On the first layer of anti-cyclotomic $\mathbf{Z}_p$-extension of imaginary quadratic fields

By Jangheon OH

Department of Applied Mathematics, College of Natural Sciences,
Sejong University, Seoul, 143-747, Korea

(Communicated by Heisuke HIRONAKA, M.J.A., March 12, 2007)

Abstract: In this paper, we give an explicit description of the first layer of anti-cyclotomic $\mathbf{Z}_p$-extension of imaginary quadratic fields.

Key words: Iwasawa theory; anti-cyclotomic extension; Kunner extension; Minkowski unit.

1. Introduction. For each prime number p, a $\mathbf{Z}_p$-extension of a number field k is an extension $k = k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset k_\infty$ with $Gal(k_\infty/k) \simeq \mathbf{Z}_p$, the additive group of p-adic integers. Let k be an imaginary quadratic field, and K an abelian extension of k. K is called an anti-cyclotomic extension of k if it is Galois over $\mathbf{Q}$, and $Gal(k/\mathbf{Q})$ acts on $Gal(K/k)$ by -1. By class field theory, the compositum M of all $\mathbf{Z}_p$-extensions over k becomes a ${\mathbf{Z}_p}^2$-extension, and M is the compositum of the cyclotomic $\mathbf{Z}_p$-extension and the anti-cyclotomic $\mathbf{Z}_p$-extension of k. For $p = 2, 3$, the explicit construction of the first layer k_1^a of the anti-cyclotomic $\mathbf{Z}_p$-extension of k is given in [2, 3]. The purpose of this paper is to give an explicit description of the first layer k_1^a of the anti-cyclotomic $\mathbf{Z}_p$-extension of an imaginary quadratic field k whose class number is not divisible by $p > 3$. Let $k_z = k(\zeta_p)$ and let σ, τ with $\sigma(\zeta_p) = {\zeta_p}^t$ be generators of $Gal(k_z/k), Gal(k_z/\mathbf{Q}(\zeta_p))$, respectively. The main result of this paper is as follows:

Theorem 1. *Let X be a vector space over a finite field F_p with a basis $\{x_1, \cdots, x_{p-1}\}$ and A be a linear map such that $Ax_i = x_{i+1}$ for $i = 1, \cdots, p-2$ and $Ax_{p-1} = x_1$. Let $x = \sum_i a_i x_i$ be an eigenvector of A corresponding to an eigenvalue t. Let $k = \mathbf{Q}(\sqrt{-D})$ be an imaginary quadratic field whose class number is not divisible by $p > 3$ and assume k is not contained in $\mathbf{Q}(\zeta_p)$. 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 $k_1^a = k(\eta)$, where $\eta = Tr_{k_z(\sqrt[p]{\varepsilon})/k_1^a}(\sqrt[p]{\varepsilon})$.*

Since p does not divide the degree $[k_z^+ : \mathbf{Q}]$, one can always choose a unit α such that ϵ is not a p-power in the maximal real subfield k_z^+ of k_z. See Remark 1 of this paper.

2. Proof of theorems. To prove Theorem 1 we need lemmas.

Lemma 1. *Let p be an odd prime, and k_1^2 be the compositum of first layers of $\mathbf{Z}_p$-extension of an imaginary quadratic field k. Then $Gal(k_1^2/\mathbf{Q}) \simeq D_p \oplus \mathbf{Z}/p$, where D_p is the dihedral group of order $2p$.*

Proof. See [2]. □

Lemma 2. *Let k be an imaginary quadratic number field whose class number is not divisible by $p > 3$. Then the only cyclic extensions of degree p over k unramified outside p which are Galois over $\mathbf{Q}$ are the first layers of anti-cyclotomic and cyclotomic $\mathbf{Z}_p$-extension of k.*

Proof. Let H be the Hilbert class field of k and let F be the maximal abelian extension of k unramified outside p. Then [4] class field theory shows that

$$Gal(F/H) \simeq (\prod_{\mathfrak{p}|p} U_{\mathfrak{p}})/E^-,$$

where E^- is the closure of the global units of k, embedded in local units $\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}$ diagonally. So in this case $Gal(F^p/k) \simeq \mathbf{Z}_p^2$, where F^p is the maximal abelian p-extension of k unramified outside p. Let $N \supseteq k$ be a cyclic p-extension of k, which is Galois over $\mathbf{Q}$, contained in k_1^2. Then by Lemma 1, we see that $Gal(k_1^2/N) =< s^a u^b >$, where $Gal(k_1^2/k_1) =< s >, Gal(k_1^2/k_1^a) =< u >$. Since the non-trivial element of $Gal(k/\mathbf{Q})$ acts on $Gal(N/k)$ by 1 or -1, it can be easily checked that $a = 0$, or $b = 0$. In other words, N should be either the first layer of cyclotomic $\mathbf{Z}_p$-extension of k, or of anti-cyclotomic $\mathbf{Z}_p$-extension of k. □

Now we are ready to prove Theorem 1. First

2000 Mathematics Subject Classiffcation. 11R23.

note that the characteristic polynomial of A is

$$x^{p-1} - 1$$

and $x^{p-1} - 1$ splits completely in $F_p[x]$. Therefore the eigenvector exists. Write $L_z = k_z(\sqrt[p]{\varepsilon})$. Let $H =< \epsilon \mod(k_z^*)^p >$ be the Kummer group for the Kummer extension L_z/k_z, and let $X = Gal(L_z/k_z)$. Then $Gal(k_z/\mathbf{Q})$ acts on H and X, and the Kummer pairing

$$H \times X \longrightarrow \mu_p$$

is a perfect $Gal(k_z/\mathbf{Q})$-equivariant pairing. Hence, by the construction of ε, σ and τ, one can easily see that $\sigma(\varepsilon) = \varepsilon^t \mod(k_z^*)^p$ and $\tau(\varepsilon) = \varepsilon^{-1}$. Therefore the generators σ and τ act on X trivially and inversely, respectively. It follows that $Gal(L_z/k)$ is cyclic of order $(p-1)p$. Then there exists the unique intermediate field M of L_z/k with $[M : k] = p$, and the uniqueness of M asserts that $M/\mathbf{Q}$ is a Galois extension. It follows that $Gal(M/\mathbf{Q}) \simeq Gal(L_z/\mathbf{Q}(\zeta_p)) \simeq D_p$. Since M/k is a cyclic extension of degree p unramified outside p, we have $M = k_1^a$ by Lemma 2. Therefore, by [1, Theorem 5.3.5], we conclude that $k_1^a = k(\eta)$ with $\eta = Tr_{L_z/k_1^a}(\sqrt[p]{\varepsilon})$. $\square$

Example 1. *Let $k = \mathbf{Q}(\sqrt{-3})$ and $p = 5$. Then we can take $t = 2$, and in this case the eigenvector of A is $-x_1 + 2x_2 + x_3 + 3x_4$. If we take $\alpha = (\zeta_{15} - 1)({\zeta_{15}}^{-1} - 1)$, then $\epsilon = \alpha^{-1+2\sigma+\sigma^2+3\sigma^3}$. If we write $\varepsilon = \sum a_i x^i|_{x=\zeta_{15}}$ and ε is a 5-th power of a unit in $k_z = \mathbf{Q}(\zeta_{15})$, then we have*

$$\sum a_i x^i - (\sum b_i x^i)^5 \in (x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)\mathbf{Z}[x]$$

for some integers a_i, b_i. This implies that $\sum a_i 3^i$ should be a 5-th power modulo 4561. But we can easily compute by Maple that $\sum a_i 3^i = 3938$, which is not a 5-th power modulo 4561.

Remark 1. *If we choose a unit $\alpha(\mod E^p)$ to be a generator of the $\mathbf{Z}[Gal(k_z^+/\mathbf{Q})]$-module E/E^p, where E is the unit group of k_z^+, then ϵ is not a p-th power in k_z^+. Moreover $\tau\epsilon/\epsilon \neq 1$ since ϵ is an eigenvector for t whose order in F_p^* is p-1. A referee pointed out to me that such a unit α always exists by using so called "Minkowski unit"* [4, Lemma 5.27].

Acknowledgements. The Author thanks the referee for valuable comments, as well as the referee of author's previous paper [3] for pointing out to me the key idea.

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD) (KRF − 2005-015-C00006).

References

[1] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer, New York, 2000.

[2] J. M. Kim and J. Oh, Defining Polynomial of the first layer of anti-cyclotomic $\mathbf{Z}_3$-extension of 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 $\mathbf{Z}_2^2$-extension over imaginary quadratic fields, Proc. Japan Acad. Ser.A Math. Sci. **76** (2000), no. 9, 132–134.

[4] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.