Special units and ideal class groups of extensions of imaginary quadratic fields

BY Byungchul Cha

Department of Mathematics and Computer Science, Hendrix College
Conway, AR 72032, USA.
email: cha@hendrix.edu

(Received 14 December 2005)

1. Introduction

Let $K$ be an imaginary quadratic field, and let $F$ be an abelian extension of $K$, containing the Hilbert class field of $K$. We fix a rational prime $p > 2$ which does not divide the number of roots of unity in the Hilbert class field of $K$. Also, we assume that the prime $p$ does not divide the order of the Galois group $G := \text{Gal}(F/K)$. Let $A_F$ be the ideal class group of $F$, and $E_F$ be the group of global units of $F$. The purpose of this article is to study the Galois module structures of $A_F$ and $E_F$.

More precisely, we fix an irreducible $\mathbb{Z}_p$-representation $\chi$ of $G$, and let $A_F^\chi$ be the $\chi$-part of the Sylow $p$-subgroup of $A_F$. We will show in Theorem 5 that the exponent of $A_F^\chi$ is the least power $p^k$ of $p$ such that, for a certain unit $\rho$ of $F$, the element $\rho^{p^k}$ is a special unit for a certain prime ideal of $F$. (See §2 for the definition of special units.) A similar result for real prime cyclotomic extensions of $\mathbb{Q}$ was proved earlier by Thaine [7].

Let us, temporarily, take $K = \mathbb{Q}$. Also, let $F$ be a real abelian extension of $K$ such that $[F : K]$ is not divisible by the fixed odd prime $p$. Sinnott [6] showed that the orders of the two groups, the $p$-part of $A_F$ and the $p$-part of the quotient of $E_F$ by the subgroup of cyclotomic units in $F$, are the same. However, these two groups are not isomorphic in general. Recently, Seo studied in [4] and [5] the $\text{Gal}(F/K)$-module structures of these groups in detail. Building upon Coleman’s theory of circular distributions [1], as well as Rubin’s notion of special units [2], Seo defines higher special units and conjectures that the $p$-part of the ideal class group of $F$ is isomorphic to the filtration group of global units of $F$ given by its higher special units as $\text{Gal}(F/K)$-modules. (See [4] and [5] for the precise statement of the conjecture.) In giving evidence toward his conjecture, Seo utilizes the Euler system of cyclotomic units to get an upper bound of the orders of ideal class groups, and the aforementioned result of Thaine to get a lower bound. Our work in this paper can be thought of as an attempt to generalize Seo’s program to abelian extensions of imaginary quadratic fields, by providing a counterpart for Thaine’s result in this new setting. In particular, our main theorem (Theorem 5) is a weaker analogue of Theorem 2.1 (i) in [5]. Note, however, that we do not assume that the dimension of the $\mathbb{Z}_p$-representation $\chi$ is one.

2. Definitions

For a number field $R$, we write $\mathcal{O}_R$ for its ring of integers. Throughout this article, we fix the following data:
The group of all special units at $\ell$

Byungchul Cha

Suppose $Z$ for any $F$ is a unique extension $A$ of convenience. We will write $B$ that, if exists an element $\xi$ in $F$ of global units of $E$, we have a natural isomorphism $\xi = \xi \bmod \ell$. Write $G = \text{Gal}(F^\ell/F)$, which is cyclic of order $M$. For each $\ell \in L$, we fix a generator $\sigma_\ell$ of $G_\ell$. We let

$$N_\ell = \sum_{\tau \in G_\ell} \tau = \sum_{i=0}^{M-1} \sigma_\ell^i \in \mathbb{Z}[G_\ell].$$

We now define special units following [7]. See also [2], [3, §1], and [5].

DEFINITION 1. Let $\ell \in L$. An element $\xi \in \mathcal{O}_F$ is called a special unit at $\ell$ if there exists an element $\xi(\ell) \in F(\ell)^\times$ such that

(i) $N_\ell(\xi(\ell)) = 1$.

(ii) There exists a fractional ideal $m_F(\ell)$ of $F(\ell)$ such that the principal ideal of $F(\ell)$ generated by $\xi(\ell)$ is equal to $m_F(\ell)^{(1-\sigma_\ell)^2}$.

(iii) $\xi(\ell) \equiv \xi^{(N(\ell)-1)/M} \bmod \ell$ for all primes above $\ell$.

The group of all special units at $\ell$ will be denoted by $S_F(\ell)$. Also, $\xi$ is called a special unit in $F/K$ if it is a special unit at $\ell$ for all but finitely many $\ell \in L$. The group of all special units in $F/K$ is denoted by $S_F$.

Let $\chi$ be an irreducible $\mathbb{Z}_p$-representation of $G$. We write $e_\chi$ for the $\chi$-idempotent

$$e_\chi := \frac{1}{[F : K]} \sum_{\tau \in G} \text{Tr}(\chi(\tau)) \tau^{-1} \in \mathbb{Z}_p[G].$$

For any $\mathbb{Z}[G]$-module $B$, we define the $\chi$-component $B^\chi$ of $B$ as $B^\chi := e_\chi(B \otimes \mathbb{Z}_p)$. Note that, if $B$ is finite, $B^\chi$ can be regarded as a submodule of $B$.

3. Main Theorem and Proof

Many of our notations are taken from [3], which we reproduce here for the reader’s convenience. We will write $A_F$ for the ideal class group of $F$, and $E_F$ for the group of global units of $F$. The Galois group $G$ acts on both groups, turning them into $G$-modules. Let $E_F$ and $S_F$ be the images of $E_F$ and $S_F$ in $F^\times/(F^\times)^M$ respectively. Then, we have a natural isomorphism $(E_F/S_F)^\times \cong E_F^\times/S_F^\times$. We fix an element $\rho \in E_F^\times$ whose image generates $E_F^\chi/\mu_{p\infty}(F)^\chi$ over $\mathbb{Z}_p[G]^\chi$. Note that $E_F^\chi/\mu_{p\infty}(F)^\chi$ is free, of rank 1 as a $(\mathbb{Z}/M\mathbb{Z})[G]^\chi$-module, (see the proof of Theorem 3.2 in [3]). In particular, the order of $\rho$ in $E_F^\chi/\mu_{p\infty}(F)^\chi$ is equal to $M$.

For any prime $\ell$ of $K$, write $I_\ell = \oplus_{\ell \mid \ell} \mathbb{Z}$. If $y \in F^\times$, then $[y]_\ell$ will mean the projection of the fractional ideal generated by $y$ onto $I_\ell/MI_\ell$. Note that $[y]_\ell$ is well-defined for $y \in F^\times/(F^\times)^M$. 

We will frequently use the following two theorems of Rubin [3, Proposition 2.3 and Theorem 3.1], respectively.

**Theorem 2.** Suppose $\ell \in \mathcal{L}$. There is a unique $G$-equivariant isomorphism

$$
\varphi_\ell : (\mathcal{O}_F/\ell \mathcal{O}_F)^\times/((\mathcal{O}_F/\ell \mathcal{O}_F)^\times)^M \to \mathcal{I}_\ell/\mathcal{M}_\ell
$$

which makes the following diagram commute:

\[
\begin{array}{ccc}
(\mathcal{O}_F/\ell \mathcal{O}_F)^\times/((\mathcal{O}_F/\ell \mathcal{O}_F)^\times)^M & \xrightarrow{x \mapsto (x^{1-\sigma_\ell})^{1/d}} & F(\ell)^\times \\
\varphi_\ell & \downarrow & \downarrow \\
\mathcal{I}_\ell/\mathcal{M}_\ell & \xrightarrow{x \mapsto [x^{\ell}])_\ell} & \\
\end{array}
\]

where $\sigma_\ell$ is the reduction of $x^{1-\sigma_\ell}$ in $\oplus_{\chi} \mathcal{O}_F(\ell)/\chi \simeq \mathcal{O}_F/\ell \mathcal{O}_F$ and $d = (N(\ell)-1)/M$.

**Theorem 3.** Suppose $\chi \neq 1$, $M \in \mathbb{Z}$ is a power of $p$, $\beta \in (F^\times/(F^\times)^M)^\times$, and $\hat{A}$ is a $\mathbb{Z}[G]$-quotient of $A_F^\times$. Let $m$ be the order of $\beta$ in $F^\times/(F^\times)^M$, $W$ the $G$-submodule of $F^\times/(F^\times)^M$ generated by $\beta$, $H$ the unramified extension of $F$ corresponding to $\hat{A}$, and $L = H \cap F(\mu_M,W^{1/M})$. Then, there is a $\mathbb{Z}[G]$-generator $\epsilon'$ of $\text{Gal}(L/F)$ such that for every $\epsilon \in \hat{A}$ whose restriction to $L$ is $\epsilon'$, there are infinitely many primes $\lambda$ of $F$ of degree one such that

(i) the projection of the class of $\lambda$ into $\hat{A}$ is $\epsilon$,

(ii) $N(\ell) \equiv 1 \pmod{M}$, where $\ell$ is the prime of $K$ below $\lambda$,

(iii) $[\beta]_\ell = 0$ and there is a $u \in ((\mathbb{Z}/M\mathbb{Z})[G])^\times$ such that $\varphi_\ell(\beta) = u(M/m)\lambda$.

In order to apply these theorems to our situation, we let $\hat{A} := A_F^\times$ and $\beta := \rho$. The order of $\rho$ in $F^\times/(F^\times)^M$ is equal to $M$. Also, we let $W$ be the $G$-submodule of $F^\times/(F^\times)^M$ generated by $\rho$, $H$ the unramified extension of $F$ corresponding to $\hat{A}$, and $L = H \cap F(\mu_M,W^{1/M})$. Then, by (the proof of) Theorem 3, there exists a $\mathbb{Z}[G]$-generator $\epsilon' \in \text{Gal}(L/F)$.

Next, we want to select an element $c$ of $\hat{A} \simeq \text{Gal}(H/F)$ such that its order is equal to the exponent of $\hat{A}$, and that the restriction of $c$ (regarded as an element of $\text{Gal}(H/F)$) to $L$ is equal to $\epsilon'$.

**Lemma 4.** Suppose that

$$
\mathcal{M} \to \mathcal{M}' \to 0
$$

is an exact sequence of finite $(\mathbb{Z}/M\mathbb{Z})[G]^\times$-modules. Assume that $\mathcal{M}'$ can be generated by $m' \in \mathcal{M}'$ over $(\mathbb{Z}/M\mathbb{Z})[G]^\times$. Then, there exists $m \in \mathcal{M}$ such that its order is equal to the exponent of $\mathcal{M}$ and its image in $\mathcal{M}'$ is equal to $m'$.

**Proof.** Take $x \in \mathcal{M}$ such that its order is equal to the exponent of $\mathcal{M}$. Let $x'$ be the image of $x$ in $\mathcal{M}'$. Then, $x' = r \cdot m'$ for some $r \in (\mathbb{Z}/M\mathbb{Z})[G]^\times$. If $r$ is a unit of $(\mathbb{Z}/M\mathbb{Z})[G]^\times$, then $r^{-1}x$ has the desired property, and we are done. Therefore, assume that $r$ is not a unit. Take $y \in \mathcal{M}$ whose image in $\mathcal{M}'$ is $m'$. If the order of $y$ in $M$ is equal to the exponent of $\mathcal{M}$, then $y$ has the desired property and we are done. Therefore, assume that the order of $y$ in $\mathcal{M}$ is less than the exponent of $\mathcal{M}$. Since $(\mathbb{Z}/M\mathbb{Z})[G]^\times$ is a local ring, the element $1 + r$ in $(\mathbb{Z}/M\mathbb{Z})[G]^\times$ is a unit. Therefore, $(1 + r)^{-1}(x + y) \in \mathcal{M}$ has the desired property.
This lemma enables us to select an element \( \varepsilon \) of \( \mathcal{A}_F^\lambda \) such that its order is equal to the exponent of \( \mathcal{A}_F^\lambda \), and the restriction of \( \varepsilon \) (regarded as an element of \( \text{Gal}(H/F) \)) to \( L \) is equal to \( \varepsilon' \). For these data, we apply Theorem 3 and obtain a prime \( \lambda \) of \( F \) whose degree is one.

We set up some more notations. Until the end of this paper, we use the following:
- \( \lambda \): the prime of \( F \) satisfying the conclusion of Theorem 3.
- \( \ell \): the prime of \( K \) below \( \lambda \).
- \( l \): the rational prime number below \( \ell \).
- \( L \): the field \( F(\ell) \).
- \( \lambda_L \): the unique prime of \( L \) above \( \lambda \).
- \( \rho_0 \): a lift of \( \rho \) in \( E_F \).

Recall that \( \varepsilon \) is an element of \( \mathcal{A}_F^\lambda \) whose order is the same as the exponent of \( \mathcal{A}_F^\lambda \). By Theorem 3, \( \lambda \) is in the class \( \varepsilon \).

We are now ready to state and prove our main theorem. The proof of the theorem will occupy the rest of this article.

**Theorem 5.** The order of \( \varepsilon \) in \( \mathcal{A}_F^\lambda \) is \( p^k \) where \( k \) is the least integer such that \( \rho_0^{p^k} \) is a special unit at \( \ell \).

For an element \( x \in F^\times \), we denote by \((x)\) the principal ideal of \( F \) generated by \( x \). When \( x \) is an element of \( L^\times \), we write \((x)_L\) for the principal ideal of \( L \) generated by \( x \). We extend the elements of \( G \) to \( \text{Gal}(L/K) \) so that \( \sigma_\ell \) commutes with \( G \).

Let \( \xi := \rho_0^{p^k} \). By the definition of \( k \), \( \xi \) is a special unit at \( \ell \); therefore, there exists \( \xi(\ell) \in L^\times \) such that \( N_{L/K}(\xi(\ell)) = 1 \) and \( \xi(\ell) \equiv \xi^{(p^k(p-1))}/M \) modulo all primes above \( \ell \). Also, there exists a fractional ideal \( m_\ell \) of \( L \) such that \( (\xi(\ell))_L = m_\ell^{(1-\sigma_\ell)^2} \). By Hilbert theorem 90, there exists \( \alpha \in \mathcal{O}_L^\times \) with \( \xi(\ell) = \alpha/\alpha^\sigma \). In the diagram in Theorem 2, we see that the element \( \alpha \) is mapped to (the projection of) \( \xi \) in \( (\mathcal{O}_F/\ell\mathcal{O}_F)^\times \)/\( (\mathcal{O}_F/\ell\mathcal{O}_F)^\times \)^\( M \) under the left vertical map. Note that the part (3) of Theorem 3 says that

\[
\varphi_\ell(\rho) = u\lambda
\] (3.1)

for a unit \( u \) of \((\mathbb{Z}/M\mathbb{Z})[G]^\times \). By the commutativity of the diagram, together with (3.1), we have that

\[
[N_\ell \alpha]_\ell = p^k u \cdot \lambda.
\] (3.2)

We calculate \([N_\ell \alpha]_\ell \) in a different way. Let \( m' = m_\ell^{(1-\sigma_\ell)} \). By the definition of \( \alpha \), the fractional ideal \( (\alpha)_L \cdot (m')^{-1} \) is fixed by the action of \( \sigma_\ell \). The only primes ramifying in \( L/F \) are the ones above \( \ell \); therefore, \( (\alpha)_L = m_\ell \cdot m' \cdot \lambda^{\sum_{\sigma \in G} a_{\sigma} \sigma} \) for a fractional ideal \( m \) of \( \mathcal{O}_F \) and for some integers \( a_{\sigma} \). Taking norms from \( L \) to \( F \) of both sides, we obtain

\[
(N_\ell \alpha) = m^M \cdot \lambda^{\sum_{\sigma \in G} a_{\sigma} \sigma}.
\] (3.3)

Recall that \( M \) is taken to be greater than or equal to the exponent of the Sylow \( p \)-group of \( \mathcal{A}_F \). This implies that the ideal class \( (\sum_{\sigma \in G} a_{\sigma} \sigma) \varepsilon \) is equal to zero in \( \mathcal{A}_F^\lambda \). On the other hand, projecting the equation (3.3) onto \( \mathcal{I}_\ell/M\mathcal{I}_\ell \), we get

\[
[N_\ell \alpha]_\ell = \left( \sum_{\sigma \in G} a_{\sigma} \sigma \right) \lambda,
\] (3.4)
as elements of $\mathcal{I}_\ell/M\mathcal{I}_\ell$. From (3.2) and (3.4),
\[ p^k u \cdot \lambda = \left( \sum_{\sigma \in G} a_\sigma \sigma \right) \lambda \]
modulo $M$. This shows that $p^k$ kills the ideal class $uc$, therefore, $c$ as well.

To finish the proof of Theorem 5, we assume, for the sake of contradiction, that $p^{k-1}$ kills $c$, that is, there exists an element $\zeta \in \mathcal{O}_F$ such that $\lambda p^{k-1} = (\zeta)$ as ideals of $\mathcal{O}_F$. In particular, $\zeta$ is a $\lambda$-unit.

**Lemma 6.** Fix an element $\bar{u} \in \mathbb{Z}[G]$ which is congruent to $u$ modulo $M$. There exists an element $\gamma \in L^\times$ such that
\[ (\chi^{\bar{u}}) = (N_{L/F}(\gamma)) \]
as ideals of $F$.

**Proof.** We will show that there exists a unit $y \in \mathcal{O}_F$ such that $y\zeta^{\bar{u}}$ belongs to $N_{L/F}(L^\times)$. By Hasse’s norm theorem, it is sufficient to prove that $y\zeta^{\bar{u}}$ is a local norm at every primes of $F$. Since $L/F$ is unramified outside primes dividing $\ell$, we need to show this only at primes lying above $\ell$.

To simplify notations, we let
\[ \mathcal{O}_{F,M,\ell^\times} := \left( (\mathcal{O}_F/\ell \mathcal{O}_F)^\times / ((\mathcal{O}_F/\ell \mathcal{O}_F)^\times)^M \right)^\times. \]
Since the map $\varphi_\ell$ restricts to an isomorphism of $(\mathbb{Z}/M\mathbb{Z})[G]^{\times}$-modules
\[ \varphi_\ell : \mathcal{O}_{F,M,\ell^\times} \longrightarrow (\mathcal{I}_\ell/M\mathcal{I}_\ell)^\times = (\mathbb{Z}/M\mathbb{Z})[G]^{\times} \times, \]
the equation (3.1) implies that $\rho$ generates $\mathcal{O}_{F,M,\ell^\times}$ over $(\mathbb{Z}/M\mathbb{Z})[G]^{\times}$.

First, we choose an element $\gamma'$ in $L^\times$ such that $\zeta/N_{L/F}(\gamma')$ is a unit at primes dividing $\ell$. This is possible because $\zeta$ is a $\ell$-unit and $L/F$ is totally ramified at primes dividing $\ell$. We let $x$ be the projection of $(\zeta/N_{L/F}(\gamma'))^{\bar{u}}$ in $\mathcal{O}_{F,M,\ell^\times}$. Since (the image of) $\rho$ generates $\mathcal{O}_{F,M,\ell^\times}$ over $(\mathbb{Z}/M\mathbb{Z})[G]^{\times}$ we can select $u_1 \in (\mathbb{Z}/M\mathbb{Z})[G]^{\times}$ such that $x = u_1 \cdot \rho$ as elements of $\mathcal{O}_{F,M,\ell^\times}$. This proves that $\zeta^{\bar{u}}$ is congruent to $\rho_{0}^{-\bar{u}} \cdot N_{L/F}(\gamma'^{\alpha})$ modulo primes over $\ell$ up to an $M$-th power. Note that, by local class field theory, an $M$-th power is always in a norm group at primes over $\ell$. Therefore, $\rho_{0}^{-\bar{u}} \cdot \zeta^{\bar{u}}$ is a norm at primes over $\ell$ and the proof is complete.

Let $\gamma \in L^\times$ be an element satisfying the conclusion in the above lemma. Obviously, we have that
\[ N_{L/F}((\gamma)_L) = \lambda^{\bar{u}p^{k-1}}. \]  
(3.5)
Therefore,
\[ (\gamma)_L = \bar{a}^{1-\sigma} \lambda_L \bar{u}^{\bar{p}^{k-1}} \]
for some fractional ideal $a$ of $L$ not divisible by primes over $\ell$. We define an element $\xi(\ell)'$ of $L^\times$ by
\[ \xi(\ell)' := \gamma^{1-\sigma}. \]
Then, clearly, $N_\ell(\xi(\ell)') = 1$ and $(\xi(\ell))'_L = a^{(1-\sigma)^2}$. Finally, the image of $\gamma$ by the right vertical map in Theorem 2 is, by (3.5), $p^{k-1} u \cdot \lambda$. By the commutativity of the diagram in Theorem 2, $\xi(\ell)'$ is congruent to $\rho_0^{p^{k-1}}$ at primes over $\ell$. This contradicts the definition of $k$; therefore, Theorem 5 is proved.
Acknowledgement. The author is grateful to Professor Soogil Seo for sharing his preprint [5].

REFERENCES