Osada, H.
Osaka J. Math.
41 (2004), 1–9

ON THE IDEAL CLASS GROUPS OF RAY CLASS FIELDS OF ALGEBRAIC NUMBER FIELDS

HIROYUKI OSADA

(Received June 8, 2001)

For an algebraic number field k, $C(k)$ and $\tilde{k}$ denote the ideal class group and the Hilbert class field of k, respectively. For an abelian group G and an integer m, G^m means the subgroup of G consisting of m-th powers of the elements of G. Let $h(k)$, $R(k)$ and $D(k)$ be the class number, the regulator and the absolute value of the discriminant of k, respectively. For an integer $m > 1$, k_m denotes the class field of k corresponding to ray modulo m. Let ζ_m be a primitive m-th root of unity. Let q be a prime and k/Q be a real cyclic extension of degree q. Let m be the conductor of k. In the paper [5], we showed that $C(Q(\zeta_m + \zeta_m^{-1}))$ has a subgroup which is isomorphic to $C(k)^q$. In this paper we generalize the above result in Theorem 1. And we show that for any given integer $n > 1$, there exist infinitely many mutually prime positive integers m such that
(1) m has at most two different prime factors and any prime factor of m is congruent to $1 \pmod 4$,
(2) $C(Q(\zeta_m + \zeta_m^{-1}))$ has a subgroup which is isomorphic to Z/A_mZ for some integer $A_m > n$
(Corollary of Theorem 3). Further we give some applications of the following Theorem 1.

Theorem 1. *Let L/k be an abelian extension and K be a subfield of L such that K/k is an extension of degree n. Then $C(L)$ has a subgroup which is isomorphic to $C(K)^{nh(k)}$.*

Proof. By Galois theory, we have the following exact sequence

$$\mathrm{Gal}(\tilde{L}/L) \to \mathrm{Gal}(\tilde{K}/K) \to \mathrm{Gal}(L \cap \tilde{K}/K) \to 0.$$

Hence by class field theory, we have the following exact sequence

$$C(L)^{N_{L/K}} \to C(K)^f \to \mathrm{Gal}(L \cap \tilde{K}/K) \to 0,$$

where $N_{L/K}$ is the norm map from $C(L)$ to $C(K)$. Now we write the class groups additively. Let $x \in C(K)$ and $G = \mathrm{Gal}(K/k)$. Since $h(k) \cdot C(k) = 0$, we have that

$\sum_{\sigma\in G}\sigma(h(k)x) = 0$. Hence $nh(k)x = nh(k)x - \sum_{\sigma\in G}\sigma(h(k)x) = \sum_{\sigma\in G}(1-\sigma)h(k)x$. Since $L\cap\tilde{K}/k$ is an abelian extension, the group G acts trivially on $\mathrm{Gal}(L\cap\tilde{K}/K)$ by conjugation. From the G-homomorphism f maps each $(1-\sigma)h(k)x$ to 0, it follows that $f(nh(k)x) = 0$. By exactness, we see that the image $C(L)$ contains $nh(k)x$. Since $N_{L/K}(C(L))$ has a subgroup $C(K)^{nh(k)}$, we see that $C(L)$ has a subgroup which is isomorphic to $C(K)^{nh(k)}$. This completes the proof. □

EXAMPLE. Let $K = Q(\sqrt{145})$ and $L = Q(\zeta_{145} + \zeta_{145}^{-1})$. By $C(K)$ is isomorphic to $Z/4Z$ and Theorem 1, we see that $C(L)$ has a subgroup which is isomorphic to $Z/2Z$. And we see that $L\cap\tilde{K} = Q(\sqrt{5},\sqrt{29})$.

Lemma 1. *For any given integer $r > 1$, let q_i $(1 \leqq i \leqq r-1)$ be odd primes such that $q_1 < q_2 < \cdots < q_{r-1}$. Let $n > q_1$ be an integer and $m = (2nq_1q_2\cdots q_{r-1})^2 + 1$. If m is a square-free integer, then $C(Q(\sqrt{m}))$ has a subgroup which is isomorphic to Z/S_mZ for some integer $S_m > r$.*

Proof. Let $F = Q(\sqrt{m})$ and $u = 2nq_1q_2\cdots q_{r-1}$. Since $n > q_1$ and $q_1 < q_2 < \cdots < q_{r-1}$, we see that $q_1^r < u/2$. Since $m \equiv 1 \pmod{q_1}$, we have that $(q_1) = ßß'$ and $ß \neq ß'$, where ß and $ß'$ are prime ideals in F. Now we assume that $ß^s$ is a principal ideal in F for some positive integer s. Then there exist integers x and y such that

$$ß^s = \left(\frac{x+y\sqrt{m}}{2}\right) \quad \text{and} \quad x \equiv y \pmod 2.$$

Hence we have

$$q_1^s = \left|\frac{x^2-y^2m}{4}\right|,$$

that is,

$$\pm 4q_1^s = x^2 - y^2m.$$

If $y = 0$, then we have $x^2 = 4q_1^s$. Hence s is necessarily $2t$ for some integer t. Since $x = \pm 2q_1^t$, we have

$$ß^{2t} = (q_1^t) = ß^t ß'^t.$$

Therefore we have $ß = ß'$. This contradicts $ß \neq ß'$. Hence we have $y \neq 0$. Let x_0 be an integer and y_0 be the smallest positive integer satisfying

$$ß^s = \left(\frac{x_0+y_0\sqrt{m}}{2}\right),$$

that is,

$$ß^s = \left(\frac{\pm|x_0| + y_0\sqrt{m}}{2}\right).$$

Let $\varepsilon = \pm u + \sqrt{m}$. Since ε are units of F, we have

$$ß^s = \left(\frac{(\pm|x_0| + y_0\sqrt{m})(\mp u + \sqrt{m})}{2}\right),$$

that is,

$$ß^s = \left(\frac{-|x_0|u + y_0 m \pm (|x_0| - y_0 u)\sqrt{m}}{2}\right).$$

From $||x_0| - y_0 u| > 0$ and the definition of y_0, we have

$$||x_0| - y_0 u| \geqq y_0.$$

Hence either $|x_0| - y_0 u \geqq y_0$ or $-|x_0| + y_0 u \geqq y_0$. So either

$$\pm 4q_1^s = x_0^2 - y_0^2 m \geqq y_0^2(u+1)^2 - y_0^2(u^2+1) = 2uy_0^2 \geqq 2u.$$

or

$$\pm 4q_1^s = x_0^2 - y_0^2 m \leqq y_0^2(u-1)^2 - y_0^2(u^2+1) = -2uy_0^2 \leqq -2u.$$

Therefore in each case $4q_1^s \geqq 2u$, that is, $q_1^s \geqq u/2$. If $r \geqq s$, then this contradicts $q_1^r < u/2$. So if $r \geqq s$, $ß^s$ is not a principal ideal in F. Now we assume that $t = S_m$ is the smallest positive integer such that $ß^t$ is a principal ideal in F. From the above argument, we see that $C(F)$ has a subgroup which is isomorphic to $Z/S_m Z$ for some integer $S_m > r$. This completes the proof. □

Lemma 2. *Let $G(n) = an^2 + bn + c$ be an irreducible polynomial with $a > 0$ and $c \equiv 1 \pmod 2$. Then there exist infinitely many integers n such that $G(n)$ has at most two prime factors* (*see Iwaniec* [2, Theorem]).

Theorem 2. *For any given integer $r > 1$, there exist infinitely many mutually prime positive integers m such that*
(1) *m has at most two different prime factors and any prime factor of m is congruent to* $1 \pmod 4$,
(2) *$C(Q(\sqrt{m}))$ has a subgroup which is isomorphic to $Z/S_m Z$ for some integer $S_m > r$.*

Proof. For any given integer $r > 1$, let $m = (2nq_1q_2\cdots q_{r-1})^2 + 1$, where $q_i (1 \leqq i \leqq r-1)$ are odd primes such that $q_1 < q_2 < \cdots < q_{r-1}$ and $n > q_1$ is an integer.

Then by Lemma 2, there exist infinitely many integers n such that m has at most two different prime factors. It is easy to see that any prime factor of m is congruent to 1 (mod 4). Hence by Lemma 1, we have this theorem. □

Theorem 3. *Let k be an algebraic number field. Then for any given integer $n > 1$, there exist infinitely many mutually prime positive integers m such that*
(1) *m has at most two different prime factors and any prime factor of m is congruent to* $1 \pmod 4$,
(2) *$C(k_m)$ has a subgroup which is isomorphic to Z/A_mZ for some integer $A_m > n$.*

Proof. By Theorem 2, for any given integer $r > 1$, there exists a positive integer m such that
(1) m has at most two different prime factors and any prime factor of m is congruent to $1 \pmod 4$,
(2) $C(Q(\sqrt{m}))$ has a subgroup which is isomorphic to Z/S_mZ for some integer $S_m > r$.
Let $F = Q(\sqrt{m})$, $(D(k), m) = 1$ and $K = kF$. Then $C(K)$ has a subgroup which is isomorphic to $C(F)$. By k_m contains K, $[K : k] = 2$ and Theorem 1, we see that $C(k_m)$ has a subgroup which is isomorohic to $C(K)^{2h(k)}$. Hence by Theorem 2, for any given integer $r > 1$, there exist infinitely many mutually prime positive integers m such that
(1) m has at most two different prime factors and any prime factor of m is congruent to $1 \pmod 4$,
(2) $C(k_m)$ has a subgroup which is isomorphic to $2h(k)(Z/S_mZ)$ for some integer $S_m > r$.
Let $r \geqq 2nh(k)$ for any given integer $n > 1$ and $2h(k)(Z/S_mZ) = Z/A_mZ$. Then we have $A_m > n$. Thus this theorem is proved. □

Putting $k = Q$ in Theorem 3, we have

Corollary. *For any given integer $n > 1$, there exist infinitely many mutually prime positive integers m such that*
(1) *m has at most two different prime factors and any prime factor of m is congruent to* $1 \pmod 4$,
(2) *$C(Q(\zeta_m + \zeta_m^{-1}))$ has a subgroup which is isomorphic to Z/A_mZ for some integer $A_m > n$.*

Theorem 4. *Let k be an algebraic number field and $t > 1$ be an integer. Then for any given integer $n_i > 1$ $(1 \leqq i \leqq t)$, there exist infinitely many mutually prime positive integers $m_1, m_2, \ldots, m_t$ such that*
(1) *m_i has at most two different prime factors and any prime factor of m_i is congruent to* $1 \pmod 4$,

(2) *$C(k_{m_1m_2\cdots m_t})$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{t} Z/A_{m_i}Z$ for some integer $A_{m_i} > n_i$.*

Proof. By Theorem 2, for any given integer $r_i > 1$ $(1 \leqq i \leqq t)$, there exist mutually prime positive integers m_i such that
(1) m_i has at most two different prime factors and any prime factor of m_i is congruent to $1 \pmod 4$,
(2) $C(Q(\sqrt{m_i}))$ has a subgroup which is isomorphic to $Z/S_{m_i}Z$ for some integer $S_{m_i} > r_i$.
Let $F = Q(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_t})$. Then $C(F)$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{t} Z/S_{m_i}Z$. Let $(D(k), m_i) = 1$ $(1 \leqq i \leqq t)$ and $K = kF$. Then $C(K)$ has a subgroup which is isomorphic to $C(F)$. By $k_{m_1m_2\cdots m_t}$ contains $K, [K : k] = 2^t$ and Theorem 1, we see that $C(k_{m_1m_2\cdots m_t})$ has a subgroup which is isomorphic to $C(K)^{2^t h(k)}$. Hence by Theorem 2, for any given integer $r_i > 1$ $(1 \leqq i \leqq t)$, there exist infinitely many mutually prime positive integers $m_1, m_2, \ldots, m_t$ such that
(1) m_i has at most two different prime factors and any prime factor of m_i is congruent to $1 \pmod 4$,
(2) $C(k_{m_1m_2\cdots m_t})$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{t} 2^t h(k)(Z/S_{m_i}Z)$ for some integer $S_{m_i} > r_i$.
Let $r_i \geqq 2^t n_i h(k)$ for any given integer $n_i > 1$ and $2^t h(k)(Z/S_{m_i}Z) = Z/A_{m_i}Z$. Then we have $A_{m_i} > n_i$. Thus we have this theorem. □

Putting $k = Q$ in Theorem 4, we have

Corollary. *Let $t > 1$ be an integer. Then for any given integer $n_i > 1$ $(1 \leqq i \leqq t)$, there exist infinitely many mutually prime positive integers $m_1, m_2, \ldots, m_t$ such that*
(1) *m_i has at most two different prime factors and any prime factor of m_i is congruent to $1 \pmod 4$,*
(2) *$C(Q(\zeta_{m_1m_2\cdots m_t} + \zeta_{m_1m_2\cdots m_t}^{-1}))$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{t} Z/A_{m_i}Z$ for some integer $A_{m_i} > n_i$.*

Lemma 3. *Let $n > 1$ be an integer. For given finite sets S_1, S_2, S_3 of primes satisfying $S_i \cap S_j = \phi$ if $i \neq j$, there exist infinitely many imaginary (resp. real) quadratic number fields F such that*
(a) *the ideal class group of F has a subgroup which is isomorphic to $Z/nZ \oplus Z/nZ$ (resp. Z/nZ),*

$$\text{(b) all primes contained in } S_i \begin{cases} \text{are decomposed in } F & (i = 1), \\ \text{remain prime in } F & (i = 2), \\ \text{are ramified in } F & (i = 3) \end{cases}$$

(*see Yamamoto* [8, Theorem 2]).

Theorem 5. *Let k be an algebraic number field and A be any finite abelian group. Then there exist infinitely many mutually prime positive square-free integers t such that*
(1) $t \equiv 1 \pmod 4$,
(2) *$C(k_t)$ has a subgroup which is isomorphic to A.*

Proof. Let A be any finite abelian group. Then A is isomorphic to $\bigoplus_{i=1}^{s} Z/n_i Z$ for some integers $n_i > 1$ and $s \geqq 1$. It suffices to prove this theorem for the case $s > 1$. By Lemma 3, for given integer n_i $(1 \leqq i \leqq s)$, there exist mutually prime positive square-free integers m_i such that
(1) $m_i \equiv 1 \pmod 4$,
(2) $C(Q(\sqrt{m_i}))$ has a subgroup which is isomorphic to $Z/2^s h(k) n_i Z$.
Now we put $t = m_1 m_2 \cdots m_s$. Let $F = Q(\sqrt{m_1}, \sqrt{m_2}, \dots, \sqrt{m_s})$. Let $(D(k), D(F)) = 1$ and $K = kF$. Then $C(K)$ has a subgroup which is isomorphic to $C(F)$ and $C(F)$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{s} Z/2^s h(k) n_i Z$. By k_t contains K, $[K : k] = 2^s$ and Theorem 1, we see that $C(k_t)$ has a subgroup which is isomorphic to $C(K)^{2^s h(k)}$. Hence $C(k_t)$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{s} Z/n_i Z$. Therefore by Lemma 3, we have this theorem. $\square$

Putting $k = Q$ in Theorem 5, we have

Corollary. *Let A be any finite abelian group. Then there exist infinitely many mutually prime positive square-free integers t such that*
(1) $t \equiv 1 \pmod 4$,
(2) *$C(Q(\zeta_t + \zeta_t^{-1}))$ has a subgroup which is isomorphic to A.*

REMARK. $k_m \cap k_n = \tilde{k}$, if $(m, n) = 1$.

The Brauer-Siegel theorem. *Let k be a normal algebraic number field of degree n over Q. Then*

$$\frac{\log(h(k)R(k))}{\log\sqrt{D(k)}} \to 1 \quad \textit{as} \quad \frac{n}{\log D(k)} \to 0$$

(*see Lang* [3, Chapter IX]).

Theorem 6. *Let k be a totally imaginary algebraic number field and $h(k) = 2^s$ for an integer $s \geqq 0$. Let p be an odd prime such that $p \equiv 3 \pmod 4$. Then there exist infinitely many primes p such that for any given integer $n > 1$, $C(k_p)$ has a subgroup which is isomorphic to $C(Q(\sqrt{-p}))$ with $h(Q(\sqrt{-p})) > n$.*

Proof. We assume that $D(k) < p$. Let $F = Q(\sqrt{-p})$ and $K = kF$. Then $C(K)$ has a subgroup which is isomorphic to $C(F)$. By k_p contains K, $[K : k] = 2$ and

Theorem 1, $C(k_p)$ has a subgroup which is isomorphic to $C(K)^{2h(k)}$. From $h(k) = 2^s$ for an integer $s \geqq 0$ and $2 \nmid h(F)$, we see that $C(F)^{2h(k)} = C(F)$. Therefore $C(k_p)$ has a subgroup which is isomorphic to $C(F)$. On the other hand, we see that $R(F) = 1$ and $D(F) = p$. Hence by the Brauer-Siegel theorem, we have

$$\frac{\log h(F)}{\log \sqrt{p}} \to 1 \quad \text{as} \quad p \to \infty.$$

So by Dirichlet's theorem on prime numbers in arithmetic progressions, there exist infinitely many primes p such that for any given integer $n > 1$, $C(k_p)$ has a subgroup which is isomorphic to $C(F)$ with $h(F) > n$. This completes the proof. $\square$

Lemma 4. *There exist infinitely many primes p such that $p|h(Q(\zeta_p))$, that is, $p|B_{2s}$ for some integer s $(2 \leqq 2s \leqq p-3)$, where B_{2s} are the Bernoulli numbers* (*see* [1]).

Lemma 5. *Let p be an odd prime such that $p|h(Q(\zeta_p))$. Let f_p be the number of s satisfying $p|B_{2s}$ $(2 \leqq 2s \leqq p-3)$. Then $C(Q(\zeta_p))$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{f_p} Z/pZ$* (*see Ribet* [6, Main Theorem]).

Theorem 7. *Let k be a totally imaginary algebraic number field and p be an odd prime such that $p|h(Q(\zeta_p))$. Let f_p be as in* Lemma 5. *Then there exist infinitely many primes p such that $C(k_p)$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{f_p} Z/pZ$.*

Proof. Let $D(k) < p$ and $h(k) < p$. Let $F = Q(\zeta_p)$ and $K = kF$. Then $C(K)$ has a subgroup which is isomorphic to $C(F)$. By k_p contains K, $[K : k] = p-1$ and Theorem 1, $C(k_p)$ has a subgroup which is isomorphic to $C(K)^{(p-1)h(k)}$. So by Lemma 4, Lemma 5 and $(h(k)(p-1), p) = 1$, there exist infinitely many primes p such that $C(k_p)$ has a subgroup which is isomorphic to $\bigoplus_{i=1}^{f_p} Z/pZ$. This completes the proof. $\square$

Lemma 6. *Let p be an odd prime such that $p \equiv 2^{a+1}+1 \pmod{2^{a+2}}$ with $a \geqq 1$. Let k and k_0 be the subfields of $Q(\zeta_p)$ such that $[k : Q] = 2^{a+1}$ and $[k_0 : Q] = 2^a$, respectively. And let $h_1 = h(k)/h(k_0)$. Then*

$$\frac{\log h_1}{2^{a-1}\log p} \to 1 \quad \textit{as} \quad p \to \infty.$$

Proof. Let $R(k) = R$ and $R(k_0) = R_0$. Then it is known that $R = 2^{2^a-1}R_0$. By $D(k) = p^{2^{a+1}-1}$, $D(k_0) = p^{2^a-1}$ and the Brauer-Siegel theorem, we have

$$\frac{\log(h(k)R)}{\log \sqrt{D(k)}} \to 1 \quad \text{and} \quad \frac{\log(h(k_0)R_0)}{\log \sqrt{D(k_0)}} \to 1 \quad \text{as} \quad p \to \infty.$$

Since

$$\frac{\log(h(k)R)}{\log\sqrt{D(k)}}=\frac{\log h_1}{\log\sqrt{D(k)}}+\frac{\log(h(k_0)R_0)}{(2^a-1/2)\log p}+\frac{(2^a-1)\log 2}{(2^a-1/2)\log p}$$

and

$$\frac{\log(h(k_0)R_0)}{(2^a-1/2)\log p}=\frac{\log(h(k_0)R_0)}{\log\sqrt{D(k_0)}}\cdot\frac{2^a-1}{2^{a+1}-1},$$

it follows that

$$\frac{\log h_1}{2^{a-1}\log p}\to 1\quad\text{as}\quad p\to\infty.$$

This completes the proof. □

Theorem 8. *Let k be a totally imaginary algebraic number field and $h(k)=2^s$ for an integer $s\geqq 0$. Let p be an odd prime such that $p\equiv 2^{a+1}+1 \pmod{2^{a+2}}$ with $a\geqq 1$. Let F be the subfield of $Q(\zeta_p)$ such that $[F:Q]=2^{a+1}$. Then for any given integer $n>1$, there exist infinitely many primes p such that $C(k_p)$ has a subgroup which is isomorphic to $C(F)$ with $h(F)>n$.*

Proof. Let $D(k)<p$ and $K=kF$. Then $C(K)$ has a subgroup which is isomorphic to $C(F)$. By k_p contains K, $[K:k]=2^{a+1}$ and Theorem 1, $C(k_p)$ has a subgroup which is isomorphic to $C(K)^{2^{a+1}h(k)}$. By genus theory, we see that $2\nmid h(F)$. From $h(k)=2^s$ for an integer $s\geqq 0$ and $2\nmid h(F)$, we see that $C(F)^{2^{a+1}h(k)}=C(F)$. Hence $C(k_p)$ has a subgroup which is isomorphic to $C(F)$. By Lemma 6 and Dirichlet's theorem on prime numbers in arithmetic progressions, for any given integer $n>1$, there exist infinitely many primes p such that $C(k_p)$ has a subgroup which is isomorphic to $C(F)$ with $h(F)>n$. This completes the proof. □

References

[1] Z.I. Borevich and I.R. Shafarevich: Number Theory, Academic Press, London and New York, 1966.

[2] H. Iwaniec: *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), 171–188.

[3] S. Lang: Algebraic numbers, Addison-Wesley, 1964.

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

[5] H. Osada: *Note on the class-number of the maximal real subfield of a cyclotomic field*, II, Nagoya Math. J. **113** (1989), 147–151.

[6] K. Ribet: *A modular construction of unramified p-extensions of $Q(\mu_p)$*, Invent. Math. **34** (1976), 151–162.

[7] T. Takagi: *Über eine Theorie des relativ-Abel'schen Zahlkörpers*, J. Coll. Sci. Imp. Univ. Tokyo. **41** (1920), 1–133.

[8] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

2-14 Kamiitabashi 2-chome
Itabashi-ku, Tokyo
174-0076, Japan