Commun. Korean Math. Soc. **19** (2004), No. 1, pp. 23–27

NORMS AND UNITS ON THE BASIC $\mathbb{Z}_3$-EXTENSION OF CERTAIN CUBIC FIELDS

JANGHEON OH

ABSTRACT. In this paper we explicitly compute the orders of ambiguous ideal class groups of layers of the basic $\mathbb{Z}_3$-extension of certain cubic fields and give an example for Greenberg's conjecture.

1. Introduction

Let k be a number field, p a prime number. Let $k = k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset k_\infty$ be a $\mathbb{Z}_p$-extension of k with Galois groups $Gal(k_n/k) \simeq \mathbb{Z}/p^n\mathbb{Z}$ and A_n the p-Sylow subgroup of the ideal class group of k_n. Then, by Iwasawa, there exists integers $\mu_p(k)$, $\lambda_p(k)$ and $\nu_p(k)$ such that $|A_n| = p^{\lambda_p(k)n+\mu_p(k)p^n+\nu_p(k)}$ for sufficiently large n. Greenberg's conjecture [3] claims that both $\mu_p(k), \lambda_p(k)$ vanishes for the cyclotomic $\mathbb{Z}_p$-extension, contained in the field obtained by adjoining all p-power roots of unity to k, of any totally real number field k. In this paper we explicitly compute the orders of ambiguous ideal class groups of layers of the basic $\mathbb{Z}_3$-extension of certain cubic fields and give an example for Greenberg's conjecture.

2. Examples

Throughout this paper from now on a $\mathbb{Z}_p$-extension is the cyclotomic $\mathbb{Z}_p$-extension. Let L be a totally real number field and k a real cyclic extension of degree p over L, which satisfies $k \cap L_\infty = L$. Let

$$S_{k_\infty/L_\infty} = \{w : \text{prime ideal of } k_\infty \mid w \text{is prime to} p \text{and ramified in} k_\infty/L_\infty\}.$$

Received May 2, 2003.
2000 Mathematics Subject Classification: 11R23.
Key words and phrases: Greenberg's conjecture, class number, cyclotomic units.
This work was supported by Korea Research Foundation Grant (KRF-2002-003-C00004).

THEOREM 1. [2, Theorem 3.5] *Let L be a totally real number field of finite degree and k a real cyclic extension of degree p over L. Assume that L_∞ has only one prime ideal lying over p and that the class number of L is not divisible by p. Then, the following are equivalent:*

(1) $\mu_p(k) = \lambda_p(k) = 0$.

(2) *For any prime ideal $w \in S_{k_\infty/L_\infty}$, the order of ideal class of w is prime to p.*

Let K be a cyclic extension of a number field F. Let $G = Gal(K/F)$. For each valuation v of F we let $e(v)$ be the ramification index of v in K/F. We put $e(K/F) = \prod_v e(v)$. We let E_K denote the group of units, $h(F)$ the class number of F, C_K the group of ideal classes, C_K^G the set of ambiguous ideal class groups, and $C_K'^G$ the set of ideal class groups containing an ambiguous ideal of K, respectively. We will use the following "genus formula" and the cyclotomic units:

THEOREM 2. [4, Lemma 4.1] *Let K/F be a cyclic extension with Galois group G. Then*

$$|C_K^G| = \frac{h(F)e(K/F)}{[K:F][E_F : N_{K/F}K^* \cap E_F]}, \quad |C_K'^G| = \frac{h(F)e(K/F)}{[K:F][E_F : N_{K/F}E_K]}.$$

THEOREM 3. [5, Lemma 8.1] *Let p be a prime and $m \geq 1$.*

(a) *The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$ are generated by -1 and the units $\zeta_{p^m}^{(1-a)/2}\frac{1-\zeta_{p^m}^a}{1-\zeta_{p^m}}, 1 < a < \frac{1}{2}p^m, (a,p) = 1$.*

(b) *The cyclotomic units $C_{p^m}^+$ of $\mathbb{Q}(\zeta_{p^m})^+$ are of finite index in the full unit group $E_{p^m}^+$, and $h_{p^m}^+ = [E_{p^m}^+ : C_{p^m}^+]$ where $h_{p^m}^+$ is the class number of $\mathbb{Q}(\zeta_{p^m})^+$.*

REMARK 1. Note that p does not divide $h_{p^m}^+$ for all $m \geq 1$.

From now on $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$. Note that the m-th layer $\mathbb{Q}_m$ is equal to the maximal real subfield $\mathbb{Q}(\zeta_{3^{m+1}})^+$ of $\mathbb{Q}(\zeta_{3^{m+1}})$. Let

$$p \equiv 1 \mod 3^{\ell+1}, \not\equiv 1 \mod 3^{\ell+2}, \ell \geq 1 \tag{1}$$

be a prime number. Denote θ be a solution of a polynomial $f(x) = x^3 - 3px - pu$, where $p = \frac{u^2+3v^2}{4}$ and u, v are integers such that $3 \mid v$. Then the number field $k^{p,\ell} = \mathbb{Q}(\theta)$ is cyclic over $\mathbb{Q}$, and only p is ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$(see [1, Theorem 6.4.11]). Note that p splits completely in

$\mathbb{Q}_\ell = \mathbb{Q}(\zeta_{3^{\ell+1}} + \zeta_{3^{\ell+1}}^{-1})$. Let $\mathfrak{p}_i$, $\mathfrak{q}_i$ with $i = 1, \cdots, 3^\ell$ prime ideals of $\mathbb{Q}_\ell$, $k_\ell^{p,\ell}$ above p, respectively. Then

$$S_{k_\infty/\mathbb{Q}_\infty} = \{\mathfrak{q}_i | i = 1, \cdots, 3^\ell\}.$$

If we could show that every $\mathfrak{q}_i$ is a principal ideal, then the Greenberg's conjecture for the number field $k^{p,\ell}$ is to be proved by Theorem 1. Let A_ℓ be the 3-part of the ideal class group of the ℓth layer of $k^{p,\ell}$. If the order $|A_\ell^{Gal(k_\ell^{p,\ell}/\mathbb{Q}_\ell)}|$ is 1, then $\mathfrak{q}_i$'s are principal ideals since the class of $\mathfrak{q}_i$ in A_ℓ is actually in $A_\ell^{Gal(k_\ell^{p,\ell}/\mathbb{Q}_\ell)}$.

THEOREM 4. *Let δ be a unit in $\mathbb{Q}_\ell$. Then δ is a norm from $k_\ell^{p,\ell}$ if and only if δ is a cubic in the finite field $\mathbb{Z}[\zeta_{3^{\ell+1}} + \zeta_{3^{\ell+1}}^{-1}]/\mathfrak{p}_i$ for all i.*

PROOF. Suppose that there is an element $\alpha \in k_\ell^{p,\ell}$ such that

$$N_{k_\ell^{p,\ell}/\mathbb{Q}_\ell}(\alpha) = \delta.$$

Then $N_{k_\ell^{p,\ell}/\mathbb{Q}_\ell}(x + y\theta + z\theta^2) = \delta$ for some $x, y, z \in \mathbb{Q}_\ell$. Clearing denominators, we have $N_{k_\ell^{p,\ell}/\mathbb{Q}_\ell}(a + b\theta + c\theta^2) = t^3\delta$ for some integer t and $a, b, c \in \mathbb{Z}[\zeta_{3^{\ell+1}} + \zeta_{3^{\ell+1}}^{-1}]$. Direct computation shows that the norm $N_{k_\ell^{p,\ell}/\mathbb{Q}_\ell}(a + b\theta + c\theta^2)$ equals to

$$\begin{aligned} &a^3 + 6 \cdot pca^2 + (-3 \cdot pb^2 - u \cdot pbc + 9 \cdot p^2c^2)a \\ &+ pu(b^3 - 3 \cdot pbc^2 + u \cdot pc^3). \end{aligned}$$

Suppose p divides m. Hence we see that p divides a. Now then the first three terms of the above is divisible by p^2, which, in turn, implies that p divides b. So we see that the first three terms are actually divisible by p^3, which implies that $b^3 - 3 \cdot pbc^2 + u \cdot pc^3$ is divisible by p^2. So p also divides c. Hence we may assume that t is relatively prime to p. Reducing the above equation by mod p, we have $a^3 \equiv t^3\delta \bmod p$. Conversely, assume that δ is a cubic in the finite field $\mathbb{Z}[\zeta_{3^{\ell+1}} + \zeta_{3^{\ell+1}}^{-1}]/\mathfrak{p}_i$. Then, by Hensel's Lemma, we see that δ is a local norm from $k_{\ell\ \mathfrak{p}_i}^{p,\ell}$. Since $k_\ell^{p,\ell}/\mathbb{Q}_\ell$ is unramified outside above p, δ is a local norm everywhere. Hence δ is a global norm. □

EXAMPLE 1. Let $p = 19$ and $\gamma = \zeta_9 + \zeta_9^{-1}$. Then γ satisfies the equation $x^3 - 3x + 1 = 0$. Note that $x^3 - 3x + 1 \equiv (x + 16)(x + 10)(x + 12) \bmod 19$. Let $\mathfrak{p}_1 = (x + 16, 19), \mathfrak{p}_2 = (x + 10, 19), \mathfrak{p}_3 = (x + 12, 19)$ be the prime ideals of $\mathbb{Q}_1$ above 19, and

$$\epsilon_1 = (\zeta_9^{1/2} + \zeta_9^{-1/2})(\zeta_9 + \zeta_9^{-1}), \epsilon_2 = \zeta_9^{1/2} + \zeta_9^{-1/2}, \epsilon_3 = \epsilon_1\epsilon_2, \epsilon_4 = \epsilon_1\epsilon_2^2,$$

$$\epsilon_5 = \epsilon_1^2, \quad \epsilon_6 = \epsilon_2^2, \quad \epsilon_7 = \epsilon_1^2\epsilon_2, \quad \epsilon_8 = \epsilon_1^2\epsilon_2^2$$

be the cyclotomic units of $\mathbb{Q}_1$. We have the following table by simple computation with Maple. So by Theorem 2, $|A_1^{Gal(k_1^{19,1}/\mathbb{Q}_1)}| = 1$. We see that the Greenberg's conjecture holds in this case by Theorem 1. In fact, the 3-part of the ideal class group of k is trivial and 3 is inert in $k/\mathbb{Q}$, hence by a theorem of Iwasawa, we see that the 3-part of the ideal class group of k_n is trivial for all $n \geq 0$.

Table 1. $p = 19$.

i	$\epsilon_i^{(19-1)/3} \bmod \mathfrak{p}_1$	$\epsilon_i^{(19-1)/3} \bmod \mathfrak{p}_2$	$\epsilon_i^{(19-1)/3} \bmod \mathfrak{p}_3$
1	1	11	7
2	11	1	7
3	11	11	11
4	7	11	1
5	7	7	7
6	7	1	11
7	11	7	1
8	7	7	7

EXAMPLE 2. Let $p = 307$ and $\gamma = \zeta_9 + \zeta_9^{-1}$. Note that $x^3 - 3x + 1 \equiv (x + 281)(x + 247)(x + 86) \bmod 307$. Let $\mathfrak{p}_1 = (x + 281, 307), \mathfrak{p}_2 = (x + 247, 307), \mathfrak{p}_3 = (x + 86, 307)$ be the prime ideals of $\mathbb{Q}_1$ above 307. The computation table as in Example 1 is as follows. So by Theorem 2, $|A_1^{Gal(k_1^{307,1}/\mathbb{Q}_1)}| = 3$. In this case we do not know whether the Greenberg's conjecture holds or not. Here we need information on the index $[E_{\mathbb{Q}_1} : N_{k_1^{307,1}/\mathbb{Q}_1} E_{k_1^{307,1}}]$ of which computation seems to be very hard.

Table 2. $p = 307$.

i	$\epsilon_i^{(307-1)/3} \bmod \mathfrak{p}_1$	$\epsilon_i^{(307-1)/3} \bmod \mathfrak{p}_2$	$\epsilon_i^{(307-1)/3} \bmod \mathfrak{p}_3$
1	17	17	17
2	289	289	289
3	1	1	1
4	289	289	289
5	289	289	289
6	17	17	17
7	17	17	17
8	1	1	1

EXAMPLE 3. Let $p = 2341$ and $\gamma = \zeta_9 + \zeta_9^{-1}$. Note that $x^3 - 3x + 1 \equiv (x + 737)(x + 1659)(x + 2286) \bmod 2341$. Let $\mathfrak{p}_1 = (x + 737, 2341), \mathfrak{p}_2 = (x + 1659, 2341), \mathfrak{p}_3 = (x + 2286, 2341)$ be the prime ideals of $\mathbb{Q}_1$ above 2341, In this example, we see that

$$\epsilon_i^{(2341-1)/3} \equiv 1 \bmod \mathfrak{p}_j,$$

for all $1 \leq i \leq 8, 1 \leq j \leq 3$. So by Theorem 2, $|A_1^{Gal(k_1^{2341,1}/\mathbb{Q}_1)}| = 3^2$.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1995.

[2] T. Fukuda, K. Komatsu, M. Ozaki and H. Taya, *On Iwasawa λ_p-Invariants of Relative Real Cyclic Extensions of Degree p*, Tokyo J. Math. **20** (1997), no. 2, 475–480.

[3] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284.

[4] S. Lang, *Cyclotomic Fields I and II*, Springer-Verlag, New York, 1990.

[5] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1996.

Department of Applied Mathematics
Sejong University
Seoul 143-747, Korea
E-mail: oh@sejong.ac.kr