Korean J. Math. **26** (2018), No. 2, pp. 293–297
https://doi.org/10.11568/kjm.2018.26.2.293

CONSTRUCTION OF THE HILBERT CLASS FIELD OF SOME IMAGINARY QUADRATIC FIELDS

Jangheon Oh

Abstract. In the paper [4], we constructed 3-part of the Hilbert class field of imaginary quadratic fields whose class number is divisible exactly by 3. In this paper, we extend the result for any odd prime p.

1. Introduction

When the order of the sylow 3-subgroup of the ideal class group of an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-d})$ and $\mathbb{Q}(\sqrt{3d})$ is 3 and 1 respectively, we [4] explicitly constructed 3-part of the Hilbert class field of k. We briefly explain the construction. First, using Kummer theory, we construct everywhere unramified extension $H_z = k_z(\alpha)$ over $k_z = k(\zeta_3)$ such that the degree $[H_z : k_z]$ is 3. The Galois group of H_z/k is $\mathbb{Z}_6$ and the unique subfield M of H_z, whose degree over k is 3, is the desired 3-part of Hilbert class field of k. Moreover, M is $k(\beta)$, where $\beta = Tr_{H_z/M}(\alpha)$ and α is a unit of $\mathbb{Q}(\sqrt{3d})$. The explicit computation of α is given in the paper [3].

In this paper, we extend the result for any odd prime p. The proof in this paper is similar to that in the case of $p = 3$. Throughout this paper, d is a square free positive integer and k an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ such that $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

Received March 08, 2018. Revised June 5, 2018. Accepted June 7, 2018.
2010 Mathematics Subject Classification: 11R23.
Key words and phrases: Iwasawa theory, Hilbert class field, Kummer extension.

2. Proof of Theorems

Denote $k(\zeta_p)$ by L. Then L is a CM field, and let L^+ be the maximum real subfield of L.

Proposition 1. *Let p be an odd prime. Then*

$$L^+ = \mathbb{Q}(\sqrt{d}\sin(\frac{2\pi}{p}) + \cos(\frac{2\pi}{p})).$$

Proof. Denote $\sqrt{-d}, \zeta_p - \zeta_p{}^{-1}, \zeta_p + \zeta_p{}^{-1}$ by α, β, γ respectively. Note that $\alpha\beta$ and γ are real numbers and

$$L = \mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha\beta, \gamma)(\alpha).$$

Hence $L^+ = \mathbb{Q}(\alpha\beta, \gamma) = \mathbb{Q}(\sqrt{d}\sin(\frac{2\pi}{p}), \cos(\frac{2\pi}{p}))$. Let σ be an element of $Gal(L/\mathbb{Q})$ such that $\sigma(\alpha) = -\alpha$ and $\sigma(\zeta_p) = \zeta_p$. Then $\sigma(\alpha\beta + \gamma) = -\alpha\beta + \gamma \in \mathbb{Q}(\alpha\beta + \gamma)$, which completes the proof. $\square$

Remark 1. Note that $L^+ = \mathbb{Q}(\sqrt{3d})$ when $p = 3$.

We denote by $M_K, A_K, E_K, \chi, \omega$ the maximal unramified elementary abelian p-extension of a number field K, the p-part of ideal class group of K, the set of units of K, the nontrivial character of $Gal(k/\mathbb{Q})$, and the Teichmuller character, respectively. By Kummer theory, there is a subgroup $B \subset L^\times/(L^\times)^p$ such that $M_L = L(\sqrt[p]{B})$ and a nondegenerate pairing

$$Gal(M_L/L) \times B \to \mu_p.$$

Since $Gal(M_L/L) \simeq A_L/A_L{}^p$, we have a map $\phi : B \to A_{L,p} := \{x \in A_L | x^p = 1\}$ and $Ker(\phi) \simeq$ subgroup of $E_L/E_L{}^p$. From this pairing, we have an induced nondegenerate pairing

$$Gal(M_L/L)_\chi \times B_{\chi\omega} \to \mu_p,$$

where we write $M = \bigoplus_\psi M_\psi$ for the character ψ's of $G = Gal(L/\mathbb{Q})$ and the $\mathbb{Z}_p[G]$-module M(See [5]).

The map ϕ is G-linear, so we have an induced map $\phi_{\chi\omega}$ from ϕ

$$\phi_{\chi\omega} : B_{\chi\omega} \to (A_{L,p})_{\chi\omega}.$$

Note that $(E_L/{E_L}^p)_{\chi\omega} = (E_{L^+}/{E_{L^+}}^p)_{\chi\omega}$ and the order of $(E_{L^+}/{E_{L^+}}^p)_{\chi\omega}$ is p(See [2]). Hence we have

$$\begin{aligned} p\text{-}rank(Gal(M_L/L)_\chi) &= p\text{-}rank(B_{\chi\omega}) \\ \le p\text{-}rank(ker(\phi_{\chi\omega})) &+ p\text{-}rank((A_L/{A_L}^p)_{\chi\omega}) \\ &\le 1 + p\text{-}rank((Gal(M_L/L)_{\chi\omega}) \end{aligned}$$

Since $[E_L : \mu_p E_{L^+}] = 1$ or 2 and $\chi(\neq \omega)$ is an odd character, the order of $(E_L/{E_L}^p)_\chi$ is 1. So similarly as above we have

$$\begin{aligned} p\text{-}rank(Gal(M_L/L)_{\chi\omega}) &= p\text{-}rank(B_\chi) \\ \le p\text{-}rank(ker(\phi_\chi)) &+ p\text{-}rank((A_L/{A_L}^p)_\chi) \\ &\le p\text{-}rank(Gal(M_L/L)_\chi) \end{aligned}$$

Since p and $p-1$ is relatively prime, we see that $Gal(M_L/L)_\chi \simeq Gal(M_k/k)_\chi \simeq A_k/{A_k}^p$. Therefore we proved the following theorem.

THEOREM 2.1. *We have the inequality.*

$$p\text{-}rank((A_L/{A_L}^p)_{\chi\omega}) \le p\text{-}rank(A_k/{A_k}^p) \le 1 + p\text{-}rank((A_L/{A_L}^p)_{\chi\omega}).$$

REMARK 2. Theorem 2.1 is already known for $p = 3$. The above proof just follows the proof for $p = 3$.

Let N_K be the maximal abelian p-extension of a number field K unramified outside above p, and X_K be $Gal(N_K/K)/Gal(N_K/K)^p$. Then, by Kummer theory again, we have a nondegenerate pairing

$$S_{\chi\omega} \times X_{L,\chi} \to \mu_p,$$

where S is a subset of $L^\times/L^{\times p}$ corresponding to X_L. It is seen [2] that

$$S \simeq E_L/{E_L}^p \times A_L/{A_L}^p \times < p > / < p >^p .$$

So $S_{\chi\omega} = (E_L/{E_L}^p)_{\chi\omega} \times (A_L/{A_L}^p)_{\chi\omega}$. Note again that the order of $(E_L/{E_L}^p)_{\chi\omega}$ is p. Hence, if the order of $(A_L/{A_L}^p)_{\chi\omega}$ is 1, then $(N_L)_\chi = L(\sqrt[p]{\epsilon})$, where $\epsilon \in (E_{L^+}/{E_{L^+}}^p)_{\chi\omega}$.

THEOREM 2.2. *Let p be a prime $p > 3$. Assume that the order of A_k is p and that of $(A_L/{A_L}^p)_{\chi\omega}$ is 1. Then M_k is the unique subfield of $L(\sqrt[p]{\epsilon})$ such that the degree $[M_k : k] = p$, where $\epsilon \in (E_{L^+}/{E_{L^+}}^p)_{\chi\omega}$. Moreover,*

$$M_k = k(Tr_{(N_L)_\chi/M_k}(\sqrt[p]{\epsilon}))$$

Proof. Since p and $p-1$ is relatively prime, we see that

$$(X_k)_\chi \simeq (X_L)_\chi.$$

The complex conjugate acts on the Hilbert class field of k inversely, so the condition in Theorem 2.2 implies that

$$M_k = (M_k)_\chi = (N_k)_\chi.$$

The galois group $Gal((M_L)_\chi/k)$ is an abelian group of order $p(p-1)$, so $(M_L)_\chi$ contains the unique subfield F whose degree over k is p. Hence $M_k = F$ and by Kummer theory(see for example [1]) we see that $F = k(Tr_{(N_L)_\chi/M_k}(\sqrt[p]{\epsilon}))$. □

REMARK 3. When the order of A_k is p, then that of $(A_L/{A_L}^p)_{\chi\omega}$ is 1or p by Theorem 2.1. We proved the above theorem for $p = 3$(See [4]). The construction of the unit ϵ in Theorem 2.2 is given in [3].

The compositum L_k of all $\mathbb{Z}_p$-extension of k is the $\mathbb{Z}_p^2$-extension of k. The L_k is the product of the cyclotomic $\mathbb{Z}_p$-extension and the anti-cyclotomic $\mathbb{Z}_p$-extension of k. The following theorem tells when the first layer k_1^a of the anti-cyclotomic $\mathbb{Z}_p$-extension is unramified everywhere over k.

THEOREM 2.3. *Let p be a prime $p(>3)$. The first layer k_1^a of the anti-cyclotomic $\mathbb{Z}_p$-extension is unramified everywhere over k if and only if*

$$p\text{-}rank(A_k/{A_k}^p) = 1 + p\text{-}rank((A_L/{A_L}^p)_{\chi\omega}).$$

Proof. By class field theory, $Gal(N_k/H_k) \simeq (\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}})/E \simeq \mathbb{Z}_p^2$, where H_k is the p-part of Hilbert class field of k, $U_{1,\mathfrak{p}}$ local units congruent to 1 modulo $\mathfrak{p}$, , and E the closure of global units of k in $\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$. And note that $(N_k)_\chi$ is the compositum of the anti-cylotomic $\mathbb{Z}_p$-extension of k and H_k. Assume that $p\text{-}rank(A_k/{A_k}^p) = 1 + p\text{-}rank((A_L/{A_L}^p)_{\chi\omega})$. Then since $(X_k)_\chi \simeq (X_L)_\chi$, we have

$$\begin{aligned} p\text{-}rank((X_k)_\chi) &= p\text{-}rank((X_L)_\chi = p\text{-}rank(S_{\chi\omega}) \\ &= p\text{-}rank((E_L^+/E_L^{+p})_{\chi\omega}) + p\text{-}rank((A_L/{A_L}^p)_{\chi\omega}) \\ &= 1 + p\text{-}rank((A_L/{A_L}^p)_{\chi\omega}) = p\text{-}rank(A_k/{A_k}^p). \end{aligned}$$

Hence the first layer k_1^a should be a part of H_k. Assume not that $p\text{-}rank(A_k/{A_k}^p) = 1 + p\text{-}rank((A_L/{A_L}^p)_{\chi\omega})$. Then, by Theorem 2.1, $p\text{-}rank(A_k/{A_k}^p) = p\text{-}rank((A_L/{A_L}^p)_{\chi\omega})$, and hence $p\text{-}rank((X_k)_\chi) = 1 + p\text{-}rank(A_k/{A_k}^p)$, so the first layer k_1^a should be ramified over k. □

References

[1] H.Cohen, *Advanced Topics in Computational Number Theory*, Springer, 1999.
[2] J.Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D dissertation, University of Washington, 1986.
[3] J.Oh, *On the first layer of anti-cyclotomic $\mathbb{Z}_p$-extension of imaginary quadratic fields*, Proc. of The Japan Acad. Ser.A **83** (2007) (3),19–20.
[4] J.Oh, *Construction of 3-Hilbert class field of certain imaginary quadratic fields*, Proc. of The Japan Acad. Ser.A **86** (2010) (1), 18–19.
[5] L.Washington, *Introduction to cyclotomic fields*, Springer, New York, 1982.

Jangheon Oh
Faculty of Mathematics and Statistics
Sejong University
Seoul 143-747, Korea
E-mail: oh@sejong.ac.kr