N. Nakagoshi
Nagoya Math. J.
Vol. 115 (1989), 151–164

ON THE UNRAMIFIED EXTENSIONS OF THE PRIME CYCLOTOMIC NUMBER FIELD AND ITS QUADRATIC EXTENSIONS

NORIKATA NAKAGOSHI

§ 1. Introduction

It is interesting to know what kinds of primes are the factors of the class number of an algebraic number field, and especially to find ones being prime to the degree. About this matter it is desirable to construct the unramified Abelian extensions plainly. In this paper we shall show some of them for the prime cyclotomic number field and its quadratic extensions using the units of subfields.

Let l be an odd prime and ζ be a primitive l-th root of unity. Let $k = \boldsymbol{Q}(\zeta)$ be the l-th cyclotomic number field over the field $\boldsymbol{Q}$ of rationals. If l is irregular, then there is an even integer r with $2 \leqq r \leqq l-3$ such that the Bernoulli number B_{l-1-r} is divisible by l. In § 3 it will be proved that the existence of this even index r is equivalent to that of the cyclotomic unit in the subfield of k, of degree $(l-1)/(r, l-1)$, giving the unramified extension of k, of degree l by adjunction of its l-th root to k, under the assumption of Vandiver's conjecture on the second factor of the class number. When $l \equiv 1 \pmod 4$, this equivalence is related to N.C. Ankeny, E. Artin and S.D. Chowla's conjecture that $u \not\equiv 0 \pmod l$ for the fundamental unit $\varepsilon_l = (t + u\sqrt{l})/2 > 1$ of $\boldsymbol{Q}(\sqrt{l})$ which is not yet proved. We shall give in detail that $u \equiv 0 \pmod l$ if and only if $k(\sqrt[l]{\varepsilon_l})$ is unramified of degree l over k without Vandiver's conjecture.

In § 4 we shall consider a relative quadratic extension $K = k(\sqrt{d})$ where d is a square free rational integer prime to l. Let $l^* = (-1)^{(l-1)/2}l$. If d is a quadratic residue modulo l^2, then we shall give the elementary conditions to obtain the unramified Abelian extensions of degree l and l^2 over K by adjunctions of the l-th roots of the real units of $\boldsymbol{Q}(\sqrt{l^*}, \sqrt{d})$

Received May 9, 1988.

without any assumption on the class numbers of K and its subfield. Some examples satisfying these conditions are shown in § 5. In order to get these conditions we utilize the structure of the prime residue class groups modulo the l-th powers of the prime divisors of K lying above l. This elementary construction of unramified extensions is nowhere to be seen.

Here we call to mind some papers dealing with the class numbers of relative quadratic extensions. M. Gut [4] proved that if an algebraic number field F contains ζ and has a prime divisor lying above l, of absolute degree 1, then there exist infinitely many relative quadratic extensions of F whose class numbers are multiples of l and their primitive elements are quadratic units over F. O. Neumann [7] constructed infinitely many quadratic extensions whose class numbers are divisible by 3, over an algebraic number field whose class number is prime to 3. G. Gras [3] showed that if the class number of $\boldsymbol{Q}(\sqrt{d})$ is divided by l, then there exists a unit ξ of $k_0((\zeta-\zeta^{-1})\sqrt{d})$ such that $k(\sqrt{d}, \sqrt[l]{\xi})$ is unramified over $k(\sqrt{d})$ where k_0 is the maximal real subfield of k. C.J. Parry [8], [9] denoted the necessary and sufficient conditions that the class number of $\boldsymbol{Q}(\sqrt{5}, \sqrt{d})$ is divisible by 5. G. Gras' and C.J. Parry's results are based on the class number relations and the "Spiegelungssatz" for $k(\sqrt{d})$.

I am thankful to Prof. H. Yokoi for his pertinent suggestion.

§ 2. Preliminaries

Let $K = k(\sqrt{d})$ be a quadratic extension of the l-th cyclotomic number field k where d is a square free rational integer prime to l. We assume that d is a quadratic residue modulo l. Let $\lambda = 1-\zeta$ be a generator of the prime ideal of k lying above l. Then the ideal (λ) splits completely in K, say $(\lambda) = \mathfrak{L}_1\mathfrak{L}_2$ where $\mathfrak{L}_1 \neq \mathfrak{L}_2$. If there is a unit ε of K such that ε is an l-th power residue modulo $\mathfrak{L}_i^l$ for $i = 1, 2$, then $K(\sqrt[l]{\varepsilon})$ is unramified over K. Since the prime residue class group modulo $\mathfrak{L}_i^l$ is of type $(l-1, l, \cdots, l)$ for each $i = 1, 2$ (cf. Theorem 3 of [6]), we can choose Takagi's basis $\{\kappa_a\}_{1\leqq a\leqq l-1}$ for their Sylow l-subgroups (cf. [10]): κ_a $(1 \leqq a \leqq l-1)$ are integers of k defined uniquely by

$$\begin{cases} \kappa_1 = \zeta, & \kappa_a \equiv 1-\lambda^a \pmod{\lambda^{a+1}}, \\ \kappa_a^\sigma \equiv \kappa_a^{g^a} \pmod{\lambda^{l+1}} \end{cases}$$

where g is a primitive root modulo l and $\sigma = (\zeta \to \zeta^g)$ is a generator of the Galois group of k over $\boldsymbol{Q}$. For any number μ of K which is prime to $\mathfrak{L}_1$ we let $t_a(\mu)$ be the exponents determined by the congruence

$$(*) \qquad \mu \equiv \mu^l \mu_1^{t_1(\mu)} \cdots \kappa_{l-1}^{t_{l-1}(\mu)} \pmod{\mathfrak{L}_1^l}.$$

If μ is in k, then $t_a(\mu)$ are given by Kummer's logarithmic derivatives.

For an algebraic number field F, numbers α, β and an ideal $\mathfrak{A}$ of F we use the notation $\alpha \underset{(l)}{=} \beta$ in F, and $\alpha \underset{(l)}{\equiv} \beta \pmod{\mathfrak{A}}$ in F, if α/β is an l-th power of a number of F, and α/β is congruent to an l-th power of a number of F modulo $\mathfrak{A}$, respectively.

Now we look through the exponents $t_a(\mu)$ of the congruence (*). Let $l^* = (-1)^{(l-1)/2} l$.

LEMMA 1. (i) *If μ is a unit of k and congruent to a rational integer modulo λ^l, then $\mu \underset{(l)}{\equiv} 1 \pmod{\lambda^l}$ in k.*

(ii) *If μ is in $\boldsymbol{Q}(\sqrt{l^*})$ and prime to λ, then $t_a(\mu) = 0$ for a with $1 \leqq a < l-1$ and $a \neq (l-1)/2$. In particular, if μ is a unit of $\boldsymbol{Q}(\sqrt{l^*})$, then $t_{l-1}(\mu) = 0$.*

Proof. (i) Let $\mu \equiv r \pmod{\lambda^l}$ with a rational integer r. Since there is a rational integer v such that $\mu^l \equiv v \pmod{\lambda^{l-1}}$, it follows from (*) with respect to the modulus λ^{l-1} that $r \equiv v \prod_{1 \leqq a \leqq l-2} \kappa_a^{t_a(\mu)} \pmod{\lambda^{l-1}}$. By the $(l-1)$st power of this congruence we have $(l-1)t_a(\mu) \equiv 0 \pmod{l}$, also $t_a(\mu) = 0$ for $a = 1, \cdots, l-2$.

For the unit μ of k we have $t_{l-1}(\mu) \equiv (1 - N_{k/\boldsymbol{Q}}(\mu))/l \equiv 0 \pmod{l}$ (cf. [10]). Thus $\mu \underset{(l)}{\equiv} 1 \pmod{\lambda^l}$.

(ii) Let g be a primitive root modulo l and $\sigma = (\zeta \to \zeta^g)$ be a generator of the Galois group of k over $\boldsymbol{Q}$.

Let $\mu = x + y\sqrt{l^*}$ with rational numbers x and y. From the congruence (*) with respect to the modulus λ^l it follows $\sigma(\mu) \equiv (\sigma(\mu))^l \prod_a \kappa_a^{g a t_a(\mu)} \pmod{\lambda^l}$. Since $\sqrt{l^*} = \sum_{b=1}^{l-1} \left(\frac{b}{l}\right)\zeta^b$ where $\left(\frac{b}{l}\right)$ are Legendre's symbols, we have $\sigma(\sqrt{l^*}) = \left(\frac{g}{l}\right)\sqrt{l^*} = -\sqrt{l^*}$. Hence we have

$$x - y\sqrt{l^*} \equiv (x - y\sqrt{l^*})^l \prod_a \kappa_a^{g a t_a(\mu)} \pmod{\lambda^l}.$$

Therefore

$$N_{Q(\sqrt{l^*})/Q}(\mu) = x^2 - l^*y^2 \equiv (x^2 - l^*y^2)^l \prod \kappa_a^{(1+g^a)t_a(\mu)} \pmod{\lambda^l}$$

where $(x^2 - l^*y^2)^{l-1} \equiv 1 \pmod{\lambda^{l-1}}$. Thus $(1 + g^a)t_a(\mu) \equiv 0 \pmod{l}$ for $a = 1, \cdots, l-2$, also $t_a(\mu) = 0$ for a with $1 \leqq a < l-1$ and $a \neq (l-1)/2$.

If μ is a unit of $Q(\sqrt{l^*})$, then $t_{l-1}(\mu) = 0$.

LEMMA 2. *Let d be a square free rational integer prime to l. Assume that d is a quadratic residue modulo l.*

(i) *If μ is in $Q(\sqrt{d})$, prime to $\mathfrak{L}_1$, then $t_a(\mu) = 0$ for $a = 1, \cdots, l-2$.*

(ii) *Let $l^*d > 0$ and μ be a unit of $Q(\sqrt{l^*d})$. Then $t_a(\mu) = 0$ for a with $1 \leqq a \leqq l-1$ and $a \neq (l-1)/2$.*

Proof. We also denote by $\sigma = (\zeta \to \zeta^g)$ a generator of the Galois group of K over $Q(\sqrt{d})$.

(i) Since $\mathfrak{L}_1$ is an ambiguous ideal with respect to $\langle\sigma\rangle$, it follows from (*) that

$$\sigma(\mu) \equiv (\sigma(\mu))^l \prod_a \kappa_a^{g^a t_a(\mu)} \pmod{\mathfrak{L}_1^l},$$

that is,

$$\mu \equiv \mu^l \prod_a \kappa_a^{g^a t_a(\mu)} \pmod{\mathfrak{L}_1^l}.$$

Hence $(g^a - 1)\, t_a(\mu) \equiv 0 \pmod{l}$ for $a = 1, \cdots, l-1$, also $t_a(\mu) = 0$ for $a = 1, \cdots, l-2$.

(ii) Let μ be a unit of the real quadratic number field $Q(\sqrt{l^*d})$. From the congruence (*) we have

$$\sigma(\mu) \equiv (\sigma(\mu))^l \prod_a \kappa_a^{g^a t_a(\mu)} \pmod{\mathfrak{L}_1^l}.$$

Since

$$\mu \cdot \sigma(\mu) = N_{Q(\sqrt{l^*d})/Q}(\mu) = \pm 1,$$

we have

$$\pm\mu^{-1} \equiv (\pm\mu^{-1})^l \prod_a \kappa_a^{g^a t_a(\mu)} \pmod{\mathfrak{L}_1^l}.$$

Therefore $(1 + g^a)\, t_a(\mu) \equiv 0 \pmod{l}$ for $a = 1, \cdots, l-1$, also $t_a(\mu) = 0$ for a with $1 \leqq a \leqq l-1$ and $a \neq (l-1)/2$. The lemma is proved.

Now the system of the fundamental units of $Q(\sqrt{l^*}, \sqrt{d})$ is composed of those of its real quadratic subfields, or the 2nd roots of their products. When we wish to obtain the unramified extensions of K, of degree l using the l-th roots of the units of $Q(\sqrt{l^*}, \sqrt{d})$, it is sufficient to examine the fundamental unit of each quadratic subfield, taking into account of

Lemmas 1 and 2. If μ is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$ or $\boldsymbol{Q}(\sqrt{l^*d})$, then Lemma 2 does not make the exponent $t_{l-1}(\mu)$ or $t_{(l-1)/2}(\mu)$ clear. In § 4 we shall show that if d is a quadratic residue modulo l^2, then the exponents $t_a(\mu)$ for μ of $\boldsymbol{Q}(\sqrt{l^*}, \sqrt{d})$ are all determined by Kummer's logarithmic derivatives in k.

§ 3. Unramified extensions and prime cylotomic units

Let B_i be the Bernoulli numbers defined in a power series about the origin of $x/(e^x - 1)$. Let g be a primitive root modulo l and $\sigma = (\zeta \to \zeta^g)$ be a generator of the Galois group of k over $\boldsymbol{Q}$. For a positive divisor r_0 of $(l-1)$ we denote by k_{r_0} the fixed field to the subgroup $\langle \sigma^{r_0} \rangle$, which is of degree r_0 over $\boldsymbol{Q}$.

Let $A(r) = \prod_{a=1}^{l-1} \left(\frac{1-\zeta^a}{1-\zeta}\right)^{a^r}$ be cyclotomic units of k for positive integers r. When r_0 is a positive divisor of $(l-1)$, we define $\varepsilon(r/r_0) = N_{k/k_{r_0}}(A(r))$. We let h^+ be the class number of the maximal real subfield of k. Vandiver's conjecture is that $h^+ \not\equiv 0 \pmod{l}$.

THEOREM 1. *Let r $(2 \leqq r \leqq l-3)$ be an even integer and $d_0 = (r, l-1)$ be the greatest common divisor of r and $l-1$.*

Then $B_{l-1-r} \equiv 0 \pmod{l}$ if and only if $k(\sqrt[l]{\varepsilon(r/r_0)})$ is unramified over k where $r_0 = (l-1)/d_0$. If $h^+ \not\equiv 0 \pmod{l}$, then $[k(\sqrt[l]{\varepsilon(r/r_0)}) : k] = l$.

Proof. Since $\sum_{a=1}^{l-1} a^r \equiv 0 \pmod{l}$ and $r\, r_0 \equiv 0 \pmod{l-1}$, we have

$$\begin{aligned}
\sigma^{r_0} A(r) &= \prod_{a=1}^{l-1} \{(1-\zeta^{ag^{r_0}})/(1-\zeta^{g^{r_0}})\}^{a^r} \\
&= \prod_{a=1}^{l-1} \left(\frac{1-\zeta^{ag^{r_0}}}{1-\zeta} \Big/ \frac{1-\zeta^{g^{r_0}}}{1-\zeta}\right)^{a^r} \\
&= \prod_{(l)\ b=1}^{l-1} \left(\frac{1-\zeta^b}{1-\zeta}\right)^{b^r g^{(l-1-r_0)r}} \underset{(l)}{=} A(r).
\end{aligned}$$

Therefore

$$\varepsilon(r/r_0) = N_{k/k_{r_0}} A(r) = \prod_{j=0}^{d_0-1} \sigma^{r_0 j} A(r) \underset{(l)}{=} A(r)^{d_0},$$

also $k(\sqrt[l]{\varepsilon(r/r_0)}) = k(\sqrt[l]{A(r)})$. If $B_{l-1-r} \equiv 0 \pmod{l}$, then by Theorem 2 of [12] we find that $A(r) \underset{(l)}{\equiv} 1 \pmod{\lambda^{l+1}}$, and thus $k(\sqrt[l]{A(r)})$ is unramified over k.

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

Conversely, suppose that $k(\sqrt[l]{\varepsilon(r/r_0)})$ is unramified over k. Then $\varepsilon(r/r_0) \underset{(l)}{\equiv} 1 \pmod{\lambda^l}$ and $A(r) \underset{(l)}{\equiv} 1 \pmod{\lambda^l}$. Since the l-th power of an integer of k is congruent to a rational integer modulo λ^{l-1}, $A(r)$ is congruent to a rational integer modulo λ^{l-1}. Thus $B_{l-1-r} \equiv 0 \pmod{l}$ by Theorem 2 of [12].

Let $\sigma_a = (\zeta \to \zeta^a)$ be elements of the Galois group of k over $\boldsymbol{Q}$ and

$$E_{l-1-r} = \prod_{a=1}^{l-1} \left(\zeta^{(1-g)/2} \frac{1-\zeta^g}{1-\zeta}\right)^{a^{l-1-r}\sigma_a^{-1}}$$

be the cyclotomic units defined in Chapter 8 of [11] for even r with $2 \leqq r \leqq l-3$. Then we have as above

$$E_{l-1-r} \underset{(l)}{=} \prod_{b=1}^{l-1} \left(\frac{1-\zeta^{bg}}{1-\zeta} \Big/ \frac{1-\zeta^b}{1-\zeta}\right)^{b^r}$$
$$\underset{(l)}{=} \prod_{a=1}^{l-1} \left(\frac{1-\zeta^a}{1-\zeta}\right)^{a^r(g^{l-1-r}-1)} \underset{(l)}{=} (A(r))^{g^{l-1-r}-1}.$$

If $h^+ \not\equiv 0 \pmod{l}$, then $E_{l-1-r} \underset{(l)}{\not\equiv} 1$ in k by Corollary 8.15 of [11], and therefore $[k(\sqrt[l]{\varepsilon(r/r_0)}) : k] = l$.

Remark. If r is a positive integer and r_0 is a positive divisor of $l-1$ such that $rr_0 \not\equiv 0 \pmod{l-1}$. Then $\varepsilon(r/r_0) = N_{k/k_{r_0}} A(r) \underset{(l)}{=} 1$ in k, because $\sum_{j=0}^{(l-1)/r_0-1} g^{j(l-1-r_0)r} \equiv 0 \pmod{l}$.

In Table 1 we show some irregular primes l for which

$$d_0 = (r, l-1-r) > 2 \quad \text{and} \quad r_0 = (l-1)/d_0 < (l-1)/2.$$

Let $l \equiv 1 \pmod 4$ and consider whether $k(\sqrt[l]{\varepsilon_l})$ is unramified over k by the fundamental unit ε_l of $\boldsymbol{Q}(\sqrt{l})$.

PROPOSITION 1. *Let $l \equiv 1 \pmod 4$ and $\varepsilon_l = (t + u\sqrt{l})/2 > 1$ be the fundamental unit of $\boldsymbol{Q}(\sqrt{l})$. Then $k(\sqrt[l]{\varepsilon_l})$ is an unramified extension of degree l over k if and only if $u \equiv 0 \pmod l$.*

Proof. First we can prove that $\varepsilon_l \underset{(l)}{\not\equiv} 1$ in k. Indeed, if $\varepsilon_l = z^l$ for some z of k, then $N_{k/\boldsymbol{Q}(\sqrt{l})}\varepsilon_l = z_l^l$, also $\varepsilon_l^{(l-1)/2} = z_l^l$ where $z_l = N_{k/\boldsymbol{Q}(\sqrt{l})}z$. Hence z_l is a unit of $\boldsymbol{Q}(\sqrt{l})$ and we have $\varepsilon_l = \varepsilon_l^l/\varepsilon_l^{l-1} = (\varepsilon_l/z^2)^l$. Since ε_l is the fundamental unit of $\boldsymbol{Q}(\sqrt{l})$, there is a rational integer c such that $\varepsilon_l/z^2 = \pm\varepsilon_l^c$. It then follows that $\varepsilon_l = \pm\varepsilon_l^{cl}$ which is impossible.

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

It follows from Lemma 1 that

$$\varepsilon_l \equiv \varepsilon_l^l \kappa^{t_{(l-1)/2}(\varepsilon_l)} \pmod{\lambda^l}.$$

Now suppose that $k(\sqrt[l]{\varepsilon_l})/k$ is unramified. Then $\varepsilon_l \underset{(l)}{\equiv} 1 \pmod{\lambda^l}$, so $t_{(l-1)/2}(\varepsilon_l) = 0$. Since there is a rational integer a_l such that $\varepsilon_l^l \equiv a_l \pmod{\lambda^{l-1}}$, we have $\varepsilon_l \equiv a_l \pmod{\lambda^{l-1}}$ and hence $u\sqrt{l} \equiv 2a_l - t \pmod{\lambda^{l-1}}$ which implies $2a_l - t \equiv 0 \pmod{l}$, so $u\sqrt{l} \equiv 0 \pmod{\lambda^{l-1}}$. Thus $u \equiv 0 \pmod{l}$.

Conversely, suppose that $u \equiv 0 \pmod{l}$. Then $\varepsilon_l \equiv t/2 \pmod{\lambda^l}$. It then follows from Lemma 1 that $\varepsilon_l \underset{(l)}{\equiv} 1 \pmod{\lambda^l}$ and $k(\sqrt[l]{\varepsilon_l})$ is unramified over k.

Now it is known in [5] and [1] that

$$\frac{u}{t} h(\boldsymbol{Q}(\sqrt{l})) \equiv B_{(l-1)/2} \pmod{l}$$

where $h(\boldsymbol{Q}(\sqrt{l}))$ is the class number of $\boldsymbol{Q}(\sqrt{l})$ and $h(\boldsymbol{Q}(\sqrt{l})) < l$. This shows that $u \equiv 0 \pmod{l}$ is equivalent to $B_{(l-1)/2} \equiv 0 \pmod{l}$.

We note that

$$\begin{aligned}\varepsilon_l^{-2h(\boldsymbol{Q}(\sqrt{l}))} &= \prod_{a=1}^{l-1} (1-\zeta^a)^{(a/l)} = \prod_{a=1}^{l-1} \left(\frac{1-\zeta^a}{1-\zeta}\right)^{(a/l)} \\ &= \prod_{(l)\ a=1}^{l-1} \left(\frac{1-\zeta^a}{1-\zeta}\right)^{a^{(l-1)/2}} = A((l-1)/2),\end{aligned}$$

because $(a/l) \equiv a^{(l-1)/2} \pmod{l}$.

Remark. We have no primes $l \equiv 1 \pmod 4$ such that $B_{(l-1)/2} \equiv 0 \pmod{l}$ for $l < 6{,}270{,}713$ (cf. [2]).

§ 4. Relative quadratic extensions

Let d be a square free rational integer prime to l and $K = k(\sqrt{d})$. We shall give the sufficient conditions of a unit ε of $\boldsymbol{Q}(\sqrt{l^*}, \sqrt{d})$ making it possible that $K(\sqrt[l]{\varepsilon})$ is an unramified extension of K, of degree l,

Proposition 2. *Let d be a square free rational integer such that $d \equiv x_0^2 \pmod{l^2}$ with a rational integer x_0, prime to l. Let*

$$\varepsilon = a_0 + a_1\sqrt{l^*} + a_2\sqrt{d} + a_3\sqrt{l^*d}$$

be a unit of $\boldsymbol{Q}(\sqrt{l^*}, \sqrt{d})$ with $a_j \in \boldsymbol{Q}$. Let $\tau = (\sqrt{d} \to -\sqrt{d})$ be a generator of the Galois group of $\boldsymbol{Q}(\sqrt{d})$ over $\boldsymbol{Q}$.

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

Suppose that (i) $\varepsilon \underset{(l)}{\neq} 1$ *in* K, (ii) $\varepsilon \cdot \tau(\varepsilon) \underset{(l)}{=} 1$ *in* $\boldsymbol{Q}(\sqrt{l^*})$,
(iii) $t_{(l-1)/2}(a_0 + a_2x_0 + (a_1 + a_3x_0)\sqrt{l^*}) = 0$,
(iv) $\{(a_0 + a_2x_0)^2 - l^*(a_1 + a_3x_0)^2\}^{(l-1)/2} \equiv 1 \pmod{l^2}$.
Then $K(\sqrt[l]{\varepsilon})$ *is an unramified extension of* K, *of degree* l.

Proof. We identify τ with a generator of the Galois group of K over k. Let $\mathfrak{L}_2 = \tau(\mathfrak{L}_1)$. Since $l = (\mathfrak{L}_1\mathfrak{L}_2)^{l-1}$, we have

$$d - x_0^2 = (\sqrt{d} - x_0)(\sqrt{d} + x_0) \equiv 0 \pmod{(\mathfrak{L}_1\mathfrak{L}_2)^{2(l-1)}}$$

where $2(l-1) \geqq l$. If $\sqrt{d} - x_0 \equiv 0 \pmod{\mathfrak{L}_1\mathfrak{L}_2}$, then $\tau(\sqrt{d} - x_0) \equiv 0 \pmod{\mathfrak{L}_1\mathfrak{L}_2}$ and also $x_0 \equiv 0 \pmod{l}$ which is contrary to the assumption. Hence we may assume that $\sqrt{d} \equiv x_0 \pmod{\mathfrak{L}_1^l}$. Then

$$\begin{aligned}\varepsilon &= a_0 + a_1\sqrt{l^*} + a_2\sqrt{d} + a_3\sqrt{l^*d} \\ &\equiv a_0 + a_2x_0 + (a_1 + a_3x_0)\sqrt{l^*} \pmod{\mathfrak{L}_1^l}.\end{aligned}$$

Put $\xi = a_0 + a_2x_0 + (a_1 + a_3x_0)\sqrt{l^*}$ which is a number of $\boldsymbol{Q}(\sqrt{l^*})$, prime to λ. For this number ξ we can obtain the exponents $t_{(l-1)/2}(\xi)$ and $t_{l-1}(\xi)$ by Kummer's logarithmic derivatives. It then follows from Lemma 1

$$(**) \qquad \xi \equiv \xi^l \kappa^{t_{(l-1)/2}(\xi)}_{(l-1)/2} \kappa^{t_{l-1}(\xi)}_{l-1} \pmod{\mathfrak{L}_1^l}$$

If $t_{(l-1)/2}(\xi) = 0$ and $t_{l-1}(\xi) \equiv (1 - N_{k/\boldsymbol{Q}}(\xi))/l = (1 - N_{\boldsymbol{Q}(\sqrt{l^*})/\boldsymbol{Q}}(\xi)^{(l-1)/2})/l \equiv 0 \pmod{l}$, then $\varepsilon \equiv \xi \underset{(l)}{\equiv} 1 \pmod{\mathfrak{L}_1^l}$ Moreover, if $\varepsilon \cdot \tau(\varepsilon) \underset{(l)}{=} 1$ in $\boldsymbol{Q}(\sqrt{l^*})$, then by (**) we have

$$\tau(\varepsilon) \equiv (\tau(\xi))^l \kappa^{t_{(l-1)/2}(\xi)}_{(l-1)/2} \kappa^{t_{l-1}(\xi)}_{l-1} \pmod{\mathfrak{L}_2^l},$$

also

$$\varepsilon^{-1} \underset{(l)}{\equiv} (\varepsilon^{-1})^l \kappa^{t_{(l-1)/2}(\xi)}_{(l-1)/2} \kappa^{t_{l-1}(\xi)}_{l-1} \pmod{\mathfrak{L}_2^l}.$$

If the conditions (ii), (iii) and (iv) are satisfied by the unit ε, then $\varepsilon \underset{(l)}{\equiv} 1 \pmod{\mathfrak{L}_i^l}$ for $i = 1, 2$. Thus $K(\sqrt[l]{\varepsilon})$ is unramified over K. Finally, if $\varepsilon \underset{(l)}{\neq} 1$ in K, then $[K(\sqrt[l]{\varepsilon}) : K] = l$.

THEOREM 2. *Let* d *be a square free rational integer such that* $d \equiv x_0^2 \pmod{l^2}$ *with a rational integer* x_0 *prime to* l.

(I) *Let* $d > 0$ *and* $\varepsilon_d = a_0 + a_2\sqrt{d} > 1$ *be the fundamental unit of* $\boldsymbol{Q}(\sqrt{d})$ $(a_0, a_2 \in \boldsymbol{Q})$. *If* $(a_0 + a_2x_0)^{l-1} \equiv 1 \pmod{l^2}$. *then* $K(\sqrt[l]{\varepsilon_d})$ *is an unramified extension of* K, *of degree* l.

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

(II) *Let* $l^*d > 0$ *and* $\varepsilon_{l^*d} = a_0 + a_3\sqrt{l^*d} > 1$ *be the fundamental unit of* $\boldsymbol{Q}(\sqrt{l^*d})$ $(a_0, a_3 \in \boldsymbol{Q})$. *If* $t_{(l-1)/2}(a_0 + a_3x_0\sqrt{l^*}) = 0$, *then* $K(\sqrt[l]{\varepsilon_{l^*d}})$ *is an unramified extension of* K, *of degree* l.

According to H. Yokoi [13] we know that (i) if $d = b^2l^4 + 4$ is square free for a rational integer $b > 0$, then $(bl^2 + \sqrt{b^2l^4 + 4})/2$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$; (ii) if $d = b^2l^4 + 1$ is square free for a rational integer $b > 0$, then $\varepsilon_d = bl^2 + \sqrt{b^2l^4 + 1}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$. These units satisfy the condition of (I) of this Theorem. Some pairs (l, d) satisfying the condition of (I) are also shown in Table 2.

Proof. (I) Suppose that $\varepsilon_d = w^l$ for some w in K. Then $N_{K/\boldsymbol{Q}(\sqrt{d})}\varepsilon_d = N_{K/\boldsymbol{Q}(\sqrt{d})}w^l$, also $\varepsilon_d^{l-1} = w_d^l$ where $w_d = N_{K/\boldsymbol{Q}(\sqrt{d})}w$. We see that w_d is a unit of $\boldsymbol{Q}(\sqrt{d})$. Since $\varepsilon_d = \varepsilon_d^l/\varepsilon_d^{l-1} = (\varepsilon_d/w_d)^l$ and ε_d is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$, it is a contradiction. Thus $\varepsilon_d \underset{(l)}{\neq} 1$ in K.

We let ε_d be ε of Proposition 2 with $a_1 = a_3 = 0$. Then

$$\varepsilon_d \cdot \tau(\varepsilon_d) = N_{\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}}\varepsilon_d = \pm 1 = (\pm 1)^l \quad \text{and} \quad t_{(l-1)/2}(a_0 + a_2x_0) = 0\,,$$

because $a_0 + a_2x_0$ is a rational number prime to l. Thus, if $(a_0 + a_2x_0)^{l-1} \equiv 1 \pmod{l^2}$, then by Proposition 2 we see that $K(\sqrt[l]{\varepsilon_d})$ is an unramified extension of K, of degree l.

(II) Let $l^*d > 0$ and ε_{l^*d} be the fundamental unit of $\boldsymbol{Q}(\sqrt{l^*d})$. Then it can be proved that $\varepsilon_{l^*d} \underset{(l)}{\neq} 1$ in K as above. We let ε_{l^*d} be ε of Proposition 2 with $a_1 = a_2 = 0$. It then follows that

$$\begin{aligned}\varepsilon_{l^*d} \cdot \tau(\varepsilon_{l^*d}) &= N_{\boldsymbol{Q}(\sqrt{l^*d})/\boldsymbol{Q}}\varepsilon_{l^*d} = a_0^2 - l^*da_3^2 \\ &= \begin{cases} \pm 1 = (\pm 1)^l, & \text{if } l \equiv 1 \pmod 4 \text{ and } d > 0, \\ +1 = (+1)^l, & \text{if } l \equiv -1 \pmod 4 \text{ and } d < 0. \end{cases}\end{aligned}$$

Since $d \equiv x_0^2 \pmod{l^2}$, we have $a_0^2 - l^*da_3^2 \equiv a_0^2 - l^*a_3^2x_0^2 \pmod{l^2}$, and then $(a_0^2 - l^*a_3^2x_0^2)^{(l-1)/2} \equiv 1 \pmod{l^2}$. Thus the conditions (i), (ii) and (iv) of Proposition 2 are satisfied by $\varepsilon = \varepsilon_{l^*d}$. If $t_{(l-1)/2}(a_0 + a_3x_0\sqrt{l^*}) = 0$, then $K(\sqrt[l]{\varepsilon_{l^*d}})$ is an unramified extension of K, of degree l, as desired.

PROPOSITION 3. *Let* d *be a square free rational integer prime to* l. *Let* $l^*d > 0$ *and* $\varepsilon_{l^*d} = a_0 + a_3\sqrt{l^*d} > 1$ *be the fundamental unit of* $\boldsymbol{Q}(\sqrt{l^*d})$ $(a_0, a_3 \in \boldsymbol{Q})$.

If $a_0^{l-1} \equiv 1 \pmod{l^2}$ *and* $a_3 \equiv 0 \pmod{l}$, *then* $K(\sqrt[l]{\varepsilon_{l^*d}})$ *is an unramified extension of* K, *of degree* l.

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

Proof. Let $\mathfrak{L}$ be a prime divisor of K lying above l and $\tau = (\sqrt{d} \to -\sqrt{d})$ be a generator of the Galois group of K over k. Since $\mathfrak{L}$ and $\tau(\mathfrak{L})$ are unramified over k and $\varepsilon_{l*d} \underset{(l)}{\neq} 1$ in K, it is enough to show that ε_{l*d} is the l-th power residue modulo $\mathfrak{L}^l$ and $\tau(\mathfrak{L})^l$. Under the assumption of Proposition 3 it follows that $\varepsilon_{l*d} \equiv a_0 \pmod{\mathfrak{L}^l}$ where $a_0 \equiv a_0^l \kappa_{l-1}^{t_{l-1}(a_0)} \pmod{\lambda^l}$ and $t_{l-1}(a_0) \equiv (1 - N_{k/\boldsymbol{Q}}(a_0))/l \equiv (1 - a_0^{l-1})/l \equiv 0 \pmod{l}$. Therefore $\varepsilon_{l*d} \underset{(l)}{\equiv} 1 \pmod{\mathfrak{L}^l}$ and $\pm(\varepsilon_{l*d})^{-1} \underset{(l)}{\equiv} 1 \pmod{\tau(\mathfrak{L})^l}$, as was to be shown.

For example, let $l \equiv 1 \pmod 4$ and $b \not\equiv 0 \pmod l$. If $d = b(bl^3 \pm 2)$ is square free for $b > 0$ and if $\varepsilon_{ld} = bl^3 \pm 1 + l\sqrt{bl(bl^3 \pm 2)}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{ld})$, then $K(\sqrt[l]{\varepsilon_{ld}})$ is unramified over K, of degree l.

There are some examples of l and d satisfying the conditions of Proposition 3 which are shown in Table 3.

COROLLARY. *Let* $l \equiv 1 \pmod 4$, $d > 0$ *and* $d \equiv x_0^2 \pmod{l^2}$ *with a rational integer* x_0 *prime to* l. *Let* $\varepsilon_d = a_{01} + a_2\sqrt{d} > 1$, $\varepsilon_{ld} = a_{02} + a_3\sqrt{ld} > 1$ *be the fundamental unit of* $\boldsymbol{Q}(\sqrt{d})$ *and* $\boldsymbol{Q}(\sqrt{ld})$, *respectively.*

If $(a_{01} + a_2x_0)^{l-1} \equiv 1 \pmod{l^2}$, $a_{02}^{l-1} \equiv 1 \pmod{l^2}$ *and* $a_3 \equiv 0 \pmod l$, *then* $K(\sqrt[l]{\varepsilon_d}, \sqrt[l]{\varepsilon_{ld}})$ *is an unramified extension of* K *whose Galois group over* K *is of type* (l, l).

We have some pairs (l, d) satisfying these conditions which are shown in Table 4.

Proof. From the 1st assertion (I) of Theorem 2 and Propositon 3 it follows that $K(\sqrt[l]{\varepsilon_d})$ and $K(\sqrt[l]{\varepsilon_{ld}})$ are both unramified extensions of K, of degree l. It is enough to show that $\varepsilon_d \underset{(l)}{\neq} \varepsilon_{ld}$ in K. Suppose that $\varepsilon_d = \varepsilon_{ld}\omega^l$ for some ω in K. Since $\sigma(\varepsilon_{ld}) = a_{02} - a_3\sqrt{ld}$ and $N_{K/\boldsymbol{Q}(\sqrt{d})}(\varepsilon_d) = N_{K/\boldsymbol{Q}(\sqrt{d})}(\varepsilon_{ld}\omega^l)$, we have $\varepsilon_d^{l-1} = (\pm 1)^{(l-1)/2}\omega_d^l = \omega_d^l$ where $\omega_d = N_{K/\boldsymbol{Q}(\sqrt{d})}(\omega)$ and $(l-1)/2 \equiv 0 \pmod 2$. Then ω_d is a unit of $\boldsymbol{Q}(\sqrt{d})$ and $\varepsilon_d = \varepsilon_d^l/\varepsilon_d^{l-1} = (\varepsilon_d/\omega_d)^l$ which is impossible, because ε_d is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$. Thus we have the corollary.

Remark. If d is prime to l and if there is a real unit ε of $\boldsymbol{Q}(\sqrt{l^*}, \sqrt{d})$ such that ε is the l-th power residue modulo the l-th power of each prime divisor of K lying above l, then $K(\sqrt[l]{\varepsilon})$ is unramified over K, even though d is not a quadratic residue modulo l^2. For examples, if $d = b^2l^4 \pm 2$ is square free for $b > 0$ and $\varepsilon_d = b^2l^4 \pm 1 + bl^2\sqrt{b^2l^4 \pm 2}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$, then $\varepsilon_d \equiv 1 \pmod{l^2}$, so $K(\sqrt[l]{\varepsilon_d})$ is unramified over K, of degree l.

§ 5. Examples

In the following Tables 2, 3 and 4 we denote by h_m the class number of a quadratic number field $\boldsymbol{Q}(\sqrt{m})$. The odd prime factors of the class number of $\boldsymbol{Q}(\sqrt{m_1}, \sqrt{m_2})$ are those of the class number of its quadratic subfields.

I am grateful to Y. Kida of Kanazawa Univ., giving me these many examples using a computer with his excellent programs.

Table 1 (Examples for Theorem 1)

l	$l-1-r$	r	$d_0=(r, l-1)$	$r_0=(l-1)/d_0$
37	32	4	4	9
103	24	78	6	17
421	240	180	60	7
491	336	154	14	35
613	522	90	18	34
631	80	550	10	63
647	272	374	34	19
673	408	264	24	28
761	260	500	20	38
929	520	408	8	116
1129	348	780	12	94
1983	1058	874	46	42
2017	1204	812	28	72
2357	2204	152	76	31
2441	366	2074	122	20
2861	352	2508	44	65
3329	1378	1950	26	128
3433	1300	2132	52	66
3617	16	3600	16	113
4003	2610	1392	58	69
4027	2332	1694	22	183
4523	456	4066	38	119
4951	1914	3036	66	75
6263	3286	2976	62	101
6529	1564	4934	68	96
6871	2010	4860	30	229
7309	324	6984	36	203

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

Table 2 (Examples for (I) of Theorem 2)

l	x_0	d	h_d	h_{l*d}
3	1	82	4	12
	2	58	2	12
	4	43	1	12
5	1	51	2	4
	2	629	2	4
	3	109	1	2
	4	191	1	2
	6	161	1	2
	7	574	6	4
	8	39	2	4
	9	581	1	2
	11	271	1	2
	12	69	1	2
7	1	295	2	4
	2	494	2	40
	3	303	2	40
	4	751	1	32
	5	74	2	16
	6	771	2	40
	8	505	4	28
	9	179	1	32
	10	149	1	8
	11	23	1	16
	12	2594	2	160
	13	218	2	48
	15	470	2	64
	16	403	2	32
	17	583	2	48
	18	1353	2	72
	19	1194	2	48
	20	449	1	56
	22	1121	1	56
	23	1754	2	80
	24	1311	4	48

Table 3 (Examples for Proposition 3)

l	d	$l*d$	h_d	h_{l*d}
3	−26	78	6	2
	−53	159	6	2
	−107	321	3	3
5	14	70	1	2
	23	115	1	2
	26	130	2	4
	31	155	1	2
	123	615	2	4
	127	635	1	2
	129	645	1	2
7	−34	238	4	2
	−73	511	4	2
	−118	826	6	2
13	61	793	1	4

https://doi.org/10.1017/S0027763000001598 Published online by Cambridge University Press

Table 4 (Examples for Corollary).

l	x_0	d	ld	h_d	h_{l*d}
5	1	426	2130	2	4
	2	629	3145	2	4
	3	509	2545	1	4
	4	191	955	1	2
	6	2386	11930	2	4
	7	574	2870	6	4
	8	1389	6945	1	10
	9	581	2905	1	2
	11	2671	13355	1	4
	12	3169	15845	1	4
13	1	23830	309790	2	4
	9	9883	128479	1	2
	12	2003	26039	1	6

References

[1] N. C. Ankeny, E. Artin and S. D. Chowla, The class number of real quadratic number fields, Ann. of Math., (2) **56** (1952), 479–493.

[2] B. D. Beach, H. C. Williams and C. R. Zarnke, Some computer results on units in quadratic and cubic fields, Proc. of the 25th Summer Meeting of the Canadian Math. Congress, Lakehead Univ., 1971, 609–648; MR 49#2656.

[3] G. Gras, Extensions Abélienne non ramifiées de degré premier d'un corps quadratique, Bull. Soc. Math. France, **100** (1972), 177–193.

[4] M. Gut, Relativequadratische Zahlkörper, deren Klassenzahl durch eine vorgegebene ungerade Primzahl teibar ist, Comment. Math. Helv., **28** (1954), 270–277.

[5] A. A. Kiselev, An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers (Russian), Dokl. Akad. Nauk SSSR, 61 (1948), 777–779; MR 10, p. 236.

[6] N. Nakagoshi, The structure of the multiplicative group of residue classes modulo p^{N+1} Nagoya Math. J., **73** (1979), 41–60.

[7] O. Neumann, Relativ-quadratische Zahlkörper, deren Klassenzahlen durch 3 teilbar sind, Math. Nachr., **56** (1973), 281–306.

[8] C. J. Parry, Real quadratic fields with class number divisible by five, Math. Comp., **31** (1977), 1019–1029.

[9] C. J. Parry, On the class number of relative quadratic fields, Math. Comp., **32** (1978), 1261–1270.

[10] T. Takagi, Zur Theorie der Kreiskörper, J. reine angew. Math., **157** (1927), 246–255.

[11] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

[12] ——, On some cyclotomic congruences of F. Thaine, Proc. Amer. Math. Soc., **93** (1985), 10–14.

[13] H. Yokoi, On real quadratic fields containing units with norm -1, Nagoya Math. J., **33** (1968), 139–152.

Department of Mathematics
Toyama University
Gofuku 3190, Toyama 930
Japan