Tôhoku Math. Journ.
31 (1979), 91-96.

ON CYCLOTOMIC Z_2-EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

YÛJI KIDA

(Received March 4, 1978, revised October 13, 1978)

Let $K = \boldsymbol{Q}(\sqrt{-m})$ for a positive square-free integer m. For each $n \geqq 0$, let $\boldsymbol{B}_n$ be the maximal real subfield of the cyclotomic field of the 2^{n+2}-th roots of unity. Let $\boldsymbol{B}_\infty = \bigcup_{n=0}^{\infty} \boldsymbol{B}_n$ and let $K_\infty = \boldsymbol{B}_\infty \cdot K$. Then the extension K_∞/K is called a cyclotomic $\boldsymbol{Z}_2$-extension. Let h_n be the class number of $K_n = \boldsymbol{B}_n \cdot K$ and let 2^{e_n} be the exact power of 2 dividing h_n. Iwasawa proved, in [2] and [3], that there exist an integer $n_0 \geqq 0$ and an integer c such that

$$(1) \qquad e_n = \lambda n + c \quad \text{for all} \quad n \geqq n_0 ,$$

where λ is the invariant of this $\boldsymbol{Z}_2$-extension.

The group-theoretic meaning of this invariant λ is as follows. Let A_n be the 2-Sylow subgroup of the ideal class group of K_n. For each $m \geqq n \geqq 0$, the norm map from K_m to K_n defines a morphism from A_m to A_n. Let X be the limit of this projective system, then as an abelian group

$$(2) \qquad X \cong \boldsymbol{Z}_2^\lambda \oplus T ,$$

where T is a finite abelian 2-group. This integer λ coincides with that of (1).

We always define the natural action of $\Gamma = \mathrm{Gal}(K_\infty/K)$ on X and call X the Iwasawa module for K_∞/K as a Γ-module. The action of Γ will be used in Section 4.

In this paper, we shall determine the right hand side of (2), especially the invariant λ, and find a value of n_0 satisfying (1).

Finally, the author would like to express his hearty thanks to Professor K. Uchida for his kind encouragement and guidance.

(Added on October 13, 1978)

After this paper was accepted for publication, the author received the preprint by B. Ferrero entitled "The cyclotomic $\boldsymbol{Z}_2$-extension of imaginary quadratic fields" in which he proves the same formula for the invariant λ by a purely algebraic method. Moreover, his Theorem 5 c) and f) implies the torsion subgroup T in our Theorem 1 is in fact of order 2.

1. It is clear that $\boldsymbol{Q}(\sqrt{-m})\cdot\boldsymbol{B}_n = \boldsymbol{Q}(\sqrt{-2m})\cdot\boldsymbol{B}_n$ for all $n \geqq 1$, and in the case of $m = 1$ or 3, $\lambda = c = 0$ is well-known, so it may be sufficient to treat only the case that m is an odd integer bigger than 3. In this case, every $K_n (n \geqq 0)$ contains no roots of unity other than ± 1. For simplicity, we shall use the following notations.

$e^{(2)}N$: the exponent of the exact power of 2 dividing a natural number N.

$d^{(2)}A$: the 2-rank of a compact abelian group A.

LEMMA 1. *The class number of $\boldsymbol{B}_n$ in the narrow sense, hence also in the wide sense, is odd for all $n \geqq 0$.*

PROOF. It is well-known in the wide sense, and the proof is almost the same (see Iwasawa [1] and [2]).

Let $a(K_n)$ be the number of the ambiguous ideal classes in $K_n/\boldsymbol{B}_n$, and let s_n be the number of the ramified prime ideals in $K_n/\boldsymbol{B}_n$. Then a well-known formula states that

$$(3) \qquad a(K_n) = h(\boldsymbol{B}_n)\cdot\frac{2^{s_n+2^n-1}}{[E_n : E_n \cap \mathcal{N}K_n]} \quad \text{for all} \quad n \geqq 0\,,$$

where $h(\boldsymbol{B}_n)$ is the class number of $\boldsymbol{B}_n$, E_n is the unit group of $\boldsymbol{B}_n$ and $\mathcal{N}$ is the norm map from K_n to $\boldsymbol{B}_n$. The following lemma is essential to our theorems, which was suggested to the author by Professor K. Uchida.

LEMMA 2. $[E_n : E_n \cap \mathcal{N}K_n] = 2^{2^n}$ *for all* $n \geqq 0$.

PROOF. Let $\boldsymbol{B}_n^*$ be the multiplicative group of all non-zero elements of $\boldsymbol{B}_n$, and let $\boldsymbol{B}_{n,+}^*$ be its subgroup of totally positive elements. Let P be the principal ideal group of $\boldsymbol{B}_n$, and let P_+ be its subgroup of ideals generated by $\boldsymbol{B}_{n,+}^*$, then it holds that

$$P/P_+ \cong \boldsymbol{B}_n^*/E_n\cdot\boldsymbol{B}_{n,+}^*\,.$$

But by Lemma 1, the left hand side vanishes, therefore

$$\boldsymbol{B}_n^* = E_n\cdot\boldsymbol{B}_{n,+}^*\,.$$

In any finite algebraic number field, there exist elements with an arbitrary signature, so the above equality states that there exist in E_n elements with an arbitrary signature. On the other hand, since K_n is an imaginary abelian field, any element of $\mathcal{N}K_n$ is totally positive. Therefore

$$[E_n : E_n \cap \mathcal{N}K_n] \geqq 2^{2^n}\,.$$

Conversely, it is clear that

$$E_n \cap \mathcal{N} K_n \supset E_n^2 ,$$

then by Dirichlet's unit theorem,

$$[E_n : E_n \cap \mathcal{N} K_n] \leqq [E_n : E_n^2] = 2^{2^n} .$$

This completes the proof.

LEMMA 3. $e^{(2)}a(K_n) = s_n - 1$ *for all* $n \geqq 0$.

PROOF. Apply $e^{(2)}$ to both sides of (3), then the lemma follows at once from Lemmas 1 and 2.

LEMMA 4. $e^{(2)}a(K_n) = d^{(2)}A_n$ *for all* $n \geqq 0$.

PROOF. Let J be the generator of Gal $(K_n/\boldsymbol{B}_n)$. Then for any element c of A_n, c^{1+J} is the natural image of an ideal class of $\boldsymbol{B}_n$. But by Lemma 1, c^{1+J} is of odd order, so c^{1+J} must be 1. Therefore $c^2 = 1$ if and only if $c = c^J$.

Combining this with Lemma 3, we have the following proposition.

PROPOSITION 1. $d^{(2)}A_n = s_n - 1$ *for all* $n \geqq 0$.

As K_∞/K is a cyclotomic $\boldsymbol{Z}_2$-extension, it is well-known that s_n is constant for all sufficiently large n (the exact value of this constant will be given later). Thus we have another proof of the vanishing of the invariant μ of this $\boldsymbol{Z}_2$-extension (see Iwasawa [3]).

2. As $K_{n+1}/\boldsymbol{B}_n$ is an abelian extension of type (2, 2), there exists an intermediate field L_n of degree 2 over $\boldsymbol{B}_n$ different from K_n and $\boldsymbol{B}_{n+1}$. For an abelian field k, let $h(k)$, $R(k)$, $W(k)$, and $\hat{k}$ be its class number, regulator, the number of roots of unity contained in k and the group of Dirichlet characters, respectively. For a Dirichlet character θ, let f_θ be its conductor and let $M(\theta) = L(1, \theta)\cdot\sqrt{f_\theta}$, where $L(s, \theta)$ is of course usual Dirichlet's L-function. Then a class number formula states that

$$h(k)R(k) = \frac{W(k)}{2^i(2\pi)^j} \prod_\theta M(\theta) ,$$

where θ ranges over all non-principal elements of $\hat{k}$, and i and $2j$ are the numbers of real and complex conjugate fields of k, respectively. Applying this formula to each K_n, we get

$$\frac{h(K_{n+1})R(K_{n+1})}{h(K_n)R(K_n)} = (2\pi)^{-2^n} \prod_\theta M(\theta) \qquad \text{for all} \quad n \geqq 0 ,$$

where θ ranges over all the elements of $\hat{K}_{n+1}$ not contained in $\hat{K}_n$.

The right hand side $= (2\pi)^{-2^n}\{\prod_{\theta_1} M(\theta_1)\}\{\prod_{\theta_2} M(\theta_2)\}$,

$$= \frac{h(L_n)h(\boldsymbol{B}_{n+1})R(L_n)R(\boldsymbol{B}_{n+1})}{h(\boldsymbol{B}_n)^2R(\boldsymbol{B}_n)^2} ,$$

where θ_1(resp. θ_2) ranges over all the elements of $\hat{L}_n$ (resp. $\hat{\boldsymbol{B}}_{n+1}$) not contained in $\hat{\boldsymbol{B}}_n$. Hence we get

$$\frac{h(K_{n+1})}{h(K_n)} = \frac{h(L_n)h(\boldsymbol{B}_{n+1})}{h(\boldsymbol{B}_n)^2} \cdot \frac{R(L_n)R(\boldsymbol{B}_{n+1})R(K_n)}{R(\boldsymbol{B}_n)^2R(K_{n+1})} .$$

By our assumption, $W(K_n) = W(L_n) = 2$ and some prime ideal of $\boldsymbol{B}_n$ not dividing 2 must be ramified in K_n and L_n for all $n \geqq 0$. Thus the unit index is 1 in each case, that is,

$$R(K_n)/R(\boldsymbol{B}_n) = R(L_n)/R(\boldsymbol{B}_n) = 2^{2^n-1} \qquad \text{for all} \quad n \geqq 0 .$$

Therefore

$$(4) \qquad h(K_{n+1})/h(K_n) = h(L_n)h(\boldsymbol{B}_{n+1})/2h(\boldsymbol{B}_n)^2 \qquad \text{for all} \quad n \geqq 0 .$$

Since $h(\boldsymbol{B}_n)$ is prime to 2 for all $n \geqq 0$ by Lemma 1, we get the following lemma by applying $e^{(2)}$ to both sides of (4).

LEMMA 5. $e_{n+1} - e_n = -1 + e^{(2)}h(L_n)$ *for all* $n \geqq 0$.

Let $a(L_n)$ be the number of the ambiguous ideal classes in $L_n/\boldsymbol{B}_n$, and let t_n be the number of the ramified prime ideals in $L_n/\boldsymbol{B}_n$. Then the same argument as in the preceding section shows that $e^{(2)}a(L_n) = t_n - 1$ for all $n \geqq 0$. Hence we get the following proposition.

PROPOSITION 2. $e_{n+1} - e_n \geqq t_n - 2$ *for all* $n \geqq 0$,
especially $\lambda \geqq t_n - 2$ *for all* $n \geqq n_0$.

3. If 2 is ramified in $K/\boldsymbol{Q}$, every prime ideal of $\boldsymbol{B}_n$ is ramified in K_n and L_n at the same time. If 2 is not ramified in $K/\boldsymbol{Q}$, a unique prime ideal of $\boldsymbol{B}_n$ dividing 2 is not ramified in K_n, but is ramified in L_n. Every other prime ideal of $\boldsymbol{B}_n$ is ramified in K_n and L_n at the same time. Hence we get the following proposition.

PROPOSITION 3.

$$t_n = \begin{cases} s_n + 1 & \text{\textit{if}} \quad m \equiv 3 \pmod 4 . \\ s_n & \text{\textit{if}} \quad m \equiv 1 \pmod 4 . \end{cases}$$

Combining this with Propositions 1 and 2, we get that for all $n \geqq n_0$

$$s_n - 1 = d^{(2)}A_n \geqq \lambda \geqq s_n - 1 \qquad \text{if} \quad m \equiv 3 \pmod 4 ,$$
$$s_n - 1 = d^{(2)}A_n \geqq \lambda \geqq s_n - 2 \qquad \text{if} \quad m \equiv 1 \pmod 4 .$$

As we stated before, s_n is constant for all sufficiently large n. If we denote this constant by s_∞, then $d^{(2)}A_n = s_\infty - 1$ for all sufficiently large n. Therefore $d^{(2)}X = s_\infty - 1$ by the properties of projective limits. When $m \equiv 1 (\mathrm{mod}\ 4)$, the cases $\lambda = s_\infty - 1$ and $s_\infty - 2$ are possible. But the former means X is torsion-free as an abelian group, a contradiction to the following lemma. Hence $\lambda = s_\infty - 2$ must hold.

LEMMA 6. *If* $m \equiv 1 (\mathrm{mod}\ 4)$, $c^* = (c(2_0), \cdots, c(2_n), \cdots)$ *is of order* 2 *in* X, *where* 2_n *is a unique prime ideal of* K_n *dividing* 2 *and* $c(2_n)$ *is the ideal class of* K_n *containing* 2_n *for each* $n \geqq 0$.

PROOF. Clearly c^* is contained in X and 2_n^2 is principal even in B_n for all $n \geqq 0$. It is easily shown that 2_0 is not principal in K_0. Hence 2_n cannot be principal in K_n for any $n \geqq 0$.

Finally we must find the exact value of s_∞. It is clear that 2 has a unique prime divisor in $\boldsymbol{B}_n$ for all $n \geqq 0$. For odd primes, the theory of the cyclotomic fields shows the following.

LEMMA 7. *An odd prime* p *is completely decomposed in* $\boldsymbol{B}_{n(p)}/\boldsymbol{Q}$ *and is not decomposed in* $\boldsymbol{B}_\infty/\boldsymbol{B}_{n(p)}$, *where* $n(p) = -3 + e^{(2)}(p^2 - 1)$.

If a prime p is ramified in $K/\boldsymbol{Q}$, every prime ideal of $\boldsymbol{B}_n$ dividing p must be ramified in $K_n/\boldsymbol{B}_n$, and conversely. Therefore s_∞ is the sum of the decomposition numbers in $\boldsymbol{B}_\infty/\boldsymbol{Q}$ of all the ramified primes in $K/\boldsymbol{Q}$, that is,

$$s_\infty = \begin{cases} \sum_{p|m} 2^{n(p)} & \text{if} \quad m \equiv 3 \pmod 4 . \\ 1 + \sum_{p|m} 2^{n(p)} & \text{if} \quad m \equiv 1 \pmod 4 . \end{cases}$$

Consequently we get the following theorem.

THEOREM 1. *Let* $K = \boldsymbol{Q}(\sqrt{-m})$ *or* $\boldsymbol{Q}(\sqrt{-2m})$, *where* m *is a square-free odd integer bigger than* 3, *and let* X *be the Iwasawa module for the cyclotomic* $\boldsymbol{Z}_2$*-extension of* K. *Then as an abelian group*

$$X \cong \begin{cases} \boldsymbol{Z}_2^\lambda & \text{if} \quad m \equiv 3 \pmod 4 , \\ \boldsymbol{Z}_2^\lambda \oplus T & \text{if} \quad m \equiv 1 \pmod 4 , \end{cases}$$

where T *is a non-trivial finite cyclic* 2*-group and in both cases,* $\lambda = -1 + \sum_{p|m} 2^{n(p)}$, *where* $n(p) = -3 + e^{(2)}(p^2 - 1)$.

4. Next we shall find a value of n_0 satisfying (1). As usual, let $\Gamma = \mathrm{Gal}(K_\infty/K)$ and let γ be a fixed topological generator of Γ, and put $\gamma_n = \gamma^{2^n}$, $\omega_n = 1 - \gamma_n$ for each $n \geqq 0$.

When $m \equiv 3 (\mathrm{mod}\ 4)$, X is torsion-free as an abelian group. Iwasawa's argument in [2] Sections 3-2, 7-4 and 7-5 really shows that we can take n_0 to be $s+1$ if $2X \supset \omega_s X$. In general, $d^{(2)}X \geqq d^{(2)}\{X/\omega_n X\} \geqq d^{(2)}A_n$ for all $n \geqq 0$. Thus if $d^{(2)}X = d^{(2)}A_s$, $[X: 2X] = d^{(2)}\{X/\omega_s X\} = [X: 2X]/[\omega_s X: \omega_s X \cap 2X]$, that is $2X \supset \omega_s X$. From the preceding section, $d^{(2)}A_s = d^{(2)}X$ if $s \geqq \max_{p|m} n(p)$. Therefore we can take n_0 to be $1+\max_{p|m} n(p)$.

When $m \equiv 1 \pmod 4$, X has torsion as an abelian group, but is strictly-finite as a Γ-module.

LEMMA 8. *The projection from $\prod_{n=0}^{\infty} A_n$ to A_0 induces an injection from T to A_0.*

PROOF. Let c be an element of T of order 2^i. Then since T is cyclic, $2^{i-1}c$ coincides with c^* of Lemma 6. Taking the 0-th factors, we get $2^{i-1}c_0 = c(2_0)$. We are done since $c(2_0)$ is of order 2 in A_0.

By this lemma, we have $(T+\omega_n X)/\omega_n X \cong T$ for all $n \geqq 0$. Let $X^* = X/T$, then it holds that $2^{e_n} = [X: \omega_n X] = [X^*: \omega_n X^*][T]$ for all $n \geqq 0$. Applying Iwasawa's method to X^*, we can get the same result as that in the preceding case.

THEOREM 2. *Let the notations be as in the introduction and Theorem 1. Then it holds that*

$$e_n = \lambda n + c \qquad \text{for all} \quad n \geqq 1 + \max_{p|m} n(p).$$

REFERENCES

[1] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257-258.

[2] K. IWASAWA, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., 65 (1959), 183-226.

[3] K. IWASAWA, On the μ-invariants of $\mathbf{Z}_l$-extensions, In: Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, 1-11.

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
YAMAGATA UNIVERSITY
YAMAGATA, 990 JAPAN