Ki-Seng Tan

Refined theorems of the Birch and Swinnerton-Dyer type


<http://www.numdam.org/item?id=AIF_1995__45_2_317_0>
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 \( E \) 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], [Mil]), who establish the classical Birch and Swinnerton-Dyer conjecture in that context, subject only to the hypothesis that some \( \ell \)-primary component of the Shafarevitch-Tate group is finite (for any \( \ell \)).

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 \( \Theta_D \) is defined via the modular form associated to \( E \). 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 \( E \). 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.
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 $\Theta_{p^n}$, 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) $\Theta_D$ 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 $\text{III}$, $E(Q)_{\text{tor}}$, etc. The left-hand side is just the image of $\Theta_D$ 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 $r > \text{rk}(E(Q))$. 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 $\text{rk}(E(Q)) = 0$, see [GSt].

To generalize the conjecture to each elliptic curve $E/K$ 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 $\Theta_D$ 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 $\Theta_D$ 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 $\Theta_G$. 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 $\Theta_G$ 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 $(\ell, \ldots, \ell)$ for some prime number $\ell$ (the horizontal case). The reason for choosing this type of group is that the augmentation quotient $\mathcal{P}^G / \mathcal{P}^{G-1}$ ($\mathcal{I}$ 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 $z$th degree homogeneous polynomial functions on the space $G' = \text{Hom}_{\mathbb{F}_\ell}(G, \mathbb{F}_\ell)$. 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 $\ell$ 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 $E/K$, and in the number field case, it is also true for $E_{\ell'/K}$ 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 $\ell$ is outside a finite set of primes which depends only on $E/K$ (see Definition 3.13). Under these assumptions, we have $z \cdot \Theta_G \in I^e$ (Theorem 3.12) and the $e$th 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 $\mathbb{F}_p^*$ (Theorem 3.16). Theorem 3.21 says conjecture 2 is true, if $K$ is a function field with characteristic $\ell$, $\text{rk}(\mathcal{E}(K)) = 0$ 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 \( \mathbb{A} = \mathbb{A}_K, \mathbb{A}^* = \mathbb{A}_K^\times \) for the adèlle ring and the idèlle 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 \( S_\infty \) will denote the set of all archimedean places of \( K \).

An extended divisor is a formal sum

\[
D = \sum_v \alpha_v \cdot v, \quad \alpha_v \in \mathbb{Z},
\]

with the restriction that \( \text{ord}_v(D) = \alpha_v \) 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 \( D_\infty \) respectively. The support of \( D \), denoted \( \text{Supp}(D) \), is the set consisting of places \( v \) such that \( \text{ord}_v(D) \neq 0 \).

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

Assumption 1. — Each quasi-character \( \chi \) of the idèlle class group \( K^\times \setminus \mathbb{A}_K^\times \) is assumed to be trivial on the connected component of \( K_v^\times \) for each archimedean \( v \).
Thus for real $v$, the component $\chi_v$ 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 $\chi$ even or odd at $v$, respectively. For each finite $v$, use $\alpha_v(\chi) \cdot v$ to denote the conductor of the $v$-component $\chi_v$. From this we define the extended conductor of $\chi$ as the extended divisor

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

For a non-archimedean place $v \not\in \text{Supp}(D_\chi)$, the value $\chi_v(\pi_v)$ for a prime element $\pi_v$ of $\mathcal{O}_v$ is independent of the choice of $\pi_v$. 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

$$U_{D_0} = \prod_{v \not\in \text{Supp}(D_0)} \mathcal{O}_v^* \cdot \prod_{v \in \text{Supp}(D_0)} (1 + \pi_v^{\text{ord}_v(D)} \cdot \mathcal{O}_v),$$

$$U_{D_\infty} = \left( \prod_{v \not\in \text{Supp}(D_\infty)} K_v^* \right) \cdot \left( \prod_{v \in \text{Supp}(D_\infty)} \mathbb{R}_v^+ \right),$$

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 $v \not\in \text{Supp}(D)$ the prime element $\pi_v$ determines an element $[v] \in W_D$ called the Frobenius element. This is independent of the choice of $\pi_v$.

A quasi-character $\chi$ of the Weil group $W_D$ can be pulled back to a quasi-character (also denoted by $\chi$) 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 $\chi$ of $W_D$ is called primitive if $D_\chi = D$.

Let $R$ be a subring of $\mathbb{C}$. A quasi-character $\chi$ of $W_D$ can be extended uniquely to an $R$-algebra homomorphism from the group ring $R[W_D]$ to $\mathbb{C}$.
All the $\mathcal{R}$-algebra homomorphisms from $R[W_D]$ to $\mathbb{C}$ can be obtained in this way.

Let $E$ be an elliptic curve defined over $K$. For each non-archimedean place $v$, let $E/\mathcal{O}_v$ be the Néron model of $E_{\mathcal{O}_v}$ and let $E_{/k_v}$ be the special fibre of $E_{/\mathcal{O}_v}$ at $v$. Denote by $E_0_{/k_v}$, $E_0(K_v)$ the part of $E(K_v)$ whose reduction at $v$ is in $E_0_{/k_v}$, and $E_1(K_v)$ the part of $E_0(K_v)$ with trivial reduction. The number of $k_v$-rational components of $E_{/k_v}$ will be denoted by $m_v$. The arithmetic conductor of $E/K$ will be denoted by $N$.

For a real place $v$, let $m_v$ denote the number of components of $E(K_v)$ regarded as a topological group. Then $m_v$ is either 1 or 2. Denote the identity component of $E(K_v)$ by $E_0(K_v)$.

For a non-archimedean place $v$, let $\lambda_v$ be the integer defined by

$$\lambda_v = \begin{cases} 
1 + q_v - |E_0(k_v)| & \text{for good reduction,} \\
q_v - |E_0(k_v)| & \text{for bad reduction.}
\end{cases}$$

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

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

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

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

is defined as

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

If $\chi_0$ is the trivial character, we denote

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

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 $G_v = \text{Gal}(L_w/K_v)$. Sometimes we denote $L_w = L_v$ when the choice of $w$ is not important.
1.2. The global period.

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

Let $\mu = (\mu_v)$, where for each place $v$ of $K$, $\mu_v$ 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

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

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 $\omega$ on $E$. Then $\omega$ and $\mu_v$ determine a Haar measure $|\omega|_v \mu_v$ on the compact analytic group $E(K_v)$ in a well-known way (cf. [W2]).

For archimedean $v$, define the local period

\[
\Omega_v = \int_{E(K_v)} |\omega|_v \mu_v.
\]

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

\[
\Omega_v = \left| \frac{\omega}{\omega_{0,v}} \right|_v.
\]

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

\[ \Omega = \Omega_{E/K} = \Omega_K := \prod_v \Omega_v. \]  

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

Consider a Weierstrass equation of \( E \) over \( K \),

\[ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \]

and the differential \( \omega \) (see [T3]),

\[ \omega = dx/2y + a_1 x + a_3 = dy/3x^2 + 2a_2 x + a_4 - a_1 y. \]

Let \( \delta \) be the discriminant associated to this equation. For each non-archimedean place \( v \), choose a minimal Weierstrass equation and take the corresponding invariant differential \( \omega'_v \) in the similar way and let \( \delta_v \) be the discriminant of this equation.

Definition 1.2. — Define the global discriminant \( \Delta = \Delta_K \) by

\[ \Delta = \sum_{v \in S_{\infty}} \text{ord}_v(\delta_v) \cdot v. \]  

Since each \( \omega'_v \) can be extended to a Néron differential over \( O_v \), we have the following equality of divisors

\[ \Delta - 12 \cdot \sum_{v \in S_{\infty}} \text{ord}_v \left( \frac{\omega}{\omega'_0} \right) \cdot v = (\delta). \]  

Note that if \( K \) is a function field with constant field \( \mathbb{F}_q \), then \( \Omega \) is just the norm of \( \sum_{v \notin S_{\infty}} \text{ord}_v(\omega/\omega'_0) \cdot v \), so (8) and the multiplication formula together imply

\[ \Omega = q^{-\deg(\Delta)/12}. \]  

Let \( \chi \) be a character of the idèle class group and \( L/K \) the cyclic extension determined by \( \chi \). Let \( \text{Odd}_\chi \) be the set of real places where \( \chi \) is odd. For each \( v \in \text{Odd}_\chi \), let \( w \) be the unique complex place of \( L \) sitting over \( v \).
DEFINITION 1.3. — The relative global period $\Omega_{\chi}$ is defined as

$$\Omega_{\chi} = \prod_{v \in \text{Odd}_d} (-1)^{2/m_v} \cdot \frac{\int_{E(L_v)} |\omega| w \cdot \mu_w}{\int_{E(L_v)} |\omega| v \cdot \mu_v} \cdot \prod_{v \in \text{Odd}_d} \Omega_v.$$

The definition depends on $\chi$ and $E$. It is independent of the choice of $\omega$.

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

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

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

Notice that $\Delta_K$ 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 $\text{Gal}(L/K)$ with a character of the idèle class group of $K$. By the definitions of $\Omega$ and $\Omega_{\chi}$, the multiplication formula and (8), we have

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

1.3. The Gauss sum.

Let $\Psi$ be a non-trivial character of the additive group $K \setminus A_K$ and $\phi$ a differential idèle attached to $\Psi$ [W1]. The Gauss sum is now defined as follows.

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

$$\tau_{\chi, v} = \sum_{x \in \phi_v^{-1}\pi_v^{-\alpha_v}(O_v^* / 1 + \pi_v^{\alpha_v} O_v)} \Psi_v(x) \chi(x). \quad (13)$$

Otherwise, define

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

The Gauss sum is defined as

$$\tau_{\chi} = \prod_v \tau_{\chi, v}. \quad (15)$$

It is easy to see that the definition of $\tau_{\chi}$ is independent of the choice of $\Psi$, $\phi$ and $\pi_v$. 
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 $\chi$ of $W_{D+\infty} = (\mathbb{Z}/D)^*$, our Gauss sum $\tau_\chi$ equals $2\sqrt{-1}$ times the usual Gauss sum of $\chi^{-1}$. We define the Gauss sum so as to avoid the appearance of $\chi^{-1}$ 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

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

**Lemma 1.7.** — Let $\chi$ be a character and $\bar{\tau}_\chi$ be the complex conjugate of $\tau_\chi$ 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 $\chi$ 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 $\chi$ of $W_D$.

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

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

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

be the ring homomorphism induced by the projection. Also let

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

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 $\Theta_D$ is the unique element of $R[W_D]$ which satisfies the following properties:

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

(a) If $v \in \text{Supp}(N) \cup \text{Supp}(D)$ is non-archimedean, then

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

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

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

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

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

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

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

(e) If $v \notin \text{Supp}(D)$ 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 $\chi$ of $W_D$, we have

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

where $\Omega_\chi$ and $\tau_\chi$ are the relative global period and the Gauss sum.

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

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

Since the group ring $\mathbb{C}[W_D]$ is reduced, by (19) $\Theta_D$ 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 $E$ 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 $E$ such that $\Theta_D$ is in $\mathbb{Z}[M^{-1}][W_D]$. If $K$ is a function
field of characteristic $p$ and $E$ 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 $\Theta_D$ always exists inside $\mathbb{Z}[p^{-1}][W_D]$, and the denominators of the
coefficients of $\Theta_D$ are bounded for all admissible $D$. In particular, when $K$
is a rational function field and $E$ is semi-stable, the denominators of the
coefficients are all bounded by

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

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
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 $E'/K$ denote the dual elliptic curve of $E/K$ and $P/K$ the canonical
biextension (see [Mu], [SGA7 I]), associated to the duality, of $E/K$ and $E'/K$
by $\mathbb{G}_m$. We can identify $E'/K$ with $E_K$. 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 $P(K_v)$ is a triple $(\alpha_v, \beta_v, \rho_v)$ of morphisms:

$$\begin{cases}
\alpha_v : A_v \rightarrow E(K_v), \\
\beta_v : B_v \rightarrow E'(K_v), \\
\rho_v : K^*_v \rightarrow C_v.
\end{cases}$$
Let $P_v := (\alpha_v^*, \beta_v^*)P(K_v)$ be the biextension obtained from $P(K_v)$ by pullback via homomorphisms $\alpha_v$ and $\beta_v$.

**Definition 2.2.** — A local trivialization, $(\alpha_v, \beta_v, \rho_v, \psi_v)$, of $P(K_v)$ consists of a local modification $(\alpha_v, \beta_v, \rho_v)$ and a local splitting $\psi_v$, 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 $\psi_v$ 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 $E$ inside $S$.

**Example:** five important local trivializations.

(L1) The trivial trivialization, for $v$ archimedean and not in $S$. Here $A_v = E(K_v)$, $B_v = E'(K_v)$, $C_v = \{1\}$, $\alpha_v, \beta_v, \rho_v$ are the obvious homomorphisms and $\psi_v$ is the trivial mapping.

(L2) The real ramified trivialization, for $v$ real and in $S$. Here $A_v = E_0(K_v)$, $B_v = E_0'(K_v)$, $C_v = \mathbb{R}^*/\mathbb{R}_+^* \simeq \mp 1$, $\alpha_v, \beta_v, \rho_v$ are the obvious homomorphisms, and $\psi_v$ is the unique continuous splitting.

(L3) The Néron unramified trivialization, for $v$ non-archimedean and not in $S$. Here $A_v = E(K_v)$, $B_v = E_0(K_v)$, $C_v = K_v^*/\mathcal{O}_v^* \simeq \mathbb{Z}$, $\alpha_v, \beta_v, \rho_v$ are the obvious homomorphisms, and $\psi_v$ 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 $A_v = E(K_v)$, $B_v = E_0'(K_v)$, $C_v = K_v^*/(1 + \pi_v \cdot \mathcal{O}_v)$, $\alpha_v, \beta_v, \rho_v$ are the obvious homomorphisms, and $\psi_v$ 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 $E_{/K_v}$. The Tate parametrization gives exact sequences (of rigid analytic groups)
Here $A_v = B_v = C_v = K_v^*$, $\alpha_v, \beta_v, \rho_v$ are the obvious homomorphisms, and $\psi_v$ is the unique analytic splitting.

Remarks.

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

$$0 \to C_v \to \{a\}(\rho_\ast P_v) \to \{a\} \times B_v \to 0.$$  

These splittings of group extensions for all $a \in A_v$ also determine the splitting $\psi_v$. It is true that in any of the cases (L1)–(L5), the group $\text{Hom}(B_v, \text{Hom}(B_v, C_v))$ (for either topological groups or rigid analytic groups) is trivial. Therefore the local splitting $\psi_v$ 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 $E'$ with $E$, 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 $\psi_v$). 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 (L$i$) 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
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 $K_v^* \cdot A_v \cdot B_v \cdot \{a_v\} P_w \cdot P_w\{b_v\}$ 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 $\pm 1$. 

### 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 $i_v : E(K) \to E(K_v)$ 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,

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

(22)

Thus, a point $a \in A_S$ is described by a point $x \in \mathcal{E}(K)$ 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 $\beta$) associated to $\{B_v\}_v$. Then $A_S$ and $B_S$ fit into the exact sequences

$$
0 \to \prod_{v \in S_m} \langle Q_v \rangle \to A_S \to \mathcal{E}(K) \to 0,
$$

and

$$
0 \to \prod_{v \in S_m} \langle Q_v \rangle \to B_S \xrightarrow{\beta} \mathcal{E}(K) \to 0.
$$

(23)

(24)

Let

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

and define

$$
C_S = K^* \setminus A_K^*/U_S.
$$

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

$$
\begin{array}{ccc}
0 & \to & K^* \\
\| & & \downarrow \pi_s \\
0 & \to & P(S) \xrightarrow{\pi_s} A_S \times B_S \xrightarrow{\alpha \times \beta} 0
\end{array}
$$

(25)

$$
\begin{array}{ccc}
0 & \to & K^* \\
\| & & \downarrow f \\
0 & \to & \mathbb{P}(K) \xrightarrow{f} \mathcal{E}(K) \times \mathcal{E}'(K) \to 0.
\end{array}
$$
The injection $i = (i_v)$ (see [MI], p.111) and the map $\prod_v \psi_v$ induce

\begin{equation}
\Psi : P_S \to \prod_v P_v \overset{\prod_v \psi_v}{\longrightarrow} \prod_v C_v \to C_S.
\end{equation}

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 $\Psi(K^*) = 0 \subset C_S$, 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 $E$, 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

$$K_v^* \to A_K^* \to C_S.$$ 

Then we have (see [MT2])

\begin{equation}
\langle [Q_{v_0}], [Q_{v_0}]' \rangle_s = \overline{Q}_{v_0}.
\end{equation}

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

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

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

Denote by $\langle \cdot, \cdot \rangle$ the Néron-Tate pairing. If $K$ is a function field with $q$ equal to the order of the constant field, then $\langle \cdot, \cdot \rangle$ 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

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

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 $a = (a^v, (a^v)^v) \in A_S$, $b = (b^v, (b^v)^v) \in B_S$ and $v_0 \in S_m$. Then the following are true:

(a) The pairings $\langle a, [Q_{v_0}]_S \rangle_S$ 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 $\langle a, [Q_{v_0}]_S \rangle_G = 0$ (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

$$
\begin{array}{cccccccc}
0 & \rightarrow & K^* & \rightarrow & \{a\} P_S & \stackrel{\pi_S}{\rightarrow} & \{a\} \times B_S & \rightarrow & 0 \\
\| & & \downarrow{\gamma_S} & & \downarrow{\alpha \times \beta} & & & & \\
0 & \rightarrow & K^* & \stackrel{f}{\rightarrow} & \{x\} P(K) & \rightarrow & \{x\} \times E'(K) & \rightarrow & 0.
\end{array}
$$

The formula (27) can be generalized in the following way.
Locally at each \( v \), we have

\[
\begin{array}{c}
0 \rightarrow K_v^* \rightarrow \{a_v\}P_v \xrightarrow{\pi_v} \{a_v\} \times B_v \rightarrow 0 \\
0 \rightarrow K_v^* \rightarrow \{x\}P(K_v) \xrightarrow{f_v} \{x\} \times \mathbb{E}'(K_v) \rightarrow 0.
\end{array}
\] 

(30)

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

\[
\begin{array}{c}
K_v^*/N_{G_v}(L_w^*) \rightarrow \{a_v\}P_v/N_{G_v}\{a_v\}P_w \\
H^1(G_v, \{x\} \times \mathbb{E}'(L_w)) \xrightarrow{\partial} K_v^*/N_{G_v}(L_w^*) \rightarrow \{x\}P(K_v)/N_{G_v}\{x\}P(K_w).
\end{array}
\]

(31)

Recall that there is a local duality pairing (see [M12], p. 53, p. 354 and [T1]), which is a perfect pairing

\[
(\cdot, \cdot)_v : \mathbb{E}(K_v) \times H^1(K_v, \mathbb{E}) \rightarrow \mathbb{Q}/\mathbb{Z}.
\]

(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 \( x \in \mathbb{E}(K_v) \), \( \xi \in H^1(G_v, \mathbb{E}'(L_w)) \) and \((x, \xi)_v \in \mathbb{Q}/\mathbb{Z}\) is the value of the local duality pairing. Let \( \partial \) be the map in (31). Then \((x, \xi)_v\) equals the image of \( \xi \) under the following composition of maps

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

**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 $\{x\} \times E'(K)$, there is a unique $p \in \{x\} P_S$ such that,

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

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

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

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

$$
\begin{array}{cccccc}
0 & \longrightarrow & K^*_{v_0} & \longrightarrow & P_{v_0}(Q_{v_0}) & \longrightarrow & A_v \times \{Q_{v_0}\} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \gamma_{v_0} & & \downarrow \alpha_{v_0} \times \beta_{v_0} & \\
0 & \longrightarrow & K^*_{v_0} & \longrightarrow & \mathbb{P}(K_{v_0})_{\{0\}} & \longrightarrow & E(K_{v_0}) \times \{0\} & \longrightarrow & 0.
\end{array}
$$

Note that we can identify $\mathbb{P}(K_{v_0})_{\{0\}}$ with $E(K_{v_0}) \times K^*_{v_0}$. The element $x \times 1 \in \mathbb{P}(K_{v_0})_{\{0\}}$ is also in $\{x\} P(K)$. Using the expressions in terms of zero cycles and divisors, we can show directly that $x \times 1$ is the identity of the group $\{x\} P(K)$. 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 $P(L_{w_0})_{\{0\}}$ with $E(L_{w_0}) \times L^*_{w_0}$. Suppose that $a_{v_0} = NG_{v_0}(a_{w_0})$ 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 $p_{v_0} = NG_{v_0}(p_{w_0})$. By Lemma 2.4, $\psi_{v_0}(p_{v_0})$ is a $G_{v_0}$-norm and $\langle a, [Q_{v_0}] \rangle_S = 0$. 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}/NG_{v_0}(\{a_{v_0}\}P_{w_0})$. Then $\bar{p}_{v_0}$ generates the kernel of the map $\gamma_{v_0}$. By Lemma 2.4, the local splitting $\psi_{v_0}$ induces

$$\bar{\psi}_{v_0} : \{a_{v_0}\}P_{v_0}/NG_{v_0}(\{a_{v_0}\}P_{w_0}) \rightarrow K_{v_0}^*/NG_{v_0}(L_{w_0}^*).$$

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

$$\bar{\eta}_{v_0} : \{x\}P(K_{v_0})/NG_{v_0}(\{x\}P(K_{w_0})) \rightarrow K_{v_0}^*/NG_{v_0}(L_{w_0}^*)$$

such that $j \circ \bar{\eta}_{v_0}$ is the identity map. It then follows that the map $\partial$ 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 $a'_{v_0} \in NG_{v_0}(A_{w_0})$ 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 $E(K)_{tor}$.

**DEFINITION 2.13.** — Denote

$$r_K = \text{rk}(E(K)),$$

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

$$w = |E(K)_{tor}|.$$
Define the discriminant of the $S$-pairing as

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

If $(a'_i)$ and $(b'_j)$ are another pair of compatible bases, then the induced determinant $\det_{1 \leq i, j \leq r} ((a'_i, b'_j)_S)$ differs from that induced from $(a_i)$ and $(b_j)$ by at most an element of $\text{Sym}_r(C_S)$, 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

$$Z_{T,S} : \mathbb{Z}\left[\frac{1}{w}\right] \otimes \text{Sym}_n(C_S) \to \mathbb{Z}\left[\frac{1}{w}\right] \otimes \text{Sym}_n(C_T).$$

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

$$U_{S,T} : \mathbb{Z}\left[\frac{1}{w}\right] \otimes \text{Sym}_n(C_T) \to \mathbb{Z}\left[\frac{1}{w}\right] \otimes \text{Sym}_n(C_S)$$

such that for all $c_i \in C_S$,

$$U_{S,T} \circ Z_{T,S}(c_1 \otimes c_2 \otimes \cdots \otimes c_n) = 2^{|S_{\infty} \cap (S-T)|} \prod_{v \in S-T-S_{\infty}} (q_v - 1) \cdot c_1 \otimes c_2 \otimes \cdots \otimes c_n.$$

**Definition 2.14.** — Denote

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

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

$$D_S = D_S(E) := \sum_{S_m \subseteq T \subseteq S} (-1)^{(T-S_m)} U_{S,T}(j_T \text{ disc}_T) \in \mathbb{Z}\left[\frac{1}{w}\right] \otimes \text{Sym}_r(C_S).$$

Then $D_S$ is corrected in the sense that when $S$ varies, the $D_S$ 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

\begin{equation}
(37) \quad r' = \begin{cases} 
  r & \text{if } v \text{ is not split multiplicative for } E, \\
  r + 1 & \text{if } v \text{ is split multiplicative for } E.
\end{cases}
\end{equation}

Suppose that $v$ is a non-archimedean place of $K$. Let $n_v = \#(E_0(k_v))$. If $v$ is not a split multiplicative place of $E$, then (see [MT2])

\begin{equation}
(38) \quad Z_{S,S'}(D_{S'}) = (q_v - 1 - n_v) \cdot D_S.
\end{equation}

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

\[ B_{S_m \cup \{v\}} \to (E'/E'_0)(k_v). \]

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

\begin{equation}
(39) \quad c(S_m, v) \cdot Z_{S,S'}(D_{S'}) = Q_v \cdot D_S \in \mathbb{Z}\left[\frac{1}{w}\right] \otimes \text{Sym}_r(C_S).
\end{equation}

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

\begin{equation}
(40) \quad Z_{S,S'}(D_{S'}) = (-1)^{2/m_v} \cdot m_v \cdot D_S \in R \otimes \text{Sym}_r(C_S).
\end{equation}

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 $E$ is a Weil curve over $\mathbb{Q}$ or $E$ is defined over a function field.

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

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

\[ S = \text{Supp}(D). \]

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

\[ W_D \xrightarrow{\text{pr}_D} G, \quad \text{pr}_S : C_S \longrightarrow W_D \xrightarrow{\text{pr}_D} G. \]

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

\[ \Theta_G = \text{pr}_D(\Theta_D), \]

and the corrected discriminant as

\[ D_G = \text{pr}_S(D_S). \]

**Assumption 4.** — There is a positive integer \( M \) such that \( \Theta_G \) 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 \( E(K)_{\text{tor}} \). Under Assumption 4, we have

\[ D_G \in \mathbb{Z}
\left[\frac{1}{M}\right] \otimes \text{Sym}_r(G). \]

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

\[ \begin{cases} G \longrightarrow I/I^2 \\ g \mapsto 1 - g \end{cases} \]

can be extended to a homomorphism of graded algebras

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

We denote

\[ \det_G = d(D_G) \in I^r/I^{r+1}. \]
**Definition 3.3.** — Let \( \text{ord}(\Theta_G) \) be the maximal \( n \) such that \( \Theta_G \in I^n \). If \( \text{ord}(\Theta_G) \geq n \), we denote by \( \Theta_G^{(n)} \) the image of \( \Theta_G \) under the quotient map \( I^n \to I^n/I^{n+1} \).

**Definition 3.4.** — Define

\[
\phi_S = \phi_{S_m} = \left| \text{coker} \left\{ E'(K) \to \prod_{v \notin S_m \cup S_{\infty}} E'/E'_0(k_v) \right\} \right|.
\]

Let \( III_K \) be the Shafarevich-Tate group of \( E/K \).

The Mazur-Tate conjecture is the following:

**Conjecture 1** (see [MT2]). — We have \( \text{ord}(\Theta_G) \geq r \), \( III_K \) finite, and

\[
\theta_G^{(r)} = |III_K| \cdot \phi_S \cdot \det_G.
\]

Note that \( \Theta_G \) 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 \( \omega \), a place \( v \) is said to be **bad** if either it is archimedean or \( \text{ord}_v(\omega/\omega_0, v) \neq 0 \). Let \( S \) be a finite set of places containing all the bad places for \( \omega \) and all the places where \( E \) has bad reduction. For such an \( S \) there is an associated \( L \)-function \( L_S^*(s) \) (see [T2]). Let \( R(E/K) \) 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 $\Sha(K)$ is finite, and at $s = 1$, the associated $L$-series $L^*_S(s)$ has order of vanishing equal to $r_K$. Furthermore, we have

\[
\lim_{s \to 1} \frac{L_S^*(s)}{(s-1)^{r_K}} = \frac{|\Sha(K)| \cdot R(E/K)}{w^2}
\]

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

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

It follows that formula (45) is equivalent to

\[
\lim_{s \to 1} \frac{L(s)}{(s-1)^{r_K}} = \frac{|\Sha(K)| \cdot R(E/K) \cdot \prod_v m_v}{w^2} \Omega \cdot |\mu|^{-1}.
\]

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

Theorem 3.6 (see [T2], [Mil]). — 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 $\ell$-primary part of the Shafarevich-Tate group is finite for some prime number $\ell$.
   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 $\chi_0$ is the trivial character of $A_K^*$, 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 \(A_K^n\). Let \(\chi_s\) denote the quasi-character of \(W_D\) which sends each element \(x \in W_D\) to \(\|x\|^s\). Then \(\chi_s\) induces a ring isomorphism

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

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

\[
\Omega^{-1} \cdot |\mu| \cdot L(s + 1) \pmod{(1 - q^{-s})^{r\kappa+1}} .
\]

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

\[
|\Pi_K| \cdot \phi_s \cdot w^{-2} \cdot [E'(K) : B_S] \cdot \frac{R(E/K)}{\log(q) \kappa} (1 - q^{-s})^{r\kappa} \pmod{(1 - q^{-s})^{r\kappa+1}} .
\]

Directly from Definition 3.4, we have \([E'(K) : B_S] = \prod_v m_v\). 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 \(\Theta_G\) 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 \(z \cdot \mathcal{D}_G \in \text{Sym}_n(G)\), 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 \((\ell, \ldots, \ell)\)-type for some fixed prime \(\ell\). 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

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

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

$$(47) \quad d : \bigoplus_n \text{Sym}_n(G) \rightarrow \text{gr}(\mathbb{Z}[G]).$$

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

$$d_{(x)} : \mathbb{F}_\ell[t] \rightarrow \text{gr}(\mathbb{Z}[G]).$$

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

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

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

Consider the dual space of $G$,

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

Via the isomorphism

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

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

$$\tilde{f}(\chi) = \zeta^{f(g)}.$$ 

**Definition 3.7.** — For an element $\Theta \in \mathbb{Z}[G]$, denote by $\text{ord}(\Theta)$ the maximal $n$ such that $\Theta \in I^n$. Also, denote by $o(\chi, \Theta) = \text{ord}_{(1-\zeta)}(\chi(\Theta))$ the valuation of the element $\chi(\Theta)$ at the prime ideal $(1 - \zeta)$ of the Dedekind domain $\mathbb{Z}[\zeta]$. 
If \( \text{ord}(\Theta) \geq n \), then we have \( o(\chi, \Theta) \geq n \) for every \( \chi \in \hat{G} \). Therefore \( \chi \) 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 \( \chi \). 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 \( f \in \mathbb{Z}[t] \) is a homogeneous polynomial of degree \( n \). Let

\[
\theta = d(\zeta)(f) \in I^n/I^{n+1}.
\]

Then \( \theta \) is the image of \( f(1 - x_1, \ldots, 1 - x_k) \) under the quotient \( I^n \to I^n/I^{n+1} \). 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

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

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

(a) \( \theta \) is trivial in \( I^n/I^{n+1} \),

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

(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 $\tilde{f}_1 = 0$. By the induction hypothesis, we have $f_1 \in J$. Since $\tilde{t}_1 \cdot \tilde{f}_2 = 0$, we have

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

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

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

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

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

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

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

and consequently,

$$(1 - x_i)^\ell \cdot (1 - x_j) \equiv \ell \cdot (1 - x_i) \cdot (1 - x_j) \pmod{I^{\ell+2}}$$

and

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

Therefore, if $f \in J$, then $\theta$ is trivial. $\square$

By (50), if $\Theta \in I^n$ and $n > 0$, then $\ell \cdot \Theta \in I^{n+\ell-1}$. This multiplication by $\ell$ 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 $\ell$, then the multiplication by $z$ induces an isomorphism $I^n/I^{n+1} \sim I^n/I^{n+1}$.  

Proof. — Let $\theta \in I^n/I^{n+1}$, and $f, g \in \mathbb{Z}[\ell]$ homogeneous of degree $n$, $n + \ell - 1$ such that $d(z)f = \theta$ and $d(z)g = \ell(\theta)$. 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 $\mathbb{Z}_\ell$. $\Box$

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 until Section 5. As in 3.3, we continue to assume that $G$ is of the $(\ell, \ldots, \ell)$-type for a fixed $\ell$. 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 $z \cdot D_G \in \text{Sym}_r(G)$. As before, if $z\Theta$ is in $I^n$, then we denote by $(z\Theta_G)^{\langle n \rangle}$ its image in $I^n/I^{n+1}$. Also denote

$$z \text{det}_G = d(z \cdot D_G) \quad \text{and} \quad e = (\ell - 1) \cdot \text{ord}_\ell(z) + r.$$ 

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 $\text{ord}(z\Theta_G) \geq e$ and

$$(z\Theta_G)^{\langle e \rangle} = |\Pi_K| \cdot \phi_S \cdot z \text{det}_G.$$ 

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

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 \((E, G)\) and \( r > 0 \), then we have \( z\Theta_G \in I^e \).

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

\[
(52) \quad d(\mathbb{F}) \left( \bar{f}_1 \right) = \left( z\Theta_G \right)^{(e)}
\]

and

\[
(53) \quad d(\mathbb{F}) \left( \bar{f}_2 \right) = |\Pi_K| \cdot \phi_S \cdot z\det G.
\]

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

Conjecture 2'. — We have:

\[
(54) \quad \bar{f}_1 = \bar{f}_2.
\]

Definition 3.13. — The pair \((\ell, G)\) will be called good, if the Birch and Swinnerton-Dyer conjecture is true for \((E, G)\) and

\[
(55) \quad 6 \cdot w \cdot |\Pi_K| \cdot \prod_{v \notin S_{\infty}} m_v \neq 0 \pmod{\ell}.
\]

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

Theorem 3.14. — Suppose that \( r > 0 \) and \((\ell, G)\) 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 \( (\ell,G) \) 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 \( d_{(\pm)} \) defined in 3.3. For an element \( y \in G \), let \( f_y \in \mathbb{F}_\ell[\ell] \) be the unique linear polynomial such that \( d_{(\pm)}(f_y) = d(y) \).

**Definition 3.17.** — A homogeneous \( f \in \mathbb{F}_\ell[\ell] \) 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 \( h_1, h_2 \in \mathbb{F}_\ell[\ell] \) are \( e \)-th degree homogeneous polynomials and \( h_2 \) is special. If \( h_1 \) and \( h_2 \) have the same zero set, then there exists a \( c \in \mathbb{F}_\ell^* \) such that \( h_1 = c \cdot h_2 \).

**Proof.** — Suppose that \( h_2 = \prod_{i=1}^{e} f_{y_i} \) and \( (t) = (t_1, t_2, \ldots, t_k) \). 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, \( h'(t) \), such that

\[
h_1(t) = h_1(0, t_2, \ldots, t_k) + t_1 \cdot h'_1(t).
\]

Since \( h_1 \) and \( h_2 \) have the same zero set and \( h_2(0, t_2, \ldots, t_k) = 0 \), we see that \( h_1(0, t_2, \ldots, t_k) = 0 \) and \( h_1 = \tilde{t}_1 \cdot \tilde{h}'_1 \). 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

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

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 $h$ and $f_{y^e}$ 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 $h$ must equal to that of $\tilde{t}_1$ and both $\tilde{h}_1$ and $\tilde{h}_2$ are proportional to $\tilde{t}_1^2$.

When $S = S_m$, $r_K = 0$ and $(\ell, G)$ 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 $Q_{v_i}$ (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 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 $m_{v_i} = \text{ord}_v(Q_{v_i})$, $a_i$ must be divisible by $p$.

**Theorem 3.21.** — Suppose that $r > 0$, $(\ell, G)$ 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 $(\ell, G)$ is still good. Then by the first statement, there is a $c \in \mathbb{F}_\ell^*$ such that

\[ (*) \quad \bar{f}_1 = c \cdot \bar{f}_2. \]

We need to show that $c = 1$. By Lemma 3.20 again, we can assume that the constant field extension of degree $\ell$ 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 $E/K$) 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 $|\Pi K|$ and $\phi_S$ are prime to $\ell$, and $y_i \neq 1 \in G$ for $i = 1, \ldots, r$. Since $\bar{f}_2 = |\Pi K| \cdot \phi_S \cdot \left( \prod_{i=1}^{r} \bar{f}_{y_i} \right)$, it is nontrivial.

\[ \square \]

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 $\chi \in \hat{G}$ 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 \( o(\chi, |\mathbb{II}| \cdot \phi_S \cdot z\text{det}_G) \) is greater than \( e \). Since the result for the trivial character is obvious, we can assume that \( \chi \) is nontrivial. As in Section 3, \( \ell \) 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 \( \ell \), \((\ell, G)\) is good, \( D \) is the conductor of the abelian extension \( L/K \), and \( \chi \) 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

\[
\begin{align*}
    r_K &= \text{rk}(E(K)), \\
    r_L &= \text{rk}(E(L)), \\
    r^L &= r^E(L).
\end{align*}
\]

We also denote

\[
\begin{align*}
    r_K &= \text{rk}(E(K)), \\
    r_L &= \text{rk}(E(L)).
\end{align*}
\]

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

(a) \( r_L > r_K \); \\
(b) \( \mathbb{II}_L \) has non-trivial \( \ell \)-primary part.

**4.1. The valuation of the discriminant.**

The pairing \( \langle \cdot, \cdot \rangle_G \) induces a pairing

\[
\langle \cdot, \cdot \rangle_{G, F_\ell} : A_S \otimes F_\ell \times B_S \otimes F_\ell \to G.
\]

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

\[
\text{disc}_{G, F_\ell} \in \text{Sym}_r G.
\]

Let \( \text{pr}_S \) be the projection \( G_S \to G \) and \( \text{disc}_S \) the discriminant defined in 2.3. Then \( \text{pr}_S(\text{disc}_S) \) and \( \text{disc}_{G, F_\ell} \) differ at most by a constant in \( F_\ell^* \).

The pairing \( \langle \cdot, \cdot \rangle_{G, F_\ell} \) is degenerate if and only if the discriminant \( \text{disc}_{G, F_\ell} \) 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, \( (\ell, G) \) is good, and \( \chi \) is a nontrivial character of \( G \). Then \( o(\chi, |\text{III}| \cdot \phi_S \cdot z\det_G) > e \) if and only if at least one of the following is true:

(a) We have

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

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

Proof. — By (43) and (55), the numbers \( |\text{III}| \) and \( \phi_S \) are relatively prime to \( \ell \). By Lemma 3.9, we see that

\[
o(\chi, |\text{III}| \cdot \phi_S \cdot z\det_G) = o(\chi, \det_G) - r + e.
\]

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

\[
\chi(U_{S,T}(c)) = 1 \quad \text{for all} \quad c \in C_T.
\]

Therefore

\[
o(\chi, \det_G) = o(\chi, j_S \cdot d \circ \text{pr}_S(\text{disc}_G)).
\]

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

\[
d \circ \text{pr}_S(\text{disc}_G) = 0.
\]

This will follow from the facts that \( \text{pr}_S(\text{disc}_G) \) is proportional to \( \text{disc}_{G, \mathbb{F}_\ell} \) and \( d \) is an isomorphism for \( G \cong \mathbb{F}_\ell \). \( \square \)
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 [M12].

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

Let $\lambda_0$ and $\lambda_1$ be the localization maps:

$$
\lambda_0 : E(K, \ell) \to \prod_v E(K_v, \ell),
$$

$$
\lambda_1 : H^1(K, E, \ell) \to \bigoplus_v H^1(K_v, E, \ell).
$$

These and the above identifications induce the following sequence:

$$
H^1(K, E, \ell) \xrightarrow{\lambda_1} \bigoplus_v H^1(K_v, E, \ell) \xrightarrow{\lambda_5} E(K, \ell)^*.
$$

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

**Theorem 4.4** (Global Duality, [T1], [M12]). — If the $\ell$-primary part of $\mathfrak{I}$ 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 $A^0_S$ be the kernel of the natural morphism,

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

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

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

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

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

It is degenerate of the second kind, if

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

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 $H^1(K, E)$ is called of $G$-type if its image under the localization map $H^1(K, E) \rightarrow \bigoplus_v H^1(K_v, E)$ is contained in $\bigoplus_v H^1(G_v, E(L_v))$.

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

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

has nontrivial cokernel.

The natural maps

$$\bigoplus H^1(G_v, E(L_v)) \rightarrow \bigoplus H^1(K_v, E),$$

$$\prod_v E(K_v) \rightarrow \prod_v (K_v)/N_{G_v}(L_v)$$
and the local duality pairing induce a perfect pairing

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

The natural morphism

\[ E(K) \longrightarrow \prod_v E(K_v) \longrightarrow \prod_v E(K_v)/N_{G_v}(L_v) \]

has nontrivial cokernel if and only if the natural morphism

\[ \bigoplus H^1(G_v, E(L_v)) \longrightarrow \bigoplus H^1(K_v, E) \overset{\lambda^*_G}{\longrightarrow} E(K, \ell)^* \]

has nontrivial kernel. Here \( \lambda^*_G \) is the map defined in 4.2. The lemma is then a consequence of Theorem 4.4.

Denote \( E(G_v) = E(K_v)/\sigma_{G_v}(E(L_v)). \)

Since \((\ell, G)\) is good, by (55) and Lang’s theorem (see [T1]), \( E(G_v) \) is trivial for \( v \not\in S \). For \( v \in S - S_m \), the extension \( L/K \) is tamely ramified at \( v \), and \( E(G_v) \simeq E(k_v)/\ell \cdot E(k_v) \). For \( v \in S_m \), it is well-known that \( E(G_v) \) is either trivial or cyclic of order \( \ell \). It is nontrivial if and only if the local period \( Q_v \) is a \( G_v \)-norm in \( K_v^\ast \). Let

\[ S_m^0 = \{ v \in S_m \mid E(G_v) \text{ is nontrivial} \}. \]

Then we have

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

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

(a) \[ \left| \text{cokernel}\left\{ B_{S_m} \rightarrow \prod_{v \in S - S_m - S_{\infty}} E'(k_v) \right\} \right| \equiv 0 \pmod{\ell}. \]

(b) The pairing \( \langle \cdot, \cdot \rangle_G \) is degenerate of the first kind.
Proof. — Let

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

Then we have the diagram,

$$
\begin{array}{c}
0 \to E^0(K) \to E(K) \to E(K)/E^0(K) \to 0 \\
\downarrow \quad \quad \downarrow \\
0 \to \prod_{v \in S_m} E(G_v) \to \prod_{v \in S_m} E(G_v) \times \prod_{v \in S-S_m} E(k_v) \to \prod_{v \in S-S_m} E(k_v) \to 0.
\end{array}
$$

Since for $v \in S-S_m$, the number $\ell$ is prime to the residual characteristic of $v$, $E_1(K_v)$ (defined in 1.1) has trivial $\ell$-primary part, by (57) we see that

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

if and only if

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

Also

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

if and only if

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

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

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

if and only if

$$|\text{cokernel}\left\{ E(K) \to \prod_{v \in S-S_m} E(k_v) \right\}| \equiv 0 \pmod{\ell}. $$
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
\[ \text{cokernel}\left\{ E(K)^0 \to \prod_{v \in S_0^0} E(G_v) \right\} \equiv 0 \pmod{\ell}. \]

Recall the map \( \beta \) defined in (24). We have the following commutative diagram
\[
\begin{array}{ccc}
0 & \to & \bigoplus_{v \in S_0^0} \mathbb{Z}[Q_v]' \\
& & \downarrow \quad \beta \\
& & B_S \\
& \downarrow & \downarrow \\
0 & \to & \prod_{v \in S_0^0} B_v / N_{G_v}(B_w) \\
& & \text{im}\left\{ B_S \to \prod_{v \in S_0^0} B_v / N_{G_v}(B_w) \right\} \\
& & \to \prod_{v \in S_0^0} \mathbb{E}(G_v). \\
\end{array}
\]

It is then sufficient to show that (b) holds if and only if
\[ \text{cokernel}\left\{ B_S \to \prod_{v \in S_0^0} B_v / N_{G_v}(B_w) \right\} \equiv 0 \pmod{\ell}. \]

By Lemma 2.11, the global pairing \( \langle \cdot, \cdot \rangle_G \) induces a pairing
\[ \bigoplus_{v \in S_0^0} \mathbb{Z}/\ell \cdot \mathbb{Z}[Q_v] \times \text{Im}\left\{ B_S \to \prod_{v \in S_0^0} B_v / N_{G_v}(B_w) \right\} \to G. \]

By counting and by Lemma 2.11, we see that (59) holds if and only if there is an element
\[ a \in \bigoplus_{v \in S_0^0} \mathbb{Z}[Q_v] \cap \mathcal{N} - \bigoplus_{v \in S_0^0} \ell \cdot \mathbb{Z}[Q_v]. \]

To complete the proof, we need to show that
\[ \mathcal{N} \cap A_S^0 \subset \left( \mathcal{N} \cap \bigoplus_{v \in S_0^0} \mathbb{Z} \cdot [Q_v] \right) + \ell \cdot A_S^0. \]

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 \( E(K_v)/N_{G_v}(L_v) \) is nontrivial. Therefore \( a \) is an element of \( \bigoplus_{v \in S_0^0} \mathbb{Z} \cdot [Q_v] + \ell \cdot A_S^0. \)
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

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

has trivial $\ell$-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 $E'$ with $E$ 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

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

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 $(\ell, G)$ is good, the order of torsion $w$ is relatively prime to $\ell$, $A_S \otimes \mathbb{Z}_\ell$ and $B_S \otimes \mathbb{Z}_\ell$ are free $\mathbb{Z}_\ell$-modules. We can choose a basis of $A_S \otimes \mathbb{Z}_\ell$, $\{a_1, \ldots, a_r\}$, such that $\{b_1 = \ell^{\mu_1} \cdot a_1, \ldots, b_r = \ell^{\mu_r} \cdot a_r\}$ 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

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

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

**Lemma 4.11.** Assume that $G$ is cyclic of order $\ell$, $(\ell, G)$ is good, $D$ equals the the conductor of the extension $L/K$, and the cokernel of the map $E(K) \to \prod_{v \in S - S_m} E(k_v)$ has trivial $\ell$-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 $N - (A_S^0 \cup \ell \cdot A_S)$, 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

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

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 $b' \not\in B_{v_0} = E_1(K_{v_0})$ (see (L4) in 2.1). As before, let $w_0$ be a chosen place of $L$ sitting over $v_0$, and $G_{v_0} = \text{Gal}(L_{w_0}/K_{v_0})$. As $\ell$ is prime to the residue character ($= \ell'$) of $K_{v_0}$ and $E_1(L_{w_0})$ is a $\mathbb{Z}_{\ell'}$-module, we have

$$E_1(K_{v_0}) = N_{G_{v_0}}(E_1(L_{w_0})).$$

Let $y_{w_0} \in E_1(L_{w_0})$ 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

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

Since $G_{v_0}$ acts trivially on $E(L_{w_0})/E_1(L_{w_0})$ and $b' \not\in E_1(L_{w_0})$, we must have $\xi \neq 0$.

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

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

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 $\alpha$ (defined in 2.2) and the biextension $\mathbb{P}/K$ (defined in 2.1). Let $\tilde{P}_S = (\alpha^*, \alpha^*)\mathbb{P}(K)$. Then $\tilde{P}_S$ 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 $\tilde{P}_S$ and obtain the diagram

$$
\begin{array}{ccc}
0 & \longrightarrow & K^* \\
\| & & \| \\
0 & \longrightarrow & K^* \\
\end{array}
\quad
\begin{array}{ccc}
\longrightarrow & \longrightarrow & \longrightarrow \\
\pi_S & \pi_S & \pi_S \\
\longrightarrow & \longrightarrow & \longrightarrow \\
A_S \times A_S & A_S \times B_S & 0
\end{array}
$$

Let $p'$ be a lifting of $a' \times b'$ in $\{a'\}P_S$. 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 $E(L_{w_0}) \times E_1(L_{w_0})$. We have the following diagram of exact sequences:

$$
\begin{array}{ccc}
0 & \longrightarrow & L^*_{w_0} \\
\| & & \| \\
0 & \longrightarrow & L^*_{w_0}
\end{array}
\quad
\begin{array}{ccc}
\longrightarrow & \longrightarrow & \longrightarrow \\
\pi_{v_0} & \pi_{v_0} & \pi_{v_0} \\
\longrightarrow & \longrightarrow & \longrightarrow \\
\{a'\} \times E(L_{w_0}) & \{a'\} \times E_1(L_{w_0}).
\end{array}
$$

The lower row of the diagram induces the exact sequence

\begin{equation}
0 \longrightarrow C_{v_0}/\ell \cdot C_{v_0} \longrightarrow \{a'\} P_{v_0} / N_{G_{v_0}}(\{a'\} P_{w_0}) \\
\longrightarrow \{a'\} \times E_1(K_{v_0})/N_{G_{v_0}}(E_1(L_{w_0})) = 0.
\end{equation}

By Lemma 2.4, $\psi_{v_0}$ 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

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

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 \((p'_v - \eta)\) defines a class
\[
\{p'_v - \eta\} \in H^1(G_{v_0}, \{a'\} P(L_{w_0})).
\]
We have
\[
\pi_{v_0}^*\{p'_v - \eta\} = \{a'\} \times \xi \in H^1(G_{v_0}, \{a'\} \times \mathbb{E}(L_{w_0})).
\]
Consequently,
\[
\partial(\{a'\} \times \xi) = 0,
\]
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 \((a'_v, \xi)_{v_0} = 0\), a contradiction. \(\square\)

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

**Definition 4.12.** — Let
\[
\langle G \rangle \mathbb{E} = \text{Ker}\left\{ \mathbb{E}(K) \to \prod_v \mathbb{E}(G_v) \right\},
\]
\[
\langle G \rangle \mathbb{E}' = \text{Ker}\left\{ \mathbb{E}'(K) \to \prod_v \mathbb{E}'(G_v) \right\}.
\]
Denote
\[
B^1_S = \text{Ker}\left\{ B_S \to \prod_{v \in S - S_m} \mathbb{E}'(G_v) \right\}.
\]
Let \(\alpha: A_S \to \mathbb{E}(K)\) be the map in (22). Then \(\alpha(B^1_S) \subset \langle G \rangle \mathbb{E}\). At every \(v \in S - S_m\), since the extension \(L_v/K_v\) is totally (and tamely) ramified, we have \(N_{G_v}(L_v/K_v) = \ell \cdot \mathbb{E}(K_v)\). This and the assumption that the cokernel of \(\mathbb{E}(K) \to \prod_{v \in S - S_m} \mathbb{E}(k_v)\) has trivial \(\ell\)-part imply that there exists an integer \(n\) such that \((n, \ell) = 1\) and
\[
n \cdot \langle G \rangle \mathbb{E} \subset \ell \cdot \mathbb{E}(K) + \alpha(B_S).
\]
For each \(x \in \langle G \rangle \mathbb{E}\), consider the exact sequence:
\[
0 \to L^* \to \{x\} \mathbb{P}(L) \xrightarrow{f} \{x\} \times \mathbb{E}'(L) \to 0.
\]
Locally we have the exact sequence

$$0 \to K_v^*/N_{G_v}(L_v^*) \to \{x\}^{\mathbb{P}(K_v)/N_{G_v}(\{x\}^{\mathbb{P}(L_v)}) \overset{f}{\to} \{x\} \times E(G_v).$$

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

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

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

$$t_v = (t \pmod{N_{G_v}((x)\mathbb{P}(L_v)))} \in K_v^*/N_{G_v}(L_v^*).$$

By the class field theory, we have the map

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

**Definition 4.13.** — The Schneider pairing,

$$\langle \cdot, \cdot \rangle_{\text{Sch}} : (G)E \times (G)E' \to G,$$

is defined as follows. For $x \in G_E$, $y \in G_E'$, the pairing $\langle x, y \rangle_{\text{Sch}}$ is defined by

$$\langle x, y \rangle_{\text{Sch}} = \sum_v \lambda_v(t_v).$$

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 $\ell$. 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

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

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

**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:

\[
0 \to K_v^*/N_{G_v}(L_w^*) \xrightarrow{\sim} \{a\}P_v/N_{G_v}(\{a\}P_w) \xrightarrow{-} \{a\} \times B_v/N_{G_v}(B_w).
\]

Since \( b_v \) is a \( G_v \)-norm, we have

\[ p_v \in K_v^* \cdot N_{G_v}(\{a\}P_w). \]

Let \( \psi_v \) 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 \( \langle x, y \rangle_{Sch} \).

Suppose that \( v \in S_m \). Then \( B_v = K_v^* \) and the kernel of the map \( \gamma_v : \{a_v\}P_v \to \{x\}P(K_v) \) 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 \( a_v' \in L_w^* \) such that

\[ N_{G_v}(a_v') = a_v. \]

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 \( \psi_v \) induces a splitting,

\[ \tilde{\psi}_v : \{x\}P(K_v)/N_{G_v}(\{x\}P(L_w)) \longrightarrow K_v^*/N_{G_v}(L_w^*). \]

Then by (65), we have

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

This shows that \( p_v \) and \( t \) respectively contribute the same amount to \( \langle a, b \rangle_G \) and \( \langle x, y \rangle_{Sch} \). \( \square \)
DEFINITION 4.15. — We define the null space of the Schneider pairing as

\[ NS = \{ x \in (G)E | \langle x, y \rangle_{\text{Sch}} = 0 \text{ for all } y \in (G)E' \}. \]

Obviously, we have \( \ell \cdot (G)E \subset NS \). We say that the Schneider pairing is degenerate if \( NS \neq \ell \cdot (G)E \).

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

Suppose that \( x \in NS - \ell \cdot (G)E \). 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,

\[ \langle a, b \rangle_G = \langle x, y \rangle_{\text{Sch}} = 0. \]

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 \( N - A_S^0 \cup \ell \cdot A_S \). 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 \( \ell \) if necessary, we can assume that \( a \in B_S \). Let \( y \) be an element of \( (G)E' = (G)E \). If \( y = \alpha(b) \in A(B_S^1) \), then by Lemma 2.11 and Lemma 4.14,

\[ \langle x, y \rangle_{\text{Sch}} = \langle a, b \rangle_G = 0. \]

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

\[ \langle x, y \rangle_{\text{Sch}} = \langle x, \ell \cdot y' \rangle_{\text{Sch}} = \langle \ell \cdot b', a \rangle_G = 0. \]

By (63), \( x \in NS \). Since \( a \not\in A_S^0 \cup \ell \cdot A_S \), \( x \not\in \ell \cdot (G)E \) and the Schneider pairing is degenerate.

It follows directly from the definitions that

\[ (66) \quad \ell \cdot E(K) \subset N_G(E(L)) \subset NS. \]

To prove Proposition 4.1, we need to study the group \( NS/N_G(E(L)) \). Let

\[ \text{res} : H^1(K, E) \longrightarrow H^1(L, E) \]

be the restriction map of cohomology groups. Denote

\[ \Theta_{L/K} = \text{res}(H^1(K, E)) \cap \Theta_L^G. \]
LEMMA 4.17. — Assume that $G$ is cyclic of order $\ell$ and $(\ell, G)$ is good. We have

$$\mathcal{N}S/N_G(E(L)) \simeq \mathcal{H}_L^G/\mathcal{H}_L/K.$$

Proof. — Consider the diagram

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

(67)

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

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 $x \in (G')E'$, we can find an $\xi$ in $H^1(L, E)^G$ and an $(\eta_v)_v$ in $\bigoplus_v H^1(K_v, E)$ such that

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

and

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

The element $\xi$ is unique up to elements of $\text{res}(H^1(K, E))$, and for the chosen $\xi$, the element $\eta_v$ is unique up to elements of $\text{inf}_v(H^1(G_v, E(L_v)))$.

The element $x$ is in $\mathcal{N}S$ if and only if

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

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

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

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

$$\eta''_v = \eta_v - \eta'_v.$$

By replacing $\xi$ by $\xi - \text{res}(\eta'')$, we see that when $x$ is in $\mathcal{N}S$, the element $\xi$ can be chosen as in $\mathcal{H}_L^G$ and vice versa. \qed
The following lemma is a consequence of Lemma 4.16, (66) and Lemma 4.17.

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

\[
N_G(E(L))/\ell \cdot E(K) \cdot \left| \frac{\Pi E}{\Pi L/K} \right| \equiv 0 \pmod{\ell}. \tag{68}
\]

**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 \(A_f^\ell\) 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

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

if both the denominator and the numerator are finite.

Let \(G\) be a cyclic group and \(A\) a \(G\)-module. Let \(h_4(A)\) be the order of the cohomology group \(H^4(G, A)\). 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 \(\ell\) 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

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

Taking \(A = E(L)\) in (69), we get

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

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 $(\ell, G)$ is good, $\ell$ is relatively prime to $w$ and $|\Pi_K|$. We have

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

Also, $\Pi_L$ has non-trivial $\ell$-primary part if and only if

$$|\Pi^G_L| \equiv 0 \pmod{\ell}.$$ 

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

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

As a consequence of Lemma 4.9, the pairing $(\cdot, \cdot)_G$ 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 $E(K) \to \prod_{v \in S - S_m} E(k_v)$ has trivial $\ell$-primary part. By Lemma 4.3, Lemma 4.9, Lemma 4.18 and the above arguments we only need to show that

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

if and only if

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

But this is just a direct consequence of (70). \hfill \Box

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 $z \Theta_G \in Z[G]$. 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 $\ell$, $D$ is the conductor of the abelian extension $L/K$, and $\chi$ is a nontrivial character of $G$. The following are true:

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

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

(b) Assume that $(\ell, G)$ 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) $\mathbb{III}_L$ has non-trivial $\ell$-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 $\chi_0$ be the trivial character of $G$. Since $r > 0$, by Definition 1.8 and (46), we have

$$\chi_0(\Theta_G) = 0.$$  

(72)

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

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

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

$$o(\chi_0, z \cdot \det_G) > e.$$  

(73)

Recall that $S = \text{Supp}(D)$. Theorem 3.14 is a consequence of Proposition 3.8, Proposition 4.1 and Proposition 5.1.  \( \Box \)
5.2. The product formula.

As before, assume that $G$ is cyclic of order $\ell$. Suppose that $\ell$ 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 $E$ has additive reduction at $v$, then it also has additive reduction at $w$. Because $\ell$ is prime to 2, if $E$ 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.

\[
L_{E/K}(s) = \prod_{\chi \in \hat{G}} L_{E/L}(\chi, s).
\]

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

\[
o(\chi, \Theta_G) = \frac{1}{\ell - 1} \cdot \prod_{\psi \in \hat{G} - \{\text{id}\}} o(\psi, \tau_\psi \cdot \Omega_\psi^{-1} \cdot |\mu_K| \cdot |L(\psi, 1))\).
\]

By Lemma 1.7, we have

\[
\prod_{\psi \in \hat{G} - \{\text{id}\}} \tau_\psi = \|D\|^{-\frac{1}{2}(\ell - 1)}.
\]

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

\[
|\Delta_{L/K}| \neq 0 \pmod{\ell}.
\]

By (10) and (12), we have

\[
\prod_{\psi \in \hat{G} - \{\text{id}\}} \Omega_\psi^{-1} = \frac{\Omega_K}{\Omega_L}.
\]

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

\[
o(\chi, \Theta_G) = \text{ord}_\ell\left(\|D\|^{-\frac{1}{2}(\ell - 1)} \cdot |\mu_K|^{\ell - 1} \cdot \frac{\Omega_K}{\Omega_L} \cdot \lim_{s \to 1} \frac{L_{E/L}(s)}{L_{E/K}(s)}\right).
\]

Recall that if $(\ell, G)$ is good then the Birch and Swinnerton-Dyer conjecture is true for $(E, G)$ (see 3.4). In this case, the Birch and Swinnerton-Dyer conjecture is true for $E/L$ unless $K$ is a function field.
Lemma 5.2. — Suppose that $G$ is cyclic of order $\ell$ and $(\ell, G)$ is good.

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

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

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

$$o(\chi, \Theta_G) = \operatorname{ord}_\ell \left\{ \|D\|^{-(\ell-1)} \cdot \frac{|\mu_K|^{\ell}}{|\mu|} \cdot \frac{I_{11}}{I_{11}^K} \cdot \frac{\frac{R(E_L)}{R(E_K)}}{\prod_{w \text{ over } L} \frac{m_w}{\prod_{v \text{ over } K} m_v}} \right\}.$$ 

If the Birch and Swinnerton-Dyer conjecture is not true for $E/L$, then by Theorem 3.6, (74) and (75), $\chi(\Theta_G) = 0$. If the Birch and Swinnerton-Dyer conjecture is true for $E/L$ 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 $E(L)_{\text{tor}}$ is prime to $\ell$. Since $(\ell, G)$ is good, $\ell$ is prime to $w = |E(K)_{\text{tor}}| = |E(L)_{\text{tor}}^G|$. \qed

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)

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

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

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

\[
\frac{R(\mathbb{E}_L)}{R(\mathbb{E}_K)} = \rho^\kappa.
\]

For a fixed \( v \), we have

\[
\prod_{w|v} \frac{m_w}{m_v} \begin{cases} 
\in \mathbb{Z} & \text{if } v \notin S_m, \\
\ell & \text{if } v \in S_m.
\end{cases}
\]

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

\[ \square \]

BIBLIOGRAPHY


A. WEIL, Adèles and Algebraic Groups, Birkhauser, Boston, 1982.