On the Stark–Shintani units and the ideal class groups in the cyclotomic $\mathbb{Z}_p$-extensions of class fields over real quadratic fields

by

TSUYOSHI ITOH (Tokyo)

1. Introduction. First, we briefly explain the Stark–Shintani conjecture. Let $F$ be a real quadratic field and $H(\mathfrak{f})$ (resp. $K(\mathfrak{f})$) the narrow ray class group (resp. the narrow ray class field) of $F$ modulo $\mathfrak{f}$, where $\mathfrak{f}$ is an integral ideal of $F$. Let $M$ be an abelian extension of $F$ such that exactly one infinite prime of $F$ (corresponding to the prescribed embedding into the real number field $\mathbb{R}$) splits in $M$. Let $\mathfrak{f}$ be the conductor of $M$ over $F$ and $\nu$ a totally positive integer of $F$ with the property that $\nu + 1 \in \mathfrak{f}$ and denote by the same letter $\nu$ the narrow ray class modulo $\mathfrak{f}$ represented by $(\nu)$. We know that $M$ is a quadratic extension of the maximal totally real subfield $M^+$ of $M$ and that the Galois group $\text{Gal}(M/M^+)$ is generated by $\sigma(\nu)$, where $\sigma : H(\mathfrak{f}) \to \text{Gal}(K(\mathfrak{f})/F)$ denotes the Artin map.

We define the Stark–Shintani ray class invariants by

$$X_{\mathfrak{f}}(c) = \exp(\zeta'_F(s, c) - \zeta'_F(0, c\nu))$$

for $c \in H(\mathfrak{f})$, where

$$\zeta_F(s, c) = \sum_{a \in c} \frac{1}{N(a)^s},$$

and $\zeta'_F(s, c)$ denotes its derivative. For the subgroup $G$ of $H(\mathfrak{f})$ corresponding to the extension $M/F$ we put

$$X_{\mathfrak{f}}(c, G) = \prod_{g \in G} X_{\mathfrak{f}}(cg)$$

for $c \in H(\mathfrak{f})$.

In this situation, the Stark–Shintani conjecture is formulated as follows:

2000 Mathematics Subject Classification: 11R23, 11R27.

Key words and phrases: Stark–Shintani units, $\mathbb{Z}_p$-extension.
Conjecture. There exists a positive integer $m$ such that:

(i) $X_t(c, G)^m$ is a unit of $M$ for each $c \in H(f)$,

(ii) $\{X_t(c, G)^m\}_{\sigma(c')} = X_t(cc', G)^m$ for any $c, c' \in H(f)$.

Shintani proved that the conjecture is true when $M^+$ is an abelian extension over $\mathbb{Q}$ (cf. [7, Theorem 2]).

Let $p$ be an odd prime, $M_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $M$, and $M_n$ the $n$-th layer of $M_\infty/M$, that is, $M_n$ is the unique cyclic extension field over $M$ of degree $p^n$ which is contained in $M_\infty$. Arakawa pointed out that if $M^+$ is an abelian extension over $\mathbb{Q}$, the conjecture is true for all $M_n$, and he also gave the class number formula in terms of these units (cf. [1]).

In this paper, we assume that $M$ and $p$ satisfy the following two conditions (P) and (D):

(P) The Stark–Shintani conjecture holds for all $M_n$. Namely, for each $n$ there exists an integer $t(n)$ such that $X_{f_n}(c, G_n)^{t(n)}$ is a unit in $M_n$ which satisfies $\{X_{f_n}(c, G_n)^{t(n)}\}_{\sigma(c')} = X_{f_n}(cc', G_n)^{t(n)}$ for all $c, c' \in H(f_n)$, where $f_n$ is the conductor of $M_n$ and $G_n$ is the subgroup of $H(f_n)$ which corresponds to $M_n$. Moreover, $t(n)$ is prime to $p$ for each $n$.

(D) The prime $p$ does not divide $[M : F]$ and for any subfield $M'$ of $M$ over $F$ with $M' \nsubseteq M^+$, any prime divisor $p$ of $f$ is a divisor of the conductor of $M'/F$ or a divisor of $p$. Moreover, if $p$ is a prime divisor of $p$ which does not divide the conductor of $M'$, then the decomposition field of $p$ in $M'/F$ is $(M')^+$.

Remark. If $M$ is a quadratic extension of $F$ and no prime above $p$ splits in $M/F$, then conditions (P) and (D) are satisfied (cf. [4, Theorem 1]).

Under conditions (P) and (D), we let $E_n$ be the full unit group of $M_n$ and $C_n$ the subgroup of $E_n$ generated by $X_{f_n}(c, G_n)$ with $c \in H(f_n)/G_n$. We also put

$$E_n^- = \{u \in E_n \mid N_{M_n/M_n^+}(u) = 1\}.$$  

Because $X_{f_n}(c, G_n)^{\sigma(\nu_n)} = X_{f_n}(c, G_n)^{-1}$ where $\nu_n$ is an element of $H(f_n)/G_n$ which corresponds to the generator of $\text{Gal}(M_n/M_n^+)$ by class field theory, we see that $C_n \subseteq E_n^-$. Then by Arakawa’s class number formula which we recall later, we can see that $C_n$ has a finite index in $E_n^-$.  

Our main theorem in this paper is the following:

Main Theorem. Let $F$ be a real quadratic field and $M$ an abelian extension over $F$ in which exactly one infinite prime of $F$ corresponding to the prescribed embedding of $F$ into $\mathbb{R}$ splits. Suppose that $M$ and $p$ satisfy conditions (P) and (D). Let $A_n$ be a Sylow $p$-subgroup of the ideal class group of $M_n$ and $A_n^- = \{c \in A_n \mid c^{\sigma(\nu_n)} = c^{-1}\}$, where $M_n^+$ is the maximal totally real subfield of $M_n$, and let $B_n$ be a Sylow $p$-subgroup of $E_n^-/C_n$.  

Moreover, we assume that $|A_n^-|$ is bounded with respect to $n$ and that all primes of $F$ above $p$ do not split in $M/M^+$. Then for any sufficiently large $n$, there exists an isomorphism

$$A_n^- \cong B_n$$

as Galois modules.

**Remark.** This theorem is an analogue to Ozaki’s result for the cyclotomic $\mathbb{Z}_p$-extension and the cyclotomic units of real abelian fields (cf. [6]).

**Acknowledgements.** The author would like to thank Professor K. Komatsu for checking results and giving useful advice.

### 2. Properties of Stark–Shintani units

Nakagawa dealt in [4], [5] with the Stark–Shintani units in the cyclotomic $\mathbb{Z}_p$-extension of certain abelian extensions of real quadratic fields. He rewrote Arakawa’s class number formula in terms of $X_f(c, G)$ and showed that each Tate cohomology group $\tilde{H}^i(\Gamma_{m,n}, C_m) = 0$ always vanishes for $i = 0, 1$.

Assume that $M$ and $p$ satisfy conditions (P) and (D). Let $f_n, c_n, G_n$ and $\nu_n$ be as in the previous section.

For any character $\chi$ of $H(f_n)/G_n$ with $\chi(\nu_n) = -1$, we know that

$$L'_F(0, \chi) = \sum_{c \in H(f_n)/(G_n, \nu_n)} \chi(c) \log X_{f_n}(c, G_n),$$

where $L_F(s, \chi)$ is the Hecke $L$-function of $F$ associated to $\chi$. Let $f_\chi$ be the conductor of $\chi$ and $\tilde{\chi}$ the primitive character associated to $\chi$. Then we have the equality

$$L'_F(0, \chi) = L'_F(0, \tilde{\chi}) \prod_{p | f_n, p \nmid f_\chi} (1 - \tilde{\chi}(p)).$$

Under assumption (D), we know that $\tilde{\chi}(p) = -1$ for every $p$ such that $p | f_n$ and $p \nmid f_\chi$.

Using the same method as in [1] or [5], we have another version of Arakawa’s class number formula.

**Theorem 1** (cf. [5, Theorem 1]). Assume that $M$ and $p$ satisfy conditions (P) and (D). Let $h(M_n)$ (resp. $h(M_n^+)$) be the class number of $M_n$ (resp. $M_n^+$). Then

$$h(M_n)/h(M_n^+) = (\text{power of } 2) \cdot t(n)^{-[M_n^+: F]} \cdot [E_n^- : C_n].$$

Moreover, Nakagawa showed the following:

**Theorem 2** (cf. [5, Proposition 2]). For any integers $m \geq n > 0$,

(i) $\tilde{H}^i(\Gamma_{m,n}, C_m) = 0$ for all $i$,

(ii) the natural map $E_n^-/C_n \to E_m^-/C_m$ is injective.
3. Proof of the main theorem. We fix an odd prime \( p \). Let \( I_n \) (resp. \( P_n \)) be the ideal group (resp. the principal ideal group) of \( M_n \) and \( A_n \) a Sylow \( p \)-subgroup of the ideal class group of \( M_n \). We identify all \( \sigma(\nu_n) \) and write this as \( \tau \). For any \( \text{Gal}(M_n/M_n^+) \)-module \( N \), let the relative part of \( N \) be \( N^- = \{ c \in N \mid c^\tau = c^{-1} \} \). Let \( I_n^{(p)} \) be the subgroup of \( I_n \) such that \( I_n^{(p)}/P_n \cong A_n \). Since \( p \) is odd, we find that
\[
0 \to P_n^- \to (I_n^{(p)})^- \to A_n^- \to 0
\]
is an exact sequence.
Moreover, we put \( P_0^n = \{ (\alpha) \in P_n \mid \alpha \alpha^\tau = \varepsilon \varepsilon^\tau \text{ with some } \varepsilon \in E_n \} \), which is a subgroup of \( P_n^- \).

**Lemma 1.** For any non-negative integer \( n \),

(i) \( P_n^-/P'_n \) has exponent 2,

(ii) the following sequence is exact:
\[
0 \to E_n^- \to (M_n^\times)^- \to P'_n \to 0.
\]

**Proof.** For any \( (\alpha) \in P_n^- \), we see that \( \alpha \alpha^\tau = \varepsilon \) with some \( \varepsilon \in E_n^+ \), where \( E_n^+ \) is the unit group of \( M_n^+ \). Then (i) follows.

(ii) We only show the surjectivity of the mapping \( (M_n^\times)^- \to P'_n \), since the remainder is clear. For any \( (\alpha) \in P'_n \), we have \( \alpha \alpha^\tau = \varepsilon \varepsilon^\tau \) with some \( \varepsilon \in E_n \). Then the fact that \( \alpha = (\varepsilon^{-1} \alpha) \) and \( \varepsilon^{-1} \alpha \in M_n^- \) gives the surjectivity. \( \blacksquare \)

**Lemma 2.** For any \( m \geq n \geq 0 \),

(i) \( H^1(M_{m,n},(M_n^\times)^-) = 0 \),

(ii) \( H^1(M_{m,n},E_n^-) \cong (P'_n)^{M_{m,n}}/P'_n \).

**Proof.** (i) We denote by \( N_{m,n} \) the norm from \( M_m \) to \( M_n \) and fix a generator \( \gamma \) of \( \text{Gal}(M_m/M_n) \). For any element \( \alpha \) of \( (M_n^\times)^- \) which satisfies \( N_{m,n}(\alpha) = 1 \), there exists an element \( \beta \) of \( M_n^\times \) such that \( \alpha = \beta/\beta^\gamma \) by Hilbert’s Theorem 90. It is sufficient to show that \( \beta \) can be taken from \( (M_m^\times)^- \).

Because \( \alpha \in (M_m^\times)^- \), we see that \( x := \beta/\beta^\gamma \) is in \( N_{M_m/M_m^+}(M_m^\times) \cap (M_m^+)^\times \). Therefore \( x^2 \) is in \( N_{M_m/M_m^+}(M_m^\times) \). On the other hand, \( x^{p^{m-n}} = N_{M_n/M_n^+}(\beta)N_{m,n}(\beta)^\gamma \) is also in \( N_{M_m/M_m^+}(M_m^\times) \). Since \( p \) is prime to 2, we have \( x \in N_{M_n/M_n^+}(M_n^\times) \). Let \( x = y\gamma \) with some \( y \in M_n^\times \). Then
\[
\alpha = \beta/\beta^\gamma = \beta y^{-1}/(\beta y^{-1})^\gamma
\]
with \( \beta y^{-1} \in (M_m^\times)^- \). This completes the proof of (i).
(ii) Taking the cohomology groups of the exact sequence of Lemma 1(ii), we have the exact sequence
\[ 0 \to E_n^- \to (M_n^\times)^- \to (P'_m)^{\Gamma_{m,n}} \]
\[ \to H^1(\Gamma_{m,n}, E_m^-) \to H^1(\Gamma_{m,n}, (M_m^\times)^-) = 0. \]
From this (ii) follows. ■

Taking the $p$-part of the cohomology of the exact sequence
\[ 0 \to C_m \to E_m^- \to E_m^-/C_m \to 0, \]
by Lemma 2(ii) we obtain
\[ (1) \quad (P'_m)^{\Gamma_{m,n}}/P_n^- \cong \hat{H}^{-1}(\Gamma_{m,n}, E_m^-) \cong \hat{H}^{-1}(\Gamma_{m,n}, B_m). \]

**Proposition 1.** Assume that no prime of $M^+$ above $p$ splits in $M$. Then
\[ (P_m^-)^{\Gamma_{m,n}}/P_n^- \cong \ker(j_{m,n}) \]
for all $m > n \geq 0$. Here $j_{m,n} : A_n^- \to A_m^-$ is the lift map of the ideal class groups.

**Proof.** For any principal ideal $(\alpha)$ in $(P_m^-)^{\Gamma_{m,n}}$, we have $(\alpha) = 2I \in I_n^\times$ by assumption because all ramified primes in $M_m/M_n$ are above $p$. Then
\[ (P_m^-)^{\Gamma_{m,n}}/P_n^- \cong (I_n^- \cap P_m^-)/P_n^- \cong \ker(j_{m,n}). \]

We now finish the proof of our main theorem. Since $|A_n^-|$ is bounded with respect to $n$, $|B_n|$ is also bounded by Theorem 1. Therefore there exists a positive integer $n_0$ such that $A_m^- \cong A_n^-$ (by the norm map) and $B_n \cong B_m$ (by natural injection) for all $m > n \geq n_0$. Then for any $n \geq n_0$, taking a sufficiently large $m$, we have
\[ \hat{H}^{-1}(\Gamma_{m,n}, B_m) \cong B_m \cong B_n \quad \text{and} \quad \ker(j_{m,n}) = A_n^- . \]

Then by (1) and Proposition 1, it is sufficient to show that $(P'_m)^{\Gamma_{m,n}}/P_n^'$ is isomorphic to $(P_m^-)^{\Gamma_{m,n}}/P_n^-$. We note that both groups are $p$-groups with the same order. Therefore the isomorphism easily follows by Lemma 1(i). This completes the proof of the main theorem. ■

**Remark.** We can show the main theorem replacing $X_f(c, G)$ by another invariant $Y_f(c, G)$ introduced in [7], by using Arakawa’s original class number formula. In this case, assumption (D) is not necessary.

**4. Examples.** Since the field $M$ considered in the preceding sections is not totally real, the assumption that $|A_n^-|$ is bounded with respect to $n$ may seem strong. In fact, if $p$ splits completely in $M$, then $|A_n|$ is always unbounded and in the case of the CM-field, if $p$ divides the “minus part” of the ideal class group, then the “minus part” in the cyclotomic $\mathbb{Z}_p$-extension is unbounded (cf. [3]). Thus there is the problem to find “non-trivial” examples
which satisfy the assumptions of the main theorem. The author has found some such examples. Let $F = \mathbb{Q}(\sqrt{6})$, $M = F(\sqrt{6} + 20\sqrt{6})$ and $p = 3$. Then $p$ does not split in $M$. Since $M$ is a quadratic extension over $F$, assumptions (P) and (D) are satisfied. By using KASH, we see that the class number of $M$ is 6 and that of $M_1$ is 24. Then by Theorem 1 of [2], $|A_n| = |A_{n-1}|$ is bounded. By the same method, we find that the case of $F = \mathbb{Q}(\sqrt{2})$ and $M = F(\sqrt{5} + 13\sqrt{2})$ also satisfies the assumptions of the main theorem for $p = 3$.

References


Department of Mathematics
School of Science and Engineering
Waseda University
3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan
E-mail: tsitoh@mn.waseda.ac.jp

Received on 14.9.2000
and in revised form on 25.6.2001