42. On Hasse's Argorithm to Calculate Fundamental Units of Real Cyclic Biquadratic Fields*)

By Ken-ichi YOSHINO

Department of Mathematics, Kanazawa Medical University

(Communicated by Shokichi IYANAGA, M. J. A., June 7, 1994)

1. Introduction. Let K be a real cyclic biquadratic field with conductor F and k the quadratic subfield of K with conductor f. Let E_K and E_k be the groups of units of K and k, respectively. Hasse [1] defined the unit index of K as $Q_K = [E_K : HE_k]$, where H is the group of relative units of K, i.e., $H = \{\eta \in E_K ; N_{K/k}(\eta) = \pm 1\}$. Then $Q_K = 1$ or 2. Let E be the relative fundamental unit of K, i.e., H is generated by ± 1, E and the conjugate of E and let ε be the fundamental unit of k. For a number A of K, A is uniquely written in the form $A = \frac{1}{2}\left(u + \frac{v\tau(\chi) + \overline{v\tau(\chi)}}{2}\right) = [u, v]$, where u, v are elements of k, $\boldsymbol{Q}(\sqrt{-1})$, respectively and $\tau(\chi)$ is the Gauss sum of a generator χ of the character group of K (cf. [1] §8). We call u and v the coordinates of A. If A is an integer of K, then u and v are integers of k and $\boldsymbol{Q}(\sqrt{-1})$, respectively. Let s be a generator of the Galois group of K over $\boldsymbol{Q}$. Let $A' = A^s$, $A'' = A^{s^2}$, $A''' = A^{s^3}$ be the conjugates of A. Let $a + bi$ be the basis number of K ("Basiszahl" von K in [1] p. 30).

If $Q_K = 2$, then there exists the unique positive unit E^* of K such that $E_K = \langle -1, E^*, E^{*\prime}, E^{*\prime\prime} \rangle$ and

(1) $$E^*E^{*\prime} = \pm E, \qquad N_{K/k}(E^*) = \pm \varepsilon.$$

E^* is called the fundamental unit of K. By using (1) Hasse described a method of calculating the coordinates of E^* from ε and E ([1], §12 B). We put $E = [(x_0 + x_1\sqrt{f})/2,\ y_0 + y_1 i]$ and $E^* = [(x_0^* + x_1^*\sqrt{f})/2,\ y_0^* + y_1^* i]$. Hasse's method is summarized as follows: To get the non-equivalent solutions (x_0^*, x_1^*), we examine the principal ideals (α) of k such that $N((\alpha)) = |x_0|$. And, to get the non-equivalent solutions (y_0^*, y_1^*), we examine the ideals $\boldsymbol{a}$ of k such that $N(\boldsymbol{a}) = |x_1|/G$ and $\boldsymbol{a} \in C_{\hat{\varphi}}^{-1}$, where $G = F/f$ and $C_{\hat{\varphi}}$ is the ideal class of k which is corresponding to the primitive quadratic form $\hat{\varphi}(y^*) = b(y_0^{*2} - y_1^{*2})/2 + ay_0^*y_1^*$ with determinant f. We note that if $Q_K = 2$ then G divides x_1. In this way we obtain a finite number of candidates $(x_0^*, x_1^*, y_0^*, y_1^*)$ for E^*. Among them there are solutions of (1). However, if we use Hasse's method to calculate the coordinates of E^* from ε and E, then the calculation is complicated in general, because the number of candidates for E^* is large.

In this note we shall modify Hasse's method and give a simple algorithm. That is, our method is based upon the following fact: $Q_K = 2$ if and only if

*) Partially supported by Grant-in-Aid for Scientific Research (No. 05640073), Ministry of Education, Science and Culture, Japan.