Central Extensions and Hasse Norm Principle over Function Fields

Sunghan BAE and Hwanyup JUNG

Korea Advanced Institute of Science and Technology
(Communicated by S. Kaneyuki)

0. Introduction.

Let $K/k$ be a finite extension of global fields. Let $J(K)$ be the idele group of $K$ and $N_{K/k}$ the norm map from $K$ to $k$. We say that Hasse norm principle holds for $K/k$ if $k^* \cap N_{K/k}J(K) = N_{K/k}K^*$.

In number field case, several authors have studied the validity of Hasse norm principle for abelian extensions. It is very closely tied up with central extensions. In [Ge2], Gerth gave necessary and sufficient conditions for Hasse norm principle to hold for cyclotomic fields. In [K], Kagawa gave conditions for Hasse norm principle to hold for maximal real subfields of cyclotomic fields. Central extensions are also useful in studying ideal class groups ([CoRo], [Fr], [Fu3]).

Let $k = F_q(T)$ be the rational function field over finite field $F_q$, where $q = p^f$, $p = \text{char}(k)$ and $A = F_q[T]$. For any monic polynomial $m \in A$, let $k(\Lambda_m)$ be the $m$-th cyclotomic function field and $k(\Lambda_m)^+$ its maximal real subfield.

In this paper, we define central class fields of Galois extensions of function fields, give necessary and sufficient conditions for Hasse norm principle to hold for $k(\Lambda_m)$ and $k(\Lambda_m)^+$, and find lower bounds for the $\ell$-rank of ideal class groups of $k(\Lambda_m)$ and $k(\Lambda_m)^+$.

1. Central class field and Genus field.

Let $k$ be a global function field over a finite field $F_q$. Let $\infty$ be a place of degree 1 of $k$ and $\mathcal{O}_k$ the ring of regular elements outside $\infty$ of $k$. Let $E_k$ be the unit group of $\mathcal{O}_k$, which is just $F_q^*$. We write $k_\infty$ to be the completion of $k$ at $\infty$. We fix a sing function $\text{sgn} : k_\infty^* \rightarrow F_q^*$ and choose a uniformizer $\pi$ of $k_\infty$ with $\text{sgn}(\pi) = 1$. Denote by $\tilde{C}$ the field $k_\infty(\sqrt[1]{-\pi})$. In the following we mean by an extension of $k$, a separable extension of $k$ for which any embeddings into $k_\infty^{ac}$ lies in $\tilde{C}$ viewing as a subfield of $k_\infty^{ac}$.
Let $K$ be a finite Galois extension of $k$ and $S_\infty(K)$ the set of places of $K$ lying above $\infty$. Let $\mathcal{O}_K$ be the integral closure of $\mathcal{O}_k$ in $K$. For each $v \in S_\infty(K)$, the completion $K_v$ of $K$ at $v$ is a finite Galois extension of $k_\infty$ in $\tilde{C}$. Let $N_v$ be the norm map from $K_v$ to $k_\infty$. Define a sign map

\[ sgn_v : K_v^* \to \mathbb{F}_q^* \]

by $sgn_v(x) = sgn(N_v(x))$.

Let $J(K)$ be the idele group of $K$ and

$$U(K) = \{(x_w) \in J(K) : x_w \text{ is unit in } K_w, \quad \omega \notin S_\infty(K)\},$$

$$U_+(K) = \{(x_w) \in U(K) : sgn_v(x_v) = 1, \quad v \in S_\infty(K)\}.$$

Let $H_K$ and $H_K^+$ be the Hilbert class field and narrow Hilbert class field of $\mathcal{O}_K$, respectively. Then by class field theory, $H_K$ corresponds to $K^*U(K)$ and $H_K^+$ to $K^*U_+(K)$, i.e.

$$Gal(H_K/K) \simeq J(K)/K^*U(K),$$

$$Gal(H_K^+/K) \simeq J(K)/K^*U_+(K).$$

Let $Cl(\mathcal{O}_K)$ and $Cl_+(\mathcal{O}_K)$ be the ideal class group and narrow ideal class group of $\mathcal{O}_K$ respectively. Then we also have

$$Cl(\mathcal{O}_K) \simeq Gal(H_K/K),$$

$$Cl_+(\mathcal{O}_K) \simeq Gal(H_K^+/K).$$

We define the genus field $G(K/k)$ to be the maximal extension of $k$ in $H_K$ which is the composite of $K$ and some abelian extension of $k$. Similarly we can define the narrow genus field $G_+(K/k)$ replacing $H_K$ by $H_K^+$.

An extension $L/K$ is called central extension of $K/k$ if it is Galois extension over $k$ and $Gal(L/K)$ is contained in the center of $Gal(L/k)$. We write $Z(K/k)$ and $Z_+(K/k)$ for the maximal central extension of $K/k$ inside $H_K$ and $H_K^+$, respectively. We call $Z(K/k)$ the central class field and $Z_+(K/k)$ the narrow central class field of $K/k$, respectively. Then one can follow Furuta ([Fu1], [Fu2]) to get the following two lemmas.

**Lemma 1.1.** Let $K/k$ be a finite Galois extension and denote $G = G(K/k)$ and $G_+ = G_+(K/k)$.

(i) The genus group $Gal(G/K)$ of $K/k$ is given as

$$Gal(G/K) \simeq N_{K/k}J(K)/(N_{K/k}J(K) \cap (K^*N_{K/k}U(K)))$$

and its order, called the genus number of $K/k$, is given by

$$g_{K/k} = \frac{h(k) \prod_v e_v}{[K_0 : k][E_k : E_k \cap N_{K/k}U(K)]}$$

where $K_0$ is the maximal abelian extension of $k$ contained in $K$, $e_v$ is the ramification index of a place $v$ of $k$ in $K_0$, and $h(k)$ is the ideal class number of $\mathcal{O}_k$.

(ii) The narrow genus group $Gal(G_+/K)$ of $K/k$ is given as

$$Gal(G_+/K) \simeq N_{K/k}J(K)/(N_{K/k}J(K) \cap (K^*N_{K/k}U_+(K)))$$
and its order, called the narrow genus number of $K/k$, is given by

$$g_{K/k}^+ = \frac{h_+(k) \prod_{v \neq \infty} e_v}{[K_0 : k]}$$

where $h_+(k)$ is the narrow ideal class number of $\mathcal{O}_k$.

**Lemma 1.2.** Let $K/k$ be a finite Galois extension. Denote $Z = Z(K/k)$, $Z_+ = Z_+(K/k)$. Then the Galois groups $Gal(Z/K)$ and $Gal(Z_+/K)$ are given as;

$$Gal(Z/K) \simeq \frac{N_{K/k}J(K)}{N_{K/k}K^*N_{K/k}U(K)}.$$  

$$Gal(Z_+/K) \simeq \frac{N_{K/k}J(K)}{N_{K/k}K^*N_{K/k}U_+(K)}.$$ 

Denote 

$$A(K/k) = (k^* \cap N_{K/k}J(K))/N_{K/k}K^*$$

and

$$B(K/k) = (k^* \cap (N_{K/k}U(K)N_{K/k}K^*))/N_{K/k}K^*$$

$$= E_k \cap N_{K/k}J(K)/E_k \cap N_{K/k}K^*.$$ 

Then it is easy to show that $Gal(Z/G)$ is isomorphic to $A(K/k)/B(K/k)$. Similarly one can get

$$Gal(Z_+/G_+) \simeq A(K/k),$$

since $E_k \cap N_{K/k}U_+(K)$ is trivial. In the number field case it is only true when the base field $k$ is the field of rational numbers.

Following Frölich [Fr] we have

**Proposition 1.3.** i) The exponents of $Gal(Z/G)$ and $Gal(Z_+/G_+)$ divide $[K : k]$.  

ii) If $Cl(\mathcal{O}_k)$ is trivial, then the exponents of $Gal(Z/K)$ and $Gal(Z_+/K)$ divide $[K : k]$. 

iii) Suppose that $K = G(K/k)$ (resp. $K = G_+(K/k)$), or that $Cl(\mathcal{O}_k)$ is trivial. If $[K : k]$ is a power of a prime number $\ell$, then $K = Z(K/k)$ (resp. $K = Z_+(K/k)$) if and only if the $\ell$-part of $Cl(\mathcal{O}_K)$ (resp. $Cl_+(\mathcal{O}_K)$) is trivial.

2. **Hasse Norm Principle.**

We say Hasse Norm Principle (HNP, for short) holds for $K/k$ if every local norm in $k$ is a global norm, that is, $A(K/k)$ is trivial. Thus HNP holds for $K/k$ if and only if $Z_+(K/k) = G_+(K/k)$. When $K/k$ is finite abelian, then there is a nice criterion for HNP to holds.

**Proposition 2.1** ([R, Theorem 2]). Let $K/k$ be a finite abelian extension. Then HNP holds for $K/k$ if and only if HNP holds for every maximal subextensions of prime exponent.
Now let $K/k$ be a finite abelian extension of exponent $\ell$, where $\ell$ is a prime number. Let $G = \text{Gal}(K/k)$ and $X_G$ be the group of characters of $G$. If $[K : k] = \ell^r$, we may view $G$ and $\wedge^2 G$ as $\mathbb{F}_{\ell}$-vector space of dimension $r$ and $\binom{r}{2}$, respectively. Let $\{\chi_1, \chi_2, \ldots, \chi_r\}$ be a basis of $X_G$ over $\mathbb{F}_{\ell}$. Let $S$ be the set of all finite primes of $k$ which ramify on $K$. For each prime $\mathfrak{p} \in S$, let $\{g_1, g_2, \ldots, g_s\}$ be a basis of the decomposition group $G_{\mathfrak{p}}$ over $\mathbb{F}_{\ell}$. Let $[\delta_{tu,\alpha\beta}]_{\mathfrak{p}}$ be the matrix over $\mathbb{F}_{\ell}$ with $s(s - 1)/2$ rows and $r(r - 1)/2$ columns whose entry $\delta_{tu,\alpha\beta}$ in the $tu$ row and $\alpha\beta$ column is defined by the relation:

$$(\chi_{\alpha} \wedge \chi_{\beta})(g_t \wedge g_u) = \delta_{tu,\alpha\beta},$$

where $\zeta_{\ell}$ is a fixed primitive $\ell$-th root of unity and $\wedge$ is the exterior product. Let $\Delta(K/k)$ be the matrix over $\mathbb{F}_{\ell}$ whose rows consist of all the rows of the matrices $[\delta_{tu,\alpha\beta}]_{\mathfrak{p}}$ as $\mathfrak{p}$ runs over all elements of $S$.

**PROPOSITION 2.2** ([Gel, Theorem 3]). Let $K/k$ be a finite abelian extension of exponent $\ell$. Then the followings are equivalent:

(i) HNP holds for $K/k$.

(ii) $A(K/k)$ has trivial $\ell$-rank.

(iii) $\Delta(K/k)$ has rank $r(r - 1)/2$, where $r$ is the $\ell$-rank of $\text{Gal}(K/k)$.

Now we use this criterion to test the HNP for the cyclotomic function fields and maximal real subfields of cyclotomic function fields.

3. **HNP for $k(\Lambda_m)/k$.**

Let $k$ be the rational function field $\mathbb{F}_q(T)$ over finite field $\mathbb{F}_q$, $q = p^f$, $p = \text{char}(k)$ and $A = \mathbb{F}_q[T]$. Let $\infty$ be the place of $k$ corresponding to $(1/T)$. Let $m$ be a monic polynomial with irreducible factorization

(*)

$$m = p_1^{e_1}p_2^{e_2} \cdots p_z^{e_z},$$

and let $d_i = \deg p_i$ for each $i$. For each prime number $\ell$, $k(\Lambda_m)_\ell$ denotes the maximal extension of $k$ of exponent $\ell$ contained in $k(\Lambda_m)$ and we will write $\Delta_\ell(m)$ for $\Delta(k(\Lambda_m)_\ell/k)$. We assume that $q$ is odd.

If $z = 1$ in (*), then $p_1$ is the only finite prime of $k$ which ramify (in fact, totally) in $k(\Lambda_m)$. So the decomposition group $G_{p_1}$ of $p_1$ is all of $G$ and so HNP holds for $k(\Lambda_m)/k$.

If $z \geq 4$ in (*), then $z < z(z - 1)/2$. Since 2-rank of $\text{Gal}(k(\Lambda_m)/k)$ is $z$, $\Delta_2(m)$ has at most $z$ rows. So HNP does not hold for $k(\Lambda_m)_2/k$ and also for $k(\Lambda_m)/k$, by Proposition 2.1. It remains to consider the cases: $z = 2$ and $z = 3$.

**THEOREM 3.1.** Let $m = p_1^{e_1}p_2^{e_2}$. Then HNP holds for $k(\Lambda_m)/k$ if and only if the following conditions are satisfied:

(i) For each prime divisor $\ell$ of $(q^{d_1} - 1, q^{d_2} - 1)$

$$X^\ell \equiv p_1 \mod p_2$$
or

\[ X^\ell \equiv p_2 \mod p_1 \]

is not solvable.

(ii) If \( e_1, e_2 \geq 2 \), then \( q = p \) and \( d_i = 1, e_i = 2 \) for some \( i \) and

\[ X^p \equiv p_j \mod p_i^2 \quad (j \neq i) \]

is not solvable.

**PROOF.** By Proposition 2.2, we need to consider the validity of HNP for \( k(\Lambda_m)_{\ell}/k \) for each prime number \( \ell \).

For \( \ell \neq p \), if \( \ell \) does not divide \( (q^{d_1} - 1, q^{d_2} - 1) \), then \( k(\Lambda_m)_{\ell}/k \) is cyclic extension and so HNP holds.

For a prime divisor \( \ell \) of \( (q^{d_1} - 1, q^{d_2} - 1) \), \( G = Gal(k(\Lambda_m)_{\ell}/k) \simeq \langle \mathbb{Z}/\ell \mathbb{Z} \rangle^2 \). Let \( \chi_i \) be a multiplicative character on the inertia group \( T_{p_i} \) of order \( \ell \), \( t_i \) an element of \( T_{p_i} \) dual to \( \chi_i \), and \( \sigma_{ij} \) the Frobenius automorphism at the prime \( p_i \) in the extension \( k(\Lambda_{p_j}) \). Define

\[ e_{i,j}^{(\ell)} \in \mathbb{F}_\ell \] (\( i \neq j \)) as \( \chi_i(\sigma_{ji}) = \zeta_{\ell}^{e_{i,j}^{(\ell)}} \), where \( \zeta_{\ell} \) is a fixed primitive \( \ell \)-th root of unity. We use \( e_{i,j} \) for \( e_{i,j}^{(\ell)} \) for simplicity where no confusion arises. Then the matrix \( \Delta_{\ell}(m) \) is given as

\[
\begin{pmatrix}
\varepsilon_{2,1} \\
-\varepsilon_{1,2}
\end{pmatrix},
\]

by taking a basis \( \{t_i, \sigma_{ij}\} \) of \( G_{p_i} \). So \( \Delta_{\ell}(m) \) has rank 1 if and only if \( \varepsilon_{2,1} \neq 0 \) or \( \varepsilon_{1,2} \neq 0 \). But \( \varepsilon_{i,j} \neq 0 \) is equivalent that \( X^\ell \equiv p_j \mod p_i \) is not solvable.

Now we consider the case \( \ell = p \). If \( e_i = 1 \) for some \( i \), then \( k(\Lambda_m)_{p} = k(\Lambda_{p_i})_p \) \((j \neq i)\) for which HNP holds. So we only need to consider the case that \( e_1, e_2 \geq 2 \). From Theorem 3.3 in [Cl], we know that \( Gal(k(\Lambda_{p_i})_p)/k \) has \( p \)-rank \( r_i \) as

\[ r_i = \log_p q \times d_i \times \left\{ e_i - 1 - \left[ \frac{e_i - 1}{p} \right] \right\}. \]

Let \( T_{p_i} \) be the inertia group of \( p_i \) in \( G = Gal(k(\Lambda_{m})_{p}/k) \). Then \( G = T_{p_1}T_{p_2} \), so \( p \)-rank of \( G \) is \( r = r_1 + r_2 \). Since \( G_{p_i}/T_{p_i} \) is a cyclic group, \( p \)-rank of \( G_{p_i} \) is \( r_i \) or \( r_i + 1 \). Hence \( p \)-rank of \( H^{-3}(G_{p_i}, \mathbb{Z}) \) is \( \left( \begin{array}{c} r_i \end{array} \right) \) or \( \left( \begin{array}{c} r_i + 1 \end{array} \right) \) and

\[ p \text{-rank of } \mathcal{A}(k(\Lambda_m)_{p}/k) \geq \left( \begin{array}{c} r \end{array} \right) - \sum_{i=1}^{2} \left( \begin{array}{c} r_i + 1 \end{array} \right). \]

Hence HNP holds for \( k(\Lambda_m)_{p}/k \) only if \( r_1r_2 - (r_1 + r_2) \leq 0 \). The right hand side occurs if and only if \( r_1 = r_2 = 2 \) or \( r_i = 1 \) for some \( i \).

When \( r_1 = r_2 = 2 \), let \( \{\chi_{1,1}, \chi_{1,2}\} \) be a basis of the dual group of \( T_{p_1} \) over \( \mathbb{F}_p \) and \( \{\chi_{2,1}, \chi_{2,2}\} \) basis of the dual group of \( T_{p_2} \) over \( \mathbb{F}_p \). Then with respect to the basis \( \{\chi_{1,1} \wedge X_{1,2}, X_{1,1} \wedge X_{2,1}, X_{1,1} \wedge X_{2,2}, X_{1,2} \wedge X_{2,1}, X_{1,2} \wedge X_{2,2}, X_{2,1} \wedge X_{2,2}\} \), by choosing suitable bases...
of $G_{p_i}$'s the matrix $\Delta_p(m)$ is given by

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & [p_1, \chi_2,1] & [p_1, \chi_2,2] & 0 & 0 \\
0 & 0 & [p_1, \chi_2,1] & [p_1, \chi_2,2] & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & -[p_2, \chi_1,1] & 0 & -[p_2, \chi_1,2] & 0 \\
0 & 0 & -[p_2, \chi_1,1] & 0 & -[p_2, \chi_1,2] & 0 \\
\end{pmatrix},
$$

where $[p_i, \chi_{j,k}] \in \mathbb{F}_p (i \neq j)$ is defined by $\chi_{j,k}(\sigma_{ij}) = \zeta_p^{[p_i, \chi_{j,k}]}$, $\sigma_{ij}$ is defined similarly as before. Since the determinant

$$
\det(\Delta_p(m)) = -[p_1, \chi_2,1][p_1, \chi_2,2][p_2, \chi_1,1][p_2, \chi_1,2] + [p_1, \chi_2,2][p_1, \chi_2,1][p_2, \chi_1,1][p_2, \chi_1,2] = 0,
$$

HNP does not hold for $K(\Lambda_m)_p/K$.

When $r_i = 1$ and $r_j \geq 1$ arbitrary, clearly we have $q = p$ and $d_i = 1, e_i = 2$. In this case, $T_{p_i} \simeq \mathbb{Z}/p\mathbb{Z}$ and $T_{p_j} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_j}$. Let $\chi_1$ be a character modulo $p_i^2$ of order $p$ and $\{\chi_2,1, \chi_2,2, \ldots, \chi_2,r_j\}$ be a basis of dual group of $T_{p_j}$. With respect to the basis $\{\chi_1, \chi_2,1, \chi_2,2, \ldots, \chi_2,r_j\}$, again by choosing suitable bases for $G_{p_i}$'s the matrix $\Delta_p(m)$ is given by

$$
\begin{pmatrix}
[p_i, \chi_2,1] & [p_i, \chi_2,2] & \cdots & [p_i, \chi_2,r_j] & 0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \\
-[p_j, \chi_1] & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
0 & -[p_j, \chi_1] & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & -[p_j, \chi_1] & 0 & 0 & \cdots & 0 \\
\end{pmatrix}.
$$

So we see that $\Delta_p(m)$ has rank $r(r-1)/2$, where $r = r_j + 1$, if and only if $[p_j, \chi_1] \neq 0$. And this condition is equivalent to the fact that $X^p \equiv p_j mod p_i^2$ is not solvable. $\square$

For a prime divisor $\ell$ of $q - 1$ and monic irreducible polynomial $p$, let $(\frac{q}{p})_\ell$ be the $\ell$-th reciprocity symbol. For another monic irreducible polynomial $q \neq p$, define $[q, p]_\ell \in \mathbb{F}_\ell$ as

$$
\left(\frac{q}{p}\right)_\ell = \xi_\ell^{[q, p]_\ell},
$$

where $\xi_\ell$ is a fixed primitive $\ell$-th root of unity. From the $\ell$-th reciprocity law

$$
\left(\frac{q}{p}\right)_\ell \left(\frac{p}{q}\right)_\ell^{-1} = (-1)^{\frac{q-1}{\ell}\deg(p)\deg(q)},
$$
we see that \([q, p]_{\ell} = [p, q]_{\ell}\), except the case that \(q \equiv 3 \mod 4\), \(\ell = 2\) and \(\deg(p), \deg(q) \equiv 1 \mod 2\). And in this exceptional case, we have \([q, p]_{2} = [p, q]_{2} + 1\).

**Theorem 3.2.** Let \(m = p_{1}^{e_{1}}p_{2}^{e_{2}}p_{3}^{e_{3}}\). Then HNP holds for \(k(\Lambda_{m})/k\) if and only if the following conditions are satisfied:

(i) \(q = 3\)

(ii) \([p_{1}, p_{3}][p_{2}, p_{1}][p_{3}, p_{2}] \neq [p_{1}, p_{2}][p_{3}, p_{1}][p_{2}, p_{3}]\)

(iii) For any odd prime divisor \(\ell\) of \((q^{d_{1}} - 1, q^{d_{2}} - 1, q^{d_{3}} - 1)\),

\[\varepsilon_{2,1}\varepsilon_{3,2}\varepsilon_{1,3} \neq \varepsilon_{1,2}\varepsilon_{3,1}\varepsilon_{2,3}\]

where let \(\chi_{i}\) denote a character of \(T_{\mathfrak{p}_{i}}\) of order \(\ell\) and \(\varepsilon_{i,j} \in F_{\ell}\) \((i \neq j)\) is defined as \(\chi_{i}(p_{j}) = \zeta_{\ell}^{e_{i,j}}\), and \(\zeta_{\ell}\) is a fixed primitive \(\ell\)-th root of unity.

(iv) For odd prime number \(\ell\) dividing exactly two of \(q^{d_{1}} - 1\), \(q^{d_{2}} - 1\), and \(q^{d_{3}} - 1\) (say \(q^{d_{i}} - 1\) and \(q^{d_{j}} - 1\)), then

\[X^{\ell} \equiv p_{i} \mod p_{j}\quad \text{or}\quad X^{\ell} \equiv p_{j} \mod p_{i}\]

is not solvable.

(v) If \(e_{i} \geq 2\) \((i = 1, 2, 3)\), then \(d_{i} = 1\), \(e_{i} = 2\) for all \(i\).

(vi) If exactly two of \(e_{1}\), \(e_{2}\) and \(e_{3} \geq 2\) (say \(e_{j}\), \(e_{k} \geq 2\)), then \(q = p\), \(d_{j} = 1\), \(e_{j} = 2\) for some \(j\) and \(X^{p} \equiv p_{k} \mod p_{j}^{2}\) is not solvable.

**Proof.** For each prime divisor \(\ell\) of \(q - 1\), let \(\chi_{i}\) be the character defined by \(\left(\frac{p_{i}}{\ell}\right)\).

With respect to the basis \(\{\chi_{1} \wedge X_{2}, \chi_{1} \wedge X_{3}, X_{2} \wedge X_{3}\}\), the matrix \(\Delta_{\mathfrak{p}_{i}}(m)\) is given by

\[
\begin{pmatrix}
[p_{2}, p_{1}]_{\ell} & [p_{3}, p_{1}]_{\ell} & 0 \\
-[p_{1}, p_{2}]_{\ell} & 0 & [p_{3}, p_{2}]_{\ell} \\
0 & -[p_{1}, p_{3}]_{\ell} & -[p_{2}, p_{3}]_{\ell}
\end{pmatrix},
\]

and its determinant

\[
\det(\Delta_{\mathfrak{p}_{i}}(m)) = [p_{2}, p_{1}]_{\ell}[p_{3}, p_{2}]_{\ell}[p_{1}, p_{3}]_{\ell} - [p_{1}, p_{2}]_{\ell}[p_{3}, p_{1}]_{\ell}[p_{2}, p_{3}]_{\ell}.
\]

Note that \(q = 3\) is the only one such that \(q \equiv 3 \mod 4\) and 2 is the unique prime divisor. Except the case that \(q = 3, \ell = 2\), \(\det(\Delta_{\mathfrak{p}_{i}}(m)) = 0\) hence HNP does not hold for \(k(\Lambda_{m})_{\ell}/k\).

Thus we must have \(q = 3\) and so we get (i) and (ii).

For (iii), we only replace the \(\ell\)-th reciprocity symbol \(\left(\frac{p_{i}}{\ell}\right)\) by a character \(\chi_{i}\) modulo \(p_{i}\) of order \(\ell\) to get the condition. (iv) is just the case of (i) in Theorem 3.1.

Now we consider the case \(\ell = p = 3\). When at most one of \(e_{1}\), \(e_{2}\) and \(e_{3}\) is greater than 1 (say \(e_{i}\)), then the decomposition group \(G_{p_{i}}\) of \(p_{i}\) is all of \(G = Gal(k(\Lambda_{m})_{p}/k)\). So HNP always holds for \(k(\Lambda_{m})_{p}/k\).

When exactly two of \(e_{1}\), \(e_{2}\) and \(e_{3}\) are greater than 1, this is just the case of (ii) in Theorem 3.1.

Now assume that \(e_{1}, e_{2}, e_{3} \geq 2\). Let \(T_{\mathfrak{p}_{i}}\) be the inertia group of \(p_{i}\) in \(G = Gal(k(\Lambda_{m})_{p}/k)\). Then \(G = T_{p_{1}}T_{p_{2}}T_{p_{3}}\) so \(p\)-rank of \(G\) is \(r = r_{1} + r_{2} + r_{3}\). Since \(G_{p_{i}}/T_{p_{i}}\) is a cyclic group,
$p$-rank of $G_{p_i}$ is $r_i$ or $r_i + 1$. Hence $p$-rank of $H^{-3}(G_{p_i}, \mathbb{Z})$ is $(r_i^2)$ or $(r_i^2 + 1)$ and $p$-rank of $\mathcal{A}(k(\Lambda_{m})_{p}/k)) \geq \binom{r_i^2 - 1}{2} - \sum_{i=1}^{3} \binom{r_i^2 + 1}{2} = (r_1r_2 + r_1r_3 + r_2r_3) - (r_1 + r_2 + r_3)$.

Thus HNP holds for $k(\Lambda_{m})_{p}/k$ only if $(r_1r_2 + r_1r_3 + r_2r_3) - (r_1 + r_2 + r_3) \leq 0$. The right side occurs if and only if $r_1 = r_2 = r_3 = 1$ (i.e. $d_i = 1, e_i = 2$ for all $i$). In this case, any element of $(F_p[\mathfrak{T}]/\mathfrak{p}_i^2)^{\times}$ can be written uniquely as $c_0(1 + c_1\mathfrak{p}_i) \mod \mathfrak{p}_i^2$, where $c_0, c_1 \in F_p$, and $\chi_i (c_0(1 + c_1\mathfrak{p}_i) \mod \mathfrak{p}_i^2) = c_1$ defines a character modulo $\mathfrak{p}_i^2$ of order $p$. With respect to the basis $\{\chi_1 \wedge \chi_2, \chi_1 \wedge \chi_3, \chi_2 \wedge \chi_3\}$, the matrix $\Delta_3(m)$ is given by,

$$
\begin{pmatrix}
(p_1 - p_2)^{-1} & (p_1 - p_3)^{-1} & 0 \\
-(p_2 - p_1)^{-1} & 0 & (p_2 - p_3)^{-1} \\
0 & -(p_3 - p_1)^{-1} & -(p_3 - p_2)^{-1}
\end{pmatrix},
$$

and its determinant $\det(\Delta_3(m))$ is

$$(p_1 - p_2)^{-1}(p_2 - p_3)^{-1}(p_3 - p_1)^{-1} - (p_2 - p_1)^{-1}(p_1 - p_3)^{-1}(p_3 - p_2)^{-1}$$

which is not zero. Here we note that $p_i - p_j$ is an element of $F_p^{\times}$ since $p_i$ and $p_j$ are monic of degree $1$. So we get (v). (vi) is just the case of (ii) in Theorem 3.1.

REMARK. From (ii) of the Theorem 3.2, we must have that at most one of deg $p_i$’s is even.

4. HNP for $k(\Lambda_{m})^{\perp}/k$.

Let $m = p_1^{e_1}p_2^{e_2} \cdots p_z^{e_z}$ be as before. First we note that $k(\Lambda_{m})_{\ell}^{\perp} = k(\Lambda_{m})_{\ell}$, for any prime number $\ell \mid q - 1$. Thus it suffices to consider $k(\Lambda_{m})_{\ell}^{\perp}$ for $\ell \mid q - 1$; We will write $\Delta_{\ell}(m)^{\perp}$ for $\Delta(k(\Lambda_{m})_{\ell}^{\perp}/k)$.

For $\ell \mid q - 1$, we know ([A, Lemma 3.2]) that if $d_i \equiv 0 \mod \ell$, then $k(\sqrt[\ell]{\mathfrak{p}_i}) \subset k(\Lambda_{p_i})^{\perp}$ and otherwise $k(\sqrt[\ell]{\mathfrak{p}_i}) \subset k(\Lambda_{p_i})^{\perp}$, where $1 \leq n_i \leq \ell - 1$ and $n_id_i \equiv 1 \mod \ell$. Hence if $d_i \equiv 0 \mod \ell$ for all $i$, then

$$k(\Lambda_{m})_{\ell}^{\perp} = k(\Lambda_{m})_{\ell} = k(\sqrt[\ell]{\mathfrak{p}_1}, \sqrt[\ell]{\mathfrak{p}_2}, \cdots, \sqrt[\ell]{\mathfrak{p}_z}).$$

LEMMA 4.1. Suppose that $d_1, d_2 \not\equiv 0 \mod \ell$. Then $k(\sqrt[\ell]{p_1^{n_1}p_2^{(\ell-1)n_2}})$ is the unique cyclic extension of degree $\ell$ over $k$ contained in $k(\Lambda_{p_1p_2})^{\perp}$. $(p_1^{n_1}p_2^{(\ell-1)n_2})^{\ell}$ defines a character of $Gal(k(\sqrt[\ell]{p_1^{n_1}p_2^{(\ell-1)n_2}})/k)$ of order $\ell$.

PROOF. By Lemma 3.2([A]), we see that $k(\sqrt[\ell]{p_1^{n_1}p_2^{(\ell-1)n_2}})$ is contained in $k(\Lambda_{p_1p_2})$. Since $p_1^{n_1}p_2^{(\ell-1)n_2}$ is monic and its degree satisfies $n_1d_1 + (\ell - 1)n_2d_2 \equiv 0 \mod \ell$,

$$k(\sqrt[\ell]{p_1^{n_1}p_2^{(\ell-1)n_2}}) \subset k(\Lambda_{p_1p_2})^{\perp}.$$
From the Chinese remainder theorem \((\frac{p_1}{\ell})_{\ell}^{n_1}(\frac{p_2}{\ell})_{\ell}^{-n_2}\) is nontrivial and so has order \(\ell\). Now it suffices to show that \((\frac{c}{\ell})_{\ell}^{n_1}(\frac{c}{\ell})_{\ell}^{-n_2} = 1\) for any \(c \in F_q^*\). But it follows from the formula
\[
\left(\frac{c}{p}\right)_{\ell} = c^{\frac{q-1}{\ell}} \deg p,
\]
for any monic irreducible polynomial \(p\) and \(c \in F_q^*\). \(\square\)

If \(d_1, d_2, \cdots, d_k \not\equiv 0 \mod \ell\) and \(d_{i+1}, \cdots, d_z \equiv 0 \mod \ell\), then by Lemma 4.1, we see that
\[
k(\Lambda_m)_{\ell}^+ = k\left(\sqrt[p_1]{p_2(\ell-1) n_2}, \cdots, \sqrt[p_1]{p_1(\ell-1) n_1}, \sqrt[\ell]{\mathfrak{p}_{i+1}}, \cdots, \sqrt[\ell]{\mathfrak{p}_z}\right),
\]
so its Galois group has \(\ell\)-rank \(z-1\).

Clearly as in \(k(\Lambda_m)\), if \(z = 1\), then HNP holds for \(k(\Lambda_m)^+/K\). If \(z \geq 5\), then \(Gal(k(\Lambda_m)_{\ell}^+/K)\) has 2-rank at least \(z-1 \geq 4\). So HNP does not hold for \(k(\Lambda_m)_{\ell}^+/K\).

It remains to consider: \(z = 2, z = 3\) and \(z = 4\).

**THEOREM 4.2.** Let \(m = p_1^{e_1}p_2^{e_2}\). Then HNP holds for \(k(\Lambda_m)^+/k\) if and only if the following conditions are satisfied;

(i) For a prime number \(\ell \nmid q - 1\), HNP holds for \(k(\Lambda_m)_{\ell}/k\).

(ii) For a prime number \(\ell \mid q - 1\), if \(d_1 \equiv d_2 \equiv 0 \mod \ell\), then
\[
\left(\frac{p_2}{p_1}\right)_{\ell} \neq 1 \quad \text{or} \quad \left(\frac{p_1}{p_2}\right)_{\ell} \neq 1.
\]

**PROOF.** For \(\ell \mid q - 1\), if \(d_i \not\equiv 0 \mod \ell\) for some \(i\), then \(k(\Lambda_m)_{\ell}^+/k\) is cyclic extension and so HNP holds. If \(d_1 \equiv d_2 \equiv 0 \mod \ell\), \(k(\Lambda_m)_{\ell}^+ = k(\Lambda_m)_{\ell}\). So we get (ii). \(\square\)

**THEOREM 4.3.** Let \(m = p_1^{e_1}p_2^{e_2}p_3^{e_3}\). Then HNP holds for \(k(\Lambda_m)^+/k\) if and only if the following conditions are satisfied;

(i) For a prime number \(\ell \nmid q - 1\), HNP holds for \(k(\Lambda_m)_{\ell}/k\).

(ii) For a prime number \(\ell \mid q - 1\), at most two of \(d_1, d_2, d_3\) are divisible by \(\ell\) and

(1) if \(d_i \not\equiv 0 \mod \ell\) and \(d_j \equiv d_k \equiv 0 \mod \ell\), then \(\left(\frac{p_i}{p_k}\right)_{\ell} \neq 1\).

(2) if \(d_i, d_j \not\equiv 0 \mod \ell\) and \(d_k \equiv 0 \mod \ell\), then \(\left(\frac{p_i}{p_k}\right)_{\ell} \neq 1\) or \(\left(\frac{p_j}{p_k}\right)_{\ell} \neq 1\).

(3) if \(d_1, d_2, d_3 \not\equiv 0 \mod \ell\) then \(n_2 \epsilon_{2,1} \neq n_1 \epsilon_{1,2}, n_2 \epsilon_{1,2} \neq n_3 \epsilon_{3,2} \neq n_1 \epsilon_{1,3} \neq n_2 \epsilon_{2,3}\).

Here \(\epsilon_{i,j}\) is given as in Theorem 3.2.

**PROOF.** For a prime number \(\ell \mid q - 1\), if \(d_1, d_2, d_3\) are all divisible by \(\ell\), then
\[
k(\Lambda_m)_{\ell}^+ = k(\Lambda_m)_{\ell}
\]
for which HNP does not hold (Theorem 3.2).

When \(d_i \not\equiv 0 \mod \ell\) and \(d_j \equiv d_k \equiv 0 \mod \ell\), \(k(\Lambda_m)_{\ell}^+ = k(\sqrt[p_j]{p_j^{(\ell-1)n_1}}, \sqrt[p_k]{p_k})\). Since \(\left(\frac{p_j}{p_k}\right)_{\ell} = \left(\frac{p_k}{p_j}\right)_{\ell}\), we get the condition as (ii) in Theorem 3.1.

When \(d_i, d_j \not\equiv 0 \mod \ell\) and \(d_k \equiv 0 \mod \ell\), \(k(\Lambda_m)_{\ell}^+ = k(\sqrt[p_i]{p_i^{(\ell-1)n_1}}, \sqrt[p_k]{p_k})\). Let \(\chi_{i,j}\) be the character defined by \(\left(\frac{p_i}{p_j}\right)_{\ell}^{n_1}\) and \(\chi_k\) be characters defined by \(\left(\frac{p_k}{p_j}\right)_{\ell}\). With respect
to $\chi_{i,j} \wedge \chi_{k}$, $\Delta^{+}_\ell(m)$ is given by
\[
\begin{pmatrix}
\epsilon_{k,i} \\
-\epsilon_{k,j} \\
-n_{i}\epsilon_{i,k} + n_{j}\epsilon_{j,k}
\end{pmatrix}.
\]
Since $d_{k} \equiv 0 \text{ mod } \ell$, $\epsilon_{k,i} = \epsilon_{i,k}$, $\epsilon_{j,k} = \epsilon_{k,j}$ and so $\Delta^{+}_\ell(m)$ has rank 1 if and only if $\epsilon_{k,i} \neq 0$ or $\epsilon_{k,j} \neq 0$.

When $d_{1}, d_{2}, d_{3} \neq 0 \text{ mod } \ell$, $k(\Lambda_{m})^{+} = k\left(\sqrt[\ell]{\mathfrak{p}_{1}^{n_{1}}\mathfrak{p}_{2^{(\ell-1)n_{2}}}}, \sqrt[\ell]{\mathfrak{p}_{1}^{n_{1}}\mathfrak{p}_{3^{(\ell-1)n_{3}}}}\right)$. Let $\chi_{i,j}$ be the character defined by $(\overline{\mathfrak{p}_{i}})^{n_{i}}(\overline{\mathfrak{p}_{j}})^{-n_{j}}$. Then $\chi_{2,3} = \chi_{1,3}/\chi_{1,2}$. With respect to $\chi_{1,2} \wedge \chi_{1,3}$ and suitably chosen bases, the matrix $\Delta^{+}_\ell(m)$ is given by
\[
\begin{pmatrix}
n_{2}\epsilon_{2,1} - n_{3}\epsilon_{3,1} \\
-n_{1}\epsilon_{1,2} + n_{3}\epsilon_{3,2} \\
n_{1}\epsilon_{1,3} - n_{2}\epsilon_{2,3}
\end{pmatrix}.
\]
So we get the condition. \square

Similar, but more complicated, process will give the following Theorem, whose proof we will omit.

**Theorem 4.4.** Let $m = p_{1}^{e_{1}}p_{2}^{e_{2}}p_{3}^{e_{3}}p_{4}^{e_{4}}$. Then HNP holds for $k(\Lambda_{m})^{+}/k$ if and only if the following conditions are satisfied;

(i) At least one of $e_{i}$'s is 1.

(ii) Any common prime divisor of $(q^{d_{1}} - 1)$, $(q^{d_{2}} - 1)$, $(q^{d_{3}} - 1)$ and $(q^{d_{4}} - 1)$ is a divisor of $q - 1$.

(iii) For each prime number $\ell | q - 1$, at least two of $d_{1}, d_{2}, d_{3} and d_{4}$ are not divisible by $\ell$.

(1) If $d_{i}, d_{j} \not\equiv 0 \text{ mod } \ell$ and $d_{k}, d_{m} \equiv 0 \text{ mod } \ell$, then
\[
\left(\frac{p_{m}}{p_{k}}\right)_{\ell} \neq 1 \text{ and } \epsilon_{i,k}\epsilon_{j,m} \neq \epsilon_{i,m}\epsilon_{j,k}.
\]

(2) If $d_{i}, d_{j}, d_{k} \not\equiv 0 \text{ mod } \ell$ and $d_{m} \equiv 0 \text{ mod } \ell$, then except the case that $q \equiv 3 \text{ mod } 4, \ell = 2$,
\[
n_{j}(\epsilon_{i,j}\epsilon_{j,m}\epsilon_{k,m}) - n_{k}(\epsilon_{i,k}\epsilon_{j,m}\epsilon_{k,m}) - n_{i}(\epsilon_{i,j}\epsilon_{i,m}\epsilon_{k,m}) + n_{k}(\epsilon_{j,k}\epsilon_{i,m}\epsilon_{k,m}) \neq 0.
\]
In the case that $q \equiv 3 \text{ mod } 4, \ell = 2$,
\[
\epsilon_{i,m}\epsilon_{j,m} \neq 0, \quad \epsilon_{i,m}\epsilon_{k,m} \neq 0 \quad \text{or} \quad \epsilon_{j,m}\epsilon_{k,m} \neq 0.
\]

(3) If $d_{1}, d_{2}, d_{3}, d_{4} \not\equiv 0 \text{ mod } \ell$, then except the case that $q \equiv 3 \text{ mod } 4, \ell = 2$,
\[
(n_{1}\epsilon_{1,2} - n_{3}\epsilon_{1,3})(-n_{1}\epsilon_{1,2} + n_{4}\epsilon_{2,4})(-n_{1}\epsilon_{1,3} + n_{4}\epsilon_{3,4})
\]
\[
+ (n_{1}\epsilon_{1,2} - n_{3}\epsilon_{2,3})(n_{2}\epsilon_{1,2} - n_{4}\epsilon_{1,4})(-n_{1}\epsilon_{1,3} + n_{4}\epsilon_{3,4})
\]
\[
+ (n_{1}\epsilon_{1,3} - n_{2}\epsilon_{2,3})(n_{3}\epsilon_{1,3} - n_{4}\epsilon_{1,4})(n_{1}\epsilon_{1,2} - n_{4}\epsilon_{2,4}) \neq 0.
\]
In the case that $q \equiv 3 \text{ mod } 4$, $\ell = 2$,

\[
(\varepsilon_{1,4} + \varepsilon_{2,4})(\varepsilon_{1,2} + \varepsilon_{2,3} + 1) - (\varepsilon_{1,4} + \varepsilon_{3,4})(\varepsilon_{2,3} + \varepsilon_{2,4}) \neq 0
\]

\[
(\varepsilon_{1,4} + \varepsilon_{2,4})(\varepsilon_{2,3} + \varepsilon_{3,4} + 1) - (\varepsilon_{1,4} + \varepsilon_{3,4})(\varepsilon_{1,3} + \varepsilon_{2,3}) \neq 0,
\]

or

\[
(\varepsilon_{2,3} + \varepsilon_{2,4})(\varepsilon_{2,3} + \varepsilon_{3,4} + 1) - (\varepsilon_{1,2} + \varepsilon_{2,3} + 1)(\varepsilon_{1,3} + \varepsilon_{2,3}) \neq 0.
\]

(iv) For $\ell \nmid q - 1$, HNP holds for $K(\Lambda_{\mathfrak{p}_{i}^{e_{i}}}^{r_{j}}\mathfrak{p}_{k}^{e_{k}})^{\ell}/K$, for any $\{i, j, k\} \subset \{1, 2, 3, 4\}$.

**COROLLARY 4.5.** HNP holds for $k(\Lambda_{m})^{+}/k$ but dose not hold for $k(\Lambda_{m})/k$ if and only if HNP holds for every maximal subfield of $k(\Lambda_{m})^{+}/k$ whose Galois group over $k$ exponent $\ell$, $\ell \nmid q - 1$ and moreover, one of the following conditions is satisfied;

(i) $m = p_{1}^{e_{1}}p_{2}^{e_{2}}$: There exist a prime number $\ell | q - 1$ such that $d_{i} \not\equiv 0 \text{ mod } \ell$ for one

(ii) $i$ and $\left(\frac{p_{2}}{p_{1}}\right)_{\ell} = \left(\frac{p_{1}}{p_{2}}\right)_{\ell} = 1$.

(i) When $q \not\equiv 3$, HNP always dose not hold for $k(\Lambda_{m})/k$.

(2) When $q = 3$, and if $d_{1} \equiv d_{2} \equiv d_{3} \equiv 1 \text{ mod } 2$, $\left(\frac{p_{2}}{p_{1}}\right)_{2} = \left(\frac{p_{1}}{p_{2}}\right)_{2} = \left(\frac{p_{1}}{p_{3}}\right)_{2}$ does not hold.

(3) When $q = 3$, and if $d_{i} \equiv d_{j} \equiv 1 \text{ mod } 2$ and $d_{k} \equiv 0 \text{ mod } 2$, $\left(\frac{p_{1}}{p_{k}}\right)_{2} \not\equiv \left(\frac{p_{k}}{p_{1}}\right)_{2}$.

(iii) $m = p_{1}^{e_{1}}p_{2}^{e_{2}}p_{3}^{e_{3}}p_{4}^{e_{4}}$: HNP always dose not hold for $k(\Lambda_{m})/k$.

5. **Ideal Class Groups.**

Let $\ell$ be a prime. For a finite abelian $\ell$-extension $K$ of $k$, we say that it is maximal if it is the maximal $\ell$-extension of $k$ in $k(\Lambda_{m})$, where $m$ is the conductor of $K$. By the conductor $m$ of $K$, we mean the smallest monic polynomial $m$ such that $K$ is contained in $k(\Lambda_{m})$. From now on we assume that $K$ is a maximal abelian $\ell$-extension of $k$ with conductor $m$, say $m = p_{1}^{e_{1}}p_{2}^{e_{2}} \cdots p_{t}^{e_{t}}$ and $\Gamma = Gal(K/k)$. Let $K_{i}$ be the maximal abelian $\ell$-extension of $k$ in $k(\Lambda_{p_{i}^{e_{i}}})$. Then $K$ is the composite of those $K_{i}$. For each $i$, let $\Gamma_{i}$ be the inertia group and decomposition group of $p_{i}$ in $K$, respectively. Clearly $\Gamma = \prod_{i} \Gamma_{i}$. If $\ell \neq char(k)$, $m$ must be square free with $q^{deg(p_{i})} \equiv 1 \text{ mod } \ell$ and each inertia group $T_{i} \simeq Gal(K_{i}/k) \simeq \mathbb{Z}/\ell^{a_{i}}$, where $a_{i}$ is the maximal exponent of $\ell$ which divides $q^{deg(p_{i})} - 1$. If $\ell = p = char(k)$, each $e_{i}$ must be larger than 1 and the inertia group $T_{i}$ is an abelian $p$-group with $p$-rank

\[
\delta_{i} = f \times \deg(p_{i}) \times \left( e_{i} - 1 - \left\lfloor \frac{e_{i} - 1}{p} \right\rfloor \right),
\]

where $q = p^{f}$.

For any finite abelian group $G$, $r_{\ell}(G)$ denotes the $\ell$-rank of $G$. Following [CoRo] we have

**PROPOSITION 5.1.** Let $K$ be as above. Then
\( (i) \ \ell \neq \text{char}(k); \]
\[ r_{\ell}(\text{Cl}(O_K)) \geq \frac{s(s-3)}{2} - \varepsilon, \]
where \( \varepsilon = 1 \text{ if } \ell \mid q - 1 \) and otherwise \( \varepsilon = 0. \)

\( (ii) \ \ell = p = \text{char}(k); \]
\[ r_{\ell}(\text{Cl}(O_K)) \geq \sum_{i<j} \delta_i \delta_j - \sum_i \delta_i. \]

**Corollary 5.2.** Let \( m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \) and denote \( O_m = O_{k(A_m)}. \) For \( \ell \neq \text{char}(k), \)
let \( t_\ell \) be the number of \( p_i \) such that \( q^{\deg(p_i)} \equiv 1 \mod \ell. \) Then

\( (i) \ \ell \neq \text{char}(k); \]
\[ r_{\ell}(\text{Cl}(O_m)) \geq \frac{t_\ell(t_\ell-3)}{2} - \varepsilon, \]
where \( \varepsilon \) is defined as in Proposition 5.1.

\( (ii) \ \ell = p = \text{char}(k); \]
\[ r_{\ell}(\text{Cl}(O_m)) \geq \sum_{i<j} \delta_i \delta_j - \sum_i \delta_i. \]

Let \( K \) be a maximal abelian \( \ell \)-extension of \( k \) with conductor \( m. \) Let \( K^+ = K \cap k(A_m)^+. \)
It is the maximal abelian \( \ell \)-extension of \( k \) in \( k(A_m)^+. \) For the case that \( \ell \neq \text{char}(k) \) and \( \ell \nmid q - 1, \) or \( \ell = p = \text{char}(k), K^+ \) is equal to \( K. \) Thus we have the following;

**Proposition 5.3.** Let \( m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \) and denote \( O_m^+ = O_{k(A_m)^+}. \)

\( (i) \ \ell \neq \text{char}(k) \text{ and } \ell \nmid q - 1; \]
\[ r_{\ell}(\text{Cl}(O_m^+)) \geq \frac{t_\ell(t_\ell-3)}{2}. \]

\( (ii) \ \ell = p = \text{char}(k); \]
\[ r_{\ell}(\text{Cl}(O_m^+)) \geq \sum_{i<j} \delta_i \delta_j - \sum_i \delta_i. \]

Now suppose that \( \ell \mid q - 1. \) Let \( \varepsilon^+ \) be the \( \ell \)-rank of \( B(K^+/k), \) i.e. the \( \ell \)-rank of \( E_k \cap N_{K+/k} U(K^+) / E_k \cap N_{K+/k} (K^+) \). Then as in [CoRo] one can show that \( \varepsilon^+ = 0. \)

**Proposition 5.4.** Suppose that \( \ell \mid q - 1. \) Let \( K \) be the maximal abelian \( \ell \)-extension of \( k \) with conductor \( m = p_1 p_2 \cdots p_s, \) and \( K^+ = K \cap k(A_m)^+. \)

\( (i) \ \text{If } \deg(p_i) \equiv 0 \mod \ell \text{ for all } i, \text{ then } \]
\[ r_{\ell}(\text{Cl}(O_{K^+})) \geq \frac{s(s-3)}{2}. \]

\( (ii) \ \text{If } \deg(p_i) \not\equiv 0 \mod \ell \text{ for some } i, \text{ then } \]
\[ r_{\ell}(\text{Cl}(O_{K^+})) \geq \frac{s^2 - 5s + 2}{2}. \]
PROOF. In case (i), $k(\sqrt[\ell]{\mathfrak{p}_1}, \cdots, \sqrt[\ell]{\mathfrak{p}_s}) \subset K^+$ and in case (ii) $K = K^+k(\sqrt[\ell]{-\mathfrak{p}_i})$, where $n_i \deg \mathfrak{p}_i \equiv 1 \mod \ell$, by Lemma 3 of [A]. Then the result follows as in the Theorem 2, (i), (ii) of [CoRo].

COROLLARY 5.5. Suppose that $\ell \mid q - 1$ and $m = p_1^e_1 p_2^e_2 \cdots p_s^e_s$.
(i) If $\deg(p_i) \equiv 0 \mod \ell$ for all $i$, then
\[ r_\ell(Cl(\mathcal{O}_m^+)) \geq \frac{s(s - 3)}{2}. \]
(ii) If $\deg(p_i) \not\equiv 0 \mod \ell$ for some $i$, then
\[ r_\ell(Cl(\mathcal{O}_m^+)) \geq \frac{s^2 - 5s + 2}{2}. \]

Assume that $\ell \neq \text{char}(k)$ and $\ell \nmid q - 1$. Let $K$ be a maximal abelian $\ell$-extension of $k$ with conductor $m = p_1 p_2 \cdots p_s$. From the genus number formula (Lemma 1.1), $K = G(K/k)$ and since $B(K/k)$ is trivial, we have
\[ Gal(Z(K/k)/K) \cong \mathcal{A}(K/k). \]

Let $\Delta_\ell(K/k)$ be the matrix defined in Section 2. Then we have
\[ \ell\text{-rank of } \mathcal{A}(K/k) = \left(\frac{s}{2}\right) - \text{rank of } \Delta_\ell(K/k). \]

Then we have

THEOREM 5.6. Suppose that $\ell \neq \text{char}(k)$ and $\ell \nmid q - 1$. Let $K$ be the maximal abelian $\ell$-extension with conductor $m = p_1 p_2 \cdots p_s$. Then the ideal class number $h(\mathcal{O}_K)$ of $\mathcal{O}_K$ is prime to $\ell$ in exactly the following cases;
(i) $m = p_1$.
(ii) $m = p_1 p_2$ and $X^\ell \equiv p_1 \mod p_2$ or $X^\ell \equiv p_2 \mod p_1$ is not solvable.
(iii) $m = p_1 p_2 p_3$ with
\[ \det \begin{pmatrix} -\epsilon_{1,2} & -\epsilon_{1,3} & 0 \\ \epsilon_{2,1} & 0 & -\epsilon_{2,3} \\ 0 & \epsilon_{3,1} & \epsilon_{3,2} \end{pmatrix} \neq 0. \]

Moreover if $s > 3$, then $\ell \mid h(\mathcal{O}_K)$.

References


Present Address:
Department of Mathematics, KAIST,
Taejon, 305–701 Korea.