VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-012-0081-2
Math. Slovaca **63** (2013), No. 1, 53–62

AN EXTENDED STICKELBERGER IDEAL OF THE COMPOSITUM OF A BICYCLIC FIELD AND AN IMAGINARY QUADRATIC FIELD

Veronika Trnková

(*Communicated by Stanislav Jakubec*)

ABSTRACT. We consider certain extension of the Stickelberger ideal of the compositum of a bicyclic field and a quadratic imaginary field, obtained by adding new annihilators to the Stickelberger ideal. We compute the index of this extension, from which we get some divisibility properties for the relative class number of the compositum.

1. Introduction

The Stickelberger ideal for abelian fields (i.e. algebraic number fields having over $\mathbb{Q}$ a commutative Galois group G) was introduced by W. Sinnott in 1980 in the paper [4]. It is an ideal of the group ring $\mathbb{Z}[G]$ and has a very important property: it consists of elements which annihilate the class group of the corresponding abelian field. Usually, there exist much more such elements. However, these other annihilators we can not, in contrast to the elements of the Stickelberger ideal, define by an explicit formula.

In [1] C. Greither and R. Kučera proved the existence of certain annihilator of the class group of the compositum of an imaginary quadratic field and a cyclic field. This annihilator is not contained in the Stickelberger ideal of the compositum, but can be expressed in terms of a known Stickelberger element.

Let us consider the compositum of an imaginary quadratic field F and a bicyclic field K. We call a field bicyclic if its Galois group is a non-cyclic group of order l^2 for an odd prime l. Except for F, proper imaginary subfields of

2010 Mathematics Subject Classification: Primary 11R20, 11R29.
Keywords: Stickelberger ideal, bicyclic field, class number.
The author was supported under the project GD201/09/H012 of the Czech Science Foundation.

KF are just the composita of F and cyclic subfields of K. Therefore, for these subfields, there exist new annihilators, described by Greither and Kučera, which are not contained in the Stickelberger ideal. Mapping these new annihilators to the group ring $\mathbb{Z}[G]$, we can gain new annihilators of the class group of KF. Hence we can consider the extension of Stickelberger ideal, obtained by adding annihilators which were constructed in such a way.

The index of the Stickelberger ideal S of KF was computed by P. Kraemer in [3]. Our aim is to compute the index of the extended Stickelberger ideal and to show that if there are at least three primes ramifying in K, the extended Stickelberger ideal is strictly larger then S. The resulting index is determined by the Hasse unit index and the relative class number of KF, and by the degree of K and the number of primes ramifying in K, while the index of S depends, in addition, on what subfields K possesses. Moreover, knowing the index of the extended Stickelberger ideal we can easily deduce divisibility of the relative class number of KF by a certain power of l.

2. The compositum of a bicyclic field and an imaginary quadratic field, and the Stickelberger ideal

Let us take an arbitrary bicyclic field K of degree l^2, where l is an odd prime, i.e. $K/\mathbb{Q}$ is a Galois extension whose Galois group G_K is isomorphic to $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. Assume that l does not ramify in K. Let us denote by f the conductor and by h_K the class number of K. The non-trivial subfields of K will be denoted by $K_0, K_1, \ldots, K_l$ and their conductors by $f_0, f_1, \ldots, f_l$, respectively.

From [2: Lemma 3.1] we know that f is square-free. Hence we can write $f = p_1 p_2 \ldots p_z$, where $p_1, p_2, \ldots, p_z$ are pairwise distinct primes. Moreover, $z \geq 2$, because G_K is non-cyclic. Further, for each $i \in \{0, \ldots, l\}$, let us take the set $P_i = \{j \in \{1, \ldots, z\} : p_j \nmid f_i\}$ and set $z_i = z - |P_i|$. So z_i equals the number of ramifying primes in $K_i/\mathbb{Q}$.

We take an imaginary quadratic field F such that $p_1, \ldots, p_z$ split completely in F and the number l does not ramify in F. This means, among others, that the number w of roots of unity in KF is not divisible by l. Let m be the conductor of F and $Q \in \{1, 2\}$ the Hasse unit index of the compositum KF. The class number h_{KF} of KF is the product of the relative class number h_{KF}^- and h_K. For the Galois group G of KF we have $G = \langle G_K \cup \{J\} \rangle$ where J means the complex conjugation.

For each i, let $\delta_i \in G$ be a fixed automorphism whose restriction to K_iF is a generator of $\mathrm{Gal}(K_iF/F)$, by abuse of notation denoted by δ_i as well. For each i and each $j \in P_i$, let k_{ij} be the non-negative integer satisfying $k_{ij} < l$

and $\delta_i^{k_{ij}} = \mathrm{Frob}^{-1}(p_j, K_iF)$. This means that Frobenius automorphisms of all primes dividing f are determined by numbers k_{ij}.

We will denote the group ring $\mathbb{Z}[G]$ by R. Let A be the set of all elements α of the group ring R such that $(1+J)\alpha$ lies in $(\sum_{\sigma\in G}\sigma)R$. The G-module A contains the Stickelberger ideal S (see [4]). Let us recall the definition of S. For an abelian field L and its subfield M, let $\mathrm{res}_{L/M} : \mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}(M/\mathbb{Q})]$ be the ring homomorphism determined for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ by restriction $\mathrm{res}_{L/M}(\sigma) = \sigma|_M$ and let $\mathrm{cor}_{L/M} : \mathbb{Q}[\mathrm{Gal}(M/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})]$ be the additive group homomorphism satisfying

$$\mathrm{cor}_{L/M}(\tau) = \sum_{\substack{\tau'\in\mathrm{Gal}(L/\mathbb{Q})\\ \tau'|_M=\tau}} \tau'$$

for $\tau \in \mathrm{Gal}(M/\mathbb{Q})$. The Stickelberger ideal S is defined as the intersection of $\mathbb{Z}[G]$ and

$$S' = \Big\langle \mathrm{cor}_{KF/\mathbb{Q}_n\cap KF}\mathrm{res}_{\mathbb{Q}_n/\mathbb{Q}_n\cap KF} \sum_{\substack{0<t\le n\\ (t,n)=1}} \Big\langle -\frac{at}{n}\Big\rangle \sigma_{n,t}^{-1};\ n\in\mathbb{N}, a\in\mathbb{Z}\Big\rangle,$$

where $\mathbb{Q}_n$ is the n-th cyclotomic field, automorphism $\sigma_{n,t}$ of $\mathbb{Q}_n$ maps each n-th root of unity to its t-th power, and $\langle x\rangle$ denotes the fractional part of a real number x. We set $M^- = \frac{1-J}{2}M \cap M$ for an arbitrary G-module M.

According to [3: Corollary 5.1] S'^- for our field KF is generated as a G-module by elements θ_{KF}^-, θ_F^- and $\theta_{K_iF}^-$ for every subfield K_iF, where

$$\theta_{KF}^- = \frac{1-J}{2}\mathrm{res}_{\mathbb{Q}_{fm}/KF} \sum_{(t,fm)=1} \Big\langle\frac{t}{fm}\Big\rangle \sigma_{fm,t}^{-1}$$

$$\theta_F^- = \frac{1-J}{2}\mathrm{cor}_{KF/F}\mathrm{res}_{\mathbb{Q}_m/F} \sum_{(t,m)=1} \Big\langle\frac{t}{m}\Big\rangle \sigma_{m,t}^{-1}$$

$$\theta_{K_iF}^- = \frac{1-J}{2}\mathrm{cor}_{KF/K_iF}\mathrm{res}_{\mathbb{Q}_{f_im}/K_iF} \sum_{(t,f_im)=1} \Big\langle\frac{t}{f_im}\Big\rangle \sigma_{f_im,t}^{-1}$$

We will write $S'^- = \langle \theta_{KF}^-, \theta_F^-, \{\theta_{KF_i}^- :\ i\in\{0,\dots,l\}\}\rangle_G$. Moreover, denote by T the subgroup of S'^- generated as a G-module by θ_F^- and by all $\theta_{K_iF}^-$.

3. The construction of an extended Stickelberger ideal

Let us denote by $\mathbb{Z}_l$ the ring of l-adic integers. Due to [1: Theorem 6.1] there exists for each i an annihilator $\vartheta_i' \in \mathbb{Z}_l[\mathrm{Gal}(K_iF/F)]$ of the minus part of the l-Sylow subgroup of the class group of K_iF of the form $(\delta_i - 1)\vartheta'_{i0}$ for $\vartheta'_{i0} \in \mathbb{Z}_l[\mathrm{Gal}(K_iF/F)]$ such that

$$(1-J)(\delta_i - 1)^{z_i - 1}\vartheta'_i = (1-J)\mathrm{res}_{\mathbb{Q}_{f_i m}/K_iF} \sum_{(t, f_i m)=1} \Big\langle \frac{t}{f_i m} \Big\rangle \sigma^{-1}_{f_i m, t}.$$

Lemma 1. *For each $i \in \{0, \dots, l\}$ we have*

$$\vartheta'_i \in \mathbb{Q}[\mathrm{Gal}(K_iF/F)].$$

P r o o f. The statement follows from

$$((\delta_i - 1)\sum_{j=1}^{l-1} j\delta_i^j)^{z_i - 1}\vartheta'_i = (l - \sum_{j=0}^{l-1} \delta_i^j)^{z_i-1}\vartheta'_i = l^{z_i - 1}\vartheta'_i$$

since $\vartheta'_i = (\delta_i - 1)\vartheta'_{i0}$ and $(\delta_i - 1)^{z_i-1}\vartheta'_i \in \mathbb{Q}[\mathrm{Gal}(K_iF/F)]$ according to [1: Theorem 6.1]. □

We can set ϑ_i for $\frac{1-J}{2}\mathrm{cor}_{KF/K_iF}\vartheta'_i$. Then we have

$$\vartheta_i = \frac{1-J}{2}(\delta_i - 1)\mathrm{cor}_{KF/K_iF}\vartheta'_{i0}.$$

Recall that the group ring $\mathbb{Z}[G]$ is denoted by R. The following lemma gives some properties of ϑ_i.

Lemma 2. *For each i we have $\theta^-_{K_iF} = (\delta_i - 1)^{z_i-1}\vartheta_i$. Moreover, $l^{z_i-1}\vartheta_i \in S'$ and $w\vartheta_i \in R$.*

P r o o f. By substituting we obtain

$$\begin{aligned}
\theta^-_{K_iF} &= \frac{1-J}{2}\mathrm{cor}_{KF/K_iF}\mathrm{res}_{\mathbb{Q}_{f_i m}/K_iF} \sum_{(t, f_i m)=1} \Big\langle \frac{t}{f_i m} \Big\rangle \sigma^{-1}_{f_i m, t} \\
&= \frac{1-J}{2}\mathrm{cor}_{KF/K_iF}(\delta_i - 1)^{z_i - 1}\vartheta'_i \\
&= (\delta_i - 1)^{z_i-1}\vartheta_i.
\end{aligned}$$

Since $\theta^-_{K_iF} \in S'$, we can similarly as in the proof of the previous lemma show that the same holds for $l^{z_i-1}\vartheta_i$. [4: Proposition 2.1] states that $[S' : S] = w$, therefore $wl^{z_i-1}\vartheta_i \in S \subseteq R$. From the fact that $\vartheta'_i \in \mathbb{Z}_l[\mathrm{Gal}(K_i/F)]$ and consequently $\vartheta_i \in \mathbb{Z}_l[G]$ we obtain $w\vartheta_i \in R$. □

We can consider the additive group $Z' \subseteq \mathbb{Q}[G]$ generated as a G-module by S' and all elements ϑ_i. The submodule of Z'^- generated by θ^-_F and all ϑ_i is called V. Similarly as in the definition of Stickelberger ideal, we set $Z = Z' \cap R$. Clearly, $S \subseteq Z$. Therefore we call Z the extended Stickelberger ideal of KF. We want to show that Z annihilates the class group $\mathcal{C}$ of KF. We need the following lemma:

Lemma 3. *The index $[Z : S]$ is a power of l and the index $[Z' : Z] = w$.*

Proof. From the previous lemma it follows that the index $[Z' : S']$ is a power of l and consequently the same holds for the index $[Z : S]$. Lemma 2 also gives that $[Z' : Z]$ divides a power of w. On the other hand,

$$[Z' : Z] \cdot [Z : S] = [Z' : S] = w \cdot [Z' : S'].$$

We obtain $[Z' : Z] = w$, because $l \nmid w$. $\square$

Proposition 4. *The ideal Z annihilates the class group $\mathcal{C}$ of KF.*

Proof. Since S annihilates $\mathcal{C}$ (see [4: Theorem 3.1]), we get using the previous lemma that Z annihilates every q-Sylow subgroup of the class group $\mathcal{C}$ for a prime $q \neq l$.

From [1: Lemma 1.6] it follows that each ϑ_i annihilates the minus part of the l-Sylow subgroup of $\mathcal{C}$, and hence the same does Z. Since the plus part of the l-Sylow subgroup of $\mathcal{C}$ is annihilated by ϑ_i trivially, the statement is proved. $\square$

4. Finding a basis of Z'^-/V

First, we express θ^-_{KF} in terms of generators of the G-module V. By substituting $(\delta_i - 1)^{z_i - 1}\vartheta_i$ for $\theta^-_{KF_i}$ (see Lemma 2) in [3: Corollary 5.2] we obtain the following proposition:

Proposition 5. *The Stickelberger element θ^-_{KF} satisfies*

$$l \cdot \theta^-_{KF} = \sum_{i=0}^{l} (\delta_i - 1)^{z_i - 1}\vartheta_i \prod_{j \in P_i} (1 - \delta_i^{k_{ij}}).$$

Proposition 6. *The set $M = \{\theta^-_F\} \cup \{\delta_i^j \cdot \vartheta_i;\ 0 \le i \le l,\ 0 \le j \le l-2\}$ forms a $\mathbb{Z}$-basis of V.*

Proof. Since $\vartheta_i = (\delta_i - 1)\vartheta_{i0}$, where $\vartheta_{i0} = \frac{1-J}{2}\mathrm{cor}_{KF/K_iF}\vartheta'_{i0} \in \mathbb{Z}_l[G]$, we have $\Big(\sum\limits_{j=0}^{l-1} \delta_i^j\Big)\vartheta_i = 0$. Therefore $\delta_i^{l-1} \cdot \vartheta_i$ can be expressed in terms of elements of M and V is generated by M.

Recall that T is the G-module generated by θ^-_F and by all $\theta^-_{K_iF}$. Since $T \subseteq V \subseteq \frac{1}{w}R^-$, and $\mathbb{Z}$-rank of both R^- and T is equal to l^2 (see [3: Proposition 5.2]), the $\mathbb{Z}$-rank of V is equal to l^2 as well. This is exactly the number of elements of M, and therefore the set M is a basis of V. $\square$

If for a certain i there exists $j \in P_i$ such that $k_{ij} = 0$, the following equality holds:

$$\vartheta_i(\delta_i - 1)^{z_i - 1} \prod_{j \in P_i} (1 - \delta_i^{k_{ij}}) = 0.$$

Hence we do not have to consider all such i in the product from Proposition 5. Let q denote the number of subfields K_i such that k_{ij} is non-zero for every $j \in P_i$. For the simplicity we can assume that subfields K_i are numbered in such a way that this holds just for $i \in \{0, \dots, q-1\}$. Further, in what follows, we will write $\mathbb{F}_l$ for the finite field of l elements.

Proposition 7. *Let $d = l - z$ and $\mu_i(\delta_i) = (-1)^{z_i - 1} \prod\limits_{j \in P_i} \sum\limits_{h=0}^{k_{ij}-1} \delta_i^h$ for each $i \in \{0, \dots, q-1\}$. Then*

$$l \cdot \theta_{KF}^- = \sum_{i=0}^{q-1} \vartheta_i \cdot \mu_i(\delta_i)(1 - \delta_i)^{l-1-d}.$$

Moreover, $\mu_i(\delta_i)$ is not divisible by $1 - \delta_i$ in $\mathbb{F}_l[\langle\delta_i\rangle]$.

P r o o f. By rewriting the statement of Proposition 5 we obtain

$$\begin{aligned} l \cdot \theta_{KF}^- &= \sum_{i=0}^{q-1} \vartheta_i \cdot (\delta_i - 1)^{z_i - 1} \prod_{j \in P_i} ((1 - \delta_i) \sum_{h=0}^{k_{ij}-1} \delta_i^h) \\ &= \sum_{i=0}^{q-1} \vartheta_i \cdot \mu_i(\delta_i)(1 - \delta_i)^{|P_i| + z_i - 1} \end{aligned}$$

The first statement follows from $|P_i| + z_i = z = l - d$.

Now let us prove the second statement. We have $\delta_i \equiv 1 \pmod{1 - \delta_i}$, so

$$\mu_i(\delta_i) \equiv (-1)^{z_i - 1} \prod_{j \in P_i} k_{ij} \pmod{1 - \delta_i}.$$

However, each k_{ij} is non-zero, because $i < q$, therefore the right side of the congruence is a unit in $\mathbb{F}_l[\langle\delta_i\rangle]$. On the other hand, $(1 - \delta_i) \sum\limits_{j=0}^{l-1} \delta_i^j = 0$, and so $1 - \delta_i$ is not a unit. Hence $1 - \delta_i$ does not divide $\mu_i(\delta_i)$. □

Let σ be a fixed generator of $\mathrm{Gal}(KF/K_0F)$ and τ a fixed generator of $\mathrm{Gal}(KF/K_1F)$. Then for every $i \geq 2$ there exists a generator of $\mathrm{Gal}(KF/K_iF)$ of the form $\tau\sigma^{l-n_i}$, where $n_i \in \{1, \dots, l-1\}$ is uniquely determined. This implies that restrictions of τ and σ^{n_i} to K_iF are the same for all $i \in \{2, \dots, l\}$, so we can assume that $\delta_0 = \tau$ and $\delta_i = \sigma$ for $i \in \{1, \dots, l\}$.

Since Z'^-/V is a G-module generated by θ_{KF}^- and $l \cdot \theta_{KF}^- \in V$ by Proposition 7, the quotient Z'^-/V forms a vector space over $\mathbb{F}_l$. For polynomials

$v_1, \ldots, v_m \in \mathbb{Z}[s,t]$, the set $U = \{\theta_{KF}^- \cdot v_1(\sigma,\tau), \ldots, \theta_{KF}^- \cdot v_m(\sigma,\tau)\}$ is a basis of Z'^-/V if and only if both

$$\langle U \cup V \rangle = Z'^-$$

and for each choice of $c_i \in \mathbb{Z},\ i \in \{1,\ldots,m\}$ the following implication holds:

$$\theta_{KF}^- \cdot \sum_{i=1}^{m} c_i v_i(\sigma,\tau) \in V \Rightarrow c_1 \equiv \cdots \equiv c_m \equiv 0 \pmod{l}.$$

In order to determine generators of Z'^-/V we need the following two lemmas similarly as in [2] and [5]:

Lemma 8. *Let $g,\ h \in \mathbb{Z}[t]$ and $N(t) = \sum_{j=0}^{l-1} t^j$. Then $\vartheta_i \cdot g(\delta_i) = \vartheta_i \cdot h(\delta_i)$ if and only if $g(t) \equiv h(t) \pmod{N(t)}$ in $\mathbb{Z}[t]$.*

Lemma 9. *If $d \le 0$, we have*

$$\vartheta_i \cdot \mu_i(\delta_i)(1-\delta_i)^{l-1-d} \in l \cdot V.$$

Using these lemmas, we can prove the statement, which reduces the set of generators of Z'^-/T:

Proposition 10. *Let $v \in \mathbb{F}_l[s,t]$ be a polynomial and assume that $d > 0$. Then $\theta_{KF}^- \cdot v(1-\sigma, 1-\tau) \in V$ is satisfied if and only if all the following conditions hold in $\mathbb{F}_l[s,t]$:*

$$\begin{aligned} v(0,t) &\equiv 0 \pmod{t^d} \qquad &&\text{if} \quad q > 0,\\ v(s,0) &\equiv 0 \pmod{s^d} \qquad &&\text{if} \quad q > 1, \end{aligned}$$

and for all $i \in \{2,\ldots,q\}$

$$v(s, 1-(1-s)^{n_i}) \equiv 0 \pmod{s^d}$$

Proof. Similarly as the proof of [2: Proposition 4.1] using Lemmas 8 and 9. □

Now, we can formulate the following theorem, which states that the set of generators, obtained by applying Proposition 10 is a basis:

Theorem 11. *The set*

$$U = \{(1-\tau)^i (1-\sigma)^j \theta_{KF}^- :\ i,j \ge 0,\ i+j < d\}$$

is a basis of the vector space Z'^-/V.

Proof. The theorem can be proved analogously to [5: Theorem 12]. □

5. Computing the index $[A : Z]$

In order to compute the index $[A : Z]$, we first compute the index $[V : T]$.

Lemma 12.

$$[V : T] = l^{zl-l-1}$$

P r o o f. Due to Lemma 8, $\langle\vartheta_i\rangle_G \cong \mathbb{Z}[t]/\Big(\sum_{i=0}^{l-1} t^i\Big)\mathbb{Z}[t]$. Let $\zeta_l = \mathrm{e}^{\frac{2\pi\mathrm{i}}{l}}$ be the l-th primitive root of unity. Since this quotient ring is isomorphic to $\mathbb{Z}[\zeta_l]$, Lemma 2 gives

$$\langle\vartheta_i\rangle_G/\langle\theta^-_{K_iF}\rangle_G \cong \mathbb{Z}[\zeta_l]/(\zeta_l - 1)^{z_i-1}\mathbb{Z}[\zeta_l].$$

Hence the number of elements of the quotient group is equal to l^{z_i-1}. [3: Proposition 3.1] states that the sets P_i are pairwise disjoint and $\sum_{i=0}^{l} |P_i| = z$, hence

$$[V : T] = \prod_{i=0}^{l} l^{z_i-1} = l^{z(l+1)-\sum_{i=0}^{l}|P_i|-(l+1)} = l^{zl-l-1}.$$

□

For any finitely generated G-modules L, $M \subseteq \mathbb{Q}[G]$ such that $\mathbb{Q}M = \mathbb{Q}L$ we denote the generalized index of M in L by $(L : M)$. See [4: page 187].

Proposition 13.

$$(R^- : Z'^-) = \begin{cases} \frac{1}{Qw} l^{\frac{1}{2}(l^2-2lz+l+2)} h^-_{KF} & z \geq l \\ \frac{1}{Qw} l^{-\frac{1}{2}(z+1)(z-2)} h^-_{KF} & z \leq l-1 \end{cases}$$

P r o o f. For $z \geq l$ we have $[Z'^- : V] = 1$ from Proposition 7 and Lemma 9. If $z \leq l-1$, Theorem 11 gives

$$[Z'^- : V] = l^{|U|} = l^{\frac{(l-z)(l-z+1)}{2}}.$$

Using the fact that $(R^- : T) = \frac{1}{Qw} l^{\frac{l(l-1)}{2}} h^-_{KF}$ due to [3: Theorem 7.1] and Lemma 12, the statement follows from

$$(R^- : Z'^-) = (R^- : T\,)/([Z'^- : V] \cdot [V : T]).$$

□

Theorem 14. *If $z \geq l$, then*

$$[A : Z] = \frac{1}{Q} l^{\frac{1}{2}(l^2-2lz+l+2)} h^-_{KF}.$$

For $z \leq l-1$ we have

$$[A : Z] = \frac{1}{Q} l^{-\frac{1}{2}(z+1)(z-2)} h^-_{KF}.$$

P r o o f. Since $\{a \in A :\ (1+J)\cdot a = 0\} = A^- = R^-$ and $\{a \in Z' :\ (1+J)\cdot a = 0\} = Z'^-$, we obtain using [4: Lemma 1.2] for G-modules A and Z' and $1+J \in \mathbb{Q}[G]$ the equality

$$(A : Z') = (R^- : Z'^-)\cdot((1+J)A : (1+J)Z').$$

Moreover, $(1+J)A = \big(\sum_{\sigma\in G}\sigma\big)\mathbb{Z}$, and we have $(1+J)Z' = (1+J)S'$, which is equal to $\big(\sum_{\sigma\in G}\sigma\big)\mathbb{Z}$ due to [4: Lemma 2.1]. We get the equality

$$[A : Z] = [Z' : Z]\cdot(R^- : Z'^-),$$

and the statement follows from the previous proposition and Lemma 3. □

Corollary 15. *The ideal Z coincides with the Stickelberger ideal S if and only if $z = 2$.*

P r o o f. Since $S \subseteq Z$, the equality $S = Z$ holds if and only if $[A : Z] = [A : S]$. From [3: Theorem 7.2] we have

$$[A : S] = \frac{1}{Q} l^{\frac{1}{2}l(l-1) - \sum\limits_{0\le i<a_i}(a_i - i)} h^-_{KF},$$

where $a_i = l - 1 - |P_i|$ for each $i < q$ and $a_i = -\infty$ for $i \ge q$. Here, subfields K_i are numbered in such a way that $a_i \ge a_{i+1}$ for each $i \in \{0,\dots,l-1\}$. From this formula and the formula for the index $[A : Z]$ (Theorem 14) we can see that the equality of the indices is equivalent to the equality of the powers of l in both of them.

For the power of l in the index $[A : S]$ we have

$$\frac{1}{2}l(l-1) - \sum_{0\le i<a_i}(a_i - i) \ge 0.$$

On the other hand, if $z \ge l$, we have the inequality

$$\frac{1}{2}(l^2 - 2lz + l + 2) \le \frac{1}{2}(l + 2 - l^2)$$

for the power of l in $[A : Z]$. Since $l \ge 3$, the right side of this inequality is negative.

In the case that $z \le l-1$ and $z \ge 3$ we have

$$-\frac{1}{2}(z+1)(z-2) < 0$$

as well. Therefore in both cases the ideal Z is strictly larger then S.

For $z = 2$, the field K has two proper subfields having a prime conductor and the conductor of all the other subfields is equal to f. [5: Lemma 10] states that

$q \geq l - z + 1 = l - 1$. Hence we get

$$\frac{1}{2}l(l-1) - \sum_{0 \leq i < a_i} (a_i - i) = \frac{1}{2}l(l-1) - \sum_{i=0}^{l-2}(l-1-i) = 0.$$

Therefore the equality $Z = S$ holds just for $z = 2$. □

6. Divisibility of the class number of KF

Immediately from Theorem 14 we obtain the following divisibility property of the relative class number h^-_{KF} by a power of l:

Corollary 16. *If $z \geq l$, the relative class number of KF is divisible by $l^{\frac{1}{2}(2lz-l^2-l-2)}$. In the case that $z \leq l-1$ the relative class number of KF is divisible by $l^{\frac{(z+1)(z-2)}{2}}$.*

From this corollary and the divisibility property for K deduced in [5: Corollary 18], we get this result on the class number of KF:

Corollary 17. *If $z \geq l$, the class number of KF is divisible by $l^{(2lz-l^2-2l-1)}$. In the case that $z \leq l-1$ the class number of KF is divisible by $l^{z(z-2)}$.*

Acknowledgement. I would like to thank Radan Kučera for guiding me through my work on this paper.

REFERENCES

[1] C. Greither and R. Kučera: *Annihilators of the minus class group of imaginary abelian field*, Ann. Inst. Fourier 57 (2007), 1623–1653.
[2] KRAEMER, P.: *Circular units in bicyclic fields*, J. Number Theory **105** (2004), 302–321.
[3] KRAEMER, P.: *Stickelberger ideal of a compositum of a real bicyclic field and quadratic imaginary field*, Math. Slovaca **56** (2006), 415–425.
[4] SINNOTT, W.: *On the Stickelberger ideal and circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.
[5] TRNKOVÁ, V.: *Enlargement of the group of circular units of a bicyclic field*, J. Number Theory **129** (2009), 28–35.

Received 9. 7. 2010
Accepted 1. 11. 2010

Department of Mathematics
Masaryk University
Kotlářská 2
CZ–611 37 Brno
CZECH REPUBLIC
E-mail: xtrnkova@math.muni.cz