Abstract

Let $L/\mathbb{Q}$ be a cyclic extension of degree $p$ where $p$ is an odd unramified prime in $L/\mathbb{Q}$, and let $p_1, \ldots, p_s$ be the rational primes that are ramified in $L/\mathbb{Q}$. A new method of proof for showing the existence of subgroups in $H(L)_p$, the $p$-part of the class group of $L$, is introduced. It is purely arithmetical in the sense that it is solely based on the $p$th residuacity of $p_i$ modulo $p_j$, $p_i \neq p_j$.

Mathematics Subject Classification: 11R18, 11R20, 11R37, 11A15
Keywords: cyclic extensions, class groups, power residues

1 Introduction and Background

Class groups of number fields play a central role in class field theory due to their connections with unit groups [9], unramified extensions, and other number field invariants. Determining the structure of the class group $H(F)$ of a number field $F$ can be a formidable task and it is one of the main problems in computational number theory. The $p$-part, or the $p$-Sylow subgroup, of $H(F)$ is relevant for example in Iwasawa theory, elliptic curves, and for a long time it was of interest to Fermat’s last theorem due to Kummer’s famous criterion, namely, if $p 
mid |H(Q(\zeta_p))|$ then $x^p + y^p = z^p$ has no nontrivial integer solutions [12]; as customary, for any integer $k \geq 3$, $\zeta_k \in \mathbb{C}$ denotes a primitive $k$th root of unity and $Q(\zeta_k)$ the $k$th cyclotomic field.

Throughout the paper, $L/Q$ denotes a cyclic extension of degree $p$ where $p$ is an odd unramified prime in $L/Q$. One has $H(L) = H(L)_p \oplus H(L)_{\neq p}$ where $H(L)_p$ is the $p$-part of $H(L)$ and $H(L)_{\neq p}$ the prime-to-$p$ part of $H(L)$. The cardinality of $H(L)$, that is, the class number of $L$, is denoted by $h(L)$.

Relevant results needed for the rest of the work are in order. First, the conductor of $L$, that is, the smallest positive integer $n$ such that $L$ is contained in the $n$th cyclotomic field $K = Q(\zeta_n)$, is of the form $n = p_1 \cdots p_s$ where $p_1, \ldots, p_s$ are distinct odd primes with $p_i \equiv 1 \pmod{p}$, $i = 1, \ldots, s$; furthermore, the discriminant of $L$, $\text{Disc}(L)$, equals $n^{p-1}$, see [4, p. 186]. Hence, $p_1, \ldots, p_s$ are precisely the rational primes that are ramified in $L/Q$. Since each one of them ramifies completely, one has $p_i \mathfrak{O}_L = p_i^e$ where $p_i^e$ is the prime ideal of $\mathfrak{O}_L$ lying above $p_i$, $i = 1, \ldots, s$. If $\theta$ is a generator of $\text{Gal}(L/Q)$ and $t = \text{Tr}_{K/L}(\zeta_n)$ then $L$ can be expressed as $L = Q(t)$ and $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis for $L$, see [8, p. 166].

In [6], using class field theory, Gerth III proved that when the rational primes that ramify in $L/Q$ satisfy certain $p$th power residuacity conditions, $H_p(L) \cong (\mathbb{Z}/p\mathbb{Z})^{*-1}$. The contribution of the present paper is a self-contained and new proof that, under the same conditions, $H_p(L)$ contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$ for $r = 1, \ldots, s$. Furthermore, each subgroup is given explicitly, and several examples are provided to illustrate the result.

Before proceeding, we provide a brief history of the subject and introduce further notation. By a theorem of Leopoldt [7], it is known that $p \nmid h(L)$ if and only if exactly one rational prime ramifies in $L/Q$. Conner and Hurrelbrink [3] proved that if $p \mid h(L)$ then exactly two rational primes ramify in $L/Q$. Conversely, by [3, Theorem 26.9], if exactly two primes $p_1$ and $p_2$ ramify and $p \neq p_1, p_2$, then $p \mid h(L)$ if and only if either $p_1$ is not a $p$th power modulo $p_2$ or $p_2$ is not a $p$th power modulo $p_1$. Recall that a rational integer $a$ is a $p$th residue modulo a prime $q$ if $a$ is not divisible by $q$ and the congruence $x^p \equiv a$
(mod q) has a solution [5, Section III]. By Euler’s criterion, a is a pth residue
mod q if and only if $a^{(q-1)/p} \equiv 1 \pmod{q}$ [10, Chapter VII]. By an abuse of
notation, but for convenience, we will write $(a|q)_p = 1$ or $(a|q)_p = -1$ according
to whether a is a pth residue modulo q or not. In regards to more recent work,
an algorithm for computing $H(F)_p$ with $F/Q$ Abelian was proposed in [1].
However, in contrast to the present paper, the assumption in the former is that $p \nmid [F : Q]$.

The main result, namely, Theorem 2, is presented in the next section along
with auxiliary results and examples. The Conclusion is presented in Section
3.

2 $\nu$th Power Residuacity and the Structure of $H(L)_p$

All of $L/Q, p, n, p_1, \ldots, p_s$, and $p_{p_1}, \ldots, p_{p_s}$ remain exactly as defined in the
previous section. Given any fractional ideal $a \in \mathcal{O}_L$, we use $[a]$ to denote the
equivalence class of a in $H(L)$.

\textbf{Lemma 1.} Let $i$ be any integer in $\{1, \ldots, s\}$. If $p_{p_i}$ is principal then $(p_i|p_j)_p = 1$ for all $j$ in $\{1, \ldots, s\} \setminus \{i\}$.

\textit{Proof.} Let $p_{p_i} = (\alpha_i)$ for some $\alpha_i \in \mathcal{O}_L$. Without loss of generality, we may
assume $N_{L/Q}(\alpha_i) = p_i$. For all $j \in \{1, \ldots, s\} \setminus \{i\}$, since $\alpha_i \notin p_{p_j}$, we have
$\alpha_i \equiv c_j \pmod{p_{p_j}}$ for some $c_j \in \{1, \ldots, p_j - 1\}$. Thus,

$$p_i = N_{L/Q}(\alpha_i) = \prod_{k=0}^{p-1} \theta^k(\alpha_i) \equiv c_j^p \pmod{p_{p_j}},$$

whence $c_j^p \equiv p_i \pmod{p_{p_j}}$. \hfill \Box

\textbf{Corollary 1.} If $(p_i|p_j)_p = -1$ for any $i, j$ in $\{1, \ldots, s\}$ with $i \neq j$ then
$[p_{p_i}] \cong (\mathbb{Z}/p\mathbb{Z})$, and consequently $H(L)_p$ is non-trivial.

\textbf{Example 1.} Let $p = 3, p_1 = 7, p_2 = 13$ and $L$ a subfield of $\mathbb{Q}(\zeta_9)$ with
$[L : \mathbb{Q}] = 3$ and conductor 91. By Theorem 26.9 in [3] (as stated in the
Introduction), $|H(L)_3| = 3$. From Corollary 1, $p_7$ is non-principal for $(7|13)_3 = -1$. Thus, $H(L)_3 = \langle p_7 \rangle$. Table 1 lists $H(L)_3$ where $L$ is a subfield of $\mathbb{Q}(\zeta_n)$
with $[L : \mathbb{Q}] = 3$ and conductor $n = p_1p_2$ with $p_1, p_2$ in $\{7, 13, 19, 31, 37, 43\}$,
and $p_1 \neq p_2$. In all cases, $|H(L)_3| = 3$.

\textbf{Example 2.} Let $p = 3, p_1 = 7, p_2 = 13, p_3 = 19, n = p_1p_2p_3 = 1729$, and $L$
a subfield of $\mathbb{Q}(\zeta_n)$ of conductor $n$. Then $p_7, p_{19}$, and $p_{19}$ are all non-principal


\[
\begin{array}{cccccc}
 n & p_1 & p_2 & (p_1|p_2)_3 & (p_2|p_1)_3 & H(L)_3 \\
 91 & 7 & 13 & -1 & 1 & \langle [p_7] \rangle \\
 133 & 7 & 19 & 1 & -1 & \langle [p_{19}] \rangle \\
 217 & 7 & 31 & -1 & -1 & \langle [p_7] \rangle \\
 259 & 7 & 37 & -1 & -1 & \langle [p_7] \rangle \\
 301 & 7 & 43 & -1 & 1 & \langle [p_7] \rangle \\
 247 & 13 & 19 & -1 & -1 & \langle [p_{13}] \rangle \\
 403 & 13 & 31 & -1 & 1 & \langle [p_{13}] \rangle \\
 481 & 13 & 37 & -1 & -1 & \langle [p_{13}] \rangle \\
 559 & 13 & 43 & -1 & -1 & \langle [p_{13}] \rangle \\
 589 & 19 & 31 & -1 & 1 & \langle [p_{19}] \rangle \\
 703 & 19 & 37 & -1 & 1 & \langle [p_{19}] \rangle \\
 817 & 19 & 43 & -1 & -1 & \langle [p_{19}] \rangle \\
 1147 & 31 & 37 & 1 & -1 & \langle [p_{37}] \rangle \\
 1333 & 31 & 43 & -1 & -1 & \langle [p_{31}] \rangle \\
 1591 & 37 & 43 & -1 & 1 & \langle [p_{37}] \rangle \\
\end{array}
\]

Table 1: $H(L)_3$ for certain cubic fields of conductor $p_1p_2$

for $(7|13)_3 = (13|19)_3 = (19|7)_3 = -1$. Thus, $3$ divides $h(L)$. If we can show that $\langle \langle [p_7] \rangle \rangle \neq \langle \langle [p_{13}] \rangle \rangle$, we can immediately conclude that $H(L)_3$ has a subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ and $h(L)$ is a multiple of $3^2$. This will be done after we state and prove a corollary to the next theorem.

**Theorem 1.** [11, p. 184] Let $\Omega$ be a principal fractional ideal of $\mathcal{O}_L$ and $q_1, \ldots, q_r$ prime ideals of $\mathcal{O}_L$. Then $\Omega$ can be written as the quotient $(\alpha)/\langle \beta \rangle$ of two integral principal ideals such that none of the ideals $q_i$, $i = 1, \ldots, r$ divides both $(\alpha)$ and $(\beta)$.

**Corollary 2.** Let $a = p_{p_{11}}^{a_1} \cdots p_{p_{1u}}^{a_u}$ and $b = p_{p_{21}}^{b_1} \cdots p_{p_{2v}}^{b_v}$ where $1 \leq r < i_1 < \cdots < i_u \leq s$ and $1 \leq r < j_1 < \cdots < j_v \leq s$. If $\lbrack a \rbrack = \lbrack b \rbrack$ then

\[
\left( \prod_{\ell=1}^{u} p_{p_{1\ell}}^{a_{\ell}} \right) \left( \prod_{\ell=1}^{v} p_{p_{2\ell}}^{b_{\ell}} \right) = 1 \quad \text{for } k = 1, \ldots, r.
\]

**Proof.** Consider the ideal $\mathcal{J} = \left( \prod_{\ell=1}^{u} p_{p_{1\ell}}^{a_{\ell}} \right) \left( \prod_{\ell=1}^{v} p_{p_{2\ell}}^{b_{\ell}} \right)^{-1}$. By hypothesis, $\mathcal{J} = ((a)/(b))$ for some $a, b \in \mathcal{O}_L, b \neq 0$. By Theorem 1, we may assume that neither $a$ nor $b$ belongs to any of the ideals $p_{p_{11}}, \ldots, p_{p_{1u}}$. On the other hand, taking the (ideal) norm $N(\cdot)$ on both sides of $\prod_{\ell=1}^{u} p_{p_{1\ell}}^{a_{\ell}} = ((a)/(b)) \cdot \prod_{\ell=1}^{v} p_{p_{2\ell}}^{b_{\ell}}$, we obtain

\[
\prod_{\ell=1}^{u} p_{p_{1\ell}}^{a_{\ell}} = N((a)/(b)) \cdot \prod_{\ell=1}^{v} p_{p_{2\ell}}^{b_{\ell}}
\]
For each $1 \leq k \leq r$, there exists $c_k \in \{1, \ldots, p_k - 1\}$ such that $a/b \equiv c_k \pmod{p_k}$, whence $\theta^j(a/b) \equiv c_k \pmod{p_k}$ for $j = 0, \ldots, p - 1$. From $N((a)/(b)) = N_{L/Q}(a/b)$, it follows that

$$N_{L/Q}(a/b) = \prod_{j=0}^{p-1} \theta^j(a/b) \equiv c_k^p \pmod{p_k},$$

that is, $\prod_{\ell=1}^u p_{i\ell}^{c_{\ell}} \equiv c_k^p \cdot \prod_{\ell=1}^v p_{j\ell}^{b_{\ell}} \pmod{p_k},$

and the corollary is proved. \hfill \Box

**Example 3** (Example 2, cont’d). We have already seen that the ideals $p_7, p_{13}$, and $p_{19}$ are non-principal. Now,

(i) $(\frac{19}{p_7})_3 = (10 \mid 19)_3 = -1$, so by Corollary 2, $[p_7] \neq [p_{13}]$.

(ii) $(\frac{13^2}{p_9})_3 = (16 \mid 19)_3 = -1$, so by Corollary 2, $[p_7] \neq [p_{13}]^2$.

In conclusion, $h(L)$ is a multiple of $3^2$. Moreover, $([p_7]) \oplus ([p_{13}])$ is a subgroup of $H(L)_p$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

The next theorem is the main result of the present work. When its hypotheses are satisfied, it immediately provides a method for determining subgroups of $H(L)_p$.

**Theorem 2.** Notation as before, let $p_1, \ldots, p_r$, $2 \leq r \leq s$, be such that

$$(p_1|p_2)_p = \cdots = (p_{k-2}|p_k)_p = 1 \quad \text{and} \quad (p_{k-1}|p_k)_p = -1$$

for $k = 2, \ldots, r$. Then $\langle [p_{p_1}], \ldots, [p_{p_{r-1}}] \rangle \cong (\mathbb{Z}/p\mathbb{Z})^{r-1}$.

**Proof.** We will use induction on $r$. The case $r = 2$ can be handled by Corollary 1, so we will treat the case $2 < r < s$. Assuming that

$$(p_1|p_k)_p = \cdots = (p_{k-2}|p_k)_p = 1 \quad \text{and} \quad (p_{k-1}|p_k)_p = -1$$

for $k = 2, \ldots, r + 1$, we will show that

$$\langle [p_{p_1}], \ldots, [p_{p_{r-1}}], [p_{p_r}] \rangle \cong (\mathbb{Z}/p\mathbb{Z})^r. \quad (1)$$

By Corollary 1, $\langle [p_{p_r}] \rangle \cong (\mathbb{Z}/p\mathbb{Z})$, so the isomorphism in (1) can be justified by showing that $[p_{p_r}] \not\in \langle [p_{p_1}], \ldots, [p_{p_{r-1}}] \rangle$. By way of contradiction, suppose $[p_{p_r}] = [p_{p_1}]^{e_1} \cdots [p_{p_{r-1}}]^{e_{r-1}}$ for some choice of non-negative integers $e_1, \ldots, e_{r-1}$, that is, $[p_{p_r}] = [p_{p_1}]^{e_1} \cdots [p_{p_{r-1}}]^{e_{r-1}}$. By Corollary 2,

$$N \left( \frac{p_{p_1}^{e_1} \cdots p_{p_{r-1}}^{e_{r-1}}}{p_{p_r}} \right) \equiv c_{r+1}^p \pmod{p_{p_{r+1}}},$$

that is, $\prod_{i=1}^{r-1} p_i^{e_i} \equiv c_{r+1}^p \cdot p_r \pmod{p_{r+1}}$

for some $c_{r+1} \in \{1, \ldots, p_{r+1} - 1\}$. Since $(p_i|p_{r+1})_p = 1$ for $i = 1, \ldots, r - 1$, the latter congruence implies $(p_r|p_{r+1})_p = 1$, a contradiction. Thus, $[p_{p_r}] \not\in \langle [p_{p_1}], \ldots, [p_{p_{r-1}}] \rangle$, as desired. \hfill \Box
Example 4. Let $p = 3$, $p_1 = 7, p_2 = 13, p_3 = 19, p_4 = 223, p_5 = 373$, $n = p_1 \cdots p_5 = 143816491$, and $L$ a subfield of $\mathbb{Q}(\zeta_n)$ of conductor $n$. We have:

(i) $(p_1|p_2)_3 = -1$;

(ii) $(p_1|p_3)_3 = 1, (p_2|p_3) = -1$;

(iii) $(p_1|p_4)_3 = (p_2|p_4)_3 = 1, (p_3|p_4)_3 = -1$;

(iv) $(p_1|p_5)_3 = (p_2|p_5)_3 = (p_3|p_5)_3 = 1, (p_4|p_5)_3 = -1$.

By Theorem 2, $H(L)_3$ has a subgroup generated by $[p_7], [p_{13}], [p_{19}], \text{ and } [p_{223}]$. Hence, $h(L)$ is a multiple of $3^4$.

Example 5. Let $p = 5$, $p_1 = 11, p_2 = 31, p_3 = 61, p_4 = 191, p_5 = 541$, $n = p_1 \cdots p_5 = 2149388131$, and $L$ a subfield of $\mathbb{Q}(\zeta_n)$ of conductor $n$. We have:

(i) $(p_1|p_2)_5 = -1$;

(ii) $(p_1|p_3)_5 = 1, (p_2|p_3) = -1$;

(iii) $(p_1|p_4)_5 = (p_2|p_4)_5 = 1, (p_3|p_4)_5 = -1$;

(iv) $(p_1|p_5)_5 = (p_2|p_5)_5 = (p_3|p_5)_5 = 1, (p_4|p_5)_5 = -1$.

By Theorem 2, $H(L)_5$ has a subgroup generated by $[p_{11}], [p_{31}], [p_{61}], \text{ and } [p_{191}]$. Hence, $h(L)$ is a multiple of $5^4$.

3 Conclusion

A method for explicitly determining subgroups of the $p$-part of the class group of $L$ where $L/\mathbb{Q}$ is a cyclic extension of degree $p$ and conductor $n = p_1 \cdots p_s$ with $p_i \equiv 1 \pmod{p}, i = 1, \ldots, s$, was introduced. Its effectiveness relies on the assumption that $p_i$ is a $p$th residue modulo $p_j$ for $j = 1, \ldots, i - 2$, but not a $p$th residue modulo $p_{i-1}$ for $i = 2, \ldots, r$. Despite this limitation, the method allowed us to easily tackle several cases that may have been otherwise computationally challenging even for state-of-the-art algorithms [2]. Therefore, the technique could conceivably be applied prior to those algorithms, hence reducing their computational costs to a reasonable degree. The actual limitation of the presented technique is unknown to us, so we leave this as a topic for future research.
References


Received: August 12, 2016; Published: October 7, 2016