PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 118, Number 1, May 1993

THE HASSE NORM PRINCIPLE FOR ELEMENTARY ABELIAN EXTENSIONS

MITSUKO HORIE

(Communicated by William Adams)

Dedicated to the memory of Professor Makoto Ishida

ABSTRACT. Let K/k be an elementary abelian extension of finite algebraic number fields. The Hasse norm principle for K/k and its relation to the Hasse norm principles for all proper subextensions of K/k will be discussed. The central class field of K/k with $k = \mathbb{Q}$ will also be studied.

Let K/k be a Galois extension of finite algebraic number fields. We denote by J_K and J_k the idele groups of K and k, respectively, and we write $N_{K/k}$ for the norm map $J_K \to J_k$. The multiplicative groups $K^\times$ and $k^\times$ are considered, in the usual manner, to be subgroups of J_K and J_k, respectively. The group of global norms $N_{K/k}K^\times$ becomes a subgroup of $N_{K/k}J_K \cap k^\times$ with finite index. We will say that "the Hasse norm principle holds for K/k", when $N_{K/k}J_K \cap k^\times = N_{K/k}K^\times$. The classical Hasse norm theorem asserts that if K/k is a cyclic extension, then the Hasse norm principle holds for K/k. We know that if the Hasse norm principle holds for an abelian extension K/k, then it also holds for each proper subextension F/k of K/k (cf. [6]). However, the converse of this fact is not always true. In fact, there are well-known examples of K/k such that $k = \mathbb{Q}$, the Hasse norm principle does not hold for $K/\mathbb{Q}$, and the proper subfields of K are cyclic over $\mathbb{Q}$ (see [3, 7]). Moreover, when the extension K/k is abelian, the most essential is the case where the Galois group $\mathrm{Gal}(K/k)$ is an elementary abelian group (cf. [2, 6]).

Now, let l be a fixed prime number. Throughout the following, we assume that $\mathrm{Gal}(K/k)$ is an elementary abelian l-group with rank n; $[K:k] = l^n$. For an elementary abelian l-group A and for its subgroups A_1, A_2, we denote by $A_1 \wedge A_2$ the subgroup of the exterior square $\bigwedge^2 A$ of A generated by all elements $a_1 \wedge a_2$ with $a_1 \in A_1$, $a_2 \in A_2$;

$$A_1 \wedge A_2 = \langle a_1 \wedge a_2 \mid a_1 \in A_1,\, a_2 \in A_2 \rangle.$$

Of course we identify $A_1 \wedge A_1$ with the exterior square $\bigwedge^2 A_1$ of A_1, regarding any elementary abelian l-group as a vector space over the finite field $\mathbb{F}_l$ with l

Received by the editors September 3, 1991.
1991 *Mathematics Subject Classification*. Primary 11R20.
Key words and phrases. Hasse norm principle, central extension.

elements. The dual space of each vector space V over $\mathbb{F}_l$ will be denoted by V^*:

$$V^* = \mathrm{Hom}_{\mathbb{F}_l}(V, \mathbb{F}_l).$$

Given any intermediate field F of K/k, we put $X_F = \mathrm{Gal}(F/k)^*$, for the sake of simplicity. We moreover put $G = \mathrm{Gal}(K/k)$, whence $X_K = G^*$. We denote by ι the linear isomorphism from $\bigwedge^2 X_K$ onto $(\bigwedge^2 G)^*$ such that

$$(\iota(\chi \wedge \chi'))(g \wedge g') = \chi(g)\chi'(g') - \chi(g')\chi'(g)$$

for any $\chi, \chi' \in X_K$ and any $g, g' \in G$. For each prime v of k, D_v denotes the decomposition group of v for K/k. Let P denote the set of finite primes of k ramified in K.

In the present paper, we will first prove:

Theorem 1. *Let F be an intermediate field of K/k. Then*

$$(N_{F/k}J_F \cap k^\times)/N_{F/k}F^\times \cong \left(\bigcap_{v\in P}\left(\bigwedge^2 D_v\right)^\perp\right) \cap \iota\left(\bigwedge^2 X_F\right),$$

where $(\bigwedge^2 D_v)^\perp$ is the annihilator of $\bigwedge^2 D_v$ in $(\bigwedge^2 G)^*$.

By means of Theorem 1, we will next prove Theorems 2 and 3 below.

Theorem 2. *Assume that n is odd. Then the Hasse norm principle holds for K/k if and only if it holds for every proper subextension F/k of K/k.*

Theorem 3. *If n is even, then there exist infinitely many examples of K, with $k = \mathbb{Q}$, such that the Hasse norm principle does not hold for $K/\mathbb{Q}$ but does hold for every proper subextension of $K/\mathbb{Q}$.*

1

This section is devoted to proving Theorem 1.

Put $H = \mathrm{Gal}(K/F)$. Let Cor_v denote, for each $v \in P$, the corestriction map

$$H_2(D_vH/H, \mathbb{Z}) \to H_2(G/H, \mathbb{Z}),$$

and let f be the homomorphism

$$\bigoplus_{v\in P} H_2(D_vH/H, \mathbb{Z}) \to H_2(G/H, \mathbb{Z})$$

defined by

$$f\left(\sum_{v\in P} z_v\right) = \sum_{v\in P} \mathrm{Cor}_v\, z_v, \qquad z_v \in H_2(D_vH/H, \mathbb{Z}).$$

Then, it follows from Tate [7, p. 198] that

$$(N_{F/k}J_F \cap k^\times)/N_{F/k}F^\times \cong \mathrm{Coker}\, f$$

(cf. also [4, 5]). Note that the diagram

$$\begin{array}{ccc} H_2(D_vH/H, \mathbb{Z}) & \xrightarrow{\mathrm{Cor}_v} & H_2(G/H, \mathbb{Z}) \\ \downarrow & & \downarrow \\ \bigwedge^2(D_vH/H) & \longrightarrow & \bigwedge^2(G/H) \end{array}$$

is commutative. Here the lower horizontal arrow is the homomorphism induced by the natural injection $D_vH/H \hookrightarrow G/H$, and the vertical arrows are the canonical isomorphisms. Thus, we obtain

$$(N_{F/k}J_F \cap k^\times)/N_{F/k}F^\times \cong \bigcap_{v\in P}\left(\bigwedge^2(D_vH/H)\right)^{\perp_H},$$

where $(\bigwedge^2(D_vH/H))^{\perp_H}$ is the annihilator of $\bigwedge^2(D_vH/H)$ in $(\bigwedge^2(G/H))^*$. Let

$$\pi\colon \bigwedge^2 G \to \bigwedge^2(G/H)$$

be the surjective $\mathbb{F}_l$-linear map induced by the natural map $G \to G/H$. Then π induces an injective $\mathbb{F}_l$-linear map

$$\pi^*\colon \left(\bigwedge^2(G/H)\right)^* \to \left(\bigwedge^2 G\right)^*$$

such that $\pi^*(\alpha) = \alpha \circ \pi$, $\alpha \in (\bigwedge^2(G/H))^*$. In view of

$$\begin{aligned}\dim_{\mathbb{F}_l}(G\wedge H) &= \binom{\dim_{\mathbb{F}_l} H}{2} + (\dim_{\mathbb{F}_l} H)(n - \dim_{\mathbb{F}_l} H)\\ &= \binom{n}{2} - \dim_{\mathbb{F}_l}\left(\bigwedge^2(G/H)\right),\end{aligned} \tag{1}$$

we obtain $\operatorname{Ker}\pi = G\wedge H$. Therefore

$$\pi^{-1}\left(\bigwedge^2(D_vH/H)\right) = \left(\bigwedge^2 D_v\right) + (G\wedge H),$$

namely,

$$\pi^*\left(\left(\bigwedge^2(D_vH/H)\right)^{\perp_H}\right) = (G\wedge H)^\perp \cap \left(\bigwedge^2 D_v\right)^\perp.$$

Here $(G\wedge H)^\perp$ is the annihilator of $G\wedge H$ in $(\bigwedge^2 G)^*$. On the other hand, X_F is the annihilator of H in $X_K = G^*$, so that $\iota(\bigwedge^2 X_F) \subset (G\wedge H)^\perp$. Hence it follows from (1) that

$$(G\wedge H)^\perp = \iota\left(\bigwedge^2 X_F\right).$$

Therefore, the injectivity of π^* proves Theorem 1.

2

To prove Theorem 2, we prepare the next lemma.

Lemma 1. *Assume that* X_K *is spanned by* $\chi_1, \dots, \chi_n$ *over* $\mathbb{F}_l$, *let* γ *be a nontrivial element of* $\bigwedge^2 X_K$, *and write*

$$\gamma = \sum_{1\le i<j\le n} m_{ij}(\chi_i \wedge \chi_j), \qquad m_{ij} \in \mathbb{F}_l \ (1 \le i < j \le n).$$

Let $M_\gamma = M_\gamma(\chi_1, \dots, \chi_n)$ *denote the skew-symmetric* $(n \times n)$*-matrix whose* (i, j)*-component is* m_{ij}, $1 \le i < j \le n$. *Then* $\det M_\gamma = 0$ *if and only if there exists a proper intermediate field* F *of* K/k *such that* $\gamma \in \bigwedge^2 X_F$.

Proof. Let $\{g_i\}_{1\le i\le n}$ be the basis of G over $\mathbb{F}_l$ such that, for any $i, j \in \{1, \dots, n\}$, $\chi_i(g_j) = 1$ or 0 according as $i = j$ or not. Note that $\gamma \in \bigwedge^2 X_F$ for some proper intermediate field F of K/k if and only if there is a nontrivial vector $(\nu_i)_{1\le i\le n}$ in $\mathbb{F}_l^n$ such that

$$\gamma \in \bigwedge^2 X_{F'}, \tag{2}$$

with F' the fixed field of $\langle \prod_{i=1}^n g_i^{\nu_i} \rangle$ in K. However, as already seen in the proof of Theorem 1,

$$\iota\left(\bigwedge^2 X_{F'}\right) = \left(G \wedge \left\langle \prod_{i=1}^n g_i^{\nu_i} \right\rangle\right)^\perp .$$

Hence (2) is equivalent to the condition that

$$\iota(\gamma)\left(g \wedge \prod_{i=1}^n g_i^{\nu_i}\right) = 0 \quad \text{for all } g \in G. \tag{3}$$

Since

$$\begin{aligned}\iota(\gamma)\left(g_s \wedge \prod_{i=1}^n g_i^{\nu_i}\right) &= \iota(\gamma)\left(-\sum_{1\le i<s} \nu_i(g_i \wedge g_s) + \sum_{s<i\le n} \nu_i(g_s \wedge g_i)\right) \\ &= \sum_{1\le i<s} (-m_{is})\nu_i + \sum_{s<i\le n} m_{si}\nu_i ,\end{aligned}$$

(3) is satisfied by some nontrivial $(\nu_i)_{1\le i\le n} \in \mathbb{F}_l^n$ if and only if $\det M_\gamma = 0$. The lemma is thus proved.

Proof of Theorem 2. Let n be odd and take the basis $\{\chi_i\}_{1\le i\le n}$ of X_K in Lemma 1. Assume that the Hasse norm principle does not hold for K/k so that, by Theorem 1, $\bigcap_{v\in P}(\bigwedge^2 D_v)^\perp$ contains a nontrivial element, say c. Since n is odd, $\det M_{\iota^{-1}(c)} = 0$ where $M_{\iota^{-1}(c)}$ is the skew-symmetric matrix in Lemma 1 with $\gamma = \iota^{-1}(c)$. Hence, by Lemma 1, $\iota^{-1}(c)$ is contained in $\bigwedge^2 X_F$ for some proper intermediate field F of K/k. This fact implies

$$\left(\bigcap_{v\in P}\left(\bigwedge^2 D_v\right)^\perp\right) \cap \iota\left(\bigwedge^2 X_F\right) \ni c \neq 0.$$

Theorem 1 then shows that the Hasse norm principle does not hold for F/k. Therefore Theorem 2 is proved.

In the following, we will be concerned with the case $k = \mathbb{Q}$. For any prime $p \equiv 1 \pmod{2l}$, we denote by $C^{(p)}$ the cyclic extension over $\mathbb{Q}$ of degree l with conductor p.

Let U be a finite set of primes $\equiv 1 \pmod{2l}$, and let S, T be subsets of U. Then we let $\Phi(U; S, T)$ denote the set of primes $q \equiv 1 \pmod{2l}$ which are not in U and satisfy, for each $p \in U$, the following conditions:

(i) q remains prime in $C^{(p)}$ if and only if p belongs to S,
(ii) p remains prime in $C^{(q)}$ if and only if p belongs to T.

Lemma 2. *In the above, $\Phi(U; S, T)$ is an infinite set whenever $l > 2$.*

Let W be a finite set of pairs of distinct primes $\equiv 1 \pmod 4$ such that, for any distinct pairs (p_1, p_1'), (p_2, p_2') in W, $\{p_1, p_1'\} \cap \{p_2, p_2'\} = \varnothing$. Let Y, Z be subsets of W. Then we let $\Psi(W; Y, Z)$ denote the set of pairs (q, q') of distinct primes $\equiv 1 \pmod 4$ which are not in W and satisfy, for each pair $(p, p') \in W$, the following conditions:

(iii) $\left(\frac{pp'}{q}\right) = -1$ if and only if $(p, p') \in Y$,
(iv) $\left(\frac{qq'}{p}\right) = -1$ if and only if $(p, p') \in Z$,
(v) $\left(\frac{pp'}{q}\right) = \left(\frac{pp'}{q'}\right)$ and $\left(\frac{qq'}{p}\right) = \left(\frac{qq'}{p'}\right)$

where $(-)$ denotes the Legendre symbol.

Lemma 3. *$\Psi(W; Y, Z)$ is an infinite set.*

Proofs of Lemmas 2 *and* 3. For any prime $q \equiv 1 \pmod{2l}$, a prime $p \in U$ remains prime in $C^{(q)}$ if and only if the primes of $\mathbb{Q}(\zeta)$ above q remain prime in $\mathbb{Q}(\zeta, \sqrt[l]{p})$, where ζ is a primitive lth root of unity. Therefore, Lemma 2 follows from Chebotarev's density theorem.

Next, we can take infinitely many pairs (q, q') of primes $\equiv 1 \pmod 4$ such that

$$\left(\frac{p}{q}\right) = \left(\frac{p'}{q}\right) = \left(\frac{p}{q'}\right) = \left(\frac{p'}{q'}\right) = 1 \qquad \text{for } (p, p') \notin Y \cup Z,$$

$$\left(\frac{p}{q}\right) = \left(\frac{p'}{q}\right) = 1, \quad \left(\frac{p}{q'}\right) = \left(\frac{p'}{q'}\right) = -1 \qquad \text{for } (p, p') \in Z \setminus Y,$$

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = 1, \quad \left(\frac{p'}{q}\right) = \left(\frac{p'}{q'}\right) = -1 \qquad \text{for } (p, p') \in Y \setminus Z,$$

$$\left(\frac{p}{q}\right) = \left(\frac{p'}{q'}\right) = 1, \quad \left(\frac{p}{q'}\right) = \left(\frac{p'}{q}\right) = -1 \qquad \text{for } (p, p') \in Y \cap Z.$$

Such pairs (q, q') satisfy conditions (iii), (iv), and (v).

Proof of Theorem 3. It is well known that Theorem 3 holds for $n = 2$. Let $n \geq 4$. We first consider the case $l > 2$. Let p_1 be a prime $\equiv 1 \pmod l$, p_2 a prime in $\Phi(\{p_1\}; \{p_1\}, \varnothing)$, and p_3 a prime in $\Phi(\{p_1, p_2\}; \{p_2\}, \{p_1, p_2\})$. Noting that any natural number $\nu \geq 4$ is uniquely written in the form

$$\nu = \binom{i}{2} + \mu \quad \text{with } i \geq 3, \ 1 \leq \mu \leq i,$$

we can take a prime $p_\nu \in \Phi(\{p_1, p_2, p_3, \dots, p_{\binom{i}{2}}\}; S_{i,\mu}, T_{i,\mu})$, where

$$S_{i,\mu} = \{p_\mu\} \text{ or } \{p_{\binom{\mu}{2}}\} \quad \text{according as} \mu \le 3 \text{ or } \mu \ge 4,$$
$$T_{i,\mu} = \{p_{\binom{i}{2}}\} \text{ or } \varnothing \qquad \text{according as } \mu = 1 \text{ or } \mu \ge 2.$$

Next, for each $i \in \{1, \dots, n\}$, put

$$f_i = p_i, \quad \prod_{\mu=1}^{i-1} p_{\binom{i-1}{2}+\mu}, \quad \text{or} \quad \prod_{\mu=1}^{n-2} p_{\binom{n-1}{2}+\mu}$$

according as $i \le 3$, $4 \le i \le n-1$, or $i = n$, and take a cyclic extension F_i of degree l over $\mathbb{Q}$ with conductor f_i. We then let $K = \prod_{i=1}^n F_i$. The existence of infinitely many such examples of K is guaranteed by Lemma 2.

For each $i \in \{1, \dots, n\}$, let K_i denote the maximal subfield of K with conductor prime to f_i: $K_i = \prod_{j \ne i} F_j$. Further, take a genarator g_i of $\mathrm{Gal}(K/K_i)$ and let $h_{i,p}$ denote, for each $p \in P$ dividing f_i, the element of $\mathrm{Gal}(K/F_i)$ such that the restriction $h_{i,p}|K_i$ coincides with the Frobenius automorphism $\left(\frac{K_i/\mathbb{Q}}{p\mathbb{Z}}\right)$. Then $D_p = \langle g_i, h_{i,p} \rangle$. Note that we can write uniquely

$$h_{i,p} = \prod_{j \ne i} g_j^{a_{j,p}} \quad \text{with } a_{j,p} \in \mathbb{F}_l. \tag{4}$$

It also follows that $\{g_i\}_{1 \le i \le n}$ forms a basis of the vector space $G = \mathrm{Gal}(K/\mathbb{Q})$ over $\mathbb{F}_l$. Let $\{\chi_i\}_{1 \le i \le n}$ be the basis of X_K such that, for any $i, j \in \{1, \dots, n\}$, $\chi_i(g_j) = 1$ or 0 according as $i = j$ or not. Given any $j \in \{1, \dots, n\}$, χ_j is naturally considered an element of X_{F_j}. We then put

$$\psi_j(b) = \chi_j\left(\left(\frac{F_j/\mathbb{Q}}{b\mathbb{Z}}\right)\right) \quad \text{for } b \in \mathbb{Z} \text{ prime to } f_j.$$

Now, in (4),

$$a_{j,p} = \chi_j(g_j^{a_{j,p}}) = \chi_j(h_{i,p}|F_j) = \chi_j\left(\left(\frac{K_i/\mathbb{Q}}{p\mathbb{Z}}\right)|F_j\right) = \chi_j\left(\left(\frac{F_j/\mathbb{Q}}{p\mathbb{Z}}\right)\right) = \psi_j(p).$$

Consequently,

$$D_p = \left\langle g_i, \prod_{j \ne i} g_j^{\psi_j(p)} \right\rangle \quad \text{for} \quad p \in P, \ p \mid f_i, \ 1 \le i \le n.$$

It follows from the choice of $p_1, \dots, p_{\binom{n-1}{2}+n-2}$ that

$$\psi_j(p_1) \ne 0 \quad \text{if and only if} \quad j = 3,$$
$$\psi_j(p_2) \ne 0 \quad \text{if and only if} \quad j = 1 \text{ or } 3,$$
$$\psi_j(p_3) \ne 0 \quad \text{if and only if} \quad j = 2 \text{ or } 4,$$

and that, for each $\nu = \binom{i-1}{2} + \mu \in \{4, \dots, \binom{n-1}{2} + n - 2\}$ with $1 \le \mu \le i - 1$,

$$\psi_j(p_\nu) \ne 0 \quad \text{if and only if} \quad j = \mu \text{ or } j = \mu + 2 = i + 1.$$

Therefore we have

$$\bigwedge^2 D_{p_1} = \langle g_1 \wedge g_3 \rangle, \qquad \bigwedge^2 D_{p_2} = \langle -\psi_1(p_2)(g_1 \wedge g_2) + \psi_3(p_2)(g_2 \wedge g_3) \rangle,$$
$$\bigwedge^2 D_{p_3} = \langle -\psi_2(p_3)(g_2 \wedge g_3) + \psi_4(p_3)(g_3 \wedge g_4) \rangle,$$

and, for $\nu = \binom{i-1}{2} + \mu \geq 4$, $1 \leq \mu \leq i-1$,

$$\bigwedge^2 D_{p_\nu} = \begin{cases} \langle g_i \wedge g_\mu \rangle & \text{if } 1 \leq \mu \leq i-2, \\ \langle -\psi_{i-1}(p_\nu)(g_{i-1} \wedge g_i) + \psi_{i+1}(p_\nu)(g_i \wedge g_{i+1}) \rangle & \text{if } \mu = i-1, \end{cases}$$

so that $\dim_{\mathbb{F}_l} \langle \bigwedge^2 D_p \rangle_{p \in P} = \binom{n}{2} - 1$, i.e., $\dim_{\mathbb{F}_l} \bigcap_{p \in P} (\bigwedge^2 D_p)^\perp = 1$. Put

$$\gamma = \sum_{i=1}^{n-1} m_i (\chi_i \wedge \chi_{i+1})$$

with $m_1 = 1$, $m_2 = \psi_1(p_2)\psi_3(p_2)^{-1}$, and $m_i = \psi_{i-1}(p_{\binom{i}{2}})\psi_{i+1}(p_{\binom{i}{2}})^{-1} m_{i-1}$ for $i \in \{3, \dots, n-1\}$. Then, from the definition of ι, we easily see that

$$\iota(\gamma) \in \bigcap_{p \in P} \left(\bigwedge^2 D_p \right)^\perp, \quad \text{whence } \bigcap_{p \in P} \left(\bigwedge^2 D_p \right)^\perp = \langle \iota(\gamma) \rangle.$$

Moreover, it follows that

$$\det M_\gamma = \prod_{u=1}^{n/2} m_{2u-1}^2 \neq 0,$$

where $M_\gamma = M_\gamma(\chi_1, \dots, \chi_n)$ is the skew-symmetric matrix introduced in Lemma 1. Therefore, Lemma 1 implies $(\bigcap_{p \in P} (\bigwedge^2 D_p)^\perp) \cap \iota(\bigwedge^2 X_F) = \{0\}$ for each proper subfield F of K. Theorem 1 thus concludes the proof of Theorem 3 for $l > 2$.

In the case $l = 2$, let (p_1, p_1') be a pair of distinct primes $\equiv 1 \pmod 4$, (p_2, p_2') a pair of primes in $\Psi(\{(p_1, p_1')\}; \{(p_1, p_1')\}, \varnothing)$, and (p_3, p_3') a pair of primes in

$$\Psi(\{(p_1, p_1'), (p_2, p_2')\}; \{(p_2, p_2')\}, \{(p_1, p_1'), (p_2, p_2')\}).$$

For each $\nu = \binom{i}{2} + \mu$ with $i \geq 3$ and $1 \leq \mu \leq i$, we take a pair (p_ν, p_ν') in

$$\Psi(\{(p_1, p_1'), (p_2, p_2'), (p_3, p_3'), \dots, (p_{\binom{i}{2}}, p'_{\binom{i}{2}})\}; Y_{i,\mu}, Z_{i,\mu}),$$

where

$$Y_{i,\mu} = \{(p_\mu, p_\mu')\} \text{ or } \{(p_{\binom{\mu}{2}}, p'_{\binom{\mu}{2}})\} \quad \text{according as } \mu \leq 3 \text{ or } \mu \geq 4,$$
$$Z_{i,\mu} = \{(p_{\binom{i}{2}}, p'_{\binom{i}{2}})\} \text{ or } \varnothing \quad \text{according as } \mu = 1 \text{ or } \mu \geq 2.$$

Next, putting for each $i \in \{1, \dots, n\}$,

$$d_i = p_i p_i', \quad \prod_{\mu=1}^{i-1} p_{\binom{i-1}{2}+\mu} p'_{\binom{i-1}{2}+\mu}, \quad \text{or} \quad \prod_{\mu=1}^{n-2} p_{\binom{n-1}{2}+\mu} p'_{\binom{n-1}{2}+\mu}$$

according as $i \leq 3$, $4 \leq i \leq n-1$ or $i = n$, we let

$$K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n}).$$

Then, quite similarly as in the case $l > 2$, we can prove Theorem 3 for $l = 2$ by using Theorem 1 and Lemmas 1 and 3.

3

In this section, we assume $k = \mathbb{Q}$ from the beginning. Let $\widehat{K}$ denote the maximal unramified central extension of K in the narrow sense, i.e., the maximal extension of K such that $\widehat{K}$ is a Galois extension over $\mathbb{Q}$, the center of $\mathrm{Gal}(\widehat{K}/\mathbb{Q})$ contains $\mathrm{Gal}(\widehat{K}/K)$, and any finite prime of K is unramified in $\widehat{K}$. We denote by $\mathscr{K}$ the genus field of K in the narrow sense, i.e., the maximal abelian extension over $\mathbb{Q}$ containing K such that any finite prime of K is unramified in $\mathscr{K}$. For each intermediate field L of $\widehat{K}/\mathscr{K}$, put

$$\mathfrak{X}_L = \mathrm{Gal}(L/\mathscr{K})^*.$$

It is known (cf. [1, 6, 4]) that

$$\mathrm{Gal}(\widehat{K}/\mathscr{K}) \cong (N_{K/\mathbb{Q}}J_K \cap \mathbb{Q}^\times)/N_{K/\mathbb{Q}}K^\times. \tag{5}$$

As studied in the previous paper [4], there exists a $\mathbb{F}_l$-linear map ρ from $\bigwedge^2 G$ onto $\mathrm{Gal}(\widehat{K}/\mathscr{K})$ such that

$$\rho(\sigma|_K \wedge \tau|_K) = \sigma\tau\sigma^{-1}\tau^{-1}|\widehat{K}, \qquad \sigma, \tau \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q}),$$

where $\widetilde{K}$ is the Hilbert class field of K in the narrow sense. Let ρ^* denote the injective linear map from $\mathfrak{X}_{\widehat{K}}$ into $(\bigwedge^2 G)^*$ induced by ρ:

$$\rho^*(\beta) = \beta \circ \rho, \qquad \beta \in \mathfrak{X}_{\widehat{K}}.$$

The following Theorem 4 is a modification of Theorem 1 in [4].

Theorem 4. *Let F be a subfield of K, and let $\widehat{F}$ denote the maximal unramified central extension of F in the narrow sense. Then $\widehat{F}\mathscr{K}$ is the maximal central extension of F in $\widehat{K}$ and*

$$\rho^*(\mathfrak{X}_{\widehat{F}\mathscr{K}}) = \left(\bigcap_{p\in P}\left(\bigwedge^2 D_p\right)^\perp\right) \cap \iota\left(\bigwedge^2 X_F\right).$$

Proof. We may consider F to be the same as in §1, whence we use the notation $H = \mathrm{Gal}(K/F)$, π, π^*, etc. Let L be the maximal central extension of F in $\widehat{K}$. Put $\mathscr{G} = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ and $\mathscr{H} = \mathrm{Gal}(\widetilde{K}/F)$. Then $\mathrm{Gal}(\widetilde{K}/L) = [\mathscr{G}, \mathscr{H}]$. Noting that the correspondence

$$(\sigma\mathscr{H}, \tau\mathscr{H}) \mapsto \sigma\tau\sigma^{-1}\tau^{-1}[\mathscr{G}, \mathscr{H}], \qquad \sigma, \tau \in \mathscr{G},$$

defines a skew symmetric bilinear map from $\mathscr{G}/\mathscr{H} \times \mathscr{G}/\mathscr{H}$ onto $[\mathscr{G}, \mathscr{G}]/[\mathscr{G}, \mathscr{H}]$, we obtain a linear map r from $\bigwedge^2(G/H)$ onto $\mathrm{Gal}(L/\mathscr{K})$ such that

$$r((\sigma|K)H \wedge (\tau|K)H) = (\sigma\tau\sigma^{-1}\tau^{-1})|L, \qquad \sigma, \tau \in \mathscr{G}.$$

Let r^* denote the injective linear map from $\mathfrak{X}_L$ into $(\bigwedge^2(G/H))^*$ induced by r:

$$r^* = \beta \circ r, \qquad \beta \in \mathfrak{X}_L.$$

Since the diagram

$$\begin{array}{ccc} \mathrm{Gal}(\widehat{K}/\mathscr{K}) & \xleftarrow{\ \rho\ } & \bigwedge^2 G \\ \downarrow & & \downarrow \pi \\ \mathrm{Gal}(L/\mathscr{K}) & \xleftarrow[\ r\ ]{} & \bigwedge^2 (G/H) \end{array}$$

commutes, with the vertical arrow on the left the restriction map, it follows that

$$\pi^* \circ r^*(\beta) = \rho^*(\beta), \qquad \beta \in \mathfrak{X}_L.$$

Hence we find that

$$\rho^*(\mathfrak{X}_L) \subset \operatorname{Im}\rho^* \cap \operatorname{Im}\pi^* = \left(\bigcap_{p\in P}\left(\bigwedge^2 D_p\right)^{\perp}\right) \cap \iota\left(\bigwedge^2 X_F\right).$$

On the other hand, $\mathfrak{X}_{\widehat{F}\mathscr{K}} \cong (N_{F/\mathbb{Q}}J_F \cap \mathbb{Q}^\times)/N_{F/\mathbb{Q}}F^\times$ (cf. (5)) so that, by Theorem 1,

$$\rho^*(\mathfrak{X}_{\widehat{F}\mathscr{K}}) \cong \left(\bigcap_{p\in P}\left(\bigwedge^2 D_p\right)^{\perp}\right) \cap \iota\left(\bigwedge^2 X_F\right).$$

Theorem 4 now follows from $L \supset \widehat{F}\mathscr{K}$.

Corollary. *Let* γ *be an element of* $\bigwedge^2 X_K$ *with* $\iota(\gamma) \in \bigcap_{p\in P}(\bigwedge^2 D_p)^{\perp}$. *Then there exists a unique cyclic extension* L *of degree* l *over* $\mathscr{K}$ *contained in* $\widehat{K}$ *for which* $\rho^*(\mathfrak{X}_L)$ *is generated by* $\iota(\gamma)$. *Moreover, if* F *is a subfield of* K *such that* $\gamma \in \bigwedge^2 X_F$, *then* L *is a subfield of* $\widehat{F}\mathscr{K}$.

We conclude the paper with a result immediately obtained from Theorems 2 and 3.

Proposition. (i) *If* n *is odd, then* $\widehat{K}$ *is the composite of the genus field* $\mathscr{K}$ *of* K *in the narrow sense and the maximal unramified central extensions* $\widehat{F}$ *in the narrow sense of all proper subfields* F *of* K:

$$\widehat{K} = \left(\prod_{F \subsetneqq K} \widehat{F}\right)\mathscr{K}.$$

(ii) *If* n *is even, then there exist infinitely many examples of* K *such that*

$$\widehat{K} \supsetneqq \left(\prod_{F \subsetneqq K} \widehat{F}\right)\mathscr{K}.$$

References

1. D. A. Garbanati, *The Hasse norm theorem for non-cyclic extensions of the rationals*, Proc. London Math. Soc. (3) **37** (1978), 143–164.
2. F. Gerth, *The Hasse norm principle for abelian extensions of number fields*, Bull. Amer. Math. Soc. **83** (1977), 264–266.
3. H. Hasse, *Beweis eines Satzes und Wiederlung einer Vermutung über das allgemeine Normenrestsymbol*, Nachr. Ges. Wiss. Göttingen (1931), 64–69.
4. M. Horie, *On central extensions of elementary abelian fields*, J. Number Theory **36** (1990), 95–107.
5. ——, *The Hasse principle for elementary abelian fields*, Mem. Fac. Sci. Kyushu Univ. Ser. A **45** (1991), 41–54.

6. M. J. Razar, *Central and genus fields and the Hasse norm theorem*, Compositio Math. **35** (1977), 281–298.

7. J. Tate, *Global class field theory*, Algebraic Number Theory (J. W. Cassels and A. Fröhlich, eds.), Academic Press, London and New York, 1967.

Department of Mathematics, Osaka University, Toyonaka, Osaka 560, Japan

Current address: Department of Mathematics, Ochanomizu University, Otsuka, Bunkyo-ku, Tokyo 112, Japan

E-mail address: A0494@JPNOCHA1