

A p -TH ROOT OF A MINKOWSKI UNIT

JANGHEON OH*

ABSTRACT. The purpose of this paper is to show that there exists a unit whose p -th root generates the first layer of anti-cyclotomic \mathbb{Z}_p -extension of certain imaginary quadratic number 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 and the anti-cyclotomic \mathbb{Z}_p -extension of k . In the paper[4], using Kummer theory and class field theory, we constructed for odd primes the first layer k_1^a of the anti-cyclotomic \mathbb{Z}_p -extension of an imaginary quadratic field whose class number is not divisible by p under the assumption that a unit ε constructed in the paper [4](see Theorem 1 of this paper) is not a p -power of a unit. In this paper, we will show that there always exists such a unit ε that is not a p -power of a unit.

2. Main Theorem

We begin this section by explaining how to construct a cyclic extension M_p of prime degree p of an imaginary quadratic field k , which is unramified outside p over k and $Gal(M_p/\mathbb{Q}) \simeq D_p$, the dihedral group of order $2p$. From now on, we let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ and let σ, τ with $\sigma(\zeta_p) = \zeta_p^t$ be generators of

Received May 10, 2010; Accepted August 12, 2010.

2010 Mathematics Subject Classification: Primary 11R23.

Key words and phrases: anti-cyclotomic extension, Minkowski unit, Kummer extension.

*This work was supported by the faculty research fund of Sejong University in 2009.

$Gal(k_z/k), Gal(k_z/\mathbb{Q}(\zeta_p))$, respectively, where ζ_p a primitive p -th root of unity and $k_z = k(\zeta_p)$. Then we have the following theorem which is the main theorem refinement of [4, Theorem 1].

THEOREM 2.1. (See [6, Theorem 1]) *Let X be a vector space over a finite field F_p with a basis $\{x_1, \dots, x_{p-1}\}$ and A be a linear map such that $Ax_i = x_{i+1}$ for $i = 1, \dots, p - 2$ and $Ax_{p-1} = x_1$. Let $x = \sum_i a_i x_i$ be an eigenvector of A corresponding to an eigenvalue t satisfying $\sigma(\zeta_p) = \zeta_p^t$. Let $k = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field such that $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Assume that $\varepsilon = \tau(\epsilon)\epsilon^{-1}$ is not a p -power of a unit in k_z , where $\epsilon = \prod_i (\alpha)^{a_i \sigma^{i-1}}$ for some unit $\alpha \in k_z$. Then $k_z(\sqrt[p]{\varepsilon})$ contains a unique cyclic extension M_p of prime degree p of k , which is unramified outside p over k and $Gal(M_p/\mathbb{Q}) \simeq D_p$, and $M_p = k(\eta)$ where $\eta = Tr_{k_z(\sqrt[p]{\varepsilon})/M_p}(\sqrt[p]{\varepsilon})$.*

Before proving our main theorem, we need a lemma.

LEMMA 2.2. (See [7, Lemma 5.27]) *Let K/\mathbb{Q} be a real finite Galois extension then let $\sigma_1, \dots, \sigma_{r+1}$ be the elements of $Gal(K/\mathbb{Q})$. There exists a unit α of K such that the set of units $\{\alpha^{\sigma_i} | 1 \leq i \leq r\}$ is multiplicatively independent, hence generates a subgroup of finite index in the full group of units E_K (such a unit is called a Minkowski unit).*

REMARK 2.1. By above lemma, we see that $E_K \odot \mathbb{Q} \simeq \mathbb{Q}[Gal(K/\mathbb{Q})] / (\sigma_1 + \dots + \sigma_{r+1})$, therefore $E_K/E_K^p \simeq \mathbb{F}_p[Gal(K/\mathbb{Q})] / (\sigma_1 + \dots + \sigma_{r+1})$ when $p \nmid [K : \mathbb{Q}]$.

Note that the characteristic polynomial of the map A in Theorem 1 is $x^{p-1} - 1$. Therefore the eigenvector for any nonzero t in F_p always exists. Now we will prove our main theorem that ε in Theorem 1 is not a p -power of a unit in k_z . Actually, it is enough to show that the unit ε is not a p -power of a unit in M^+ which is the maximal real subfield of k_z because of the well-known fact that $[E_{k_z} : WM^+] = 1$ or 2 . Here W is the group of roots of unity in k_z . Let notations be the same as in Theorem 1. By abuse of notation, let σ, τ denote by the extensions of σ, τ to k_z with $\sigma|_{\mathbb{Q}(\sqrt{-d})} = \text{identity}$ and $\tau|_{\mathbb{Q}(\zeta_p)} = \text{identity}$.

THEOREM 2.3. *Let $p > 3$ be a prime. Then the unit ε in Theorem 1 is not a p -power of a unit in k_z if α is a Minkowski unit in M^+ .*

Proof. First we prove the theorem in the case of $p \equiv 1$ modulo 4. The unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p})$. It follows that the maximal real subfield M^+ of k_z is

$$\mathbb{Q}(\zeta_p + \zeta_p^{-1}, \sqrt{-d}(\zeta_p - \zeta_p^{-1})).$$

Let $x = \sum_i a_i x_i$ be an eigenvector of A corresponding to an eigenvalue t satisfying $\sigma(\zeta_p) = \zeta_p^t$ and $t^{\frac{p-1}{2}} \equiv -1$ modulo p . Note that

$$\begin{aligned} \sigma^{\frac{p-1}{2}}(\zeta_p - \zeta_p^{-1}) &= \zeta_p^{t^{\frac{p-1}{2}}} - \zeta_p^{-t^{\frac{p-1}{2}}} = \zeta_p^{-1} - \zeta_p \\ \sigma^{\frac{p-1}{2}}(\sqrt{-d}) &= (\sqrt{-d}) \\ \tau(\zeta_p - \zeta_p^{-1}) &= (\zeta_p - \zeta_p^{-1}), \tau(\sqrt{-d}) = -(\sqrt{-d}). \end{aligned}$$

So $\sigma^{\frac{p-1}{2}}((\sqrt{-d})(\zeta_p - \zeta_p^{-1})) = -(\sqrt{-d})(\zeta_p - \zeta_p^{-1})$ and $\tau((\sqrt{-d})(\zeta_p - \zeta_p^{-1})) = -(\sqrt{-d})(\zeta_p - \zeta_p^{-1})$. Therefore $\sigma^{\frac{p-1}{2}}, \tau \notin H = Gal(k_z/M^+)$, which implies that $\sigma|_{M^+}$ is a generator of $Gal(M^+/\mathbb{Q})$ and $\tau|_{M^-} = (\sigma|_{M^-})^{\frac{p-1}{2}}$. Now we choose α as a Minkowski unit in M^+ . Then we have

$$\begin{aligned} \varepsilon &= \left(\prod_i \alpha^{a_i \sigma^{i-1}}\right)^{(\tau-1)} \\ &= \left(\prod_i \alpha^{a_i (\sigma|_{M^+})^{i-1}}\right)^{((\sigma|_{M^-})^{\frac{p-1}{2}} - 1)} \\ &= \left(\prod_i \alpha^{a_i (\sigma|_{M^+})^{i-1}}\right)^{(t^{\frac{p-1}{2}} - 1)} \\ &= \epsilon^{-2} u^p, \end{aligned}$$

where u is a unit in M^+ . This completes the proof by the Remark 1 above. Next we will prove the theorem in the case of $p \equiv 3$ modulo 4. Then the maximal real subfield M^+ of k_z is $\mathbb{Q}(\zeta_p + \zeta_p^{-1}, \sqrt{dp})$ since $\mathbb{Q}(\sqrt{-p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. It is clear that

$$\begin{aligned} \sigma^{\frac{p-1}{2}}(\sqrt{dp}) &= -\sqrt{dp}, \sigma^{\frac{p-1}{2}}(\zeta_p + \zeta_p^{-1}) = \zeta_p + \zeta_p^{-1} \\ \tau(\sqrt{dp}) &= -\sqrt{dp}, \tau(\zeta_p + \zeta_p^{-1}) = \zeta_p + \zeta_p^{-1}. \end{aligned}$$

Therefore the order of $\sigma|_{M^-}$ is $p-1$ and $\sigma|_{M^+}^{\frac{p-1}{2}} = \tau|_{M^-}$. Now we easily check as in the case of $p \equiv 1$ modulo 4 that $\varepsilon = \epsilon^{-2} u^p$, where u is a unit in M^+ , which implies that ε is not a p -power of a unit in k_z by Remark 1. \square

THEOREM 2.4. *Let p be an odd prime which is greater than 3, d a square free positive integer and $k = \mathbb{Q}(\sqrt{-d})$ an imaginary quadratic field such that $p \nmid h_k$. Then*

$$k_1^a = k(\eta)$$

where η is as in Theorem 1.

Proof. Let F be the maximal abelian p -extension of k unramified outside p . Then class field theory (see [7, Corollary 13.6]) shows that

$$\text{Gal}(F/k) \simeq \left(\prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}} \right),$$

where $U_{1,\mathfrak{p}}$ is the local units of k which is congruent to 1 mod \mathfrak{p} . Hence F , which is equal to the compositum K of all \mathbb{Z}_p -extension of k in this case, contains a unique D_p -extension k_1^a of \mathbb{Q} (cf.[4, Lemma2]). Therefore $M_p = k_1^a = k(\eta)$ since M_p and k_1^a are D_p -extensions of \mathbb{Q} contained in F . \square

REMARK 2.2. For $p = 2, 3$, the explicit construction of the first layer of the anti-cyclotomic \mathbb{Z}_p -extension of k is given in [2, 3]. For Kummer extension of a number field which does not contain roots of unity, see [1].

References

- [1] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer, 1999
- [2] J. M. Kim and J. Oh, *Defining Polynomial of the first layer of anti-cyclotomic \mathbb{Z}_3 -extension over imaginary quadratic fields of class number 1*, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 3, 18-19.
- [3] J. Oh, *The first layer of \mathbb{Z}_3^2 -extension over imaginary quadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), no. 9, 132-134.
- [4] 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.
- [5] J. Oh, *A note on the first layers of \mathbb{Z}_p -extensions*, Commun. Korean Math. Soc. **24** (2009), no.3, 1-4.
- [6] J. Oh, *Construction of 3-Hilbert class field of certain imaginary quadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), no. 1, 18-19.
- [7] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Math. **83** (1982), Springer-Verlag

*

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