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 ∂_{v_m} to be an isomorphism was presented. Based on the method, an algorithm was presented to prove ∂_{v_m} 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 $Q\left(\sqrt{-19}\right)$ and $Q\left(\sqrt{-20}\right)$. J.Browkin [3] improved estimates of Skalba, and applied these estimates in the case $Q\left(\sqrt{-23}\right)$.

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 $v_1, v_2, \cdots, v_n, \cdots$ (1) be all finite places of F ordered in such a way that $Nv_{m-1} \le Nv_m$ for $m = 2,3,\cdots$, where Nv_m is the norm of v_m.

For $m \ge 1$ let $S_m = \{v_1, v_2, \cdots, v_m\}$. 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 v_m is denoted by k_{v_m}.

Let $K_2^{S_m}(F)$ be the subgroup of K_2F generated by symbols $\{a,b\}$, where $a,b \in U_{S_m}$. Then $K_2F = \bigcup_{m=1}^{\infty} K_2^{S_m}(F)$.

Let $\partial_{v_m} : K_2F \to k_{v_m}^*$ be the tame symbol corresponding to v_m and

$$\partial = \oplus_{m=1}^{\infty} \partial_{v_m} : K_2F \to \oplus_{m=1}^{\infty} k_{v_m}^* . \qquad (2)$$

Since $\partial_{v_m}(K_2^{S_{m-1}}(F)) = 0$, there is an induced map (also denoted by ∂_{v_m})

$$\partial_{v_m} : K_2^{S_m}(F) / K_2^{S_{m-1}}(F) \to k_{v_m}^* . \qquad (3)$$

If the prime ideal of $O_{S_{m-1}}$ corresponding to v_m is principal generated by π_m, i.e., $v_m O_{S_{m-1}} = \{x \in O_{S_{m-1}} \mid v_m(x) \ge 1\} = \pi_m O_{S_{m-1}}$, we get the following commutative diagram

Table 1. commutative diagram

$$\begin{tikzcd} & U_{S_{m-1}} \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ K_2^{S_m}(F)/K_2^{S_{m-1}}(F) \arrow[rr, "\partial_{v_m}"] & & k_{v_m}^* \end{tikzcd}$$

where $\alpha(u) = \{u, \pi_m\} (\operatorname{mod} K_2^{S_{m-1}}(F))$ and $\beta(u) = u(\operatorname{mod} \pi_m)$ for $u \in U_{S_{m-1}}$. We know that if ∂_{v_m} is an isomorphism for every $m > N$, where N is a positive integer, then $K_2 O_F \subseteq K_2^{S_N}(F)$. Since the group $K_2^{S_N}(F)$ 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 $\mathfrak{p}$ of O_F is earlier than ν_m if the valuation corresponding to $\mathfrak{p}$ appears before ν_m in the sequence (1).

Let Q_F be a set of representatives $\mathfrak{q}$ of all ideal classes satisfying that $\mathfrak{q} \subseteq O_F$, and for each integral ideal $\mathfrak{a}$, if $\mathfrak{a}$ is in the same ideal class with $\mathfrak{q}$, then $N\mathfrak{q} \le N\mathfrak{a}$.

Lemma 1 [3]. If $W = \{1 \ne w \in O_F \mid (w) = \mathfrak{pq}$ or $\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, where $\mathfrak{p}$ is earlier than ν_m and $\mathfrak{q}, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3 \in Q_F\} \bigcup U$, then $U_{S_{m-1}}$ is generated by W.

Lemma 2. Suppose that the prime ideal of $O_{S_{m-1}}$ corresponding to ν_m is principal generated by π_m. If $a,b \in U \bigcap O_F$, $\nu_m(a-b)=1$ and $\nu_{m+i}(a-b)=0(i=1,2,3,\cdots)$, then $a \in bU_1$.

Proof. If $a,b \in U \bigcap O_F$, $\nu_m(a-b)=1$ and $\nu_{m+i}(a-b)=0(i=1,2,3,\cdots)$, there is an element $u \in U_{S_{m-1}}$ 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 ∂_{ν_m} being bijective.

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

(1) $g^{N\nu_m - 1} \in U_1$;

(2) $U_{S_{m-1}}$ is generated by gU_1.

then ∂_{ν_m} is an isomorphism.

Proof. Let $\langle gU_1 \rangle$ is a subgroup of $U_{S_{m-1}}/U_1$, which is generated by gU_1. Form (2) it follows that $\langle gU_1 \rangle = U_{S_{m-1}}/U_1$, and hence we get $|\langle gU_1 \rangle| \ge N\nu_m - 1$, where $|\langle gU_1 \rangle|$ is the order of $\langle gU_1 \rangle$. By (1) above, we have $|\langle gU_1 \rangle| \le N\nu_m - 1$, so $|U_{S_{m-1}}/U_1| = |\langle gU_1 \rangle| = N\nu_m - 1$. Since β is surjective and $U_1 \subseteq \ker(\alpha) \subseteq \ker(\beta)$, we get $|U_{S_{m-1}}/\ker(\beta)| = N\nu_m - 1$ and $\ker(\beta) = U_1$. Therefore ∂_{ν_m} is an isomorphism.

Applications

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

Algorithm. Input: the prime ideal $\mathfrak{p}$ corresponding to ν_m.

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

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

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

(c) If there is not an element $g \in g^{'}(\mathrm{mod}\,\nu_m)$ such that $g \in U_{S_{m-1}}$, return FALSE. Else compute an element $g \in g^{'}(\mathrm{mod}\,\nu_m) \bigcap U_{S_{m-1}}$ such that $g^{N\nu_m - 1} \in U_1$ using GP/PARI. If there is no such an element g, return FALSE. Else go to Step (d).

(d) Compute an integer n $(1 \le n \le N\nu_m - 1)$ such that $w \in g^n(\mathrm{mod}\,\nu_m)$, where $w \in W$. If $w - g^n$ satisfies $\nu_m(w-g^n)=1$ and $\nu_{m+i}(w-g^n)=0$ ($i=1,2,3,\cdots$) for each $w \in W$, return

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 ∂_{v_m} to be an isomorphism.

References

[1] J. Tate: Appendix to "*The Milnor ring of a global field" by H. Bass and J. Tate, Algebraic K-theory*, Lecture Notes in Math, 342, Berlin-Heidelberg-New York, Springer (1973), p. 429-446

[2] M. Skabla: *Generalization of Thue's theorem and computation of the group* K_2O_F, J. of Number Theory, 46 (1994), p. 303-322

[3] J. Browkin: *Computing the tame kernel of quadratic imaginary field*, Math. of Computation, Vol. 69, No. 232 (2000), p. 1667-1683