ANNALES DE L'INSTITUT FOURIER

KI-SENG TAN

Refined theorems of the Birch and Swinnerton-Dyer type

Annales de l'institut Fourier, tome 45, nº 2 (1995), p. 317-374

<http://www.numdam.org/item?id=AIF_1995__45_2_317_0>

Ann. Inst. Fourier, Grenoble
45, 2 (1995), 317–374

REFINED THEOREMS OF THE BIRCH AND SWINNERTON-DYER TYPE

by Ki-Seng TAN

Introduction.

In their paper [MT2], B. Mazur and J. Tate propose conjectures which are analogues of the classical Birch and Swinnerton-Dyer conjecture for each Weil curve $\mathbb{E}$ defined over $\mathbb{Q}$. In this paper we will generalize the context of their conjectures by replacing $\mathbb{Q}$ by any global field, even of finite characteristic, and sharpen, in a certain way, the statement of their conjectures. Our main result, then, will be to establish the truth of a part of these new sharpened conjectures, provided that one assume the truth of the classical Birch and Swinnerton-Dyer conjectures. This is particularly striking in the function field case, where these results can be viewed as being a refinement of the earlier work of Tate and Milne (see [T2] , [Ml1]), who establish the classical Birch and Swinnerton-Dyer conjecture in that context, subject only to the hypothesis that some ℓ-primary component of the Shafarevitch-Tate group is finite (for any ℓ).

As in the classical Birch and Swinnerton-Dyer conjecture, the main part of the Mazur-Tate conjectures also contains two parts: one is about the «order of vanishing» and the other, the «leading term» (the refined formula). In the Mazur-Tate conjectures, the analogue of the classical L-function is the *theta element.* For each positive integer D, the theta element Θ_D is defined via the modular form associated to $\mathbb{E}$. It is an element of the group ring $\mathbb{Z}[M^{-1}][(\mathbb{Z}/\pm D\mathbb{Z})^*]$, where M is an integer which depends only on $\mathbb{E}$. The theta element interpolates the special values of the L-series attached to the characters of the group $(\mathbb{Z}/\pm D\mathbb{Z})^*$, and is

Key words: Elliptic curve – L-function – Birch and Swinnerton-Dyer conjecture – Mazur-Tate conjecture – Height pairing – Corrected discriminant.
Math. classification: 11G40 – 11G05 – 11G07 – 14G25 – 14K15.

in fact characterized by this property. This theta element can be viewed as a « D-adic L-function », in the sense that if we take $D = p^n$ for a prime p, and $n \geq 1$, and take the projective limit of Θ_{p^n}, then essentially the p-adic L-function studied in [MTT] is obtained.

The « order of vanishing » conjecture says that for D admissible (see Section 3.1) Θ_D should be in the r-th power of the augmentation ideal I. Here r is the rank of the associated *extended Mordell-Weil group* (see 2.2).

In the refined formula (see conjecture 1 in Section 3.1), the analogue of the elliptic regulator is called the *corrected discriminant*. It is defined via the Mazur-Tate global pairing which depends on D. There is a canonical mapping sending the corrected discriminant into an element of I^r/I^{r+1}. The right-hand side of the refined formula is a product of this element and other arithmetic data of the elliptic curve such as the orders of Ш, $\mathbb{E}(\mathbb{Q})_{\mathrm{tor}}$, etc. The left-hand side is just the image of Θ_D in I^r/I^{r+1}. The conjecture can be viewed as the finite « exponentiation » of the conjecture raised by Mazur, Tate and Teitbaum in [MTT] (see also [MT2]). An interesting feature of these conjectures is the possibility of the « extra order of vanishing », which occurs when $r > rk(\mathbb{E}(\mathbb{Q}))$. In this case, the extra rank of the extended Mordell-Weil group comes from the number of split-multiplicative primes dividing D, and the local Tate period is involved in the conjecture. For result about the case $r = 1$ and $rk(\mathbb{E}(\mathbb{Q})) = 0$, see [GSt].

To generalize the conjecture to each elliptic curve $\mathbb{E}_{/K}$ over a global field K, we need to define the theta element and the corrected discriminant in the general context. The Mazur-Tate pairing and the associated corrected discriminant are actually defined for every global field as long as D is admissible [MT2]. Over the function field, Deligne has shown [D] that every non-constant elliptic curve is modular. Using this, in [M], Mazur defines an associated theta element. In [Tn2] the theta element for any elliptic curve is studied. It is shown that the theta element is in the group ring $\mathbb{Z}[p^{-1}][W_D]$, where p is the characteristic of the field. The coefficients of Θ_D have bounded denominators. For certain cases, a bound can be obtained as a function of the genus of the field and the arithmetic conductor of the elliptic curve.

Over number fields, not much about the theta elements is known except for the case discussed in [MT2] .

In this paper, for each extended divisor D of K (see 1.1), we define the theta element Θ_D as an element of the group ring of the Weil group W_D

characterizing the abelian extensions of K with the conductors dividing D, provided that the analytic continuations of some L-series exist. It is defined to interpolate special values of the L-series attached to characters of W_D. Notice that this definition makes sense for the number field case as well.

For each quotient group G of W_D, we define, via the quotient map, the theta element Θ_G. Assuming that there is an integer M such that $\Theta_G \in \mathbb{Z}[M^{-1}][G]$ (this is true in the Mazur-Tate case and in the function field case) and that D is admissible, we then propose the conjecture (conjecture 1), which generalizes the main part of Mazur-Tate conjecture. Over the function field, this conjecture generalizes the classical Birch and Swinnerton-Dyer conjecture (see 3.2).

Conjecture 1 depends on the chosen integer M. If $r > 0$ and G is killed by M, then it is easy to show that $\Theta_G \in I^i$ for every $i > 0$ and conjecture 1 is trivially true (see 3.3). It is then natural to multiply Θ_G by an integer z such that $z \cdot \Theta_G \in \mathbb{Z}[G]$ and to try to sharpen the conjecture using $z \cdot \Theta_G$. In this paper, we treat the case where G is of the type $(\ell, \dots, \ell)$ for some prime number ℓ (the horizontal case). The reason for choosing this type of group is that the augmentation quotient I^i/I^{i+1} (I being the augmentation ideal of $\mathbb{Z}[G]$) is well studied. A theorem of Passi and Vermani (see [PV], restated as Proposition 3.8 in this paper) identifies this $\mathbb{F}_\ell$-space with the space of $\mathbb{F}_\ell$-valued ith degree homogeneous polynomial functions on the space $G' = \mathrm{Hom}_{\mathbb{F}_\ell}(G, \mathbb{F}_\ell)$. Using this, we are led to believe that $z \cdot \Theta_G$ should be in I^e, for some $e \geq r$ defined in 3.4, and hence, the sharpened conjecture, conjecture 2, is of a refined formula of two elements of I^e/I^{e+1}. We have $e > r$ if and only if ℓ divides z. If this is the case, then conjecture 1, which deals with I^r/I^{r+1}, is trivial while conjecture 2 usually is not.

The main results proved in this paper concern conjecture 2. Assume that G is horizontal. Let L/K be the field extension with Galois group equal to G. To obtain our main theorems, we need to assume that the Birch and Swinnerton-Dyer conjecture is true for $\mathbb{E}_{/K}$, and in the number field case, it is also true for $\mathbb{E}_{/L'}$ for every intermediate field extension L'/K. As our conjectures relate the analytic and the arithmetic feature of an elliptic curve, this kind of assumption seems inevitable unless we are expecting to prove some result about the Birch and Swinnerton-Dyer conjecture. To simplify the argument and to avoid certain difficulties, we also assume that ℓ is outside a finite set of primes which depends only on $\mathbb{E}_{/K}$ (see Definition 3.13). Under these assumptions, we have $z \cdot \Theta_G \in I^e$ (Theorem 3.12) and the eth degree homogeneous polynomial functions corresponding to both sides of the formula in conjecture 2 have the same zero set (Theorem 3.14). These are the main theorems of this paper. They imply that if either G is cyclic or $e = 1$, then conjecture 2 is true up to a non-zero constant in $\mathbb{F}_l^*$ (Theorem 3.16). Theorem 3.21 says conjecture 2 is true, if K is a function field with characteristic ℓ, $\mathrm{rk}(\mathbb{E}(K)) = 0$ and $\Theta_D \in \mathbb{Z}_\ell[G]$. For the examples of elliptic curves satisfying these additional conditions, see [Tn2].

This paper is organized in the following way. In Section 1, we discuss the definition of the theta element. In Section 2, we recall briefly the Mazur-Tate pairing, and the associated corrected discriminant. We also derive some related results to be used in the proofs contained in Section 4.

In Section 3, we discuss the conjectures and state the main results of this paper. Conjecture 1 is proposed in 3.1. In 3.2, we show that in the function field case it generalizes the classical Birch and Swinnerton-Dyer conjecture. In 3.4, we propose conjecture 2 and show that in some special case we can use the main theorems to deduce the truth of conjecture 2.

The proofs of the main theorems, Theorem 3.12 and 3.14, required some preliminary developments. The necessary technical tools are given in Section 4 and 5 and the proofs of the main theorems then follow easily, and thus are postponed until Section 5. The proofs of the main theorems rely on the thorough understanding of the possible degeneracies of the Mazur-Tate pairing. This is the main content of Section 4.

Section 5 then concludes the paper by using the results of Section 4, the Birch and Swinnerton-Dyer Formula, and a product formula for the L-functions (in 5.2) to complete the proofs of the main theorems.

We should remark that some of our main results and their method of proof are analogous to those used by Gross [G], in his formulation of a conjectured refined class number formula, which itself is an analogue of the Mazur-Tate conjecture. In this conjecture, the theta element interpolates the special values of the abelian L-functions and the counterpart of the corrected discriminant is the G-regulator. Gross also uses the product formula of the L-function, the classical class number formula, and the genus theory to obtain a result for the horizontal case. As the Birch and Swinnerton-Dyer formula is an analogue of the class number formula, our theory in Section 4 can be viewed as «the genus theory for elliptic curves». Recently in [Tn4], new results about the Gross conjecture for the «vertical case» (e.g. $G \simeq \mathbb{Z}_\ell$) have been obtained. We hope to discuss the vertical case for the Mazur-Tate conjecture in a forthcoming paper.

Part of this paper is from my Ph. D. Thesis. I would like to thank Barry Mazur, Benedict Gross and my advisor John Tate for their encouragement and suggestions. Thanks also to the referee for valuable criticisms and suggestions and to Dan Rockmore for his patient reading of several versions of the manuscript.

1. The theta element.

In this section, we define the theta element associated to an elliptic curve over a global field and discuss some of its basic properties. To make such a definition, we need to assume the existence of the analytic continuations to $s = 1$ of certain associated L-functions. When the global field is a function field or the elliptic curve is a Weil curve over $\mathbb{Q}$, the theta element will have good rational and integral properties.

1.1. Notations and assumptions.

Let K be a global field. We use the usual notations $\mathbb{A} = \mathbb{A}_K$, $\mathbb{A}^* = \mathbb{A}_K^*$ for the adèle ring and the idèle group of K. For each place v, use respectively the notations K_v, $\mathcal{O}_v$, k_v, q_v, for the completion of K at v, the v-integers of K_v, the residue field (for non-archimedean v) and its order. The notation S_∞ will denote the set of all archimedean places of K.

An *extended divisor* is a formal sum

$$D = \sum_v \alpha_v \cdot v, \qquad \alpha_v \in \mathbb{Z},$$

with the restriction that $\mathrm{ord}_v(D) := \alpha_v$ is 0 for complex v and either 0 or 1 for real v. The finite (non-archimedean) part and the infinite (archimedean) part of D will be denoted by D_0 and D_∞ respectively. The *support of* D, denoted $\mathrm{Supp}(D)$, is the set consisting of places v such that $\mathrm{ord}_v(D) \neq 0$.

Throughout, *whenever* we refer to a quasi-character, we assume that it has the following property.

ASSUMPTION 1. — Each quasi-character χ of the idèle class group $K^* \setminus \mathbb{A}_K^*$ is assumed to be trivial on the connected component of K_v^* for each archimedean v.

Thus for real v, the component χ_v depends only on its value at -1. This is either 1 or -1, in which case we write $\alpha_v(\chi) = 0$ or 1, and call χ *even* or *odd* at v, respectively. For each finite v, use $\alpha_v(\chi) \cdot v$ to denote the *conductor* of the v-component χ_v. From this we define the *extended conductor of* χ as the extended divisor

$$D_\chi = \sum_v \alpha_v(\chi) \cdot v.$$

For a non-archimedean place $v \notin \mathrm{Supp}(D_\chi)$, the value $\chi_v(\pi_v)$ for a prime element π_v of $\mathcal{O}_v$ is independent of the choice of π_v. Thus define

$$\chi(v) = \chi(\pi_v).$$

Analogously, we also define the extended conductor of an abelian extension L/K in the obvious way.

For an extended divisor D, let

$$U_{D_0} = \prod_{v \notin \mathrm{Supp}(D_0)} \mathcal{O}_v^* \cdot \prod_{v \in \mathrm{Supp}(D_0)} \left(1 + \pi_v^{\mathrm{ord}_v(D)} \cdot \mathcal{O}_v\right),$$

$$U_{D_\infty} = \Big(\prod_{v \notin \mathrm{Supp}(D_\infty)} K_v^*\Big) \cdot \Big(\prod_{v \in \mathrm{Supp}(D_\infty)} \mathbb{R}_+^*\Big),$$

where only the non-archimedean (resp. archimedean) v are taken in the first (resp. second) formula. Let $U_D = U_{D_\infty} \times U_{D_0}$. Then U_D can be embedded into $\mathbb{A}^*$ in the obvious way. The (discrete) *Weil group* is defined as

$$W_D = K^* \setminus \mathbb{A}^*/U_D.$$

The Weil group is finite in the number field case. In the function field case, it is an extension of $\mathbb{Z}$ by a finite group. For a place $v \notin \mathrm{Supp}(D)$ the prime element π_v determines an element $[v] \in W_D$ called the *Frobenius element.* This is independent of the choice of π_v.

A quasi-character χ of the Weil group W_D can be pulled back to a quasi-character (also denoted by χ) of the idèle class group $K^* \setminus \mathbb{A}^*$. The quasi-characters obtained from W_D are those whose extended conductors divide D. A quasi-character χ of W_D is called *primitive* if $D_\chi = D$.

Let R be a subring of $\mathbb{C}$. A quasi-character χ of W_D can be extended uniquely to an R-algebra homomorphism from the group ring $R[W_D]$ to $\mathbf{C}$.

All the R-algebra homomorphisms from $R[W_D]$ to $\mathbb{C}$ can be obtained in this way.

Let $\mathbb{E}$ be an elliptic curve defined over K. For each non-archimedean place v, let $\mathbb{E}_{/\mathcal{O}_v}$ be the Néron model of $\mathbb{E}_{/K_v}$ and let $\mathbb{E}_{/k_v}$ be the special fibre of $\mathbb{E}_{/\mathcal{O}_v}$ at v. Denote by $\mathbb{E}_{0_{/k_v}}$ the connected component of $\mathbb{E}_{/k_v}$, $\mathbb{E}_0(K_v)$ the part of $\mathbb{E}(K_v)$ whose reduction at v is in $\mathbb{E}_{0_{/k_v}}$, and $\mathbb{E}_1(K_v)$ the part of $\mathbb{E}_0(K_v)$ with trivial reduction. The number of k_v-rational components of $\mathbb{E}_{/k_v}$ will be denoted by m_v. The arithmetic conductor of $\mathbb{E}_{/K}$ will be denoted by N.

For a real place v, let m_v denote the number of components of $\mathbb{E}(K_v)$ regarded as a topological group. Then m_v is either 1 or 2. Denote the identity component of $\mathbb{E}(K_v)$ by $\mathbb{E}_0(K_v)$.

For a non-archimedean place v, let λ_v be the integer defined by

$$\lambda_v = \begin{cases} 1 + q_v - |\mathbb{E}_0(k_v)| & \text{for good reduction,} \\ q_v - |\mathbb{E}_0(k_v)| & \text{for bad reduction.} \end{cases} \tag{1}$$

For each quasi-character χ and each non-archimedean v not in $\mathrm{Supp}(\chi)$, let

$$L_v(\chi, s) = \begin{cases} 1 - \lambda_v \cdot \chi(v) \cdot q_v^{-s} + \chi(v)^2 \cdot q_v^{1-2s} & \text{if } v \notin \mathrm{Supp}(N), \\ 1 - \lambda_v \cdot \chi(v) \cdot q_v^{-s} & \text{if } v \in \mathrm{Supp}(N). \end{cases} \tag{2}$$

For other v, let $L_v(\chi, s) = 1$. The associated L-series

$$L(\chi, s) = L_{\mathbb{E}_{/K}}(\chi, s)$$

is defined as

$$L(\chi, s) = \prod_v L_v(\chi, s).$$

If χ_0 is the trivial character, we denote

$$L(s) = L_{\mathbb{E}_{/K}}(s) = L(\chi_0, s).$$

In this paper, a field extension L/K is always abelian, with its Galois group usually denoted by G. For a place v of K, we will fix a place w of L, which is sitting over v. Denote $G_v = \mathrm{Gal}(L_w/K_v)$. Sometimes we denote $L_v = L_w$ when the choice of w is not important.

1.2. The global period.

In this section we define the *relative global period* Ω_χ of $\mathbb{E}_{/K}$ associated to a character χ of $\mathbb{A}^*/K^*$. The basic idea comes from Tate's paper [T2].

Let $\mu = (\mu_v)$, where for each place v of K, μ_v is the Haar measure such that

$$\begin{cases} \mu_v(\mathcal{O}_v) = 1 & \text{if } v \text{ non-archimedean,} \\ \mu_v = \text{Lebesgue measure} & \text{if } v \text{ archimedean.} \end{cases}$$

Let d_K, r_2 and g_K denote respectively, the absolute discriminant, the number of complex places and, in the function field case, the genus of K. Recall (*cf.* [W1]) that the measure $|\mu|$ of the compact quotient $\mathbb{A}/K$ can be evaluated as

$$|\mu| = \begin{cases} \|d_k\|^{-1/2}\, 2^{-r_2} & \text{in the number field case,} \\ q^{g_K-1} & \text{in the function field case.} \end{cases} \tag{3}$$

For $x \in K_v$, let $|x|_v$ denote the normalized absolute value, *i.e.*,

$$\mu_v(xU) = |x|_v \cdot \mu_v(U) \quad \text{for } U \subset K_v.$$

Choose a nonzero K-rational first degree invariant differential form ω on $\mathbb{E}$. Then ω and μ_v determine a Haar measure $|\omega|_v\mu_v$ on the compact analytic group $\mathbb{E}(K_v)$ in a well-known way (*cf.* [W2]).

For archimedean v, define the *local period*

$$\Omega_v = \int_{\mathbb{E}(K_v)} |\omega|_v\, \mu_v. \tag{4}$$

For non-archimedean v, let $\omega_{0,v}$ be a local Néron differential, *i.e.* a first degree invariant differential form on the Néron minimal model $\mathbb{E}_{/\mathcal{O}_v}$ such that the restriction $\bar{\omega}_{0,v}$ of $\omega_{0,v}$ on the special fibre $\mathbb{E}_{k_v}$ is nonzero. On the generic fibre, we have $\omega/\omega_{0,v} \in K_v^*$, and define the *local period* Ω_v as

$$\Omega_v = \left|\frac{\omega}{\omega_{0,v}}\right|_v. \tag{5}$$

We put these local data together to define the *global period.*

DEFINITION 1.1. — *With the notation of* (4) *and* (5), *the* global period *is defined as*

(6) $$\Omega = \Omega_{\mathbb{E}/K} = \Omega_K := \prod_v \Omega_v.$$

By the multiplication formula of the norms, $\prod_v |x|_v = 1$, for all $x \in K^*$ and we see that the definition of Ω is independent of the choice of ω.

Consider a Weierstrass equation of $\mathbb{E}$ over K,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and the differential ω (see [T3]),

$$\omega = \mathrm{d}x/2y + a_1x + a_3 = \mathrm{d}y/3x^2 + 2a_2x + a_4 - a_1y.$$

Let δ be the discriminant associated to this equation. For each non-archimedean place v, choose a minimal Weierstrass equation and take the corresponding invariant differential ω'_v in the similar way and let δ_v be the discriminant of this equation.

DEFINITION 1.2. — *Define the global discriminant* $\Delta = \Delta_K$ *by*

(7) $$\Delta = \sum_{v \notin S_\infty} \mathrm{ord}_v(\delta_v) \cdot v.$$

Since each ω'_v can be extended to a Néron differential over $\mathcal{O}_v$, we have the following equality of divisors

(8) $$\Delta - 12 \cdot \sum_{v \notin S_\infty} \mathrm{ord}_v\Big(\frac{\omega}{\omega_{0,v}}\Big) \cdot v = (\delta).$$

Note that if K is a function field with constant field $\mathbb{F}_q$, then Ω is just the norm of $\sum_{v \notin S_\infty} \mathrm{ord}_v(\omega/\omega_{0,v}) \cdot v$, so (8) and the multiplication formula together imply

(9) $$\Omega = q^{-\deg(\Delta)/12}.$$

Let χ be a character of the idèle class group and L/K the cyclic extension determined by χ. Let Odd_χ be the set of real places where χ is odd. For each $v \in \mathrm{Odd}_\chi$, let w be the unique complex place of L sitting over v.

DEFINITION 1.3. — *The* relative global period Ω_χ *is defined as*

$$\Omega_\chi = \prod_{v\in \mathrm{Odd}_\chi} (-1)^{2/m_v} \cdot \frac{\int_{\mathbb{E}(L_w)} |\omega|_w \cdot \mu_w}{\int_{\mathbb{E}(L_v)} |\omega|_v \cdot \mu_v} \cdot \prod_{v\notin \mathrm{Odd}_\chi} \Omega_v. \tag{10}$$

The definition depends on χ and $\mathbb{E}$. It is independent of the choice of ω.

DEFINITION 1.4. — *For each finite separable extension L/K, define the* relative discriminant *(of the elliptic curve $\mathbb{E}$) as*

$$\Delta_{L/K} := \Delta_K - \Delta_L. \tag{11}$$

Here we view Δ_K and hence $\Delta_{L/K}$ as a divisor of L.

Notice that Δ_K is an effective divisor supported only on places which are both ramified (under the extension) and bad (for the elliptic curve). Using (8), one can easily see that $\Delta_{L/K}$ is divisible by 12.

For an abelian extension L/K, by the class field theory we identify each character of $\mathrm{Gal}(L/K)$ with a character of the idèle class group of K. By the definitions of Ω and Ω_χ, the multiplication formula and (8), we have

$$\Omega_L = \|\Delta_{L/K}\|^{-1/12} \cdot \prod_{\chi\in \widehat{\mathrm{Gal}(L/K)}} \Omega_\chi. \tag{12}$$

1.3. The Gauss sum.

Let Ψ be a non-trivial character of the additive group $K \setminus \mathbb{A}_K$ and ϕ a differential idèle attached to Ψ [W1]. The *Gauss sum* is now defined as follows.

DEFINITION 1.5. — *For each place v and quasi-character χ, we define $\tau_{\chi,v}$ as follows. If v is non-archimedean and $\alpha_v = \mathrm{ord}_v(D) > 0$, define*

$$\tau_{\chi,v} = \sum_{x\in \phi_v^{-1}\pi_v^{-\alpha_v}\cdot(\mathcal{O}_v^*/1+\pi_v^{\alpha_v}\mathcal{O}_v)} \Psi_v(x)\chi(x). \tag{13}$$

Otherwise, define

$$\tau_{\chi,v} = \left(2\sqrt{-1}\right)^{\alpha_v}\chi(\phi_v^{-1}). \tag{14}$$

The Gauss sum *is defined as*

$$\tau_\chi = \prod_v \tau_{\chi,v}. \tag{15}$$

It is easy to see that the definition of τ_χ is independent of the choice of Ψ, ϕ and π_v.

Note that our Gauss sums are slightly different from the usual ones. When $K = \mathbb{Q}$, for each positive integer D we can identify $(\mathbb{Z}/D)^*$ with $W_{D+\infty}$ by identifying each prime number p, such that $(p, D) = 1$, with the element $[p] \in W_{D+\infty}$. In this case, for any primitive character χ of $W_{D+\infty} = (\mathbb{Z}/D)^*$, our Gauss sum τ_χ equals $2\sqrt{-1}$ times the usual Gauss sum of χ^{-1}. We define the Gauss sum so as to avoid the appearance of χ^{-1} in the definition of the theta element (see [MT2] and Section 1.4).

The following lemma can be proved by the usual method (see for example [L]).

DEFINITION 1.6. — *For an extended divisor D, define its norm as*

$$\|D\| := \|D_0\| \cdot 2^{-\#\operatorname{Supp}(D_\infty)}. \tag{16}$$

LEMMA 1.7. — *Let χ be a character and $\bar{\tau}_\chi$ be the complex conjugate of τ_χ viewed as complex numbers. Then $\tau_{\chi^{-1}} = \bar{\tau}_\chi$ and*

$$\tau_\chi \cdot \bar{\tau}_\chi = \|D_\chi\|^{-1}.$$

1.4. Theta elements.

In this section, we define the theta element by identifying its characteristic properties.

Throughout, *whenever* we refer to a quasi-character χ of W_D (*cf.* Assumption 1) we assume that it has the following property:

ASSUMPTION 2. — *For any extended divisor D, we assume that the* analytic continuation $L(\chi, 1)$ is defined *for each quasi-character χ of W_D.*

Examples in which Assumption 2 is satisfied include Weil curves and curves over function fields.

Let R be a subring of $\mathbf{C}$. Suppose D and D' are two extended divisor of K such that $D' \succeq D$. Let

$$Z_D : R[W_{D'}] \longrightarrow R[W_D] \tag{17}$$

be the ring homomorphism induced by the projection. Also let

$$V_{D'} : R[W_D] \longrightarrow R[W_{D'}] \tag{18}$$

be the trace map.

Using the above notations we may now define the associated theta element $\Theta_D \in R[W_D]$ using the following characteristic properties.

DEFINITION 1.8. — *The theta element Θ_D is the unique element of $R[W_D]$ which satisfies the following properties:*

(i) *The compatibility property: for $D' \succeq D$, we have the following:*

(a) *If $v \notin \mathrm{Supp}(N) \cup \mathrm{Supp}(D)$ is non-archimedean, then*

$$Z_D(\Theta_{v+D}) = \left(\lambda_v - [v] - [v]^{-1}\right) \cdot \Theta_D.$$

(b) *If $v \in \mathrm{Supp}(N)$ and $v \notin \mathrm{Supp}(D)$, then*

$$Z_D(\Theta_{v+D}) = \left(\lambda_v - [v]^{-1}\right) \cdot \Theta_D.$$

(c) *If v is non-archimedean, $v \notin \mathrm{Supp}(N)$ and $v \in \mathrm{Supp}(D)$, then*

$$Z_D(\Theta_{v+D}) - \lambda_v \cdot \Theta_D + V_{D'}(\Theta_{D-v}) = 0.$$

(d) *If $v \in \mathrm{Supp}(N)$ and $v \in \mathrm{Supp}(D)$, then*

$$Z_D(\Theta_{v+D}) = \lambda_v \cdot \Theta_D.$$

(e) *If $v \notin \mathrm{Supp}(D)$ is real, then*

$$Z_D(\Theta_{v+D}) = (-1)^{2/m_v} \cdot m_v \cdot \Theta_D.$$

(ii) *Special Values: for each primitive quasi-character χ of W_D, we have*

$$\chi(\Theta_D) = \tau_\chi \cdot \Omega_\chi^{-1} \cdot |\mu| \cdot L(\chi, 1),$$

where Ω_χ and τ_χ are the relative global period and the Gauss sum.

Note that the defining properties determine the values $\chi(\Theta_D)$ for each quasi-character χ of W_D. In fact, from the compatibility property, there is an algebraic number C_χ which is a polynomial (with rational coefficients) in $\chi(v)$ and λ_v, $v \in \mathrm{Supp}(D)$, such that

$$\chi(\Theta_D) = C_\chi \cdot \tau_\chi \cdot \Omega_\chi^{-1} \cdot |\mu| \cdot \mathrm{L}(\chi, 1). \tag{19}$$

Since the group ring $\mathbb{C}[W_D]$ is reduced, by (19) Θ_D is uniquely determined as an element of it. In the number field case, the existence of $\Theta_D \in \mathbb{C}[W_D]$ follows from using the inverse Fourier transform. In case that $K = \mathbb{Q}$ and $\mathbb{E}$ is a Weil curve, our definition agrees with the formula given by

Mazur and Tate (see [MT2], [Tn1]). In this case, there is an integer M depending only on $\mathbb{E}$ such that Θ_D is in $\mathbb{Z}[M^{-1}][W_D]$. If K is a function field of characteristic p and $\mathbb{E}$ is not a constant curve, then, after a slight modification (see [Tn2]), our definition agrees with the formula given by Mazur [M]. In the function field case, for each elliptic curve, the theta element Θ_D always exists inside $\mathbb{Z}[p^{-1}][W_D]$, and the denominators of the coefficients of Θ_D are bounded for all admissible D. In particular, when K is a rational function field and $\mathbb{E}$ is semi-stable, the denominators of the coefficients are all bounded by

$$q^{\deg(N)/2-\deg(\Delta_K)/12-g_K-1}.$$

2. The Mazur-Tate pairings.

2.1. Local trivializations.

In [MT1] and [MT2], Mazur and Tate introduce various local Néron type pairings for abelian varieties. As pointed out by Zarhin in [Z], the Néron type pairings between zero cycles and divisors are equivalent to splittings of the canonical biextension. This is the method used in the above papers. These local pairings can be put together to define a system of global pairings which are the analogues of the global Néron-Tate pairing. In this section, we recall some basic definitions and constructions of local trivializations.

Let $\mathbb{E}'_{/K}$ denote the dual elliptic curve of $\mathbb{E}_{/K}$ and $\mathbb{P}_{/K}$ the canonical biextension (see [Mu], [SGA7 I]), associated to the duality, of $\mathbb{E}_{/K}$ and $\mathbb{E}'_{/K}$ by $\mathbb{G}_m$. We can identify $\mathbb{E}'_{/K}$ with $\mathbb{E}_{/K}$. But in the global pairing they do not play symmetric roles. As in [MT2], different notations for them will be used. If P is a biextension of commutative groups A and B by the commutative group C, then for $a \in A$, $b \in B$, we denote by ${}_{\{a\}}P$, $P_{\{b\}}$ the subsets of P which sit over $\{a\} \times B$ and $A \times \{b\}$ respectively. By identifying $\{a\} \times B$ with B and $A \times \{b\}$ with A, ${}_{\{a\}}P$ and $P_{\{b\}}$ become group extensions of $\{a\} \times B$ and $A \times \{b\}$ by C.

Definition 2.1. — *Let v be a place of K. A* local modification *of $\mathbb{P}(K_v)$ is a triple $(\alpha_v, \beta_v, \rho_v)$ of morphisms:*

$$\begin{cases} \alpha_v & : \quad A_v \longrightarrow \mathbb{E}(K_v), \\ \beta_v & : \quad B_v \longrightarrow \mathbb{E}'(K_v), \\ \rho_v & : \quad K_v^* \longrightarrow C_v. \end{cases}$$

Let $P_v := (\alpha_v{}^*, \beta_v{}^*)\mathbb{P}(K_v)$ be the biextension obtained from $\mathbb{P}(K_v)$ by pullback via homomorphisms α_v and β_v.

DEFINITION 2.2. — *A* local trivialization, $(\alpha_v, \beta_v, \rho_v, \psi_v)$, *of* $\mathbb{P}(K_v)$ *consists of a local modification* $(\alpha_v, \beta_v, \rho_v)$ *and a* local splitting ψ_v, *i.e. a map from* P_v *to* C_v *such that (cf.* [MT1])

(a) $\psi_v(c \cdot x) = \rho_v(c) \cdot \psi(x)$ *for* $c \in K_v^*$ *and* $x \in P_v$;

(b) *for each* $a_v \in A_v$ *(resp.* $b_v \in B_v$*) the restriction of* ψ_v *to* ${}_{\{a_v\}}P_v$ *(resp.* $P_{v\{b_v\}}$*) is a group homomorphism.*

In (L1)–(L5) below are five canonical local trivializations

$$\delta_v = (\alpha_v, \beta_v, \rho_v, \psi_v)$$

used for defining the global pairings. For the explicit definition of the canonical splittings and their expressions in terms of the zero cycles and divisors, see [MT2] (also the following remarks).

Let S be a finite set whose elements are real or non-archimedean places of K, and let $S_m \subseteq S$ denote the subset of S consisting of all the split multiplicative places of $\mathbb{E}$ inside S.

Example: five important local trivializations.

(L1) *The trivial trivialization*, for v archimedean and not in S. Here $A_v = \mathbb{E}(K_v)$, $B_v = \mathbb{E}'(K_v)$, $C_v = \{1\}$, α_v, β_v, ρ_v are the obvious homomorphisms and ψ_v is the trivial mapping.

(L2) *The real ramified trivialization*, for v real and in S. Here $A_v = \mathbb{E}_0(K_v)$, $B_v = \mathbb{E}_0'(K_v)$, $C_v = \mathbb{R}^*/\mathbb{R}_+^* \simeq \pm 1$, α_v, β_v, ρ_v are the obvious homomorphisms, and ψ_v is the unique continuous splitting.

(L3) *The Néron unramified trivialization*, for v non-archimedean and not in S. Here $A_v = \mathbb{E}(K_v)$, $B_v = \mathbb{E}_0'(K_v)$, $C_v = K_v^*/\mathcal{O}_v^* \simeq \mathbb{Z}$, α_v, β_v, ρ_v are the obvious homomorphisms, and ψ_v is the unique splitting. This corresponds to the non-archimedean local Néron pairing.

(L4) *The tamely ramified trivialization*, for v non-archimedean and in $S - S_m$. Here $A_v = \mathbb{E}(K_v)$, $B_v = \mathbb{E}_1'(K_v)$, $C_v = K_v^*/(1 + \pi_v \cdot \mathcal{O}_v)$, α_v, β_v, ρ_v are the obvious homomorphisms, and ψ_v is the unique splitting.

(L5) *The split multiplicative trivialization*, for $v \in S_m$. Let Q_v be the multiplicative period of the Tate curve $\mathbb{E}_{/K_v}$. The Tate parametrization gives exact sequences (of rigid analytic groups)

$$\text{(20)} \qquad \begin{cases} 0 \to \langle Q_v \rangle \longrightarrow K_v^* \xrightarrow{\alpha_v} \mathbb{E}(K_v) \to 0, \\ 0 \to \langle Q_v \rangle \longrightarrow K_v^* \xrightarrow{\beta_v} \mathbb{E}'(K_v) \to 0. \end{cases}$$

Here $A_v = B_v = C_v = K_v^*$, α_v, β_v, ρ_v are the obvious homomorphisms, and ψ_v is the unique analytic splitting.

Remarks.

(1) By Definition 2.2, for each $a \in A_v$, the splitting ψ_v induces a splitting of the following extension of either topological groups or rigid analytic groups

$$\text{(21)} \qquad 0 \to C_v \longrightarrow {}_{\{a\}}(\rho_* P_v) \longrightarrow \{a\} \times B_v \to 0.$$

These splittings of group extensions for all $a \in A_v$ also determine the splitting ψ_v. It is true that in any of the cases (L1)–(L5), the group $\mathrm{Hom}(B_v, \mathrm{Hom}(B_v, C_v))$ (for either topological groups or rigid analytic groups) is trivial. Therefore the local splitting ψ_v is canonical (see [MT1], Lemma in p. 721 and p. 726).

(2) By the canonical property, the splitting in (L4) «extends» the splitting in (L3) in the following sense. If $x \in P_v$ is eligible for both splittings in (L3) and (L4) (for different S), then the splitting on x in (L3) can be obtained by applying to x the splitting in (L4) and then applying the quotient map $K_v^*/(1 + \pi_v \cdot \mathcal{O}_v) \to K_v^*/\mathcal{O}_v^*$.

(3) In any of the cases (L1)–(L5), we can identify $\mathbb{E}'$ with $\mathbb{E}$, and B_v with a subgroup of A_v. Then P_v and $P_v' := (\beta_v^*, \alpha_v^*)\mathbb{P}(K_v)$ are subgroups of $(\alpha_v^*, \alpha_v^*)\mathbb{P}(K_v)$. On P_v', we have the canonical splitting $\psi_v' : P_v' \to C_v$ (the «mirror image» of ψ_v). By the uniqueness of the splitting of (21), on $P_v \cap P_v'$, we have $\psi_v = \psi_v'$.

(4) Note that for a fixed S, each place v satisfies exact one of the conditions of (L1)–(L5). A place v is said to be *of type i*, if it satisfies the condition of (Li) for $i = 1, \ldots, 5$. Let L/K be an abelian extension. For a place v, the associated local extension L_w/K_v is called *compatible with the set S*, if a finite set $S(L)$ of places of L can be chosen such that if v is of type i (with respect to S), then w is also of type i (with respect to $S(L)$). In this case, the set $S(L)$ is called *compatible with S at v*. If v is complex or split multiplicative, or w is neither complex nor split multiplicative, then L_w/K_v is compatible with S. In particular, if $[L_w : K_v]$ is prime to 2, then L_w/K_v is compatible with S (see [T5]). For the rest of this paper, if an extension

L/K is given, we will always assume that a set $S(L)$ has been chosen. Thus, for each place w of L, there is the associated trivialization δ_w. If L_w/K_v is compatible with the set S, then we assume that the set $S(L)$ is also compatible with S at v. Suppose that either L_w/K_v is compatible with S or v is archimedean. Then we have a natural embedding of P_v into P_w. For points $a_v \in A_v$ and $b_v \in B_v$, the Galois group $G_v = \mathrm{Gal}(L_w/K_v)$ acts on the groups ${}_{\{a_v\}}P_w$ and $P_{w\{b_v\}}$ with the groups of fixed elements containing ${}_{\{a_v\}}P_v$ and $P_{v\{b_v\}}$ respectively. Furthermore, the canonical property implies that except for the case in which $K_v = \mathbb{R}$ and $L_w = \mathbb{C}$, the restriction to P_v of the splitting on P_w equals the original splitting on P_v.

Let N_{G_v} denote the norm mapping for a G_v-module.

DEFINITION 2.3. — *Let $a_v \in A_v$ and $b_v \in B_v$. An element of K_v^*, A_v, B_v, ${}_{\{a_v\}}P_v$ or $P_{v\{b_v\}}$ will be called a* G_v-norm, *if it is in the image of the norm mapping N_{G_v} on the corresponding group L_w^*, A_w, B_w, ${}_{\{a_v\}}P_w$ or $P_{w\{b_v\}}$.*

The following lemma is a direct consequence of Remark 4.

LEMMA 2.4. — *Suppose that L_w/K_v is compatible with S. If either $p \in {}_{\{a_v\}}P_w$ and $N_{G_v}(p) \in {}_{\{a_v\}}P_v$, or $p \in P_{w\{b_v\}}$ and $N_{G_v}(p) \in P_{v\{b_v\}}$, then*

$$\psi_v \circ N_{G_v}(p) = N_{G_v} \circ \psi_w(p).$$

LEMMA 2.5. — *Suppose that v is real and L_w/K_v is not compatible with S. If an element p_v of the groups ${}_{\{a_v\}}P_v$ (resp. $P_{v\{b_v\}}$) is a G_v-norm, then we have $\psi_v(p_v) = 0$.*

Proof. — We have $K_v = \mathbb{R}$ and $L_w = \mathbb{C}$. Then both ${}_{\{a_v\}}P_w$ and $P_{w\{b_v\}}$ are connected. Since the norm mapping and the splitting are continuous, $\psi_v(x)$ must be in the identity component of ± 1. □

2.2. Global pairings.

In this section, We recall the definition of the global pairing and also discuss some of its useful properties.

For given K and S, the *extended Mordell-Weil group* is defined as follows. For each v, let $i_v : \mathbb{E}(K) \to \mathbb{E}(K_v)$ be the canonical map. Also let (A_v, B_v, C_v) and $\delta_v = (\alpha_v, \beta_v, \rho_v, \psi_v)$ be one of the local trivializations defined in (L1)–(L5) in Section 2.1. The group A_S is the abelian group such that the following diagram is cartesian,

$$\begin{array}{ccc} A_S & \xrightarrow{\alpha} & \mathbb{E}(K) \\ \downarrow & & \downarrow{\scriptstyle i=(i_v)} \\ \prod_v A_v & \xrightarrow{\prod \alpha_v} & \prod_v \mathbb{E}(K_v) \end{array} \tag{22}$$

Thus, a point $a \in A_S$ is described by a point $x \in \mathbb{E}(K)$ together with an element $(a_v)_v \in \prod_v A_v$ such that $\alpha_v(a_v) = i_v(x)$ for all v. Write $a = (x, (a_v))$. Similarly, define the group B_S (and the homomorphism β) associated to $\{B_v\}_v$. Then A_S and B_S fit into the exact sequences

$$0 \to \prod_{v \in S_m} \langle Q_v \rangle \longrightarrow A_S \longrightarrow \mathbb{E}(K) \to 0, \tag{23}$$

and

$$0 \to \prod_{v \in S_m} \langle Q_v \rangle \longrightarrow B_S \xrightarrow{\beta} \mathbb{E}'(K) \longrightarrow \Big(\prod_{v \in S-(S_\infty \cup S_m)} \mathbb{E}'(k_v) \Big) \times \Big(\prod_{v \notin (S_\infty - S) \cup (S - S_\infty)} (\mathbb{E}'/\mathbb{E}'_0)(k_v) \Big). \tag{24}$$

Let

$$U_S = \Big(\prod_{v \in S_\infty - S} K_v^* \Big) \times \Big(\prod_{v \in S_\infty \cap S} \mathbb{R}_+^* \Big) \times \Big(\prod_{v \notin S \cup S_\infty} \mathcal{O}_v^* \Big) \times \Big(\prod_{v \in S-(S_\infty \cup S_m)} (1 + \pi_v \cdot \mathcal{O}_v) \Big) \times \Big(\prod_{v \in S_m} (1) \Big),$$

and define

$$C_S = K^* \setminus \mathbb{A}_K^* / U_S.$$

The Mazur-Tate canonical *S-pairing* $\langle \cdot , \cdot \rangle_S : A_S \times B_S \to C_S$ is a pairing induced from (L1)–(L5). It is defined as follows. Let $P_S = (\alpha^*, \beta^*)\mathbb{P}(K)$. Then P_S is a biextension of $A_S \times B_S$ by K^*, and we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^* & \longrightarrow & P_S & \xrightarrow{\pi_s} & A_S \times B_S & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle \alpha \times \beta} & & \\ 0 & \longrightarrow & K^* & \longrightarrow & \mathbb{P}(K) & \xrightarrow{f} & \mathbb{E}(K) \times \mathbb{E}'(K) & \longrightarrow & 0. \end{array} \tag{25}$$

The injection $i = (i_v)$ (see [MI], p.111) and the map $\prod_v \psi_v$ induce

$$\Psi : P_S \xrightarrow{i_s} \prod_v P_v \xrightarrow{\prod_v \psi_v} \prod_v C_v \longrightarrow C_S. \tag{26}$$

Let $a \in A_S$ and $b \in B_S$. By (25), there is an element $p \in P_S$ such that $\pi_S(p) = a \times b$.

DEFINITION 2.6. — *For $a \in A_S$, $b \in B_S$, let $p \in P_S$ be such that $\pi_S(p) = a \times b$. Then*

$$\langle a, b \rangle_S = \Psi(p) \in C_S.$$

Since p is unique up to elements of K^*, and $\Psi(K^*) = 0 \in C_S$, the pairing is well-defined.

Suppose that $v_0 \in S_m$ and Q_{v_0} is the local Tate period. Using the embedding $A_{v_0} \to \prod_v A_v$, we can view Q_{v_0} as an element $\prod_v A_v$. By the self-duality of $\mathbb{E}$, we can also view Q_{v_0} as an element of $\prod_v B_v$.

DEFINITION 2.7. — *Define*

$$[Q_{v_0}] := (0, Q_{v_0}) \in A_S, \quad [Q_{v_0}]' := (0, Q_{v_0}) \in B_S.$$

Denote by $\overline{Q}_{v_0}$ the image of Q_{v_0} under the natural map

$$K_v^* \longrightarrow \mathbb{A}_K^* \longrightarrow C_S.$$

Then we have (see [MT2])

$$\left\langle [Q_{v_0}], [Q_{v_0}]' \right\rangle_S = \overline{Q}_{v_0}\,. \tag{27}$$

DEFINITION 2.8. — *Suppose that for a fixed S, G is a quotient of C_S and $C_S \xrightarrow{\mathrm{pr}} G$ is the quotient map. We define the G-pairing $\langle \cdot\, , \cdot \rangle_G$ by the composition of maps*

$$\langle \cdot\, , \cdot \rangle_G : A_S \times B_S \xrightarrow{\langle \cdot\, , \cdot \rangle_S} C_S \xrightarrow{\mathrm{pr}} G.$$

Note that the G-pairing depends on the set S, too.

Denote by $(\cdot\, , \cdot)$ the Néron-Tate pairing. If K is a function field with q equal to the order of the constant field, then $(\cdot\, , \cdot)$ is related to $\langle \cdot\, , \cdot \rangle_G$ for some special S and G. Namely, if $S = \emptyset$ and $G = \mathbb{Z}$ is the quotient of C_S defined by the degree map, then we have

$$(28)\qquad \langle a, b\rangle_Z = \frac{1}{\log(q)} \cdot \big(\alpha(a), \beta(b)\big), \quad \text{for all } a \in A_S,\ b \in B_S.$$

For the rest of this section, we assume that G is a finite quotient of C_S. Then G is the Galois group of a finite abelian extension L/K which is unramified outside S and at most tamely ramified at each $v \in S - S_m$.

DEFINITION 2.9. — *Suppose that L/K is compatible at every non-archimedean place of K (see Remark 4 in 2.1). Let $a \times b \in A_S \times B_S$. Call an element $p \in_{\{a\}} P_S$ (resp. $P_{S\{b\}}$)* a locally normed element *(with respect to G) if each v-component of $i_S(p)$ is in $N_{G_v}({}_{\{a\}}P_w)$ (resp. $N_{G_v}(P_{w\{b\}})$).*

Then Lemma 2.4 and Lemma 2.5 together imply the following.

LEMMA 2.10. — *Suppose that L/K is compatible with S at every non-archimedean place of K. Let p be an element of P_S such that $\pi_S(p) = a \times b$. If p is a locally normed element of P_S with respect to G (viewed as an element of either ${}_{\{a\}}P_S$ or $P_{S\{b\}}$), then $\langle a, b\rangle_G = 0$.*

The formula (27) can be generalized in the following way.

LEMMA 2.11. — *Suppose that $a = (x, (a_v)_v) \in A_S$, $b = (y, (b_v)_v) \in B_S$ and $v_0 \in S_m$. Then the following are true*:

(a) *The pairings $\langle a, [Q_{v_0}]'\rangle_S$ and $\langle [Q_{v_0}], b\rangle_S$ depend only on a_{v_0} and b_{v_0}.*

(b) *Suppose that G is a cyclic quotient of C_S. Then $\langle a, [Q_{v_0}]'\rangle_G = 0$ (resp. $\langle [Q_{v_0}], b\rangle_G = 0$) if and only if a_{v_0} (resp. b_{v_0}) is a G_{v_0}-norm.*

In order to prove Lemma 2.11, we need the following result. The diagram (25) induces

$$(29)\qquad \begin{array}{ccccccccc} 0 & \longrightarrow & K^* & \longrightarrow & {}_{\{a\}}P_S & \xrightarrow{\pi_S} & \{a\} \times B_S & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \gamma_S} & & \downarrow{\scriptstyle \alpha\times\beta} & & \\ 0 & \longrightarrow & K^* & \longrightarrow & {}_{\{x\}}\mathbb{P}(K) & \xrightarrow{f} & \{x\} \times \mathbb{E}'(K) & \longrightarrow & 0. \end{array}$$

Locally at each v, we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_v^* & \longrightarrow & {}_{\{a_v\}}P_v & \xrightarrow{\pi_v} & \{a_v\} \times B_v & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \gamma_v} & & \downarrow{\scriptstyle \alpha_v \times \beta_v} & & \\ 0 & \longrightarrow & K_v^* & \longrightarrow & {}_{\{x\}}\mathbb{P}(K_v) & \xrightarrow{f_v} & \{x\} \times \mathbb{E}'(K_v) & \longrightarrow & 0. \end{array} \tag{30}$$

Since G is cyclic, taking cohomology groups, we have the following diagram

$$\begin{array}{ccccc} & & K_v^*/N_{G_v}(L_w^*) & \longrightarrow & {}_{\{a_v\}}P_v/N_{G_v}({}_{\{a_v\}}P_w) \\ & & \| & & \downarrow{\scriptstyle \bar{\gamma}_v} \\ H^1(G_v, \{x\} \times \mathbb{E}'(L_w)) & \xrightarrow{\partial} & K_v^*/N_{G_v}(L_w^*) & \xrightarrow{j} & {}_{\{x\}}\mathbb{P}(K_v)/N_{G_v}({}_{\{x\}}\mathbb{P}(K_w)). \end{array} \tag{31}$$

Recall that there is a *local duality pairing* (see [Ml2], p. 53, p. 354 and [T1]), which is a perfect pairing

$$(\cdot, \cdot)_v : \mathbb{E}(K_v) \times H^1(K_v, \mathbb{E}) \longrightarrow \mathbb{Q}/\mathbb{Z}. \tag{32}$$

The inflation map identifies $H^1(G_v, \mathbb{E}(L_v))$ with a subgroup of $H^1(K_v, \mathbb{E})$. Directly from the definition of the local duality pairing, we have the following lemma.

LEMMA 2.12. — *Let v be a place of K. Suppose that $x \in \mathbb{E}(K_v)$, $\xi \in H^1(G_v, E'(L_w))$ and $(x, \xi)_v \in \mathbb{Q}/\mathbb{Z}$ is the value of the local duality pairing. Let ∂ be the map in (31). Then $(x, \xi)_v$ equals the image of ξ under the following composition of maps*

$$H^1(G_v, E'(L_w)) \xrightarrow{\sim} H^1(G_v, \{x\} \times \mathbb{E}'(L_w))$$
$$\xrightarrow{\partial} K_v^*/N_{G_v}(L_w^*) \subset \mathrm{Br}(K_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Proof of Lemma 2.11. — We show part (a). Part (b) follows similarly.

Note that the diagrams (29) and (30) are nothing but pullbacks of the group extensions via the right vertical arrows. With the notations used there, since $\alpha \times \beta(a \times [Q_{v_0}]')$ is the identity of the group $\{x\} \times \mathbb{E}'(K)$, there is a unique $p \in_{\{a\}} P_S$ such that,

$$\pi_S(p) = a \times [Q_{v_0}]' \quad \text{and} \quad \gamma_S(p) = \text{identity in } {}_{\{x\}}\mathbb{P}(K).$$

Suppose that $i_S(p) = (p_v)_v \in \prod_v P_v$. Then p_{v_0} is the unique element of ${}_{\{a_{v_0}\}}P_{v_0}$ such that

$$\pi_{v_0}(p_{v_0}) = a_{v_0} \times Q_{v_0} \quad \text{and} \quad \gamma_{v_0}(p_{v_0}) = \text{identity in } {}_{\{x\}}\mathbb{P}(K_{v_0}).$$

If $v \neq v_0$, then p_v is the identity of the group ${}_{\{a_v\}}P_v$ and $\psi_v(p_v) = 0 \in C_v$. It follows that $\langle a, [Q_{v_0}]\rangle_S$ equals the image of $\psi_{v_0}(p_{v_0})$ in C_S and depends only on a_{v_0}. This shows the first statement.

To evaluate $\psi_{v_0}(p_{v_0})$, we consider the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K_{v_0}^* & \longrightarrow & P_{v_0\{Q_{v_0}\}} & \xrightarrow{\pi_v} & A_v \times \{Q_{v_0}\} & \longrightarrow & 0 \\
 & & \Big\| & & \Big\downarrow{\scriptstyle \gamma_{v_0}} & & \Big\downarrow{\scriptstyle \alpha_{v_0} \times \beta_{v_0}} & & \\
0 & \longrightarrow & K_{v_0}^* & \longrightarrow & \mathbb{P}(K_{v_0})_{\{0\}} & \xrightarrow{f_{v_0}} & \mathbb{E}(K_{v_0}) \times \{0\} & \longrightarrow & 0.
\end{array}$$

Note that we can identify $\mathbb{P}(K_{v_0})_{\{0\}}$ with $\mathbb{E}(K_{v_0}) \times K_{v_0}^*$. The element $x \times 1 \in \mathbb{P}(K_{v_0})_{\{0\}}$ is also in ${}_{\{x\}}\mathbb{P}(K_v)$. Using the expressions in terms of zero cycles and divisors, we can show directly that $x \times 1$ is the identity of the group ${}_{\{x\}}\mathbb{P}(K_v)$. As a consequence, p_{v_0} is the unique element of $P_{v_0\{Q_{v_0}\}}$ such that

$$\pi_{v_0}(p_{v_0}) = a_{v_0} \times Q_{v_0} \quad \text{and} \quad \gamma_{v_0}(p_{v_0}) = x \times 1.$$

Fix a place w_0 of L sitting over v_0 and let G_{v_0} be the decomposition subgroup associated to w_0. Then L_{w_0}/K_{v_0} is compatible with S (see Remark 4 in 2.1). We also identify $\mathbb{P}(L_{w_0})_{\{0\}}$ with $\mathbb{E}(L_{w_0}) \times L_{w_0}^*$. Suppose that $a_{v_0} = N_{G_{v_0}}(a_{w_0})$ is a G_{v_0}-norm. Let p_{w_0} be the unique element of $P_{w_0\{Q_{v_0}\}}$ such that

$$\pi_{w_0}(p_{w_0}) = a_{w_0} \times Q_{v_0} \quad \text{and} \quad \gamma_{w_0}(p_{w_0}) = \alpha_{w_0}(a_{w_0}) \times 1 \ \in \ \mathbb{P}(L_{w_0})_{\{0\}}.$$

Then $p_{v_0} = N_{G_{v_0}}(p_{w_0})$. By Lemma 2.4, $\psi_{v_0}(p_{v_0})$ is a G_{v_0}-norm and $\langle a, [Q_{v_0}]\rangle_G = 0$. This shows the «if» part of the second statement.

Consider the diagram (31) for $v = v_0$. Let $\bar{p}_{v_0}$ be the image of p_{v_0} in ${}_{\{a_{v_0}\}}P_{v_0}/N_{G_{v_0}}({}_{\{a_{v_0}\}}P_{w_0})$. Then $\bar{p}_{v_0}$ generates the kernel of the map $\bar{\gamma}_{v_0}$. By Lemma 2.4, the local splitting ψ_{v_0} induces

$$\bar{\psi}_{v_0} : {}_{\{a_{v_0}\}}P_{v_0}/N_{G_{v_0}}({}_{\{a_{v_0}\}}P_{w_0}) \longrightarrow K^*_{v_0}/N_{G_{v_0}}(L^*_{w_0}).$$

If $\langle a, [Q_{v_0}]_G\rangle = 0$ then $\bar{\psi}_{v_0}(\bar{p}_{v_0}) = 0$ and the map $\bar{\psi}_{v_0}$ induces a map

$$\bar{\eta}_{v_0} : {}_{\{x\}}\mathbb{P}(K_{v_0})/N_{G_{v_0}}\big({}_{\{x\}}\mathbb{P}(K_{w_0})\big) \longrightarrow K^*_{v_0}/N_{G_{v_0}}(L^*_{w_0})$$

such that $j \circ \bar{\eta}_{v_0}$ is the identity map. It then follows that the map ∂ is trivial. By Lemma 2.12 and the local duality, we see that x is a G_{v_0}-norm.

Since x is a G_{v_0}-norm, we can find an $a'_{v_0} \in N_{G_{v_0}}(A_{w_0})$ such that $\alpha_{v_0}(a'_{v_0}) = x$. Let $a' = (x, a'_v) \in A_S$ be such that $a'_v = a_v$ for $v \neq v_0$. Then $a' = a + n \cdot [Q_{v_0}]$ for some integer n, and by the «if» part of the second statement of the lemma, we have $\langle a', [Q_{v_0}]'\rangle_G = 0$. As a consequence, we have $\langle n \cdot [Q_{v_0}], [Q_{v_0}]'\rangle_G = 0$. By (27), $Q^n_{v_0} \in K^*_{v_0}$ must be a G_{v_0}-norm and so is a_{v_0}. □

2.3. The corrected discriminant.

In this section we recall the definition of the *corrected discriminant* (see [MT2]) associated to the global pairings defined in 2.2. The corrected discriminants are the analogues of the regulators for the Néron-Tate pairing.

According to the recipe detailed in [MT2] , we have to choose a pair of compatible orientations on the real vector spaces $A_S \otimes \mathbb{R}$ and $B_S \otimes \mathbb{R}$. In our situation, these two spaces are naturally isomorphic and a pair of orientations on them is compatible if and only if under the natural isomorphism, they become the same orientation.

Let (a_i) and (b_j) be a pair of compatible bases of A_S and B_S modulo the torsion elements, i.e., they give compatible orientations on $A_S \otimes \mathbb{R}$ and $B_S \otimes \mathbb{R}$. Note that by (23) and (24) the groups of torsion elements of both A_S and B_S are embedded into $\mathbb{E}(K)_{\text{tor}}$.

DEFINITION 2.13. — *Denote*

$$r_K = \operatorname{rk}\big(\mathbb{E}(K)\big),$$

$$r := r_K + \#S_m = \operatorname{rk}(A_S) = \operatorname{rk}(B_S),$$

$$w = \big|\mathbb{E}(K)_{\text{tor}}\big|.$$

Define the discriminant *of the S-pairing as*

$$\operatorname{disc}_S = \left|(A_S)_{\mathrm{tor}}\right|^{-1}\left|(B_S)_{\mathrm{tor}}\right|^{-1}\det_{1\le i,j\le r}\big(\langle a_i, b_j\rangle_S\big) \in \mathbb{Z}\Big[\frac{1}{w}\Big] \otimes \operatorname{Sym}_r(C_S).$$

If (a'_i) and (b'_j) are another pair of compatible bases, then the induced determinant $\det_{1\le i,j\le r}(\langle a'_i, b'_j\rangle_S)$ differs from that induced from (a_i) and (b_j) by at most an element of $\operatorname{Sym}_r(C_S)$, and this element is killed by w. So the definition of the discriminant is independent of the choice of the basis.

Suppose that $S_m \subseteq T \subseteq S$. For each positive integer n, the projection $C_S \to C_T$ induces the $\mathbb{Z}[w^{-1}]$-morphism

$$\mathcal{Z}_{T,S} : \mathbb{Z}\Big[\frac{1}{w}\Big] \otimes \operatorname{Sym}_n(C_S) \longrightarrow \mathbb{Z}\Big[\frac{1}{w}\Big] \otimes \operatorname{Sym}_n(C_T). \tag{33}$$

There is a unique $\mathbb{Z}[w^{-1}]$-morphism

$$\mathcal{U}_{S,T} : \mathbb{Z}\Big[\frac{1}{w}\Big] \otimes \operatorname{Sym}_n(C_T) \to \mathbb{Z}\Big[\frac{1}{w}\Big] \otimes \operatorname{Sum}_n(C_S) \tag{34}$$

such that for all $c_i \in C_S$,

$$\begin{aligned}\mathcal{U}_{S,T} \circ \mathcal{Z}_{T,S}&(c_1 \otimes c_2 \otimes \cdots \otimes c_n) \\ &= 2^{|S_\infty \cap (S-T)|} \cdot \Big(\prod_{v\in S-T-S_\infty} (q_v - 1)\Big) \cdot c_1 \otimes c_2 \otimes \cdots \otimes c_n.\end{aligned} \tag{35}$$

DEFINITION 2.14. — *Denote*

$$j_S = \Big|\operatorname{cokernel}\Big(B_{S_m} \to \prod_{v\in S-S_m-S_\infty} \mathbb{E}'_0(k_v) \times \prod_{v\in S\cap S_\infty} (\mathbb{E}'/\mathbb{E}'_0)(k_v)\Big)\Big|.$$

The corrected discriminant *of the S-pairing is defined as*

$$\begin{aligned}\mathcal{D}_S &= \mathcal{D}_S(\mathbb{E}) \\ &:= \sum_{S_m\subseteq T\subseteq S} (-1)^{\#(T-S_m)}\,\mathcal{U}_{S,T}(j_T \operatorname{disc}_T) \in \mathbb{Z}\Big[\frac{1}{w}\Big] \otimes \operatorname{Sym}_r(C_S).\end{aligned} \tag{36}$$

Then $\mathcal{D}_S$ is corrected in the sense that when S varies, the $\mathcal{D}_S$ are related by desirable compatibility formulae (see [MT2] and [T4]). We conclude this section by recalling these formulae. Let $S' = S \cup \{v\}$, and r' the rank of $A_{S'}$. Then

$$r' = \begin{cases} r & \text{if } v \text{ is not split multiplicative for } \mathbb{E}, \\ r+1 & \text{if } v \text{ is split multiplicative for } \mathbb{E}. \end{cases} \tag{37}$$

Suppose that v is a non-archimedean place of K. Let $n_v = \#(\mathbb{E}_0(k_v))$. If v is not a split multiplicative place of $\mathbb{E}$, then (see [MT2])

$$\mathcal{Z}_{S,S'}(\mathcal{D}_{S'}) = (q_v - 1 - n_v) \cdot \mathcal{D}_S. \tag{38}$$

Let $c(S_m, v)$ be the order of the image of the natural mapping

$$B_{S_m \cup \{v\}} \longrightarrow (\mathbb{E}'/\mathbb{E}'_0)(k_v).$$

If v is a split multiplicative place of $\mathbb{E}$, then (see [MT2])

$$c(S_m, v) \cdot \mathcal{Z}_{S,S'}(\mathcal{D}_{S'}) = \bar{Q}_v \cdot \mathcal{D}_S \in \mathbb{Z}\left[\frac{1}{w}\right] \otimes \operatorname{Sym}_{r'}(C_S). \tag{39}$$

If v is a real place, then (see [T4])

$$\mathcal{Z}_{S,S'}(\mathcal{D}_{S'}) = (-1)^{2/m_v} \cdot m_v \cdot \mathcal{D}_S \in R \otimes \operatorname{Sym}_r(C_S). \tag{40}$$

3. The Mazur-Tate conjectures.

3.1. The Mazur-Tate conjecture

In this section, we describe the Mazur-Tate conjecture. To do this, we need to make an assumption about the theta element (see Assumption 4 below). This assumption is satisfied when $\mathbb{E}$ is a Weil curve over $\mathbb{Q}$ or $\mathbb{E}$ is defined over a function field.

Definition 3.1. — *Let $D = \sum_v \operatorname{ord}_v(D) \cdot v$ be an extended divisor. We say that D is* admissible, *if $\operatorname{ord}_v(D) \leq 1$ unless v is a split multiplicative place of $\mathbb{E}$.*

Suppose that S is a finite set of places of K containing the support of an admissible divisor D. Then the Weil group W_D is a quotient of the group C_S defined in 2.2. Recall that the definition of the theta element depends on the divisor D, while the definition of the corrected discriminant depends on the set S.

ASSUMPTION 3. — *For the remainder of this paper, assume*

$$S = \mathrm{Supp}(D).$$

Let G be a quotient group of W_D, and consider the quotient maps

$$W_D \xrightarrow{\mathrm{pr}_D} G, \quad \mathrm{pr}_S : C_S \longrightarrow W_D \xrightarrow{\mathrm{pr}_D} G.$$

These maps can be extended to morphisms of the group rings and morphisms of the symmetric tensors.

DEFINITION 3.2. — *We define the theta element as*

$$\Theta_G = \mathrm{pr}_D(\Theta_D),$$

and the corrected discriminant as

$$\mathcal{D}_G = \mathrm{pr}_S(\mathcal{D}_S).$$

ASSUMPTION 4. — There is a positive integer M such that Θ_G is in the group ring $\mathbb{Z}[M^{-1}][G]$ and M is large enough such that it is divisible by w.

Recall that w is the order of the group $\mathbb{E}(K)_{\mathrm{tor}}$. Under Assumption 4, we have

$$\mathcal{D}_G \in \mathbb{Z}\left[\frac{1}{M}\right] \otimes \mathrm{Sym}_r(G). \tag{41}$$

Let I be the augmentation ideal of the group ring $\mathbb{Z}[M^{-1}][G]$. The natural morphism

$$\begin{cases} G \longrightarrow I/I^2 \\ g \longmapsto 1-g \end{cases} \tag{42}$$

can be extended to a homomorphism of graded algebras

$$d\colon \bigoplus_n \mathbb{Z}\left[\frac{1}{M}\right] \otimes \mathrm{Sym}_n(G) \longrightarrow \mathbb{Z}\left[\frac{1}{M}\right] \oplus I/I^2 \oplus \cdots \oplus I^n/I^{n+1} \cdots.$$

We denote

$$\det_G = d(\mathcal{D}_G) \in I^r/I^{r+1}.$$

DEFINITION 3.3. — *Let* $\mathrm{ord}(\Theta_G)$ *be the maximal* n *such that* $\Theta_G \in I^n$. *If* $\mathrm{ord}(\Theta_G) \geq n$, *we denote by* $\theta_G^{(n)}$ *the image of* Θ_G *under the quotient map* $I^n \to I^n/I^{n+1}$.

DEFINITION 3.4. — *Define*

$$\phi_S = \phi_{S_m} = \left|\mathrm{coker}\left\{\mathbb{E}'(K) \to \prod_{v \notin S_m \cup S_\infty} \mathbb{E}'/\mathbb{E}'_0(k_v)\right\}\right|. \tag{43}$$

Let $Ш_K$ *be the Shafarevich-Tate group of* $\mathbb{E}_{/K}$.

The Mazur-Tate conjecture is the following:

CONJECTURE 1 (see [MT2]). — We have $\mathrm{ord}(\Theta_G) \geq r$, $Ш_K$ finite, and

$$\theta_G^{(r)} = |Ш_K| \cdot \phi_S \cdot \det{}_G\,. \tag{44}$$

Note that Θ_G and $\det_G$ depend on the admissible divisor D. But conjecture 1 basically depends only on G, as we have the following compatibility lemma. It can be proved directly by using the compatibility property of the theta element together with (1), (38), (39), (40).

LEMMA 3.5. — *Suppose that* D', D *are two admissible divisor and* $D' \succeq D$. *Let* G *be a quotient of* W_D *and* G' *a quotient of* G. *If conjecture* 1 *is true for* (D, G), *then it is also true for* (D', G').

3.2. The conjecture of Birch and Swinnerton-Dyer.

This section begins with the review of the Birch and Swinnerton-Dyer conjecture for elliptic curves over a global field. The basic reference is [T2]. When K is a function field, this conjecture is a special case of conjecture 1. We will show this at the end of this section.

Recall the notations in 1.2. For a fixed invariant differential ω, a place v is said to be *bad* if either it is archimedean or $\mathrm{ord}_v(\omega/\omega_{0,v}) \neq 0$. Let S be a finite set of places containing all the bad places for ω and all the places where $\mathbb{E}$ has bad reduction. For such an S there is an associated L-function $L_S^*(s)$ (see [T2]). Let $R(\mathbb{E}_{/K})$ be the regulator defined by using the Néron-Tate canonical pairing on the Mordell-Weil group.

BIRCH AND SWINNERTON-DYER CONJECTURE. — *The Shafarevich-Tate group $Ш_K$ is finite, and at $s = 1$, the associated L-series $L_S^*(s)$ has order of vanishing equal to r_K. Further more, we have*

$$\lim_{s\to 1} \frac{L_S^*(s)}{(s-1)^{r_K}} = \frac{|Ш_K| \cdot R(\mathbb{E}_{/K})}{w^2}. \tag{45}$$

Let χ_0 be the trivial character and $L(s) = L(\chi_0, s)$ denote the Hasse-Weil L-function. Recall the measure $|\mu|$ and the period Ω defined in 1.2. We have (see [T2])

$$L_S^*(s) = \frac{|\mu| \cdot \prod_{v\in S} L_v(1)}{\Omega \cdot \prod_v m_v \cdot \prod_{v\in S} L_v(s)} L(s).$$

It follows that formula (45) is equivalent to

$$\lim_{s\to 1} \frac{L(s)}{(s-1)^{r_K}} = \frac{|Ш_K| \cdot R(\mathbb{E}_{/K}) \cdot \prod_v m_v}{w^2} \Omega \cdot |\mu|^{-1}. \tag{46}$$

When K is a function field, the Birch and Swinnerton-Dyer conjecture reduces to a conjecture about the finiteness of $Ш_K$.

THEOREM 3.6 (see [T2], [Ml1]). — *Suppose that K is a function field. Then the following statements are true:*

(1) *At $s = 1$, the order of vanishing of $L(s)$ is always $\geq r_K$.*

(2) *The following statements are equivalent:*

(a) *The conjecture of Birch and Swinnerton-Dyer is true.*

(b) *The ℓ-primary part of the Shafarevich-Tate group is finite for some prime number ℓ.*

(c) *The order of vanishing of $L(s)$ at $s = 1$ equals r_K.*

Remark. — Recall that $r = r_K + \#S_m$. If $r > 0$ and χ_0 is the trivial character of $\mathbb{A}_K^*$, then by using the defining properties of the theta element (see Definition 1.8), we see that the Birch and Swinnerton-Dyer conjecture implies that $\Theta_D \in I$. If $r = 0$, then by using the same method, we see that conjecture 1 is just a consequence of the Birch and Swinnerton-Dyer conjecture.

We conclude this section by showing that when K is a function field, conjecture 1 generalizes the Birch and Swinnerton-Dyer conjecture. Let

$D = 0$, $S = \emptyset$, $G = \mathbb{Z}$ and the quotient map $W_D \to G$ be the map induced by the degree map on $\mathbb{A}_K^*$. Let χ_s denote the quasi-character of W_D which sends each element $x \in W_D$ to $\|x\|^s$. Then χ_s induces a ring isomorphism

$$\chi_s : \mathbb{Z}\Big[\frac{1}{M}\Big][G] \longrightarrow \mathbb{Z}\Big[\frac{1}{M}\Big][q^{-s}].$$

This isomorphism sends I^r to $(1-q^{-s})^r$. Apply χ_s to the equation (44) of conjecture 1. Then by Definition 1.8, the left-hand side of equation (44) becomes

$$\Omega^{-1} \cdot |\mu| \cdot L(s+1) \pmod{(1-q^{-s})^{r_K+1}}.$$

By (28), the right-hand side of (44) becomes

$$|\text{Ш}_K| \cdot \phi_S \cdot w^{-2} \cdot [\mathbb{E}'(K) : B_S] \cdot \frac{R(\mathbb{E}_{/K})}{\log(q)^{r_K}} (1-q^{-s})^{r_K} \pmod{(1-q^{-s})^{r_K+1}}.$$

Directly from Definition 3.4, we have $\phi_S \cdot [\mathbb{E}'(K) : B_S] = \prod_v m_v$. It then follows that (44) is equivalent to (46).

3.3. The horizontal case.

Suppose that G is a finite group with order dividing M. Then it is true that if I is the augmentation ideal of the group ring $\mathbb{Z}[M^{-1}][G]$, then $I = I^n$ for every positive integer n. Furthermore, as explained in the remark at the end of 3.2, if $r > 0$ and the Birch and Swinnerton-Dyer conjecture is true, then we should have $\Theta_G \in I = I^n$. In this case, conjecture 1 is a consequence of the Birch and Swinnerton-Dyer conjecture. This phenomenon would not occur, if we can work over $\mathbb{Z}[G]$ instead of $\mathbb{Z}[M^{-1}][G]$. For this reason, we would like to modify Θ_G and $\mathcal{D}_G$ in a way such that their «coefficients» are all integers. For instance, when G is finite, we can find an integer z such that $z\Theta_G \in \mathbb{Z}[G]$ and $z \cdot \mathcal{D}_G \in \mathrm{Sym}_r(G)$, and then study this new theta element and new discriminant. For the rest of this paper, we will consider this for the case where G is «horizontal», *i.e.*, it is a group of $(\ell, \dots, \ell)$-type for some fixed prime ℓ. We will raise a conjecture (conjecture 2) similar to conjecture 1, and prove some partial results about it.

For the remainder of this paper, we assume that G is horizontal. In this section, we will reprove a theorem of Passi and Vermani concerning the augmentation quotients of the integral group ring (see [PV]).

Let I be the augmentation ideal of the group ring $\mathbb{Z}[G]$. Define the associated graded algebra

$$\mathrm{gr}\big(\mathbb{Z}[G]\big) := \mathbb{Z} \oplus (I/I^2) \oplus (I^2/I^3) \oplus \cdots .$$

As in 3.1, there is a canonical epimorphism of graded algebras

$$d\colon \bigoplus_n \mathrm{Sym}_n(G) \longrightarrow \mathrm{gr}\big(\mathbb{Z}[G]\big). \tag{47}$$

Let $\underline{x} = \{x_1, x_2, \dots, x_k\}$ be a basis of G as a vector space over $\mathbb{F}_l$ and $\underline{t} = \{t_1, \dots, t_k\}$ a set of k variables. Then the assignment $t_i \mapsto x_i$ extends to a non-canonical isomorphism of graded algebras between $\mathbb{F}_\ell[\underline{t}]$ and $\bigoplus_n \mathrm{Sym}_n(G)$. Composing this isomorphism with d, we get a noncanonical epimorphism

$$d_{(\underline{x})} : \mathbb{F}_\ell[\underline{t}] \longrightarrow \mathrm{gr}\big(\mathbb{Z}[G]\big).$$

The theorem of Passi and Vermani says that the kernel of $d_{(\underline{x})}$ is the ideal generated by

$$\ell x_i,\ x_i^\ell x_j - x_j^\ell x_i \quad \text{for} \quad i, j, = 1, 2, \dots, k.$$

In the following, this result will be restated as Proposition 3.8.

Consider the dual space of G,

$$G' = \mathrm{Hom}(G, \mathbb{F}_\ell).$$

Via the isomorphism

$$\mathbb{F}_\ell[\underline{t}] \simeq \bigoplus_n \mathrm{Sym}_n(G),$$

we view each polynomial $f(\underline{t}) \in \mathbb{Z}[\underline{t}]$ as a $\mathbb{F}_\ell$-valued function $\bar{f}$ on G'. Suppose that ζ is a chosen primitive ℓ-th root of 1. Then via ζ, we can identify G' with the dual group $\widehat{G}$ and also identify $\bar{f}$ with a $\mathbb{C}$-valued function on $\widehat{G}$. Namely, if $\chi \in \widehat{G}$ and $\underline{s} = (s_1, \dots, s_k)$ is such that $\chi(x_i) = \zeta^{s_i}$, then

$$\bar{f}(\chi) = \zeta^{f(\underline{s})}. \tag{48}$$

Definition 3.7. — *For an element* $\Theta \in \mathbb{Z}[G]$, *denote by* $\mathrm{ord}(\Theta)$ *the maximal* n *such that* $\Theta \in I^n$. *Also, denote by* $o(\chi, \Theta) = \mathrm{ord}_{(1-\zeta)}(\chi(\Theta))$ *the* valuation *of the element* $\chi(\Theta)$ *at the prime ideal* $(1 - \zeta)$ *of the Dedekind domain* $\mathbb{Z}[\zeta]$.

If $\mathrm{ord}(\Theta) \geq n$, then we have $o(\chi, \Theta) \geq n$ for every $\chi \in \widehat{G}$. Therefore χ induces a map from $\mathbb{Z}[G]/I^n$ to $\mathbb{Z}[\zeta]/(1-\zeta)^n$. By abuse of notation, we also denote this map by χ. Thus for an element $\theta \in \mathbb{Z}[G]/I^n$, it still makes sense to say either $o(\chi, \theta) = i$ for $i < n$, or $o(\chi, \theta) \geq n$. Suppose that $f \in \mathbb{Z}[\underline{t}]$ is a homogeneous polynomial of degree n. Let

$$\theta = d_{(\underline{x})}(f) \in I^n/I^{n+1}.$$

Then θ is the image of $f(1 - x_1, \ldots, 1 - x_k)$ under the quotient $I^n \longrightarrow I^n/I^{n+1}$. We can relate $\chi(\theta)$ and $\bar{f}(\chi)$ in the following way. Note that for $x, y \in \mathbb{Z}[G]$, we have

$$(1-x) \cdot (1-y) = (1-x) + (1-y) - (1 - x \cdot y),$$

and consequently,

$$1 - \zeta^n \equiv n \cdot (1-\zeta) \pmod{(1-\zeta)^2}.$$

Using this, we obtain

$$\chi(\theta) \equiv \bar{f}(\chi) \cdot (1-\zeta)^n \pmod{(1-\zeta)^{n+1}}. \tag{49}$$

PROPOSITION 3.8 (see [PV]). — *Suppose that $f \in \mathbb{Z}[\underline{t}]$ is a homogeneous polynomial of degree $n > 0$ and $\theta = d_{(\underline{x})}(f) \in I^n/I^{n+1}$. Then the following statements are equivalent:*

(a) *θ is trivial in I^n/I^{n+1},*

(b) *$o(\chi, \theta) \geq n+1$ for all characters $\chi \in \widehat{G}$,*

(c) $\bar{f} = 0$.

(d) *f is in the ideal J generated by*

$$\ell x_i,\ x_i^\ell x_j - x_j^\ell x_i \quad \text{for} \quad i, j = 1, 2, \ldots k.$$

Proof.

(a) $\Rightarrow$ (b): trivial.

(b) $\Rightarrow$ (c): by (49).

(c) $\Rightarrow$ (d): We prove this by induction. It is obvious for $n = 1$. In general, write $f = f_1 + t_1 \cdot f_2$ such that f_1 contains only the variables $t_2, \ldots, t_k$.

By taking $t_1 = 0$, we see that $\bar{f}_1 = 0$. By the induction hypothesis, we have $f_1 \in J$. Since $\bar{t}_1 \cdot \bar{f}_2 = 0$, we have

$$f_2(1, s_2, \dots, s_k) \equiv 0 \pmod{\ell} \quad \text{for all} \quad s_2, \dots, s_k \in \mathbb{Z}.$$

Thus by a theorem of Chevalley (see [BS], Section 1.1), $f_2(1, t_2/t_1, \dots, t_k/t_1)$ is in the ideal of $\mathbb{Z}[t_2/t_1, \dots, t_k/t_1]$ which is generated by the elements ℓ and $(t_i/t_1)^\ell - t_i/t_1$ for $i = 2, \dots, k$. So there are polynomials $g_i, i = 2, \dots, k$, such that

$$f_2(t_1, t_2, \dots, t_k) \equiv \sum_{i=2}^{k} g_i \cdot (t_i^\ell - t_i t_1^{\ell-1}) \pmod{\ell}.$$

This shows that $t_1 \cdot f_2$ is in J and so is f.

(d) $\Rightarrow$ (a): for $x \in G$, we can write

$$1 = \big(1 + (x-1)\big)^\ell = 1 + (x-1)^\ell + \ell \cdot (x-1)\big(1 + (x-1)h(x)\big).$$

Since $1 + (x-1)h(x) = 1 - (x-1)h(x) + \cdots$ is invertible in the I-adic completion of $\mathbb{Z}[G]$, we have

$$\ell \cdot (1-x) \equiv (1-x)^\ell \pmod{I^{\ell+1}}, \tag{50}$$

and consequently,

$$\begin{aligned} (1-x_i)^\ell \cdot (1-x_j) &\equiv \ell \cdot (1-x_i) \cdot (1-x_j) && \pmod{I^{\ell+2}} \\ &\equiv (1-x_i) \cdot (1-x_j)^\ell && \pmod{I^{\ell+2}}. \end{aligned}$$

Therefore, if $f \in J$, then θ is trivial. □

By (50), if $\Theta \in I^n$ and $n > 0$, then $\ell \cdot \Theta \in I^{n+\ell-1}$. This multiplication by ℓ induces a homomorphism of groups

$$\ell : I^n/I^{n+1} \longrightarrow I^{n+\ell-1}/I^{n+\ell}.$$

In fact, we have the following.

LEMMA 3.9. — *The following are true:*

(a) *For every $n > 0$, the map $\ell : I^n/I^{n+1} \longrightarrow I^{n+\ell-1}/I^{n+\ell}$ is an injection.*

(b) *If z is an integer prime to ℓ, then the multiplication by z induces an isomorphism $I^n/I^{n+1} \xrightarrow{\sim} I^n/I^{n+1}$.*

Proof. — Let $\theta \in I^n/I^{n+1}$, and $f, g \in \mathbb{Z}[\underline{t}]$ homogeneous of degree n, $n+\ell-1$ such that $d_{(\underline{x})}(\bar{f}) = \theta$ and $d_{(\underline{x})}(\bar{g}) = \ell(\theta)$. Then by (50) and Proposition 3.8 , $\bar{f} = \bar{g}$ as functions on G'. The first statement then follows from Proposition 3.8 .

Since z is invertible in $\mathbb{Z}_\ell$, the second statement follows after we tensor everything with $\mathbb{Z}_\ell$. □

3.4. Conjecture 2.

In this section, we will propose a refinement of conjecture 1. Then we will discuss the main results about this refined conjecture. Their proofs will be postponed untill Section 5. As in 3.3, we continue to assume that G is of the $(\ell, \dots, \ell)$-type for a fixed ℓ. Let I be the augmentation ideal of $\mathbb{Z}[G]$.

DEFINITION 3.10. — *Suppose that z is an integer such that $z\Theta \in \mathbb{Z}[G]$ and $z \cdot \mathcal{D}_G \in \mathrm{Sym}_r(G)$. As before, if $z\Theta$ is in I^n, then we denote by $(z\theta_G)^{(n)}$ its image in I^n/I^{n+1}. Also denote*

$$z\mathrm{det}_G = d(z \cdot \mathcal{D}_G) \quad \textit{and} \quad e = (\ell - 1) \cdot \mathrm{ord}_\ell(z) + r.$$

Then Lemma 3.9 and conjecture 1 together suggest the following conjecture.

CONJECTURE 2. — *Assume that G is horizontal, $\Theta_G \in \mathbb{Q}[G]$ and $r > 0$. Then we have $\mathrm{ord}(z\Theta_G) \geq e$ and*

$$(z\theta_G)^{(e)} = |\text{Ш}_K| \cdot \phi_S \cdot z\mathrm{det}_G . \tag{51}$$

Note that the number e and hence the conjecture depend on z. But by Lemma 3.9, we see that for every z' divisible by z, conjecture 2 is true for the pair (G, z') if and only if it is true for the pair (G, z).

As before, we denote by L/K the field extension corresponding to G.

DEFINITION 3.11. — *When K is a number field, we say that the conjecture of Birch and Swinnerton-Dyer is* true *for $(\mathbb{E}, G)$, if the conjecture is true for $\mathbb{E}_{/K}$, and for every cyclic subextension L'/K of L/K, it is also true for $\mathbb{E}_{/L'}$. When K is a function field, we say that the conjecture of Birch and Swinnerton-Dyer is* true *for $(\mathbb{E}, G)$, if it is true for $\mathbb{E}_{/K}$.*

In 5.1, we will show the following theorem.

THEOREM 3.12. — *Assume that $\ell \neq 2, 3$. If the Birch and Swinnerton-Dyer conjecture is true for $(\mathbb{E}, G)$ and $r > 0$, then we have $z\Theta_G \in I^e$.*

Suppose that the Birch and Swinnerton-Dyer conjecture is true for $(\mathbb{E}, G)$. By Proposition 3.8 and Theorem 3.12 , let $f_1, f_2 \in \mathbb{Z}[\underline{t}]$ be homogeneous polynomials of degree e such that

$$d_{(\underline{x})}(\bar{f}_1) = (z\theta_G)^{(e)} \tag{52}$$

and

$$d_{(\underline{x})}(\bar{f}_2) = |\text{Ш}_K| \cdot \phi_S \cdot z\det_G . \tag{53}$$

Then in this case (51) is equivalent to the following.

CONJECTURE 2′. — We have:

$$\bar{f}_1 = \bar{f}_2 . \tag{54}$$

DEFINITION 3.13. — *The pair (ℓ, G) will be called* good , *if the Birch and Swinnerton-Dyer conjecture is true for $(\mathbb{E}, G)$ and*

$$6 \cdot w \cdot |\text{Ш}_K| \cdot \prod_{v \notin S_\infty} m_v \not\equiv 0 \pmod{\ell}. \tag{55}$$

If Ш_K is finite, then (55) is satisfied for almost all ℓ. In 5.1, we will show the following theorem.

THEOREM 3.14. — *Suppose that $r > 0$ and (ℓ, G) is good. If $\bar{f}_1$ and $\bar{f}_2$ are defined by (52) and (53), then their zero sets on G' are the same. Namely, for $g' \in G'$, $\bar{f}_1(g') = 0$ if and only if $\bar{f}_2(g') = 0$.*

Recall that $S = \text{Supp}(D)$. Conjecture 2 depends on the choice of D. But by Proposition 3.8 and the compatibilities of the theta element (see Definition 1.8) and the discriminant (see (38), (39),(40)), we have the following lemma.

LEMMA 3.15. — *Suppose that D is an admissible divisor and G is a quotient of W_D. Then any one of conjecture 2, Theorem 3.12 and Theorem 3.14 is true for (D, G), if and only if it is true for every pair (D', H) where D' is an admissible divisor such that $D' \succeq D$, and H is a cyclic quotient of G.*

Usually, Theorem 3.14 is not strong enough to imply (54). However, if $e = 1$, then f_1 and f_2 are linear functionals. In this case, if they have the same zero set, then they are proportional to each other, *i.e.*, (54) is true up to a constant in $\mathbb{F}_\ell^*$. The same is true when G is cyclic, since in this case the space of e-th degree homogeneous functions on G' is of dimension one over $\mathbb{F}_\ell$. Thus we have the following theorem.

THEOREM 3.16. — *Suppose that $r > 0$ and (ℓ, G) is good. If $e = 1$ or G is cyclic, then (54) is true up to a constant in $\mathbb{F}_\ell^*$.*

To push our results a little further, we need to make the following considerations. Recall the isomorphisms d and $d_{(\underline{x})}$ defined in 3.3. For an element $y \in G$, let $f_y \in \mathbb{F}_\ell[\underline{t}]$ be the unique linear polynomial such that $d_{(\underline{x})}(f_y) = d(y)$.

DEFINITION 3.17. — *A homogeneous $f \in \mathbb{F}_\ell[\underline{t}]$ is called* special, *if there exist $y_1, \ldots, y_e \in G$ satisfying the condition that $f = \prod_{i=1}^{e} f_{y_i}$ and every subset of $(e-1)$ elements of $\{y_1, \ldots, y_e\}$ spans an $(e-1)$-dimensional subspace of G.*

LEMMA 3.18. — *Suppose that $h_1, h_2 \in \mathbb{F}_\ell[\underline{t}]$ are e-th degree homogeneous polynomials and h_2 is special. If $\bar{h}_1$ and $\bar{h}_2$ have the same zero set, then there exists a $c \in \mathbb{F}_\ell^*$ such that $\bar{h}_1 = c \cdot \bar{h}_2$.*

Proof. — Suppose that $h_2 = \prod_{i=1}^{e} f_{y_i}$ and $(\underline{t}) = (t_1, t_2, \ldots, t_k)$. Without loss of generality, we can assume that $f_{y_i} = t_i$ for $i = 1, \ldots, e-1$. Then we can write

$$h_2 = t_1 \cdots t_{e-1} \cdot f_{y_e}.$$

There is an $(e-1)$-th degree homogeneous polynomial, $h'(\underline{t})$, such that

$$h_1(\underline{t}) = h_1(0, t_2, \ldots, t_k) + t_1 \cdot h_1'(\underline{t}).$$

Since $\bar{h}_1$ and $\bar{h}_2$ have the same zero set and $\bar{h}_2(0, t_2, \ldots, t_k) = 0$, we see that $\bar{h}_1(0, t_2, \ldots, t_k) = 0$ and $\bar{h}_1 = \bar{t}_1 \cdot \bar{h}_1'$. We can then replace h_1 by $t_1 \cdot h'$ if necessary and assume that h_1 is divisible by t_1. Using a similar argument, we can assume that

$$h_1(\underline{t}) = t_1 \cdots t_{e-1} \cdot h(\underline{t}).$$

Since h_1 is homogeneous of degree equal to e, the polynomial h must be a linear form. Suppose that f_{y_e} is not proportional to any of the f_{y_i} for

$i = 1, \ldots, e-1$. Then the zero sets of $\bar{h}$ and $\bar{f}_{y_e}$ are the same. Since they are both linear, they must be proportional to each other, and the lemma is proved. Suppose that f_{y_e} is proportional to some f_{y_i}. Since h_2 is special, this can happen only when $e = 2$. In this case, the zero set of $\bar{h}$ must equal to that of $\bar{t}_1$ and both $\bar{h}_1$ and $\bar{h}_2$ are proportional to $\bar{t}_1^2$. □

When $S = S_m$, $r_K = 0$ and (ℓ, G) is good, the polynomial f_2 can be chosen as a product of linear factors. This is explained in the following. Suppose $S_m = \{v_1, \ldots, v_r\}$. For $v_i \in S_m$, let $y_i \in G$ be the image of $\overline{Q}_{v_i}$ (defined in 2.2) under the projection $C_S \to G$. Then by (27), (39), (43) and (55), we see that if $e = r$, then f_2 can be taken to be proportional to the product $\prod_{i=1}^{e} f_{y_i}$. If $e > r$, then by (50), f_2 can still be taken as a product of linear forms (in this case, f_2 cannot be special).

DEFINITION 3.19. — *We call a quotient group G of C_S* special *if G is horizontal and f_2 can be taken taken to be a special polynomial.*

LEMMA 3.20. — *Suppose that $S = S_m$, $r_K = 0$, $e = r$, and K is a function field of characteristic $p = \ell$. Then each horizontal quotient of C_S is a quotient of some special quotient H of C_S.*

Proof. — By a result of Kisilevsky (see [K], or [Tn4]), as a topological group, the pro-p completion of C_S is a countable product of $\mathbb{Z}_p$. It is enough to show that in C_S, if $\prod_{i=1}^{e-1} \bar{Q}_{v_i}^{a_i}$ is a p-th power for some integers a_i, $i = 1, \ldots, e-1$, then each a_i is divisible by p. Under the hypothesis, there are $u_i \in K_{v_i}^*$ for $i = 1, \ldots, e$ and $u \in K^*$ such that

$$Q_{v_i}^{a_i} = u_i^p \cdot u, \text{ in } K_{v_i} \text{ for } i = 1, \ldots, e-1,$$

and

$$1 = u_e^p \cdot u \text{ in } K_{v_e}.$$

By the local Leopoldt lemma (see [K], [Tn4]), the element u must be a p-th power in K^*. This implies that every $Q_{v_i}^{a_i}$, for $i = 1, \ldots, e-1$, is a p-th power in $K_{v_i}^*$. Since by (55), p is relatively prime to $m_{v_i} = \mathrm{ord}_v(Q_{v_i})$, a_i must be divisible by p. □

THEOREM 3.21. — *Suppose that $r > 0$, (ℓ, G) is good and f_1, f_2 are defined by* (52) *and* (53). *Then the following are true:*

(a) *If the polynomial f_2 can be chosen to be special, then $\bar{f}_1$ and $\bar{f}_2$ are proportional to each other.*

(b) *Assume that K is a function field with characteristic $p = \ell$ and $r_K = 0$. If $S = S_m$ and for every horizontal quotient H of C_S, $\Theta_H \in \mathbb{Z}_\ell[H]$, then conjecture 2 is true.*

The first statement is a consequence of Lemma 3.18. To show the second statement, we first use Lemma 3.20 to find a special quotient of C_S, which has G as a quotient. By Lemma 3.15, we can replace G by this special group. Note that after doing so, the pair (ℓ, G) is still good. Then by the first statement, there is a $c \in \mathbb{F}_\ell^*$ such that

$$(*) \qquad \bar{f}_1 = c \cdot \bar{f}_2.$$

We need to show that $c = 1$. By Lemma 3.20 again, we can assume that the constant field extension of degree ℓ is contained in L. The Galois group of this constant field extension is a quotient of G. We then replace G by this quotient and still call it G. After doing so, the equation (*) still holds. Note that since $e = r$, the equation (54) is equivalent to (44). The quotient map $C_S \to G$ factors through the degree map $C_S \to \mathbb{Z}$. As explained in 3.2, the Birch and Swinnerton-Dyer conjecture (for $\mathrm{E}_{/K}$) is equivalent to the formula (44) (for $\mathbb{Z}$). Assuming the Birch and Swinnerton-Dyer conjecture, the formula (44) is also true for $\mathbb{Z}$. By taking the quotient map from $\mathbb{Z}$ to G, we see that (44) is true for G. This implies

$$\bar{f}_1 = \bar{f}_2 .$$

By Lemma 3.9, we have $c = 1$ unless $\bar{f}_2 = 0$. But by (55), both $|\text{Ш}_K|$ and ϕ_S are prime to ℓ, and $y_i \neq 1 \in G$ for $i = 1, \ldots, r$. Since $\bar{f}_2 = |\text{Ш}_K| \cdot \phi_S \cdot \left(\prod_{i=1}^{r} \bar{f}_{y_i}\right)$, it is nontrivial. □

4. The degeneration.

To prove Theorem 3.14 , we need to compare the zero sets of the two functions $\bar{f}_1$ and $\bar{f}_2$. By Lemma 3.15, we can assume that the admissible divisor D is the conductor of the abelian extension L/K. In this section, we study the zero set of $\bar{f}_2$ under the above assumption. For a positive integer n, a character $\chi \in \widehat{G}$ and an element $\theta \in I^n/I^{n+1}$, let $o(\chi, \theta)$ be the valuation defined in 3.3. By Proposition 3.8 , we need to determine whether $o(\chi, |\text{Ш}| \cdot \phi_S \cdot z\det_G)$ is greater than e. Since the result for the trivial character is obvious, we can assume that χ is nontrivial. As in Section 3, ℓ is a prime number and G denotes the Galois group of the abelian extension L/K.

ASSUMPTION 5. — In this section, we assume that G is cyclic of order ℓ, (ℓ, G) is good, D is the conductor of the abelian extension L/K, and χ is a nontrivial character of G.

Note that by Remark 4 in 2.1, since $(\ell, 2) = 1$, the extension is compatible with the set S at every place. Thus Lemma 2.4 can be applied.

Our main result is the following proposition, which will be proved in 4.5. Recall that

$$r_K = \operatorname{rk}\big(\mathbb{E}(K)\big).$$

We also denote

$$r_L = \operatorname{rk}\big(\mathbb{E}(L)\big).$$

PROPOSITION 4.1. — *Suppose that G is cyclic of order ℓ, (ℓ, G) is good, D is the conductor of the abelian extension L/K, and χ is a nontrivial character of G. Then $o(\chi, |\text{Ш}| \cdot \phi_S \cdot z\det_G) > e$ if and only if at least one of the following is true:*

(a) $r_L > r_K$;

(b) Ш_L *has non-trivial ℓ-primary part.*

4.1. The valuation of the discriminant.

The pairing $\langle\cdot\,,\cdot\rangle_G$ induces a pairing

$$\langle\cdot,\cdot\rangle_{G,\mathbb{F}_\ell} : A_S \otimes \mathbb{F}_\ell \times B_S \otimes \mathbb{F}_\ell \longrightarrow G.$$

Since (ℓ, G) is good and ℓ is prime to w (see (55)), the $\mathbb{F}_\ell$-dimensions of $A_S \otimes \mathbb{F}_\ell$ and $B_S \otimes \mathbb{F}_\ell$ both equal r. By fixing a basis for these $\mathbb{F}_\ell$-vector spaces, we can define the discriminant of $\langle\cdot,\cdot\rangle_{G,\mathbb{F}_\ell}$

$$\operatorname{disc}_{G,\mathbb{F}_\ell} \in \operatorname{Sym}_r G.$$

Let pr_S be the projection $C_S \to G$ and disc_S the discriminant defined in 2.3. Then $\operatorname{pr}_S(\operatorname{disc}_S)$ and $\operatorname{disc}_{G,\mathbb{F}_\ell}$ differ at most by a constant in F_ℓ^*. The pairing $\langle\cdot,\cdot\rangle_{G,\mathbb{F}_\ell}$ is degenerate if and only if the discriminant $\operatorname{disc}_{G,\mathbb{F}_\ell}$ is trivial.

Definition 4.2. — *We will say that the pairing $\langle\cdot,\cdot\rangle_G$ is* degenerate, *if the pairing $\langle\cdot,\cdot\rangle_{G,\mathbb{F}_\ell}$ is degenerate.*

Lemma 4.3. — *Suppose that G is cyclic, (ℓ, G) is good, and χ is a nontrivial character of G. Then $o(\chi, |\text{Ш}|\cdot\phi_S\cdot z\det_G) > e$ if and only if at least one of the following is true:*

(a) *We have*

$$\left|\mathrm{cokernel}\left\{B_{S_m}\to\prod_{v\in S-S_m-S_\infty}\mathbb{E}'(k_v)\right\}\right|\equiv 0 \pmod{\ell}.$$

(b) *The pairing $\langle\cdot\,,\cdot\rangle_G$ is degenerate.*

Proof. — By (43) and (55), the numbers $|\text{Ш}|$ and ϕ_S are relatively prime to ℓ. By Lemma 3.9, we see that

$$o\big(\chi, |\text{Ш}|\cdot\phi_S\cdot z\det_G\big) = o(\chi,\det_G) - r + e.$$

Recall the morphisms d (defined in 3.3, (47)) and $\mathcal{U}_{S,T}$ (defined in 2.3, (34)). Since the support of the conductor of χ is S, we can view χ as a character of C_S. For each proper subset T of S, we have

$$\chi\big(\mathcal{U}_{S,T}(c)\big) = 1 \quad \text{for all } c\in C_T.$$

Therefore

$$o(\chi,\det_G) = o\big(\chi, j_S\cdot d\circ \mathrm{pr}_S(\mathrm{disc}_S)\big).$$

By (55) and Definition 2.14, we see that (a) holds if and only if

$$j_S\equiv 0 \pmod{\ell}.$$

It then remains to show that (b) holds if and only if

$$d\circ\mathrm{pr}_S(\mathrm{disc}_S) = 0.$$

This will follow from the facts that $\mathrm{pr}_S(\mathrm{disc}_S)$ is proportional to $\mathrm{disc}_{G,\mathbb{F}_\ell}$ and d is an isomorphism for $G\simeq\mathbb{F}_\ell$. $\square$

4.2. The global duality theorem.

In this section we recall the global duality theorem of Tate and Milne. We need only a part of it. The references are [T1] and [Ml2].

Denote by $\mathbb{E}(K,\ell)$ and $\mathbb{E}(K_v,\ell)$ the ℓ-adic completion of the groups $\mathbb{E}(K)$ and $\mathbb{E}(K_v)$. Also, denote by $H^1(K,\mathbb{E},\ell)$ and $H^1(K_v,\mathbb{E},\ell)$ the ℓ-primary components of the cohomology groups $H^1(K,\mathbb{E})$ and $H^1(K_v,\mathbb{E})$. Using the local duality theorem, we can identify $H^1(K_v,\mathbb{E},\ell)$ with the topological dual group of $\mathbb{E}(K_v,\ell)$.

Let λ_0 and λ_1 be the localization maps:

$$\lambda_0 : \mathbb{E}(K,\ell) \longrightarrow \prod_v \mathbb{E}(K_v,\ell),$$
$$\lambda_1 : H^1(K,\mathbb{E},\ell) \longrightarrow \bigoplus_v H^1(K_v,\mathbb{E},\ell).$$

These and the above identifications induce the following sequence:

$$H^1(K,\mathbb{E},\ell) \xrightarrow{\lambda_1} \bigoplus_v H^1(K_v,\mathbb{E},\ell) \xrightarrow{\lambda_0^*} \mathbb{E}(K,\ell)^*. \tag{56}$$

Here $\mathbb{E}(K,\ell)^*$ is the topological dual of the compact group $\mathbb{E}(K,\ell)$. The global duality theorem says the following.

THEOREM 4.4 (Global Duality, [T1], [Ml2]). — *If the ℓ-primary part of* Ш *is finite, then the sequence* (56) *is exact.*

4.3. The null space of the pairing.

DEFINITION 4.5. — *Define the* null space *of the G-pairing as*

$$\mathcal{N} = \{a \in A_S \mid \langle a,b\rangle_G = 0, \text{ for all } b \in B_S\}.$$

Then we have

$$\ell \cdot A_S \subset \mathcal{N}.$$

The pairing $\langle\cdot,\cdot\rangle_G$ is degenerate if and only if

$$\mathcal{N} \neq \ell \cdot A_S.$$

In this and the next sections, we study this degenerate situation.

Let A_S^0 be the kernel of the natural morphism,

$$A_S \longrightarrow \prod_{v \in S_m} \mathbb{E}(K_v).$$

Then A_S^0 is generated by the local periods $[Q_v], v \in S_m$. Since (ℓ, G) is good, the assumption about the order of the torsions (see (55)) implies that

$$A_S^0 \cap \ell \cdot A_S = \ell \cdot A_S^0.$$

DEFINITION 4.6. — *We say that the pairing* $\langle \cdot, \cdot \rangle_G$ *is* degenerate of the first kind, *if*

$$\mathcal{N} \cap A_S^0 \neq \ell \cdot A_S^0.$$

It is degenerate of the second kind, *if*

$$\mathcal{N} \cap A_S^0 = \ell \cdot A_S^0 \quad \text{and} \quad \mathcal{N} \neq \ell \cdot A_S.$$

Note that $\langle \cdot, \cdot \rangle_G$ is degenerate if and only if it is either degenerate of the first kind or degenerate of the second kind. In this section, we will treat the first case.

DEFINITION 4.7. — *A nontrivial element of $H^1(K, \mathbb{E})$ is called of* G-type *if its image under the localization map $H^1(K, \mathbb{E}) \to \bigoplus_v H^1(K_v, \mathbb{E})$ is contained in $\bigoplus_v H^1(G_v, \mathbb{E}(L_v))$.*

LEMMA 4.8. — *Assume that G is cyclic of order ℓ and (ℓ, G) is good. There is a nontrivial G-type element in $H^1(K, \mathbb{E})$ if and the only if the natural morphism*

$$\mathbb{E}(K) \longrightarrow \prod_v \mathbb{E}(K_v) \longrightarrow \prod_v \mathbb{E}(K_v)/N_{G_v}(\mathbb{E}(L_v))$$

has nontrivial cokernel.

The natural maps

$$\bigoplus H^1(G_v, \mathbb{E}(L_v)) \longrightarrow \bigoplus H^1(K_v, \mathbb{E}),$$

$$\prod_v \mathbb{E}(K_v) \longrightarrow \prod_v (K_v)/N_{G_v}(L_v)$$

and the local duality pairing induce a perfect pairing

$$\bigoplus H^1(G_v, \mathbb{E}(L_v)) \times \prod_v \mathbb{E}(K_v)/N_{G_v}(\mathbb{E}(L_v)) \longrightarrow \mathbb{F}_\ell.$$

The natural morphism

$$\mathbb{E}(K) \longrightarrow \prod_v \mathbb{E}(K_v) \longrightarrow \prod_v \mathbb{E}(K_v)/N_{G_v}(L_v)$$

has nontrivial cokernel if and only if the natural morphism

$$\bigoplus H^1(G_v, \mathbb{E}(L_v)) \longrightarrow \bigoplus H^1(K_v, \mathbb{E}) \xrightarrow{\lambda_0^*} \mathbb{E}(K, \ell)^*$$

has nontrivial kernel. Here λ_0^* is the map defined in 4.2. The lemma is then a consequence of Theorem 4.4. □

Denote

$$\mathbb{E}_{(G_v)} = \mathbb{E}(K_v)/N_{G_v}(\mathbb{E}(L_v)).$$

Since (ℓ, G) is good, by (55) and Lang's theorem (see [T1]), $\mathbb{E}_{(G_v)}$ is trivial for $v \notin S$. For $v \in S - S_m$, the extension L/K is tamely ramified at v, and $\mathbb{E}_{(G_v)} \simeq \mathbb{E}(k_v)/\ell \cdot \mathbb{E}(k_v)$. For $v \in S_m$, it is well-known that $\mathbb{E}_{(G_v)}$ is either trivial or cyclic of order ℓ. It is nontrivial if and only if the local period Q_v is a G_v-norm in K_v^*. Let

$$S_m^0 = \{v \in S_m \mid \mathbb{E}_{(G_v)} \text{ is nontrivial}\}.$$

Then we have

$$\mathbb{E}_{(G_v)} \simeq \begin{cases} \mathbb{Z}/\ell\mathbb{Z} & \text{for } v \in S_m^0, \\ \mathbb{E}(K_v)/\ell \cdot \mathbb{E}(K_v) & \text{for } v \in S - S_m, \\ 0 & \text{otherwise.} \end{cases} \tag{57}$$

LEMMA 4.9. — *Assume that G is cyclic of order ℓ, (ℓ, G) is good and D equals the conductor of the extension L/K. There is a nontrivial G-type element in $H^1(K, \mathbb{E})$ if and only if at least one of the following is true:*

(a)

$$\left|\text{cokernel}\left\{B_{S_m} \to \prod_{v \in S - S_m - S_\infty} \mathbb{E}'(k_v)\right\}\right| \equiv 0 \pmod{\ell}.$$

(b) *The pairing $\langle \cdot , \cdot \rangle_G$ is degenerate of the first kind.*

Proof. — Let

$$\mathbb{E}^0(K) = \ker\Big\{\mathbb{E}(K) \to \prod_{v\in S-S_m} \mathbb{E}(k_v)\Big\}.$$

Then we have the diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{E}^0(K) & \longrightarrow & \mathbb{E}(K) & \longrightarrow & \mathbb{E}(K)/\mathbb{E}^0(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in S_m} \mathbb{E}_{(G_v)} & \longrightarrow & \prod_{v\in S_m} \mathbb{E}_{(G_v)} \times \prod_{v\in S-S_m} \mathbb{E}(k_v) & \longrightarrow & \prod_{v\in S-S_m} \mathbb{E}(k_v) & \longrightarrow & 0. \end{array} \tag{58}$$

Since for $v \in S - S_m$, the number ℓ is prime to the residual characteristic of v, $\mathbb{E}_1(K_v)$ (defined in 1.1) has trivial ℓ-primary part, by (57) we see that

$$\Big|\text{cokernel}\Big\{\mathbb{E}(K) \to \prod_{v\in S-S_m} \mathbb{E}(k_v)\Big\}\Big| \equiv 0 \pmod{\ell}$$

if and only if

$$\Big|\text{cokernel}\Big\{\mathbb{E}(K) \to \prod_{v\in S-S_m} \mathbb{E}_{(G_v)}\Big\}\Big| \equiv 0 \pmod{\ell}.$$

Also

$$\Big|\text{cokernel}\Big\{\mathbb{E}(K) \to \prod_{v\in S_m} \mathbb{E}_{(G_v)} \times \prod_{v\in S-S_m} \mathbb{E}(k_v)\Big\}\Big| \equiv 0 \pmod{\ell}$$

if and only if

$$\Big|\text{cokernel}\Big\{\mathbb{E}(K) \to \prod_{v\in S} \mathbb{E}_{(G_v)}\Big\}\Big| \equiv 0 \pmod{\ell}.$$

Since $S_\infty = \emptyset$ (Assumption 3), we have

$$\Big|\text{cokernel}\Big\{B_{S_m} \to \prod_{v\in S-S_m-S_\infty} \mathbb{E}'(k_v)\Big\}\Big| \equiv 0 \pmod{\ell}$$

if and only if

$$\Big|\text{cokernel}\Big\{\mathbb{E}(K) \to \prod_{v\in S-S_m} \mathbb{E}(k_v)\Big\}\Big| \equiv 0 \pmod{\ell}.$$

By these and by applying the «snake lemma» to the diagram (58), we see that it is sufficient to show that (b) is true if and only if

$$\left|\operatorname{cokernel}\left\{\mathbb{E}(K)^0 \to \prod_{v\in S_m^0} \mathbb{E}_{(G_v)}\right\}\right| \equiv 0 \pmod{\ell}.$$

Recall the map β defined in (24). We have the following commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \bigoplus_{v\in S_m^0} \mathbb{Z}[Q_v]' \arrow[r] \arrow[d] & B_S \arrow[r, "\beta"] \arrow[d] & \mathbb{E}^0(K) \arrow[r] \arrow[d] & 0 \\ & 0 \arrow[r] & \prod_{v\in S_m^0} B_v/N_{G_v}(B_w) \arrow[r, "\sim"] & \prod_{v\in S_m^0} \mathbb{E}_{(G_v)}. & \end{tikzcd}$$

It is then sufficient to show that (b) holds if and only if

$$\left|\operatorname{cokernel}\left\{B_S \to \prod_{v\in S_m^0} B_v/N_{G_v}(B_w)\right\}\right| \equiv 0 \pmod{\ell}. \tag{59}$$

By Lemma 2.11, the global pairing $\langle\cdot\,,\cdot\rangle_G$ induces a pairing

$$\bigoplus_{v\in S_m^0} \mathbb{Z}/\ell\cdot\mathbb{Z}[Q_v] \times \operatorname{Im}\left\{B_S \to \prod_{v\in S_m^0} B_v/N_{G_v}(B_w)\right\} \longrightarrow G.$$

By counting and by Lemma 2.11, we see that (59) holds if and only if there is an element

$$a \in \bigoplus_{v\in S_m^0} \mathbb{Z}[Q_v] \cap \mathcal{N} - \bigoplus_{v\in S_m^0} \ell\cdot\mathbb{Z}[Q_v].$$

To complete the proof, we need to show that

$$\mathcal{N} \cap A_S^0 \subset \Big(\mathcal{N} \cap \bigoplus_{v\in S_m^0} \mathbb{Z}\cdot[Q_v]\Big) + \ell\cdot A_S^0.$$

For this, suppose that

$$a = \sum_{v\in S_m} \alpha_v \cdot [Q_v] \in \mathcal{N} \cap A_S^0 - \ell\cdot A_S^0.$$

If $v \in S_m$ such that $\alpha_v \not\equiv 0 \pmod{\ell}$, then by (27), we see that Q_v is a G_v-norm and $\mathbb{E}(K_v)/N_{G_v}(L_v)$ is nontrivial. Therefore a is an element of $\bigoplus_{v\in S_m^0} \mathbb{Z}\cdot[Q_v] + \ell\cdot A_S^0$. $\square$

4.4. Schneider pairing.

In this section, we study the second kind degeneration for the pairing $\langle\cdot,\cdot\rangle_G$. We will assume that the cokernel of the map

$$\mathbb{E}(K) \longrightarrow \prod_{v\in S-S_m} \mathbb{E}(k_v)$$

has trivial ℓ-primary part. Under this technical assumption, our theory will be sufficient for the proof of Proposition 4.1.

To simplify the notation, we will identify $\mathbb{E}'$ with $\mathbb{E}$ and view B_S as a subgroup of A_S in the obvious way.

DEFINITION 4.10. — *Define the pairing $\langle\cdot,\cdot\rangle'_G : B_S \times A_S \to G$ as the «mirror image» of $\langle\cdot,\cdot\rangle_G$, i.e.,*

$$\langle b,a\rangle'_G = \langle a,b\rangle_G, \quad \text{for } a\in A_S,\ b\in B_S.$$

By Remark 3 in 2.1, we have

$$\langle b,a\rangle_G = \langle b,a\rangle'_G = \langle a,b\rangle_G, \quad \text{for all } a,b\in B_S. \tag{60}$$

We can extend the pairing $\langle\cdot,\cdot\rangle_G$ to $A_S\otimes\mathbb{Z}_\ell \times B_S\otimes\mathbb{Z}_\ell$, and also make the similar extension for $\langle\cdot,\cdot\rangle'_G$. These extensions do not change the degenerate situation of the pairing. Since (ℓ,G) is good, the order of torsion w is relatively prime to ℓ, $A_S\otimes\mathbb{Z}_\ell$ and $B_S\otimes\mathbb{Z}_\ell$ are free $\mathbb{Z}_\ell$-modules. We can choose a basis of $A_S\otimes\mathbb{Z}_\ell$, $\{a_1,\dots,a_r\}$, such that $\{b_1=\ell^{\mu_1}\cdot a_1,\dots,b_r=\ell^{\mu_r}\cdot a_r\}$ is a basis of $B_S\otimes\mathbb{Z}_\ell$ and $\mu_1\geq\ldots\geq\mu_r$. Let m be greatest integer such that $\mu_m>0$. By (60), we have

$$\langle a_i,b_j\rangle_G = \ell^{\mu_j}\cdot\langle a_i,a_j\rangle'_G = 0, \quad i=m+1,\dots,r;\ j=1,\dots,m. \tag{61}$$

By choosing a generator of G, we identify G with $\mathbb{F}_\ell$.

LEMMA 4.11. — *Assume that G is cyclic of order ℓ, (ℓ,G) is good, D equals the the conductor of the extension L/K, and the cokernel of the map $\mathbb{E}(K)\to\prod_{v\in S-S_m}\mathbb{E}(k_v)$ has trivial ℓ-primary part. Then*

(a) *The matrix $(\langle a_i,b_j\rangle_G)_{1\leq i,j\leq m}$ is non-degenerate over $\mathbb{F}_\ell$.*

(b) *If a is an element of $\mathcal{N}-(A_S^0\cup\ell\cdot A_S)$, then for each $v\in S_m$, a_v is a G_v-norm, and $a\in A_S\cap B_S\otimes\mathbb{Z}_\ell\subset A_S\otimes\mathbb{Z}_\ell$.*

Proof. — Assertion (b) is a direct consequence of (a) and Lemma 2.11. To show (a), suppose that (a) is false. Then following from (61), there is a $b \in (B_S \cap \ell \cdot A_S) - \ell \cdot B_S$ such that

$$(*) \qquad \langle a', b\rangle_G = 0, \quad \text{for all } a' \in A_S.$$

Thus, we wish to show that (*) cannot happen.

Let $b' \in A_S$ such that $b = \ell \cdot b'$. Since b' is not in B_S, we can find $v_0 \in S - S_m$ such that $b' \notin B_{v_0} = \mathbb{E}_1(K_{v_0})$ (see (L_4) in 2.1). As before, let w_0 be a chosen place of L sitting over v_0, and $G_{v_0} = \mathrm{Gal}(L_{w_0}/K_{v_0})$. As ℓ is prime to the residue character $(= l')$ of K_{v_0} and $\mathbb{E}_1(L_{w_0})$ is a $\mathbb{Z}_{l'}$-module, we have

$$\mathbb{E}_1(K_{v_0}) = N_{G_{v_0}}\big(\mathbb{E}_1(L_{w_0})\big).$$

Let $y_{w_0} \in \mathbb{E}_1(L_{w_0})$ be such that

$$N_{G_{v_0}}(y_{w_0}) = b.$$

Then $N_{G_{v_0}}(b' - y_{w_0}) = 0$ and $b' - y_{w_0}$ defines a class

$$\xi \in H^1(G_{v_0}, \mathbb{E}(L_{w_0})).$$

Since G_{v_0} acts trivially on $\mathbb{E}(L_{w_0})/\mathbb{E}_1(L_{w_0})$ and $b' \notin \mathbb{E}_1(L_{w_0})$, we must have $\xi \neq 0$.

By assumption, cokernel$\big\{\mathbb{E}(K) \to \prod_{v\in S-S_m} \mathbb{E}(K_v)\big\}$ has trivial ℓ-primary part, so we can find an

$$a' = \big(x', (a'_v)_v\big) \in A_S \cap \bigoplus_{1\le i\le m} \mathbb{Z}_\ell a_i$$

with the condition that for $v \neq v_0$, $a'_v \in B_v$, and for $v = v_0$, $a'_{v_0} \in A_{v_0}$ such that the local duality pairing

$$(a_{v_0}, \xi)_{v_0} \neq 0.$$

In the following, we will complete the proof by showing that the global pairing $\langle a', b\rangle_G$ is nontrivial.

Recall the map α (defined in 2.2) and the biextension $\mathbb{P}_{/K}$ (defined in 2.1). Let $\widetilde{P}_S = (\alpha^*, \alpha^*)\mathbb{P}(K)$. Then $\widetilde{P}_S$ is a biextension of $A_S \times A_S$ by K^*.

As we identify B_S with a subgroup of A_S, we can also identify P_S with a subset of $\widetilde{P}_S$ and obtain the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K^* & \longrightarrow & \widetilde{P}_S & \xrightarrow{\pi_S} & A_S \times A_S & \longrightarrow & 0 \\
 & & \| & & \cup & & \cup & & \\
0 & \longrightarrow & K^* & \longrightarrow & P_S & \xrightarrow{\pi_S} & A_S \times B_S & \longrightarrow & 0.
\end{array}$$

Let p' be a lifting of $a' \times b'$ in ${}_{\{a'\}}\widetilde{P}_S$. Then $p = \ell \cdot p' \in_{\{a'\}} P_S$ is a lifting of $a' \times b$ in P_S. Suppose that $v \neq v_0$. Then $a'_v \in B_v$. By Remark (3) at the end of 2.1, we have

$$\psi_v(p_v) = \psi'_v(p_v) = \ell \cdot \psi'_v(p'_v) \in \ell \cdot C_v.$$

By the definition of the global pairing, the v-component of p has no contribution to the pairing $\langle a', b\rangle_G$.

Since G is totally ramified at v_0, by the class field theory [AT], $G \simeq C_{v_0}/\ell \cdot C_{v_0}$. Let P_{w_0} be the subset of $\mathbb{P}(L_{w_0})$ sitting over $\mathbb{E}(L_{w_0}) \times \mathbb{E}_1(L_{w_0})$. We have the following diagram of exact sequences:

$$\begin{array}{ccccccc}
0 & \longrightarrow & L^*_{w_0} & \longrightarrow & {}_{\{a'\}}\mathbb{P}(L_{w_0}) & \xrightarrow{\pi_{v_0}} & \{a'\} \times \mathbb{E}(L_{w_0}) \\
 & & \| & & \cup & & \cup \\
0 & \longrightarrow & L^*_{w_0} & \longrightarrow & {}_{\{a'\}}P_{w_0} & \xrightarrow{\pi_{v_0}} & \{a'\} \times \mathbb{E}_1(L_{w_0}).
\end{array}$$

The lower row of the diagram induces the exact sequence

$$\begin{aligned}(62)\quad 0 \to C_{v_0}/\ell \cdot C_{v_0} &\xrightarrow{\sim} {}_{\{a'\}}P_{v_0}/N_{G_{v_0}}\big({}_{\{a'\}}P_{w_0}\big) \\ &\longrightarrow \{a'\} \times \mathbb{E}_1(K_{v_0})/N_{G_{v_0}}(\mathbb{E}_1\big(L_{w_0})\big) = 0.\end{aligned}$$

By Lemma 2.4, ψ_{v_0} induces the inverse of the isomorphism in the above sequence. If $\langle a', b\rangle_G = 0$, then

$$\psi_{v_0}(p_{v_0}) \in \ell \cdot C_{v_0},$$

hence

$$p_{v_0} \in N_{G_{v_0}}\big({}_{\{a'\}}P_{w_0}\big).$$

Suppose that $p_{v_0} = N_{G_{v_0}}(\eta)$, where $\eta \in {}_{\{a'\}}P_{w_0}$. Then

$$N_{G_{v_0}}(p'_{v_0} - \eta) = 0$$

and $(p'_{v_0} - \eta)$ defines a class

$$\{p'_{v_0} - \eta\} \in H^1\big(G_{v_0}, {}_{\{a'\}}P(L_{w_0})\big).$$

We have

$$\pi_{v_0 *}(\{p'_{v_0} - \eta\}) = \{a'\} \times \xi \in H^1\big(G_{v_0}, \{a'\} \times \mathbb{E}(L_{w_0})\big).$$

Consequently,

$$\partial\big(\{a'\} \times \xi\big) = 0,$$

where $\partial : \{a\} \times H^1(G_{v_0}, \mathbb{E}(L_{w_0})) \to H^2(G_{v_0}, L_{w_0})$ is the boundary map of cohomology groups induced by the above diagram. By Lemma 2.12, this implies that $(a'_{v_0}, \xi)_{v_0} = 0$, a contradiction. □

Recall that for each v, we have $\mathbb{E}_{(G_v)} = \mathbb{E}(K_v)/\mathbb{E}(L_v)$.

DEFINITION 4.12. — *Let*

$$^{(G)}\mathbb{E} = \operatorname{Ker}\Big\{\mathbb{E}(K) \to \prod_v \mathbb{E}_{(G_v)}\Big\},$$

$$^{(G)}\mathbb{E}' = \operatorname{Ker}\Big\{\mathbb{E}'(K) \to \prod_v \mathbb{E}'_{(G_v)}\Big\}.$$

Denote

$$B_S^1 = \operatorname{Ker}\Big\{B_S \to \prod_{v \in S_m} \mathbb{E}'_{(G_v)}\Big\}.$$

Let $\alpha : A_S \longrightarrow \mathbb{E}(K)$ be the map in (22). Then $\alpha(B_S^1) \subset {}^{(G)}\mathbb{E}$. At every $v \in S - S_m$, since the extension L_v/K_v is totally (and tamely) ramified, we have $N_{G_v}(\mathbb{E}(L_v)) = \ell \cdot \mathbb{E}(K_v)$. This and the assumption that the cokernel of $\mathbb{E}(K) \to \prod_{v \in S - S_m} \mathbb{E}(k_v)$ has trivial ℓ-part imply that there exists an integer n such that $(n, \ell) = 1$ and

$$n \cdot {}^{(G)}\mathbb{E} \subset \ell \cdot \mathbb{E}(K) + \alpha(B_S). \tag{63}$$

For each $x \in {}^{(G)}\mathbb{E}$, consider the exact sequence:

$$0 \to L^* \longrightarrow {}_{\{x\}}\mathbb{P}(L) \xrightarrow{f} \{x\} \times \mathbb{E}'(L) \to 0. \tag{64}$$

Locally we have the exact sequence

$$(65)\quad 0 \to K_v^*/N_{G_v}(L_v^*) \longrightarrow {}_{\{x\}}\mathbb{P}(K_v)/N_{G_v}\big({}_{\{x\}}\mathbb{P}(L_v)\big) \xrightarrow{f_*} \{x\} \times \mathbb{E}_{(G_v)}.$$

Note that in the above exact sequence we have 0 at the left end, because $x \in N_{G_v}(\mathbb{E}(L_v))$ and by Lemma 2.12, we have the trivial map

$$H^1\big(G_v, \{x\} \times \mathbb{E}'(L_v)\big) \xrightarrow{\partial} K_v^*/N_{G_v}(L_v^*).$$

Suppose that $y \in {}^{(G)}\mathbb{E}'$. We identify ${}^{(G)}\mathbb{E}'$ with a subset of $\{x\} \times \mathbb{E}'(K)$ and via (64) lift y to some $t \in_{\{x\}} \mathbb{P}(K)$. Since locally, $y \in N_{G_v}(\mathbb{E}'(L_v))$, by (65), we have

$$\bar{t}_v : = \big(t \pmod{N_{G_v}({}_{\{x\}}\mathbb{P}(L_v))}\big) \in K_v^*/N_{G_v}(L_v^*).$$

By the class field theory, we have the map

$$\lambda_v : K_v^*/N_{G_v}(L_v^*) \longrightarrow G_v \longrightarrow G.$$

DEFINITION 4.13. — *The* Schneider pairing,

$$\langle\cdot,\cdot\rangle_{\mathrm{Sch}} : {}^{(G)}\mathbb{E} \times {}^{(G)}\mathbb{E}' \longrightarrow G,$$

is defined as follows. For $x \in {}^{G}\mathbb{E}$, $y \in {}^{G}\mathbb{E}'$, the pairing $\langle x, y\rangle_{\mathrm{Sch}}$ is defined by

$$\langle x, y\rangle_{\mathrm{Sch}} = \sum_v \lambda_v(\bar{t}_v).$$

This method of defining a pairing is first used in [S] for the p-adic pairing.

LEMMA 4.14. — *Assume that G is cyclic of order ℓ. Suppose that $a = (x, (a_v)) \in A_S$, $b = (y, (b_v)) \in B_S$ such that a_v is a G_v-norm in A_v for all v and b_v is a G_v-norm in B_v for all v. Then we have*

$$\text{(a)}\qquad \langle x, y\rangle_{\mathrm{Sch}} = \langle a, b\rangle_G,$$

$$\text{(b)}\qquad \langle y, x\rangle_{\mathrm{Sch}} = \langle b, a\rangle'_G = \langle a, b\rangle_G.$$

Proof. — We prove formula (a), then (b) can be proved by a similar method. Recall the diagrams (29) and (30). Let $p \in {}_{\{a\}}P_S$ be a lifting of $a \times b \in \{a\} \times B_S$, and $t = \gamma_S(p)$. Locally, we have $t = \pi_v(p_v)$. The diagram (30) induces the following exact sequence:

$$0 \to K_v^*/N_{G_v}(L_w^*) \xrightarrow{\sim} {}_{\{a\}}P_v/N_{G_v}\big({}_{\{a\}}P_w\big) \longrightarrow \{a\} \times B_v/N_{G_v}(B_w).$$

Since b_v is a G_v-norm, we have

$$p_v \in K_v^* \cdot N_{G_v}\big({}_{\{a\}}P_w\big).$$

Let ψ_v be the local splitting described in 2.1. If $v \notin S_m$, then by Lemma 2.4, we get

$$\bar{t}_v \equiv \psi_v(p_v) \pmod{N_{G_v}(L_w^*)}.$$

This shows that p and t respectively contribute the same amount to $\langle a, b\rangle_G$ and $\langle x, y\rangle_{\mathrm{Sch}}$.

Suppose that $v \in S_m$. Then $B_v = K_v^*$ and the kernel of the map $\gamma_v : {}_{\{a_v\}}P_v \to {}_{\{x\}}\mathbb{P}(K_v)$ is generated by the element $\epsilon \in {}_{\{a_v\}}P_v$ such that

$$\gamma_v(\epsilon) = 0 \quad \text{and} \quad \pi_v(\epsilon) = a_v \times Q_v.$$

Since a_v is a G_v-norm, there is $a'_w \in L_w^*$ such that

$$N_{G_v}(a'_w) = a_v.$$

Let $\epsilon' \in P_w$ be such that

$$\gamma_w(\epsilon') = 0 \quad \text{and} \quad \pi_w(\epsilon') = a'_w \times Q_v.$$

Then as elements of $P_{w\{Q_v\}}$, we have

$$N_{G_v}(\epsilon') = \epsilon.$$

By Lemma 2.4, $\psi_v(\epsilon) \in N_{G_v}(L_w^*)$ and ψ_v induces a splitting,

$$\bar{\psi}_v : {}_{\{x\}}\mathbb{P}(K_v)/N_{G_v}\big({}_{\{x\}}\mathbb{P}(L_w)\big) \longrightarrow K_v^*/N_{G_v}(L_w^*).$$

Then by (65), we have

$$\bar{t}_v = \bar{\psi}_v(t) \equiv \psi_v(p_v) \pmod{N_{G_v}(L_w^*)}.$$

This shows that p_v and t respectively contribute the same amount to $\langle a, b\rangle_G$ and $\langle x, y\rangle_{\mathrm{Sch}}$. □

Definition 4.15. — *We define the* null space *of the Schneider pairing as*

$$\mathcal{N}S = \{x \in {}^{(G)}\mathbb{E} \mid \langle x, y\rangle_{\mathrm{Sch}} = 0 \text{ for all } y \in {}^{(G)}\mathbb{E}'\}.$$

Obviously, we have $\ell \cdot {}^{(G)}\mathbb{E} \subset \mathcal{N}S$. *We say that the Schneider pairing is* degenerate *if* $\mathcal{N}S \neq \ell \cdot {}^{(G)}\mathbb{E}$.

Lemma 4.16. — *Assume that G is cyclic of order ℓ, (ℓ, G) is good, D equals the the conductor of the extension L/K, and the cokernel of the map $\mathbb{E}(K) \to \prod_{v\in S-S_m} \mathbb{E}(k_v)$ has trivial ℓ-primary part. The pairing $\langle\cdot\,,\cdot\rangle_G$ is degenerate of the second kind, if and only if the pairing $\langle\cdot\,,\cdot\rangle_{\mathrm{Sch}}$ is degenerate.*

Suppose that $x \in \mathcal{N}S - \ell \cdot {}^{(G)}\mathbb{E}$. Then x is a G_v-norm for every v. We can find $a = (x, (a_v)_v) \in A_S$ such that for every v, a_v is a G_v-norm. Let $b = (y, (b_v)_v) \in B_S^1$. Then by Lemma 4.14,

$$\langle a, b\rangle_G = \langle x, y\rangle_{\mathrm{Sch}} = 0.$$

By Lemma 2.11, we can find $a' \in a + A_S^0$ such that $\langle a', b\rangle_G = 0$, for all $b \in B_S$. This implies that $\langle\cdot\,,\cdot\rangle_G$ is degenerate of the second kind.

Suppose that $a = (x, (a_v)_v)$ is an element of $\mathcal{N} - A_S^0 \cup \ell \cdot A_S$. Then by Lemma 2.11 and Lemma 4.11, $a \in B_S \otimes \mathbb{Z}_\ell$ and for every v, a_v is a G_v-norm in A_v. After multiplying a with an integer relatively prime to ℓ if necessary, we can assume that $a \in B_S$. Let y be an element of ${}^{(G)}\mathbb{E}' = {}^{(G)}\mathbb{E}$. If $y = \alpha(b) \in \alpha(B_S^1)$, then by Lemma 2.11 and Lemma 4.14,

$$\langle x, y\rangle_{\mathrm{Sch}} = \langle a, b\rangle_G = 0.$$

If $y = \ell \cdot y' \in \ell \cdot \mathbb{E}(K)$ and $\alpha(b') = y'$ for some $b' \in A_S$, then by Lemma 4.14,

$$\langle x, y\rangle_{\mathrm{Sch}} = \langle x, \ell \cdot y'\rangle_{\mathrm{Sch}} = \langle \ell \cdot b', a\rangle_G = 0.$$

By (63), $x \in \mathcal{N}S$. Since $a \notin A_S^0 \cup \ell \cdot A_S$, $x \notin l \cdot {}^{(G)}\mathbb{E}$ and the Schneider pairing is degenerate. □

It follows directly from the definitions that

$$\ell \cdot \mathbb{E}(K) \subset N_G(\mathbb{E}(L)) \subset \mathcal{N}S. \tag{66}$$

To prove Proposition 4.1, we need to study the group $\mathcal{N}S/N_G(\mathbb{E}(L))$. Let

$$\mathrm{res} : H^1(K, \mathbb{E}) \longrightarrow H^1(L, \mathbb{E})$$

be the restriction map of cohomology groups. Denote

$$\text{Ш}_{L/K} = \mathrm{res}(H^1(K, \mathbb{E})) \cap \text{Ш}_L^G.$$

LEMMA 4.17. — *Assume that G is cyclic of order ℓ and (ℓ, G) is good. We have*

$$\mathcal{NS}/N_G(\mathbb{E}(L)) \simeq \text{Ш}_L^G/\text{Ш}_{L/K}.$$

Proof. — Consider the diagram

$$\begin{array}{ccccccc} H^1(G,\mathbb{E}(L)) & \xrightarrow{\text{inf}} & H^1(K,\mathbb{E}) & \xrightarrow{\text{res}} & H^1(L,\mathbb{E})^G & \xrightarrow{d} & H^2(G,\mathbb{E}(L)) \\ \downarrow & & \downarrow & & \downarrow & & \\ \bigoplus_v H^1(G_v,\mathbb{E}(L_v)) & \xrightarrow{(\text{inf}_v)} & \bigoplus_v H^1(K_v,\mathbb{E}) & \xrightarrow{(\text{res}_v)} & \bigoplus_v H^1(L_v,\mathbb{E})^{G_v}. & & \end{array} \tag{67}$$

Here the rows are exact, the vertical arrows are the localization maps. For $\xi \in H^1(L,\mathbb{E})$, denote by $(\xi_v)_v$ its image in $\bigoplus_v H^1(L_v,\mathbb{E})$. Since G is cyclic, we indentify $H^2(G,\mathbb{E}(L))$ with $\mathbb{E}(K)/N_G(\mathbb{E}(L))$. Then an element $x \in \mathbb{E}(K)$ determines a class $\bar{x} \in H^2(G,\mathbb{E}(L))$.

Recall that $(\cdot\,,\cdot)_v$ is the local duality pairing. Using another definition of the Schneider pairing (see Proposition 3.1 of [Tn3]), for every $x \in {}^{(G)}\mathbb{E}$, we can find an ξ in $H^1(L,\mathbb{E})^G$ and an $(\eta_v)_v$ in $\bigoplus_v H^1(K_v,\mathbb{E})$ such that

$$d(\xi) = \bar{x}, \quad \text{res}_v(\eta_v) = \xi_v,$$

and

$$\langle x, y\rangle_{\text{Sch}} = \sum_v (y,\eta_v)_v, \ \text{ for all } \ y \in {}^{(G)}\mathbb{E}'.$$

The element ξ is unique up to elements of $\text{res}(H^1(K,\mathbb{E}))$, and for the chosen ξ, the element η_v is unique up to elements of $\text{inf}_v(H^1(G_v,\mathbb{E}(L_v)))$. The element x is in $\mathcal{NS}$ if and only if

$$\sum_v (y,\eta_v)_v = 0, \ \text{ for all } \ y \in {}^{(G)}\mathbb{E}'.$$

If $x \in \mathcal{NS}$, then from the above argument and the local duality, there is an element $(\eta_v')_v \in \bigoplus_v \text{inf}_v(H^1(G_v,\mathbb{E}(L_v)))$ such that for every $y \in \mathbb{E}'(K)$,

$$\sum_v (y,\eta_v')_v = \sum_v (y,\eta_v)_v.$$

By Theorem 4.4, there is an $\eta'' \in H^1(K,\mathbb{E})$ such that, for every v,

$$\eta_v'' = \eta_v - \eta_v'.$$

By replacing ξ by $\xi - \text{res}(\eta'')$, we see that when x is in $\mathcal{NS}$, the element ξ can be chosen as in Ш_L^G and vice versa. □

The following lemma is a consequence of Lemma 4.16, (66) and Lemma 4.17.

LEMMA 4.18. — *Suppose that* (ℓ, G) *is good,* D *equals the conductor of the extension* L/K*, and the cokernel of the map* $\mathbb{E}(K) \to \prod_{v \in S - S_m} \mathbb{E}(k_v)$ *has trivial* ℓ*-primary part. Then* $\langle\cdot,\cdot\rangle_G$ *is degenerate of the second kind if and only if*

$$|N_G(\mathbb{E}(L))/\ell \cdot \mathbb{E}(K)| \cdot |\text{Ш}_L^G/\text{Ш}_{L/K}| \equiv 0 \pmod{\ell}. \tag{68}$$

4.5. The Herbrand quotient computation.

In this section, we finish the proof of Proposition 4.1. We begin this section by reviewing some relevant results about the Herbrand quotient (see [AT] for details).

Let A be an abelian group and f an endomorphism of A. Denote by A_f and A^f the kernel and the image of f respectively. Also, let g be an endomorphism of A such that $g \circ f = f \circ g = 0$. Define

$$q(A) := q_{f,g}(A) := \frac{|A_f/A^g|}{|A_g/A^f|},$$

if both the denominator and the numerator are finite.

Let G be a cyclic group and A a G-module. Let $h_i(A)$ be the order of the cohomology group $H^i(G, A)$. Define the *Herbrand quotient*

$$h_{2/1}(A) = \frac{h_2(A)}{h_1(A)},$$

if both the denominator and the numerator are finite. If G is cyclic of order ℓ and A is a G-module such that $q_{0,\ell}(A)$ is defined, then (see [AT]) $q_{0,\ell}(A^G)$ and $h_{2/1}(A)$ are defined and

$$\left(h_{2/1}(A)\right)^{\ell-1} = \frac{q_{0,\ell}(A^G)^\ell}{q_{0,\ell}(A)}. \tag{69}$$

Taking $A = \mathbb{E}(L)$ in (69), we get

$$\left|H^1(G, \mathbb{E}(L))\right| \cdot \ell^{r_K} = \left|\mathbb{E}(K)/N_G(\mathbb{E}(L))\right| \cdot \ell^{(r_L - r_K)/(\ell-1)}. \tag{70}$$

Note that (70) implies that the number $(r_L - r_K)$ is divisible by $(\ell - 1)$.

We can now easily prove Proposition 4.1.

Proof of Proposition 4.1. — Since (ℓ, G) is good, ℓ is relatively prime to w and $|Ш_K|$. We have

$$|\mathbb{E}(K)/\ell \cdot \mathbb{E}(K)| = \ell^{r_K}. \tag{71}$$

Also, $Ш_L$ has non-trivial ℓ-primary part if and only if

$$|Ш_L^G| \equiv 0 \pmod{\ell}.$$

By the diagram (67), we see that there is a nontrivial G-type element of $H^1(K, \mathbb{E})$ (see 4.3) if and only if

$$|Ш_{L/K}| \cdot |H^1(G, \mathbb{E}(L))| \equiv 0 \pmod{\ell}.$$

As a consequence of Lemma 4.9, the pairing $\langle \cdot , \cdot \rangle_G$ is degenerate if and only if either it is degenerate of the first kind or it is degenerate of the second kind and the cokernel of the map $\mathbb{E}(K) \to \prod_{v \in S - S_m} \mathbb{E}(k_v)$ has trivial ℓ-primary part. By Lemma 4.3, Lemma 4.9, Lemma 4.18 and the above arguments we only need to show that

$$\ell^{(r_L - r_K)/(\ell-1)} \cdot |Ш_L^G| \equiv 0 \pmod{\ell}$$

if and only if

$$|Ш_L^G| \cdot |H^1(G, \mathbb{E}(L))| \cdot \left(\frac{\ell^{r_K}}{\mathbb{E}(K)/N_G(\mathbb{E}(L))} \right) \equiv 0 \pmod{\ell}.$$

But this is just a direct consequence of (70). $\square$

5. The valuation of the theta element.

We now prove the main theorems (Theorem 3.12 and Theorem 3.14). Let $z \in Z$ be such that $z\Theta_G \in \mathbb{Z}[G]$. We will study the valuation $o(\chi, z\Theta_G)$. The main result of this section is the following proposition, the proof will be postponed until 5.3. In 5.1, we will use this proposition to prove Theorem 3.12 and Theorem 3.14. Recall that G is always a quotient of the Weil group W_D.

Proposition 5.1. — *Assume that G is cyclic of order ℓ, D is the conductor of the abelian extension L/K, and χ is a nontrivial character of G. The following are true:*

(a) *If the Birch and Swinnerton-Dyer conjecture is true for $(\mathbb{E}, G)$, where $\ell \neq 2, 3$ and $r > 0$, then*

$$o(\chi, z\Theta_G) \geq e.$$

(b) *Assume that (ℓ, G) is good. Then $o(\chi, z\Theta_G) > e$ if and only if at least one of the following is true.*

(i) $r_L > r_K$.

(ii) $Ш_L$ *has non-trivial ℓ-primary part.*

5.1. The proof of the main theorems.

In this section, we complete the proof of Theorem 3.12 and Theorem 3.14.

Proof of Theorem 3.12 and Theorem 3.14. — By Lemma 3.15, it is sufficient to prove the theorems for the case where G is cyclic, D equals the conductor of L/K. Let χ_0 be the trivial character of G. Since $r > 0$, by Definition 1.8 and (46), we have

$$\chi_0(\Theta_G) = 0. \tag{72}$$

This and Proposition 5.1 show that for all $\chi \in \widehat{G}$,

$$o(\chi, \Theta_G) \geq e.$$

Since $z \cdot \Theta_G \in I$, Theorem 3.12 is then a consequence of Proposition 3.8.

Since $z \cdot \det_G \in I$, we have

$$o(\chi_0, z \cdot \det_G) > e. \tag{73}$$

Recall that $S = \mathrm{Supp}(D)$. Theorem 3.14 is a consequence of Proposition 3.8 , Proposition 4.1 and Proposition 5.1. □

5.2. The product formula.

As before, assume that G is cyclic of order ℓ. Suppose that ℓ is prime to 6. By Tate's algorithm [T5], for each non-archimedean place v of K and a place w of L sitting over v, if $\mathbb{E}$ has additive reduction at v, then it also has additive reduction at w. Because ℓ is prime to 2, if $\mathbb{E}$ has non-split multiplicative reduction at v, then the same is true of its reduction at w. By these and (2), we get the following product formula for the L-functions.

$$L_{\mathbb{E}/K}(s) = \prod_{\chi \in \widehat{G}} L_{\mathbb{E}/L}(\chi, s). \tag{74}$$

Suppose that D is the conductor of the abelian extension L/K and $\Theta_G \in \mathbb{Q}[G]$. As χ runs through all nontrivial characters of G, the values of $\chi(\Theta_G)$ are conjugate in the cyclotomic field $\mathbb{Q}[\zeta_l]$. By Definition 1.8, for a nontrivial character χ of G, we have

$$o(\chi, \Theta_G) = \frac{1}{\ell - 1} \cdot \prod_{\psi \in \widehat{G} - \{\mathrm{id}\}} o\big(\psi, \tau_\psi \cdot \Omega_\psi^{-1} \cdot |\mu_K| \cdot L(\psi, 1)\big). \tag{75}$$

By Lemma 1.7, we have

$$\prod_{\psi \in \widehat{G} - \{\mathrm{id}\}} \tau_\psi = \|D\|^{-\frac{1}{2}(\ell - 1)}. \tag{76}$$

Recall the relative discriminant $\Delta_{L/K}$ defined in (11). Since L/K has tame ramification at $v \in S - S_m$,

$$\left|\Delta_{L/K}\right| \not\equiv 0 \pmod{\ell}. \tag{77}$$

By (10) and (12), we have

$$\prod_{\psi \in \widehat{G} - \{\mathrm{id}\}} \Omega_\psi^{-1} = \frac{\Omega_K}{\Omega_L}. \tag{78}$$

For each $\gamma \in \mathbb{Q}^*$, denote by $\mathrm{ord}_\ell(\gamma)$ the ℓ-adic valuation, with the normalization that $\mathrm{ord}_\ell(\ell) = 1$. Then by (75), (76), (77) and (78), we obtain, for every nontrivial character χ of G,

$$o(\chi, \Theta_G) = \mathrm{ord}_\ell\Big(\|D\|^{-\frac{1}{2}(\ell-1)} \cdot |\mu_K|^{\ell - 1} \cdot \frac{\Omega_K}{\Omega_L} \cdot \lim_{s \to 1} \frac{L_{\mathbb{E}/L}(s)}{L_{\mathbb{E}/K}(s)}\Big). \tag{79}$$

Recall that if (ℓ, G) is good then the Birch and Swinnerton-Dyer conjecture is true for $(\mathbb{E}, G)$ (see 3.4). In this case, the Birch and Swinnerton-Dyer conjecture is true for $\mathbb{E}/L$ unless K is a function field.

LEMMA 5.2. — *Suppose that G is cyclic of order ℓ and (ℓ, G) is good.*

(a) *If either the Birch and Swinnerton-Dyer conjecture is not true for $\mathbb{E}/L$ or $r_L > r_K$, then*

$$\chi(\Theta_G) = 0.$$

(b) *If $r_L = r_K$ and the and Swinnerton-Dyer conjecture is true for both $\mathbb{E}/K$ and $\mathbb{E}/L$, then*

$$o(\chi, \Theta_G) = \mathrm{ord}_\ell \left\{ \|D\|^{-\frac{1}{2}(\ell-1)} \cdot \frac{|\mu_K|^\ell}{|\mu_L|} \cdot \left| \frac{\text{Ш}_L}{\text{Ш}_K} \right| \cdot \frac{R(\mathbb{E}_L)}{R(\mathbb{E}_K)} \cdot \frac{\prod_{w \text{ over } L} m_w}{\prod_{v \text{ over } K} m_v} \right\}. \tag{80}$$

If the Birch and Swinnerton-Dyer conjecture is not true for $\mathbb{E}/L$, then by Theorem 3.6, (74) and (75), $\chi(\Theta_G) = 0$. If the Birch and Swinnerton-Dyer conjecture is true for $\mathbb{E}/L$ and $r_L > r_K$, then (45), (74) and (75) imply that $\chi(\Theta_G) = 0$. This shows (a). The second statement is basically a consequence of (46) and (79). It remains to show that the order of $\mathbb{E}(L)_{\mathrm{tor}}$ is prime to ℓ. Since (ℓ, G) is good, ℓ is prime to

$$w = |\mathbb{E}(K)_{\mathrm{tor}}| = |\mathbb{E}(L)_{\mathrm{tor}}^G|. \qquad \square$$

5.3. The conductor and the discriminant.

In this section, we complete the proof of Proposition 5.1. First we consider the following formulae about the conductors and the discriminant.

Recall that d_K is the discriminant of the field K (see 1.2). Let $d_{L/K}$ be the relative discriminant of the extension L/K. We have (see [W1], Sect. 13.10, Thm. 9)

$$\|d_{L/K}\| = \prod_{\psi \in \widehat{G} - \{\mathrm{id}\}} \|D_\psi\| = \|D\|^{\ell-1}.$$

Also (see [W1], Sect. 8.4, Prop. 13 and 14),

$$|\mu_L| = |\mu_K|^\ell \cdot \|d_{L/K}\|^{-\frac{1}{2}}.$$

These imply that

$$\|D\|^{-\frac{1}{2}(\ell-1)} \cdot \frac{|\mu_K|^\ell}{|\mu_L|} = 1. \tag{81}$$

Proof of Proposition 5.1. — By Lemma 5.2, it is sufficient to prove the proposition for the case where $r_K = r_L$ and the Birch and Swinnerton-Dyer conjecture is true for both $\mathbb{E}/K$ and $\mathbb{E}/L$. Then we can use the formulae (80) and (81). In (80), we have

$$\frac{R(\mathbb{E}_L)}{R(\mathbb{E}_K)} = \ell^{r_K}. \tag{82}$$

For a fixed v, we have

$$\frac{\prod_{w \mid v} m_w}{m_v} \begin{cases} \in \mathbb{Z} & \text{if } v \notin S_m, \\ = \ell & \text{if } v \in S_m. \end{cases} \tag{83}$$

The first statement then follows. To show the second statement, we only note that since ℓ is prime 6, it is also prime to $\left(\prod_{w \mid v} m_w\right)/m_v$, for $v \notin S_m$. □

BIBLIOGRAPHY

[AT] E. ARTIN and J. TATE, Class Field Theory, Benjamin, New York, 1967.

[BS] Z. BOREVICH and I.R. SHAFAREVICH, Number Theorey, English translation, Academic Press, New York, 1966.

[D] P. DELIGNE, Les constants, etc., Séminaire Delange-Poisot-Poitou, 11^{e} année 19, 1970.

[G] B. GROSS, On the value of abelian L-functions at $s = 0$, J. Fac. Sci. Univ. Tokyo Sect. IA, Math., 35 (1988), 177–197.

[GSt] R. GREENBERG and G. STEVENS, p-adic L-functions and p-adic modular forms, Invent. Math., 111 (1993), 407–447.

[K] H. KISILEVSKY, Multiplicative independence in function fields, J. Number Theory, 44 (1993), 352–355.

[L] S. LANG, Algebraic Number Theory, Graduate Texts in Mathematics, Vol. 110, Springer-Verlag, New York, 1986.

[M] B. MAZUR, Letter to J. Tate, 1987.

[Ml1] J. MILNE, On a conjecture of Artin and Tate, Annals of Math., 102 (1975), 517–533.

[Ml2] J. MILNE, Arithmetic Duality Theorems, Academic Press, New York, 1986.

[Mu] D. MUMFORD, Biextensions of formal groups, in the Proceedings of the Bombay Colloquium on Algebraic Geometry, Tata Institute of Fundamental Research Studies in Mathematics 4, London, Oxford University Press, 1968.

[MT1] B. MAZUR and J. TATE, Canonical pairing via biextensions, in Arithmetic and Geometry, Progr. Math., Vol. 35 (1983), 195–237, Birkhäuser, Boston-Basel-Stuttgart.

[MT2] B. MAZUR and J. TATE, Refined conjectures of the Birch and Swinnerton-Dyer type, Duke Math. J., 54/2 (1987), 711–750.

[MTT] B. MAZUR, J. TATE and J. TEITELBAUM, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math., 84 (1986), 1–84.

[PV] I.B.S. PASSI and L.R. VERMANI, The associated graded ring of an integral group ring, Math. Proc. Camb. Phil. Soc., 82 (1977), 25–33.

[S] J. SILVERMAN, Arithmetic of Elliptic Curves, Graduate Texts in Math., Vol. 106, Springer-Verlag, New York, 1986.

[SGA7 I] A. GROTHENDIECK et al., Séminaire de géométrie algébrique du Bois Marie, 1967/69, Groupes de monodromie en géométrie algébrique, Lecture Notes in mathematics 288, Springer, Berlin-Heidelberg-New York, 1972.

[T1] J. TATE, Duality theorems in Galois cohomology over number fields, in Proc. Intern. Congress Math., Stockholm (1962), 231–241.

[T2] J. TATE, On the conjecture of Birch and Swinnerton-Dyer and a geometric analogue, Séminaire Bourbaki n° 306 (1966).

[T3] J. TATE, The arithmetic of elliptic curves, Invent. Math., 23 (1974), 179–206.

[T4] J. TATE, Letter to B. Mazur, 1988.

[T5] J. TATE, Algorithm for determining the type of a singular fiber in an elliptic pencil, Modular Functions of One Variable IV, Lecture Notes in Math. 476 (1975), p. 33–53, Springer-Verlag, Berlin-Heidelberg-New York.

[Tn1] K.-S. TAN, Refined conjectures of the Birch and Swinnerton-Dyer Type, Harvard University, Dept. of Mathematics, Ph. D. Thesis, 1990.

[Tn2] K.-S. TAN, Modular elements over function fields, Journal of Number Theory, 45 (1993, n° 3), 295–311.

[Tn3] K.-S. TAN, On the p-adic height pairings, AMS Proceedings on the p-adic Monodromy, to appear.

[Tn4] K.-S. TAN, On the special values of abelian L-function, submitted to J. Fac. Sci. Univ. Tokyo.

[W1] A. WEIL, Basic Number Theory, Grundl. Math. Wiss. Bd. 144, Springer–Verlag, New York, 1967.

[W2] A. WEIL, Adèles and Algebraic Groups, Birkhauser, Boston, 1982.

[Z] J.G. ZARHIN, Néron pairing and quasicharacters, Izv. Akad. Nauk. SSSR Ser. Mat. 36 (3), 497–509, 1972. (Math. USSR Izvestija, Vol. 6, No. 3, 491–503).

Manuscrit reçu le 30 mai 1994.

KI–SENG TAN,
Dept. of Mathematics
Columbia University
New York, NY 10027 (USA).

Current address:
Dept. of Math. and Computer Science
Rutgers University
Newark, NJ 07102 (USA).