On Gross’s Refined Class Number Formula for Elementary Abelian Extensions

By Joongul Lee

Abstract. In this paper we consider the conjecture of Gross on the special values of abelian L-functions when the Galois group G is an elementary abelian $l$-group. Under some restrictions, we prove that the conjecture holds when the class number of the base field is prime to $l$.

1. Introduction

Suppose $L/K$ is an abelian extension of global fields and let $G = \text{Gal}(L/K)$. In [3], B. Gross has conjectured a congruence relation involving the Stickelberger element in $\mathbb{Z}[G]$, class number of $K$ and the generalized regulator. The relation can be thought of as a generalization of the classical class number formula which describes the leading term of the Taylor expansion of $\zeta_K(s)$ at $s = 0$ in terms of the class number and the regulator of $K$. In this paper we consider the case when $G$ is an elementary abelian $l$-group. Our main result is Theorem 3, which states that the conjecture holds when the class number of $K$ is prime to $l$ and (when $K$ contains a primitive $l$-th root of unity) $T$ contains a place whose degree is prime to $l$. This improves the result that Gross obtained when $G$ is cyclic of prime order (see [3]).

I would like to thank Benedict Gross, Ki-Seng Tan and Felipe Voloch for helpful discussions and suggestions, and especially my teacher John Tate for continuous support and encouragement. I would also like to thank the referee for valuable comments.

2. The conjecture of Gross

Let $L/K$ be an abelian extension of global fields with Galois group $G$. Let $S$ be a finite non-empty set of places of $K$ which contains all archimedean places and places ramified in $L$, and let $T$ be a finite non-empty set of places

1991 Mathematics Subject Classification. Primary 11S40; Secondary 11R29, 11R37.
of $K$ which is disjoint from $S$. Let $n = |S| - 1$. For a finite place $v$ of $K$, let $\mathbb{F}_v$ be the residue field of $v$.

For a complex character $\chi \in \hat{G} = \text{Hom}(G, \mathbb{C}^*)$, the associated modified $L$-function is defined as

\[
L_{S,T}(\chi, s) = \prod_{v \in T} (1 - \chi(g_v)N_v^{1-s}) \prod_{v \notin S} (1 - \chi(g_v)N_v^{-s})^{-1},
\]

where $g_v \in G$ is the Frobenius element for $v$.

The Fourier inversion formula tells us that there is a unique element $\theta_G \in \mathbb{C}[G]$ which satisfies

\[
\chi(\theta_G) = L_{S,T}(\chi, 0)
\]

for all $\chi \in \hat{G}$. In fact, $\theta_G \in \mathbb{Z}[G]$ by works of Weil, Siegel, Deligne-Ribet and Cassou-Noguès (see [3] for more information).

Let $Y$ be the free $\mathbb{Z}$-module generated by the places $v \in S$ and $X = \{ \sum_{v \in S} a_v \cdot v \mid \sum a_v = 0 \}$ the subgroup of elements of degree zero in $Y$. Let $U_T$ denote the group of $S$-units which are congruent to 1 (mod $T$) (in other words, $S$-units which are congruent to 1 (mod $v$) for all $v \in T$). Then $U_T$ is a free $\mathbb{Z}$-module of rank $n$ if $K$ is a function field, and to ensure that the same is true if $K$ is a number field we require that $T$ either contains places of different residue characteristics or contains a place $v$ whose absolute ramification index $e_v$ is strictly less than $(p - 1)$, where $p$ is the characteristic of $\mathbb{F}_v$. This assumption makes $U_T$ a free $\mathbb{Z}$-module.

Let $J$ denote the idele group of $K$, and $f : J \to G$ be the Artin reciprocity map. Let $\lambda_G$ be the homomorphism

\[
\lambda_G : U_T \longrightarrow \quad G \otimes X
\[
\varepsilon \quad \mapsto \quad \sum_{S} f(1,1,\ldots,\varepsilon_v,\ldots,1) \cdot v.
\]

We choose bases $\langle \varepsilon_1, \ldots, \varepsilon_n \rangle$ and $\langle x_1, \ldots, x_n \rangle$ for $U_T$ and $X$. With respect to the chosen bases, we obtain an $n \times n$ matrix $((g_{ij}))$ for $\lambda_G$ with entries in $G$.

Let $I \subset \mathbb{Z}[G]$ be the augmentation ideal, which is defined as the kernel of the ring homomorphism

\[
\mathbb{Z}[G] \quad \longrightarrow \quad \mathbb{Z}
\[
\quad g \quad \mapsto \quad 1.
\]
It is well known that the map \( g \mapsto g - 1 \pmod{I^2} \) gives an isomorphism \( G \cong I/I^2 \) of abelian groups. We may therefore consider the matrix for \( \lambda_G \) as having entries \( \eta_{ij} = g_{ij} - 1 \) in \( I/I^2 \). We define

\[
\det \lambda_G = \sum_{\sigma \in \text{Sym}(n)} \text{sign}(\sigma) \eta_{\sigma(1)} \eta_{\sigma(2)} \cdots \eta_{\sigma(n)}
\in I^n/I^{n+1}.
\]

Now we can state the main conjecture.

**Conjecture 1** (Gross). \( \theta_G \equiv m \cdot \det \lambda_G \pmod{I^{n+1}} \).

Here \( m = \pm h_{S,T} \) is the modified class number of the \( S \)-integers of \( K \) and the sign depends on the choice of ordered bases of \( X \) and \( U_T \) (see [3]). We summarize some basic facts on Conjecture 1.

**Proposition 2.**

(a) Suppose \( S \subset S' \) and \( T \subset T' \). If Conjecture 1 holds for the set \( S \) and \( T \), it holds for \( S' \) and \( T' \).

(b) Suppose \( H \) is a subgroup of \( G \). The natural map \( \mathbb{Z}[G] \rightarrow \mathbb{Z}[G/H] \) maps \( \theta_G \) and \( \det \lambda_G \) to \( \theta_{G/H} \) and \( \det \lambda_{G/H} \) respectively. Hence Conjecture 1 holds for \( G/H \) if it holds for \( G \).

(c) Conjecture 1 holds for \( G \) if and only if it holds for all its \( p \)-Sylow quotients.

(d) If \( S \) contains a place \( v \) that splits completely in \( L \), then \( \theta_G \equiv m \cdot \det \lambda_G \equiv 0 \pmod{I^{n+1}} \).

(e) If \( n = 0 \) then \( \det \lambda_G = 1, m = h_{S,T}, I^n/I^{n+1} = \mathbb{Z} \), and conjecture 1 holds because it is equivalent to the classical class number formula.

See [3, 8] for (a) and (b). (c) was pointed out by J. Tate. For (d) we note that the Euler factor for \( v \) is zero, so \( \theta_G = 0 \), and also the row of the matrix of \( \lambda_G \) which correspond to \( v \) is zero and hence \( \det \lambda_G \equiv 0 \pmod{I^{n+1}} \). (e) follows from the definitions of the related quantities.

In [3], B. Gross proved that the Conjecture 1 holds when \( S \) consists of the archimedean places of \( K \). He also treated the case when \( G \cong \mathbb{Z}/l\mathbb{Z} \) is cyclic of prime order. In this case, \( I^n/I^{n+1} \cong \mathbb{Z}/l\mathbb{Z} \) for \( n \geq 1 \), and Gross proved that his conjecture is true up to an element of \( (\mathbb{Z}/l\mathbb{Z})^* \), in the sense that \( \theta_G \) always belongs to \( I^n \) (hence we are comparing two elements in \( I^n/I^{n+1} \)) and that \( \theta_G \in I^{n+1} \) if and only if \( m \cdot \det \lambda_G \in I^{n+1} \). In [9],
M. Yamagishi treated the case when $K = \mathbb{Q}$ and got some partial result, and N. Aoki proved that the conjecture is true for $K = \mathbb{Q}$ in [1]. D. Hayes proved a refined version of the Stark conjecture (conjectured by Gross) for function fields in [4], which implies Conjecture 1 for $n = 1$. In [6], K.-S. Tan proved the case when $K$ is a function field of characteristic $p$ and $G$ is a $p$-group.

3. The main theorem

Let $l$ be a prime. Our goal is to prove the following theorem.

**Theorem 3.** Suppose $G$ is an elementary abelian $l$-group. If $K$ is a function field suppose also that $h_K$, the number of divisor classes of degree 0 of $K$, is prime to $l$, and, in case $K$ contains a primitive $l$-th root of unity, $T$ contains a place whose degree is prime to $l$. Then conjecture 1 holds.

If $K$ is a number field, the existence of the archimedean places assures that Conjecture 1 is true when $l \geq 3$ since the archimedean places split completely in $L$, and when $l = 2$ Conjecture 1 follows from the work of Gross and corollary 5 below. Therefore we may assume that $K$ is a function field. Also, since Tan proved Conjecture 1 for $p$-groups ([6]), we may assume that $l$ is different from the characteristic of $K$. Hence we will be dealing only with tame ramification. Also we may assume that $T$ consists of a single place whose degree is prime to $l$ if $K$ contains a primitive $l$-th root of unity, via proposition 2.

Let $S = \{v_0, v_1, \ldots, v_n\}$, $n = |S| - 1$, and $T = \{v_T\}$. Let $K_S$ be the maximal extension of $K$ unramified outside of $S$ whose Galois group is an elementary abelian $l$-group. Let $G_S = \text{Gal}(K_S/K)$, and for $i = 0, \ldots, n$, let $I_i \subset G_S$ be the inertia group of $v_i$. Let $D_T$ be the decomposition group of $v_T$. Notice that $I_i$ is cyclic because $K_S/K$ has only tame ramification, and that $D_T$ is also cyclic because $v_T$ is unramified in $K_S$ and its residue field is finite. It follows from proposition 2 that we may assume that $n \geq 1$. We can also assume without loss of generality that $L = K_S$, and that all the places in $S$ are ramified in $K_S$.

Here is our strategy for proving Theorem 3. We first discuss the structure of $I^n/I^{n+1}$, and we find a homogeneous polynomial $f$ of degree $n$ with
coefficients in \( \mathbb{F}_l \) which may be viewed as a function on \( \hat{G}_S \) with values in \( \mathbb{F}_l \), such that the validity of the conjecture is equivalent to the vanishing of \( f \) on \( \hat{G}_S \). Next we study the structure of \( G_S \) in section 5., and we show that \( I_0, \ldots, I_n \) generate a subgroup of \( G_S \) of rank \( n \) or \( n + 1 \), depending on whether \( K \) contains a primitive \( l \)-th root of unity or not. We also show that \( I_0, \ldots, I_n, D_T \) generate a subgroup of \( G_S \) of rank \( n + 1 \) when \( K \) contains a primitive \( l \)-th root of unity. In section 6. we prove that if a polynomial function on \( \hat{G}_S \) vanishes on \( n + 1 \) linearly independent subspaces of codimension 1 and its degree is bounded by \( n \), then it must vanish on \( \hat{G}_S \). It turns out that this is exactly what we need in order to make the induction on \( n = |S| - 1 \) work, and the induction is carried out in section 7.

4. The structure of \( I^n/I^{n+1} \)

Choose a primitive \( l \)-th root of unity \( \zeta \in \mathbb{C}^* \), and let \( \lambda = \zeta l - 1 \). \((\lambda)\) is a prime ideal in \( \mathbb{Z}[\zeta] \) whose residue field is isomorphic to \( \mathbb{Z}/l\mathbb{Z} \), and we have \((l) = (\lambda)^{l-1}\). Also note that a character \( \chi \in \hat{G} \) can be extended by linearity to a ring homomorphism \( \chi : \mathbb{Z}[G] \longrightarrow \mathbb{C} \).

**Lemma 4** (Passi-Vermani). *Suppose \( G \) is an elementary abelian \( l \)-group. If \( \xi \in I \), then, for each integer \( k \geq 1 \), \( \xi \in I^k \) if and only if \( \lambda^k \mid \chi(\xi) \) for every complex character \( \chi \in \hat{G} \).*

**Proof.** See [3] for the case when \( G \cong \mathbb{Z}/l\mathbb{Z} \), and [5, 7] for elementary abelian case. \( \square \)

As we discussed in section 2., Gross proved that both \( \theta_G \) and \( m \cdot \det \lambda_G \) are in \( I^n \) when \( G \) is cyclic of prime order, which, together with Lemma 4, implies that both \( \theta_G \) and \( m \cdot \det \lambda_G \) are in \( I^n \) when \( G \) is an elementary abelian group.

**Corollary 5.** *Suppose \( G = \text{Gal}(L/K) \) is an elementary abelian \( l \)-group. Then the conjecture holds for \( L/K \) if and only if it holds for \( L'/K \) for all cyclic subextensions \( L'/K \) of \( L/K \).*

**Proof.** Set \( \xi = \theta_G - m \cdot \det \lambda_G \) and apply lemma 4. \( \square \)
Let $N = \dim_{\mathbb{F}_l} \hat{G} - 1$ and choose a basis $\{\chi_0, \ldots, \chi_N\}$ of $\hat{G}$. In general, we have

$$\zeta^m_l - 1 = (\zeta_l - 1)(\zeta_l^{m-1} + \ldots + 1) \equiv m(\zeta_l - 1) \pmod{\lambda^2}. \quad (6)$$

Hence, given $\chi = \prod_{i=0}^{N} \chi_i^{m_i} \in \hat{G}$ and $\sigma \in G$, we may write

$$\chi(\sigma - 1) = \zeta^{\sum a_i m_i}_l - 1 \equiv \sum a_i m_i \cdot \lambda \pmod{\lambda^2}, \quad (7)$$

where $a_i \in \mathbb{F}_l$ is defined by $\chi_i(\sigma) = \zeta_l^{a_i}$. If $\xi \in I^n$, then since $\chi_i$ can be written as a linear combination of $\prod_{j=1}^{n} (\tau_j - 1)$ where $\tau_j \in G$ for all $j$, we have

$$\chi(\xi) \equiv p(m_0, \ldots, m_N) \cdot \lambda^n \pmod{\lambda^{n+1}}, \quad (8)$$

where $p(X_0, \ldots, X_N) \in \mathbb{F}_l[X_0, \ldots, X_N]$ is a homogeneous polynomial of degree $n$. We can see from Lemma 4 that $\xi \in I^{n+1}$ if and only if $p = 0$ as a function on $\hat{G}$.

For $\chi \in \hat{G}$, define

$$f(\chi) = \frac{\chi(\theta_G - m \cdot \det \lambda_G)}{\lambda^n} \pmod{\lambda}. \quad (9)$$

The above argument shows that $f$ can be represented by a homogeneous polynomial of degree $n$. Let $K_\chi$ be the fixed field of $\ker \chi$. Then $f(\chi) = 0$ if and only if the conjecture holds for $K_\chi/K$ with respect to $S$ and $T$.

We also note that if $K$ contains an $l$-th root of unity and $T$ contains a place $v$ that splits completely in $L$, then the modifying Euler factor for $v$ is $(1 - Nv)$ which is divisible by $l$. Since $l \cdot \xi \in I^{m+(l-1)}$ whenever $\xi \in I^m$, which follows from lemma 4, $\theta_G$ will be in $I^{n+1}$. With the work of Gross, that implies $m \cdot \det \lambda_G \in I^{n+1}$. As a result, Conjecture 1 holds trivially (in the sense that the conjecture becomes $0 = 0$) when $K$ contains an $l$-th root of unity and $T$ contains a place that splits completely in $L$.

5. The structure of $G_S$

In this section, we study the structure of $G_S$ and the inertia groups of $S$ in $G_S$ using class field theory. (reference:[2])
Let $\mathbb{F}_q$ be the exact field of constants of $K$. For each place $v$ of $K$, let $K_v$ be the completion of $K$ at $v$, $U_v$ the set of local units in $K_v$, and $U_v^1 \subset U_v$ the local units which are congruent to 1 (mod $v$).

Let $J_0$ be the set of ideles of degree 0. It is easy to see that $J$ is (non-canonically) isomorphic to $\mathbb{Z} \times J_0$, because $K$ is known to have a divisor (not necessarily prime) of degree 1.

There is an exact sequence

\begin{equation}
0 \to (\prod_{v \in S} \mathbb{F}_v^*)/\mathbb{F}_q^* \to J/K^* \cdot \prod_{v \notin S} U_v \cdot \prod_{v \in S} U_v^1 \to J/K^* \cdot \prod_v U_v \to 0.
\end{equation}

If we let $K_{\text{unr}}$ be the maximal unramified abelian extension of $K$, and $K'_S$ the maximal abelian extension of $K$ unramified outside of $S$ and tamely ramified in $S$, then $J/K^* \cdot \prod_{v \notin S} U_v \cdot \prod_{v \in S} U_v$ and $J/K^* \cdot \prod_v U_v$ have dense images in $\text{Gal}(K'_S/K)$ and $\text{Gal}(K_{\text{unr}}/K)$ respectively, via the Artin reciprocity map.

Observe that $J/K^* \cdot \prod_v U_v$ is isomorphic to $\mathbb{Z} \times H$, where $H = J_0/K^* \cdot \prod_v U_v$ and since we assume that $h_K = |H|$ is not divisible by $l$, we have $(\mathbb{Z} \times H) \otimes \mathbb{Z}/l\mathbb{Z} = \mathbb{Z}/l\mathbb{Z}$ and $\text{Tor}(\mathbb{Z} \times H, \mathbb{Z}/l\mathbb{Z}) = 0$. Hence tensoring the exact sequence with $\mathbb{Z}/l\mathbb{Z}$ preserves the exactness;

\begin{equation}
0 \to (\prod_{v \in S} \mathbb{F}_v^*)/\mathbb{F}_q^* \to J/J^1 \cdot K^* \cdot \prod_{v \notin S} U_v \cdot \prod_{v \in S} U_v^1 \to \mathbb{Z}/l\mathbb{Z} \to 0,
\end{equation}

where $\mathbb{F}_q^*$ is the image of $\mathbb{F}_q^*$ in $\prod_{v \in S} \mathbb{F}_v^*/\mathbb{F}_v^{*l}$. Class field theory tells us that $G_S$ is isomorphic to the middle term of the exact sequence, hence $G_S$ is isomorphic to $\mathbb{Z}/l\mathbb{Z} \times (\prod_{v \in S} \mathbb{F}_v^*/\mathbb{F}_v^{*l})/\mathbb{F}_q^*$ and $I_i$ is the image of $\mathbb{F}_v^*/\mathbb{F}_v^{*l}$ in $G_S$.

If we look at the map

\begin{equation}
\mathbb{F}_q^* \to \prod_{v \in S} \mathbb{F}_v^* \to \prod_{v \in S} \mathbb{F}_v^*/\mathbb{F}_v^{*l},
\end{equation}

then since $\mathbb{F}_q^*$ is cyclic and $\prod_{v \in S} \mathbb{F}_v^*/\mathbb{F}_v^{*l}$ is killed by $l$, $\mathbb{F}_q^*$ is either 0 or cyclic of order $l$. It is clear that $\hat{\mathbb{F}}_q^* = 0$ when $q \equiv 1$ (mod $l$). When $q \equiv 1$ (mod $l$), we can see, for example by using Kummer theory, that $\mathbb{F}_q^*$ is contained in $(\mathbb{F}_v^*)^l$ if and only if deg $v$ is divisible by $l$. Hence $\mathbb{F}_q^*$ is non-trivial only when $q \equiv 1$ (mod $l$) and there is a place $v \in S$ such that $l$ does not divide deg $v$. 

Gross Class Number Formula

379
For each $i = 0, \ldots, n$, let $\sigma_i \in G_S$ be a generator of $I_i$, and $\sigma_T$ a generator of $D_T$. When $\mathbb{F}_q^* = 0$, $\{\sigma_i\}_{i=0}^n$ are linearly independent, viewing $G_S$ as a vector space over $\mathbb{F}_q$, and $\dim_{\mathbb{F}_q} G_S = n + 2$. On the other hand, when $\mathbb{F}_q^* \neq 0$, it gives a non-trivial linear relation among $\sigma_j$'s for $j$ such that $l \nmid \deg v_j$, and hence $\dim_{\mathbb{F}_q} G_S = n + 1$. As we have seen before, this case happens only when $K$ contains a primitive $l$-th root of unity and there is a place in $S$ whose degree is prime to $l$. In that case, we may assume that $l$ does not divide $\deg v_0$, then $\{\sigma_i\}_{i=1}^n$ are linearly independent. Furthermore, with the assumption $l \nmid \deg v_T$, $v_T$ does not split completely in $K \cdot \mathbb{F}_{q^l}$, which is the maximal unramified extension in $K_S$ by class field theory and the assumption $l \nmid h$. Hence $\sigma_T \notin \langle \sigma_0, \ldots, \sigma_n \rangle$, which implies that $\{\sigma_T, \sigma_1, \ldots, \sigma_n\}$ are linearly independent. Hence we have proved the following theorem.

**Theorem 6.** (a) If $K$ does not contain a primitive $l$-th root of unity, then the inertia groups of places in $S$ are linearly independent in $G_S$. (b) If $K$ contains a primitive $l$-th root of unity, then the inertia groups of places in $S$ generate a subgroup of $G_S$ of rank at least $n$, and the decomposition group of $v_T$ is not contained in the subgroup as long as $\deg v_T$ is prime to $l$.

**Remark.** This argument shows that the assumption on $T$ is necessary only when $\mathbb{F}_q^*$ is non-trivial, i.e. when $K$ contains an $l$-th root of unity and $S$ contains a place whose degree is prime to $l$.

6. **Functions on the $\mathbb{F}_l$-vector space**

Let $V$ be a $\mathbb{F}_l$-vector space of dimension $N + 1$. Choose a basis $\{w_0, \ldots, w_N\}$ of $V$, and for $i = 0, \ldots, N$ define $X_i \in \text{Hom}(V, \mathbb{F}_l)$ by $X_i(w_j) = \delta_{ij}$. We may view a polynomial $f \in \mathbb{F}_l[X_0, \ldots, X_N]$ as a function on $V$ via the above identification.

The goal of this section is to prove the following theorem, which will be used in proving Theorem 3.

**Theorem 7.** Suppose $f \in \mathbb{F}_l[X_0, \ldots, X_N]$ is a polynomial of degree $\leq n$, which we view as a function on $V$, and $\{V_i\}_{i=0}^n$ are $n + 1$ linearly independent subspaces of codimension 1 in $V$. If $f$ vanishes on $V_i$ for all $i$, then $f$ vanishes on $V$. 
Definition. We say that a polynomial \( p(X_0, \ldots, X_N) \in \mathbb{F}_l[X_0, \ldots, X_N] \) is reduced if for each \( X_i \), \( \deg_{X_i} p(X_0, \ldots, X_N) < l \).

Lemma 8. Every function on \( V \) with values in \( \mathbb{F}_l \) can be uniquely expressed as a reduced polynomial in \( \mathbb{F}_l[X_0, \ldots, X_N] \).

Proof. This is a well-known result, and we give a short proof here. Observe that for \( a_i \in \mathbb{F}_l \), \( i = 0, \ldots, N \), we have

\[
\prod_{i=0}^{N} (1 - (x_i - a_i)^{l-1}) = \begin{cases} 
1 & \text{if } x_i = a_i \text{ for all } i, \\
0 & \text{otherwise.}
\end{cases}
\]

By taking linear combination, we see that any function on \( V \) can be represented by a reduced polynomial. Uniqueness follows from counting such polynomials. \( \square \)

For each polynomial \( p(X_0, \ldots, X_N) \in \mathbb{F}_l[X_0, \ldots, X_N] \), we can associate the reduced polynomial \( p_r(X_0, \ldots, X_N) \) of \( p(X_0, \ldots, X_N) \), which is reduced and defines the same function on \( V \) as \( p(X_0, \ldots, X_N) \). We can get \( p_r(X_0, \ldots, X_N) \) from \( p(X_0, \ldots, X_N) \) by using the relations \( X_i^l = X_i \) for all \( i \) to replace \( X_i^m \) by \( X_i^{m-(l-1)} \) until \( m < l \). Notice that for each \( i \), \( \deg_{X_i} p_r \leq \deg_{X_i} p \), and hence \( \deg p_r \leq \deg p \).

Lemma 9. Suppose \( p(X_0, \ldots, X_N) \) is a reduced polynomial. If \( p(0, x_1, \ldots, x_N) = 0 \) for all \( (x_1, \ldots, x_N) \in \mathbb{F}_l^N \), then \( X_0 \mid p(X_0, \ldots, X_N) \).

Proof. Write \( p(X_0, \ldots, X_N) = X_0 \cdot q(X_0, \ldots, X_N) + r(X_1, \ldots, X_N) \). For all \( (x_1, \ldots, x_N) \in \mathbb{F}_l^N \), \( r(x_1, \ldots, x_N) = p(0, x_1, \ldots, x_N) - 0 \cdot q(0, x_1, \ldots, x_N) = 0 \). Since \( r \) is also reduced, we conclude that \( r = 0 \). \( \square \)

Proof of Theorem 7. By change of coordinates, we may assume that for each \( i = 0, \ldots, n \), \( V_i \) is given by the equation \( X_i = 0 \). Let \( f_r \) be the reduced polynomial of \( f \). According to Lemma 9, \( f_r \) is divisible by \( X_i \) for all \( i \) and since we have unique factorization, it follows that \( f_r \) is divisible by \( \prod_{i=0}^{n} X_i \). Since we have \( \deg f_r \leq \deg f \leq n \), it follows that \( f_r = 0 \), and hence \( f \) vanishes on \( V \). \( \square \)
7. The induction step

We prove Theorem 3 by induction on $n$. When $n = 0$, the conjecture holds as noted in Proposition 2.

Suppose $n \geq 2$. For each $i = 0, \ldots, n$, let $S_i = S \setminus \{v_i\}$. Then $\widehat{G_{S_i}}$ is the orthogonal of $I_i$, hence is a subspace of codimension 1 in $\widehat{G_S}$ since we assumed that $v_i$ is ramified in $K_S$. Note that $v_i$ is unramified in $K_{S_i}$.

By induction we can assume that for all $i = 0, \ldots, n$, Conjecture 1 holds for $K_{S_i}/K$ with respect to $S_i$ and $T$. Then Proposition 2 shows that Conjecture 1 holds for $K_{S_i}/K$ with respect to $S$ and $T$. Hence $f|_{\widehat{G_{S_i}}} = 0$. When $K$ does not contain a primitive $l$-th root of unity, it follows from Theorem 6 and Theorem 7 that $f = 0$ on $\widehat{G_S}$.

If $K$ contains a primitive $l$-th root of unity, we let $G_T = G_S/D_T$. Then the place $v_T$ will split completely in $K_\chi$ for all $\chi \in \widehat{G_T}$ which implies, as we discussed at the end of section 4., that we have $f|_{\widehat{G_T}} = 0$. Again, it follows from Theorem 6 and Theorem 7 that $f = 0$ on $\widehat{G_S}$, and hence $\theta_{G_S} \equiv m \cdot \det \lambda_{G_S} \pmod{I^{n+1}}$ in all cases. □

References

(Received July 18, 1996)

Department of Mathematics
The Ohio State University
Columbus, OH 43210
U.S.A.
E-mail: jlee@math.ohio-state.edu