ACTA ARITHMETICA
XCI.2 (1999)

The Stickelberger element of an imaginary quadratic field

by

Peter Schmid (Tübingen)

1. Introduction. Sinnott [5] has introduced Stickelberger ideals for all abelian number fields. These ideals (of the integral group algebra of the Galois group) annihilate the ideal class group of the field and, for non-real fields, their indices give interpretations of the minus part of the class number. In general, the so-called Sinnott module, occurring in the index formula, is not easy to deal with for arbitrary abelian fields. Recently Kučera [3] was able to compute this index for a compositum of quadratic number fields. Here we handle the very special case of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$, where $D = -d$ is its (negative) discriminant.

Recall that d is the conductor of K, hence $\mathbb{Q}(\zeta_d)$ is the smallest cyclotomic field containing K. For $a \in G(d) = (\mathbb{Z}/d\mathbb{Z})^*$ let $\sigma_a : \zeta_d \mapsto \zeta_d^a$ be the corresponding automorphism of $\mathbb{Q}(\zeta_d)$, and let $\{a/d\}$ be the fractional part of a. (So $\{a/d\}$ is the rational number x in the interval $[0, 1)$ such that $x - a'/d \in \mathbb{Z}$ for any integer a' representing a.) According to the definition given in Washington's book [6, p. 93] then

$$\theta = \theta_K = \sum_{a \in G(d)} \left\{ \frac{a}{d} \right\} (\sigma_a^{-1})|_K$$

is the *Stickelberger element* of K. Let $G = \langle j \rangle$ be the Galois group of $K|\mathbb{Q}$. Then $\theta \in \mathbb{Q}G$ is in the rational group algebra of G and, of course, $d\theta \in \mathbb{Z}G$. We even have the following (cf. Example (b) in [6, p. 94]):

Theorem 1. *The Stickelberger element $\theta = \theta_K$ is in the integral group ring $\mathbb{Z}G$ of the Galois group of K unless $d = 3, 4$ or 8.*

The proof is quite elementary. In what follows we exclude the cases $d = 3, 4, 8$ (where the class number $h = h_K = 1$). Then we define $\mathcal{S} = \mathcal{S}_K = \langle \theta, 1 + j \rangle$ to be the *Stickelberger ideal* to K. This (additive) join is an ideal of $\mathbb{Z}G$, and it turns out that it agrees with the notion introduced by Sinnott [5].

1991 *Mathematics Subject Classification*: 11R11, 11R29.

Note that the norm $1+j$ annihilates the ideal class group $C = \mathrm{Cl}_K$ and, therefore, j acts on C by inversion. Write $\theta = u + vj$ $(u, v \in \mathbb{Z})$. From the (analytic) class number formula we obtain $h = |C| = -(u - v)$. It is thus immediate that θ annihilates C as well.

COROLLARY. *The Stickelberger ideal $\mathcal{S} = \mathcal{S}_K$ annihilates the ideal class group C of K. In fact, $\mathbb{Z}G/\mathcal{S} \simeq \mathbb{Z}/h\mathbb{Z}$ as rings (uniquely).*

Of course, annihilation of the class group may be proved (by purely algebraic means) using Stickelberger's factorization of Gauss sums in cyclotomic fields (see Theorem 6.2 in [6] and Theorem 3.1 in [5]). On the other hand, there is also an elegant arithmetic approach to the class number formula for imaginary quadratic number fields due to Orde [4].

The (cyclic) structure of $\mathbb{Z}G/\mathcal{S}$ (as an additive group) does not really reflect the structure of the ideal class group C, because usually the annihilator of C is larger than the Stickelberger ideal:

THEOREM 2. *Let t be the number of rational primes dividing d. Assume that $t \geq 2$. Then $\theta/2^{t-2}$ is in $\mathbb{Z}G$ and annihilates $C = \mathrm{Cl}_K$.*

Here we apply the Gauss theorem on genera. It tells us that $t-1$ of the ramified prime ideals of K (lying over d) give rise to an independent set of involutions in C (but each getting principal in the genus field of K). There is no (analogous) result describing the p-primary structure of C for odd primes p. Heuristic methods (Cohen–Lenstra [2]) indicate, and experience confirms it (see e.g. Buell [1]), that the odd part of C is cyclic with probability of about 97%. We just mention the following.

ADDENDUM. *Suppose p is an odd prime. Then $\theta/p \in \mathbb{Z}G$ if and only if p is a divisor of both h and $\varphi(d)$ (Euler function).*

In this case θ/p annihilates C precisely when the p-component of C is *not* cyclic. This is a rather sophisticated comment, however, because no arithmetic condition seems to be around forcing this annihilation.

2. Quadratic characters. Let χ be an (arbitrary) primitive Dirichlet character with order 2 and conductor d. We do not insist that χ is odd. One knows that $\chi = \chi_D$ is determined by its discriminant D where $D = -d$ if χ is odd ($\chi(-1) = -1$) and $D = d$ otherwise. We define

$$u_\chi = \frac{1}{d} \sum_{\substack{a=1 \\ \chi(a)=1}}^{d} a \quad \text{and} \quad v_\chi = \frac{1}{d} \sum_{\substack{a=1 \\ \chi(a)=-1}}^{d} a.$$

Obviously du_χ, dv_χ are integers. Note also that $\varphi(d) = |G(d)|$ is an *even* integer. There are just $\varphi(d)/2$ integers a in the real interval $[1, d)$ (prime to d) for which $\chi(a) = 1$ (and the same number for which $\chi(a) = -1$).

LEMMA 1. *We have* $u_\chi + v_\chi = \varphi(d)/2$.

Proof. By the very definition $d(u_\chi + v_\chi) = \sum_{(a,d)=1} a$ (with $a \in \mathbb{Z} \cap [1,d)$). Now a is prime to d precisely when $d-a$ is prime to d, and $a+(d-a) = d$. We conclude (à la Gauss) that $2d(u_\chi + v_\chi) = \varphi(d)d$, as desired. ∎

LEMMA 2. *Suppose d is a power of an odd prime p. Then $d = p$, $D = (-1)^{(p-1)/2}p$ and $\chi = \left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Except when $p = 3$ here u_χ and v_χ are integers.*

Proof. The first statement follows from the fact that $G(p^n)$ is cyclic for all $n \geq 1$ (and χ is primitive of order 2). Let $G(p) = \langle z \rangle$. Then $z^2 \neq 1$ unless $p = 3$, and we have

$$2\sum_{y \in \mathbb{F}_p^2} y = \sum_{x \in \mathbb{F}_p} x^2 = \sum_{x \in \mathbb{F}_p} (zx)^2 = 2z^2 \sum_{y \in \mathbb{F}_p^2} y$$

in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. This gives the result for u_χ. By Lemma 1 (or directly) then v_χ is an integer as well. ∎

LEMMA 3. *Suppose d is a 2-power. Then $d = 4$ ($D = -4$) or $d = 8$ ($D = \pm 8$). Here $u_\chi = v_\chi = 1$ if χ is even ($D = 8$) and otherwise u_χ, v_χ are not integral.*

Proof. For $n \geq 3$ the group $G(2^n)$ is of type $(2, 2^{n-2})$. Hence the kernel of any character of $G(2^n)$ of order 2 contains the kernel of the natural map $G(2^n) \twoheadrightarrow G(2^3)$. The remainder is by inspection. ∎

LEMMA 4. *If d is not a prime power, then both u_χ and v_χ are integers.*

Proof. By hypothesis $d = d_1 d_2$ for relatively prime integers $d_i \geq 3$. Then $G(d) \simeq G(d_1) \times G(d_2)$ in the natural way (by the Chinese remainder theorem), and $\chi = \chi_1 \cdot \chi_2$ for unique (primitive, quadratic) Dirichlet characters χ_i with conductor d_i.

For a fixed integer $a \in \mathbb{Z} \cap [1, d_1)$ relatively prime to d_1 consider the set

$$\Sigma_a = \{x \in \mathbb{Z} : 1 \leq x \leq d,\ (x,d) = 1,\ x \equiv a \pmod{d_1}\}.$$

The cardinality of this set is $|G(d_2)| = \varphi(d_2)$. There are just $\varphi(d_2)/2$ elements $x \in \Sigma_a$ for which $\chi_2(x) = 1$ (resp. $\chi_2(x) = -1$). Since $\chi_1(x) = \chi_1(a)$ for each $x \in \Sigma_a$, and $\chi(x) = \chi_1(x)\chi_2(x)$, there are exactly $\varphi(d_2)/2$ elements $x \in \Sigma_a$ satisfying $\chi(x) = 1$ (independent of whether $\chi_1(a) = 1$ or -1). Therefore we have

$$du_\chi \equiv \frac{\varphi(d_2)}{2} \sum_{\substack{a=1 \\ (a,d_1)=1}}^{d_1} a \equiv \frac{\varphi(d_2)}{2} d_1 \frac{\varphi(d_1)}{2} \pmod{d_1},$$

where we used Lemma 1 (for χ_1) to compute the sum. It follows that $du_\chi = d_1 d_2 u_\chi$ is an integer divisible by d_1. Hence $d_2 u_\chi$ is an integer. Similarly $d_1 u_\chi$

is an integer. Using the fact that $(d_1, d_2) = 1$ we see that u_χ is an integer, as desired. By the same argument, or by Lemma 1, also v_χ is an integer. ∎

3. Proof of Theorem 1. We return to the imaginary quadratic field K with discriminant $D = -d$, Galois group $G = \langle j \rangle$, and quadratic (Kronecker) character $\chi = \chi_D$. For this χ we write $u = u_\chi$ and $v = v_\chi$. We have $\chi(a) = -1$ if $(\sigma_a^{-1})|_K = j$ and $\chi(a) = 1$ otherwise ($a \in G(d)$). Thus, by definition, the Stickelberger element of K is $\theta = u + vj$. Furthermore,

$$B_{1,\chi} = \frac{1}{d} \sum_{a=1}^{d} \chi(a) a = u - v$$

is the (generalized) Bernoulli number. By the (analytic) class number formula $h = -B_{1,\chi}$ except when $d = 3$ or $d = 4$. Excluding these two cases and also $d = 8$, from Lemmas 2–4 it follows that both u, v are integers. Consequently, $\theta = u + vj \in \mathbb{Z}G$, which is Theorem 1.

The assignment $x + yj \mapsto x - y$ is a ring epimorphism from $\mathbb{Z}G$ onto $\mathbb{Z}$, with kernel $\langle 1 + j \rangle$, mapping θ onto $u - v = -h$. Hence $\mathbb{Z}G/\mathcal{S} \simeq \mathbb{Z}/h\mathbb{Z}$, which gives the corollary to Theorem 1. ∎

Remark. Stickelberger factorization yields that $\theta = u + vj$ annihilates $C = \mathrm{Cl}_K$ (without assuming the class number formula). Then our lemmas provide for the (apparently strong) upper estimate that the exponent of C is a divisor of $-B_{1,\chi} = v - u$. However, we do not get $v > u$ in this manner, not even $B_{1,\chi} \neq 0$ (which follows from $L(1, \chi) \neq 0$). The sign involved, formulated as a problem on Gauss sums, has a long history (Gauss, Dirichlet, Kronecker, Schur).

4. Proof of Theorem 2. By Lemma 1 we have $u + v = \varphi(d)/2$. Moreover, excluding the cases $d = 3, 4$, by the class number formula $h = v - u$. Consequently,

$$(*) \qquad h = -2u + \varphi(d)/2 = 2v - \varphi(d)/2.$$

Now suppose the number of primes dividing d is $t \geq 2$. Then $\varphi(d)$ is divisible by 2^t. By the Gauss theorem on genera $C = \mathrm{Cl}_K$ has 2-rank $t - 1$. It follows that the exponent of C is a divisor of $h/2^{t-2}$. In other words, $h/2^{t-2}$ is an even integer which annihilates C. We infer from $(*)$ that both u and v are integers divisible by 2^{t-2}. From $\theta = u + vj$ it is thus immediate that $\theta/2^{t-2}$ is in $\mathbb{Z}G$ and that it annihilates C (Theorem 2).

Suppose now that p is an odd prime. If $\theta/p \in \mathbb{Z}G$, then both u and v are integers divisible by p. This forces that $d \neq 3, 4, 8$. Moreover, it follows that p divides $h = v - u$. The class number formula $(*)$ shows that p is a divisor of $\varphi(d)$. The converse is proved similarly, giving the addendum to Theorem 2. ∎

REMARK. Recall that the class number formula $(*)$ holds true when $d \neq 3, 4$. Excluding also $d = 8$ we know that u, v are integers. Then if h is odd, $\varphi(d)/2$ must be odd and so d a prime $\equiv 3 \pmod 4$. This is a weak form of the Gauss theorem on genera. Conversely, from the Gauss theorem and formula $(*)$ we may deduce that u and v are integers when $d \neq 3, 4, 8$. For then h is odd precisely when d is a prime $\equiv 3 \pmod 4$, and just in this case $\varphi(d)/2$ is odd too.

References

[1] D. A. Buell, *Class groups of quadratic fields*, Math. Comp. 30 (1976), 610–623.

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

[3] R. Kučera, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, J. Number Theory 56 (1996), 139–166.

[4] H. L. S. Orde, *On Dirichlet's class number formula*, J. London Math. Soc. (2) 18 (1978), 409–420.

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

[6] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, Heidelberg, 1997.

Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10
D-72076 Tübingen, Germany
E-mail: peter.schmid@uni-tuebingen.de

Received on 16.11.1998
and in revised form on 25.3.1999 (3511)