A note on the Leopoldt conjecture for an abelian extension of a real quadratic field

A note on the Leopoldt conjecture for an abelian extension of a real quadratic field

Hiroshi YAMASHITA

Abstract. We study the Leopoldt conjecture for an abelian extension of a real quadratic field. The method approaching this problem in the present paper is to compare representation over $\boldsymbol{Q}$ of the Galois group with that over $\boldsymbol{Q}_p$. We study the conjecture for an abelian extension of a real quadratic field.

Introduction. The Leopoldt conjecture is a conjecture that the p-adic regulator of an algebraic number field dose not vanish. In the context of Iwasawa's theory of $\boldsymbol{Z}_p$-extensions, this conjecture is interpreted as a conjecture concerning the $\boldsymbol{Z}_p$-rank of the Galois group of a maximal ablelian p-ramified p-extension of an algebraic number field. Namely, it predicts that the $\boldsymbol{Z}_p$-rank equals the value exceeding one to the number of complex places of the algebraic number field, *cf.* Theorem 13.4 in [6]. We study this conjecture in a view point from representation of Galois groups, *cf.* [3] and [4]. We make investigation into relations of rational representations and p-adic representations of finite abelian groups. We are mainly concerned in an abelian extension of an algebraic number field where the Leopoldt conjecture is true, and which is Galois over $\boldsymbol{Q}$. It is fundamental fact in such consideration that the unit group E of an algebraic number field is mapped injectively into the semi-local product U_p of groups of local units on every places lying over p. It follows from this fact that a semi-simple module contained in $\boldsymbol{Q} \otimes_{\boldsymbol{Z}} E$ dose not vanish in $\boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} U_p$. They generate simple modules over $\boldsymbol{Q}_p$. However, by the extension of coefficients, it sprits into several simple modules. The problem is how many simple factors over $\boldsymbol{Q}_p$ remain in $\boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} U_p$. We compare the representation of the Galois group on the global unit group over $\boldsymbol{Q}$ with that of a $\boldsymbol{Q}_p$-module generated by the image into the extension of coefficients of the semi-local product $U^{(e)}$ to $\boldsymbol{Q}_p$. To decompose the simple factors, we need to extend coefficients of $\boldsymbol{Q}$-representation to an algebraic extension L contained in $\boldsymbol{Q}_p$, and we assume the natural extension $L \otimes_{\boldsymbol{Z}} E \longrightarrow \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} U^{(e)}$ is injective. Our aim of the present paper is to study the Leopoldt conjecture for an abelian extension of an real quadratic field under this assumption by means of representation theory. In the following part, we denote by RG, where R is a commutative ring and G is a finite group, the group ring of G with coefficients in R.

1. Leopoldt's conjecture. Let p be a prime number and $|x|_p$ be the p-adic valuation of the field of rational numbers normalized as $|p| = p^{-1}$. Its completion is denoted by $\boldsymbol{Q}_p$. The symbol $\boldsymbol{Q}_\infty$ denotes the field of real numbers, which is the completion of $\boldsymbol{Q}$ by the absolute value $|x|_\infty$. Thus, the symbol p indicates a prime number or ∞ in this article. Let K be a finite algebraic extension of $\boldsymbol{Q}$. A valuation of K is called a p-valuation if it is equivalent to the extension of $|x|_p$. An equivalence class of p-valuations is called a p-place. Let w be a p-place of K. We choose a valuation belonging to w so that it is the extension of $|x|_p$ and fix it once for all. Denote by $|x|_w$ be the valuation belonging to w and by K_w the completion of K with it. When p is a prime number, it is a complete discrete valuation field. Let $\mathcal{O}_w$ (*resp.* $\mathfrak{p}_w$) be the valuation ring (*resp.* ideal). Since $\boldsymbol{Q}$ is included in K_w in a unique way, the p-adic field $\boldsymbol{Q}_p$ is regarded as a subfield of K_w. Hence, K_w is an algebraic extension of $\boldsymbol{Q}_p$. The ring $\mathcal{O}_w$ is the integral closure of the valuation ring $\boldsymbol{Z}_p$ of $\boldsymbol{Q}_p$. $\mathcal{O}_w$ and $\mathfrak{p}_w$ are continuous free-$\boldsymbol{Z}_p$-modules of rank $[K_w : \boldsymbol{Q}_p]$. Let $U_w^{(e)}$ be subsets of K_w defined to be

$$U_w^{(e())} = \{x : x - 1 \in \mathfrak{p}_w^e\}$$

for $e = 1, 2, \cdots$. These subsets are open and compact, which are subgroups of $K_w^\times$. The family $\{U_w^{(e)}\}$ is a basis of the system of open neighborhoods of unity. Let $\log_p(1+x)$ be the p-adic logarithm and $\exp_p(x)$ be the p-adic exponential function:

$$\log_p(1+x) = x - \frac{x}{1} + \frac{x^2}{2} - \frac{x^3}{3} + \cdots$$

$$\exp_p = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

These function are convergent when

$$|x|_w < \left(\frac{1}{p}\right)^{\frac{1}{p-1}},$$

cf. Proposition 5.7 in [6].

LEMMA 1. *Let p be a prime number. Let e_0 be the ramification index of the extension $K_w/\boldsymbol{Q}_p$ of discrete valuation fields. Then, $U_w^{(e)}$ is isomorphic to $\mathfrak{p}^e$ as topological groups when e satisfies*

$$(1) \qquad e \geq \frac{2pe_0}{p-1} > \frac{e_0}{p-1}.$$

Proof. Let π be a prime element of K_w. We have

$$|\pi|_w = \left(\frac{1}{p}\right)^{\frac{1}{e_0}}.$$

By Lemma 5.5 in [6], $\log_p\left(U_w^{(e)}\right)$ is a subgroup of $\mathfrak{p}^e$ if

$$e > \frac{e_0}{p-1}.$$

Therefore, $\mathfrak{p}_w^e$ is isomorphic to $U_w^{(e)}$ if $\exp_p(\mathfrak{p}_w^e)$ is a subgroup of $U_w^{(e)}$.

Let v be an additive valuation of K_w normalized by $v(p) = 1$. Since

$$\exp_p(\pi^e x) = 1 + \pi x + \frac{(\pi x)^2}{2!} + \cdots,$$

for $x \in \mathcal{O}_w$, we have only to prove

$$\frac{\pi^{ne}}{n!} \in \mathfrak{p}^e$$

for $n \geq 2$. We observe

$$v(\pi^{ne}) - v(n!) = \frac{ne}{e_0} - \sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right]$$
$$> n\left(\frac{e}{e_0} - \frac{p}{p-1}\right)$$
$$> \frac{np}{p-1}.$$

holds when e satisfies (1). This proves the lemma. □

We define y^a for $a \in \boldsymbol{Z}_p$ and $y \in U_w^{(e)}$ to be

$$y^a = \exp_p(a \log_p(y))$$

if e satisfies (1). Thus, $U_w^{(e)}$ is a multiplicative free $\boldsymbol{Z}_p$-module of rank $[K_w : \boldsymbol{Q}_p]$.

Let r_p be the number of p-places of K. Denote by w_i for $i = 1, \cdots, r_p$ p-places of K. The direct product

$$K_p^\times = K_{w_1}^\times \times \cdots \times K_{w_{r_p}}^\times$$

is a topological group with topology of a direct product. Since K is a subfield of K_{w_i}, $K^\times$ is embedded into $K_p^\times$ diagonally, whose embedding is denoted by Δ_p. When p is a prime number, there is an open compact subgroups

$$U_p^{(e)} = U_{w_1}^{(e)} \times \cdots \times U_{w_{r_p}}^{(e)},$$

for $e = 1, 2, \cdots$. This set of open subgroups is a basis of open neighborhoods of $K_p^\times$. Let E be the group of units of K. We define subgroups of finite index by

$$E^{(e)} = \Delta_p^{-1}(\Delta_p(E) \cap U_p^{(e)}),$$

for $e = 1, 2 \cdots$. When e satisfies (1), the group $E^{(e)}$ is a free abelian group of rank $r_\infty - 1$. Let $\overline{E^{(e)}}$ be the topological closure of $\Delta_p(E^{(e)})$ in $U_p^{(e)}$. If we take generators $\varepsilon_1, \cdots, \varepsilon_{r_\infty - 1}$ of $E^{(e)}$, every $\Delta(\varepsilon_i)$ generate closed subgroups $\Delta(\varepsilon_i)^{\boldsymbol{Z}_p}$'s in $U_p^{(e)}$. Since they are compact subgroups, we have $\overline{E^{(e)}} = \Delta(\varepsilon_1)^{\boldsymbol{Z}_p} \cdots \Delta(\varepsilon_{r_\infty})^{\boldsymbol{Z}_p}$. Therefore,

$$\dim \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}} E^{(e)} \geq \dim \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} \overline{E^{(e)}},$$

where *dim* denotes the dimension of $\boldsymbol{Q}_p$-linear spaces. The Leopoldt conjecture is interpreted in the context of Iwasawa's theory of $\boldsymbol{Z}_p$-extensions, *cf.* Theorem 13.4 in [6], which asserts that the Leopoldt conjecture for p is equivalent to attaining the equality in the inequality. The value

$$\delta_{K,p} = \dim \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}} E^{(e)} - \dim \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} \overline{E^{(e)}}$$

is called the defect value from the Leopoldt conjecture. We abbreviate a $\boldsymbol{Q}$-linear space $\boldsymbol{Q} \otimes_{\boldsymbol{Z}} E^{(e)}$ to $E^{\boldsymbol{Q}}$ and a $\boldsymbol{Q}_p$-linear space $\boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} U_p^{(e)}$ to $U^{\boldsymbol{Q}_p}$. These linear spaces are determined uniquely despite choices of positive integers e. Therefore, in the sequal part, we fix an integer e satisfying the condition (1). The inclusion ι_p of $\boldsymbol{Q}$ into $\boldsymbol{Q}_p$ and Δ_p induce a $\boldsymbol{Q}$-linear map

$$\Delta^{\boldsymbol{Q}} : E^{\boldsymbol{Q}} \longrightarrow U^{\boldsymbol{Q}_p},$$

where $\Delta^{\boldsymbol{Q}} = \iota_p \otimes \Delta_p$.

LEMMA 2. $\Delta^{\boldsymbol{Q}}$ is injective.

Proof. Let y be an element of $E^{\boldsymbol{Q}}$ which is mapped to zero by $\Delta^{\boldsymbol{Q}}$. There are positive integers m_i's and elements x_i's of

$E^{(e)}$ such that

$$y = \sum_{i=1}^{s} \frac{1}{m_i} \otimes x_i.$$

Let m be the least common multiple of m_i's and set $n_i = m/m_i$ for each i. We have

$$my = 1 \otimes \prod_{i=1}^{s} x^{n_i}.$$

Put $x = \prod x_i^{n_i}$. Since $\Delta^Q(my) = 0$ implies $\Delta_p(x) = 1$, we have $x = 1$ by injectivity of Δ_p. Hence, $y = 0$. □

2. Galois module structure. We assume K is a Galois extension of $\boldsymbol{Q}$. Let G be the Galois group. Let X_p be a set of every p-places of K. The group G acts on a set X_p, transitively. We select a place w from each set of p-places and fix it once for all. The place ${}^{\sigma}w$ is a equivalence class containing a valuation $|\sigma^{-1}x|_w$. Let H_p be the stabilizer of w. Let

$$G = \sigma_1 H_p \cup \cdots \cup \sigma_{r_p} H_p, \quad \sigma_1 = 1$$

be a decomposition into left cosets. We denote by w_i the place ${}^{\sigma_i}w$ for each i. The valuation $|x|_w$ is invariant for action of $h \in H_p$, because restriction of an arbitrary valuation $|h^{-1}x|$ for $h \in H_p$ has same values as $|x|_w$. Hence, if $\tau\sigma_i = \sigma_j h$ for $\tau \in G$ and $h \in H_p$, we have $|\tau^{-1}x|_{w_i} = |x|_{w_j}$, that is

$$|x|_{w_i} = |\tau x|_{{}^{\tau}w_i}$$

holds for every i's. Since the completion is defined through Cauchy sequences of K with respect to the metric defined by the valuation, an isomorphism of K_{w_i} onto K_{w_j} as topological fields is induced by τ in a unique way.

We determine the $\boldsymbol{Q}G$-module structure of $E^{\boldsymbol{Q}}$ by using the Minkowski unit. There is a unit of K satisfying

$$|\varepsilon|_w > 1, \quad |\varepsilon|_{w_i} < 1$$

when $i \neq 1$. This unit ε is called a Minkowski unit of K. Let E_1 be a multiplicative $\boldsymbol{Z}G$-module generated by ε. E_1 is a subgroup of E of finite index by the Dirichlete unit theorem. We may assume ε is H_∞-invariant. Moreover, since $\varepsilon^{[E:E^{(e)}]} \in E^{(e)}$, we choose the unit ε from $E^{(e)}$. We abbreviate $\sigma_i\varepsilon$ to ε_i. The correspondence $\sigma \longrightarrow \sigma\varepsilon$ defines a surjective $\boldsymbol{Z}G$-homomorphism of $\boldsymbol{Z}G/H_\infty$ onto E_1. Therefore, a surjective $\boldsymbol{Q}G$-homomorphism

$$\boldsymbol{Q}H/H_\infty \longrightarrow E^{\boldsymbol{Q}}.$$

is induced. The kernel is of one dimension over $\boldsymbol{Q}$. Since $N_{K/\boldsymbol{Q}}(\varepsilon) = 1$, it is generated by an idempotent

$$e_G = \frac{1}{|G|} \sum_{g \in G} g.$$

Let e_∞ be an idempotent

$$e_\infty = \frac{1}{|H_\infty|} \sum_{h \in H_\infty} h.$$

We have an isomorphism

$$(1 - e_G)\boldsymbol{Q}Ge_\infty \xrightarrow{\cong} E^{\boldsymbol{Q}}$$

of $\boldsymbol{Q}G$-modules.

We notice the $\boldsymbol{Q}$-linear map $\Delta^{\boldsymbol{Q}}$ is a $\boldsymbol{Q}G$-homorphism, because Δ_p is a G-homomrphism. We study the structure of $\boldsymbol{Q}_p$-subspace of $U^{\boldsymbol{Q}_p}$ generated by Im $(\Delta^{\boldsymbol{Q}})$.

THEOREM 3. *The inclusion of* $\boldsymbol{Q}$ *into* $\boldsymbol{Q}_p$ *induces an injective* $\boldsymbol{Q}G$-*homomorphism*

$$\Delta^Q : E^Q \longrightarrow U^{Q_p},$$

where E^Q is isomorphic to a subring $(1-e_G)QGe_\infty$ as a left QG-module.

We remark that U^{Q_p} is isomorphic to Q_pG.

3. Applications of representation theory. We make one more assumption that K is an abelian extension of a subfield k, where the Leopoldt conjecture is valid for p. Let H be the Galois group of K/k. We decompose G into a disjoint union of double cosets with respect to (H, H_∞):

$$(2) \quad G = H\tau_1 H_\infty \cup \cdots \cup H\tau_r H_\infty, \quad \tau_1 = 1.$$

The number r is equal to that of ∞-places of k. If we denote by QX for a subset X of QG a Q-linear subspace generated by X, the coset decomposition (2) yields

$$QGe_\infty = QH\tau_1 e_\infty \oplus \cdots \oplus QH\tau_r e_\infty.$$

Let e_H be an idempotent contained in QG defined to be

$$e_H = \frac{1}{|H|}\sum_{h\in H} h.$$

The left QH-module $(1-e_H)QGe_\infty$ is isomorphic to

$$QH(1-e_H)\tau_1 e_\infty \oplus \cdots \oplus QH(1-e_H)\tau_r e_\infty.$$

We have $(1-e_H)E^Q$ equals

$$QH(1-e_H)\varepsilon_1 \oplus \cdots \oplus QH(1-e_H)\varepsilon_r,$$

where we abbreviate $\tau_i\varepsilon$ to ε_i. Thus, the QG-homomorphism Δ^Q induces an injection

$$\Delta^Q_H : (1-e_H)E^Q \longrightarrow U^{Q_p}.$$

Denote by V a Q_p-subspace generated by Im (Δ^Q_H). Since the Leopoldt conjecture is valid for p, we have

$$\delta_{K,p} = r(|H|-1) - \dim V.$$

In our setting, the theorem of Brummer is stated as follows:

THEOREM 4 (Brumer). *If $r = 1$, then the Leopoldt conjecture is true for every prime numbers.*

This theorem is re-proved in [3] as an application of representation theory of finite groups. We shall give another approach here. Let M be a simple QH-module contained in $(1-e_H)E^Q$. There is an element μ by which M is generated over QH. Let A be a simple subring of QH whose minimal left ideal is isomorphic to M as a QH-module. Let e be identity of A and φ be the character afforded by a left QH-module A. When we extend coefficients on $\overline{Q}_p$, $A^{\overline{Q}_p}$ is decomposed into a direct sum of one-dimensional algebras:

$$A^{\overline{Q}_p} = A_1 \oplus \cdots \oplus A_n.$$

This induces decomposition of e and φ:

$$(3) \qquad e = e_1 + e_2 + \cdots + e_n,$$

$$(4) \qquad \varphi = \chi_1 + \chi_2 + \cdots + \chi_n.$$

The characters χ_i's are defined by $he_i = \chi(h)e_i$ for $h \in H$ and e_i and χ_i is related as

$$e_i = \frac{1}{|H|}\sum_{h\in H} \chi_i(h^{-1})h.$$

Let ζ be a primitive $|\chi_1|$-th root of unity. Let $\mathfrak{g}$ be the Galois group of $\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$. The group $\mathfrak{g}$ acts on the characters by values:

$$^{\sigma}\chi_i(h) = \sigma(\chi_i(h))$$

for $h \in H$. This action is transitive and without fixed points on the set of characters. Hence, $n = |\mathfrak{g}|$. Let $\mathfrak{h}$ be the Galois group of $\boldsymbol{Q}_p(\zeta)/\boldsymbol{Q}_p$. To make the connection between $\mathfrak{g}$ and $\mathfrak{h}$ clear, we choose an embedding of $\boldsymbol{Q}(\zeta)$ into $\boldsymbol{Q}_p(\zeta)$ and fix it once for all. Denote this embedding by ι_ζ. The group $\mathfrak{h}$ is regarded as the Galois group of $\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(\zeta) \cap \boldsymbol{Q}_p$ by restriction onto $\boldsymbol{Q}(\zeta)$. Put $m = |\mathfrak{h}|$ and $L = \boldsymbol{Q}(\zeta) \cap \boldsymbol{Q}_p$. Let $\tau_1 = 1, \cdots, \tau_m$ be all of the elemnts of $\mathfrak{h}$. We decompose $\mathfrak{g}$ into a disjoint union of left cosets:

$$\mathfrak{g} = \sigma_1\mathfrak{h} \cup \cdots \cup \sigma_l\mathfrak{h}, \quad \sigma_1 = 1.$$

We renumber the characters by selecting and fixing the initial character χ so that

$$\begin{array}{llll} \chi_1 = \chi, & \chi_2 = {}^{\sigma_2}\chi, & \cdots, & \chi_l = {}^{\sigma_l}\chi \\ \chi_{l+1} = {}^{\tau_2}\chi, & \chi_{l+2} = {}^{\sigma_2\tau_2}\chi, & \cdots, & \chi_2 = {}^{\sigma_l\tau_2}\chi \\ & & \cdots & \end{array}$$

$$\chi_{m_1 l+1} = {}^{\tau_m}\chi, \chi_{m_1 l+2} = {}^{\sigma_2\tau_2}\chi, \cdots, \chi_{ml} = {}^{\sigma_l\tau_m}\chi,$$

where $m_1 = m-1$. By virtue of this numbering, we obtain H-invariant objects

$$(5) \qquad \varphi_i = \sum_{j=0}^{m-1} \chi_{i+jl}, \quad \delta_i = \sum_{j=0}^{m-1} e_{\chi_{i+jl}}.$$

Since H is abelian, these elements are L-rational. Namely, δ_i is identity of the ring $\delta_i LH$ and φ_i is the character of its left regular representation of H. By (3) and (4), we have

$$(6) \qquad e = \delta_1 + \cdots + \delta_l,$$

$$(7) \qquad \varphi = \varphi_1 + \cdots + \varphi_l.$$

THEOREM 5. *Let M be a $\boldsymbol{Q}H$-simple module of $E^{\boldsymbol{Q}}$. Let V be a $\boldsymbol{Q}_p$-subspace in $U^{\boldsymbol{Q}_p}$ generated by $\Delta^{\boldsymbol{Q}}(M)$. Let Δ^L be the extension of coefficients to L of $\Delta^{\boldsymbol{Q}}$, which is defined to be $\iota_\zeta \otimes \Delta_p$:*

$$\Delta^L : L \otimes_{\boldsymbol{Q}} E^{\boldsymbol{Q}} \longrightarrow \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} U_p^{(e)}.$$

Then, $\dim_{\boldsymbol{Q}} M = \dim V$ holds if and only if $\Delta^L(\delta_i M^L)$ do not vanish for every i's.

Proof. Let μ be a generator of M. V is a $\boldsymbol{Q}_p H$-subspace generated by it over $\boldsymbol{Q}_p H$. By (6), M^L and V are decomposed into sums of simple modules $\delta_i M^L$ and $\delta_i V$, respectively. We have

$$\begin{aligned} \Delta^L(\delta_i\mu) &= \Delta^L\left(\frac{1}{|H|}\sum_{h\in H}\varphi(h^{-1})\otimes h\mu\right) \\ &= \frac{1}{|H|}\sum_{h\in H}\iota_\zeta(\varphi(h^{-1}))\otimes\Delta_p(h\mu) \\ &= \delta_i\Delta^L(\mu). \end{aligned}$$

Hence, if $\Delta^L(\delta_i\mu) \neq 0$ for every i's,

$$\begin{aligned} \dim V &= \sum_{i=1}^{l} \dim \delta_i V \\ &= \sum_{i=1}^{l} \varphi_i(1) = \varphi(1) \\ &= \dim_{\boldsymbol{Q}} M. \end{aligned}$$

Since the converse is clear, we prove the statement □

We expect the following assertion is true:

ASSERTION 1. *If there exists i such that $\Delta^L(\delta_i\mu) \neq 0$, then $\Delta^L(\delta_i\mu) \neq 0$ for every i's.*

If $L = \boldsymbol{Q}$, this assertion is clearly true.

4. Abelian extensions of a real quadratic field. Set a real quadratic field to k. We see $r = 2$ and H is a normal subgroup of G. We assume that Assertion 1 holds in K. This means Δ^L is injective. Let K^* be the maximal abelian extension of $\boldsymbol{Q}$ contained in K and denote by H^* the Galois group of K/K^*. H^* is the commutator subgroup $[G, G]$. Denote by e^* the idempotent

$$\frac{1}{|H^*|}\sum_{h\in H^*} h.$$

Since the Leopoldt conjecture is true in K^*, we focus on the map

$$\Delta^{\boldsymbol{Q}} : (1-e^*)\boldsymbol{Q}H\varepsilon_1 \oplus (1-e^*)\boldsymbol{Q}H\varepsilon_2 \longrightarrow U^{\boldsymbol{Q}_p}.$$

Let A be a simple subring contained in $(1-e^*)\boldsymbol{Q}H$. Put $M_i = A\varepsilon_i$ for $i = 1, 2$. Denote by V_i the $\boldsymbol{Q}_p$-subspaces generated by $\Delta^{\boldsymbol{Q}}(M_i)$. By Theorem 5, we have $\dim_{\boldsymbol{Q}} M_i = \dim V_i$. Let W be a sum of V_i in $U^{\boldsymbol{Q}_p}$. The dimension formula implies

$$\dim V_1 \cap V_2 = 2\dim_{\boldsymbol{Q}} A - \dim W.$$

We abbreviate τ_2 to τ. Denote by ${}^\tau\alpha$ (*resp.* α^τ) for an element α of $\boldsymbol{Q}_pH$ the left (*resp.* right) conjugation $\tau\alpha\tau^{-1}$ (*resp.* $\tau^{-1}\alpha\tau$). Since $\tau\alpha\Delta^{\boldsymbol{Q}}(\varepsilon_1) = {}^\tau\alpha\Delta^{\boldsymbol{Q}}(\varepsilon_2)$, we see

$$\begin{aligned}\tau V_1 &= \tau A^{\boldsymbol{Q}_p}\Delta^{\boldsymbol{Q}}(\varepsilon_1) = {}^\tau A^{\boldsymbol{Q}_p}\Delta^{\boldsymbol{Q}}(\varepsilon_2)\\ \tau V_2 &= \tau A^{\boldsymbol{Q}_p}\Delta^{\boldsymbol{Q}}(\varepsilon_2) = {}^\tau A^{\boldsymbol{Q}_p}\tau^2\Delta^{\boldsymbol{Q}}(\varepsilon_1)\\ &= {}^\tau A^{\boldsymbol{Q}_p}\Delta^{\boldsymbol{Q}}(\varepsilon_1)\end{aligned}$$

because of $\tau^2 \in H$. Denote by ${}^\tau V_i$ the conjugate modules τV_i for $i = 1, 2$.

The degree of an irreducible $\overline{\boldsymbol{Q}}_p$-representation of G is one or two by the theorem of N. Ito, *cf.* Corollary 11.33 in [2]. Since each character χ_i is not trivial on $[G, G]$, the induced character $\mathrm{Ind}_H^G\chi_i$ is an irreducible character of degree two. By Clifford's theorem, *cf.* Theorem 11.1 in [2], we have

$$\mathrm{Res}_H^G\mathrm{Ind}_H^G A_i^{\overline{\boldsymbol{Q}}_p} \cong A_i^{\overline{\boldsymbol{Q}}_p} \oplus {}^\tau A_i^{\overline{\boldsymbol{Q}}_p},$$

Hence, this $\overline{\boldsymbol{Q}}_pG$-module is irreducible. We reduce coefficients to $\boldsymbol{Q}$ and obtain

$$\mathrm{Res}_H^G\mathrm{Ind}_H^G A \cong A \oplus {}^\tau A.$$

The $\boldsymbol{Q}H$-modules A and ${}^\tau A$ are irreducible and are equal if and only if $e = {}^\tau e$. Since $\delta_i\Delta^{\boldsymbol{Q}}(\varepsilon_1) \neq 0$ (*resp.* ${}^\tau\delta_i\Delta^{\boldsymbol{Q}}(\varepsilon_2) \neq 0$), we have $\delta_i V_1 \cong \delta_i A^{\boldsymbol{Q}_p}$ and ${}^\tau\delta_i{}^\tau V_1 \cong {}^\tau\delta_i{}^\tau A^{\boldsymbol{Q}_p}$.

Let X be the set of characters defined by the decomposition (5). Let ${}^\tau\chi$ be the character defined by ${}^\tau\chi(h) = \chi(h^\tau)$ for a character χ of H. We observe that $X = {}^\tau X$ is equivalent to $X \cap {}^\tau X \neq \emptyset$. Hence, $e = {}^\tau e$ holds if and only if X and ${}^\tau X$ are not disjoint.

We suppose that $V_1 = V_2$. Then, ${}^\tau V_1 = {}^\tau V_2$. We note that this condition is equivalent to $\delta_i V_1 = \delta_i V_2$ holds for every i's. There are elements α, β such that

$$\begin{aligned}e\Delta^{\boldsymbol{Q}}(\varepsilon_2) &= \alpha e\Delta^{\boldsymbol{Q}}(\varepsilon_1),\\ e\Delta^{\boldsymbol{Q}}(\varepsilon_1) &= \beta e\Delta^{\boldsymbol{Q}}(\varepsilon_2),\end{aligned}$$

We see $\alpha\beta e = e$. By conjugation, we obtain

$$\begin{aligned}{}^\tau e\Delta^{\boldsymbol{Q}}(\varepsilon_1) &= \tau^{-2}\,{}^\tau\alpha{}^\tau e\Delta^{\boldsymbol{Q}}(\varepsilon_2),\\ {}^\tau e\Delta^{\boldsymbol{Q}}(\varepsilon_2) &= \tau^2\,{}^\tau\beta{}^\tau e\Delta^{\boldsymbol{Q}}(\varepsilon_1).\end{aligned}$$

We suppose $e = {}^{\tau}e$ in addition. Then, V_1 is a QG-module. We see $\tau^{-2}\,{}^{\tau}\alpha e = \beta e$ and $\tau^2\,{}^{\tau}\beta e = \alpha e$ holds in Q_pH. Thus, ${}^{\tau}\alpha\alpha e = \tau^2\beta\alpha e = \tau^2 e$. In account of the decomposition of e in Q_pH, a unique integer i^* is determined for each i so that $\delta_{i^*} = {}^{\tau}\delta_i$ holds. If $i = i^*$, $\delta_i V_i$ is a simple Q_pG-module. If $i \neq i^*$, the simple Q_pG-module containing $\delta_i V_1$ is a sum $\delta_i V_1 + \delta_{i^*} V_1$.

LEMMA 6. *There is $\sigma \in \mathfrak{g}$ for each i such that ${}^{\sigma}\chi_1 = \chi_i$ holds. Hence, if $\delta_1 \neq \delta_{1^*}$, we have $\delta_i \neq \delta_{i^*}$ for every i.*

Proof. The group $\mathfrak{g}/\mathfrak{h}$ acts on the set $\{\delta_i\}$ of idempotents transitively. Hence, there is $\sigma \in \mathfrak{g}$ such that ${}^{\sigma}\delta_1 = \delta_i$. Moreover, since

$${}^{\tau}({}^{\sigma}\chi_1) = {}^{\sigma}({}^{\tau}\chi_1)$$

hold for every i, we have $\delta_i \neq \delta_{i^*}$ if $\delta_1 \neq \delta_{1^*}$. □

We note the condition $e = {}^{\tau}e$ holds if H is a cyclic group. The set X of irreducible $\overline{Q}_p$-characters satisfies $X = {}^{\tau}X$. However, ${}^{\tau}\chi \neq \chi$ for every characters belonging to X. If $\delta_i = \delta_{i^*}$, the decomposition of δ_i is a sum of pairs of idempotents e_χ and $e_{{}^{\tau}\chi}$. Thus, the integer m must be even in (5). We conclude that

THEOREM 7. *Suppose H is cyclic. Then, $V_1 \cap V_2 = \{0\}$ if $\delta_1 = \delta_{1^*}$ and if m is odd.*

Refernces

[1] A. BRUMER; On the units of algebraic number fields, Mathematika **14**(1967), 121–124.

[2] C. W. CURTIS *and* I. REINER; Methods of representation theory with applications to finite groups and orders I, JOHN WILY & SONS, New York·Chichester·Brisbane·Toront, 1981.

[3] M. EMSALEM, H. KISILEVSKY IT AND D. WALES; Indepéndance linéare sue $\overline{Q}$ de logarithmes p-adiques de nombre algébriques et rang p-adique du groupes des unités d'un corps de nombres, J. Number Theory **19**(1984), 384–391.

[4] J.-F. JAULENT; Sur L'indépendence l-adique de nombres algébriques, J. Number Theory **20**(1985), 149–158.

[5] J. NEUKIRCH; Algebraische Zahlentheorie, Springer-Verlag Berlin Heiderberg New York, 1992.

[6] L. C. WASHINGTON; Introduction to Cyclotomic Fields Second ed.; GTM 83, Springer-Verlag New York Berlin Heiderberg, 1982.