J. Math. Soc. Japan
Vol. 34, No. 3, 1982

On the units of an algebraic number field

By Katsuya MIYAKE

(Received Jan. 26, 1981)

In this paper, we extend the transcendental method of Ax [1], to apply the result of Brumer [2] to show Leopoldt's conjecture for certain non-abelian extensions of imaginary quadratic number fields (Theorem 4 in § 6).

§ 1. Preliminaries.

Let F be a finite algebraic extension of rational number field $\boldsymbol{Q}$, and O_F the maximal order of F. For a prime divisor $\mathfrak{p}$ of F, let $F_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of F, and $O_\mathfrak{p}$ the closure of O_F in $F_\mathfrak{p}$.

Let p be a prime number, and denote the p-adic completion of $\boldsymbol{Q}$ by $\boldsymbol{Q}_p$. The closure of the ring of integers $\boldsymbol{Z}$ in $\boldsymbol{Q}_p$ is denoted by $\boldsymbol{Z}_p$. Then $F\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$ is naturally isomorphic to the direct sum $\bigoplus_{\mathfrak{p}|p} F_\mathfrak{p}$.

We denote the multiplicative groups of the invertible elements of F, $F_\mathfrak{p}$, $O_\mathfrak{p}$, etc. by $F^\times$, $F_\mathfrak{p}^\times$, $O_\mathfrak{p}^\times$, etc. Especially, $(\bigoplus_{\mathfrak{p}|p} F_\mathfrak{p})^\times$ is the direct product $\prod_{\mathfrak{p}|p} F_\mathfrak{p}^\times$. Let $W_\mathfrak{p}$ be the group of $(N_{F/\boldsymbol{Q}}(\mathfrak{p})-1)$-th roots of 1 in $F_\mathfrak{p}$. Then $O_\mathfrak{p}^\times = W_\mathfrak{p}\cdot(1+\mathfrak{p}\cdot O_\mathfrak{p})$. Put $U_0=\prod_{\mathfrak{p}|p} O_\mathfrak{p}^\times$ and $U_1=\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\cdot O_\mathfrak{p})$. The action of $\boldsymbol{Z}$ on the compact abelian group U_1 as powers induces the action of $\boldsymbol{Z}_p$ on U_1 naturally. As a $\boldsymbol{Z}_p$-module in this way, the essential rank of U_1 over $\boldsymbol{Z}_p$ is equal to $[F:\boldsymbol{Q}]$, the degree of F over $\boldsymbol{Q}$. In other words, the dimension of the vector space $U^{(p)}=U_1\otimes_{\boldsymbol{Z}}\boldsymbol{Q}=U_1\otimes_{\boldsymbol{Z}_p}\boldsymbol{Q}_p$ over $\boldsymbol{Q}_p$ is $[F:\boldsymbol{Q}]$. Note that $U_0\otimes_{\boldsymbol{Z}}\boldsymbol{Q}=U_1\otimes_{\boldsymbol{Z}}\boldsymbol{Q}=U^{(p)}$.

Let V_0 be a finitely generated subgroup of $F^\times\cap U_0$. Here $F^\times$ is considered to be diagonally imbedded in $\prod_{\mathfrak{p}|p} F_\mathfrak{p}^\times$. Put $V=V_0\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$, and $V^{(p)}=V\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$. Then the inclusion map $V_0\subset U_0$ induces a $\boldsymbol{Q}_p$-linear map $\Phi_p: V^{(p)}\to U^{(p)}$. We are interested in the dimension over $\boldsymbol{Q}_p$ of the subspace $\Phi_p(V^{(p)})$ of $U^{(p)}$. (Leopoldt's conjecture is equivalent to the injectivity of Φ_p for $V_0=O_F^\times=$ the group of the units of F.) Note that

$$\dim_{\boldsymbol{Q}_p} V^{(p)} = \dim_{\boldsymbol{Q}} V = \text{ess. rank}_{\boldsymbol{Z}} V_0\,,$$

and that $\Phi_p|_V: V\to U^{(p)}$ is injective.

We use additive notation for the vector spaces V, $V^{(p)}$, and $U^{(p)}$.

§ 2. Analysis by the automorphisms of F.

Let W_F be the group of the roots of 1 in F. Put, for V_0,

$$G=G(V_0)=\{\alpha\in\mathrm{Aut}(F)\,|\,\alpha(V_0)\subset W_F\cdot V_0\}\,.$$

Since $V=V_0\otimes_{\boldsymbol{Z}}\boldsymbol{Q}=(W_F\cdot V_0)\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$, G acts on V $\boldsymbol{Q}$-linearly, and also on $V^{(p)}$ and on $U^{(p)}$ $\boldsymbol{Q}_p$-linearly. Let $\rho: G\to GL(V;\boldsymbol{Q})$ be the representation of G on V. Then ρ induces a homomorphism of the group algebra $\boldsymbol{Q}_p[G]$ into $\mathrm{End}_{\boldsymbol{Q}_p}(V^{(p)})=\mathrm{Hom}_{\boldsymbol{Q}_p}(V^{(p)},V^{(p)})$, which is also denoted by ρ.

The $\boldsymbol{Q}_p$-linear map $\Phi_p: V^{(p)}\to U^{(p)}$ is a homomorphism of G-modules. Therefore

$$\mathrm{Ker}(\Phi_p)=\{x\in V^{(p)}\,|\,\Phi_p(x)=0\}$$

is a G-invariant subspace of $V^{(p)}$. From the complete reducibility of the representation of G over $\boldsymbol{Q}_p$ follows the existence of a G-subspace X of $V^{(p)}$ such that

$$V^{(p)}=\mathrm{Ker}(\Phi_p)\oplus X \qquad \text{(direct sum)}\,.$$

Let $\pi=\pi(V_0): V^{(p)}\to\mathrm{Ker}(\Phi_p)$ be the projection of $V^{(p)}$ onto $\mathrm{Ker}(\Phi_p)$. Regarded as an element of $\mathrm{End}_{\boldsymbol{Q}_p}(V^{(p)})$, this π satisfies

(1) $\pi\circ\pi=\pi$,

(2) $\forall g\in G\ (\pi\circ\rho(g)=\rho(g)\circ\pi)$.

In other words, π is an idempotent of the commutor $\widetilde{\rho(\boldsymbol{Q}_p[G])}$ of $\rho(\boldsymbol{Q}_p[G])$ in $\mathrm{End}_{\boldsymbol{Q}_p}(V^{(p)})$, where

$$\widetilde{\rho(\boldsymbol{Q}_p[G])}=\{\phi\in\mathrm{End}_{\boldsymbol{Q}_p}(V^{(p)})\,|\,\forall x\in\rho(\boldsymbol{Q}_p[G])(\phi\circ x=x\circ\phi)\}\,.$$

Since $V^{(p)}=V\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$, we have

$$\widetilde{\rho(\boldsymbol{Q}_p[G])}=\widetilde{\rho(\boldsymbol{Q}[G])}\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p\,,$$

$$\widetilde{\rho(\boldsymbol{Q}[G])}=\{\phi\in\mathrm{End}_{\boldsymbol{Q}}(V)\,|\,\forall x\in\rho(\boldsymbol{Q}[G])(\phi\circ x=x\circ\phi)\}\,.$$

Summing up, we have

PROPOSITION 1. *The notation and the assumptions being as above, the projection $\pi: V^{(p)}\to\mathrm{Ker}(\Phi_p)$ is an idempotent of $\widetilde{\rho(\boldsymbol{Q}[G])}\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$, where $\widetilde{\rho(\boldsymbol{Q}[G])}$ is the commutor of $\rho(\boldsymbol{Q}[G])$ in $\mathrm{End}_{\boldsymbol{Q}}(V)$.*

§ 3. Application of Brumer's result.

We prove the transcendentality of $\pi: V^{(p)}\to\mathrm{Ker}(\Phi_p)$ by Brumer's result in [2].

Let A be the algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{Q}_p$.

THEOREM 1. *Let V_0 be a finitely generated subgroup of $F^\times \cap U_0$, and let $V=V_0\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$, $V^{(p)}=V\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$, $\Phi_p: V^{(p)}\to U^{(p)}$ and $\pi: V^{(p)}\to \mathrm{Ker}(\Phi_p)$ be as above. Then we have*

$$\{\pi\circ\phi \mid \phi\in \mathrm{End}_{\boldsymbol{Q}_p}(V^{(p)})\}\cap \mathrm{End}_A(V\otimes_{\boldsymbol{Q}}A)=\{0\}\,.$$

PROOF. Suppose that $\pi\circ\phi\in\mathrm{End}_A(V\otimes_{\boldsymbol{Q}}A)$ for some $\phi\in\mathrm{End}_{\boldsymbol{Q}_p}(V^{(p)})$. Since $\mathrm{End}_A(V\otimes A)=\mathrm{End}_{\boldsymbol{Q}}(V)\otimes_{\boldsymbol{Q}}A$, we can find $\alpha_1,\cdots,\alpha_t\in\mathrm{End}_{\boldsymbol{Q}}(V)$ and $a_1,\cdots,a_t\in A$ such that

$$\pi\circ\phi=a_1\cdot\alpha_1+\cdots+a_t\cdot\alpha_t\,.$$

Put $r=\dim_{\boldsymbol{Q}}V$, and choose $u_1,\cdots,u_r\in V_0$ so that these form a basis of V over $\boldsymbol{Q}$.

Assume now that $\pi\circ\phi\neq 0$. Then for some $u\in V$, we have $\pi\circ\phi(u)\neq 0$. For each j $(1\leqq j\leqq r)$,

$$\alpha_j(u)=b_{j1}\cdot u_1+\cdots+b_{jr}\cdot u_r$$

with $b_{j1},\cdots,b_{jr}\in\boldsymbol{Q}$ because $\alpha_j\in\mathrm{End}_{\boldsymbol{Q}}(V)$. Therefore we have

$$\pi\circ\phi(u)=c_1\cdot u_1+\cdots+c_r\cdot u_r$$

with $c_\mu=b_{1\mu}\cdot a_1+\cdots+b_{t\mu}\cdot a_t\in A$ for $\mu=1,\cdots,r$. Note that all of c_μ's are not equal to zero since $\pi\circ\phi(u)\neq 0$. Now $\pi\circ\phi(u)\in\mathrm{Ker}(\Phi_p)$. Therefore we have

$$(*)\qquad c_1\cdot\Phi_p(u_1)+\cdots+c_r\cdot\Phi_p(u_r)=0\,.$$

This $\Phi_p: V^{(p)}\to U^{(p)}$ was obtained from the imbedding $V_0\subset U_0=\prod_{\mathfrak{p}\mid p}O_{\mathfrak{p}}^\times$. By $\mathfrak{p}$-adic logarithm map of $O_{\mathfrak{p}}^\times$ to $F_{\mathfrak{p}}$, we can define a $\boldsymbol{Q}_p$-linear isomorphism

$$\lambda: U^{(p)}\longrightarrow \bigoplus_{\mathfrak{p}\mid p}F_{\mathfrak{p}}\,.$$

Then composing the canonical maps

$$\bigoplus_{\mathfrak{p}\mid p}F_{\mathfrak{p}}\cong F\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p\subset\longrightarrow F\otimes_{\boldsymbol{Q}}\Omega_p\cong\Omega_p^{[F:\boldsymbol{Q}]}\,,$$

we get a $\boldsymbol{Q}_p$-linear imbedding

$$\tilde{\lambda}: U^{(p)}\longrightarrow\Omega_p^{[F:\boldsymbol{Q}]}$$

where Ω_p is the completion of the algebraic closure of $\boldsymbol{Q}_p$. Let $J=\{\iota_i: F\to\Omega_p \mid i=1,\cdots,[F:\boldsymbol{Q}]\}$ be the set of all the imbeddings of F into Ω_p. Then for $u\in V_0\subset F^\times\cap U_0$, the coordinates of the $[F:\boldsymbol{Q}]$-dimensional vector $\tilde{\lambda}\circ\Phi_p(u)$ coincides with $\log\iota_i(u)$, $i=1,\cdots,[F:\boldsymbol{Q}]$. Here this log is the p-adic logarithm of Ω_p. From $(*)$, therefore, we get a linear relation

$$c_1\cdot\log(\iota_1(u_1))+\cdots+c_r\cdot\log(\iota_1(u_r))=0$$

for $i=1$ for example. From the choice of $u_1,\cdots,u_r$, it follows that $\log(\iota_1(u_1)),\cdots,\log(\iota_1(u_r))$ are linearly independent over $\boldsymbol{Q}$. Because $c_1,\cdots,c_r$ are the elements

of A, all of which are not equal to zero, this relation contradicts Brumer's Theorem 1 in [2]. The proof is completed.

§ 4. The key theorem.

THEOREM 2. *Let the notation and the assumptions be as in Proposition* 1 *and in Theorem* 1. *If* $\widetilde{\rho(\boldsymbol{Q}[G])}\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$ *is isomorphic to a direct sum of division algebras (may be commutative), then* $\Phi_p: V^{(p)}\to U^{(p)}$ *is injective. Especially if* $\widetilde{\rho(\boldsymbol{Q}[G])}$ *is commutative, then* Φ_p *is injective for any prime* p.

For the proof, we need two propositions.

PROPOSITION 2. *Let* S *be a semi-simple algebra over* $\boldsymbol{Q}$. *Then every central idempotent of* $S\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$ *belongs to* $S\otimes_{\boldsymbol{Q}}A$.

PROOF. Let $S=S_1\oplus\cdots\oplus S_n$ be the decomposition of S to a direct sum of its simple components S_i, $i=1,\cdots,n$. Let C_i be the center of S_i. Then $C=C_1\oplus\cdots\oplus C_n$ is the center of S, and $C\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$ is the center of $S\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$. Since every idempotent of $C\otimes\boldsymbol{Q}_p$ is a sum of idempotents of $C_i\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$, $i=1,\cdots,n$, it is sufficient to show the proposition in the case that $S=C$ is a field. Suppose now that C is a finite algebraic extension field of $\boldsymbol{Q}$. Take an element a of C which generates C over $\boldsymbol{Q}$, and let $P(X)\in\boldsymbol{Q}[X]$ be the irreducible polynomial of a, that is, $P(a)=0$, whose leading coefficient is equal to 1. Then C is isomorphic to the quotient field $\boldsymbol{Q}[X]/P\cdot\boldsymbol{Q}[X]$. Let $P(X)=P_1(X)\cdots P_t(X)$ be the decomposition of $P(X)$ in $\boldsymbol{Q}_p[X]$ by the irreducible polynomials $P_j(X)$, $j=1,\cdots,t$, whose leading coefficients are equal to 1. Then each $P_j(X)$ is in $A[X]$ since A is the algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{Q}_p$. We have the decompositions

$$C\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p=\boldsymbol{Q}_p[X]/P_1\cdot\boldsymbol{Q}_p[X]\oplus\cdots\oplus\boldsymbol{Q}_p[X]/P_t\cdot\boldsymbol{Q}_p[X],$$

$$C\otimes_{\boldsymbol{Q}}A=A[X]/P_1\cdot A[X]\oplus\cdots\oplus A[X]/P_t\cdot A[X].$$

For each j, $\boldsymbol{Q}_p[X]/P_j\cdot\boldsymbol{Q}_p[X]$ is a field which contains the field $A[X]/P_j\cdot A[X]$ naturally. Let e_j be the unit element of the field $\boldsymbol{Q}_p[X]/P_j\cdot\boldsymbol{Q}_p[X]$. Then e_j belongs to $A[X]/P_j\cdot A[X]$. Since every idempotent of $C\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$ is a sum of some e_j's, it certainly belongs to $C\otimes A$. Q. E. D.

PROPOSITION 3. *Let* S *be a semi-simple algebra over a commutative field. Then every idempotent of* S *belongs to the center of* S *if and only if* S *is isomorphic to a direct sum of division algebras (may be commutative).*

PROOF. Let S be a direct sum of simple algebras $S_1,\cdots,S_n$. Each S_i is isomorphic to a full matrix algebra $M_{m_i}(D_i)$ over a division algebra D_i. If $m_i>1$ for any i, then S_i surely contains non-central idempotents, which are also non-central idempotents of S. Conversely if $m_1=\cdots=m_n=1$, then an idempotent of $S_i=D_i$ is either 0 or the unit element of D_i for $i=1,\cdots,n$. The proposition is now clear.

One can easily see Theorem 2 by Theorem 1 and Propositions 1, 2 and 3.

§ 5. Case of $V_0=O_F^\times$.

Hereafter until the end of this paper, we restrict ourselves to the case that V_0 is the group $O_F^\times$ of the units of a Galois extension F of an imaginary quadratic number field k.

In this section, we take $G=\mathrm{Gal}(F/k)$.

PROPOSITION 4. *The commutor* $\widetilde{\rho(\boldsymbol{Q}[G])}$ *of* $\rho(\boldsymbol{Q}[G])$ *in* $\mathrm{End}_{\boldsymbol{Q}}(V)$ *is isomorphic to* $\rho(\boldsymbol{Q}[G])$. *Furthermore the direct sum* $\boldsymbol{Q}\oplus\widetilde{\rho(\boldsymbol{Q}[G])}$ *of algebras is isomorphic to the group algebra* $\boldsymbol{Q}[G]$.

PROOF. Let ρ_0 be the trivial representation of G on $X_0=\boldsymbol{Q}$. It is known by Herbrand [3] that the representation $\rho_0\oplus\rho$ of G is equivalent to the regular representation of G. More precisely speaking, there exists an element ε of $V_0=O_F^\times$ such that the vectors $g(\varepsilon)$, $g\in G$, of $V=V_0\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$ satisfy only one linear relation $\sum_{g\in G} g(\varepsilon)=0$. (We use additive notation on V.) Therefore the left $\boldsymbol{Q}[G]$-modules $X=\boldsymbol{Q}[G]$ and $X_0\oplus V$ are $\boldsymbol{Q}[G]$-isomorphic. (For example, define $\phi: X\to X_0\oplus V$ by $\phi(g)=g(1\oplus\varepsilon)$ for $g\in G$.) This shows that the subalgebra $\boldsymbol{Q}\oplus\rho(\boldsymbol{Q}[G])$ of $\mathrm{End}_{\boldsymbol{Q}}(X_0\oplus V)$ is isomorphic to $\boldsymbol{Q}[G]$ which acts on $X=\boldsymbol{Q}[G]$ as left-translations. Now let $\boldsymbol{Q}[G]^*$ be the inverse algebra of $\boldsymbol{Q}[G]$. The action of $\boldsymbol{Q}[G]$ on X as right-translations defines a structure of a left $\boldsymbol{Q}[G]^*$-module on X. Then, as is well known, the commutor $\widetilde{\boldsymbol{Q}[G]}$ of all the left-translations $\boldsymbol{Q}[G]$ in $\mathrm{End}_{\boldsymbol{Q}}(X)$ is nothing but $\boldsymbol{Q}[G]^*$. Since the involution $\iota: \boldsymbol{Q}[G]\to\boldsymbol{Q}[G]$ defined by $\iota(g)=g^{-1}$ for $g\in G$ gives an isomorphism of $\boldsymbol{Q}[G]$ onto $\boldsymbol{Q}[G]^*$, $\widetilde{\boldsymbol{Q}[G]}$ is isomorphic to $\boldsymbol{Q}[G]$. Therefore the $\boldsymbol{Q}[G]$-isomorphism of X onto $X_0\oplus V$ gives an isomorphism of the commutor $\widetilde{\boldsymbol{Q}\oplus\rho(\boldsymbol{Q}[G])}$ of $\boldsymbol{Q}\oplus\rho(\boldsymbol{Q}[G])$ in $\mathrm{End}_{\boldsymbol{Q}}(X_0\oplus V)$ onto $\widetilde{\boldsymbol{Q}[G]}\cong\boldsymbol{Q}[G]$. It is obvious that $\widetilde{\boldsymbol{Q}\oplus\rho(\boldsymbol{Q}[G])}=\boldsymbol{Q}\oplus\widetilde{\rho(\boldsymbol{Q}[G])}$. The proposition is now clear.

THEOREM (Ax-Brumer). *If an algebraic number field K of finite degree is contained in an abelian extension of an imaginary quadratic number field, then for K, Leopoldt's conjecture is true for any prime p.*

PROOF. Let F be a finite abelian extension of an imaginary quadratic number field k, which contains K. Since $G=\mathrm{Gal}(F/k)$ is an abelian group, $\boldsymbol{Q}[G]$ is certainly commutative. It follows, therefore, from Proposition 4 that $\widetilde{\rho(\boldsymbol{Q}[G])}$ is commutative. Then by Theorem 2, $\Phi_p: V^{(p)}\to U^{(p)}$ is injective for any prime p. Since $V_0=O_F^\times$, this is just Leopoldt's conjecture for F, which assures Leopoldt's conjecture for the subfield K. Q. E. D.

PROPOSITION 5. *For a finite group G, and for a prime p, the group algebra $\boldsymbol{Q}_p[G]$ is isomorphic to a direct sum of division algebras (may be commutative) if and only if either* (1) *G is abelian, or*

(2) *$p=2$ and $G=G_1\times G_2$:*

$G_1=\langle a, b\rangle$: $a^4=1$, $a^2=b^2$, $b^{-1}ab=a^{-1}$;

G_2=an abelian group of exponent m or $2m$ with $m\mid(2^{2\mu+1}-1)$.

PROOF. If G is abelian, then $\boldsymbol{Q}_p[G]$ is isomorphic to a direct sum of fields for any p, as is well known. Suppose that G is not abelian, and that $\boldsymbol{Q}_p[G]$ is a direct sum of division algebras. Then any idempotent of $\boldsymbol{Q}_p[G]$ belongs to the center. Let H be a subgroup of G. Then $\iota=|H|^{-1}\cdot\sum_{h\in H}h$ is an idempotent of $\boldsymbol{Q}_p[G]$. Therefore for any $g\in G$, we have $\iota=g^{-1}\cdot\iota\cdot g$. This shows that H is a normal subgroup of G. Because any subgroup of G is normal, G has to be a Hamiltonian group. In other words, $G=G_1\times G_2$ where G_1 is as in the proposition and G_2 is an abelian group of exponent m or $2m$ for some odd m. Let Q be the algebra of Hamiltonian quaternions over $\boldsymbol{Q}$, i.e.

$$Q=\{v\cdot 1+w\cdot i+x\cdot j+y\cdot k\mid v, w, x, y\in\boldsymbol{Q}\}:$$
$$i^2=j^2=-1,\ i\cdot j=-j\cdot i=k.$$

Take a primitive n-th root ζ_n of 1 for each $n\mid m$. Then any non-commutative simple component of $\boldsymbol{Q}_p[G]$ is isomorphic to $Q\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p(\zeta_n)$ for $n\mid m$. If $p\neq 2$, then $Q\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p=M_2(\boldsymbol{Q}_p)$ is not a division algebra. Now suppose that $p=2$. Then, as is well known, $Q\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p(\zeta_n)$ is a division algebra if and only if $[\boldsymbol{Q}_p(\zeta_n):\boldsymbol{Q}_p]$ is odd. If $d=[\boldsymbol{Q}_p(\zeta_m):\boldsymbol{Q}_p]$ is odd, then $[\boldsymbol{Q}_p(\zeta_n):\boldsymbol{Q}_p]$ is also odd for $n\mid m$ because this is a divisor of d. Since m is odd, $\boldsymbol{Q}_p(\zeta_m)$ is unramified over $\boldsymbol{Q}_p$. Therefore the roots of 1 in $\boldsymbol{Q}_p(\zeta_m)$ are the $2\cdot(2^d-1)$-th roots of 1. Thus we have $m\mid 2^d-1$ for odd d. Conversely, if $m\mid 2^{d'}-1$ for odd d', then ζ_m belongs to the unramified extension of $\boldsymbol{Q}_p$ of degree d'. Therefore $d=[\boldsymbol{Q}_p(\zeta_m):\boldsymbol{Q}_p]$ divides d'. Since d' is odd, so is d. The proof is completed.

By the same way as in the above proof of Ax-Brumer Theorem, we have now

THEOREM 3. *Let K be a subfield of a Galois extension F of an imaginary quadratic number field k whose Galois group over k is isomorphic to the group of Proposition* 5, (2). *Then for $p=2$, Leopoldt's conjecture is true for K.*

§ 6. Main Theorem.

In this section, we verify Leopoldt's conjecture for some special types of Galois extensions of imaginary quadratic number fields.

NOTATION.

General quaternion group $\mathfrak{Q}_n$ of order 2^{n+1} $(n\geqq 2)$,

$$\mathfrak{Q}_n=\langle a_n, b\rangle: a_n^{2^n}=1,\ b^2=a_n^{2^{n-1}},\ b^{-1}a_nb=a_n^{-1};$$

Dihedral group $\mathfrak{D}_n$ of order 2^{n+1} $(n\geqq 2)$,

$$\mathfrak{D}_n=\langle a_n, c\rangle : a_n^{2^n}=c^2=1,\ c^{-1}a_nc=a_n^{-1};$$

Quasi-dihedral group $\tilde{\mathfrak{D}}_n$ of order 2^{n+1} $(n\geqq 3)$,

$$\tilde{\mathfrak{D}}_n=\langle a_n, d\rangle : a_n^{2^n}=d^2=1,\ d^{-1}a_nd=a_n^{-1+2^{n-1}}.$$

THEOREM 4. *If an algebraic number field K is contained in a field F satisfying the following (**), then for K, Leopoldt's conjecture is true for any prime p.*

(**) *F is a composite field $F_1\cdot F_2$ such that*

(1) *F_1 is a finite abelian extension of $\boldsymbol{Q}$, the exponent of whose Galois group $\mathrm{Gal}(F_1/\boldsymbol{Q})$ is either m or $2m$ for some odd m;*

(2) *F_2 is a Galois extension of an imaginary quadratic number field k, which is also a Galois extension of $\boldsymbol{Q}$, such that $\mathfrak{G}=\mathrm{Gal}(F_2/\boldsymbol{Q})$ and its normal subgroup $\mathfrak{G}_1=\mathrm{Gal}(F_2/k)$ belong to the following list:*

(i) $\mathfrak{G}=\langle a, b, c\rangle : a^4=c^2=1,\ b^2=a^2,\ b^{-1}ab=a^{-1},\ c^{-1}ac=b$:

$\mathfrak{G}_1=\langle a, b\rangle$;

(ii) $\mathfrak{G}=\mathfrak{Q}_{n+1}=\langle a_{n+1}, b\rangle$ $(n\geqq 2)$;

$\mathfrak{G}_1=\mathfrak{Q}_n=\langle a_n, b\rangle,\ a_n=a_{n+1}^2$;

(iii) $\mathfrak{G}=\mathfrak{D}_{n+1}=\langle a_{n+1}, c\rangle$ $(n\geqq 2)$;

$\mathfrak{G}_1=\mathfrak{D}_n=\langle a_n, c\rangle,\ a_n=a_{n+1}^2$;

(iv) $\mathfrak{G}=\tilde{\mathfrak{D}}_{n+1}=\langle a_{n+1}, d\rangle$ $(n\geqq 2)$;

$\mathfrak{G}_1=\mathfrak{Q}_n=\langle a_n, b\rangle,\ a_n=a_{n+1}^2,\ b=da_{n+1}$;

(v) $\mathfrak{G}=\tilde{\mathfrak{D}}_{n+1}=\langle a_{n+1}, d\rangle$ $(n\geqq 2)$;

$\mathfrak{G}_1=\mathfrak{D}_n=\langle a_n, c\rangle,\ a_n=a_{n+1}^2,\ c=d$.

To prove the theorem, we show that the commutor $\widetilde{\rho(\boldsymbol{Q}[G])}$ of $\rho(\boldsymbol{Q}[G])$ in $\mathrm{End}_{\boldsymbol{Q}}(V)$ is commutative. Then the theorem follows from Theorem 2 immediately. For $G_1=\mathrm{Gal}(F/k)$, the basic structure of the commutor $\widetilde{\rho(\boldsymbol{Q}[G_1])}$ of $\rho(\boldsymbol{Q}[G_1])$ in $\mathrm{End}_{\boldsymbol{Q}}(V)$ has already been seen in Proposition 4.

For a positive integer ν, let ζ_ν be a primitive 2^ν-th root of 1, and put

$$\tau_\nu=\zeta_\nu+\zeta_\nu^{-1},\quad \text{and}\quad \lambda_\nu=\zeta_\nu-\zeta_\nu^{-1}.$$

If $\nu\geqq 2$, then $\boldsymbol{Q}(\zeta_\nu)=\boldsymbol{Q}(\tau_\nu, \sqrt{-1})=\boldsymbol{Q}(\tau_\nu, \lambda_\nu)$. Note that $\boldsymbol{Q}(\tau_\nu)$ is totally real, and that $\boldsymbol{Q}(\lambda_\nu)$ is totally imaginary if $\nu\geqq 2$. We have

$$[\boldsymbol{Q}(\zeta_\nu):\boldsymbol{Q}(\tau_\nu)]=[\boldsymbol{Q}(\lambda_\nu):\boldsymbol{Q}(\tau_{\nu-1})]=2,\qquad (\nu\geqq 2),$$

$$[\boldsymbol{Q}(\zeta_\nu):\boldsymbol{Q}(\lambda_\nu)]=\begin{cases}1 & (\nu=2),\\ 2 & (\nu\geqq 3).\end{cases}$$

The following four propositions are easily seen.

PROPOSITION 6. *Let* $\mathfrak{G}=\langle a, b, c\rangle$ *be the group of Theorem* 4, (i). *Then* $\boldsymbol{Q}[\mathfrak{G}]\cong\boldsymbol{Q}^4\oplus M_2(\boldsymbol{Q})\oplus M_4(\boldsymbol{Q})$, *where* $\boldsymbol{Q}^4$ *corresponds to the abelian group* $\mathfrak{G}/\mathfrak{G}'=\mathfrak{G}/\langle a^{-1}b\rangle$, $M_2(\boldsymbol{Q})$ *to* $\psi_1\colon\mathfrak{G}\to\mathfrak{G}/\langle a^2\rangle\to GL_2(\boldsymbol{Q})$,

$$\psi_1(a)=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},\quad \psi_1(b)=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad \psi_1(c)=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

and $M_4(\boldsymbol{Q})$ *to* $\psi_2\colon G\to GL_4(\boldsymbol{Q})$,

$$\psi_2(a)=\begin{pmatrix}&-1&&\\1&&&\\&&&1\\&&-1&\end{pmatrix},\quad \psi_2(b)=\begin{pmatrix}&&-1&\\&&&-1\\1&&&\\&1&&\end{pmatrix},\quad \psi_2(c)=\begin{pmatrix}0&&&1\\&-1&0&\\&0&1&\\1&&&0\end{pmatrix}.$$

PROPOSITION 7. *For* $\mathfrak{D}_n=\langle a_n, c\rangle$ $(n\geqq 2)$,

$$\boldsymbol{Q}[\mathfrak{D}_n]\cong\boldsymbol{Q}^4\oplus\bigoplus_{\nu=2}^{n}M_2(\boldsymbol{Q}(\tau_\nu))\,,$$

where $\boldsymbol{Q}^4$ *corresponds to* $\chi_i^{(n)}\colon\mathfrak{D}_n\to\boldsymbol{Q}^\times$ $(i=0, 1, 2, 3)$,

$$\chi_i^{(n)}(a_n)=(-1)^{i(i-1)/2},\qquad \chi_i^{(n)}(c)=(-1)^i\,,$$

and $M_2(\boldsymbol{Q}(\tau_\nu))$ $(2\leqq\nu\leqq n)$ *to* $\xi_\nu^{(n)}\colon\mathfrak{D}_n\to\mathfrak{D}_n/\langle a_n^{2^\nu}\rangle\to GL_2(\boldsymbol{Q}(\tau_\nu))$,

$$\xi_\nu^{(n)}(a_n)=\begin{pmatrix}0 & -1\\ 1 & \tau_\nu\end{pmatrix},\qquad \xi_\nu^{(n)}(c)=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

PROPOSITION 8. *For* $\tilde{\mathfrak{D}}_n=\langle a_n, d\rangle$ $(n\geqq 3)$,

$$\boldsymbol{Q}[\tilde{\mathfrak{D}}_n]\cong\boldsymbol{Q}^4\oplus\bigoplus_{\nu=2}^{n-1}M_2(\boldsymbol{Q}(\tau_\nu))\oplus M_2(\boldsymbol{Q}(\lambda_n))\,,$$

where $\boldsymbol{Q}^4\oplus\bigoplus_{\nu=2}^{n-1}M_2(\boldsymbol{Q}(\tau_\nu))$ *corresponds to* $\tilde{\mathfrak{D}}_n/\langle a_n^{2^{n-1}}\rangle\cong\mathfrak{D}_{n-1}$, *and* $M_2(\boldsymbol{Q}(\lambda_n))$ *to* $\tilde{\xi}^{(n)}\colon\tilde{\mathfrak{D}}_n\to GL_2(\boldsymbol{Q}(\lambda_n))$,

$$\tilde{\xi}^{(n)}(a_n)=\begin{pmatrix}0 & 1\\ 1 & \lambda_n\end{pmatrix},\quad \tilde{\xi}^{(n)}(d)=\begin{pmatrix}1 & 0\\ \lambda_n & -1\end{pmatrix}.$$

PROPOSITION 9. *Let* Q *be the algebra of Hamiltonian quaternions over* $\boldsymbol{Q}$, *that is,*

$$Q=\{v\cdot 1+w\cdot i+x\cdot j+y\cdot k\mid v, w, x, y\in\boldsymbol{Q}\}\,,$$

$$i^2=j^2=-1,\quad i\cdot j=-j\cdot i=k\,.$$

Then for $\mathfrak{Q}_n=\langle a_n, b\rangle$ $(n\geqq 2)$,

$$\boldsymbol{Q}[\mathfrak{Q}_n]\cong\boldsymbol{Q}^4\oplus\bigoplus_{\nu=2}^{n-1}M_2(\boldsymbol{Q}(\tau_\nu))\oplus Q\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(\tau_n)\,,$$

where $\boldsymbol{Q}^4\oplus\bigoplus_\nu M_2(\boldsymbol{Q}(\tau_\nu))$ ($\boldsymbol{Q}^4$ *if* $n=2$) *corresponds to* $\mathfrak{Q}_n/\langle a_n^{2^{n-1}}\rangle\cong\mathfrak{D}_{n-1}$, *and* $Q\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(\tau_n)$ *to* $\eta^{(n)}:\mathfrak{Q}_n\to(Q\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(\tau_n))^\times$,

$$\eta^{(n)}(a_n)=\frac{1}{2}\cdot(\tau_n-\tau_n'\cdot i)\,,\qquad \eta^{(n)}(b)=j\,,$$

$$\tau_n'=\zeta_n^{1+2^{n-2}}+\zeta_n^{-1-2^{n-2}}\in\boldsymbol{Q}(\tau_n)\,.$$

Now let $F=F_1\cdot F_2$ satisfy the condition (**). By the assumption on the exponent of $\mathrm{Gal}(F_1/\boldsymbol{Q})$, we easily see that there exists a subfield F_1' of F_1 such that $F_1=F_1'\cdot(F_1\cap F_2)$ and $F_1'\cap F_2=\boldsymbol{Q}$. Replacing F_1 by F_1', we may assume that $F_1\cap F_2=\boldsymbol{Q}$. Then we have

$$G=\mathrm{Gal}(F/\boldsymbol{Q})=\mathfrak{A}\times\mathfrak{G}\,,\quad\text{and}\quad G_1=\mathrm{Gal}(F/k)=\mathfrak{A}\times\mathfrak{G}_1$$

with $\mathfrak{A}=\mathrm{Gal}(F_1/\boldsymbol{Q})$, $\mathfrak{G}=\mathrm{Gal}(F_2/\boldsymbol{Q})$ and $\mathfrak{G}_1=\mathrm{Gal}(F_2/k)$. The exponent of $\mathfrak{A}$ is either m or $2m$ for some odd m.

Let $\boldsymbol{Q}[\mathfrak{G}_1]=B_0\oplus B_1\oplus\cdots\oplus B_s$ be the decomposition of $\boldsymbol{Q}[\mathfrak{G}_1]$ to a direct sum of the commutative semi-simple subalgebra B_0 and non-commutative simple subalgebras $B_1,\cdots,B_s$. Let e_j be the unit element of B_j for $j=0,1,\cdots,s$. By Propositions 6∼9, we easily see that each non-commutative simple algebra B_j ($1\leqq j\leqq s$) is contained in only one simple component of $\boldsymbol{Q}[\mathfrak{G}]$. Moreover, all of $e_0,e_1,\cdots,e_s$ are central idempotents of $\boldsymbol{Q}[\mathfrak{G}]$, and they give a decomposition

$$Q[\mathfrak{G}]=B_0'\oplus B_1'\oplus\cdots\oplus B_s'\,,\quad B_j'=e_j\cdot\boldsymbol{Q}[\mathfrak{G}]\qquad(0\leqq j\leqq s)\,.$$

If $1\leqq j\leqq s$, then B_j' is simple.

For μ dividing m, let ζ_μ' be a primitive μ-th root of 1. Then $\boldsymbol{Q}[\mathfrak{A}]$ is isomorphic to a direct sum of algebraic number fields $\boldsymbol{Q}(\zeta_\mu')$ ($\mu\,|\,m$). (For each μ, a number of copies of $\boldsymbol{Q}(\zeta_\mu')$ may appear.) Therefore $\boldsymbol{Q}[G_1]=\boldsymbol{Q}[\mathfrak{A}]\otimes_{\boldsymbol{Q}}\boldsymbol{Q}[\mathfrak{G}_1]$ or $\boldsymbol{Q}[G]=\boldsymbol{Q}[\mathfrak{A}]\otimes_{\boldsymbol{Q}}\boldsymbol{Q}[\mathfrak{G}]$ is a direct sum of semi-simple algebras $\boldsymbol{Q}[\mathfrak{A}]\otimes_{\boldsymbol{Q}}B_0$ or $\boldsymbol{Q}[\mathfrak{A}]\otimes_{\boldsymbol{Q}}B_0'$, and $B_{j\mu}=B_j\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(\zeta_\mu')$ or $B_{j\mu}'=B_j'\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(\zeta_\mu')$ for $j=1,\cdots,s$ and for $\mu\,|\,m$, respectively. The algebras $B_{j\mu}$ and $B_{j\mu}'$ are simple. In fact, their centers are fields because they can be regarded as subalgebras of $\boldsymbol{Q}(\zeta_\nu)\otimes_{\boldsymbol{Q}}\boldsymbol{Q}(\zeta_\mu')$, which is a field since ζ_ν or ζ_μ' is a 2^ν-th or μ-th root of 1 respectively such that $(2^\nu,\mu)=1$. Note that $\boldsymbol{Q}[\mathfrak{A}]\otimes_{\boldsymbol{Q}}B_0$ is commutative. One can easily see the followings by Propositions 6∼9:

(I) In the case of (i) of the theorem, $s=1$, the center of $B_{1\mu}$ is equal to the center of $B_{1\mu}'$, and they are isomorphic to $\boldsymbol{Q}(\zeta_\mu')$.

$$[B_{1\mu}:\boldsymbol{Q}(\zeta_\mu')]=4\,,\quad\text{and}\quad[B_{1\mu}':\boldsymbol{Q}(\zeta_\mu')]=16\,;$$

(II) In the cases of (ii)∼(v) of the theorem, let $C_{j\mu}$ or $C_{j\mu}'$ be the center of

$B_{j\mu}$ or $B'_{j\mu}$ respectively. Then

$$[C'_{j\mu}: C_{j\mu}]=2, \quad \text{and} \quad [B_{j\mu}: C_{j\mu}]=4,$$
$$B'_{j\mu}=B_{j\mu}\otimes_{C_{j\mu}}C'_{j\mu}.$$

We now show that the commutor $\widetilde{\rho(\boldsymbol{Q}[G])}$ of $\rho(\boldsymbol{Q}[G])$ in $\mathrm{End}_{\boldsymbol{Q}}(V)$ is commutative. Let B be a component $\rho(\boldsymbol{Q}[\mathfrak{A}]\otimes B_0)$ or $\rho(B_{j\mu})$ of $\rho(\boldsymbol{Q}[G_1])$ and B' the component of $\rho(\boldsymbol{Q}[G])$ which contains B. Let e be the unit element of B. Then it is also the unit element of B'. Let $\tilde{B}$ and $\tilde{B}'$ be the commutors of B and B' in $\mathrm{End}_{\boldsymbol{Q}}(e(V))$ respectively. Then $\tilde{B}$ contains $\tilde{B}'$. Since $\widetilde{\rho(\boldsymbol{Q}[G])}$ is a direct sum of such $\tilde{B}'$, it is sufficient to show that each $\tilde{B}'$ is commutative.

If $B=\rho(\boldsymbol{Q}[\mathfrak{A}]\otimes B_0)$, then $B'=\rho(\boldsymbol{Q}[\mathfrak{A}]\otimes B'_0)$. By Proposition 4, $\widetilde{\rho(\boldsymbol{Q}[G_1])}$ is isomorphic to $\rho(\boldsymbol{Q}[G_1])$. We get $\tilde{B}\cong B$ by this isomorphism. Since $B=\rho(\boldsymbol{Q}[\mathfrak{A}]\otimes B_0)$ is commutative, the subalgebra $\tilde{B}'$ of $\tilde{B}\cong B$ is also commutative. If $B=\rho(B_{j\mu})$ and $B'=\rho(B'_{j\mu})$, then $e(V)$ becomes a vector space over the center $C'=\rho(C'_{j\mu})$ of B'. Then $\tilde{B}'$ coincides with the commutor of B' in $\mathrm{End}_{C'}(e(V))$. By Proposition 4, we see that the vector space $e(V)$ is isomorphic to B as $\boldsymbol{Q}$-spaces. Therefore as a vector space over $C=\rho(C_{j\mu})$, $\dim_C e(V)=4$. Then by (I) or by (II), we immediately see that $\tilde{B}'=C'$. Thus we have shown that $\widetilde{\rho(\boldsymbol{Q}[G])}$ is commutative in any case of Theorem 4. This establishes the theorem as was mentioned before.

REMARK. For $\mathfrak{G}_1=\mathfrak{Q}_n$, $\mathfrak{D}_n$ or $\tilde{\mathfrak{D}}_n$, a group $\mathfrak{G}$ which contains $\mathfrak{G}_1$ as a subgroup of index 2 is one of the following groups besides the ones of (i)$\sim$(v):

$\mathfrak{G}_1\times \boldsymbol{Z}/2\cdot\boldsymbol{Z}$;

$\mathfrak{G}_1\times(\boldsymbol{Z}/4\cdot\boldsymbol{Z})/\langle(a_n^{2^{n-1}}, 2(\mathrm{mod}\,4))\rangle$;

$\mathfrak{G}=\langle a_n, b, e\rangle: a_n^{2^n}=e^2=1, b^2=a_n^{2^{n-1}}, b^{-1}a_nb=a_n^{-1}, e^{-1}a_ne=a_n^{1+2^{n-1}}, e^{-1}b^{-1}eb=1,$

$\mathfrak{G}_1=\mathfrak{Q}_n=\langle a_n, b\rangle$ or $\tilde{\mathfrak{D}}_n=\langle a_n, (a_nbe)\rangle$;

$\mathfrak{G}=\langle a_n, c, e\rangle: a_n^{2^n}=c^2=e^2=1, c^{-1}a_nc=a_n^{-1}, e^{-1}a_ne=a_n^{1+2^{n-1}}, e^{-1}c^{-1}ec=1,$

$\mathfrak{G}_1=\mathfrak{D}_n=\langle a_n, c\rangle$ or $\tilde{\mathfrak{D}}_n=\langle a_n, (ce)\rangle$.

But to these groups, we cannot apply our arguments above.

References

[1] J. Ax, On the units of an algebraic number field, Illinois J. Math., 9 (1965), 584-589.

[2] A. Brumer, On the units of an algebraic number field, Mathematica, 14 (1967), 121-124.

[3] J. Herbrand, Sur les unites d'un corps algébrique, C.R. Acad. Sci. Paris, **192** (1931), 24-27, and 188.

Katsuya MIYAKE
Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464
Japan