Defining polynomial of the first layer of anti-cyclotomic $\mathbf{Z}_3$-extension of imaginary quadratic fields of class number 1

By Jae Moon KIM*) and Jangheon OH**), †)

(Communicated by Shigefumi MORI, M. J. A., March 12, 2004)

Abstract: In this paper, we explicitly compute defining polynomials of the first layer of anti-cyclotomic $\mathbf{Z}_3$-extension of imaginary quadratic fields of class number 1.

Key words: Iwasawa theory; anti-cyclotomic $\mathbf{Z}_3$-extension; Kummer extension; defining polynomial.

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. The first layer k_1 of the cyclotomic $\mathbf{Z}_3$-extension of k is just $k(\alpha)$ where α is a root of $x^3 - 3x + 1 = 0$. The explicit construction of the first layer of the anti-cyclotomic $\mathbf{Z}_3$-extension of k is not known. In [2], we studied, for each imaginary quadratic field k, the Galois group $Gal(F_1/\mathbf{Q})$ where F_1 is the compositum of first layers of all $\mathbf{Z}_2$-extensions of k. Moreover we constructed F_1 explicitly when k has class number 1. The purpose of this paper is to compute the defining polynomial of the first layer L of the anti-cyclotomic $\mathbf{Z}_3$-extension of an imaginary quadratic field of class number 1. The main result of this paper is as follows:

Theorem 1. *Let k_1^a be the first layer of the anti-cyclotomic $\mathbf{Z}_3$-extension of an imaginary quadratic field k of class number 1. Then k_1^a is the splitting field L of $f_{k_1^a}(x)$ over $\mathbf{Q}$.*

Table I.

k	Δ_L	$f_{k_1^a}(x)$
$\mathbf{Q}(\sqrt{-1})$	$-2^2 * 3^4$	$x^3 - 3x - 4$
$\mathbf{Q}(\sqrt{-2})$	$-2^3 * 3^4$	$x^3 - 3x - 10$
$\mathbf{Q}(\sqrt{-3})$	-3^5	$x^3 - 3$
$\mathbf{Q}(\sqrt{-7})$	$-7 * 3^4$	$x^3 - 3x - 5$
$\mathbf{Q}(\sqrt{-11})$	$-11 * 3^4$	$x^3 - 3x - 46$
$\mathbf{Q}(\sqrt{-19})$	$-19 * 3^4$	$x^3 - 3x - 302$
$\mathbf{Q}(\sqrt{-43})$	$-43 * 3^4$	$x^3 - 3x - 33710$
$\mathbf{Q}(\sqrt{-67})$	$-67 * 3^4$	$x^3 - 3x - 1030190$
$\mathbf{Q}(\sqrt{-163})$	$-163 * 3^4$	$x^3 - 3x - 15185259950$

Here Δ_L is the discriminant of L.

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. Then $Gal(L/\mathbf{Q}) \simeq D_p \oplus \mathbf{Z}/p$.*

Proof. Since p is an odd prime, the first layers k_1^a, k_1 of anti-cyclotomic and cyclotomic $\mathbf{Z}_p$-extension are linearly disjoint over k. Moreover $Gal(k_1^a/\mathbf{Q}) \simeq D_p$, the dihedral group of order $2p$, which completes the proof. □

Lemma 2. *Let k be an imaginary quadratic number field whose class number is 1. Then the only cyclic extensions of degree 3 over k unramified outside 3 which are Galois over $\mathbf{Q}$ are the first layers of anti-cyclotomic and cyclotomic $\mathbf{Z}_3$-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 3. Then [3] class field theory shows that

2000 Mathematics Subject Classification. 11R23, 11R32.

*) Department of Mathematics, College of Natural Sciences, Inha University, 253 Younghyun-dong, Nam-gu, Incheon 402-751, Korea. This paper was completed during the sabbatical year 2003.

**) Department of Applied Mathematics, College of Natural Sciences, Sejong University, 98 Gunja-dong, Gwangjin-gu, Seoul 143-747, Korea.

†) Correspondence to: J. Oh.

$$Gal(F/H) \simeq \left(\prod_{\mathfrak{p}|3} U_{\mathfrak{p}}\right)/E^-,$$

where E^- is the closure of the global units of k, embedded in local units $\prod_{\mathfrak{p}|3} U_{\mathfrak{p}}$ diagonally. So in this case $Gal(F^3/k) \simeq \mathbf{Z}_3^2$, where F^3 is the maximal abelian 3-extension of k unramified outside 3. By Lemma 1, we see that $Gal(k_1^2/\mathbf{Q}) \simeq D_3 \oplus \mathbf{Z}/3$, which has the following presentation.

$$\langle s, t, u | u^2 = s^3 = t^3 = 1, st = ts, ut = t^2 u, us = su\rangle.$$

It can be easily checked that two groups generated by st and $s^2 t$ are not normal subgroup of $Gal(k_1^2/\mathbf{Q})$. Note that the fields fixed by $\langle t\rangle$ and $\langle s\rangle$ are the first layers of anti-cyclotomic and cyclotomic $\mathbf{Z}_3$-extension of k, respectively. □

Next we need Kummer theory [1, Theorem 5.3.5]. Let k be an imaginary quadratic field, and let k_1^a be the first layer of anti-cyclotomic $\mathbf{Z}_3$-extension. Assume that k does not contain a third root of unity ζ_3, and let $k_z = k(\zeta_3)$ and $L_z = k_1^a(\zeta_3)$. Then by Kummer theory, $L_z = k_z(\sqrt[3]{\alpha})$ for some $\alpha \in k_z^*/k_z^{*3}$. Moreover, $k_1^a = k(\eta)$ with $\eta = Tr_{L_z/k_1^a}(\sqrt[3]{\alpha})$ and the defining polynomial $P(x)$ of k_1^a/k is given by the polynomial

$$(x-(\theta+\tau(\theta)))(x-(\zeta_3\theta+{\zeta_3}^2\tau(\theta)))(x-({\zeta_3}^2\theta+\zeta_3\tau(\theta))),$$

where $\theta = \sqrt[3]{\alpha}$ and τ is a nontrivial element of $Gal(L_z/k_1^a)$.

Now we are ready to prove Theorem 1. It is enough to prove Theorem 1 for k's except for $k = \mathbf{Q}(\sqrt{-3})$ whose case is trivial. Here we give a proof for the case of $k = \mathbf{Q}(\sqrt{-7})$ since proof of remaining cases are exactly the same. So let k be $\mathbf{Q}(\sqrt{-7})$, and L be the first layer of the anti-cyclotomic $\mathbf{Z}_3$-extension of k. Then the only primes ramified in L_z/k_z are the primes above 3. Hence

$$\theta = \sqrt[3]{(1-\zeta_3)^i \epsilon^j {\zeta_3}^k}$$

for integers $0 \le i, j, k \le 2$, where ϵ is the fundamental unit of $k(\zeta_3) = \mathbf{Q}(\sqrt{-7}, \sqrt{-3})$. When $\theta = \sqrt[3]{(5+\sqrt{21})/2}$ which is the third root of the fundamental unit of $\mathbf{Q}(\sqrt{21})$, then a simple computation shows that $P(x) = x^3 - 3x - 5$. The Galois group of the splitting field of $P(x)$ over $\mathbf{Q}$ is D_3. So it is enough to show that the splitting field of $P(x)$ contains $\sqrt{-7}$ by Lemma 2. Let a, b be the imaginary roots of the polynomial $x^3 - 3x - 5$. Then we can easily, for example by a Maple, check that $(a+b)/(a-b) = \sqrt{-7}r$ for some nonzero rational number r. Note that if we take θ as $\sqrt[3]{\zeta_3}$, then $P(x)$ becomes $x^3 - 3x + 1$ whose splitting field over $\mathbf{Q}$ is the first layer of the cyclotomic $\mathbf{Z}_3$-extension of $\mathbf{Q}$. Note also that $x^3 - 3x - 5 = x^3 - 3x - (\epsilon + \epsilon^{-1})$. Actually the defining polynomial $P(x)$ in Table I except for the case $\mathbf{Q}(\sqrt{-3})$ is:

$$P(x) = x^3 - 3x - (\epsilon + \epsilon^{-1}),$$

where ϵ is the fundamental unit of maximal real subfield of $k_z = k(\zeta_3)$. □

Acknowledgements. We would like to thank the anonymous referee for valuable comments. This work was supported by grant R01-2002-000-00032-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

References

[1] Cohen, H.: Advanced Topics in Computational Number Theory. Grad. Texts in Math., 193, Springer-Verlag, New York (2000).

[2] Oh, J.: The first layer of $\mathbf{Z}_2^2$-extension over imaginary quadratic fields. Proc. Japan Acad., **76A**, 132–134 (2000).

[3] Washington, L. C.: Introduction to Cyclotomic Fields. Grad. Texts in Math., 83, Springer-Verlag, New York (1982).