Q)^b \\ &= \frac{\sigma(\gamma(P))^a}{\gamma(P)^a}\frac{\sigma(\gamma(Q))^b}{\gamma(Q)^b} \\ &= \frac{\sigma\left(\gamma(P)^a\gamma(Q)^b\right)}{\gamma(P)^a\gamma(Q)^b} \end{aligned}$$

for $0 \leq a, b \leq p-1$. Thus by setting $\gamma(aP+bQ) = \gamma(P)^a\gamma(Q)^b$, our new γ satisfies all restrictions. □

Remark 4.26. In the non-rational case we are free to define $\gamma(aP) = \gamma(P)^a$ for the rational point P and for $0 \leq a \leq p-1$ but we also have the relation

$$e(\xi_\sigma, Q+P) = \frac{\gamma(\sigma^{-1}(Q+P))}{\gamma(Q+P)} = \frac{\sigma(\gamma(Q))}{\gamma(Q+P)}$$

with $\sigma(Q) = Q+P$, so we cannot in general define γ as in Lemma 4.25.

Remark 4.27. In the rational case for $p = 3$, if we choose our γ as in Lemma 4.25, then we can rewrite the expression that we found for $\Delta^{*3}_{P,Q}$ in Proposition 4.16:

$$\begin{aligned} &\alpha(Q) + \alpha(Q+P) + \alpha(Q+2P) - 3\gamma(Q)\gamma(Q+P)\gamma(Q+2P) \\ &\qquad = \alpha(Q)(1 - 2\alpha(P) + \alpha(P)^2) \\ &\qquad = \alpha(Q)(1-\alpha(P))^2 \\ &\qquad = \alpha(Q)N_{M/K}(1 + \gamma(P) + \cdots + \gamma(P)^2). \end{aligned}$$

The following theorem shows that whereas we have distinguished the rational case and the non-rational case, for practical applications we need not do so. We may always use the formula supplied by Theorem 4.22.

Theorem 4.28. *Let $P, Q \in E[p](K)$ such that P and Q generate $E[p](\overline{K})$. If $\Delta_{P,Q}$ is invertible in R_ρ then we have*

$$\{\alpha(P), \alpha(Q)\}_K = \{\alpha(P), \Delta^{*p}_{P,Q}\}_K.$$

Proof. If $\Delta_{P,Q}$ is invertible in R_ρ, then it is a Skolem–Noether element for $e(Q,P)$. This means that choosing $a = \alpha(P)$ and $b = \Delta^{*p}_{P,Q}$ in the proof of 4.7, the symbol (χ_a, b) represents R_ρ. The result follows by Theorem 4.7 and by injectivity of $\iota_{P,Q}$. □

Inspired by the case for $p = 3$, one may guess that the Hilbert symbols from Theorem 4.28 are equal precisely because their second arguments differ by the norm from Lemma 4.24. This is the statement of the following conjecture.

Conjecture 4.29. *Let K be a non-Archimedean local field of characteristic zero and R the étale algebra of $E[p](\overline{K})$ over K. Let $\alpha \in R^{\times}$ and $\rho \in (R \otimes_K R)^{\times}$ be compatible representatives for some $[\xi] \in H^1(K, E[p])$ and choose γ as in Lemma 4.25. Let $P, Q \in E[p](K)$ be such that P and Q generate $E[p](\overline{K})$.*

Then we have

$$\Delta^{*p}_{P,Q} = \alpha(Q)(1-\alpha(P))^{p-1}. \tag{4.2}$$

In fact, we can state a more general conjecture that does not involve E or any specific points of $E[p](K)$, but which is a conjecture purely on a possible equality in a certain two-dimensional $\mathbb{Q}(\zeta_p)$-algebra. To remind us what inspired the conjecture, we use the notation P and Q for indeterminates that arise from δ_P and δ_Q.

Conjecture 4.30. *Let p be an odd prime number and $A = (A, +, *)$ be the $\mathbb{Q}(\zeta_p)$-algebra given by $A = \mathbb{Q}(\zeta_p)[P,Q]/(Q * P - \zeta_p^2 * P * Q)$. Then we have*

$$\left(\sum_{i=0}^{p-1} Q * P * \zeta_p^{-i}\right)^p = Q^p * (1 - P^p)^{p-1}. \tag{4.3}$$

Lemma 4.31. *Conjecture 4.30 implies Conjecture 4.29.*

Proof. The $\mathbb{Q}(\zeta_p)$-algebra A from Conjecture 4.30 is contained in R_ρ from Conjecture 4.29 if we identify P and $Q \in A$ with δ_P and $\delta_Q \in R_\rho$ respectively. Under such identification, equations (4.2) and (4.3) are equal. □

4.6 Numerical evidence

We now present a small bit of Magma code to check equality (4.3) for any odd prime p up to a chosen bound. We generate an algebra over $\mathbb{Q}(\zeta_p)$ containing δ_Q and δ_P (and consequently also $\delta_{Q+P}, \delta_{Q+2P}, \ldots, \delta_{Q+(p-1)P}$ and $\Delta_{P,Q}$) and we impose multiplication rules for these elements. We denote $\mathtt{z} = \varepsilon(Q, P)$ and use the fact that in the rational case, with choice of γ as in Lemma 4.25 we have

$$\begin{aligned}
\delta_{Q+iP} * \delta_P &= \varepsilon(Q,P)\rho(Q+iP, P)\delta_{Q+(i+1)P} \\
&= \varepsilon(Q,P)\frac{\gamma(Q+iP)\gamma(P)}{\gamma(Q+(i+1)P)}\delta_{Q+(i+1)P} \\
&= \varepsilon(Q,P)\left\{\begin{array}{ll} 1 & \text{if } i < p-1 \\ \alpha(P) & \text{if } i = p-1 \end{array}\right\}\delta_{Q+(i+1)P}.
\end{aligned}$$

Replacing `B` with a chosen bound in the following code checks equality of (4.2) for all odd primes up to and including the chosen bound.

```
Bound := B;
for p in [3..Bound] do
  if IsPrime(p) then
    K<z> := CyclotomicField(p);
    FF<Q,P> := FreeAlgebra(K,2);
    J := ideal<FF|[Q*P - z^2*P*Q]>;
    AA<Q,P> := quo<FF|J>;
    a := AA!0;
    for i in [0..(p-1)] do
      a := a + Q*P^i*z^(p-i);
    end for;
    if a^p eq Q^p*(1-P^p)^(p-1) then
      "True for p =", p;
    else
      "False for p =", p;
    end if;
  end if;
end for;
```

Using the online MAGMA calculator with only 120 seconds of computing time, we were able to check that (4.2) is true for all odd primes up to and including 29.

A | Principal homogeneous spaces

This chapter is on principal homogeneous spaces under an elliptic curve. This topic is needed to understand the results of Chapter 3. We follow the introduction by Silverman [Sil09] Chapter X.3. Principal homogeneous spaces turn out to give a nice description of the Tate–Shafarevich group.

Definition A.1. Let E be an elliptic curve over a perfect field K. A principal homogeneous space under E over K is a smooth curve C over K together with a K-morphism $+ : C \times E \to C$ that satisfies the following properties:

1. $p + \mathcal{O} = p$ for all $p \in C(\overline{K})$,
2. $(p + P) + Q = p + (P + Q)$ for all $p \in C(\overline{K})$ and all $P, Q \in E(\overline{K})$,
3. for all $p, q \in C(\overline{K})$ there is a unique $P \in E(\overline{K})$ satisfying $p + P = q$.

Example A.2. An elliptic curve E itself together with the addition on E is a principal homogeneous space under itself over its field of definition.

For those familiar with the notion of a G-torsor for a group G, we remark that if we disregard their scheme structure, then principal homogeneous spaces under E are indeed $E(\overline{K})$-torsors. Over a smaller field however, principal homogeneous spaces may have no points, let alone a marked point. They are therefore not, in general, elliptic curves themselves.

Since the notation $+$ for the group action turns out to be intuitive, but slightly confusing, we will always denote points of E with upper case letters and points of a principal homogeneous space with lower case letters. Remark that in this chapter, and in this chapter only, we drop the convention that p denotes the odd prime number that is fixed throughout our actual calculations.

Remark A.3. Since the action of E on a principal homogeneous space C is regular, for any two points $p, q \in C(\overline{K})$ we can define $q - p \in E(\overline{K})$ as the point P such that $p + P = q$ holds.

Lemma A.4. *Let C/K be a principal homogeneous space under E/K. Then for all $p, q \in C(\overline{K})$ and all $P, Q \in E(\overline{K})$ we have the properties:*

1. $p - p = \mathcal{O}$,
2. $p + (q - p) = q$,
3. $(p + P) - p = P$,

4. $(q - Q) - (p + P) = (q - p) + Q - P.$

Proof. These are all just simple manipulations. We do need to be careful in placing the parentheses since without them some expressions would not make sense. □

To give a description of the Tate–Shafarevich group that will be useful for us, it is necessary to define an equivalence relation on the collection of principal homogeneous spaces under E over K. We will further state some technical propositions that allow us to study K-rational points on principal homogeneous spaces and in particular k_v-rational points that are needed in Theorem 3.6.

Definition A.5. We call two principal homogeneous spaces C and C' under E (all over a field K) equivalent if there is a K-isomorphism $\varphi : C \to C'$ such that the following diagram commutes:

$$\begin{tikzcd}
C(\overline{K}) \times E(\overline{K}) \arrow[r, "(\varphi{,}\mathrm{id})"] \arrow[d, "+"'] & C'(\overline{K}) \times E(\overline{K}) \arrow[d, "+'"'] \\
C(\overline{K}) \arrow[r, "\varphi"] & C'(\overline{K})
\end{tikzcd}$$

We further call the class of E the trivial class and the collection of all equivalence classes the Weil-Châtelet group denoted by $\mathrm{WC}(E/K)$.

Remark A.6. The 'group' part of the name Weil-Châtelet group is justified by the group structure induced by the map from Theorem A.10 below.

Lemma A.7. *Let C/K be a principal homogeneous space under E over K. Fix a point $p_0 \in C(\overline{K})$ and define a map $\theta_0 : E(\overline{K}) \to C(\overline{K})$ by $\theta_0(P) = p_0 + P$. Let $K(p_0)$ denote the smallest field such that $p_0 \in C(K(p_0))$ holds. Then θ_0 is an isomorphism defined over $K(p_0)$ that is equivariant under the action of E.*

Proof. See [Sil09] Proposition X.3.2. □

Corollary A.8. *The subtraction map $- : C \times C \to E$ given in Remark A.3 is a K-morphism.*

Proof. That it is a morphism follows from Lemma A.7 and the fact that subtraction on E is a morphism. That it is defined over K follows from checking the equality $\sigma(q - p) = \sigma(q) - \sigma(p)$ for $\sigma \in G_K$ and using the fact that addition on $E(\overline{K})$ and the action of $E(\overline{K})$ on $C(\overline{K})$ are defined over K. □

Proposition A.9. *Let C/K be a principal homogeneous space under E over K. Then C/K is trivial in $\mathrm{WC}(E/K)$ if and only if $C(K) \neq \emptyset$ holds.*

Proof. If C/K is in the trivial class, then by definition there exists a K-isomorphism $\theta : E \to C$ and $\theta(\mathcal{O}) \in C(K)$ holds. Conversely, let $p_0 \in C(K)$ be a point. Then the map $\theta_0 : E \to C$ given in Lemma A.7 suffices. □

We now give the theorem that shows the connection between the Weil-Châtelet group and the Tate–Shafarevich group.

THEOREM A.10. *Let E/K be an elliptic curve. For any principal homogeneous space C/K under E/K choose a point $p_0 \in C(\overline{K})$. Then the map*

$$\begin{aligned}\phi_0 : \mathrm{WC}(E/K) &\to H^1(G_K, E)\\ [C/K] &\mapsto [\sigma \mapsto \sigma(p_0) - p_0]\end{aligned}$$

is a bijection.

Proof. See [Sil09] Theorem X.3.6. □

REMARK A.11. One of the possible ways to make $\mathrm{WC}(E/K)$ into a group is to use this bijection. Phrased in the language of Weil-Châtelet groups, we find an alternative definition for the Tate–Shafarevich group.

DEFINITION A.12. Let E/K be an elliptic curve. Then its Tate–Shafarevich group Ш(E/K) is the subgroup of $\mathrm{WC}(E/K)$ given by

$$Ш(E/K) = \ker\left\{\mathrm{WC}(E/K) \longrightarrow \prod_{v \in M_K} \mathrm{WC}(E/K_v)\right\}.$$

If $x \in Ш(E/K)$ is an element that corresponds to a principal homogeneous space $C/K \in \mathrm{WC}(E/K)$, we say that C/K represents x.

When we combine this definition of Ш(E/K) with Proposition A.9 we see that elements of Ш(E/K) represented as principal homogeneous spaces always have points everywhere locally. This allows us to choose such points P_v in Theorem 3.6.

DEFINITION A.13. Let C/K be a principal homogeneous space under E/K and let $p_0 \in C(\overline{K})$ be a point. Then there is a map

$$\begin{aligned}\mathrm{sum} : \mathrm{Div}^0(C) &\longrightarrow E,\\ \sum_{p \in C(\overline{K})} n_p(p) &\mapsto \sum_{p \in C(\overline{K})} [n_p](p - p_0).\end{aligned}$$

We call this map the summation map on $C(\overline{K})$.

LEMMA A.14. *The summation map is independent of the choice of p_0.*

Proof. Let sum' be a summation map defined by the point p_0' and consider

$$\mathrm{sum}(D) - \mathrm{sum}'(D) = \sum_{p \in C(\overline{K})} [n_p]\left\{(p - p_0) - (p - p_0')\right\} = \sum_{p \in C(\overline{K})} [n_p](p_0' - p_0) = \mathcal{O}$$

by $\deg(D) = 0$. □

THEOREM A.15. *There is an exact sequence*

$$1 \longrightarrow \overline{K}^\times \longrightarrow \overline{K}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \xrightarrow{\mathrm{sum}} E(\overline{K}) \longrightarrow 0.$$

Proof. The only non-trivial statements are that the sequence is exact at $E(\overline{K})$ and at $\mathrm{Div}^0(C)$, i.e. sum is a surjective homomorphism and $\mathrm{div}(\overline{K}(C)^\times) = \ker(\mathrm{sum})$. The fact that sum is a homomorphism follows immediately from its definition and the fact that addition on an elliptic curve is commutative. Let $P \in E(\overline{K})$ be a point. Then an easy computation shows that for all $p_0 \in C(\overline{K})$ the equality $\mathrm{sum}\left((p_0 + P) - (p_0)\right) = P$ holds and thus sum is surjective.

Exactness at $\mathrm{Div}^0(C)$ follows from application of Lemma 2.2 after having fixed an isomorphism $\phi : C \to E$ defined by $p \mapsto p - p_0$ for some $p_0 \in C(\overline{K})$. □

Remark A.16. In Fact 3.4 we claimed for each $T \in E[p](\overline{K})$ the existence of degree zero divisors $\mathfrak{a}_T$ on C that satisfy $\mathrm{sum}(\mathfrak{a}_T) = T$ and functions $f_T \in \overline{k}(C)$ that satisfy $\mathrm{div}(f_T) = p\mathfrak{a}_T$. The existence of such divisors and rational functions follows from Theorem A.15.

B | Central simple algebras

This chapter deals with basic results on central simple algebras and is aimed at the reader unfamiliar with this topic. It discusses the Hasse invariant and the Hilbert norm residue symbol in terms of which the Cassels–Tate pairing can be written by Theorem 3.6 and Proposition 2.28.

Definition B.1. Let K be a field. A K-algebra is a finite-dimensional K-vector space A together with a multiplication that is associative, distributes over addition and has a unit element 1_A and together with a ring homomorphism $K \to K \cdot 1_A$ such that $K \cdot 1_A \subset Z(A)$ holds where $Z(A)$ denotes the centre of A. The multiplication on A need not in general be commutative.

B.1 The Brauer group

A lot of what is discussed here can be found in textbooks on the subject that may differ greatly in their chosen presentations. See for example [GS06], [Ser80] parts III and IV or the lecture notes of a Class Field Theory course taught by Tom Fisher [Fis05].

Definition B.2. Let K be a field and A a K-algebra. A is called

- *central* if the centre of A is K, and
- *simple* if the only two-sided ideals of A are 0 and A itself and $A \neq 0$ holds.

Example B.3. Let D be a division algebra over a field K. Then D is simple and its centre $Z(D)$ is a field extension of K. To see the latter we only need that $Z(D)$ is multiplicatively closed. Thus D is a central simple algebra over $Z(D)$.

Example B.4. Let D be a division algebra (over its centre), then for every positive integer n, the algebra $\mathrm{Mat}_n(D)$ is a central simple algebra over $Z(D)$.

Theorem B.5 (Artin–Wedderburn). *Let A be a central simple algebra over K. Then there are a division algebra D and a positive integer n such that there is an isomorphism $A \cong \mathrm{Mat}_n(D)$. These D and n are uniquely determined up to isomorphism of D.*

Proof. This is Theorem 2.1.3 from [GS06]. □

Definition B.6. For a K-algebra $(A, +, \cdot)$ we define $A^{\mathrm{opp}} = (A, +, *)$ with $a * b = b \cdot a$.

Lemma B.7. *If A is a central simple K-algebra, then A^{opp} is also a central simple K-algebra.*

Proof. Immediate from the definition. □

Proposition B.8. *Let $A \neq 0$ be a K-algebra and let $\mathrm{End}_K(A)$ be the K-algebra of endomorphisms of $(A, +)$ as a vector space. Then A is a central simple algebra if and only if*

$$\phi : A \otimes_K A^{\mathrm{opp}} \longrightarrow \mathrm{End}_K(A),$$
$$a \otimes b \mapsto (x \mapsto axb).$$

is an isomorphism of K-algebras.

Proof. This is Proposition 5.3 from [Fis05]. □

Corollary B.9. *Let L/K be a field extension. Then an algebra A over K is a central simple algebra over K if and only if $A \otimes_K L$ is a central simple algebra over L. In particular, A is a central simple algebra over K if and only if for some integer n we have $A \otimes_K \overline{K} \cong \mathrm{Mat}_n(\overline{K})$.*

Proof. If A is a central simple algebra over K, then we apply Proposition B.8 to find

$$(A \otimes_K L) \otimes_L (A^{\mathrm{opp}} \otimes_K L) \cong (A \otimes_K A^{\mathrm{opp}}) \otimes_K L \cong \mathrm{End}_K(A) \otimes_K L \cong \mathrm{End}_L(A \otimes_K L).$$

Applying Proposition B.8 in the other direction shows that $A \otimes_K L$ is central simple over L.

Conversely, if A contains a non-trivial two-sided ideal I, then $A \otimes_K L$ contains a non-trivial two-sided ideal $I \otimes_K L$. If the center of A contains an element a, then $a \otimes 1$ lies in the center of $A \otimes_K L$. Thus if $A \otimes_K L$ is central simple over L, then A is central simple over K.

The second assertion follows since the only division algebra over an algebraically closed field $\overline{K}$ is $\overline{K}$ itself. □

A further observation that can be made from the latter part of this corollary is that for A a central simple algebra over K the dimension $[A : K] = [A \otimes_K \overline{K} : \overline{K}]$ is always a square.

Corollary B.10. *If A and B are two central simple algebras over a field K, then so is $A \otimes_K B$.*

Proof. By Corollary B.9, we may write $A \otimes_K \overline{K} \cong M_n(\overline{K})$ and $B \otimes_K \overline{K} \cong M_m(\overline{K})$ for some positive integers n and m. We have $(A \otimes_K B) \otimes_K \overline{K} \cong M_{n \cdot m}(\overline{K})$ and conclude that $A \otimes_K B$ is central simple by applying Corollary B.9 again. □

Definition B.11. Let $A \cong \mathrm{Mat}_n(D)$ and $A' \cong \mathrm{Mat}_{n'}(D')$ be two central simple algebras over a field K where D and D' are division algebras. Then A and A' are called *similar* if $D \cong D'$ holds.
The Brauer group $\mathrm{Br}(K)$ of K is the set of similarity classes of central simple algebras over K with multiplication $\otimes_K$.

Remark B.12. The identity in the Brauer group $\mathrm{Br}(K)$ is the class of matrix algebras with coefficients in K. The inverse of a class $[A]$ is the class $[A^{\mathrm{opp}}]$.

The following Proposition shows why we need not consider the fields $\mathbb{R}$ and $\mathbb{C}$ for our purposes.

Proposition B.13. *The Brauer group of $\mathbb{R}$ is of order 2 and the Brauer group of $\mathbb{C}$ is trivial. Therefore the local pairing with respect to an infinite place is trivial. (This uses that p is odd.)*

Proof. For a proof of the first assertion involving the cohomological definition of the Brauer group, see [Ser80].

For a local field K (where for now we again include $K = \mathbb{R}$ and $K = \mathbb{C}$), we have $H^2(K, \mu_p) \cong \mathrm{Br}(K)[p]$. For an infinite place $v \in M_k$ we have either $k_v \cong \mathbb{R}$ or $k_v \cong \mathbb{C}$, so in particular $\mathrm{Br}(k_v)[p]$ is trivial since p is odd. Therefore q_{k_v} is trivial for infinite places $v \in M_k$. □

Remark B.14. Let K be any algebraically closed field and let D be a division algebra over K of finite dimension. Take $a \in D \setminus K$. Then we have $K \subsetneq K(a) \subsetneq D$ but $K(a)$ is a commutative division algebra and therefore a field. Thus all central simple algebras over K are isomorphic to $\mathrm{Mat}_n(K)$ for positive integer n and therefore the Brauer group of K is trivial.

B.2 Cyclic algebras

Definition B.15. Let A be a central simple algebra over K and let L/K be a finite extension. We say that A is split over L or that L splits A if there exists $n \in \mathbb{Z}_{\geq 1}$ such that we have $A \otimes_K L \cong \mathrm{Mat}_n(L)$.

Definition B.16. If L/K is a finite extension, then $\mathrm{Br}(L/K)$ is the subgroup of $\mathrm{Br}(K)$ that is represented by algebras that are split over L.

Remark B.17. Alternatively phrased, for an extension $K \subset L$ we have a homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$ given by $[A] \mapsto [A \otimes_K L]$ and $\mathrm{Br}(L/K)$ is its kernel. This immediately shows that $\mathrm{Br}(L/K)$ is a subgroup.

Proposition B.18. *Every central simple algebra A over K is split over some finite field extension L/K and we have*

$$\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$$

where the union ranges over all finite extensions of K.

Proof. See [Mil13] Proposition IV.2.17. □

Lemma B.19. *Let A be a central simple algebra over a field K and let L/K be a field extension contained in A. Then the following are equivalent:*

1. *L is a maximal commutative subalgebra of A, and*

2. $[A : K] = [L : K]^2$.

Proof. See [Mil13] Corollary IV.3.4. □

THEOREM B.20 (Splitting Theorem). *Let K be a field and A a central simple algebra over K. Let L be a finite extension of K. Then L splits A if and only if there exists a central simple algebra B over K that contains L as a maximal commutative subalgebra such that $[A] = [B] \in \mathrm{Br}(K)$ holds.*

Proof. See [Mil13] Corollary IV.3.6. □

THEOREM B.21 (Skolem–Noether). *Let K be a field, let A be a simple K-algebra and B a central K-algebra. Let $f, g : A \to B$ be two K-algebra homomorphisms. Then there is an element $b \in B^\times$ such that for all $a \in A$ we have $f(a) = bg(a)b^{-1}$.*

Proof. See [Mil13] Theorem IV.2.10. □

When we use the name Skolem–Noether theorem in the context of central simple algebras, we will mean the following Corollary.

COROLLARY B.22. *Let K be a field and A be a central simple algebra over K. Let $f : A \to A$ be a K-algebra automorphism. Then there is an invertible $a \in A$ such that for all $x \in A$ one has $f(x) = axa^{-1}$.*

Proof. Take $B = A$ in Theorem B.21. □

DEFINITION B.23. Let L/K be a cyclic field extension of degree m and σ be a generator for $\mathrm{Gal}(L/K)$. Let $b \in K^\times$ be an element. Let the group

$$L[v]_{<m} = \left\{ \sum_{i=0}^{m-1} x_i v^i : x_i \in L \right\}$$

be given the multiplication rules

- $v^i x = \sigma^i(x) v^i$ for $x \in L$, and
- $v^m = b$.

We write A for $L[v]_{<m}$ with these multiplication rules and remark without proof that A is a K-algebra. We call an algebra that can be put in this form a cyclic algebra.

PROPOSITION B.24. *Let A be a cyclic algebra over a field K. Then A is also a central simple algebra over K.*

Proof. See [Has32] (1.2) and (1.3). □

DEFINITION B.25. Let K be a field and L/K a cyclic extension. Let σ be a generator for $\mathrm{Gal}(L/K)$. We define a continuous character $\chi : G_K \to \mathbb{Q}/\mathbb{Z}$ by taking compositions as follows:

$$\begin{aligned} \chi : G_K \longrightarrow \mathrm{Gal}(L/K) &\xrightarrow{\sim} \tfrac{1}{m}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z} \\ \sigma &\longmapsto \tfrac{1}{m} \end{aligned}$$

with $m = [L : K]$.

Remark B.26. In the case of Definition B.25, L is the fixed field of $\ker \chi$ and σ is the inverse image of $\frac{1}{m}$ in $\mathrm{Gal}(L/K)$. So from only χ and b we can retrieve the central simple algebra A as given in Definition B.23.

Definition B.27. For χ as in Definition B.25 and $b \in K^\times$, we write (χ, b) for the similarity class of the central simple algebra A as given in Definition B.23.

Proposition B.28. *Let K be a field, L a cyclic extension of K, σ a generator for $\mathrm{Gal}(L/K)$ and $\chi : G_K \to \mathbb{Q}/\mathbb{Z}$ the continuous character as in Definition B.25. Then the map*

$$\begin{array}{rcl} K^\times & \to & \mathrm{Br}(L/K) \\ b & \mapsto & (\chi, b) \end{array}$$

is surjective. Moreover we have $(\chi, b_1) = (\chi, b_2)$ if and only if $b_1 b_2^{-1}$ is a norm from L.

Proof. This proof is taken from [Fis05]. Let $[A] \in \mathrm{Br}(L/K)$ be any class. By the Splitting Theorem B.20, we may assume that A contains L as a maximal commutative subalgebra. The Skolem–Noether theorem in this context B.22 assures that there is an invertible $v \in A$ such that $\sigma(x) = vxv^{-1}$ holds for all $x \in A$. Equivalently we have $v^i x = \sigma^i(x) v^i$ for all $x \in A$ and all $i \in \mathbb{Z}_{\geq 1}$.

Let $m = [L : K] = [A : L]$. It can be shown that $1, v, v^2, \ldots, v^{m-1}$ forms a basis for A as an L-vector space. Since v^m commutes with every element of L and therefore lies in the centre of A, we have $v^m \in K$ since A is central. We have $[A] = (\chi, v^m)$.

Since L is maximal commutative, the choice of v is unique up to multiplication by units of L. Let $x \in L^\times$. We have

$$(xv)^m = \left(\prod_{i=0}^{n-1} vxv^{-1} \right) v^m = \left(\prod_{i=0}^{n-1} \sigma^i(x) \right) v^m = N_{L/K}(x) v^m,$$

so indeed b is unique up to multiplication by elements of $N_{L/K}(L^\times)$. □

Remark B.29. Proposition B.28 allows us to represent any class of $\mathrm{Br}(K)$ by a cyclic algebra. In the case where K is a local field, we will use the symbol (χ, b) to define the Hilbert norm residue symbol. For the central simple algebra R_ρ and a suitable choice of χ and b, we will write R_ρ as a cyclic algebra (χ, b) and we will use its associated Hilbert symbol to calculate the Tate local pairing $[\ ,\ ]_K$.

B.3 Hasse invariant

To define the Hilbert norm residue symbol in a convenient way, we will need the Hasse invariant. This invariant was encountered in the definition of the local pairings $(\ ,\ )_v$ and further in Proposition 2.28.

For this section, let K be a local field (remember that by this we mean a finite extension of $\mathbb{Q}_\ell$ for some prime number ℓ).

Proposition B.30. *Every central simple algebra A over K is split by some finite unramified extension of K. In particular we can write*

$$\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$$

where the union only ranges over the finite unramified extensions of K.

Proof. See [Ser67], page 137-138. □

Fact B.31. Every unramified extension of a local field is Galois. See [Ser80] Theorem III.5.3.

Definition B.32. Let L/K be an unramified extension of local fields. Let $\mathcal{O}_L$ be the ring of integers of L with maximal ideal $\mathfrak{m}_L$ and let q be the order of the residue field of K. Then there exists (see [Ser80] page 23) a unique element $\mathrm{Frob}_{L/K} \in \mathrm{Gal}(L/K)$ that acts on $a \in \mathcal{O}_L$ by

$$\mathrm{Frob}_{L/K}(a) \equiv a^q \bmod \mathfrak{m}_L.$$

We call $\mathrm{Frob}_{L/K}$ the Frobenius in $\mathrm{Gal}(L/K)$. The Frobenius in $\mathrm{Gal}(L/K)$ is a generator for $\mathrm{Gal}(L/K)$.

Remark B.33. $\mathrm{Frob}_{L/K}$ is a lift of the automorphism of the residue field extension $\mathcal{O}_K/\mathfrak{m}_K \subset \mathcal{O}_L/\mathfrak{m}_L$ that is given by raising to the power q.

Definition B.34. Let L/K be an unramified extension of degree n. Let ord_K be the normalized valuation on K. Then we define a pre-Hasse invariant $\mathrm{inv}_{L/K}$ as follows:

$$\begin{aligned}\mathrm{inv}_{L/K} : \mathrm{Br}(L/K) &\longrightarrow \tfrac{1}{n}\mathbb{Z}/\mathbb{Z},\\ (\chi, b) &\mapsto \mathrm{ord}_K(b) \cdot \chi(\mathrm{Frob}_{L/K}).\end{aligned}$$

Remark B.35. Defined in such a way, $\mathrm{inv}_{L/K}$ is a homomorphism of groups and is independent of choices of χ and b. See [Fis05] pages 62-64.

Remark B.36. If A is a central simple algebra such that $[A] \in \mathrm{Br}(K/L)$ holds, then $A \otimes_L L \cong M_n(L)$ holds. If $L \subset M$ is a field extension, then we have

$$A \otimes_K M \cong (A \otimes_K L) \otimes_L M \cong M_n(L) \otimes_L M \cong M_n(M)$$

and therefore $[A] \in \mathrm{Br}(M/K)$.

Lemma B.37. *If $K \subset L \subset M$ is a tower of unramified extensions, then the following diagram is commutative*

$$\begin{tikzcd} \mathrm{Br}(L/K) \arrow[r, "\mathrm{inv}_{L/K}"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\ \mathrm{Br}(M/K) \arrow[r, "\mathrm{inv}_{M/K}"] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

where the left vertical arrow is the natural inclusion.

Proof. Proposition I.8.23b from [Ser80] shows that $\chi(\mathrm{Frob}_{M/K}) = \chi(\mathrm{Frob}_{L/K})$ holds which proves the lemma. □

This lemma allows us to define the Hasse invariant.

DEFINITION B.38. The Hasse invariant $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ is defined through the union $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$ over the unramified extensions of K by the pre-Hasse invariants.

We conclude this section with a statement that allows us to take field extensions of degree coprime to p. This is analogous to Proposition 1.14.

LEMMA B.39. *Let E/K be a finite extension. Then we have*

$$\mathrm{inv}_E(\chi|_{G_E}, b) = \mathrm{inv}_K(\chi, N_{E/K}(b)).$$

Proof. See [Fis05] Lemma 5.9. □

PROPOSITION B.40. *Let F/K be a finite extension. Let $\phi : \mathrm{Br}(K) \to \mathrm{Br}(F)$ be given by $[A] \mapsto [A \otimes_K F]$. Then the following diagram is commutative:*

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "\phi"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\times[F:K]"] \\
\mathrm{Br}(F) \arrow[r, "\mathrm{inv}_E"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Proof. See [Fis05] Lemma 5.10 or [Ser80] Proposition XIII.3.7 for a cohomological proof. □

B.4 HILBERT SYMBOL

Finally, we arrive at the Hilbert norm residue symbol that we use in our formulas for the Tate local pairing. Once again recall that by 'local field' we mean non-Archimedean local field of characteristic zero.

DEFINITION B.41. Let n be a positive integer and let K be a local field containing μ_n. Let ζ be a generator for μ_n. Let $a \in K^\times$ and $x \in K^{\mathrm{sep}}$ be such that $x^n = a$. Then we define a character

$$\begin{aligned} \chi_a : G_K \longrightarrow \mathrm{Gal}(K(x)/K) &\longrightarrow \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}, \\ (x \mapsto \zeta x) &\longmapsto \frac{1}{n} \bmod \mathbb{Z}. \end{aligned}$$

REMARK B.42. The character χ_a is independent of choice of x but not independent of choice of ζ.

DEFINITION B.43. Let n be a positive integer and let K be a local field containing μ_n. Let ζ be the generator of μ_n used to define χ_a. The Hilbert norm residue symbol, or Hilbert symbol for short, is the function $\{\ ,\ \}_{K,n} : K^\times \times K^\times \to \mu_n$ given by

$$\{a, b\}_{K,n} = \zeta^{n\,\mathrm{inv}_K(\chi_a, b)}.$$

We will leave out the reference to the index n as in all of its applications we will always use $n = p$. Where no confusion is likely to arise, we will also leave out the reference to the field K.

Remark B.44. The Hilbert symbol is well-defined. A different choice of generator for μ_n yields the same symbol. This can easily be seen using that if two nth roots of unity ζ and ζ' are both primitive, then there is an integer m coprime to n such that $\zeta' = \zeta^m$ holds. And then also $\chi_a = m\chi'_a$ holds (where χ' is defined using ζ') and we use $\mathrm{inv}_{\mathrm{K}}(m\chi, b) = m \cdot \mathrm{inv}_K(\chi, b)$.

Proposition B.45. *Let K be a local field containing μ_n. Its nth Hilbert symbol*

1. *is multiplicative in the first and second argument:*

$$\{a_1, b\}\{a_2, b\} = \{a_1a_2, b\} \text{ and } \{a, b_1\}\{a, b_2\} = \{a, b_1b_2\},$$

2. *induces a non-degenerate pairing on $K^\times/(K^\times)^n$:*

$$\{a, b\} = 1 \text{ for all } b \in K^\times \text{ if and only if } a \in \left(K^\times\right)^n,$$

3. *has the property that if b is a norm from $K(\sqrt[n]{a})$, then:*

$$\{a, b\} = 1.$$

Proof. See [Ser80] Proposition XIV.4. □

Bibliography

[Cas59] J.W.S. Cassels. Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 202:95–112, 1959.

[Cas98] J.W.S. Cassels. Second descent for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998.

[CFO$^+$08] J.E. Cremona, T.A. Fisher, C. O'Neill, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves, I Algebra. *J. reine angew. Math.*, 615:121–155, 2008.

[Fis05] T.A. Fisher. Class Field Theory, 2005. lecture notes available at `http://ricardoingles.no.sapo.pt/matematica/classfieldtheory.pdf`.

[FN13] T.A. Fisher and R.D. Newton. Computing the Cassels-Tate pairing on the 3-Selmer group of an elliptic curve. Preprint available at `http://arxiv.org/abs/1306.1410v1`, 2013.

[GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambrigde University Press, Cambridge, 2006.

[Has32] H. Hasse. Theory of cyclic algebras over an algebraic number field. *Trans. Amer. Math. Soc.*, 34:171–214, 1932.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems.* BookSurge, LLC, Charleston, second edition, 2006.

[Mil13] J.S. Milne. Class field theory, 2013. Lecture notes available at `www.jmilne.org/math`.

[PS99] B.M. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Annals of Mathematics*, 150:1109–1149, 1999.

[Ser67] J.P. Serre. Local Class Field Theory. In Cassels and Frölich, editors, *Algebraic Number Theory*, pages 129–160. Academic Press, London-New York, 1967.

[Ser80] J.P. Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1980.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves 2nd edition*, volume 106 of *Graduate Text in Mathematics.* Springer, Dordrecht Heidelberg London New York, 2009.