H. Osada
Nagoya Math. J.
Vol. 113 (1989), 147–151

NOTE ON THE CLASS-NUMBER OF THE MAXIMAL REAL SUBFIELD OF A CYCLOTOMIC FIELD, II

HIROYUKI OSADA

For an integer $m > 2$, we denote by $C(m)$ and $H(m)$ the ideal class group and the class-number of the field

$$K = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$$

respectively, where ζ_m is a primitive m-th root of unity. Let q be a prime and $k/\boldsymbol{Q}$ be a real cyclic extension of degree q. Let $C(k)$ and $h(k)$ be the ideal class group and the class-number of k. In this paper, we give a relation between $C(k)$ (resp. $h(k)$) and $C(m)$ (resp. $H(m)$) in the case that m is the conductor of k (Main Theorem). As applications of this main theorem, we give the following three propositions. In the previous paper [4], we showed that there exist infinitely many square-free integers m satisfying $n\,|\,H(m)$ for any given natural number n. Using the result of Nakahara [2], we give first an effective sufficient condition for an integer m to satisfy $n\,|\,H(m)$ for any given natural number n (Proposition 1). Using the result of Nakano [3], we show next that there exist infinitely many positive square-free integers m such that the ideal class group $C(m)$ has a subgroup which is isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^2$ for any given natural number n (Proposition 2). In paper [4], we gave some sufficient conditions for an integer m to satisfy $3\,|\,H(m)$ and $m \equiv 1 \pmod 4$. In this paper, using the result of Uchida [5], we give moreover a sufficient condition for an integer m to satisfy $4\,|\,H(m)$ and $m \equiv 3 \pmod 4$ (Proposition 3). Finally, we give numerical examples of some square-free integers m satisfying $4\,|\,H(m)$ and $m \equiv 3 \pmod 4$.

The author would like to thank the referee for his valuable advices.

MAIN THEOREM. *Let q be a prime and $k/\boldsymbol{Q}$ be a real cyclic extension of degree q. If m is the conductor of k, then the ideal class group $C(m)$ has a subgroup which is isomorphic to $C(k)^q$.*

Received August 28, 1987.

https://doi.org/10.1017/S0027763000001306 Published online by Cambridge University Press

Proof. First, we prove this Theorem in the case of $q = 2$. Let $k = \boldsymbol{Q}(\sqrt{n})$ be a real quadratic field, where n is a square-free integer. Let m be the discriminant of k. Hence m is the conductor of k. Now assume that $p_1, p_2, \cdots, p_t$ are all the prime divisors of m. Let k^* be the genus field of k, that is, $k^* = \boldsymbol{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \cdots, \sqrt{p_t^*})$, where if p is an odd prime, then $p^* = (-1)^{(p-1)/2}p$, if $p = 2$, then $p^* = -4$, 8 or -8 according $n \equiv 3 \pmod 4$, $2 \pmod 8$ or $-2 \pmod 8$ (see Ishida [1, Chapter 1]). Let $\tilde{k}$ be the Hilbert class-field of k and $M = k^* \cap \tilde{k}$. Further let H be a subgroup of the ideal class group $C(k)$ of k and H be isomorphic to the Galois group of $\tilde{k}/M$. From [1, Chapter 1], the Galois group of k^*/k is isomorphic to $(Z/2Z)^{t-1}$. Hence $C(k)^2$ is a subgroup of H. On the other hand, since $M = k^* \cap \tilde{k}$, we can see that M is contained in the real cyclotomic field $K = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$. Since k^* is the genus field of k, we have $K \cap \tilde{k} = M$. Hence we have that $K\tilde{k}/K$ is an abelian unramified extension and the Galois group of $K\tilde{k}/K$ is isomorphic to the Galois group of $\tilde{k}/M$. Since the Galois group of $\tilde{k}/M$ is isomorphic to H and H has a subgroup $C(k)^2$, the Galois group of $K\tilde{k}/K$ has a subgroup which is isomorphic to $C(k)^2$. Hence the ideal class group $C(m)$ has a subgroup which is isomorphic to $C(k)^2$.

Next, we prove this Theorem in the case of an odd prime q. Let $k/\boldsymbol{Q}$ be a cyclic extension of degree q. Let $\tilde{k}$ be the Hilbert class field of k and k^* be the genus field of k. Further let H be a subgroup of the ideal class group $C(k)$ of k and H be isomorphic to the Galois group of $\tilde{k}/k^*$. From [1, Theorem 5], we have that the Galois group of k^*/k is isomorphic to $(Z/qZ)^{t-1}$, where t is the number of distinct prime factors of the conductor m of k. It is now easy to see that $C(k)^q$ is a subgruop of H. On the other hand, k^* is contained in the real cyclotomic field $K = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$ (see Ishida [1, Theorem 5]). Since k^* is contained in $\tilde{k}$ and k^* is the genus field of k, we have $K \cap \tilde{k} = k^*$. In the same way as in the proof of this Theorem for the case $q = 2$, we can show that the ideal class group $C(m)$ has a subgroup which is isomorphic to $C(k)^q$.

Remark. Let n be a natural number. Let $h(k)$ be the class-number of k. If $n \mid h(k)$ and $q \nmid n$, then we have $n \mid H(m)$.

LEMMA 1. *If an integer $m = A^{2n} + 4B^{2n} > 5$ is square-free for natural numbers $n > 1$, A, B, the ideal class group of a real quadratic field $\boldsymbol{Q}(\sqrt{m})$ has a cyclic subgroup with order n (see Nakahara [2, Theorem 1]).*

https://doi.org/10.1017/S0027763000001306 Published online by Cambridge University Press

PROPOSITION 1. *If an integer* $m = A^{2n} + AB^{2n} > 5$ *is square-free for natural numbers* $n > 1$, *A, B, then we have*

(1) $n \mid H(m)$, *if n odd,*

(2) $(n/2) \mid H(m)$, *if n is even.*

Proof. It is clear that $m \equiv 1 \pmod 4$. Hence m is the conductor of a real quadratic field $k = \boldsymbol{Q}(\sqrt{m})$. By Lemma 1, the ideal class group $C(k)$ of k has a subgroup which is isomorphic to $\boldsymbol{Z}/n\boldsymbol{Z}$. Hence by Main Theorem, we have this Theorem.

LEMMA 2. *For any given natural number n, there exist infinitely many cubic cyclic fields k whose ideal class groups contain a subgroup isomorphic to* $(\boldsymbol{Z}/n\boldsymbol{Z})^2$ *(see Nakano* [3, *Theorem*]).

Remark. Let m be the conductors of k. From the proof of [3, Theorem], we have $3 \nmid m$, Hence m are square-free integers.

By Lemma 2, we have

COROLLARY. *For any given natural number n, there exist infinitely many cubic cyclic fields k whose ideal class groups* $C(k)$ *contain a subgroup isomorphic to* $(\boldsymbol{Z}/3n\boldsymbol{Z})^2$. *Further the conductors m of k are square-free integers.*

PROPOSITION 2. *For any given natural number n, there exist infinitely many positive square-free integers m such that the ideal class group* $C(m)$ *has a subgroup which is isomorphic to* $(\boldsymbol{Z}/n\boldsymbol{Z})^2$.

Proof. By Corollary of Lemma 2, there exist infinitely many cubic cyclic fields k such that $C(k)^3$ has a subgroup which is isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^2$ for any given natural number n. Let m be the conductors of the cubic cyclic fields k. Hence m are square-free integers. Then by Main Theorem, there exist infinitely many positive square-free integers m such that the ideal class group $C(m)$ has a subgroup which is isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^2$ for any given natural number n. This completes the proof.

LEMMA 3. *Let q be a prime and L/K be a cyclic extension of degree q. Let C(L) and C(K) be the ideal class groups of L and K, respectively. Let h(K) be the order of C(K) and p be a prime such that* $p \nmid qh(K)$. *Further let f be the order of* $p \bmod q$.

If C(L) has a subgroup which is isomorphic to $\boldsymbol{Z}/p^r\boldsymbol{Z}$, *then C(L) has a subgroup which is isomorphic to* $(\boldsymbol{Z}/p^r\boldsymbol{Z})^f$ *for some integer* $r \geqq 1$ *(see*

https://doi.org/10.1017/S0027763000001306 Published online by Cambridge University Press

Washington [6, *Theorem* 10.8]).

Let ℓ be a prime. Let q, q_1 and q_2 be primes which satisfy the following conditions

(1) 2 or 3 is not an ℓ-th power residue mod q for $\ell = 2$,

(2) 2 is not an ℓ-th power residue mod q_i ($i = 1, 2$) and 3 is an ℓ-th power residue mod q_1 but is not an ℓ-th power residue mod q_2 for an odd prime ℓ.

LEMMA 4. *Let n be a natural number. Let $m = (a^{2n} + 27)/4$ for some integer a prime to* 6. *If a has prime factors q, q_1 and q_2 which satisfy the above conditions* (1) *and* (2) *for the prime factors ℓ of n, the ideal class group of the cubic cyclic field defined by*

$$f(x) = x^3 + mx^2 + 2mx + m = 0$$

has a subgroup which is isomorphic to Z/nZ (*see Uchida* [5, *Theorem* 1]).

By Lemma 3 and Lemma 4, we have

COROLLARY. *Under the same assumptions as in Lemma* 4, *the ideal class group of the cubic cyclic field defined by*

$$f(x) = x^3 + mx^2 + 2mx + m = 0$$

has a subgroup which is isomorphic to $Z/nZ \oplus Z/n_0Z$, where $n_0 \mid n$ and any prime factor of n_0 is congruent to 2 (mod 3).

PROPOSITION 3. *Let a be an integer prime to* 6, *and assume that a has a prime factor q such that $q \equiv \pm 5$ (mod 12) or $q \equiv \pm 11$ (mod 24).*

If $m = (a^4 + 27)/4$ is a sequare-free integer, then we see that $4 \mid H(m)$ and $m = 3$ (mod 4).

Proof. It is easy to see that $m \equiv 3$ (mod 4). If $q \equiv \pm 11$ (mod 24), then we have $\left(\frac{2}{q}\right) = -1$. If $q \equiv 5$ (mod 12), then we have $\left(\frac{3}{q}\right) = -1$. Hence by Corollary, the ideal class group of the cubic cyclic field k defined by

$$f(x) = x^3 + mx^2 + 2mx + m = 0$$

has a subgroup which is isomorphic to $(Z/2Z)^2$. Since m is a square-free integer, the discriminant of k is equal to m^2 (see Uchida [5, Lemma 2]). Hence m is the conductor of k. Therefore by Main Theorem, we have $4 \mid H(m)$. This completes the proof.

Now we give some examples of square-free integers m satisfying the conditions in Proposition 3, that is, $4 \mid H(m)$ and $m \equiv 3 \pmod 4$.

163, 607, $19 \cdot 193$, $7 \cdot 1021$, 20887, 32587, $127 \cdot 769$, $7 \cdot 25261$, $373 \cdot 619$, 375163, $103 \cdot 4549$, $7 \cdot 43 \cdot 2347$, $19 \cdot 75853$, 1972627, $379 \cdot 7993$, $313 \cdot 11059$, $19 \cdot 349 \cdot 673$, $577 \cdot 8731$, 8788267, $1789 \cdot 5443$, $7 \cdot 1694941$, $7 \cdot 31 \cdot 60139$, $3259 \cdot 4813$, 17143747, 20362663, $19 \cdot 1480933$, 32769907, 35289547.

References

[1] Ishida, M., The genus fields of algebraic number fields, Lecture Notes in Math., **555**, Berlin, Heidelberg, New York: Springer 1976.

[2] Nakahara, T., On real quadratic fields whose ideal class groups have a cyclic p-subgroup, Rep. Fac. Sci. Engin. Saga Univ., **6** (1978), 91–102.

[3] Nakano, S., Ideal class groups of cubic cyclic fields, Acta Arith., **46** (1986), 297–300.

[4] Osada, H., Note on the class-number of the maximal real subfield of a cyclotomic field, Manuscripta Math., **58** (1987), 215–227.

[5] Uchida, K., Class numbers of cubic cyclic fields, J. Math. Soc. Japan, **26** (1974), 447–453.

[6] Washington, L., Introduction to cyclotomic fields, Graduate Texts in Math., **83**, Berlin, Heidelberg, New York: Springer 1982.

Department of Mathematics
Rikkyo University
Ikebukuro, Tokyo 171, Japan