Using GP/PARI to Compute Tame Kernel

MA YongSheng
Qingdao University, Shandong Province, China
mayongsheng.ok@163.com

Keywords: GP/PARI, number field, Tame kernel.

Abstract. A new method for proving \( \partial_{v_n} \) to be an isomorphism was presented. Based on the method, an algorithm was presented to prove \( \partial_{v_n} \) to be an isomorphism, which can be implemented in the GP/PARI.

Introduction

In order to compute the tame kernel of quadratic imaginary fields, J.Tate [1] offer a method. Using the method, he has determined the tame kernel of all quadratic imaginary Euclidean fields.

Using Tate’s method and a generalization of the classical theorem of Thue, Skalba [2] has determined the tame kernel of quadratic imaginary fields \( \mathbb{Q}(-19) \) and \( \mathbb{Q}(-20) \). J.Browkin [3] improved estimates of Skalba, and applied these estimates in the case \( \mathbb{Q}(-23) \).

In this paper, a new method is presented for the computation of tame kernel. Based on the new method, the computer can be used to compute the tame kernel of quadratic imaginary fields.

Notation

For any number field \( F \), let \( O_F \) be the ring of integers of \( F \) and \( U \) is the group of units of \( O_F \). In addition, let \( \nu_1, \nu_2, \ldots, \nu_n, \ldots \) (1) be all finite places of \( F \) ordered in such a way that \( N\nu_{m-1} \leq N\nu_{m} \) for \( m = 2, 3, \ldots \), where \( N\nu_{m} \) is the norm of \( \nu_{m} \).

For \( m \geq 1 \) let \( S_m = \{\nu_1, \nu_2, \ldots, \nu_m\} \). Denote by \( O_{S_m} \) the ring of \( S_m \)-integers of \( F \), by \( U_{S_m} \) the group of \( S_m \)-units, and the residue field of the place \( \nu_m \) is denoted by \( k_{\nu_m} \).

Let \( K_2^S(F) \) be the subgroup of \( K_2 F \) generated by symbols \( \{a, b\} \), where \( a, b \in U_{S_m} \). Then \( K_2 F = \bigcup_{m=1}^{\infty} K_2^S(F) \).

Let \( \partial_{v_n} : K_2^S \rightarrow k_{v_n}^* \) be the tame symbol corresponding to \( \nu_m \) and \( \partial = \bigoplus_{m=1}^{\infty} \partial_{v_m} : K_2 F \rightarrow \bigoplus_{m=1}^{\infty} k_{v_m}^* \) (2).

Since \( \partial_{v_m} (K_{2n-1}^S(F)) = 0 \), there is an induced map (also denoted by \( \partial_{v_m} \)) \( \partial_{v_m} : K_{2n}^S(F) \cap K_{2n-1}^S(F) \rightarrow k_{v_m}^* \) (3).

If the prime ideal of \( O_{S_{n+1}} \) corresponding to \( \nu_m \) is principal generated by \( \pi_m \), i.e., \( \nu_m O_{S_{n+1}} = \{x \in O_{S_{n+1}} | \nu_m(x) \geq 1\} = \pi_m O_{S_{n+1}} \), we get the following commutative diagram

Table 1. commutative diagram

\[
\begin{array}{ccc}
K_{2n}^S(F) \cap K_{2n-1}^S(F) & \xrightarrow{\partial_{v_m}} & k_{v_m}^* \\
\alpha & & \beta \\
\end{array}
\]

where \( \alpha(u) = [u, \pi_m] (mod K_{2n-1}^S(F)) \) and \( \beta(u) = u (mod \pi_m) \) for \( u \in U_{S_{n+1}} \). We know that if \( \partial_{v_m} \) is an isomorphism for every \( m > N \), where \( N \) is a positive integer, then \( K_2 O_F \subseteq K_2^S(F) \). Since the group \( K_2^S(F) \) has a finite number of generators, it is usually possible to determine the group...
$K_2O_F$ after some additional computations.

**Main Result**

We say that a prime ideal $p$ of $O_F$ is earlier than $v_m$ if the valuation corresponding to $p$ appears before $v_m$ in the sequence (1).

Let $Q_F$ be a set of representatives $q$ of all ideal classes satisfying that $q \subseteq O_F$, and for each integral ideal $a$, if $a$ is in the same ideal class with $q$, then $Nq \leq Na$.

**Lemma 1** [3]. If $W = \{1 \neq w \in O_F \mid (w) = pq \}$ or $q, q_1, q_2, q_3 \in Q_F \}$, then $U_{S_{n-1}}$ is generated by $W$.

**Lemma 2.** Suppose that the prime ideal of $O_{S_{n-1}}$ corresponding to $v_m$ is principal generated by $\pi_m$. If $a, b \in U \cap O_F$, $v_m(a - b) = 1$ and $v_m(i - b) = 0(i = 1, 2, 3, \cdots)$, then $a \in U_1$.

**Proof.** If $a, b \in U \cap O_F$, $v_m(a - b) = 1$ and $v_m(i - b) = 0(i = 1, 2, 3, \cdots)$, there is an element $u \in U_{S_{n-1}}$ such that $a - b = \pi_m u$. Therefore we get $a/b = 1 + u\pi_m/b \in U_1$.

We will give a new condition for $\partial_{v_m}$ being bijective.

**Theorem 1.** Suppose that the prime ideal of $O_{S_{n-1}}$ corresponding to $v_m$ is principal generated by $\pi_m$, and the $\beta$ corresponding to $v_m$ is surjective. Let $U_1$ be a group generated by $(1 + \pi_m U_{S_{n-1}}) \cap U_{S_{n-1}}$. If there is an element $g \in U_{S_{n-1}}$ satisfying the following conditions:

1. $g^{Nv_m - 1} \in U_1$;
2. $U_{S_{n-1}}$ is generated by $gU_1$.

then $\partial_{v_m}$ is an isomorphism.

**Proof.** Let $\langle gU_1 \rangle$ is a subgroup of $U_{S_{n-1}}/U_1$, which is generated by $gU_1$. Form (2) it follows that $\langle gU_1 \rangle = U_{S_{n-1}}/U_1$, and hence we get $|gU_1| \geq Nv_m - 1$, where $|gU_1|$ is the order of $\langle gU_1 \rangle$. By (1) above, we have $|gU_1| \leq Nv_m - 1$, so $|U_{S_{n-1}}/U_1| = |gU_1| = Nv_m - 1$. Since $\beta$ is surjective and $U_1 \subseteq \ker(\alpha) \subseteq \ker(\beta)$, we get $|U_{S_{n-1}}/\ker(\beta)| = Nv_m - 1$ and $\ker(\beta) = U_1$. Therefore $\partial_{v_m}$ is an isomorphism.

**Applications**

Based on Lemma 1, Lemma 2 and Theorem 1, an algorithm is presented in this section to prove $\partial_{v_m}$ to be an isomorphism, which can be implemented in the GP/PARI.

**Algorithm.** Input: the prime ideal $p$ corresponding to $v_m$.

Output: TRUE if there is an element $g$ satisfying Theorem 2 above, FALSE otherwise.

(a) If there is not an element $q \in Q_F$ such that $Nq < Np$ and $pq$ is principal, return FALSE. Else go to Step (b).

(b) Compute the generator $g (\text{mod} v_m)$ of $k_{v_m}^*$, where $g \in O_F$.

(c) If there is not an element $g \in g (\text{mod} v_m)$ such that $g \in U_{S_{n-1}}$, return FALSE. Else compute an element $g \in g (\text{mod} v_m) \cap U_{S_{n-1}}$ such that $g^{Nv_m - 1} \in U_1$ using GP/PARI. If there is no such an element $g$, return FALSE. Else go to Step (d).

(d) Compute an integer $n (1 \leq n \leq Nv_m - 1)$ such that $w \in g^n (\text{mod} v_m)$, where $w \in W$. If $w - g^n$ satisfies $v_m(w - g^n) = 1$ and $v_{m+1}(w - g^n) = 0 (i = 1, 2, 3, \cdots)$ for each $w \in W$, return TRUE, otherwise return FALSE.
TURE. Else go to Step (c) for another \( g \). If there is no such an element \( g \), return FALSE.

**Summary**

In order to compute the tame kernel of number fields, a new method was presented in this paper, which has been translated into an algorithm in order to prove \( \partial_v \) to be an isomorphism.

**References**

