Korean J. Math. **21** (2013), No. 3, pp. 265–270
http://dx.doi.org/10.11568/kjm.2013.21.3.265

CONSTRUCTION OF THE FIRST LAYER OF ANTI-CYCLOTOMIC EXTENSION

Jangheon Oh

Abstract. In this paper, using a theorem of Brink for prime decomposition of the anti-cyclotomic extension, we explicitly construct the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of imaginary quadratic fields.

1. Introduction

Let k be an imaginary quadratic field, and L an abelian extension of k. L is called an anti-cyclotomic extension of k if it is Galois over $\mathbb{Q}$, and $Gal(k/\mathbb{Q})$ acts on $Gal(L/k)$ by -1. For each prime number p, the compositum K of all $\mathbb{Z}_p$-extensions over k becomes a ${\mathbb{Z}_p}^2$-extension, and K is the compositum of the cyclotomic $\mathbb{Z}_p$-extension k_∞^c and the anti-cyclotomic $\mathbb{Z}_p$-extension k_∞^a of k. The layers k_n^c of the cyclotomic $\mathbb{Z}_p$-extension are well understood. Since the Hilbert class field of k is an anti-cyclotomic extension of k, determination of the first layer of the anti-cyclotomic $\mathbb{Z}_p$-extension becomes complicated as the p-rank of the p-Hilbert class field of k becomes larger. In the paper [5], using Kummer theory and class field theory, we constructed the first layer k_1^a of the anti-cyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field whose p-part of

Received May 22, 2013. Revised August 6, 2013. Accepted August 7, 2013.
2010 Mathematics Subject Classification: 11R23.
Key words and phrases: Hilbert class field, anti-cyclotomic extension, Kummer extension.
This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2010-0007244).

the ideal class group is trivial. In the paper [7], we applied the same method as in [5] to construct 3-Hilbert class fields of certain imaginary quadratic fields k which also become the first layers k_1^a of anti-cyclotomic $\mathbb{Z}_3$-extension of k. The first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension constructed in [7] is easily determined because the class number of k is 3. However, in the paper [8], we need a method which tells the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension from the rest of Hilbert class field of k because the 3-rank of the ideal class group in the example of [8] is 2. See Lemma 2 of this paper for the method we use in [8]. We briefly explain our method to compute η satisfying $k_1^a = k(\eta)$. Note that $k(\zeta_3)k_1^a = k(\zeta_3)(\sqrt[3]{\beta})$ for some $\beta \in k(\zeta_3)$ by Kummer theory. By Lemma 1, we see that β is a combination of the fundamental unit and generators of ideals of $\mathbb{Q}(\sqrt{3d})$, where $k = \mathbb{Q}(\sqrt{-d})$. Then, by Theorem 2, β can be determined. Hence, by Kummer theory again, we can determine η such that $k_1^a = k(\eta)$. In [8], we use Lemma 2 to determine β from the candidates constructed from Lemma 1. In this paper, Theorem 2(a theorem of Brink) plays the role of Lemma 2. This new method is more efficient and clear. Brink also used Theorem 2 to construct the first layer of the anti-cyclotomic $\mathbb{Z}_p$-extension of imaginary quadratic fields. However, his approach is different from ours in that he uses all possible polynomials satisfying discriminant conditions for candidates of the defining polynomial of the first layer, but we use Kummer theory for candidates of the first layer. To illustrate the method, we give an example at the end of this paper.

2. Proof of theorems

Let p be an odd prime number. Throughout this section, we denote by H_k, h_k, A_k, and M_k the p-part of Hilbert class field, the p-class number, p-part of ideal class group, and the maximal abelian p-extension of a number field k unramified outside above p, respectively. Let ζ_p be a primitive p-th root of unity. We denote $F = k(\zeta_p)$. The first layer of the anti-cyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field k may be or may not be contained in the p-Hilbert class field of k. The following Theorem gives an answer for this question when $p = 3$. We define $\mathrm{rank}_{\mathbb{Z}/p}A$ to be the dimension of A/A^p over $\mathbb{Z}/p\mathbb{Z}$ for any abelian group A.

THEOREM 1. *(= [6, Theorem 2]) Let $d \not\equiv 3 \bmod 9$ be a square-free positive integer, $k = \mathbb{Q}(\sqrt{-d})$ an imaginary quadratic field and k_∞^a the anti-cyclotomic $\mathbb{Z}_3$-extension over k. Assume that $A_{\mathbb{Q}(\sqrt{-d})}$ is 3-elementary. Then*

$$H_k \cap k_\infty^a = k \Longleftrightarrow$$
$$\mathrm{rank}_{\mathbb{Z}/3} A_{\mathbb{Q}(\sqrt{3d})} = \mathrm{rank}_{\mathbb{Z}/3} A_{\mathbb{Q}(\sqrt{-d})}.$$

REMARK 1. It is well-known that

$$\mathrm{rank}_{\mathbb{Z}/3} A_{\mathbb{Q}(\sqrt{3d})} \leq \mathrm{rank}_{\mathbb{Z}/3} A_{\mathbb{Q}(\sqrt{-d})} \leq \mathrm{rank}_{\mathbb{Z}/3} A_{\mathbb{Q}(\sqrt{3d})} + 1.$$

In the above theorem, we can replace 3 by any odd prime p if we substitute the $\chi\omega$-component $A_{F,\chi\omega}$ of A_F for $A_{\mathbb{Q}(\sqrt{3d})}$, where χ is the non-trivial character corresponding to the field $\mathbb{Q}(\sqrt{-d})$ and ω is the Teichmuller character for the prime p, without the condition that $d \not\equiv 3 \bmod 9$. However, Theorem 1 may not be true if $A_{\mathbb{Q}(\sqrt{-d})}$ is not 3-elementary. For example, if $h_k = 9$, $\mathrm{rank}_{\mathbb{Z}/3} A_k = 1$, and $H_k \cap k_\infty^a = k_1^a$, then Theorem 1 may not be true.

We need the following theorem to determine the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension from candidates constructed from Lemma 1 below.

THEOREM 2. *(= [1, Theorem 2])*
Assume that q is different from p and splits in k. We may then write

$$q^{h_k} = \begin{cases} a^2 + db^2 & \text{if } d \not\equiv 3 \bmod 4, \\ a^2 + ab + \frac{d+1}{4} b^2 & \text{if } d \equiv 3 \bmod 4 \end{cases}$$

with relatively prime $a, b \in \mathbb{Z}$. Put $\omega := \sqrt{-d}$ if $d \not\equiv 3 \bmod 4$, otherwise $\omega := \frac{1+\sqrt{-d}}{2}$. Let $n \geq 0$ be an integer and $\mathfrak{q}$ a prime ideal of k above q.
(a) Suppose p splits in k. Write $(a + b\omega)^{p-1} = a^* + b^*\omega$. Then $\mathfrak{q}$ splits completely in k_n^a iff $b^* \equiv 0 \bmod p^{n+1+\mu-\nu}$.
(b) Suppose p is inert in k. Write $(a + b\omega)^{p+1} = a^* + b^*\omega$. Then the conclusion of (a) holds.
(c) Suppose p is ramified in k and we are not in the exceptional case(see below). Then $\mathfrak{q}$ splits completely in k_n^a iff $b^* \equiv 0 \bmod p^{n+\mu-\nu}$.
(d) Suppose $p = 3$ and $d \equiv 3 \bmod 9$(the exceptional case). Write $(a + b\omega)^3 = a^* + b^*\omega$. Then $\mathfrak{q}$ splits completely in k_n^a iff $b^* \equiv 0 \bmod 3^{n+2+\mu-\nu}$.

In all cases, $\mathfrak{q}$ only splits in a finite number of steps of k^a. Here μ is the power of p of h_k and ν is the non-negative integer such that $k_\infty^a \cap H_k = k_\nu^a$.

Next we describe the $k(\zeta_3)k_1^a$ by Kummer Theory. The following Lemma is proved in [8]. We include the proof.

LEMMA 1. *(= [8, Lemma 2.3]) Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, and χ be the nontrivial character of $Gal(k/\mathbb{Q})$. Denote $F = k(\zeta_3)$. Then the compositum Fk_1^a of F and k_1^a is contained in $F(\sqrt[3]{\varepsilon}, \sqrt[3]{\alpha_1}, \cdots, \sqrt[3]{\alpha_t})$, where ε is the fundamental unit of $\mathbb{Q}(\sqrt{3d})$ and α_i satisfying $\mathfrak{p}^3 = (\alpha_i)$ for ideals $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{3d})$.*

Proof. Let $X_F := Gal(M_F/F)/3Gal(M_F/F)$ and $X_{F,\chi}$ be the χ-component of X_F for the nontrivial character χ of $Gal(k/\mathbb{Q})$. Let S be a subset of $F^\times/(F^\times)^3$ corresponding to X_F. Then, by Kummer theory, we have a perfect pairing $S_{\chi\omega} \times X_{F,\chi} \longrightarrow \mu_3$, where ω is the nontrivial character of $Gal(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$ and $S_{\chi\omega}$ is the $\chi\omega$-component of S. Note that $S \simeq E_F/{E_F}^3 \times A_F/{A_F}^3 \times <3>/<3>^3$, where E_F is the group of units of F and A_F is the 3-part of the ideal class group of F(See [4] for example). Therefore Lemma 1 follows since the $\chi\omega$-component $E_{F,\chi\omega}$ of the group of units E_F is the group of the units of the real quadratic subfield $F^+(= \mathbb{Q}(\sqrt{3d}))$ of F, and the $\chi\omega$-component $A_{F,\chi\omega}$ of A_F is the ideal class group of the real quadratic field $\mathbb{Q}(\sqrt{3d})$. □

The following statement is used in [3] to give an example with the Iwasawa invariants $\mu = \lambda = 0$ without proof. See [8] for the proof. We use Theorem 2 of this paper instead of the following Lemma used in [8] to tell k_1^a from the rest of Hilbert class field of k.

LEMMA 2. *Let p be an odd prime, $k = \mathbb{Q}(\sqrt{-d})$ an imaginary quadratic field such that $A_{\mathbb{Q}(\sqrt{-d})}$ is p-elementary, p is unramified in $k/\mathbb{Q}$, and $\zeta_3 \notin k$. Assume that $k_\infty^a \cap H_k = k_1^a$. Then the image of $Gal(X_{k,\chi}/k_\infty^a)$ in $Gal(H_k/k)$ corresponds to a subgroup B_k of the ideal class group A_k of k consisting of classes c with the following property: If $\mathfrak{a} \in c$, then $\mathfrak{a}^p = (\alpha)$, where α is an $\mathfrak{L}$-adic p-th power for every prime $\mathfrak{L}$ of k lying above p.*

Now, from Theorem 2 and Lemma 1, we can construct the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of imaginary quadratic fields.

THEOREM 3. *(See [8, Theorem 2.5.]) Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field such that $\zeta_3 \notin k$. Then one can explicitly construct*

the unique extension M_3 of F in $M_{F,\chi}$ such that $M_3 = F(\sqrt[3]{\beta})$, and $k_1^a = k(\eta)$, where $\beta \in S_{\chi\omega}$ and $\eta = Tr_{M_3/k_1^a}(\sqrt[3]{\beta})$.

Proof. Since the rank of $X_{F,\chi}$ is the same as that of A_k by Theorem 1 and Lemma 1, the extension field N_3 of degree 3 of F in $M_{F,\chi}$ is always equal to the compositum FL of F and an extension L of degree 3 of k in H_k. Moreover L is uniquely determined when N_3 is given because $Gal(FL/k)$ is a cyclic group of order 6. Let M_3 be the extension of F satisfying properties in Theorem 3, and $M_3 = FL$. Choose the set P of primes of $\mathbb{Q}$, which split completely in F. Then the primes of k above P and satisfying the condition of Theorem 2 split completely in L/k, when $L = k_1^a$. This completes the proof since a Galois extension of a number field is determined by the set of primes which split completely in the Galois extension. □

The following example is given in [8] using Lemma 2. Here we construct the same example using Theorem 2.

EXAMPLE 1. Let $k = \mathbb{Q}(\sqrt{-4027})$ be an imaginary quadratic field and $\mathfrak{p}_2$ a prime ideal of $\mathbb{Q}(\sqrt{12081})$ above 2. Then

$$k_1^a = k(\sqrt[3]{\varepsilon^2\alpha} - 2\sqrt[3]{\varepsilon^{-2}\alpha^{-1}}),$$

where ε is the fundamental unit of $\mathbb{Q}(\sqrt{12081})$ and $\mathfrak{p}_2^3 = (\alpha)$. Note that $h_{\mathbb{Q}(\sqrt{12081})} = 3, h_k = 9$, and $\mathrm{rank}_{\mathbb{Z}/3}A_k = 2$. We can take $\alpha = 81((-1 + \sqrt{12081})/2) + 4492$ and $\varepsilon = (17288113122 + 157288204\sqrt{12081})^2/12$. By Lemma 1 and Theorem 3, β is one of the following; $\varepsilon, \varepsilon\alpha, \varepsilon^2\alpha, \alpha$. Choose $q = 19$. Since $h_k = 9$, $\mu = 2$. We see that two relatively prime integers $a = 208373, b = 16550$ satisfy the equation $a^2 + ab + \frac{d+1}{4}b^2 = 19^9$. Since $p = 3$ is inert in k, we use (b) of Theorem 2. When we write $(a + b\omega)^4 = a^* + b^*\omega$, we see that

$$b^* = -3281686861138712769600$$

and $b^* \equiv 0 \mod 27 = 3^{1+1+2-1}$. Therefore, by (b) of Theorem 2, the prime $\mathfrak{q}$ of k above q splits completely in k_1^a. We can compute, by Maple,

$$irr(\sqrt[3]{\varepsilon^2\alpha}, \mathbb{Q}) \mod 19$$
$$= (x+2)(x+3)(x+8)(x+12)(x+14)(x+18).$$

However, we have $irr(\sqrt[3]{\varepsilon\alpha}, \mathbb{Q}) \bmod 19 = (x^3+9)(x^3+16), irr(\sqrt[3]{\varepsilon}, \mathbb{Q}) \bmod 19 = (x^3+9)(x^3+17)$, and $irr(\sqrt[3]{\alpha}, \mathbb{Q}) \bmod 19 = (x^3+13)(x^3+14)$. Hence $k_1^a(\zeta_3) = k(\zeta_3)(\sqrt[3]{\varepsilon^2\alpha})$. Moreover, since $\sigma \in Gal(M_3/k_1^a)$ satisfies $\sigma^2 = 1$,

we have $\sqrt[3]{\varepsilon^2\alpha}^{\sigma} = -2\sqrt[3]{\varepsilon^{-2}\alpha^{-1}}$ and therefore $\eta = Tr_{M_3/k_1^a}(\sqrt[3]{\beta}) = \sqrt[3]{\varepsilon^2\alpha} - 2\sqrt[3]{\varepsilon^{-2}\alpha^{-1}}$. Note that $b^* \not\equiv 0 \mod 3^4$, which implies that the primes of k above 19 split completely in the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of k, but the primes of k_1^a above 19 stay prime along the layers of the extension by (b) of Theorem 2.

References

[1] D.Brink, *Prime decomposition in the anti-cyclotomic extensions,* Mathematics of Computation, **76** (2007), no.260, 2127–2138.

[2] H.Cohen, *Advanced Topics in Computational Number Theory*, Springer (1999)

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

[4] J.Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D dissertation, University of Washington, 1986.

[5] J.Oh, *On the first layer of anti-cyclotomic $\mathbb{Z}_p$-extension over imaginary quadratic fields,* Proc. Japan Acad. Ser.A Math.Sci., **83** (2007), no.3, 19–20.

[6] J.Oh, *A note on the first layers of $\mathbb{Z}_p$-extensions,* Commun. Korean Math. Soc., **24** (2009), no.3, 1–4.

[7] J.Oh, *Construction of 3-Hilbert class field of certain imaginary quadratic fields,* Proc. Japan Aca. Ser.A Math. Sci., **86** (2010), no.1, 18–19 .

[8] J.Oh, *Anti-cyclotomic extension and Hilbert class field,* Journal of the Chungcheong Math. Society, **25** (2012), no.1, 91–95 .

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