Ray class field of prime conductor of a real quadratic field

By Yoshiyuki Kitaoka

Department of Mathematics, Meijo University
1-501, Shiogamaguchi, Tenpaku-ku, Nagoya, Aichi 468-8502
(Communicated by Shigefumi Mori, M. J. A., June 15, 2004)

Abstract: Let F be a real quadratic field and $\mathfrak{p}$ a prime ideal of degree 2. We construct a quadratic extension of the Hilbert class field in the ray class field of conductor $\mathfrak{p}$.

Key words: Algebraic number field; unit; distribution.

Let F be a real quadratic field and o_F, ϵ the maximal order and a fundamental unit of F, respectively, and χ the character of F, that is $\chi(p) = 1$ if and only if p splits in F for a rational prime p. For a prime number p, we define ℓ_p by

$$\begin{cases} 1 & \text{if } \chi(p) = 1, \\ (p-1)/2 & \text{if } \chi(p) = N(\epsilon) = -1, \\ p-1 & \text{if } \chi(p) = -N(\epsilon) = -1, \end{cases}$$

where N denotes the norm from F to the rational number field $\mathbf{Q}$.

Let $\mathfrak{p}$ be a prime ideal lying above p, and denoting by $E(\mathfrak{p})$ the subgroup of $(o_F/\mathfrak{p})^\times$ consisting of classes represented by units of F, we put

$$I_p = [(o_F/\mathfrak{p})^\times : E(\mathfrak{p})].$$

The class field theory tells us that the degree of the ray class field $F(\mathfrak{p})$ of conductor $\mathfrak{p}$ of F over F is a product of the class number of F and I_p. It is easy to see that ℓ_p divides I_p, and so I_p is a product of two integers ℓ_p and I_p/ℓ_p. The behavior of the number I_p/ℓ_p depends heavily on each prime. However we have shown that under generalized Riemann hypotheses the set of prime ideals satisfying $I_p/\ell_p = 1$ has a positive (modified natural) density in each case ([IK, L, M, CKY, R]). Hence the subfield $F'(\mathfrak{p})$ corresponding to the degree ℓ_p may be considered a basic part of the ray class field $F(\mathfrak{p})$.

The field $F'(\mathfrak{p})$ is given as follows:

(i) $F'(\mathfrak{p})$ = the Hilbert class field F_H when $\chi(p) = 1$,

(ii) $F'(\mathfrak{p})$ = the composite of F_H and $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ when $\chi(p) = N(\epsilon) = -1$,

(iii) $F'(\mathfrak{p})$ = a quadratic extension of the composite of F_H and $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ when $\chi(p) = -N(\epsilon) = -1$.

Here the Hilbert class field F_H is in the weak sense, i.e. it is real in this case, and ζ_p is a primitive pth root of unity.

The first aim is to describe explicitly the quadratic extension in the case (iii) (Theorem 1).

The second is to show that the fickle extension degree $I_p/\ell_p = [F(\mathfrak{p}) : F'(\mathfrak{p})]$ is controlled by the property of the Frobenius automorphism of the fields $F(\zeta_{2m}, \sqrt[m]{\epsilon})$ independent of $F(\mathfrak{p})$ (Theorem 2).

The followings are known.

Lemma 1. *Let K/F be a finite abelian extension and let $L = K(\sqrt{a})$ $(a \in K)$ be a quadratic extension of K. Then the extension L/F is abelian if and only if there is an element $b_\kappa \in K$ for any automorphism $\kappa \in \mathrm{Gal}(K/F)$ such that $\kappa(a) = ab_\kappa^2$ and $\kappa(b_\eta)b_\kappa = \eta(b_\kappa)b_\eta$ hold for any $\eta, \kappa \in \mathrm{Gal}(K/F)$.*

Lemma 2. *Let $L = K(\sqrt{a})$ be a quadratic extension of an algebraic number field K. Let $\mathfrak{p}$ be a prime ideal of K. If $\mathrm{ord}_\mathfrak{p}\, a$ is odd, then $\mathfrak{p}$ is ramified at L/K. If $\mathfrak{p} \nmid 2$ and $\mathrm{ord}_\mathfrak{p}\, a$ is even, then $\mathfrak{p}$ is unramified at L/K. If $\mathfrak{p} \mid 2$ and $\mathrm{ord}_\mathfrak{p}\, a = 0$, then $\mathfrak{p}$ is unramified at L/K if and only if $x^2 \equiv a \bmod \mathfrak{p}^{2m}$ has a solution in o_K where $m = \mathrm{ord}_\mathfrak{p}\, 2$.*

Hereafter till Theorem 1, $F = \mathbf{Q}(\sqrt{D})$ is a real quadratic field and ϵ is a fundamental unit of F and assume $N(\epsilon) = 1$. We denote the (real) Hilbert class field of F by F_H. Because of the assumption $N(\epsilon) = 1$, there is a totally positive element $\alpha \in F_H$ such that a field $F_H(\sqrt{-\alpha})$ is abelian over F and every finite place of F is unramified. We can take α so that $(\alpha, 2) = 1$. By virtue of Lemma 2, α satisfies that for a prime ideal $\mathfrak{p}$ of F, $\mathrm{ord}_\mathfrak{p}\, \alpha$ is even and $x^2 \equiv -\alpha \bmod 4$ has a solution in o_{F_H}. Using this α, we can construct the quadratic extension of F_H in question.

Lemma 3. *Let p be an odd prime number unramified at $F/\mathbf{Q}$. Put $a = (1-\zeta_p)(1-\zeta_p^{-1})\alpha$ and*

2000 Mathematics Subject Classification. 11R37.

$K = F_H(\zeta_p+\zeta_p^{-1})$, where ζ_p is a primitive pth root of unity. Then $L = K(\sqrt{a})$ is a real abelian extension of F.

Proof. a is obviously totally positive and hence L is real. For $\kappa, \eta \in \mathrm{Gal}(K/F)$, we define odd numbers m, n by $\kappa(\zeta_p + \zeta_p^{-1}) = \zeta_p^n + \zeta_p^{-n}$, $\eta(\zeta_p + \zeta_p^{-1}) = \zeta_p^m + \zeta_p^{-m}$. Then we have

$$\begin{aligned}\kappa(a)/a &= (1-\zeta_p^n)(1-\zeta_p^{-n})\kappa(\alpha)/\\ &\qquad (1-\zeta_p)(1-\zeta_p^{-1})\alpha\\ &= (\zeta_p^{n-1}+\cdots+1)\\ &\qquad \times ((\zeta_p^{-1})^{n-1}+\cdots+1)\kappa(\alpha)/\alpha\\ &= (\zeta_p^{(n-1)/2}+\cdots+\zeta_p^{-(n-1)/2})^2\\ &\qquad \times \kappa(\alpha)/\alpha.\end{aligned}$$

On the other hand, $F_H(\sqrt{-\alpha})/F$ is abelian and hence there is an element $c_\kappa \in F_H$ such that $\kappa(-\alpha)/(-\alpha) = c_\kappa^2$ and $c_\eta \eta(c_\kappa) = c_\kappa \kappa(c_\eta)$ since $\kappa_{|F_H}, \eta_{|F_H} \in \mathrm{Gal}(F_H/F)$. Now we put $b_\kappa = (\zeta_p^{(n-1)/2}+\cdots+\zeta_p^{-(n-1)/2})c_\kappa$; then $\kappa(a)/a = b_\kappa^2$ and we have, because of $p \nmid m$

$$\begin{aligned}b_\eta\eta(b_\kappa) &= (\zeta_p^{(m-1)/2}+\cdots+\zeta_p^{-(m-1)/2})c_\eta\\ &\qquad \times ((\zeta_p^m)^{(n-1)/2}+\cdots+(\zeta_p^m)^{-(n-1)/2})\\ &\qquad \times \eta(c_\kappa)\\ &= \zeta_p^{-(m-1)/2}(\zeta_p^m-1)/(\zeta_p-1)\\ &\qquad \times \zeta_p^{-m(n-1)/2}((\zeta_p^m)^n-1)/(\zeta_p^m-1)\\ &\qquad \times c_\eta\eta(c_\kappa)\\ &= \zeta_p^{(1-mn)/2}(\zeta_p^{mn}-1)/(\zeta_p-1)\\ &\qquad \times c_\eta\eta(c_\kappa).\end{aligned}$$

Hence $b_\eta\eta(b_\kappa) = b_\kappa\kappa(b_\eta)$ holds. Thus L/F is abelian. □

Lemma 4. *The conductor of L/F is p if p is an odd prime number and unramified at $F/\mathbf{Q}$.*

Proof. First, we show that every prime ideal not lying above p is unramified at L/K. Let $\mathfrak{q}$ be a prime ideal of K. If $\mathfrak{q} \nmid 2p$, then $\mathrm{ord}_\mathfrak{q}(a) = \mathrm{ord}_\mathfrak{q}(\alpha)$ is even and hence $\mathfrak{q}$ is unramified at L/K. Suppose $\mathfrak{q} \mid 2$; then by Lemma 2, we have only to show $x^2 \equiv (1-\zeta_p)(1-\zeta_p^{-1})\alpha \bmod 4$ has a solution in o_K. Since we have

$$\begin{aligned}&(1-\zeta_p)(1-\zeta_p^{-1})\\ &= (1-\zeta_p^{-(p-1)})(1-\zeta_p^{p-1})\\ &= (\zeta_p^{(p-1)/2}-\zeta_p^{-(p-1)/2})\\ &\qquad \times (\zeta_p^{-(p-1)/2}-\zeta_p^{(p-1)/2})\\ &= -(\zeta_p^{(p-1)/2}-\zeta_p^{-(p-1)/2})^2\\ &= -(\zeta_p^{(p-1)/2}+\zeta_p^{-(p-1)/2})^2+4\\ &\equiv -(\zeta_p^{(p-1)/2}+\zeta_p^{-(p-1)/2})^2 \mod 4,\end{aligned}$$

and $x^2 \equiv -\alpha \bmod 4$ has a solution in o_{F_H}, there is a solution x in o_K for $x^2 \equiv (1-\zeta_p)(1-\zeta_p^{-1})\alpha \bmod 4$. Therefore $\mathfrak{q}$ is unramified at L/K. Thus every prime ideal not lying above p is unramified at L/K and hence at L/F. Let $\mathfrak{P}$ be a prime ideal of L lying above p. For Hasse's function $\varphi_{L/F}$ with respect to $\mathfrak{P}$, and for the last non-trivial ramification group $V_t(\mathfrak{P}; L/F)$, the $\mathfrak{P}\cap F$-factor of the conductor of L/F is given by $(\mathfrak{P}\cap F)^{\varphi_{L/F}^{-1}(t)+1}$. For Hasse's function, we know $\varphi_{L/F} = \varphi_{L/F_H}\varphi_{F_H/F}$ and $\varphi_{F_H/F}$ is the identity since F_H/F is unramified. On the other hand, a divisor $[L : F_H]$ of $p-1$ is prime to p and then the first ramification group $V_1(\mathfrak{P}; L/F_H)$ is trivial since its order is a power of p. Thus $\varphi_{L/F}(v) = \varphi_{L/F_H}(v) = ev$ holds if $v \geq 0$, where e is the ramification index of $\mathfrak{P}$ at L/F_H. Since the last non-trivial ramification group of $\mathfrak{P}$ with respect to L/F is the inertia group, the contribution of $\mathfrak{P}\cap F$ to the conductor of L/F is $\mathfrak{P}\cap F$ itself. □

Thus we have shown, as a special case of Lemma 4

Theorem 1. *Let F be a real quadratic field and suppose that the norm of the fundamental unit ϵ is 1. Then for a prime number p which remains prime in F, the quadratic extension of the composite field of the Hilbert class field and $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ in the ray class field of F of conductor p is given by L in Lemma 3.*

Theorem 2. *Let F be a real quadratic field and ϵ the fundamental unit. Let p be an odd prime number unramified in F and put $F_m = F(\zeta_{2m}, \sqrt[m]{\epsilon})$ for a natural number m. Then I_p/ℓ_p is the maximal integer m relatively prime to p such that*

(i) *p is completely decomposable in F_m if $\chi(p) = 1$,*

(ii) *the Frobenius automorphism ρ of a prime ideal $\mathfrak{P}$ of F_m lying above p satisfies*

$$\zeta_m^\rho = \zeta_m^{-1}, \quad \sqrt[m]{\epsilon}^{2\rho} = \sqrt[m]{\epsilon}^{-2}$$

if $\chi(p) = N(\epsilon) = -1$.

(iii) *the Frobenius automorphism ρ of a prime ideal $\mathfrak{P}$ of F_m lying above p satisfies*

$$\zeta_{2m}^\rho = \zeta_{2m}^{-1}, \quad \sqrt[m]{\epsilon}^{\rho} = \sqrt[m]{\epsilon}^{-1}$$

if $\chi(p) = -N(\epsilon) = -1$.

Proof. This is an immediate corollary of Lemma 4 in [K2]. Define the polynomial $g(x)$ by $x-1$, $x+1$, $x+1$ according to the case (i), (ii), (iii), respectively. The automorphism $\eta \in \mathrm{Gal}(F/\mathbf{Q})$ stands for the identity in the case (i), and for the non-trivial automorphism, otherwise. Then $g(x)$ is a primitive integral polynomial of minimal degree such that the group

$$\{u^{g(\eta)} \mid u \in o_F^\times\}$$

is finite, and the order δ_1 of the group is $1, 2, 1$ according to the case (i), (ii), (iii), respectively. The polynomial $h(x)$ is defined by 1 in case of (i), and $x-1$, otherwise. Applying Lemma 4 in [K2] to this situation with $K = F$, we have, for $^\forall u \in o_F^\times$

$$mh(p)/\delta_1 \mid I_p \Leftrightarrow \sqrt[m]{u}^{\delta_1 g(\rho)} = 1$$

for the Frobenius automorphism ρ of a prime ideal $\mathfrak{P}$ of F_m lying above p, where m is supposed to be relatively prime to p. This completes the proof, since $h(p)/\delta_1 = \ell_p$ holds. $\square$

Acknowledgement. This work was partially supported by Grant-in-Aid for Scientific Research (C), The Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[CKY] Chen, Y-M. J., Kitaoka, Y., and Yu, J.: Distribution of units of real quadratic number fields. Nagoya Math. J., **158**, 167–184 (2000).

[H] Hooley, C.: On Artin's Conjecture. J. Reine Angew. Math., **225**, 209–220 (1967).

[IK] Ishikawa, M., and Kitaoka, Y.: On the distribution of units modulo prime ideals in real quadratic fields. J. Reine Angew. Math., **494**, 65–72 (1998).

[K1] Kitaoka, Y.: Distribution of units of a cubic field with negative discriminant. J. Number Theory, **91**, 318–355 (2001).

[K2] Kitaoka, Y.: Distribution of units of an algebraic number field. Galois Theory and Modular Forms, Developments in Mathematics. Kluwer Academic Publishers, Boston, pp. 287–303 (2003).

[L] Lenstra, H. W. Jr.: On Artin's conjecture and Euclid's algorithm in global fields. Invent. Math., **42**, 201–224 (1977).

[M] Masima, K.: The distribution of units in the residue class field of real quadratic fields and Artin's conjecture. RIMS Kokyuroku, **1026**, 156–166 (1998), (in Japanese).

[R] Roskam, H.: A quadratic analogue of Artin's conjecture on primitive roots. J. Number Theory, **81**, 93–109 (2000).