A note on class numbers of the simplest cubic fields

Dongho Byeon*

Department of Mathematics, Pohang University of Science and Technology
San 31 Hyoja Dong, Pohang, 790–784, KOREA

In this note, we extend the Uchida-Washington construction ([3] [4]) of the simplest cubic fields with class numbers divisible by a given rational integer, to the wildly ramified case, which was previously excluded.

The simplest cubic field is the field defined by the irreducible polynomial over the rational number field $\mathbb{Q}$ of the following form

$$f(x) = x^3 + mx^2 - (m+3)x + 1,$$

where m is a rational integer. Under the assumption that $3 \nmid m$, Uchida [3] and Washington [4] have constructed simplest cubic fields with class numbers divisible by n, where n is any given rational integer. In this note, we show that Uchida-Washington method also works in the case $3|m$.

Let m be a rational integer such that $m \equiv 3, 21 \bmod 27$, $m > 3$ and K be the cubic field defined by the polynomial

$$f(x) = x^3 + mx^2 - (m+3)x + 1.$$

*This research is supported by the Basic Science Research Institute Program, Ministry of Education (BSRI - 95 - 1431).

The discriminant of $f(x)$ is $(m^2+3m+9)^2$. We can write $m^2+3m+9 = 27bc^3$, where $3 \not| bc$ and b is cube free. It is easily seen that the prime factors of the discriminant of K are those of b and 3 (See [4]).

Lemma. *Let* $b = p_1^{a_1} \cdots p_t^{a_t}$, $a_i \in \{1, 2\}$. *Then* $t > 1$.

Proof: Suppose that $t = 0$ so that $m^2 + 3m + 9 = 27c^3$. We have

$$(m + 6)^3 - (m - 3)^3 = (9c)^3,$$

which is impossible for $m > 3$. □

Let ρ, ρ', ρ'' be the zeros of $f(x)$, E the full group of units of K, and E' the subgroup of E generated by ρ, ρ', ρ'', as in [4]. First we have

Proposition 1. *The prime ideal divisor of* 3 *in* K *cannot be a principal ideal.*

Proof: Let $\mathbf{p}$, $\mathbf{p_i}$ denote the prime divisor of 3 and p_i in the Lemma respectively. From Hasse's Klassenkörperbericht, Ia, §13 [1], we have:

> Every ambiguous class contains an ambiguous ideal and the number of ambiguous classes of K is 3^t

Put $\theta = (\rho - \rho')/(3c)$. Then

$$(\theta) = \mathbf{p_1}^{a_1} \cdots \mathbf{p_t}^{a_t}.$$

Since the classes of the ambiguous ideals $\mathbf{p}$, $\mathbf{p_1} \cdots$, $\mathbf{p_t}$ generate a group of order 3^t, there is a unique relation between them. Therefore, $\mathbf{p}$ cannot be a principal ideal.

The proof of the fact quoted from Hasse's book is somewhat intricate, so it is of interest to give a direct proof. Suppose first that the unit index $[E : E']$ is divisible by 3. Then one of the units ρ, $\rho - 1$, $\rho(\rho - 1)$, $\rho^2(\rho - 1)$ is a cube. Consider, for example, the possibility $\rho(\rho - 1) = \xi^3$. Write $\mathrm{Irr}(\xi, \mathbb{Q}) = x^3 - sx^2 + tx - n$. An easy computation gives

$$\mathrm{I}rr(\xi^3, \mathbb{Q}) = x^3 - (s^3 - 3st + 3n)x^2 + (t^3 - 3stn + 3n^2)x - n^3.$$

In the present case,

$$Irr(\rho(\rho-1),\mathbb{Q}) = x^3 - (m^2+3m+6)x^2 + 3x + 1.$$

Comparing coefficients, we obtain $n = -1$ and

$$m^2+3m+6 = s^3 - 3st - 3, \quad 3 = t^3 + 3st + 3.$$

As in the Lemma, it is easy to see that this pair of diophantine equations does not have solutions for $m > 3$. The other cases are dealt with similarly. Thus we have $3 \not| [E : E']$.

Suppose now that $\mathbf{p}$ is a principal ideal. Then

$$3\rho^a(\rho')^b = \xi^3.$$

Taking cojugates, manipulating slightly and changing notations, we are led to equations

$$3^\nu \rho(\rho-1) = \zeta^3, \text{ where } \nu \in \{1,2\},$$

which are shown to be impossible by a similar argument. Thus we have the desired result. □

Now we have

Proposition 2. *Let a and n be positive integers with $a > 1$ and $(a,6) = 1$. Let m be an integer such that $m \equiv 3, 21 \bmod 27$, $m > 3$ and $2m+3 = 9a^n$. Let K be the cubic field defined by the polynomial $f(x) = x^3+mx^2-(m+3)x+1$ and $\beta = (-1-\rho)^3/9$, where ρ is a zero of the polynomial $f(x)$. Then we have*

(i) (β) is the $3n$-th power of an ideal of K.

(ii) (β) is not a third power of a principal ideal of K.

(iii) If $2|n$ and there is a prime factor p of a such that at least one of the numbers 2,3 is a quadratic nonresidue mod ρ, then (β) is not a square of a principal ideal of K.

(iv) Let l be a prime factor of n and $l > 3$. If there are prime factors p, q of a such that 2 is an l-th power nonresidue mod p, 3 is an l-th power residue mod p, 3 is an l-th power nonresidue mod q, then β is not an l-th power of a principal ideal of K.

In particular, a has prime factors as in (iii)(iv) for each prime l dividing n, then the class number of K is a multiple of $3n$.

Proof: (i) We modify the equation in [4, Proposition 2] into $9a^n = f(x)$ and take $x = -1$. Then Washington's proof works, and we get:

> Let $\mathbf{p}$ be a prime ideal of K and $\mathbf{p} \not| 3$. If $\mathbf{p}^\mu$ is the exact power of $\mathbf{p}$ dividing $-1-\rho$ then μ is divisible by n.

Thus we easily see that $(\beta) = (-1-\rho)^3/9$ is a $3n$-th power of an ideal of K.

(ii) Suppose that (β) is the third power of a principal ideal. Then the same is true for (3), i.e., $(3) = \mathbf{p}^3$, where the prime ideal $\mathbf{p}$ is principal. But this is impossible from Proposition 1.

(iii)(iv) We get these immediately by a slight modification of Washington's method.

Suppose that a has prime factors as in (iii)(iv) for the prime factors l of $3n$. If the order of (β) is smaller than $3n$, then for a prime factor l of $3n$, (β) is the l-th power of a principal ideal of K. But this contradicts the above (ii)(iii)(iv). Thus we have completed the proof. □

Remark. In [2], Orvay discussed the family of cubic fields $K = \mathbb{Q}(\theta)$, where $\mathrm{Irr}(\theta, \mathbb{Q}) = x^3 - px + pq$, $p = (9 + 27q^2)/4$, q¿2,3 $\not| q$, and $p/9$ is squarefree. Put $1/\mu = (1-3q)/2 + \theta$. Then

$$\mathrm{I}rr(1/\mu, \mathbb{Q}) = x^3 + mx^2 - (m+3)x + 1,$$

where $m = (9q-3)/2$. Therefore, the family investigated by Orvay, in fact, is the subfamily of simplest cubic fields discussed in this note, where $m \equiv 3, 21 \bmod 27$, $m > 12$, and $(m^2+3m+9)/27$ is squarefree. mposing some conditions on q, Orvay has constructed ubic fields with even class numbers. So this note is also an extension of Orvay's work.

Acknowledgement. The author deeply thanks the refree for many helpful suggestions that improved the paper greatly. The author also thanks Prof. H. K. Kim for reading the manuscript carefully.

References

[1] H. Hasse, Bericht über neuere untersuchungen und probleme aus der theorie der algebraischen zahlkörper, Physica-Verlarg Würzburg-Wien 1970.

[2] F. C. Orvay, "Fundamental units in a family of cyclic cubic fields," Communications in Algebra, **21**, No. 11 (1993), 3953–3962.

[3] K. Uchida, "Class numbers of cubic cyclic fields," J. Math. Soc. Japan **26**, No. 3 (1974), 447–453.

[4] L. C. Washington, "Class numbers of the simplest cubic fields," Math. Computation. **48**, No. 177 (1987), 371–384.