TOKYO J. MATH.
VOL. 24, NO. 1, 2001

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 $k = \mathbf{F}_q(T)$ be the rational function field over finite field $\mathbf{F}_q$, where $q = p^f$, $p = \mathrm{char}(k)$ and $A = \mathbf{F}_q[T]$. For any monic polynomial $\mathfrak{m} \in A$, let $k(\Lambda_{\mathfrak{m}})$ be the $\mathfrak{m}$-th cyclotomic function field and $k(\Lambda_{\mathfrak{m}})^+$ 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 $k(\Lambda_{\mathfrak{m}})$ and $k(\Lambda_{\mathfrak{m}})^+$, and find lower bounds for the ℓ-rank of ideal class groups of $k(\Lambda_{\mathfrak{m}})$ and $k(\Lambda_{\mathfrak{m}})^+$.

1. Central class field and Genus field.

Let k be a global function field over a finite field $\mathbf{F}_q$. Let ∞ be a place of degree 1 of k and $\mathcal{O}_k$ the ring of regular elements outside ∞ of k. Let E_k be the unit group of $\mathcal{O}_k$, which is just $\mathbf{F}_q^*$. We write k_∞ to be the completion of k at ∞. We fix a sing function $sgn : k_\infty^* \to \mathbf{F}_q^*$ and choose a uniformizer π of k_∞ with $sgn(\pi) = 1$. Denote by $\tilde{C}$ the field $k_\infty(\sqrt[q-1]{-\pi})$. In the following we mean by an extension of k, a separable extension of k for which any embeddings into k_∞^{ac} lies in $\tilde{C}$ viewing as a subfield of k_∞^{ac}.

Received October 19, 1999
Revised March 21, 2000
Supported in part by Non Directed Research Fund, Korea Research Foundation, 1999.

Let K be a finite Galois extension of k and $S_\infty(K)$ the set of places of K lying above ∞. 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_∞ in $\tilde{C}$. Let N_v be the norm map from K_v to k_∞. Define a sign map

$$sgn_v : K_v^* \to \mathbf{F}_q^*$$

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. Similary 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

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

and

$$\begin{aligned}\mathcal{B}(K/k) &= (k^* \cap (N_{K/k}U(K)N_{K/k}K^*))/N_{K/k}K^* \\ &= E_k \cap N_{K/k}J(K)/E_k \cap N_{K/k}K^*.\end{aligned}$$

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

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

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 ℓ, then $K = Z(K/k)$ (resp. $K = Z_+(K/k)$) if and only if the ℓ-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, $\mathcal{A}(K/k)$ 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 ℓ, where ℓ is a prime number. Let $G = Gal(K/k)$ and X_G be the group of characters of G. If $[K:k] = \ell^r$, we may view G and $\bigwedge^2 G$ as $\mathbf{F}_\ell$-vector space of dimension r and $\binom{r}{2}$, respectively. Let $\{\chi_1, \chi_2 \cdots, \chi_r\}$ be a basis of X_G over $\mathbf{F}_\ell$. Let $\mathcal{S}$ be the set of all finite primes of k which ramify on K. For each prime $\mathfrak{p} \in \mathcal{S}$, let $\{\mathfrak{g}_1, \mathfrak{g}_2 \cdots, \mathfrak{g}_s\}$ be a basis of the decomposition group $G_\mathfrak{p}$ over $\mathbf{F}_\ell$. Let $[\delta_{tu,\alpha\beta}]_\mathfrak{p}$ be the matrix over $\mathbf{F}_\ell$ 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;

$$(\chi_\alpha \wedge \chi_\beta)(\mathfrak{g}_t \wedge \mathfrak{g}_u) = \zeta_\ell^{\delta_{tu,\alpha\beta}},$$

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

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

(i) *HNP holds for K/k.*
(ii) *$\mathcal{A}(K/k)$ has trivial ℓ-rank.*
(iii) *$\Delta(K/k)$ has rank $r(r-1)/2$, where r is the ℓ-rank of $Gal(K/k)$.*

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 $k(\Lambda_\mathfrak{m})/k$.

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

$$(*) \qquad \mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_z^{e_z},$$

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

If $z = 1$ in (*), then $\mathfrak{p}_1$ is the only finite prime of k which ramify (in fact, totally) in $k(\Lambda_\mathfrak{m})$. So the decomposition group $G_{\mathfrak{p}_1}$ of $\mathfrak{p}_1$ is all of G and so HNP holds for $k(\Lambda_\mathfrak{m})/k$.

If $z \geq 4$ in (*), then $z < z(z-1)/2$. Since 2-rank of $Gal(k(\Lambda_\mathfrak{m})/k)$ is z, $\Delta_2(\mathfrak{m})$ has at most z rows. So HNP does not hold for $k(\Lambda_\mathfrak{m})_2/k$ and also for $k(\Lambda_\mathfrak{m})/k$, by Proposition 2.1.

It remains to consider the cases: $z = 2$ and $z = 3$.

THEOREM 3.1. *Let $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$. Then HNP holds for $k(\Lambda_\mathfrak{m})/k$ if and only if the following conditions are satisfied*;

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

$$X^\ell \equiv \mathfrak{p}_1 \bmod \mathfrak{p}_2$$

or

$$X^{\ell} \equiv \mathfrak{p}_2 \bmod \mathfrak{p}_1$$

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*

$$X^p \equiv \mathfrak{p}_j \bmod \mathfrak{p}_i^2 \quad (j \neq i)$$

is not solvable.

PROOF. By Proposition 2.2, we need to consider the validity of HNP for $k(\Lambda_{\mathfrak{m}})_\ell/k$ for each prime number ℓ.

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

For a prime divisor ℓ of $(q^{d_1} - 1, q^{d_2} - 1)$, $G = Gal(k(\Lambda_{\mathfrak{m}})_\ell/k) \simeq (\mathbf{Z}/\ell\mathbf{Z})^2$. Let χ_i be a multiplicative character on the inertia group $T_{\mathfrak{p}_i}$ of order ℓ, $\mathfrak{t}_i$ an element of $T_{\mathfrak{p}_i}$ dual to χ_i, and σ_{ij} the Frobenius automorphism at the prime $\mathfrak{p}_i$ in the extension $k(\Lambda_{\mathfrak{p}_j})$. Define $\varepsilon_{i,j}^{(\ell)} \in \mathbf{F}_\ell$ $(i \neq j)$ as $\chi_i(\sigma_{ji}) = \zeta_\ell^{\varepsilon_{i,j}^{(\ell)}}$, where ζ_ℓ is a fixed primitive ℓ-th root of unity. We use $\varepsilon_{i,j}$ for $\varepsilon_{i,j}^{(\ell)}$ for simplicity where no confusion arises. Then the matrix $\Delta_\ell(\mathfrak{m})$ is given as

$$\begin{pmatrix} \varepsilon_{2,1} \\ -\varepsilon_{1,2} \end{pmatrix},$$

by taking a basis $\{\mathfrak{t}_i, \sigma_{ij}\}$ of $G_{\mathfrak{p}_i}$. So $\Delta_\ell(\mathfrak{m})$ 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 $X^\ell \equiv \mathfrak{p}_j \mod \mathfrak{p}_i$ is not solvable.

Now we consider the case $\ell = p$. If $e_i = 1$ for some i, then $k(\Lambda_{\mathfrak{m}})_p = k(\Lambda_{\mathfrak{p}_j^{e_j}})_p$ $(j \neq i)$ 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 $Gal(k(\Lambda_{\mathfrak{p}_i^{e_i}})/k)$ 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 $T_{\mathfrak{p}_i}$ be the inertia group of $\mathfrak{p}_i$ in $G = Gal(k(\Lambda_{\mathfrak{m}})_p/k)$. Then $G = T_{\mathfrak{p}_1} T_{\mathfrak{p}_2}$, so p-rank of G is $r = r_1 + r_2$. Since $G_{\mathfrak{p}_i}/T_{\mathfrak{p}_i}$ is a cyclic group, p-rank of $G_{\mathfrak{p}_i}$ is r_i or $r_i + 1$. Hence p-rank of $H^{-3}(G_{\mathfrak{p}_i}, \mathbf{Z})$ is $\binom{r_i}{2}$ or $\binom{r_i+1}{2}$ and

$$p\text{-rank of } \mathcal{A}(k(\Lambda_{\mathfrak{m}})_p/k) \geq \binom{r}{2} - \sum_{i=1}^{2} \binom{r_i + 1}{2}.$$

Hence HNP holds for $k(\Lambda_{\mathfrak{m}})p/k$ only if $r_1 r_2 - (r_1 + r_2) \leq 0$. 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 $T_{\mathfrak{p}_1}$ over $\mathbf{F}_p$ and $\{\chi_{2,1}, \chi_{2,2}\}$ basis of the dual group of $T_{\mathfrak{p}_2}$ over $\mathbf{F}_p$. Then with respect to the basis $\{\chi_{1,1} \wedge \chi_{1,2}, \chi_{1,1} \wedge \chi_{2,1}, \chi_{1,1} \wedge \chi_{2,2}, \chi_{1,2} \wedge \chi_{2,1}, \chi_{1,2} \wedge \chi_{2,2}, \chi_{2,1} \wedge \chi_{2,2}\}$, by choosing suitable bases of $G_{\mathfrak{p}_i}$'s the matrix $\Delta_p(\mathfrak{m})$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & [\mathfrak{p}_1, \chi_{2,1}] & [\mathfrak{p}_1, \chi_{2,2}] & 0 & 0 & 0 \\ 0 & 0 & 0 & [\mathfrak{p}_1, \chi_{2,1}] & [\mathfrak{p}_1, \chi_{2,2}] & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -[\mathfrak{p}_2, \chi_{1,1}] & 0 & -[\mathfrak{p}_2, \chi_{1,2}] & 0 & 0 \\ 0 & 0 & -[\mathfrak{p}_2, \chi_{1,1}] & 0 & -[\mathfrak{p}_2, \chi_{1,2}] & 0 \end{pmatrix},$$

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

$$\begin{aligned} &\det(\Delta_p(\mathfrak{m})) \\ &\quad = -[\mathfrak{p}_1, \chi_{2,1}][\mathfrak{p}_1, \chi_{2,2}][\mathfrak{p}_2, \chi_{1,1}][\mathfrak{p}_2, \chi_{1,2}] + [\mathfrak{p}_1, \chi_{2,2}][\mathfrak{p}_1, \chi_{2,1}][\mathfrak{p}_2, \chi_{1,1}][\mathfrak{p}_2, \chi_{1,2}] \\ &\quad = 0, \end{aligned}$$

HNP does not hold for $K(\Lambda_{\mathfrak{m}})_p/K$.

When $r_i = 1$ and $r_j \geq 1$ arbitary, clearly we have $q = p$ and $d_i = 1, e_i = 2$. In this case, $T_{\mathfrak{p}_i} \simeq \mathbf{Z}/p\mathbf{Z}$ and $T_{\mathfrak{p}_j} \simeq (\mathbf{Z}/p\mathbf{Z})^{r_j}$. Let χ_1 be a character modulo $\mathfrak{p}_i^2$ of order p and $\{\chi_{2,1}, \chi_{2,2} \cdots, \chi_{2,r_j}\}$ be a basis of dual group of $T_{\mathfrak{p}_j}$. With respect to the basis $\{\chi_1 \wedge \chi_{2,1}, \chi_1 \wedge \chi_{2,2} \cdots, \chi_1 \wedge \chi_{2,r_j}, \chi_{2,1} \wedge \chi_{2,2} \cdots, \chi_{2,r_{j-1}} \wedge \chi_{2,r_j}\}$, again by choosing suitable bases for $G_{\mathfrak{p}_i}$'s the matrix $\Delta_p(\mathfrak{m})$ is given by

$$\begin{pmatrix} [\mathfrak{p}_i, \chi_{2,1}] & [\mathfrak{p}_i, \chi_{2,2}] & \cdots & [\mathfrak{p}_i, \chi_{2,r_j}] & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \\ -[\mathfrak{p}_j, \chi_1] & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & -[\mathfrak{p}_j, \chi_1] & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -[\mathfrak{p}_j, \chi_1] & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

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

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

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

where ζ_ℓ is a fixed primitive ℓ-th root of unity. From the ℓ-th reciprocity law

$$\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)_\ell \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)_\ell^{-1} = (-1)^{\frac{q-1}{\ell} \deg(\mathfrak{p}) \deg(\mathfrak{q})},$$

we see that $[\mathfrak{q}, \mathfrak{p}]_\ell = [\mathfrak{p}, \mathfrak{q}]_\ell$, except the case that $q \equiv 3 \bmod 4$, $\ell = 2$ and $\deg(\mathfrak{p}), \deg(\mathfrak{q}) \equiv 1 \bmod 2$. And in this exceptional case, we have $[\mathfrak{q}, \mathfrak{p}]_2 = [\mathfrak{p}, \mathfrak{q}]_2 + 1$.

THEOREM 3.2. *Let* $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$. *Then HNP holds for* $k(\Lambda_{\mathfrak{m}})/k$ *if and only if the following conditions are satisfied;*

(i) $q = 3$

(ii) $[\mathfrak{p}_1, \mathfrak{p}_3]_2[\mathfrak{p}_2, \mathfrak{p}_1]_2[\mathfrak{p}_3, \mathfrak{p}_2]_2 \neq [\mathfrak{p}_1, \mathfrak{p}_2]_2[\mathfrak{p}_3, \mathfrak{p}_1]_2[\mathfrak{p}_2, \mathfrak{p}_3]_2$

(iii) *For any odd prime divisor* ℓ *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 χ_i *denote a character of* $T_{\mathfrak{p}_i}$ *of order* ℓ *and* $\varepsilon_{i,j} \in \mathbf{F}_\ell$ $(i \neq j)$ *is defined as* $\chi_i(\mathfrak{p}_j) = \zeta_\ell^{\varepsilon_{i,j}}$, *and* ζ_ℓ *is a fixed primitive* ℓ*-th root of unity.*

(iv) *For odd prime number* ℓ *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*

$$X^\ell \equiv \mathfrak{p}_i \bmod \mathfrak{p}_j \quad or \quad X^\ell \equiv \mathfrak{p}_j \bmod \mathfrak{p}_i$$

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* $X^p \equiv \mathfrak{p}_k \bmod \mathfrak{p}_j^2$ *is not solvable.*

PROOF. For each prime divisor ℓ of $q - 1$, let χ_i be the character defined by $\left(\frac{}{\mathfrak{p}_i}\right)_\ell$. With respect to the basis $\{\chi_1 \wedge \chi_2, \chi_1 \wedge \chi_3, \chi_2 \wedge \chi_3\}$, the matrix $\Delta_\ell(\mathfrak{m})$ is given by

$$\begin{pmatrix} [\mathfrak{p}_2, \mathfrak{p}_1]_\ell & [\mathfrak{p}_3, \mathfrak{p}_1]_\ell & 0 \\ -[\mathfrak{p}_1, \mathfrak{p}_2]_\ell & 0 & [\mathfrak{p}_3, \mathfrak{p}_2]_\ell \\ 0 & -[\mathfrak{p}_1, \mathfrak{p}_3]_\ell & -[\mathfrak{p}_2, \mathfrak{p}_3]_\ell \end{pmatrix},$$

and its determinant

$$\det(\Delta_\ell(\mathfrak{m})) = [\mathfrak{p}_2, \mathfrak{p}_1]_\ell[\mathfrak{p}_3, \mathfrak{p}_2]_\ell[\mathfrak{p}_1, \mathfrak{p}_3]_\ell - [\mathfrak{p}_1, \mathfrak{p}_2]_\ell[\mathfrak{p}_3, \mathfrak{p}_1]_\ell[\mathfrak{p}_2, \mathfrak{p}_3]_\ell .$$

Note that $q = 3$ is the only one such that $q \equiv 3 \bmod 4$ and 2 is the unique prime divisor. Except the case that $q = 3$, $\ell = 2$, $\det(\Delta_\ell(\mathfrak{m})) = 0$ hence HNP does not hold for $k(\Lambda_{\mathfrak{m}})_\ell/k$. Thus we must have $q = 3$ and so we get (i) and (ii).

For (iii), we only replace the ℓ-th reciprocity symbol $\left(\frac{}{\mathfrak{p}_i}\right)_\ell$ by a character χ_i modulo $\mathfrak{p}_i$ of order ℓ 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 $G_{\mathfrak{p}_i}$ of $\mathfrak{p}_i$ is all of $G = Gal(k(\Lambda_{\mathfrak{m}})_p/k)$. So HNP always holds for $k(\Lambda_{\mathfrak{m}})_p/k$.

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 $\mathfrak{p}_i$ in $G = Gal(k(\Lambda_{\mathfrak{m}})_p/k)$. Then $G = T_{\mathfrak{p}_1}T_{\mathfrak{p}_2}T_{\mathfrak{p}_3}$ so p-rank of G is $r = r_1 + r_2 + r_3$. Since $G_{\mathfrak{p}_i}/T_{\mathfrak{p}_i}$ is a cyclic group,

p-rank of $G_{\mathfrak{p}_i}$ is r_i or r_i+1. Hence p-rank of $H^{-3}(G_{\mathfrak{p}_i}, \mathbf{Z})$ is $\binom{r_i}{2}$ or $\binom{r_i+1}{2}$ and

$$p\text{-rank of } \mathcal{A}(k(\Lambda_{\mathfrak{m}})_p/k)) \geq \binom{r}{2} - \sum_{i=1}^{3}\binom{r_i+1}{2} = (r_1r_2 + r_1r_3 + r_2r_3) - (r_1 + r_2 + r_3)\,.$$

Thus HNP holds for $k(\Lambda_{\mathfrak{m}})_p/k$ 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 $(\mathbf{F}_p[T]/\mathfrak{p}_i^2)^*$ can be written uniquely as $c_0(1 + c_1\mathfrak{p}_i) \bmod \mathfrak{p}_i^2$, where $c_0, c_1 \in \mathbf{F}_p$, and $\chi_i\ (c_0(1 + c_1\mathfrak{p}_i \bmod \mathfrak{p}_i^2) = c_1$ 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 $\Delta_3(\mathfrak{m})$ is given by,

$$\begin{pmatrix} (\mathfrak{p}_1 - \mathfrak{p}_2)^{-1} & (\mathfrak{p}_1 - \mathfrak{p}_3)^{-1} & 0 \\ -(\mathfrak{p}_2 - \mathfrak{p}_1)^{-1} & 0 & (\mathfrak{p}_2 - \mathfrak{p}_3)^{-1} \\ 0 & -(\mathfrak{p}_3 - \mathfrak{p}_1)^{-1} & -(\mathfrak{p}_3 - \mathfrak{p}_2)^{-1} \end{pmatrix},$$

and its determinant $\det(\Delta_3(\mathfrak{m}))$ is

$$(\mathfrak{p}_1 - \mathfrak{p}_2)^{-1}(\mathfrak{p}_2 - \mathfrak{p}_3)^{-1}(\mathfrak{p}_3 - \mathfrak{p}_1)^{-1} - (\mathfrak{p}_2 - \mathfrak{p}_1)^{-1}(\mathfrak{p}_1 - \mathfrak{p}_3)^{-1}(\mathfrak{p}_3 - \mathfrak{p}_2)^{-1}$$

which is not zero. Here we note that $\mathfrak{p}_i - \mathfrak{p}_j$ is an element of $\mathbf{F}_p^*$, since $\mathfrak{p}_i$ and $\mathfrak{p}_j$ 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 $\mathfrak{p}_i$'s is even.

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

Let $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_z^{e_z}$ be as before. First we note that $k(\Lambda_{\mathfrak{m}})_\ell^+ = k(\Lambda_{\mathfrak{m}})_\ell$, for any prime number $\ell \nmid q-1$. Thus it suffices to consider $k(\Lambda_{\mathfrak{m}})_\ell^+$ for $\ell \mid q-1$; We will write $\Delta_\ell(\mathfrak{m})^+$ for $\Delta(k(\Lambda_{\mathfrak{m}})_\ell^+/k)$.

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

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

LEMMA 4.1. *Suppose that* $d_1, d_2 \not\equiv 0 \bmod \ell$. *Then* $k\big(\sqrt[\ell]{\mathfrak{p}_1{}^{n_1}\mathfrak{p}_2{}^{(\ell-1)n_2}}\big)$ *is the unique cyclic extension of degree* ℓ *over* k *contained in* $k(\Lambda_{\mathfrak{p}_1\mathfrak{p}_2})^+$. $\left(\frac{\ }{\mathfrak{p}_1}\right)_\ell^{n_1}\left(\frac{\ }{\mathfrak{p}_2}\right)_\ell^{-n_2}$ *defines a character of* $Gal\big(k\big(\sqrt[\ell]{\mathfrak{p}_1{}^{n_1}\mathfrak{p}_2{}^{(\ell-1)n_2}}\big)/k\big)$ *of order* ℓ.

PROOF. By Lemma 3.2([A]), we see that $k\big(\sqrt[\ell]{\mathfrak{p}_1{}^{n_1}\mathfrak{p}_2{}^{(\ell-1)n_2}}\big)$ is contained in $k(\Lambda_{\mathfrak{p}_1\mathfrak{p}_2})$. Since $\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{(\ell-1)n_2}$ is monic and its degree satisfies $n_1d_1 + (\ell-1)n_2d_2 \equiv 0 \bmod \ell$,

$$k(\sqrt[\ell]{\mathfrak{p}_1{}^{n_1}\mathfrak{p}_2{}^{(\ell-1)n_2}}) \subset k(\Lambda_{\mathfrak{p}_1\mathfrak{p}_2})^+\,.$$

From the Chinese remainder theorem $\left(\frac{}{\mathfrak{p}_1}\right)_\ell^{n_1}\left(\frac{}{\mathfrak{p}_2}\right)_\ell^{-n_2}$ is nontrivial and so has order ℓ. Now it suffices to show that $\left(\frac{c}{\mathfrak{p}_1}\right)_\ell^{n_1}\left(\frac{c}{\mathfrak{p}_2}\right)_\ell^{-n_2} = 1$ for any $c \in \mathbf{F}_q^*$. But it follows from the formula

$$\left(\frac{c}{\mathfrak{p}}\right)_\ell = c^{\frac{q-1}{\ell}\deg \mathfrak{p}},$$

for any monic irreducible polynomial $\mathfrak{p}$ and $c \in \mathbf{F}_q^*$. □

If $d_1, d_2, \cdots, d_i \not\equiv 0 \bmod \ell$ and $d_{i+1}, \cdots, d_z \equiv 0 \bmod \ell$, then by Lemma 4.1, we see that

$$k(\Lambda_{\mathfrak{m}})_\ell^+ = k\left(\sqrt[\ell]{\mathfrak{p}_1{}^{n_1}\mathfrak{p}_2{}^{(\ell-1)n_2}}, \cdots, \sqrt[\ell]{\mathfrak{p}_1{}^{n_1}\mathfrak{p}_i{}^{(\ell-1)n_i}}, \sqrt[\ell]{\mathfrak{p}_{i+1}}, \cdots, \sqrt[\ell]{\mathfrak{p}_z}\right),$$

so its Galois group has ℓ-rank $z-1$.

Clearly as in $k(\Lambda_{\mathfrak{m}})$, if $z = 1$, then HNP holds for $k(\Lambda_{\mathfrak{m}})^+/K$. If $z \geq 5$, then $Gal(k(\Lambda_{\mathfrak{m}})_2^+/k)$ has 2-rank at least $z-1 \geq 4$. So HNP does not hold for $k(\Lambda_{\mathfrak{m}})_2^+/k$.

It remains to consider: $z = 2$, $z = 3$ and $z = 4$.

THEOREM 4.2. *Let $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$. Then HNP holds for $k(\Lambda_{\mathfrak{m}})^+/k$ if and only if the following conditions are satisfied;*

(i) *For a prime number $\ell \nmid q-1$, HNP holds for $k(\Lambda_{\mathfrak{m}})_\ell/k$.*

(ii) *For a prime number $\ell \mid q-1$, if $d_1 \equiv d_2 \equiv 0 \mod \ell$, then*

$$\left(\frac{\mathfrak{p}_2}{\mathfrak{p}_1}\right)_\ell \neq 1 \quad or \quad \left(\frac{\mathfrak{p}_1}{\mathfrak{p}_2}\right)_\ell \neq 1.$$

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

THEOREM 4.3. *Let $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$. Then HNP holds for $k(\Lambda_{\mathfrak{m}})^+/k$ if and only if the following conditions are satisfied;*

(i) *For a prime number $\ell \nmid q-1$, HNP holds for $k(\Lambda_{\mathfrak{m}})_\ell/k$.*

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

(1) *if $d_i \not\equiv 0 \bmod \ell$ and $d_j \equiv d_k \equiv 0 \bmod \ell$, then $\left(\frac{\mathfrak{p}_j}{\mathfrak{p}_k}\right)_\ell \neq 1$.*

(2) *if $d_i, d_j \not\equiv 0 \bmod \ell$ and $d_k \equiv 0 \bmod \ell$, then $\left(\frac{\mathfrak{p}_i}{\mathfrak{p}_k}\right)_\ell \neq 1$ or $\left(\frac{\mathfrak{p}_j}{\mathfrak{p}_k}\right)_\ell \neq 1$.*

(3) *if $d_1, d_2, d_3 \not\equiv 0 \bmod \ell$ then $n_2\varepsilon_{2,1} \neq n_3\varepsilon_{3,1}$, $n_2\varepsilon_{1,2} \neq n_3\varepsilon_{3,2}$ or $n_1\varepsilon_{1,3} \neq n_2\varepsilon_{2,3}$. Here $\varepsilon_{i,j}$ is given as in Theorem 3.2.*

PROOF. For a prime number $\ell \mid q-1$, if d_1, d_2 and d_3 are all divisible by ℓ, then $k(\Lambda_{\mathfrak{m}})_\ell^+ = k(\Lambda_{\mathfrak{m}})_\ell$ for which HNP does not hold (Theorem 3.2).

When $d_i \not\equiv 0 \bmod \ell$ and $d_j \equiv d_k \equiv 0 \bmod \ell, k(\Lambda_{\mathfrak{m}})_\ell^+ = k(\Lambda_{\mathfrak{m}})_\ell = k(\sqrt[\ell]{\mathfrak{p}_j}, \sqrt[\ell]{\mathfrak{p}_k})$. Since $\left(\frac{\mathfrak{p}_k}{\mathfrak{p}_j}\right)_\ell = \left(\frac{\mathfrak{p}_j}{\mathfrak{p}_k}\right)_\ell$, we get the condition as (ii) in Theorem 3.1.

When $d_i, d_j \not\equiv 0 \bmod \ell$ and $d_k \equiv 0 \bmod \ell$, $k(\Lambda_{\mathfrak{m}})_\ell^+ = k\left(\sqrt[\ell]{\mathfrak{p}_i^{n_i}\mathfrak{p}_j{}^{(\ell-1)n_i}}, \sqrt[\ell]{\mathfrak{p}_k}\right)$. Let $\chi_{i,j}$ be the character defined by $\left(\frac{}{\mathfrak{p}_i}\right)_\ell^{n_i}\left(\frac{}{\mathfrak{p}_j}\right)_\ell^{-n_j}$ and χ_k be characters defined by $\left(\frac{}{\mathfrak{p}_k}\right)_\ell$. With respect to $\chi_{i,j} \wedge \chi_k$, $\Delta_\ell^+(\mathfrak{m})$ is given by

$$\begin{pmatrix} \varepsilon_{k,i} \\ -\varepsilon_{k,j} \\ -n_i\varepsilon_{i,k} + n_j\varepsilon_{j,k} \end{pmatrix}.$$

Since $d_k \equiv 0 \bmod \ell$, $\varepsilon_{k,i} = \varepsilon_{i,k}$, $\varepsilon_{j,k} = \varepsilon_{k,j}$ and so $\Delta_\ell^+(\mathfrak{m})$ has rank 1 if and only if $\varepsilon_{k,i} \neq 0$ or $\varepsilon_{k,j} \neq 0$.

When $d_1, d_2, d_3 \not\equiv 0 \mod \ell$, $k(\Lambda_\mathfrak{m})_\ell^+ = k\big(\sqrt[\ell]{\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{(\ell-1)n_2}}, \sqrt[\ell]{\mathfrak{p}_1^{n_1}\mathfrak{p}_3^{(\ell-1)n_3}}\big)$. Let $\chi_{i,j}$ be the character defined by $\big(\frac{}{\mathfrak{p}_i}\big)_\ell^{n_i}\big(\frac{}{\mathfrak{p}_j}\big)_\ell^{-n_i}$. 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 $\Delta_\ell^+(\mathfrak{m})$ is given by

$$\begin{pmatrix} n_2\varepsilon_{2,1} - n_3\varepsilon_{3,1} \\ -n_1\varepsilon_{1,2} + n_3\varepsilon_{3,2} \\ n_1\varepsilon_{1,3} - n_2\varepsilon_{2,3} \end{pmatrix}.$$

So we get the condition. □

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

THEOREM 4.4. *Let $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}\mathfrak{p}_4^{e_4}$. Then HNP holds for $k(\Lambda_\mathfrak{m})^+/k$ 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 $\ell \mid q - 1$, at least two of d_1, d_2, d_3 and d_4 are not divisible by ℓ.*

(1) *If $d_i, d_j \not\equiv 0 \bmod \ell$ and $d_k, d_m \equiv 0 \bmod \ell$, then*

$$\left(\frac{\mathfrak{p}_m}{\mathfrak{p}_k}\right)_\ell \neq 1 \quad \textit{and} \quad \varepsilon_{i,k}\varepsilon_{j,m} \neq \varepsilon_{i,m}\varepsilon_{j,k}\,.$$

(2) *If $d_i, d_j, d_k \not\equiv 0 \bmod \ell$ and $d_m \equiv 0 \bmod \ell$, then except the case that $q \equiv 3 \mod 4$, $\ell = 2$,*

$$n_j(\varepsilon_{i,j}\varepsilon_{j,m}\varepsilon_{k,m}) - n_k(\varepsilon_{i,k}\varepsilon_{j,m}\varepsilon_{k,m}) - n_i(\varepsilon_{i,j}\varepsilon_{i,m}\varepsilon_{k,m}) + n_k(\varepsilon_{j,k}\varepsilon_{i,m}\varepsilon_{k,m}) \neq 0\,.$$

In the case that $q \equiv 3 \bmod 4$, $\ell = 2$,

$$\varepsilon_{i,m}\varepsilon_{j,m} \neq 0\,, \quad \varepsilon_{i,m}\varepsilon_{k,m} \neq 0 \quad or \quad \varepsilon_{j,m}\varepsilon_{k,m} \neq 0\,.$$

(3) *If $d_1, d_2, d_3, d_4 \not\equiv 0 \bmod \ell$, then except the case that $q \equiv 3 \bmod 4$, $\ell = 2$,*

$$\begin{aligned}(n_1\varepsilon_{1,2} - n_3\varepsilon_{1,3})&(-n_1\varepsilon_{1,2} + n_4\varepsilon_{2,4})(-n_1\varepsilon_{1,3} + n_4\varepsilon_{3,4}) \\ &+ (n_1\varepsilon_{1,2} - n_3\varepsilon_{2,3})(n_2\varepsilon_{1,2} - n_4\varepsilon_{1,4})(-n_1\varepsilon_{1,3} + n_4\varepsilon_{3,4}) \\ &+ (n_1\varepsilon_{1,3} - n_2\varepsilon_{2,3})(n_3\varepsilon_{1,3} - n_4\varepsilon_{1,4})(n_1\varepsilon_{1,2} - n_4\varepsilon_{2,4}) \neq 0\,.\end{aligned}$$

In the case that $q \equiv 3 \bmod 4$, $\ell = 2$,

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

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* $K(\Lambda_{\mathfrak{p}_i^{e_i}\mathfrak{p}_j^{e_j}\mathfrak{p}_k^{e_k}})_\ell/K$, *for any* $\{i, j, k\} \subset \{1, 2, 3, 4\}$.

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

(i) $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$; *There exist a prime number* $\ell \mid q-1$ *such that* $d_i \not\equiv 0 \bmod \ell$ *for one* i *and* $\left(\frac{\mathfrak{p}_2}{\mathfrak{p}_1}\right)_\ell = \left(\frac{\mathfrak{p}_1}{\mathfrak{p}_2}\right)_\ell = 1$.

(ii) $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$;

(1) *When* $q \neq 3$, *HNP always dose not hold for* $k(\Lambda_{\mathfrak{m}})/k$.

(2) *When* $q = 3$, *and if* $d_1 \equiv d_2 \equiv d_3 \equiv 1 \bmod 2$, $\left(\frac{\mathfrak{p}_2}{\mathfrak{p}_1}\right)_2 = \left(\frac{\mathfrak{p}_3}{\mathfrak{p}_2}\right)_2 = \left(\frac{\mathfrak{p}_1}{\mathfrak{p}_3}\right)_2$ *dose not hold.*

(3) *When* $q = 3$, *and if* $d_i \equiv d_j \equiv 1 \bmod 2$ *and* $d_k \equiv 0 \bmod 2$, $\left(\frac{\mathfrak{p}_i}{\mathfrak{p}_k}\right)_2 \neq \left(\frac{\mathfrak{p}_j}{\mathfrak{p}_k}\right)_2$.

(iii) $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}\mathfrak{p}_4^{e_4}$; *HNP always dose not hold for* $k(\Lambda_{\mathfrak{m}})/k$.

5. Ideal Class Groups.

Let ℓ be a prime. For a finite abelian ℓ-extension K of k, we say that it is maximal if it is the maximal ℓ-extension of k in $k(\Lambda_{\mathfrak{m}})$, where $\mathfrak{m}$ is the conductor of K. By the conductor $\mathfrak{m}$ of K, we mean the smallest monic polynomial $\mathfrak{m}$ such that K is contained in $k(\Lambda_{\mathfrak{m}})$. From now on we assume that K is a maximal abelian ℓ-extension of k with conductor $\mathfrak{m}$, say $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ and $\Gamma = Gal(K/k)$. Let K_i be the maximal abelian ℓ-extension of k in $k(\Lambda_{\mathfrak{p}_i^{e_i}})$. Then K is the composite of those K_i. For each i, let T_i and Γ_i be the inertia group and decomposition group of $\mathfrak{p}_i$ in K, respectively. Clearly $\Gamma = \prod T_i$. If $\ell \neq char(k)$, $\mathfrak{m}$ must be square free with $q^{\deg(\mathfrak{p}_i)} \equiv 1 \bmod \ell$ and each inertia group $T_i \simeq Gal(K_i/k) \simeq \mathbf{Z}/\ell^{a_i}$, where a_i is the maximal exponent of ℓ which divides $q^{\deg(\mathfrak{p}_i)} - 1$. 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

$$\delta_i = f \times \deg(\mathfrak{p}_i) \times \left(e_i - 1 - \left[\frac{e_i - 1}{p}\right]\right),$$

where $q = p^f$.

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

PROPOSITION 5.1. *Let K be as above. Then*

(i) $\ell \neq char(k)$;

$$r_\ell(Cl(\mathcal{O}_K)) \geq \frac{s(s-3)}{2} - \varepsilon_\ell\,,$$

where $\varepsilon_\ell = 1$ *if* $\ell \mid q-1$ *and otherwise* $\varepsilon_\ell = 0$.

(ii) $\ell = p = char(k)$;

$$r_\ell(Cl(\mathcal{O}_K)) \geq \sum_{i<j} \delta_i \delta_j - \sum_i \delta_i\,.$$

COROLLARY 5.2. *Let* $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ *and denote* $\mathcal{O}_\mathfrak{m} = \mathcal{O}_{k(\Lambda_\mathfrak{m})}$. *For* $\ell \neq char(k)$, *let* t_ℓ *be the number of* $\mathfrak{p}_i$ *such that* $q^{\deg(\mathfrak{p}_i)} \equiv 1 \mod \ell$. *Then*

(i) $\ell \neq char(k)$;

$$r_\ell(Cl(\mathcal{O}_\mathfrak{m})) \geq \frac{t_\ell(t_\ell-3)}{2} - \varepsilon_\ell\,,$$

where ε_ℓ *is defined as in Proposition* 5.1.

(ii) $\ell = p = char(k)$;

$$r_\ell(Cl(\mathcal{O}_\mathfrak{m})) \geq \sum_{i<j} \delta_i \delta_j - \sum_i \delta_i\,.$$

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

PROPOSITION 5.3. *Let* $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ *and denote* $\mathcal{O}_\mathfrak{m}^+ = \mathcal{O}_{K(\Lambda_\mathfrak{m})^+}$.

(i) $\ell \neq char(k)$ *and* $\ell \nmid q-1$;

$$r_\ell(Cl(\mathcal{O}_\mathfrak{m}^+)) \geq \frac{t_\ell(t_\ell-3)}{2}\,.$$

(ii) $\ell = p = char(k)$;

$$r_\ell(Cl(\mathcal{O}_\mathfrak{m}^+)) \geq \sum_{i<j} \delta_i \delta_j - \sum_i \delta_i\,.$$

Now suppose that $\ell \mid q-1$. Let ε^+ be the ℓ-rank of $\mathcal{B}(K^+/k)$, i.e. the ℓ-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* ℓ*-extension of* k *with conductor* $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$, *and* $K^+ = K \cap k(\Lambda_\mathfrak{m})^+$.

(i) *If* $\deg(\mathfrak{p}_i) \equiv 0 \bmod \ell$ *for all* i, *then*

$$r_\ell(Cl(\mathcal{O}_{K^+})) \geq \frac{s(s-3)}{2}\,.$$

(ii) *If* $\deg(\mathfrak{p}_i) \not\equiv 0 \bmod \ell$ *for some* i, *then*

$$r_\ell(Cl(\mathcal{O}_{K^+})) \geq \frac{s^2-5s+2}{2}\,.$$

PROOF. In case (i), $k(\sqrt[\ell]{\mathfrak{p}_1}, \cdots, \sqrt[\ell]{\mathfrak{p}_s}) \subset K^+$ and in case (ii) $K = K^+k(\sqrt[\ell]{-\mathfrak{p}_i{}^{n_i}})$, where $n_i \deg \mathfrak{p}_i \equiv 1 \bmod \ell$, 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* $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$.

(i) *If* $\deg(\mathfrak{p}_i) \equiv 0 \bmod \ell$ *for all* i, *then*

$$r_\ell(Cl(\mathcal{O}_{\mathfrak{m}}^+)) \geq \frac{s(s-3)}{2}.$$

(ii) *If* $\deg(\mathfrak{p}_i) \not\equiv 0 \bmod \ell$ *for some* i, *then*

$$r_\ell(Cl(\mathcal{O}_{\mathfrak{m}}^+)) \geq \frac{s^2-5s+2}{2}.$$

Assume that $\ell \neq char(k)$ and $\ell \nmid q-1$. Let K be a maximal abelian ℓ-extension of k with conductor $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$. From the genus number formula (Lemma 1.1), $K = G(K/k)$ and since $\mathcal{B}(K/k)$ is trivial, we have

$$Gal(Z(K/k)/K) \simeq \mathcal{A}(K/k).$$

Let $\Delta_\ell(K/k)$ be the matrix defined in Section 2. Then we have

$$\ell\text{-rank of } \mathcal{A}(K/k) = \binom{s}{2} - \text{rank of } \Delta_\ell(K/k).$$

Then we have

THEOREM 5.6. *Suppose that* $\ell \neq char(k)$ *and* $\ell \nmid q-1$. *Let* K *be the maximal abelian* ℓ*-extension with conductor* $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$. *Then the ideal class number* $h(\mathcal{O}_K)$ *of* $\mathcal{O}_K$ *is prime to* ℓ *in exactly the following cases*;

(i) $\mathfrak{m} = \mathfrak{p}_1$.

(ii) $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2$ *and* $X^\ell \equiv \mathfrak{p}_1 \bmod \mathfrak{p}_2$ *or* $X^\ell \equiv \mathfrak{p}_2 \bmod \mathfrak{p}_1$ *is not solvable.*

(iii) $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ *with*

$$\det\begin{pmatrix} -\varepsilon_{1,2} & -\varepsilon_{1,3} & 0 \\ \varepsilon_{2,1} & 0 & -\varepsilon_{2,3} \\ 0 & \varepsilon_{3,1} & \varepsilon_{3,2} \end{pmatrix} \neq 0.$$

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

References

[A] B. ANGLES, On Hilbert class field towers of global function fields, *Drinfeld modules, modular schemes and applications (Alden-Biesen)*, World Sci. Publishing, (1997), 261–271.

[BK] S. BAE and J. KOO, Genus Theory for Function Fields, J. Austral. Math. Soc. Ser. A **60** (1996), 301–310.

[CaFr] J. W. S. CASSELS and A. FRÖHLICH, *Algebraic Number Theory*, Thompson Book Company, (1967).

[Cl] H. L. CLAASEN, The group of units in $GF(q)[x]/(a(x))$, Indag. Math. **39** (1977), 245–255.

[CoRo] G. CORNELL and M. ROSEN, The ℓ-rank of the real class group of cyclotomic fields, Compositio Math. **53** (1984), 133–141.

[Fr] A. FRÖHLICH, Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields, Contemp. Math. **24** (1983).

[Fu1] Y. FURUTA, The genus field and genus number in algebraic number fields, Nagoya Math. J. **29** (1967) 281–285.

[Fu2] Y. FURUTA, Über die Zentral Klassenzhal eines Relativ-Galoisschen Zhalkorpers, J. Number Theory **3** (1971), 318–322.

[Fu3] Y. FURUTA, On class field towers and the rank of ideal class groups, Nagoya Math. J. **48** (1972), 147–157.

[Ga] D. A. GARBANATI, Invariants of the ideal class group and the Hasse norm theorem, J. Reine Angew. Math. **297** (1978), 159–171.

[Ge1] F. GERTH, The Hasse norm principle for abelian extensions of number fields, Bull. Amer. Math. Soc. **83** (1977), 264–266.

[Ge2] F. GERTH, The Hasse norm principle in cyclotomic number fields, J. Reine Angew. Math. **303/304** (1978), 249–252.

[Gu] S. GURAK, On the Hasse norm principle, J. Reine Angew. Math. **299/300** (1978), 16–27.

[H] D. R. HAYES, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[K] T. KAGAWA, The Hasse norm principle for the maximal real subfields of cyclotomic fields, Tokyo J. Math. **18** (1995), 221–229.

[R] M. RAZAR, Central and Genus Class Fields and the Hasse Norm Theorem, Compositio Math. **35** (1977), 281–298.

Present Address:
DEPARTMENT OF MATHEMATICS. KAIST,
TAEJON, 305–701 KOREA.