Computation of Iwasawa ν-invariants of certain real abelian fields

Hiroki Sumida*

Abstract

Let p be a prime number and k a finite extension of $\mathbf{Q}$. It is conjectured that Iwasawa invariants $\lambda_p(k)$ and $\mu_p(k)$ vanish for all p and totally real number fields k. Using cyclotomic units and Gauss sums, we give an effective method for computing the other Iwasawa invariants $\nu_p(k)$ of certain real abelian fields. As numerical examples, we compute Iwasawa invariants associated to $k = \mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$ in the range $1 < f < 200$, $5 \leq p < 10000$.

1 Introduction

Let p be a prime number and k a finite extension of $\mathbf{Q}$. Denote by k_∞ the cyclotomic $\mathbf{Z}_p$-extension of k and by k_n the subfield of k_∞ such that $[k_n : k] = p^n$. Let $A_n(k)$ be the p-Sylow subgroup of the ideal class group of k_n and $p^{e_n(k)}$ the order of $A_n(k)$. Iwasawa proved that there are three invariants $\lambda_p(k)$, $\mu_p(k)$ and $\nu_p(k)$ such that $e_n(k) = \lambda_p(k)n + \mu_p(k)p^n + \nu_p(k)$ for all sufficiently large n (cf. [15]).

It is conjectured that μ-invariants vanish for all p and k. In fact, Ferrero and Washington proved that $\mu_p(k) = 0$ for all p and abelian number fields k in [4]. For λ-invariants, there are many (non-totally real) number fields k with $\lambda_p(k) > 0$ (cf. [7, p. 266]). On the other hand, it is conjectured that $\lambda_p(k) = \mu_p(k) = 0$ for all p and totally real number fields k, which is called

*Partially supported by the Grants-in-Aid of the Sumitomo Foundation. Partially supported by the Grants-in-Aid for Encouragement of Young Scientists (No.11740020), The Ministry of Education, Science, Sports and Culture of Japan.
Mathematics Subject Classification (2000): 11R23

Key words and phrases: Iwasawa invariant, ideal class group, cyclotomic unit, Gauss sum, Vandiver's conjecture, Greenberg's conjecture

as Greenberg's conjecture. At present, we have some numerical examples supporting this conjecture for abelian fields (e.g. [10, 12, 17, 20]). In their methods, cyclotomic units and prime numbers are used.

In [11], by a similar method, we verify $\lambda_p(k) = \mu_p(k) = 0$ for $p = 3, 5, 7$ and quadratic fields k with small discriminants, and give an upper bound for $\nu_p(k)$. However it is difficult to determine the exact value by their methods, because we need to find a p-th root of a cyclotomic unit (cf. [24, pp.420–423]). In this paper, by using cyclotomic units, Gauss sums and prime numbers, we give an effective method for computing the exact values of $\nu_p(k)$ under some technical conditions.

Using our method, we can settle the values of tables in [11] by computer calculation. Moreover we compute Iwasawa invariants associated to $k = \mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$ in the range $1 < f < 200$ and $5 \leq p < 10000$, where f is the discriminant of a real quadratic field. We can obtain some examples such that $\lambda_p(k) = \mu_p(k) = 0$ and $\nu_p(k) > 0$ for large primes p. The number of such cases seems to follow the deduction in [24, pp.158–159].

2 Result

2.1 General case

We fix an inclusion map $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$, where $\overline{F}$ is the algebraic closure of a field F. Further we fix a primitive n-th root of unity ζ_n so that $\zeta_{nm}^m = \zeta_n$ for all $m, n \geq 1$. Let p be an odd prime number and f_0 an integer such that $p | f_0$ and $p^2 \nmid f_0$. Let K be a subfield of $\mathbf{Q}(\zeta_{f_0})$ containing ζ_p whose conductor is f_0. For simplicity, we assume the following condition:

$$\text{(C1)} \qquad p \text{ does not divide } |\mathrm{Gal}(K/\mathbf{Q})|.$$

Put $f_n = f_0 p^n$. Then $K_n = K\mathbf{Q}_n \subseteq \mathbf{Q}(\zeta_{f_n})$. Further put $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$, $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $G_\infty = \mathrm{Gal}(K_\infty/\mathbf{Q}) = \Delta \times \Gamma$.

Let Φ be a $\mathbf{Q}_p$-valued character of Δ which is irreducible over $\mathbf{Q}_p$. Put

$$e_\Phi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \Phi(\delta)\delta^{-1}$$

the idempotent of the group ring $\mathbf{Q}_p[\Delta]$. This is an element of $\mathbf{Z}_p[\Delta]$ by (C1). Let ϕ be an irreducible component of Φ over $\overline{\mathbf{Q}}_p$. We say Φ is even (resp. odd) when $\phi(\rho) = 1$ (resp. $\phi(\rho) = -1$), where ρ is the complex conjugate in Δ. Let $\mathcal{O}_\phi$ be the subring of $\overline{\mathbf{Q}}_p$ generated by all $\phi(\delta)$ ($\delta \in \Delta$) over $\mathbf{Z}_p$. We identify $e_\Phi \mathbf{Z}_p[\Delta]$ with $\mathcal{O}_\phi$ by $\delta \mapsto \phi(\delta)$.

We fix a topological generator γ_0 of Γ such that $\zeta_{f_n}^{\gamma_0} = \zeta_{f_n}^{1+f_0}$ for all $n \geq 0$. We identify, as usual, the complete group ring $\mathcal{O}_\phi[[\Gamma]]$ with the power series ring $\Lambda = \mathcal{O}_\phi[[T]]$ by $\gamma_0 = 1 + T$. Thus, for a $\mathbf{Z}_p[[G_\infty]]$-module M, we regard $M(\Phi) = e_\Phi M$ as a Λ-module. Let $X_\infty = X_\infty(K) = \varprojlim A_n(K)$, where the inverse limit is taken with respect to relative norm maps. Then $X_\infty(\Phi)$ is regarded as a Λ-module in the above way. We can define $e_n(\Phi)$, $\lambda_p(\Phi)$, $\mu_p(\Phi)$ and $\nu_p(\Phi)$ for $A_n(\Phi)$ and $X_\infty(\Phi)$. Let k be a subfield of K and $\phi(\delta) = 1$ for any $\delta \in \mathrm{Gal}(K/k)$. Then, since p does not divide $[K : k]$, $N_{K_n/k_n} : A_n(K)(\Phi) \to A_n(k)(\Phi)$ is an isomorphism.

From now on, let Ψ be a non-trivial even $\mathbf{Q}_p$-valued character of Δ which is irreducible over $\mathbf{Q}_p$ and ψ its fixed irreducible component of Ψ over $\overline{\mathbf{Q}}_p$. Put $\Psi^* = \Psi^{-1}\omega$ and $\psi^* = \psi^{-1}\omega$, where ω is the Teichmüller character $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}_p$ ($\omega(a) \equiv a \mod p$). We denote by $\mathcal{O}$ both $\mathcal{O}_\psi$ and $\mathcal{O}_{\psi^*}$. We fix a prime element π of $\mathcal{O}$.

Let $L_p(s,\psi)$ be the p-adic L-function associated to ψ which is constructed in [18]. By [14, §6], there uniquely exists $G_\Psi(T) \in \mathcal{O}[[T]]$ satisfying $G_\Psi((1+f_0)^{1-s} - 1) = L_p(s,\psi)$ for all $s \in \mathbf{Z}_p$. In [4], it is shown that π does not divide $G_\Psi(T)$. Therefore, by the p-adic Weierstrass preparation theorem, we can uniquely write $G_\Psi(T) = g_\Psi(T)u_\Psi(T)$, where $g_\Psi(T)$ is a distinguished polynomial of $\mathcal{O}[T]$ and $u_\Psi(T)$ is an invertible element of $\mathcal{O}[[T]]$. In a similar way, we can define $g_{\Psi^*}(T) \in \mathcal{O}[T]$ from the power series $G_{\Psi^*}(T) \in \mathcal{O}[[T]]$ satisfying $G_{\Psi^*}((1+f_0)^s - 1) = L_p(s,\psi)$. Put $\tilde{\lambda}(\Psi) = \deg g_\Psi(T) = \deg g_{\Psi^*}(T)$.

Further, for simplicity, we assume

(C2) $$\psi(p) \neq 1 \text{ and } \psi^*(p) \neq 1.$$

For a non-negative integer n, we denote by p^{a_n} (resp. $p^{a_n^*}$) the exponent of $\Lambda/(\omega_n, g_\Psi(T))$ (resp. $\Lambda/(\omega_n, g_{\Psi^*}(T))$), where $\omega_n = (1+T)^{p^n} - 1$. Since Leopoldt's conjecture holds for K_n and p ([1, 2]), we have $a_n < \infty$. Further we have $a_n^* < \infty$ by (C2). Let $\mathbf{e}_{\Psi,n}$ (resp. $\mathbf{e}_{\Psi^*,n}$) be an element of $\mathbf{Z}[\Delta]$ such that $\mathbf{e}_{\Psi,n} \equiv e_\Psi \mod p^{a_n}$ (resp. $\mathbf{e}_{\Psi^*,n} \equiv e_{\Psi^*} \mod p^{a_n^*}$) and the sum of all the coefficients is zero. Put $N = N(n) = \max\{n, a_n - 1\}$ and $N^* = N^*(N) = \max\{N, a_N^* - 1\}$.

In [10], we define the following polynomials $X_n(T) \in \mathcal{O}[T]$ and $Y_n(T) \in \mathcal{O}[T]$:

$$X_n(T)g_\Psi(T) = p^{a_n} \text{ and } Y_n(T) \equiv X_n(T) \mod p^{a_n}.$$

In a similar way, we define $X_N^*(T) \in \mathcal{O}[T]$ and $Y_N^*(T) \in \mathcal{O}[T]$:

$$X_N^*(T)g_{\Psi^*}(T) = p^{a_N^*} \text{ and } Y_N^*(T) \equiv X_N^*(T) \mod p^{a_N^*}.$$

We define a cyclotomic unit c_n of K_n by

$$c_n = \left(N_{\mathbf{Q}(\zeta_{f_n})/K_n}\left(1 - \zeta_{f_n}\right)\right)^{\mathbf{e}_{\Psi,n}}.$$

Let $\tilde{\mathcal{O}}_N$ be the ring of integers of $\mathbf{Q}(\zeta_{f_N})$ and $\tilde{\mathfrak{L}}$ a prime ideal of $\mathbf{Q}(\zeta_{f_N})$ with $\tilde{\mathfrak{L}} \nmid f_N$ which is lying above a prime number l. Denote by $\chi_{\tilde{\mathfrak{L}}}$ the character of $(\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}})^\times$ with values in $\langle \zeta_{f_N} \rangle$, defined by the following congruence:

$$\chi_{\tilde{\mathfrak{L}}}(y) = \chi_{\tilde{\mathfrak{L}}}(y \mod \tilde{\mathfrak{L}}) \equiv y^{(|\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}}|-1)/f_N} \mod \tilde{\mathfrak{L}}, \qquad y \in \tilde{\mathcal{O}}_N \text{ with } \tilde{\mathfrak{L}} \nmid y.$$

We define a Gauss sum $g'_N(\tilde{\mathfrak{L}}) \in \mathbf{Q}(\zeta_{f_N l})$ by

$$g'_N(\tilde{\mathfrak{L}}) = - \sum_{y \in (\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}})^\times} \chi_{\tilde{\mathfrak{L}}}(y) \zeta_l^{Tr(y)},$$

where Tr denotes the trace map $\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}} \to \mathbf{Z}/l\mathbf{Z}$. Let $\mathfrak{A}$ be an ideal of K_N with $\mathfrak{A}\tilde{\mathcal{O}}_N = \prod_{i=1}^r \tilde{\mathfrak{L}}_i^{e_i}$, where $\tilde{\mathfrak{L}}_i$ is a prime ideal of $\mathbf{Q}(\zeta_{f_N})$ lying above l_i. We define a Gauss sum

$$g_N(\mathfrak{A}) = \left(\prod_{i=1}^r g'_N(\tilde{\mathfrak{L}}_i)^{e_i} \right)^{f' \mathbf{e}_{\Psi^*,N}} \in K_N^\times,$$

where $f' = f_0/p$ (cf. [22, Proposition 3.1] and [9, pp.44-45]).

Let $\mathfrak{L}$ (resp. $\mathfrak{L}^*$) be a prime ideal of K_N (resp. K_{N^*}) of degree 1 lying above a prime number l (resp. l^*). Put $F_{\mathfrak{L}} = (\mathcal{O}_N/\mathfrak{L})^\times/((\mathcal{O}_N/\mathfrak{L})^\times)^{p^{a_n}}$, $F_{\mathfrak{L}^*} = (\mathcal{O}_{N^*}/\mathfrak{L}^*)^\times/((\mathcal{O}_{N^*}/\mathfrak{L}^*)^\times)^{p^{a^*_N}}$, $F_l = \prod_{\mathfrak{L}|l} F_{\mathfrak{L}}$ and $F_{l^*} = \prod_{\mathfrak{L}^*|l^*} F_{\mathfrak{L}^*}$, where $\mathcal{O}_N$ is the ring of integers of K_N. For $L = \{l_i | 1 \le i \le s_0\}$ and $L^* = \{l^*_j | 1 \le j \le s^*\}$, let $K_N(L)$ (resp. $K_{N^*}(L^*)$) be the group of all elements of $K_N^\times$ (resp. $K_{N^*}^\times$) which are prime to all $l_i \in L$ (resp. $l^*_j \in L^*$). We define the following maps:

$$D_{N,L} : K_N(L) \to \prod_{i=1}^{s_0} F_{l_i} \quad \left(x \mapsto \left((x \mod \mathfrak{L}) \mod \left((\mathcal{O}_N/\mathfrak{L})^\times \right)^{p^{a_n}} \right)_{\mathfrak{L},i} \right)$$

and

$$D^*_{N^*,L^*} : K_{N^*}(L^*) \to \prod_{j=1}^{s^*} F_{l^*_j}, \; \left(x \mapsto \left((x \mod \mathfrak{L}^*) \mod \left((\mathcal{O}_{N^*}/\mathfrak{L}^*)^\times \right)^{p^{a^*_N}} \right)_{\mathfrak{L}^*,j} \right).$$

We fix a prime ideal $\mathfrak{L}_i | l_i$ for each i and put $L' = \{\mathfrak{L}_i | 1 \le i \le s_0\}$. We define

$$C'_n = \langle c_n^{T^m Y_n(T)} | 0 \le m \le s'_n \rangle_{\mathbf{Z}[\Delta]}$$

and

$$G'_{N,L'} = \langle g_N(\mathcal{L}_i)^{T^m Y^*_N(T)} | 1 \le m \le s'_N, \; 1 \le i \le s_0 \rangle_{\mathbf{Z}[\Delta]},$$

where $s'_n = \min\{\tilde{\lambda}(\Psi), p^n\} - 1$ and $s_0 = \dim_{\mathcal{O}/\pi} A_0(\Psi^*)/\pi A_0(\Psi^*)$. Put $L'_0 = \{\mathfrak{L}_{i,0} | \mathfrak{L}_{i,0} = N_{K_N/K_0} \mathfrak{L}_i, \; \mathfrak{L}_i \in L'\}$.

Theorem 1. *Assume* (C1) *and* (C2). *Then*

$$|A_n(\Psi)| \leq \frac{|\Lambda/(g_\Psi(T),\omega_n)|}{|D_{N,L}(C'_n)|}.$$

If $|D^*_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})| = |\Lambda/(g_{\Psi^*}(T),\omega_0)|$ *for some* L'_0 *and* $L^*_{N^*(0)}$, *then the equality holds. If* $|A_m(\Psi)| = |A_{m+1}(\Psi)|$ *for some* m, *then* $\lambda_p(\Psi) = \mu_p(\Psi) = 0$ *and* $\nu_p(\Psi) = e_m(\Psi)$.

Proof. Let $K_{n,\mathfrak{P}_n}$ be the completion of K_n at $\mathfrak{P}_n|p$ and $\mathcal{U}_{\mathfrak{P}_n}$ the group of principal units of $K_{n,\mathfrak{P}_n}$. Put $\mathcal{U}_n = \prod_{\mathfrak{P}_n|p} \mathcal{U}_{\mathfrak{P}_n}$. Let d_n be the diagonal map:

$$d_n : K_n^\times \to \prod_{\mathfrak{P}_n|p} K^\times_{n,\mathfrak{P}_n} \quad (x \mapsto (x,x,...,x)).$$

We denote by E_n the group of units of K_n and by C_n the group of cyclotomic units of K_n in the sense of [6]. Put

$$\mathcal{E}_n = \overline{\mathcal{U}_n \cap d_n(E_n)} \text{ and } \mathcal{C}_n = \overline{\mathcal{U}_n \cap d_n(C_n)},$$

where $\overline{A}$ is the topological closure in $\mathcal{U}_n$. By (C2) and [6, Theorem 2], we have the following Λ-isomorphisms:

$$\begin{array}{ccc} \mathcal{U}_n(\Psi) & \simeq & \Lambda/(\omega_n) \\ \bigcup| & & \bigcup| \\ \mathcal{E}_n(\Psi) & \simeq & V_n \\ \bigcup| & & \bigcup| \\ \mathcal{C}_n(\Psi) & \simeq & (g_\Psi(T),\omega_n)/(\omega_n). \end{array}$$

By the Iwasawa main conjecture proved in [8, 21, 25], we have

$$\begin{aligned} p^{e_n(\Psi)} &= |A_n(\Psi)| = |\mathcal{E}_n(\Psi)/\mathcal{C}_n(\Psi)| = |\mathcal{U}_n(\Psi)/\mathcal{C}_n(\Psi)|/|\mathcal{U}_n(\Psi)/\mathcal{E}_n(\Psi)| \\ &= |\Lambda/(g_\Psi(T),\omega_n)|/|\mathcal{U}_n(\Psi)^{p^{a_n}}/\mathcal{E}_n(\Psi)^{p^{a_n}}| \\ &= |\Lambda/(g_\Psi(T),\omega_n)|/|\mathcal{C}'_n(\Psi)/\mathcal{E}_n(\Psi)^{p^{a_n}}|, \end{aligned}$$

where $\mathcal{C}'_n = \overline{\mathcal{U}_n \cap (d_n(C'_n)\mathcal{C}_n^{p^{a_n}})}$. We will show that the surjective map:

$$\mathcal{C}'_n(\Psi)/\mathcal{E}_n(\Psi)^{p^{a_n}} \to D_{N,L}(C'_n)$$

is an isomorphism if $|D^*_{N^*,L^*}(G'_{N,L'})| = |\Lambda/(g_{\Psi^*}(T),\omega_N)|$. Denote by τ the canonical isomorphism:

$$\tau : (\mathbf{Z}/f_N l\mathbf{Z})^\times \to \mathrm{Gal}(\mathbf{Q}(\zeta_{f_N l})/\mathbf{Q}) \quad \left(m \mod f_N l \mapsto \tau_m \; (\zeta_{f_N l}^{\tau_m} = \zeta_{f_N l}^m)\right).$$

Put

$$\theta_N = \sum_{1 \le m < f_N,\, (m,f_N)=1} \left(1 - \frac{m}{f_N}\right) \tau_{m|K_N} \in \mathbf{Q}[\mathrm{Gal}(K_N/\mathbf{Q})].$$

By Stickelberger's theorem ([22, Proposition 3.1]), for any sufficiently large m, there exists $g' \in K_N^\times$ such that

$$(g_N(\mathfrak{L}_i)) = \mathfrak{L}_i^{f' \mathbf{e}_{\Psi^*,m} \theta_N} (g'^{p^{a_N^*}}).$$

We here have

$$\begin{aligned}
&\mathbf{e}_{\Psi^*,m} \theta_N Y_N^*(T) \\
&\quad = \ (e_{\Psi^*} + p^m Z)\theta_N Y_N^*(T) \\
&\quad \equiv \ g_{\Psi^*}(T) u(T)(X_N^*(T) + p^{a_N^*} W(T)) e_{\Psi^*} + p^m Z \theta_N Y_N^*(T) \mod \omega_N \\
&\quad \equiv \ p^{a_N^*}(1 + W(T) g_{\Psi^*}(T)) u(T) e_{\Psi^*} + p^m Z \theta_N Y_N^*(T) \mod \omega_N
\end{aligned}$$

for some $Z \in \mathbf{Z}_p[\Delta]$, $W(T) \in \mathcal{O}[T]$ and $u(T) \in \mathcal{O}[[T]]^\times$. Let L_N be the maximal unramified abelian p-extension of K_N. Let $L_N(\Psi^*)$ be the subfield of L_N corresponding to $\prod_{\Phi \ne \Psi^*} \mathrm{Gal}(L_N/K_N)(\Phi)$, where Φ runs over every $\mathbf{Q}_p$-valued character of Δ which is irreducible over $\mathbf{Q}_p$. We denote by $\left(\frac{L_N/K_N}{\mathfrak{L}_i}\right)$ the Artin symbol. Put

$$\sigma_{\mathfrak{L}_i} = \left(\frac{L_N(\Psi^*)/K_N}{\mathfrak{L}_i}\right) = \left(\frac{L_N(\Psi^*)/K_N}{\mathfrak{L}_i}\right)^{e_{\Psi^*}} = \left(\frac{L_N/K_N}{\mathfrak{L}_i}\right)^{e_{\Psi^*}}_{|L_N(\Psi^*)}.$$

Then, by Stickelberger's theorem, we have $\sigma_{\mathfrak{L}_i}^{g_{\Psi^*}(T)} = 1$. Let us consider the following map:

$$A_N(\Psi^*) \to K_N^\times/(K_N^\times)^{p^{a_N^*}} \quad (Cl(\mathfrak{A}) \mapsto \alpha^{\mathbf{e}_{\Psi^*,N}} \mod (K_N^\times)^{p^{a_N^*}}),$$

where $\alpha \in K_N^\times$ such that $\mathfrak{A}^{p^{a_N^*}} = (\alpha)$. By the proposition below,

$$|D^*_{N^*(0), L^*_{N^*(0)}}(G'_{0,L'_0})| = |\Lambda/(g_{\Psi^*}(T), \omega_0)|$$

implies that

$$\langle Cl(\mathfrak{L}_i)^{q e_{\Psi^*} T^m} | 1 \le m \le s'_N,\ 1 \le i \le s_0 \rangle_{\mathbf{Z}[\Delta]} = A_N(\Psi^*)$$

for some integer q such that $p \nmid q$. By the class field theory, we have

$$\left\langle \sigma_{\mathfrak{L}_i}^{T^m} | 1 \le m \le s'_N,\ 1 \le i \le s_0 \right\rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_N(\Psi^*)/K_N).$$

For $c \in C'_n$, since $d_n(c) \in \mathcal{U}_n^{p^{a_n}}$, $K_N(\sqrt[p^{a_n}]{c}) \subseteq L_N(\Psi^*)$. Hence $K_N(\sqrt[p^{a_n}]{c}) = K_N$ (i.e. $c \in (K_N^{\times})^{p_n^a}$) if and only if $c \mod \mathfrak{L} \in ((\mathcal{O}_N/\mathfrak{L})^{\times})^{p^{a_n}}$ for all $\mathfrak{L}|l_i$ and $l_i \in L$. This implies that $D_{N,L}(C'_n) \simeq \mathcal{C}'_n(\Psi)/\mathcal{E}_n(\Psi)^{p^{a_n}}$. Therefore the above assertion follows.

By (C2), we have $A_n(\Psi) \simeq X_\infty(\Psi)/\omega_n X_\infty(\Psi)$ (cf.[10, p. 731]). If $|A_m(\Psi)| = |A_{m+1}(\Psi)|$, then $\omega_m X_\infty(\Psi) = \omega_{m+1} X_\infty(\Psi) \subseteq (p,T)\omega_m X_\infty(\Psi)$. By Nakayama's lemma, we have $\omega_m X_\infty(\Psi) = 0$. Therefore $A_n(\Psi) \simeq X_\infty(\Psi)$ for $n \geq m$ and the last assertion follows. □

Proposition 1. *In the above setting,* $|D^*_{N^*,L^*}(G'_{N,L'})| = |\Lambda/(g_{\Psi^*}(T), \omega_N)|$ *holds for some* L^* *if and only if* $|D^*_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})| = |\Lambda/(g_{\Psi^*}(T), \omega_0)|$ *holds for some* $L^*_{N^*(0)}$.

Proof. We here have

$$\sigma_{\mathfrak{L}_i}|_{L_0(\Psi^*)} = \left(\frac{L_0(\Psi^*)/K_0}{N_{K_N/K_0}\mathfrak{L}_i}\right) = \left(\frac{L_0(\Psi^*)/K_0}{\mathfrak{L}_{i,0}}\right) = \sigma_{\mathfrak{L}_{i,0}}.$$

By Nakayama's lemma,

$$\left\langle \sigma_{\mathfrak{L}_i}^{T^m} | 1 \leq m \leq s'_N,\ 1 \leq i \leq s_0 \right\rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_N(\Psi^*)/K_N)$$

if and only if

$$\left\langle \sigma_{\mathfrak{L}_{i,0}} | 1 \leq i \leq s_0 \right\rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_0(\Psi^*)/K_0).$$

By the Chebotarev density theorem, the assertion follows. □

2.2 Special case

We explain how to use the criterion in practice. Following [11], we consider the following case.

(D1) $\qquad$ The exponent of $\mathrm{Gal}(K/\mathbf{Q})$ divides $p-1$.

(D2) $\qquad$ $\psi(p) \neq 1$ and $\psi^*(p) \neq 1$.

(D3) $\qquad$ $g_\psi(T) = T - \alpha$ for some $\alpha \in p\mathbf{Z}_p$.

By (D1), the values of ψ are contained in $\mathbf{Z}_p$ and $\Psi = \psi$. Put $\alpha^* = \dfrac{f_0 - \alpha}{1+\alpha} \in p\mathbf{Z}_p$, $e = v_p(\alpha)$ and $e^* = v_p(\alpha^*)$, where v_p is the p-adic valuation such that $v_p(p) = 1$. Then we have $a_n = n + e$, $a_n^* = n + e^*$, $N = N(n) =$

$n+e-1$, $N^* = N^*(N) = N+e^*-1 = n+e+e^*-2$ and $0 \le e_n(\psi) \le n+e$. Further

$$X_n(T) = \frac{\omega_n(T)-\omega_n(\alpha)}{T-\alpha}u \text{ and } Y_n(T) \equiv X_n(T) \mod p^{n+e}$$

and

$$X_N^*(T) = \frac{\omega_N(T)-\omega_N(\alpha^*)}{T-\alpha^*}u^* \text{ and } Y_N^*(T) \equiv X_N^*(T) \mod p^{N+e^*},$$

where $u = \dfrac{p^{n+e}}{1-(1+\alpha)^{p^n}}$ and $u^* = \dfrac{p^{N+e^*}}{1-(1+\alpha^*)^{p^N}}$.

Let $\mathfrak{L}$ (resp. $\mathfrak{L}^*$) be a prime ideal of K_N (resp. K_{N^*}) of degree 1 lying above a prime number l (resp. l^*). Put

$$D_{N,\mathfrak{L}} : K_N(\mathfrak{L}) \to F_{\mathfrak{L}} \text{ and } D^*_{N^*,\mathfrak{L}^*} : K_{N^*}(\mathfrak{L}^*) \to F_{\mathfrak{L}^*}.$$

By (D3), we have $\sigma_{\mathfrak{L}}^{\gamma_0} = \sigma_{\mathfrak{L}}^{1+\alpha^*}$. Further we have $\sigma_{\mathfrak{L}}^{\delta} = \sigma_{\mathfrak{L}}^{\psi^*(\delta)}$ for $\delta \in \Delta$. Hence the orders of $D_{N,\mathfrak{L}}(C_n')$ and $D^*_{N^*,\mathfrak{L}^*}(G'_{N,\mathfrak{L}})$ depend only on l and l^*. So we can write

$$|D_{N,l}(C_n')| = |D_{N,\mathfrak{L}}(C_n')| \text{ and } |D^*_{N^*,l^*}(G'_{N,l})| = |D^*_{N^*,\mathfrak{L}^*}(G'_{N,\mathfrak{L}})|.$$

In this case, we can write Theorem 1 as follows.

Theorem 2. *Assume* (D1)-(D3)*. For any prime number l which splits completely in $K_N/\mathbf{Q}$,*

$$|A_n(\psi)| \le \frac{p^{n+e}}{|D_{N,l}(C_n')|}.$$

If $|D^*_{e^*-1,l^*_{e^*-1}}(G'_{0,l})| = p^{e^*}$ for some $l^*_{e^*-1}$ which splits completely in $K_{e^*-1}/\mathbf{Q}$, then the equality holds. If $|A_m(\psi)| = p^{m+e-1}$ for some m, then $\lambda_p(\psi) = \mu_p(\psi) = 0$ and $\nu_p(\psi) = m+e-1$.

3 Computation of Gauss sums modulo prime ideals

Let l (resp. l^*) be a prime number such that $l \equiv 1 \mod f_N$ (resp. $l^* \equiv 1 \mod f_N l$), and g (resp. g^*) a primitive root in $\mathbf{Z}/l\mathbf{Z}$ (resp. $\mathbf{Z}/l^*\mathbf{Z}$). Let s (resp. t) be an integer satisfying $s \equiv g^{*(l^*-1)/f_N} \mod l^*$ (resp. $t \equiv g^{*(l^*-1)/l} \mod l^*$). Then, for some ideal $\mathfrak{L}|l$ of K_N and $\mathfrak{L}^*|l^*$ of $K_N(\zeta_l)$, $s \equiv \chi_{\mathfrak{L}}(g) \mod \mathfrak{L}^*$ and $t \equiv \zeta_l \mod \mathfrak{L}^*$.

We write

$$Y_N^*(T) = \sum_{j=0}^{p^N-1} a_j(1+T)^j = \sum_{j=0}^{p^N-1} a_j\gamma_0^j, \quad a_j \in \mathbf{Z}.$$

Then, by the definition of $Y_N^*(T)$, we have $a_j \equiv u^*(1+\alpha^*)^{p^N-1-j} \mod p^{N+e^*}$.

We here identify $\mathrm{Gal}(K_N/K_0)$ (resp. $\mathrm{Gal}(K_N/\mathbf{Q}_N)$) with $\mathrm{Gal}(K_N(\zeta_l)/K_0(\zeta_l))$ (resp. $\mathrm{Gal}(K_N(\zeta_l)/\mathbf{Q}_N(\zeta_l))$). Let $\mathfrak{A}_N$ be the subgroup of $(\mathbf{Z}/f_N l\mathbf{Z})^\times$ which is corresponding to $\mathrm{Gal}(\mathbf{Q}(\zeta_{f_N l})/\mathbf{Q}_N(\zeta_l))$ by the isomorphism τ. Taking an extension to $\mathrm{Gal}(\mathbf{Q}(\zeta_{f_N l})/\mathbf{Q}_N(\zeta_l))$, we write

$$\left(\sum_{\tau\in\mathrm{Gal}(\mathbf{Q}(\zeta_{f_N})/K_N)} \tau\right)\mathbf{e}_{\Psi^*,N} = \sum_{m\in\mathfrak{A}_N} b_m\tau_m, \quad b_m \in \mathbf{Z}.$$

Then we have

$$\begin{aligned} g_N(\mathfrak{L})^{Y_N^*(T)} = & \left(\prod_{j=0}^{p^N-1}\left(\prod_{m\in\mathfrak{A}_N}\left(-\sum_{y\in(\mathcal{O}_N/\mathfrak{L})^\times}\chi_{\mathfrak{L}}(y)\zeta_l^y\right)^{b_m\tau_m}\right)^{a_j\gamma_0^j}\right)^{f'} \\ \equiv & \left(\prod_{0\le j<p^N,\, m\in\mathfrak{A}_N}\left(-\sum_{i=0}^{l-2} s^{m(1+f_0)^j i} t^{g^i}\right)^{b_m a_j}\right)^{f'} \mod \mathfrak{L}^*. \end{aligned}$$

In order to compute the above sums, it suffices to compute the following discrete Fourier transforms:

$$F(w) = \sum_{0\le v<z} \zeta_z^{wv} f(v) = \zeta_{2z}^{w^2}\sum_{0\le v<z}\zeta_{2z}^{-(v-w)^2}(\zeta_{2z}^{v^2}f(v))$$

for $0 \le w < z$, where $z = f_N$ and $f(v) = \sum_{0\le i<l-1,\, i\equiv v \bmod f_N} t^{g^i}$. For $l^* \equiv 1 \mod 2f_N l$, by the famous algorithm of cyclic convolution, we can effectively compute Gauss sums modulo prime ideals (cf. [16, 6.4]).

There are another computations to find a p-th root of a cyclotomic unit in [5] and [17]. These computations become much more difficult as the extension degree of the field containing the cyclotomic unit is higher. It is necessary to do the computations with extremely accurate approximations of cyclotomic units.

4 Numerical examples

4.1 $\mathbf{Q}(\sqrt{f})$

Let p be an odd prime number and k the real quadratic field whose discriminant is f. Let φ_f be the non-trivial Dirichlet character associated to $k = \mathbf{Q}(\sqrt{f})$. Put $K = \mathbf{Q}(\sqrt{f}, \zeta_p)$. Then we have $A_n(k) = A_n(k)(\varphi_f) \simeq A_n(K)(\varphi_f)$ by [13]. The following examples satisfy (D1)-(D3) for $p = 3$.

$\mathbf{f = 29}$.
By computation, we have

$$\begin{cases} \alpha \equiv 18 \mod p^3, & e = 2, \\ \alpha^* \equiv 15 \mod p^3, & e^* = 1. \end{cases}$$

Since $|D_{1,l}(C'_0)| = p^2$ for $l = 523$, we have $|A_0(\varphi_f)| \leq p^{2-2} = 1$ by Theorem 2. Therefore we obtain

$$e_0 = e_1 = e_2 = ... \leq (=)0 \text{ and } \lambda_p(k) = \mu_p(k) = \nu_p(k) = 0.$$

In this case, we don't need to calculate a Gauss sum.

$\mathbf{f = 761}$.
By computation, we have

$$\begin{cases} \alpha \equiv 3 \mod p^2, & e = 1, \\ \alpha^* \equiv 3 \mod p^2, & e^* = 1. \end{cases}$$

Though $|D_{0,l}(C'_0)| = 1$ for some primes l, $|D_{1,l}(C'_1)| = p$ for $l = 237397$. Hence we have $|A_n(\varphi_f)| \leq p^{2-1} = p$ for $n \geq 1$ by Theorem 2.

Since $|D^*_{0,l^*_0}(G_{0,l})| = p$ and $|D_{0,l}(C'_0)| = 1$ for $l = 4567$ and $l^*_0 = 62558767$, we have $|A_0(\varphi_f)| = p$ by Theorem 2. Therefore we obtain

$$e_0 = e_1 = e_2 = ... = 1,\ \lambda_p(k) = \mu_p(k) = 0 \text{ and } \nu_p(k) = 1.$$

$\mathbf{f = 473}$.
By computation, we have

$$\begin{cases} \alpha \equiv 30 \mod p^5, & e = 1, \\ \alpha^* \equiv 84 \mod p^5, & e^* = 1. \end{cases}$$

Though $|D_{n,l}(C'_n)| = 1$ for $n \leq 4$ and some primes l, $|D_{5,l}(C'_5)| = p$ for $l = 2068903$. Hence we have $|A_n(\varphi_f)| \leq p^{6-1} = p^5$ for $n \geq 5$ by Theorem 2.

Since $|D^*_{0,l^*_0}(G_{0,l})| = p$ and $|D_{4,l}(C'_4)| = 1$ for $l = 1609147$ and $l^*_0 = 22833795931$, we have $|A_4(\varphi_f)| = p^5$ by Theorem 2. Therefore we obtain

$$e_n = n+1 \quad \text{for } n \leq 4, \quad e_n = 5 \quad \text{for } n \geq 5,\ \lambda_p(k) = \mu_p(k) = 0 \text{ and } \nu_p(k) = 5.$$

By the above procedure, we can settle the value in [11].

4.2 $\mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$

Vandiver's conjecture claims that $\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0$ for all $k = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$. By computer calculation, this conjecture is verified for $p < 12000000$ ([3]). We here replace $\mathbf{Q}$ with $\mathbf{Q}(\sqrt{f})$ and consider Iwasawa invariants associated to $k = \mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$ and $K = \mathbf{Q}(\sqrt{f}, \zeta_p)$, where f is the discriminant of a real quadratic field.

In the range $1 < f < 200$, $5 \leq p < 10000$ and $2 \leq 2i \leq p-3$, there are 171981262 pairs of $(\varphi_f\omega^{2i}, p)$ which satisfy (D1) and (D2). Among them, there are 37140 pairs with $\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 1$, 46 pairs with $\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 2$, and two pairs with $\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 3$. We verified Greenberg's conjecture $\lambda_p(\varphi_f\omega^{2i}) = \mu_p(\varphi_f\omega^{2i}) = 0$ for each of them by the method in [10]. Except for $(\varphi_{177}\omega^6, 17)$, we verified it by using cyclotomic units of k_0 or k_1. For $(\varphi_{177}\omega^6, 17)$, we used cyclotomic units of k_2 to verify it. In the range above, there are 38 pairs which don't satisfy (D2). We also verified the conjecture for each of them.

Proposition 2. $\lambda_p(\varphi_f\omega^{2i}) = \mu_p(\varphi_f\omega^{2i}) = 0$ *for all* $1 < f < 200$, $5 \leq p < 10000$ *and* $2 \leq 2i \leq p-3$.

In the following tables, we give lists of $(f, p, 2i)$ such that $\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 1$ and $\nu_p(\varphi_f\omega^{2i}) > 0$ ($v_p(\alpha) = e > 1$ or $v_p(\alpha^*) = e^* > 1$) or $\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 2, 3$. For $p = 7$, $k = \mathbf{Q}(\sqrt{m}, \zeta_p + \zeta_p^{-1})$ and $1 < m < 1000$, a list of non-trivial cases ($\nu_p > 0$) was given in [20]. Our extended computation coincides with it.

$\underline{\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 1}$

$\underline{\nu_p(\varphi_f\omega^{2i}) = 1}$

f	p	$2i$	f	p	$2i$	f	p	$2i$
12	701	542	21	199	150	33	53	30
37	43	32	53	1033	564	69	19	14
85	3697	3086	88	71	26	101	5333	2770
113	43	32	113	3373	1602	124	197	126
124	239	48	129	67	28	140	4751	120
141	5431	4826	149	43	32	149	71	16
149	229	182	157	401	56	161	101	22
168	37	22	172	73	10	173	43	32
173	101	42	181	71	52	181	6991	1628
185	827	354	188	1621	168	197	521	372

$\nu_p(\varphi_f \omega^{2i}) = 2$

f	p	$2i$
177	17	6

$v_p(\alpha) = e > 1$

f	p	$2i$	f	p	$2i$	f	p	$2i$
8	59	36	17	61	32	21	149	128
28	977	828	33	59	42	37	1091	812
41	7	4	41	283	102	44	787	148
53	7	2	53	1879	1158	57	2161	758
61	17	4	61	1747	1270	76	191	84
89	41	10	92	181	124	97	17	4
105	769	524	105	1453	162	120	2749	2196
124	41	30	140	107	74	149	797	140
149	2767	2178	152	17	12	168	43	10
173	13	4	177	31	24	184	373	72
193	7873	1886						

$v_p(\alpha^*) = e^* > 1$

f	p	$2i$	f	p	$2i$	f	p	$2i$
8	2221	1600	13	109	6	17	1319	88
28	223	126	33	31	24	33	1777	1184
41	19	12	41	421	126	60	19	14
61	7481	3516	73	11	2	73	1487	808
76	1451	418	76	4283	3484	97	367	26
109	41	32	133	1061	446	136	449	284
152	41	2	152	4027	3108	156	4637	2280
157	8221	582	165	29	26	165	89	66
165	1229	48	172	11	4	172	1487	900
177	337	74	184	1171	464	185	167	68
188	89	76						

$\underline{\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 2}$

f	p	$2i$	f	p	$2i$	f	p	$2i$
8	1151	842	21	11	4	24	29	4
24	181	84	29	569	64	37	5	2
37	89	66	37	3251	1094	40	257	232
44	653	448	53	193	14	56	1663	616
60	1277	582	60	1481	986	92	5	2
97	271	94	104	19	14	104	7919	4386
105	373	340	109	131	100	109	293	132
109	373	128	124	733	58	124	2111	1480
129	23	4	133	911	196	136	71	20
137	17	8	140	23	10	140	367	292
141	113	108	141	5939	2938	145	43	28
145	61	58	145	167	128	145	4157	3528
149	5	2	149	509	426	161	2389	646
165	11	2	172	13	10	172	47	38
173	7	4	177	157	48	181	223	26
185	17	6						

$\underline{\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 3}$

f	p	$2i$	f	p	$2i$
165	23	6	185	17	10

As in the argument of [24, pp.158–159], we can deduce that the number of exceptions to Vandiver's conjecture for $x_0 \leq p \leq x_1$ should be approximately $\frac{1}{2}(\log\log x_1 - \log\log x_0)$.

We here use a similar naive approach. For $G_{\varphi_f \omega^{2i}}(T) = \sum_{j=0}^{\infty} a_j T^j$ and an integer c, we assume that the probability of $a_j \equiv c \mod p^k$ is $1/p^k$. Further, for a cyclotomic unit c_0 with $d_0(c_0) \in \mathcal{U}_0^{p^e}$, we assume that the probability of $c_0 \in E_0^{p^k}$ is $1/p^k$ if $k \leq e$. Then, for a fixed conductor f and $x_0 \leq p \leq x_1$, we can deduce that the number of pairs $(\varphi_f \omega^{2i}, p)$ such that $\tilde{\lambda}_p = 1$ and $\nu_p > 0$ ($e > 1$ or $e^* > 1$) should be

$$\sum_{x_0 \leq p \leq x_1} \frac{p-3}{2} \left(\frac{1}{p^2} - \frac{1}{p^3} \right).$$

Let us apply this to our examples with $x_0 = 37$ and $x_1 = 10000$. Since the number of f's is 60, there should be about $60 \times 0.44645\cdots$ 'exceptions'. Our lists seem to support the deduction.

For $f = 1$ (i.e. $\psi = \psi^0$), the numerators of Bernoulli numbers B_{2i} are relatively small. We had better take this fact into consideration. By calculating their numerators, we easily see that there is no example such that $A_0(\omega^{2i}) \neq \{0\}$ for $i = 1, 2, 3, 4, 5$ and 7. Further there is no example such that $A_0(\omega^{2i}) \neq \{0\}$ for $i = \frac{p-3}{2}$ (see [19, 23]). Therefore, excluding these i's, we can deduce that 'the number of exceptions' to Vandiver's conjecture for $37 \leq p \leq q$ (q') may be smaller than E in the following table.

E	q	q'
0.1	113	149
0.2	419	450
0.3	1667	1737
0.4	8963	9058
0.5	67807	68096
0.6	799417	800172
0.7	16224227	16224227
0.8	640612703	640492743
0.9		10ˆ10.75
1.0		10ˆ13.13
1.5		10ˆ35.71
2.0		10ˆ97.07

Put $E_1(x) = \sum_{37 \leq p \leq x} \frac{p-17}{2}\frac{1}{p^2}$ and $E_2(x) = \frac{1}{2}\log\log x - 0.70476207\cdots$. Then q (resp. q') is the first prime (resp. integer) with $E_1(p) > E$ (resp. $E_2(n) > E$).

References

[1] J. Ax. On the units of an algebraic number field. *Illinois J. Math.*, 9:584–589, 1965.

[2] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[3] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and A. M. Shokrollahi. Irregular primes and cyclotomic invariants to 12 million. *J. Symbolic Comput.*, 31:89–96, 2001.

[4] B. Ferrero and L. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math.*, 109:377–395, 1979.

[5] T. Fukuda and K. Komatsu. A capitulation problem and Greenberg's conjecture on real quadratic fields. *Math. Comp.*, 65:313–318, 1996.

[6] R. Gillard. Remarques sur les unités cyclotomiques et les unités elliptiques. *J. Number Theory*, 11:21–48, 1979.

[7] R. Greenberg. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, 98:263–284, 1976.

[8] C. Greither. Class groups of abelian fields, and the main conjecture. *Ann. Inst. Fourier* (*Grenoble*), 42:449–499, 1992.

[9] H. Ichimura. Local units modulo Gauss sums. *J. Number Theory*, 68:36–56, 1998.

[10] H. Ichimura and H. Sumida. On the Iwasawa invariants of certain real abelian fields II. *Internat. J. Math.*, 7:721–744, 1996.

[11] H. Ichimura and H. Sumida. On the Iwasawa invariants of certain real abelian fields. *Tôhoku Math. J.*, 49:203–215, 1997.

[12] H. Ichimura and H. Sumida. A note on integral bases of unramified cyclic extensions of prime degree. II. *Manuscripta Math.*, 98:477–490, 1999.

[13] K. Iwasawa. A note on class numbers of algebraic number fields. *Abh. Math. Sem. Univ. Hamburg*, 20:257–258, 1956.

[14] K. Iwasawa. *Lectures on p-adic L-functions*, volume 74 of *Ann. of Math. Stud.* Princeton Univ. Press: Princeton, N.J., 1972.

[15] K. Iwasawa. On $\mathbf{Z}_l$-extensions of algebraic number fields. *Ann. of Math.*, 98:246–326, 1973.

[16] E. Knuth. *The art of computer programming, vol. 2: Seminumerical algorithms. 2nd edition.* Reading, Mass, 1981.

[17] J. S. Kraft and R. Schoof. Computing Iwasawa modules of real quadratic number fields. *Compositio Math.*, 97:135–155, 1995.

[18] T. Kubota and H.W. Leopoldt. Eine p-adische Theorie der Zetawerte, I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. reine angew. Math.*, 214/215:328–339, 1964.

[19] M. Kurihara. Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$. *Compositio Math.*, 81:223–236, 1992.

[20] M. Kurihara. The Iwasawa λ invariants of real abelian fields and the cyclotomic elements. *Tokyo J. Math.*, 22:259–277, 1999.

[21] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76:179–330, 1984.

[22] W. Sinnott. On the Stickelberger ideal and the circular units of an abelian field. *Invent. Math.*, 62:181–234, 1980.

[23] C. Soulé. Perfect forms and the Vandiver conjecture. *J. Reine Angew. Math.*, 517:209–221, 1999.

[24] L. Washington. *Introduction to Cyclotomic Fields. Second edition*, volume 83 of *Graduate Texts in Math.* Springer-Verlag: New York, 1997.

[25] A. Wiles. The Iwasawa conjecture for totally real fields. *Ann. of Math.*, 131:493–540, 1990.

Hiroki SUMIDA
Faculty of Integrated Arts and Sciences
Hiroshima University
Kagamiyama
Higashi-Hiroshima 739-8521, Japan
hiroki@mis.hiroshima-u.ac.jp