Journal of Number Theory 151 (2015) 1–6

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the Stickelberger ideal of a quadratic twist of a cyclotomic field

Akira Endô

Department of Mathematics, Kumamoto University, Kumamoto 860-8555, Japan

ARTICLE INFO

Article history:
Received 4 July 2014
Received in revised form 4 November 2014
Accepted 5 November 2014
Available online 14 January 2015
Communicated by David Goss

MSC:
11R20
11R29

Keywords:
Cyclotomic field
Stickelberger ideal
Relative class number

ABSTRACT

A system of generators of the minus part of the Stickelberger ideal of a quadratic twist of a cyclotomic field is obtained.

Let p be an odd prime number and n a natural number. As usual Q and Z mean the field of rational numbers and the ring of rational integers, respectively. Skula [4] obtained a system of generators of the minus part of the Stickelberger ideal of the p^n-th cyclotomic field $F = Q(\zeta)$, where $\zeta = \zeta_{p^n}$ is a primitive p^n-th root of unity, and gave an alternative proof for the formula of Iwasawa [3] concerning the relative class number of F. In the previous paper [1] we considered the Stickelberger ideal of a quadratic extension L of F obtained by adjoining $\sqrt{m}$, where m is a square-free rational integer.

E-mail address: endou@sci.kumamoto-u.ac.jp.

http://dx.doi.org/10.1016/j.jnt.2014.11.003
0022-314X/

Now, L has an imaginary subfield K distinct from F with $[L : K] = 2$; we call K a quadratic twist of F. In this paper we get a system of generators of the minus part of the Stickelberger ideal of K. Obviously K is a quadratic extension of the maximal real subfield F^+ of F, and coincides with $F^+((\zeta - \zeta^{-1})\sqrt{m})$ or $F^+(\sqrt{m})$ according as $m > 0$ or $m < 0$.

We may assume without loss of generality that m is prime to p. Let g be a primitive root modulo p^n, and put $r = (1/2)(p-1)p^{n-1}$. The Galois group $Gal(L/Q)$ has two generators σ and τ such that

$$\zeta^\sigma = \zeta^g, \qquad \sqrt{m}^\sigma = \sqrt{m},$$
$$\zeta^\tau = \zeta, \qquad \sqrt{m}^\tau = -\sqrt{m}.$$

In what follows, we denote the restrictions of σ and τ to K again by σ and τ, respectively. Then the Galois group $G = Gal(K/Q)$ is generated by σ and τ, and we see that $\sigma^r = \tau$ if $m > 0$, and $\sigma^r = 1$ if $m < 0$. Let χ be a quadratic Dirichlet character associated with $Q(\sqrt{m})$, and d the conductor of χ. We note that $\chi(-1) = 1$ or -1 according as $m > 0$ or $m < 0$.

For a rational integer $k \geq 0$, let g_k be a rational integer which satisfies $1 \leq g_k \leq p^n - 1$ and $g_k \equiv g^k \pmod{p^n}$. The Stickelberger element θ of level dp^n in $Z[G]$ is defined as the restriction of that for the dp^n-th cyclotomic field to its subfield K:
when $m > 0$

$$\theta = \frac{1}{dp^n}\sum_{i=0}^{r-1}\Bigg(\Bigg(\sum_a{}^{(i)+}\left(ap^n + g_i\right) + \sum_a{}^{(i+r)-}\left(ap^n + g_{i+r}\right)\Bigg)\sigma^{-i} + \Bigg(\sum_a{}^{(i)-}\left(ap^n + g_i\right) + \sum_a{}^{(i+r)+}\left(ap^n + g_{i+r}\right)\Bigg)\sigma^{-i}\tau\Bigg),$$

and when $m < 0$

$$\theta = \frac{1}{dp^n}\sum_{i=0}^{r-1}\Bigg(\Bigg(\sum_a{}^{(i)+}\left(ap^n + g_i\right) + \sum_a{}^{(i+r)+}\left(ap^n + g_{i+r}\right)\Bigg)\sigma^{-i} + \Bigg(\sum_a{}^{(i)-}\left(ap^n + g_i\right) + \sum_a{}^{(i+r)-}\left(ap^n + g_{i+r}\right)\Bigg)\sigma^{-i}\tau\Bigg).$$

Herein $\sum_a^{(k)+}$ and $\sum_a^{(k)-}$ denote the summations taken over $0 \leq a \leq d-1$ such that $\chi(ap^n + g_k) = 1$ and $\chi(ap^n + g_k) = -1$, respectively. Let $S = Z[G]\theta \cap Z[G]$, which is called the Stickelberger ideal of $Z[G]$.

Note that τ acts on K as complex conjugation. For a $Z[G]$-module M, we denote by M^- the submodule of all elements α in M satisfying $\tau\alpha = -\alpha$.

Now, let $\sum_{j=0}^{r-1}(x_j\sigma^j+y_j\sigma^j\tau)$ be an element in $Z[G]$. We then consider the condition for

$$\xi=\left(\sum_{j=0}^{r-1}\bigl(x_j\sigma^j+y_j\sigma^j\tau\bigr)\right)\theta$$

to be in $Z[G]^-$. For $k\geq 0$, let $A_k^+=\sum_a^{(k)+}a$ and $A_k^-=\sum_a^{(k)-}a$. Since $g_k+g_{k+r}=p^n$ for $k\geq 0$, we see

$$\theta=\begin{cases}\frac{1}{d}\sum_{i=0}^{r-1}((A_i^++A_{i+r}^-+\frac{\varphi(d)}{2})\sigma^{-i}+(A_i^-+A_{i+r}^++\frac{\varphi(d)}{2})\sigma^{-i}\tau) & \text{if } m>0,\\ \frac{1}{d}\sum_{i=0}^{r-1}((A_i^++A_{i+r}^++\frac{\varphi(d)}{2})\sigma^{-i}+(A_i^-+A_{i+r}^-+\frac{\varphi(d)}{2})\sigma^{-i}\tau) & \text{if } m<0.\end{cases}$$

Herein $\varphi(d)$ is the Euler function. Since $\chi((d-1-a)p^n+g_{i+r})=\chi(-1)\chi(ap^n+g_i)$, we have that when $m>0$,

$$A_i^++A_{i+r}^+=A_i^-+A_{i+r}^-=\frac{\varphi(d)}{2}(d-1),$$

and when $m<0$,

$$A_i^++A_{i+r}^-=A_i^-+A_{i+r}^+=\frac{\varphi(d)}{2}(d-1).$$

Then we obtain that

$$\theta=\sum_{i=0}^{r-1}\left(\left(\frac{1}{d}\bigl(A_i^+-A_i^-\bigr)+\frac{\varphi(d)}{2}\right)\sigma^{-i}+\left(\frac{1}{d}\bigl(A_i^--A_i^+\bigr)+\frac{\varphi(d)}{2}\right)\sigma^{-i}\tau\right)$$

and

$$\begin{aligned}\xi=\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}\Bigg(&\left(\frac{1}{d}(x_j-y_j)\bigl(A_{i+j}^+-A_{i+j}^-\bigr)+\frac{\varphi(d)}{2}(x_j+y_j)\right)\sigma^{-i}\\&+\left(\frac{1}{d}(x_j-y_j)\bigl(A_{i+j}^--A_{i+j}^+\bigr)+\frac{\varphi(d)}{2}(x_j+y_j)\right)\sigma^{-i}\tau\Bigg).\end{aligned}\tag{$*$}$$

Lemma 1. *We have $\xi\in Z[G]$ unless $m=-1$ or -3. When $m=-1$, $\xi\in Z[G]$ if and only if $\sum_{j=0}^{r-1}x_j\equiv\sum_{j=0}^{r-1}y_j \pmod 2$, and when $m=-3$, $\xi\in Z[G]$ if and only if $\sum_{j=0}^{r-1}x_j\equiv\sum_{j=0}^{r-1}y_j \pmod 3$.*

Proof. From ($*$), for ξ to be in $Z[G]$, it suffices to show $d\xi\equiv 0 \pmod d$. We see from the definition of θ that

$$dp^n\theta\equiv\begin{cases}(B^++B^-)\sum_{i=0}^{r-1}(\sigma^{-i}+\sigma^{-i}\tau) \pmod d & \text{if } m>0,\\ 2\sum_{i=0}^{r-1}(B^+\sigma^{-i}+B^-\sigma^{-i}\tau) \pmod d & \text{if } m<0,\end{cases}$$

where B^+ and B^- are sums of $1 \le a \le d-1$ such that $\chi(a) = 1$ and $\chi(a) = -1$, respectively. We here note that $B^+ + B^- \equiv 0 \pmod{d}$. Hence we have that

$$dp^n\xi \equiv \begin{cases} 0 \pmod{d} & \text{if } m > 0, \\ 2\sum_{i=0}^{r-1}((B^+\sum_{j=0}^{r-1} x_j + B^-\sum_{j=0}^{r-1} y_j)\sigma^{-i} \\ \quad + (B^-\sum_{j=0}^{r-1} x_j + B^+\sum_{j=0}^{r-1} y_j)\sigma^{-i}\tau) \pmod{d} & \text{if } m < 0. \end{cases}$$

It is easy to see that if $m \le -5$, then $B^+ \equiv B^- \equiv 0 \pmod{d}$, if $m = -1$ or -3, then $B^+ \equiv 1 \pmod{d}$ and $B^- \equiv -1 \pmod{d}$, and if $m = -2$, then $B^+ \equiv B^- \equiv 4 \pmod{8}$. Thus we have the assertion. □

On the other hand, from (∗) we have that

$$\begin{aligned}\tau\xi = \sum_{i=0}^{r-1}\sum_{j=0}^{r-1}\Bigg(&\left(\frac{1}{d}(x_j - y_j)\big(A^-_{i+j} - A^+_{i+j}\big) + \frac{\varphi(d)}{2}(x_j + y_j)\right)\sigma^{-i} \\ &+ \left(\frac{1}{d}(x_j - y_j)\big(A^+_{i+j} - A^-_{i+j}\big) + \frac{\varphi(d)}{2}(x_j + y_j)\right)\sigma^{-i}\tau\Bigg)\end{aligned}$$

and so

$$\xi + \tau\xi = \varphi(d)\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}(x_j + y_j)\big(\sigma^{-i} + \sigma^{-i}\tau\big),$$

which implies the following:

Lemma 2. *We have $\tau\xi = -\xi$ if and only if $\sum_{j=0}^{r-1}(x_j + y_j) = 0$.*

We now put

$$\begin{aligned}\alpha_0 &= \omega_3(1 - \tau)\theta \\ &= \frac{2\omega_3}{d}\sum_{i=0}^{r-1}\big(A^+_i - A^-_i\big)\big(\sigma^{-i} - \sigma^{-i}\tau\big)\end{aligned}$$

with $\omega_3 = 3$ or 1 according as $m = -3$ or not, and for $1 \le j \le r-1$

$$\begin{aligned}\alpha_j &= \big(1 - \sigma^j\big)\theta \\ &= \frac{1}{d}\sum_{i=0}^{r-1}\big(\big(A^+_i - A^-_i\big) - \big(A^+_{i+j} - A^-_{i+j}\big)\big)\big(\sigma^{-i} - \sigma^{-i}\tau\big),\end{aligned}$$

all of which are in S^- by Lemmas 1 and 2.

We have the following:

Theorem. *We have $\{\alpha_0, \alpha_1, \dots, \alpha_{r-1}\}$ as a system of generators of S^-, and see that S^- is of finite index in $Z[G]^-$ if and only if $m > 0$ or $\chi(p) = -1$, in which case*

$$\big(Z[G]^- : S^-\big) = \begin{cases} h_K^- & \text{if } m \geq -1, \\ 2h_K^- & \text{if } m < -1, \end{cases}$$

where h_K^- denotes the relative class number of K.

Proof. Suppose that $x_0, \dots, x_{r-1}, y_0, \dots, y_{r-1} \in Z$ satisfy $\sum_{j=0}^{r-1}(x_j + y_j) = 0$ and moreover $\sum_{j=0}^{r-1} x_j \equiv \sum_{j=0}^{r-1} y_j \pmod{\omega_3}$. We then see from $(*)$ that

$$\begin{aligned}
&\left(\sum_{j=0}^{r-1}\big(x_j\sigma^j + y_j\sigma^j\tau\big)\right)\theta \\
&= \frac{1}{d}\sum_{i=0}^{r-1}\sum_{j=0}^{r-1}(x_j - y_j)\big(A_{i+j}^+ - A_{i+j}^-\big)\big(\sigma^{-i} - \sigma^{-i}\tau\big) \\
&= \frac{1}{d}(x_0 - y_0)\sum_{i=0}^{r-1}\big(A_i^+ - A_i^-\big)\big(\sigma^{-i} - \sigma^{-i}\tau\big) \\
&\quad + \sum_{j=1}^{r-1}(x_j - y_j)\left(\frac{1}{d}\sum_{i=0}^{r-1}\big(A_i^+ - A_i^-\big)\big(\sigma^{-i} - \sigma^{-i}\tau\big) - \alpha_j\right) \\
&= \left(\sum_{j=0}^{r-1}(x_j - y_j)\right)\frac{1}{d}\sum_{i=0}^{r-1}\big(A_i^+ - A_i^-\big)\big(\sigma^{-i} - \sigma^{-i}\tau\big) - \sum_{j=1}^{r-1}(x_j - y_j)\alpha_j \\
&= \frac{\sum_{j=0}^{r-1}(x_j - y_j)}{2\omega_3}\alpha_0 - \sum_{j=1}^{r-1}(x_j - y_j)\alpha_j,
\end{aligned}$$

which shows that $\alpha_0, \alpha_1, \dots, \alpha_{r-1}$ form a system of generators of S^-. We define a determinant $D_{p^n}(\chi)$ of degree r by

$$D_{p^n}(\chi) = \det\left(\frac{1}{d}\big(A_{i+j}^+ - A_{i+j}^-\big)\right)_{0 \leq i,j \leq r-1}.$$

It is easy to see that the absolute value of the determinant of the transformation of $\{\sigma^{-i} - \sigma^{-i}\tau,\ 0 \leq i \leq r-1\}$, a system of generators of $Z[G]^-$, to $\{\alpha_i,\ 0 \leq i \leq r-1\}$ equals $2\omega_3|D_{p^n}(\chi)|$, and hence that S^- is of finite index in $Z[G]^-$ if and only if $D_{p^n}(\chi) \neq 0$, in which case $(Z[G]^- : S^-) = 2\omega_3|D_{p^n}(\chi)|$. In [2] we calculated $|D_{p^n}(\chi)|$ as follows:

$$\big|D_{p^n}(\chi)\big| = \begin{cases} \prod_{i=0}^{r-1}\left|\frac{1}{2}B_{1,\psi^{2i+1}\chi}\right| & \text{if } m > 0, \\ (1 - \chi(p))\prod_{i=0}^{r-1}\left|\frac{1}{2}B_{1,\psi^{2i}\chi}\right| & \text{if } m < 0. \end{cases}$$

Herein ψ is a primitive Dirichlet character of degree $2r$ associated with F, and $B_{1,\psi^k\chi}$ is the generalized Bernoulli number belonging to $\psi^k\chi$. Thus we see that $D_{p^n}(\chi) \neq 0$ if and only if $m > 0$ or $\chi(p) = -1$. The analytic formula for h_K^- says

$$h_K^- = \begin{cases} 2Q_K \prod_{i=0}^{r-1} \frac{-1}{2} B_{1,\psi^{2i+1}\chi} & \text{if } m > 0, \\ Q_K w_K \prod_{i=0}^{r-1} \frac{-1}{2} B_{1,\psi^{2i}\chi} & \text{if } m < 0, \end{cases}$$

where Q_K is the unit index of K and w_K is the number of roots of unity in K (cf. [5]). When $m \neq -1$ it is easy to see $Q_K = 1$. When $m = -1$, we also see $Q_K = 1$; otherwise there would be a unit $(1 + \sqrt{-1})/a$ of K with $a \in F^+$, from which 2 would be ramified in F^+, a contradiction. From the argument above the assertion follows. □

References

[1] A. Endô, The relative class number of certain imaginary abelian fields, Abh. Math. Semin. Univ. Hambg. 58 (1988) 237–243.
[2] A. Endô, On the Stickelberger ideal of $(2, \dots, 2)$-extensions of a cyclotomic number field, Manuscripta Math. 69 (1990) 107–132.
[3] K. Iwasawa, A class number formula for a cyclotomic field, Ann. of Math. (2) 76 (1962) 171–179.
[4] L. Skula, Another proof of Iwasawa's class number formula, Acta Arith. 39 (1981) 1–6.
[5] L. Washington, Introduction to Cyclotomic Fields, 2nd ed., Grad. Texts in Math., vol. 83, Springer-Verlag, 1997.