On indivisibility of relative class numbers of totally imaginary quadratic extensions and these relative Iwasawa invariants

By Yuuki TAKAI

Department of Mathematics, Faculty of Science and Technology, Keio University,
3-14-1 Hiyoshi, Kohoku-ku, Yokohama, Kanagawa 223-8522, Japan

(Communicated by Masaki KASHIWARA, M.J.A., Jan. 14, 2014)

Abstract: In this paper, we announce some results on indivisibility of relative class numbers of CM quadratic extensions K/F of a fixed totally real number field F which is Galois over $\mathbf{Q}$ and on vanishing of these relative Iwasawa λ_p-, μ_p-invariants. In particular, we give a lower bound of the number of such CM extensions K/F with bounded (norm of) relative discriminants. To prove them, we use Hilbert modular forms of half-integral weight.

Key words: Relative class numbers; relative Iwasawa invariants; Hilbert modular forms of half-integral weight; Sturm's theorem.

1. Introduction. The structure of ideal class groups of number fields is one of the main objects to be investigated, but little is known. For number field F, let $Cl(F)$ be the ideal class group of F and $h(F)$ be the order of $Cl(F)$ called by the class number of F. For Galois extension K/F, we define the relative ideal class group $Cl(K/F)$ as the kernel of the homomorphism $Cl(K) \to Cl(F)$ induced by the relative norm $N_{K/F} : I_K \to I_F$, where I_K, I_F are the ideal group of K, F. The order of $Cl(K/F)$ is called the relative class number of K/F, denoted by $h(K/F)$. The distribution of class numbers of number fields is still mysterious. Cohen, Lenstra and Martinet [3,4] predicted the following: Let $\Sigma = (G, F, \sigma)$ be a *situation* in the sense of [12, §. 1], *i.e.*, G be a transitive permutation group of degree $n \geq 2$, F a number field, and σ a possible signature of the infinite places of a degree n extension K/F with the Galois group of the Galois closure of K/F is isomorphic to G. For the situation Σ, we set $\mathcal{K}(\Sigma)$ as the set of the degree n extension K/F with Galois group G and signature σ. We set $\mathcal{O}_F$ as the ring of the integers of F. Then for a positive integer u depending on Σ and *good prime* p in the sense of [4, Def. 6.1], a given finite p-torsion $\mathcal{O}_F$-module H should occur as a Sylow subgroup of $Cl(K/F)$ for $K \in \mathcal{K}(\Sigma)$ with probability

$$\frac{c}{|H|^u |\mathrm{Aut}_{\mathcal{O}_L} H|}$$

for a certain constant c depending only on p and Σ. Malle [12] modified the conjecture when p-th roots of unity is in F. But, at the moment, the distribution is unmanageable except for the $p = 3$ case.

Here, we focus on the situation $\Sigma = (C_2, F, \text{complex})$ for totally real number field F, *i.e.*, $\mathcal{K}(\Sigma)$ is the set of the totally imaginary quadratic extensions over F called CM quadratic extensions. In this situation, we set

$$M(F, X) = \{K/F : \text{CM quad.ext.} \mid |N_{F/\mathbf{Q}}(D(K/F)| < X\},$$
$$M(F, X, p) = \{K/F \in M(X, F, H) \mid p \nmid h(K/F)\}.$$

Then the following is known:

- $\lim_{X\to\infty} \#M(F, X, p) = \infty$: Gauss ($p = 2, F = \mathbf{Q}$), Hartung [8] ($p = 3, F = \mathbf{Q}$), Horie [9], Brunier [1] ($p \geq 3, F = \mathbf{Q}$) and Naito [13] (general F, odd prime p, $p \nmid w_2\zeta_F(-1)$, where $w_{2,F} = \#H^0(F, \mathbf{Q}/\mathbf{Z}(2))$).
- Limit inferiors of $\#M(F, X, 3)/\#M(F, X)$: Davenport-Heilbronn [6] ($F = \mathbf{Q}$) and Datskovsky-Wright [5] (general F).
- A lower bound of $\#M(F, X, p)$: Kohnen-Ono [11] ($p \geq 3, F = \mathbf{Q}$).

In this paper, we introduce a generalization of the result of Kohnen-Ono to totally real field F which is a Galois extension over $\mathbf{Q}$ for some prime p.

The class numbers are complicate, but Iwasawa showed the following monumental formula: For number field L and odd prime number p, let L_∞ be a Galois extension over L with the Galois group $\mathrm{Gal}(L_\infty/L) \simeq \mathbf{Z}_p$, *i.e.*, $\mathbf{Z}_p$-extension of L and

2000 Mathematics Subject Classification. Primary 11F33, 11R29; Secondary 11F37, 11F41, 11R23.

doi: 10.3792/pjaa.90.33

L_n be the intermediate field of L_∞/L such that $\mathrm{Gal}(L_n/L) \simeq \mathbf{Z}/p^n\mathbf{Z}$. Then there are integers λ, μ, ν such that for all sufficiently large n

$$\# Cl(L_n)[p] = p^{\lambda n + \mu p^n + \nu},$$

where $G[p]$ is the p-part of group G. The integers $\lambda_p(L) = \lambda(L) = \lambda$, $\mu_p(L) = \mu(L) = \mu$, $\nu_p(L) = \nu(L) = \nu$ are called Iwasawa invariants of L. We remark that $\lambda(L)$ and $\mu(L)$ are very important for arithmetic applications. We return to our setting. We assume that p is odd. For CM quadratic extension K/F, we consider λ, μ, ν for those cyclotomic $\mathbf{Z}_p$-extensions, *i.e.*, each of the extensions is the composite field of K (or F) and the unique $\mathbf{Z}_p$-extension over $\mathbf{Q}$. Then we set

$$\lambda^-(K) = \lambda(K) - \lambda(F),$$
$$\mu^-(K) = \mu(K) - \mu(F),$$
$$\nu^-(K) = \nu(K) - \nu(F)$$

called relative Iwasawa invariants of K/F. Although these invariants are also strange, Friedman proved that indivisibility of relative class numbers of K/F and the decomposition condition of prime p at K/F imply vanishing of relative λ-, μ-invariants. We are also interested in the distribution of relative Iwasawa invariants. We set

$$N(F, X, p) = \{K/F \in M(X, F) \mid \lambda_p(K) = \mu_p(K) = 0\}.$$

As applications of the vanishing criterion, the followings are known:

- $\lim_{X\to\infty} \# N(F, X, p) = \infty$: Horie [9] ($p \geq 3$ and $F = \mathbf{Q}$) and Naito [13] (general F, $p \geq 3$, $p \nmid w_{2,F}\zeta_F(-1)$).
- A limite inferior of $\# N(F, X, 3)/\# N(F, X)$: Horie-Kimura [10].
- A lower bound of $\# N(F, X, p)$: Byeon [2] ($p > 3$ satisfying some conditions).

Here, we also introduce the generalization of the result of Byeon to totally real field F which is Galois over $\mathbf{Q}$ for odd prime p satisfying some conditions.

The purpose of this paper is to announce results whose proofs and detailed accounts will be published elsewhere [16].

2. Indivisibility of relative class numbers. To get the lower bound, we use Hilbert modular Eisenstein series of parallel weight 3/2. Therefore we review notion of Hilbert modular forms of half integral weight. We use the terminology in [14]. This terminology is slightly different from [15], but in the parallel weight case, the difference is only the factor of automorphy (and also "Nebentypus" character).

Let F be a totally real number field, $g = [F : \mathbf{Q}]$, $\mathfrak{d}_F$ be the different ideal of $F/\mathbf{Q}$, and $D(F)$ be the discriminant of $F/\mathbf{Q}$. Let $\mathbf{a}$ and $\mathbf{f}$ be the set of the archimedean places and the non-archimedean places of F respectively. For $v \in \mathbf{a}$ and $\xi \in F$, ξ_v denotes the image of ξ by the map $F \hookrightarrow F_v$, where F_v is the completion of F with respect to v. Let $\mathfrak{H} = \mathcal{H}^g$ be the g-tuple product of the upper-half plane. For $\xi \in F$, we set $\mathbf{e}(\xi z) = e^{2\pi\sqrt{-1}Tr(\xi z)}$, where $Tr(\xi z) = \sum_{v\in\mathbf{a}} \xi_v z_v$. For integral ideal $\mathfrak{c} \subset 4\mathcal{O}_F$, we set

$$\Gamma_0(\mathfrak{c}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(F) \;\middle|\; \begin{matrix} a, d \in \mathcal{O}_F, b \in 2\mathfrak{d}^{-1} \\ c \in 2^{-1}\mathfrak{c}\mathfrak{d} \end{matrix} \right\}.$$

To define a factor of automorphy, we use the following theta series:

$$\theta(z) = \sum_{\xi\in\mathcal{O}_F} \mathbf{e}(\xi^2 z/2).$$

We define the factor of automorphy $h(\gamma, z)$ as follows:

$$h(\gamma, z) = \theta(\gamma z)/\theta(z) \quad \text{for } \gamma \in \Gamma_0(4\mathcal{O}_F).$$

The factor $h(\gamma, z)$ satisfies

$$h(\gamma, z)^2 = \mathrm{sgn}(N_{F/\mathbf{Q}}(d_\gamma))\vartheta^*(d_\gamma \mathcal{O}_F) J(\gamma, z),$$

where ϑ^* is the ideal character associated with the extension $F(\sqrt{-1})/F$ and

$$J(\alpha, z) = \prod_{v\in\mathbf{a}} (c_v z_v + d_v) \quad \text{for } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We introduce the group

$$\mathcal{G}_F = \left\{ (\alpha, \phi_\alpha(z)) \;\middle|\; \begin{matrix} \alpha \in G_F, {}^\exists t \in \mathbf{T} \\ \text{s.t. } \phi_\alpha(z)^2 = tJ(\alpha, z) \end{matrix} \right\},$$

where $\mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\}$. The group law is defined as

$$(\alpha, \phi_\alpha(z))(\beta, \phi_\beta(z)) = (\alpha\beta, \phi_\alpha(\beta z)\phi_\beta(z)).$$

Then we have the injection $\Gamma_0(4\mathcal{O}_F) \to \mathcal{G}_F$: $\gamma \mapsto (\gamma, h(\gamma, z))$. We regard $\Gamma_0(4\mathcal{O}_F)$ as a subgroup of $\mathcal{G}_F$

For $\xi = (\alpha, \phi(z)) \in \mathcal{G}_F$ and $k \in \mathbf{Z}$, we set

$$f|_k[\xi](z) = f(\alpha z)\phi(z)^{-k}.$$

Let ψ be a Hecke character whose conductor divides $\mathfrak{c}$ and $k \in \mathbf{Z}$. Then Hilbert modular form f of parallel weight $k/2$, level $\Gamma_0(\mathfrak{c})$, and "Nebentypus" character ψ is defined to be

$$f|_k[(\gamma, h(\gamma, z))](z) = \psi(d_\gamma) f \text{ for all } \gamma \in \Gamma_0(\mathfrak{c}).$$

$M_{k/2}(\Gamma_0(\mathfrak{c}), \psi)$ denotes the vector spaces of the forms of parallel weight $k/2$, level $\Gamma_0(\mathfrak{c})$ and character ψ.

We review an Eisenstein series of weight $3/2$, denoted by $\overline{E}'$. The Eisenstein series was constructed by Shimura [14, Prop. 6.3].

Lemma 1 (Shimura)**.** *The Eisenstein series $\overline{E}'$ is a form of parallel weight 3/2, level $\Gamma_0(\mathfrak{c})$, and character ψ, and its Fourier expansion is as follows:*

$$\overline{E}' = a_0 + \sum_{\xi \in 2^{-1}\mathcal{O}_{F,+}} a_\xi \mathbf{e}(\xi z),$$

where

$$a_\xi = \beta(\xi) \frac{2^g h^-(F(\sqrt{-2\xi}))}{Q_{F(\sqrt{-2\xi})} w_{F(\sqrt{-2\xi})}},$$

$$\beta(\xi) = \sum_{\mathfrak{a},\mathfrak{b}} \mu(\mathfrak{a}) \left(\frac{F(\sqrt{-2\xi})/F}{\mathfrak{a}} \right) N_{F/\mathbf{Q}}(\mathfrak{b}),$$

the pair $(\mathfrak{a}, \mathfrak{b})$ runs the all integral ideals relatively prime to $2\mathcal{O}_F$ such that $(\mathfrak{ab})^2 | 2\xi\mathcal{O}_F$, μ is the Möbius function, $Q_{F(\sqrt{-2\xi})} \in \{\pm 1\}$ is the Hasse index of $F(\sqrt{-2\xi})$, and $w_{F(\sqrt{-2\xi})}$ is the number of roots of unity in $F(\sqrt{-2\xi})$.

Remark 1. If $p - 1 > 2g$, then $p \nmid w_{F(\sqrt{-2\xi})}$. Indeed, if a primitive p-th root of unity ζ_p is in $F(\sqrt{-2\xi})$, then $\mathbf{Q}(\zeta_p) \subset F(\sqrt{-2\xi})$, so $2g = [F(\zeta_p) : \mathbf{Q}] \geq [\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$. Thus for prime $p > 2g + 1$, the all coefficient a_ξ $(\xi \neq 0)$ is p-integral. More precisely, $p \nmid w_{F(\sqrt{-2\xi})}$ if $p \nmid w_F$ for w_F in §.1.

Showing indivisibility of the coefficients of $\overline{E}'$ of twists by quadratic characters χ_i, we prove the following indivisibility result of relative class numbers of CM quadratic extensions of fixed totally real number field which is Galois over $\mathbf{Q}$.

Theorem 1. *Let $g = [F : \mathbf{Q}]$, $D(F)$ be the discriminant of $F/\mathbf{Q}$, p be a prime such that $g \leq M(p) 2^{-\mathrm{ord}_2(M(p))}$ and $p > 2g + 1$, r a positive integer, $\epsilon_1, \epsilon_2, \ldots, \epsilon_r \in \{0, \pm 1\}$ such that $\epsilon_i \neq 0$ for some i, $\chi_1, \chi_2, \ldots, \chi_r$ be quadratic Hecke characters of F whose conductor is integral ideal $\mathcal{N}_1$, $\mathcal{N}_2, \ldots, \mathcal{N}_r$ respectively. We set the positive integer N as $N\mathbf{Z} = \mathcal{N}_1 \mathcal{N}_2 \cdots \mathcal{N}_r \cap \mathbf{Z}$ and set*

$$A = \frac{gN^2 D(F)}{8} \prod_{d | ND(F),\ d:\text{prime}} \left(1 + \frac{1}{d}\right).$$

If there is a prime number $q > (A/g)^g$ such that

$$\sum_{\substack{\xi \in 2^{-1}\mathcal{O}_{F,+},\ \chi_i(\xi) = \epsilon_i, i = 1,2,\ldots,r \\ Tr(\xi) = qg/2,\ (q\mathcal{O}_F, 2\xi\mathcal{O}_F) \neq 1}} a_\xi \not\equiv 0 \bmod p,$$

then

$$\#\left\{ K = F(\sqrt{-2\xi}) \in M(F, X, p) \;\middle|\; \begin{array}{l} \chi_i(\xi) = \epsilon_i \text{ for} \\ i = 1, 2, \ldots, r \end{array} \right\} \gg \frac{X^{\frac{1}{2g}}}{\log X},$$

where $f(x) \gg g(x)$ means that there is a positive constant C such that $f(x) > Cg(x)$ for any sufficiently large x.

Remark 2. The assumption of prime p is mild, because we can choose the prime q quite freely. Moreover, when $p \nmid D(F)$, the first assumption can be replaced to $g \leq (p-1)/2^{\mathrm{ord}_2(p-1)}$. For $g = 2$ (real quadratic case), exceptional prime p is only the Fermat primes and these are known only 3, 5, 17, 257, 65537.

Remark 3. For the technical reason, we need the assumption that F is a Galois extension of $\mathbf{Q}$. Because, we have to control the other prime $\ell \neq p$ in the proof of Theorem 1 as totally splitting at $F/\mathbf{Q}$.

As a corollary of the proof of Theorem 1, we can prove the following simple statement for sufficiently large primes.

Corollary 1. *Let F be a totally real number extention of finite Galois over $\mathbf{Q}$. Then, for sufficiently large p*

$$\#M(F, X, p) \gg \frac{X^{\frac{1}{2g}}}{\log X}.$$

3. Vanishing of relative Iwasawa invariants. If we take a certain character as the quadratic character χ in the statement of Theorem 1, we can investigate vanishing of relative Iwasawa invariants.

Friedman [7, Criterion 1.0] showed vanishing criterion of relative Iwasawa invariants of CM fields.

Lemma 2. *Let K be a CM field, K^+ the maximal totally real subfield of K, and p an odd prime. Then the followings are equivalent:*

(a) $\lambda_p^-(K) = \mu_p^-(K) = 0$,

(b) *$p \nmid h^-(K)$ and there is no prime ideal $\mathfrak{p} | p\mathcal{O}_F$ of K^+ splitting at K/K^+.*

For prime number $p \geq 3$ and its prime ideal factorization $p\mathcal{O}_F = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$, we set the character

χ_i as quadratic residue symbol:

$$\chi_i(\xi) = \left(\frac{F(\sqrt{-2\xi})/F}{\mathfrak{p}_i}\right).$$

Taking all χ_i as the character and $\epsilon_i \in \{-1, 0\}$ for $i = 1, 2, \ldots, r$ or adding an auxiliary character if $\epsilon_i = 0$ for all i, we have the following theorem:

Theorem 2. *Let $g = [F : \mathbf{Q}]$ and $D(F)$ be the discriminant of $F/\mathbf{Q}$. Let p be a prime such that $g \leq [F(\zeta_p) : F]/2^{\mathrm{ord}_2([F(\zeta_p):F])}$ and $p > 2g + 1$. We set*

$$A = \frac{gp^2 D(F)}{8} \prod_{d \mid pD(F),\ d:\mathrm{prime}} \left(1 + \frac{1}{d}\right).$$

If there is a prime number $q > (A/g)^g$ such that

$$\sum_{\substack{\xi \in 2^{-1}\mathcal{O}_{F,+}, \chi_i(\xi)=\epsilon_i\ (i=1,2,\ldots,r) \\ Tr(\xi)=qg/2,\ (q\mathcal{O}_F, 2\xi\mathcal{O}_F)\neq 1}} a_\xi \not\equiv 0 \mod p,$$

then

$$\#N(F, X, p) \gg_{F,p} \frac{X^{\frac{1}{2g}}}{\log X}.$$

Remark 4. We cannot prove the similar result to Corollary 1 for Theorem 2. Indeed, in the case of Theorem 2 the constant A depends on p. Thus even if we take sufficiently large prime p, we cannot ensure the existence of the summation indivisible by p.

We give a simple example on Theorem 2 for an exceptional prime number of Naito [13].

Example 1. Let $F = \mathbf{Q}(\sqrt{44})$, $p = 7$. (For real quadratic fields, the exceptional primes are Fermat primes.) We note that $p \mid w_F \zeta_F(-1)$, *i.e.*, this case is an exceptional case of Naito [13]. Then $A = 1008$ and $(A/g)^g = 254016$. As the prime q, we choose $q = 254027$ which is inert at F. Then we have

$$\sum_{\substack{\xi \in 2^{-1}\mathcal{O}_{F,+}, \chi_i(\xi)=-1\ (i=1,2) \\ Tr(\xi)=qg/2,\ (q\mathcal{O}_F, 2\xi\mathcal{O}_F)\neq 1}} a_\xi = \frac{2^g h^-(F(\sqrt{-q}))}{Q_{F(\sqrt{-q})} w_{F(\sqrt{-q})}}$$

$$= u \times 27686 \equiv u \times 1 \not\equiv 0 \mod 7,$$

where u is a p-unit. Thus we have

$$\#N(\mathbf{Q}(\sqrt{44}), X, 7) \gg \frac{X^{\frac{1}{4}}}{\log X}.$$

Acknowledgements. This research was partially supported by MEXT Grant-in-Aid for Young Scientists (B) (23740011), JSPS Grant-in-Aid for Scientific Research (B) (21340004) and JSPS Grant-in-Aid for Young Scientists (S) (21674001).

References

[1] J. H. Bruinier, Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms, Duke Math. J. **98** (1999), no. 3, 595–611.

[2] D. Byeon, A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms, Acta Arith. **89** (1999), no. 3, 295–299.

[3] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983* (*Noordwijkerhout, 1983*), 33–62, Lecture Notes in Math., 1068, Springer, Berlin, 1984.

[4] H. Cohen and J. Martinet, Class groups of number fields: numerical heuristics, Math. Comp. **48** (1987), no. 177, 123–137.

[5] B. Datskovsky and D. J. Wright, Density of discriminants of cubic extensions, J. Reine Angew. Math. **386** (1988), 116–138.

[6] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields. II, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[7] E. Friedman, Iwasawa invariants, Math. Ann. **271** (1985), no. 1, 13–30.

[8] P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, J. Number Theory **6** (1974), 276–278.

[9] K. Horie, A note on basic Iwasawa λ-invariants of imaginary quadratic fields, Invent. Math. **88** (1987), no. 1, 31–38.

[10] K. Horie and I. Kimura, On quadratic extensions of number fields and Iwasawa invariants for basic $\mathbf{Z}_3$-extensions, J. Math. Soc. Japan **51** (1999), no. 2, 387–402.

[11] W. Kohnen and K. Ono, Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication, Invent. Math. **135** (1999), no. 2, 387–398.

[12] G. Malle, On the distribution of class groups of number fields, Experiment. Math. **19** (2010), no. 4, 465–474.

[13] H. Naito, Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants, J. Math. Soc. Japan **43** (1991), no. 1, 185–194.

[14] G. Shimura, On Eisenstein series of half-integral weight, Duke Math. J. **52** (1985), no. 2, 281–314.

[15] G. Shimura, On Hilbert modular forms of half-integral weight, Duke Math. J. **55** (1987), no. 4, 765–838.

[16] Y. Takai, Indivisibility of relative class numbers of totally imaginary quadratic extensions and vanishing of these relative iwasawa invariants. (Preprint). `http://www.math.keio.ac.jp/~takai/pdfs/Indivisibility.pdf`.