THE STRUCTURE OF THE UNRAMIFIED ABELIAN IWASAWA MODULE OF SOME NUMBER FIELDS

Ali Mouhib
THE STRUCTURE OF THE UNRAMIFIED ABELIAN IWASAWA MODULE OF SOME NUMBER FIELDS

ALI MOUHIB

For a given positive integer \( m \), we determine an explicit infinite family of real quadratic number fields \( F \), such that the unramified abelian Iwasawa module over the \( \mathbb{Z}_2 \)-extension of \( F \), is isomorphic to \((\mathbb{Z}/2\mathbb{Z})^{2m}\).

1. Introduction

Let \( p \) be a prime number and \( \mathbb{Z}_p \) be the ring of \( p \)-adic integers. We denote by \( K \) a number field, \( K_\infty \) be the cyclotomic \( \mathbb{Z}_p \)-extension of \( K \), and for each nonnegative integer \( n \), \( K_n \) be the \( n \)-th layer of \( K_\infty \). For any nonnegative integer \( n \), we denote by \( A_n(K) \) the \( p \)-class group of \( K_n \). We simply denote by \( A(K) := A_0(K) \) the \( p \)-class group of \( K \). The unramified abelian Iwasawa module \( X_\infty(K) \) of \( K \) is defined by

\[
X_\infty(K) := \lim_{\rightarrow} A_n(K),
\]

where the projective limit is defined with respect to the norm mappings. It is well known, by Iwasawa’s results that \( X_\infty(K) \) is a finitely generated torsion \( \Lambda := \mathbb{Z}_p[[T]] \)-module and for large \( n \), we have

\[
|A_n(K)| = p^{\lambda_p(K)n+\mu_p(K)p^n+\nu_p(K)},
\]

where \( \lambda_p(K) \), \( \mu_p(K) \) and \( \nu_p(K) \) are so called Iwasawa invariants of \( K_\infty/K \). In the case where \( K \) is abelian over \( \mathbb{Q} \), we have \( \mu_p(K) = 0 \) [3]. It is conjectured that for totally real number fields \( K \), \( \lambda_p(K) = \mu_p(K) = 0 \) [5]. This conjecture, called Greenberg’s conjecture, is considered as one of the fascinating problems in Iwasawa theory of \( \mathbb{Z}_p \)-extensions. So proving the finiteness of \( X_\infty(K) \), leads us to ask the following questions:

- What about the structure of \( X_\infty(K) \)?
- What is the least nonnegative integer \( n \) such that \( X_\infty(K) \simeq A_n(K) \)?


Keywords: class group, unit group, capitulation problem, \( \mathbb{Z}_2 \)-extension.
We will deal with these questions in a special case of totally real quadratic number fields.

Next, for each group $G$ which is a finitely generated $\mathbb{Z}_p$-module, we denote by $\text{rk}_p(G)$ the $p$-rank of $G$, that is, the dimension of the $\mathbb{F}_p$-vectorial space $G/G^p$.

Note that M. Ozaki [13] constructed a nonexplicit infinite family of cyclic number fields $K$ of degree $p$, verifying Greenberg’s conjecture and such that $\text{rk}_p(X_\infty(K))$ is arbitrarily large.

For $p = 2$, several articles tackled the Greenberg’s conjecture for some totally real quadratic number fields. Precisely, for the prime numbers $\ell$ and $\ell'$, the quadratic number fields $F = \mathbb{Q}(\sqrt{\ell\ell'})$ has been studied intensively, where $\ell$ and $\ell'$ are prime numbers such that $\ell \equiv -\ell' \equiv 1 \pmod{4}$. In particular, Y. Mizusawa [9] proved that for certain quadratic number fields $F$, the Galois groups of the maximal unramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of $F$ are metacyclic pro-2-groups; he also studied the finiteness of $X_\infty(F)$ in relation with Greenberg’s conjecture. Clearly in this case $X_\infty(F)$ is of rank equal to 2. Let us mention the articles [4; 8; 9; 10; 11; 12; 14], where we have found selected explicit totally real quadratic number fields $F$ satisfying Greenberg’s conjecture.

The common point in all these articles is that the unramified abelian Iwasawa module $X_\infty(F)$ for the selected number fields $F$, is of small rank equal to 1 or 2.

Our contribution is to check Greenberg’s conjecture for a new family of fields $F = \mathbb{Q}(\sqrt{\ell\ell'})$. Precisely, we give the structure of $X_\infty(F)$ and determine the least positive integer $m$ from which the groups $A_n(F)$ stabilize. The main result of this article is the following theorem.

**Theorem 1.1.** Let $\ell$ and $\ell'$ be prime numbers such that $\ell \equiv -\ell' \equiv 1 \pmod{4}$, $F = \mathbb{Q}(\sqrt{\ell\ell'})$. Put $v_2(\ell - 1) - 2 = m$ and $v_2(\ell' + 1) - 2 = m'$. Assume that $(\ell/\ell') = -1$ and $m' \geq m$. Then we have

$$A_n(F) \simeq (\mathbb{Z}/2\mathbb{Z})^{2^n} \quad \text{for all } n \leq m \text{ and } X_\infty(F) \simeq A_m(F) \simeq (\mathbb{Z}/2\mathbb{Z})^{2^n}$$

**2. Totally real quadratic number fields verifying Greenberg’s conjecture and the structure of the unramified abelian Iwasawa module**

Let $p$ be a prime number, $K$ a number field and $K_n$ the layers of the cyclotomic $\mathbb{Z}_p$-extension of $K$. For each nonnegative integer $n$, let $L_n$ be the Hilbert $p$-class field of $K_n$ and $L'_n$ be the maximal extension of $K_n$ contained in $L_n$ in which all $p$-adic places of $K_n$ split completely. By class field theory, we have $A_n(K) \simeq \text{Gal}(L_n/K_n)$ and the subgroup $D_n(K)$ of $A_n(K)$ generated by the classes of $p$-adic primes fixes $L'_n$, in order that $\text{Gal}(L_n/L'_n) \simeq D_n(K)$. Also, for any nonnegative integer $n$, we denote by $A'_n(K)$ the group of $p$-ideal $p$-classes of $K_n$, that is, $A_n(K)/D_n(K)$. We simply denote by $A'(K) := A'_0(K)$ the group of $p$-ideal $p$-classes of $K$, that is, $A(K)/D(K)$. We define $L_\infty := \bigcup L_n$, $L'_\infty = \bigcup L'_n$ and the
Iwasawa module $X'_{\infty}(K)$ as the projective limit of the groups $A'_n(K)$ with respect to the norm maps

$$X'_{\infty}(K) = \varprojlim A'_n(K) \simeq \varprojlim Gal(L'_n/K_n) = Gal(L'_{\infty}/K_{\infty}),$$

where the second projective limit is defined with respect to the restriction maps.

Also, we define the group $D_{\infty}(K)$ as the projective limit of the groups $D_n(K)$, with respect to the norm maps

$$D_{\infty}(K) := \varprojlim D_n(K).$$

Let $\gamma$ be a topological generator of $Gal(K_{\infty}/K)$, let $w_0 = T = \gamma - 1$, and for each positive integer $n$, we denote by $w_n = \gamma^{p^n} - 1 = (1 + T)^{p^n} - 1$, $v_n = w_n/w_0$ and $\Lambda = \mathbb{Z}_p[[T]]$ the ring of formal power series, which is a local ring of maximal ideal $(p, T)$.

**Preparation to the proof of the main theorem.** We will prove the following general result giving the least layer of the cyclotomic $\mathbb{Z}_p$-extension of $K$, from which the elementary groups $A'_n(K)/p$ of the layers $K_n$ stabilize.

**Proposition 2.1.** Let $p$ be a prime number and $K$ a number field containing a unique $p$-adic place that is totally ramified in $K_{\infty}$. Suppose there exists a nonnegative integer $m$ such that $\text{rk}_p(A'_m(K)) < p^m$. Then we have

$$X'_{\infty}(K)/p \simeq A'_m(K)/p.$$

**Proof.** Since $K$ contains a unique $p$-adic place which is totally ramified in $K_{\infty}$, then the maximal abelian extension of $K_n$ contained in $L'_{\infty}$ is $K_{\infty}L'_n$, and hence $w_n X'_{\infty}(K)$ fixes $K_{\infty}L'_n$ [6]. We obtain

$$X'_{\infty}(K)/w_0 X'_{\infty}(K) \simeq Gal(K_{\infty}L'_0/K_{\infty}) \simeq Gal(L'_0/K) \simeq A'(K),$$

$$X'_{\infty}(K)/w_n X'_{\infty}(K) \simeq Gal(K_{\infty}L'_n/K_{\infty}) \simeq Gal(L'_n/K_n) \simeq A'_n(K).$$

Let $r$ be a nonnegative integer such that $\text{rk}_p(A'(K)) = r$:

$$A'(K)/p \simeq (\mathbb{Z}/p\mathbb{Z})^r.$$

Hence from Nakayama’s lemma, $X'_{\infty}(K)$ is a finitely generated $\Lambda$-module with $r$ generators. Thus the elementary $p$-group $X'_{\infty}(K)/p$ is a $\mathbb{F}_p[[T]]$-module with $r$ generators:

$$X'_{\infty}(K)/p \simeq \bigoplus_{i=1}^{r} \mathbb{F}_p[[T]]/(T^{n_i}),$$

where $n_i$ are positive integers. Clearly we have

$$\text{rk}_p(X'_{\infty}(K)) = \sum_{i=1}^{r} n_i.$$
As reported above, the groups \( A_n'(K) \) are determined by giving quotient of \( X'_\infty(K) \) over \( w_n \). Hence we obtain
\[
X'_\infty(K)/(p, w_n) \simeq A'_n(K)/p \simeq \bigoplus_{i=1}^{r} \frac{\mathbb{F}_p[[T]]}{(w_n, T^{n_i})}.
\]

Hence
\[
\text{rk}_p(A'_m(K)) = \sum_{i=1}^{r} (\min(\deg(w_m), n_i)) = \sum_{i=1}^{r} (\min(p^{n_i}, n_i)).
\]

The hypothesis, \( \text{rk}_p(A'_m(K)) < p^n \), implies \( n_i < p^{n_i} \) for each \( i = 1, \ldots, r \). We conclude that
\[
\text{rk}_p(X'_\infty(K)) = \sum_{i=1}^{r} n_i = \text{rk}_p(A'_m(K)). \qed
\]

Below we consider the quadratic number field \( F = \mathbb{Q}(\sqrt{\ell \ell'}) \), where \( \ell \) and \( \ell' \) are prime numbers such that \( \ell \equiv -\ell' \equiv 1 \pmod{4} \). Let \( m + 2 \) and \( m' + 2 \) be respectively the 2-adic valuations of \( \ell - 1 \) and \( \ell' + 1 \):
\[
v_2(\ell - 1) - 2 = m \quad \text{and} \quad v_2(\ell' + 1) - 2 = m'.
\]

Clearly in terms of decomposition in the cyclotomic \( \mathbb{Z}_2 \)-extension of \( \mathbb{Q} \), we have \( \mathbb{Q}_m \) and \( \mathbb{Q}_{m'} \) respectively the decomposition fields of \( \ell \) and \( \ell' \).

For each positive integer \( n \), denote \( \alpha_n = 2 \cos(2\pi/2^{n+2}) \). The \( n \)-th layer of the cyclotomic \( \mathbb{Z}_2 \)-extension of \( \mathbb{Q} \) is \( \mathbb{Q}_n = \mathbb{Q}(\alpha_n) \). One can verify that \( \alpha_{n+1} = \sqrt{2 + \alpha_n} \). We have \( N_{\mathbb{Q}_n/\mathbb{Q}}(2 + \alpha_n) = 2 \) and \( (2 + \alpha_n)O_{\mathbb{Q}_n} \) is the unique prime ideal of \( \mathbb{Q}_n \) lying over 2, and hence
\[
2O_{\mathbb{Q}_n} = (2 + \alpha_n)^{2^n}O_{\mathbb{Q}_n}.
\]

Put for each positive integer \( n \), \( \beta_n = 2 + \alpha_n \), so
\[
\beta_{n+1} = 2 + \alpha_{n+1} = 2 + \sqrt{2 + \alpha_n} = 2 + \sqrt{\beta_n}.
\]

Then we have
\[
\mathbb{Q}_n = \mathbb{Q}(\beta_n) \quad \text{and} \quad \mathbb{Q}_{n+1} = \mathbb{Q}_n(\sqrt{\beta_n}).
\]

Next, we denote by \( E_{\mathbb{Q}_n} \) (resp. \( E'_{\mathbb{Q}_n} \)), the group of units (resp. the group of 2-units) of \( \mathbb{Q}_n \). Clearly, the group \( E'_{\mathbb{Q}_n} \) is generated by \( \beta_n \) and \( E_{\mathbb{Q}_n} \).

**Proposition 2.2.** Suppose that \( m' \geq m \). We have:

1. If \( m = 0 \), then \( A'_n(F) = 0 \) for each nonnegative integer \( n \).
2. If \( m \geq 1 \), then \( \frac{1}{2}X'_\infty(F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus 2^{m-1} \), precisely we have
   \[
   A'_n(F) \simeq \frac{1}{2}A'_n(F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus 2^{n} \text{ for all } n \leq m - 1,
   \]
   \[
   A'_n(F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus 2^{m-1} \text{ for all } n \geq m.
   \]
Proof. By genus theory, we have $A(F) \simeq \mathbb{Z}/2\mathbb{Z}$. Since $F$ contains a unique 2-adic place, then $X'_\infty(F)/T \simeq A'(F)$ is cyclic (possible trivial). Suppose that $m = 0$, then $\ell$ is inert in $Q_1$, which is equivalent to $(2/\ell) = -1$. Hence, the 2-adic place of $F$ is inert in $Q(\sqrt{\ell}, \sqrt{\ell'})$ the genus field of $F$, thus $A'(F)$ is trivial. In that case, by Nakayama’s lemma $X'_\infty(F)$ is trivial, then we have (1). Next suppose that $m \geq 1$. Then $\ell$ splits in $Q_1$, so the 2-adic place of $F$ splits in $Q(\sqrt{\ell}, \sqrt{\ell'})$, thus $A'(F)$ is cyclic nontrivial.

On the other hand, since $A(Q_n)$ is trivial, then each class of $A_n(F)$ of order 2 is an ambiguous class relative to the extension $F_n/Q_n$. Hence we obtain

$$\frac{1}{2}A_n(F) \simeq A_n(F)^G \text{ and } \frac{1}{2}A'_n(F) \simeq A'(F)^G,$$

where $G = \text{Gal}(F_n/Q_n)$.

From $A'$ version of ambiguous class number formula applied to the extension $F_n/Q_n$ (see, for instance, [2]), we have, for each nonnegative integer $n$,

$$|A'_n(F)^G| = \begin{cases} 2^{2m+2n}[E'_Q : E'_Q \cap N_{F_n/Q_n}(F_n^*)]^{-1} & \text{for all } n \leq m - 1, \\ 2^{2m+2n}[E'_Q : E'_Q \cap N_{F_n/Q_n}(F_n^*)]^{-1} & \text{for all } m \leq n \leq m', \\ 2^{2m+2n}[E'_Q : E'_Q \cap N_{F_n/Q_n}(F_n^*)]^{-1} & \text{for all } n \geq m'. \end{cases}$$

Hence to compute the unit index $[E'_Q : E'_Q \cap N_{F_n/Q_n}(F_n^*)]$, it suffices to look to the units of $Q_n$ and $\beta_n$ whether or not they are norms in the extension $F_n/Q_n$. Clearly, the unit index $[E'_Q : E'_Q \cap N_{F_n/Q_n}(F_n^*)]$ is less than or equal to $2^{2n+1}$; we will compute this unit index. It is well known that an element $u \in E'_Q$ is a norm in the extension $F_n/Q_n$ if and only if the quadratic norm residue symbol $(u/\ell)/P$ relatively to the extension $F_n/Q_n$, is trivial for each prime ideal $\mathcal{P}$ of $Q_n$ ramified in $F_n$. Note that there is only one 2-adic place $\mathcal{Q}$ of $Q_n$ ramified in $F_n$. Then from the product formula

$$\prod_{\ell \mid \ell'} \left( \frac{u, \ell}{\mathcal{L}} \right) \prod_{\ell \mid \ell'} \left( \frac{u, \ell'}{\mathcal{L}'} \right) \left( \frac{u, \ell'}{\mathcal{Q}} \right) = 1,$$

$u$ is a norm in the extension $F_n/Q_n$ if and only if $\left( \frac{u, \ell}{\mathcal{P}} \right) = 1$, for each prime ideal $\mathcal{P}$ of $Q_n$ dividing $\ell \ell'$. In particular, since each $\ell$-adic (resp. $\ell'$-adic) place $\mathcal{L}$ (resp. $\mathcal{L}'$) of $Q_n$ is unramified in $Q_n(\sqrt{\ell})$ (resp. $Q_n(\sqrt{\ell'})$), and by the fact that $u$ is a 2-unit, we obtain

$$\left( \frac{u, \ell}{\mathcal{L}'} \right) = \sqrt{\ell} \left( \frac{Q_n(\sqrt{\ell\ell'})/Q_m}{\mathcal{L}'} \right)_{-v' \ell'(u)}^{-1} = 1, \quad \left( \frac{u, \ell'}{\mathcal{L}} \right) = \sqrt{\ell'} \left( \frac{Q_m(\sqrt{\ell\ell'})/Q_n}{\mathcal{Q}} \right)_{-v' \ell'(u)}^{-1} = 1,$$

where $\left( \frac{u/\ell}{\mathcal{P}} \right)$ denotes the Artin symbol and $v_\mathcal{P}(\ell(u))$ is the $\mathcal{P}$-adic valuation of the ideal $(u)$ of $Q_n$ generated by $u$, so $v_\mathcal{P}(\ell(u)) = 0$.

Hence, since for each prime ideal $\mathcal{P}$ dividing $\ell \ell'$, we have $\left( \frac{u, \ell}{\mathcal{P}} \right) = \left( \frac{u, \ell'}{\mathcal{P}} \right) \left( \frac{u, \ell'}{\mathcal{P}} \right)$, then $u$ is a norm in the extension $F_n/Q_n$ if and only if $u$ is a norm in the extensions.
\( \mathcal{Q}_n(\sqrt[l]{\ell})/\mathcal{Q}_n \) and \( \mathcal{Q}_n(\sqrt[l]{\ell'})/\mathcal{Q}_n \). Thus, we have the following surjective maps:

\[
\begin{align*}
&f : E_{\mathcal{Q}_n}'/E_{\mathcal{Q}_n}' \cap N_{\mathcal{F}_n}/\mathcal{Q}_n F_{\mathcal{n}}^* \to E_{\mathcal{Q}_n}'/E_{\mathcal{Q}_n}' \cap N_{\mathcal{Q}_n(\sqrt[l]{\ell})}/\mathcal{Q}_n \mathcal{Q}_n(\sqrt[l]{\ell})^* , \\
&E_{\mathcal{Q}_n}/E_{\mathcal{Q}_n} \cap N_{\mathcal{F}_n}/\mathcal{Q}_n F_{\mathcal{n}}^* \to E_{\mathcal{Q}_n}/E_{\mathcal{Q}_n} \cap N_{\mathcal{Q}_n(\sqrt[l]{\ell})}/\mathcal{Q}_n \mathcal{Q}_n(\sqrt[l]{\ell})^* .
\end{align*}
\]

Since \( \mathcal{Q}(\sqrt[l]{\ell'}) \) contains a unique 2-adic place which is totally ramified in the \( \mathbb{Z}_2 \)-extension \( (\mathcal{Q}(\sqrt[l]{\ell'}))_\infty \), then \( X'_n(\mathcal{Q}(\sqrt[l]{\ell'}))/T \simeq A'_0(\mathcal{Q}(\sqrt[l]{\ell'})) \), which is trivial. Hence \( A'_n(\mathcal{Q}(\sqrt[l]{\ell'})) \) is trivial for each nonnegative integer \( n \). Thus from the ambiguous class number formula applied to the quadratic extension \( \mathcal{Q}_n(\sqrt[l]{\ell})/\mathcal{Q}_n \), we obtain

\[
[E'_{\mathcal{Q}_n} : E_{\mathcal{Q}_n}' \cap N_{\mathcal{Q}_n(\sqrt[l]{\ell})}/\mathcal{Q}_n \mathcal{Q}_n(\sqrt[l]{\ell})^* ] = \begin{cases} 2^{2n} & \text{for all } n \leq m' , \\ 2^{2m'} & \text{for all } n \geq m' . \end{cases}
\]

Similarly, we obtain the maximality of the following unit index for \( n \leq m' \):

\[
[E_{\mathcal{Q}_n} : E_{\mathcal{Q}_n} \cap N_{\mathcal{Q}_n(\sqrt[l]{\ell})}/\mathcal{Q}_n \mathcal{Q}_n(\sqrt[l]{\ell})^* ] = \begin{cases} 2^{2n} & \text{for all } n \leq m' , \\ 2^{2m'} & \text{for all } n \geq m' . \end{cases}
\]

It follows from the above maps that

\[
[E'_{\mathcal{Q}_n} : E_{\mathcal{Q}_n}' \cap N_{\mathcal{F}_n}/\mathcal{Q}_n F_{\mathcal{n}}^* ] \geq \begin{cases} 2^{2n} & \text{for all } n \leq m' , \\ 2^{2m'} & \text{for all } n \geq m' . \end{cases}
\]

\[
[E_{\mathcal{Q}_n} : E_{\mathcal{Q}_n} \cap N_{\mathcal{F}_n}/\mathcal{Q}_n F_{\mathcal{n}}^* ] \geq \begin{cases} 2^{2n} & \text{for all } n \leq m' , \\ 2^{2m'} & \text{for all } n \geq m' . \end{cases}
\]

Therefore, since \( [E_{\mathcal{Q}_n} : E_{\mathcal{Q}_n} \cap N_{\mathcal{F}_n}/\mathcal{Q}_n F_{\mathcal{n}}^* ] \leq 2^n \), we obtain the maximality of the following unit index:

\[
[E_{\mathcal{Q}_n} : E_{\mathcal{Q}_n} \cap N_{\mathcal{F}_n}/\mathcal{Q}_n F_{\mathcal{n}}^* ] = 2^n \quad \text{for all } n \leq m' .
\]

For \( n \leq m - 1 \), from the hypotheses, the \( \ell \)-adic and \( \ell' \)-adic places of \( \mathcal{Q}_n \) split in \( \mathcal{Q}_{n+1} = \mathcal{Q}_n(\sqrt[l]{\beta_n}) \), then for each prime ideal \( \mathcal{P}|\ell \ell' \), by the properties of the norm residue symbol, \( \beta_n \) is a norm in the extension \( \mathcal{F}_n/\mathcal{Q}_n \):

\[
\left(\frac{\beta_n, \ell \ell'}{\mathcal{P}}\right) = \left(\frac{\ell \ell', \beta_n}{\mathcal{P}}\right) = \sqrt{\beta_n} \left(\frac{\mathcal{Q}_n(\sqrt[l]{\beta_n})/\mathcal{Q}_n}{\mathcal{P}}\right)^{-\nu_\mathcal{P}((\ell \ell'))} - 1 = \left(\frac{\mathcal{Q}_{n+1}/\mathcal{Q}_n}{\mathcal{P}}\right)^{-1} (\sqrt[l]{\beta_n}) = 1 ,
\]

where \( \nu_\mathcal{P}((\ell \ell')) = 1 \) is the \( \mathcal{P} \)-adic valuation of the ideal \( (\ell \ell') \) of \( \mathcal{Q}_n \) generated by \( \ell \ell' \). Hence we obtain

\[
[E'_{\mathcal{Q}_n} : E_{\mathcal{Q}_n}' \cap N_{\mathcal{F}_n}/\mathcal{Q}_n (F_{\mathcal{n}}^*) ] = [E_{\mathcal{Q}_n} : E_{\mathcal{Q}_n} \cap N_{\mathcal{F}_n}/\mathcal{Q}_n (F_{\mathcal{n}}^*) ] = 2^{2n} .
\]

It follows from the ambiguous class number formula that

\[
\left|\frac{1}{2} A_n(F)\right| = \left|\frac{1}{2} A'_n(F)\right| = |A'_n(F)^G| = 2^{2n+2n} [E'_{\mathcal{Q}_n} : E_{\mathcal{Q}_n}' \cap N_{\mathcal{F}_n}/\mathcal{Q}_n (F_{\mathcal{n}}^*) ]^{-1} = 2^{2n} .
\]

Hence we obtain (2-1) of Proposition 2.2.
Suppose now that \( n \geq m \), especially when \( n = m \), we have
\[
|A_m' (F)^G| = 2^{2^m+1} [E'_{Q_m} : E'_{Q_m} \cap N_{F_m/Q_m}(F^*_m)]^{-1}.
\]
We will prove that the unit index \([E'_{Q_m} : E'_{Q_m} \cap N_{F_m/Q_m}(F^*_m)]\) is maximal equal to \(2^{2^m+1}\). If we denote by \( U \) a fundamental system of units of \( Q_m \), it suffices to look if the system of the classes of units
\[
\{-1, \beta_m, \bar{\beta} = \bar{u} u | u \in U \}
\]
is a base of the \( \mathbb{F}_2 \)-vectorial space \( E'_{Q_m}/E'_{Q_m} \cap N_{F_m/Q_m}(F^*_m) \). From the equalities
\[
[E'_{Q_m} : E'_{Q_m} \cap N_{Q_m(\sqrt{\ell})/Q_m}(\sqrt{\ell'})^*] = [E_{Q_m} : E_{Q_m} \cap N_{Q_m(\sqrt{\ell})/Q_m}(\sqrt{\ell'})^*] = 2^m,
\]
it is clear that \( \{-1, \bar{\beta} = \bar{u} u | u \in U \} \) is a base of the \( \mathbb{F}_2 \)-vectorial space
\[
E'_{Q_m}/E'_{Q_m} \cap N_{Q_m(\sqrt{\ell})/Q_m}(\sqrt{\ell'})^*.
\]
Therefore, \( \{-1, \bar{\beta}, \bar{u} | u \in U \} \) is a base of the \( \mathbb{F}_2 \)-vectorial space
\[
E'_{Q_m}/E'_{Q_m} \cap N_{F_m/Q_m}(F^*_m).
\]
On the other hand, from the hypotheses, the \( \ell \)-adic places of \( Q_m \) are inert in \( Q_{m+1} \). Hence \( \beta_m \) is not norm in the extension \( F_m/Q_m \), precisely for each \( \ell \)-adic place \( L \) of \( Q_m \), we have
\[
\left( \frac{\beta_m, \ell'}{L} \right) = \left( \frac{\ell', \beta_m}{L} \right) = \sqrt{\beta_m} \left( \frac{Q_m(\sqrt{\ell'})/Q_m}{L} \right)^{\nu_L((\ell'))} = 1.
\]
Hence \( \beta_m \) is not norm in the extension \( F_m/Q_m \).

Also, the \( \ell' \)-adic places of \( Q_m \) are inert in \( Q_{m+1} \) if and only if \( m = m' \). Therefore, one of the following two facts can occur:

(i) In the case where \( m' \geq m + 1 \), for each \( \ell' \)-adic place \( L' \) of \( Q_m \), we have
\[
\left( \frac{\beta_m, \ell'}{L'} \right) = \left( \frac{\ell', \beta_m}{L'} \right) = \sqrt{\beta_m} \left( \frac{Q_m(\sqrt{\ell'})/Q_m}{L'} \right)^{\nu_{L'}((\ell'))} = -1.
\]
Hence, \( \beta_m \) is norm in the extension \( Q_m(\sqrt{\ell'})/Q_m \), so the kernel of the previous map \( f \) is nontrivial. Thus we obtain
\[
\ker(f) = \bar{\beta}_m \mathbb{F}_2.
\]

(ii) In the case where \( m = m' \), for each \( \ell' \)-adic place \( L' \) of \( Q_m \), we have
\[
\left( \frac{\beta_m, \ell'}{L'} \right) = \left( \frac{\ell', \beta_m}{L'} \right) = \sqrt{\beta_m} \left( \frac{Q_m(\sqrt{\ell'})/Q_m}{L'} \right)^{\nu_{L'}((\ell'))} = -1.
\]
Thus \( \beta_m \) is not norm in the extension \( Q_m(\sqrt{\ell'})/Q_m \), so \( \bar{\beta}_m \notin \ker(f) \).
Also, for each $\ell$-adic place $\mathcal{L}$ and $\ell'$-adic place $\mathcal{L}'$ of $\mathbb{Q}_m$, we have
\[
\left(\frac{-1, \ell \ell'}{\mathcal{L}}\right) = \left(\frac{-1, \ell}{\mathcal{L}}\right) = \left(\frac{-1}{\ell}\right) = 1 \quad \text{and} \quad \left(\frac{-1, \ell'}{\mathcal{L}'}\right) = \left(\frac{-1}{\ell'}\right) = -1.
\]
Consequently, in this case, $-\beta_m$ is not norm in the extension $F_m/\mathbb{Q}_m$, but norm in the extension $\mathbb{Q}_m(\sqrt{\ell'})/\mathbb{Q}_m$. Hence the kernel of $f$ is nontrivial:
\[
\ker(f) = -\bar{\beta}_m F_2.
\]
Consequently, we conclude that the system $\{-1, \bar{\beta}_m, \bar{u} | u \in U\}$ is free. Thus, we find
\[
\left|\frac{1}{2} A'_m(F)\right| = |A'_m(F)^G| = 2^{2m+2m} [E'_m : E'_m \cap N_{F_m/\mathbb{Q}_m}(F_m^*)]^{-1} = 2^{2m-1}.
\]
So clearly, $D_m(F)$ is nontrivial. Moreover, since the 2-adic place of $F_m$ is totally ramified in $F_\infty$, then for $n \geq m$, the norm map $D_n(F) \to D_m(F)$ is onto, implies that $D_n(F)$ is nontrivial. Also, since $F_n$ contains a unique 2-adic place and its square is trivial, then we have
\[
D_n(F) \simeq D_m(F) \simeq \mathbb{Z}/2\mathbb{Z}.
\]
Furthermore, since $\text{rk}_2(A'_m(F)) = 2^m - 1 < 2^m$, it follows from Proposition 2.1 that
\[
\frac{1}{2} X'_\infty(F) \simeq \frac{1}{2} A'_m(F) \simeq \frac{1}{2} A'_n(F) \simeq \mathbb{Z}/2\mathbb{Z}^{\oplus 2^{m-1}} \quad \text{for all} \ n \geq m.
\]
In addition, by the ambiguous class number formula we conclude that for each $n \geq m$,
\[
\text{rk}_2(A_n(F)) = \text{rk}_2(A_n(F)^G) = 2^m.
\]

**Corollary 2.3.** We have
\[
X'_\infty(F) \simeq X'_\infty(F) \oplus D'_\infty(F),
\]
where $D'_\infty(F) \simeq \mathbb{Z}/2\mathbb{Z}$.

**Proof.** From Proposition 2.2, for each $n \geq m$, we have
\[
D_n(F) \simeq \mathbb{Z}/2\mathbb{Z}, \quad \text{rk}_2(A'_n(F)) = 2^m - 1 \quad \text{and} \quad \text{rk}_2(A_n(F)) = 2^m.
\]
It follows that $A_n \simeq A'_n \oplus D_n(F)$. Hence, passing to the projective limit with respect to the norm maps, we have the result. \qed

**Proof of the main theorem.** From the hypotheses, we have $A(F) = A'(F) \simeq \mathbb{Z}/2\mathbb{Z}$ and generated by the class of the $\ell$-adic place. By Proposition 2.2, we have $\text{rank}(A'_m(F)) < 2^m$, then $A'(F)$ capitulates in $F_m$ [15, Lemma 7]. Consider the
Also, from Proposition 2.2, we have \( \text{rk} \) of the main theorem, we will determine an infinite family of imaginary biquadratic imaginary quadratic number field \( K \).

Application to the places in \( S \) for each nonnegative integers \( n \) for \( \ell \)-extension of \( \ell \) generated \( 3 \) \( F \) extension of \( \ell \) completely. By class field theory, we have the maximal abelian unramified 2-extension over \( F \) in \( S \) places of \( F \) other notations. For each nonnegative integer \( n \) hence \( X \((t) \) obtained in \( \nu \). On the other hand, since \( A \) is an elementary group isomorphic to \( (\nu \) \( \ell \) is a finitely generated \( \Lambda \)-module and \( w_0 \) is contained in \( (p, T) \), then by Nakayama’s lemma we obtain \( w_m X'(F) = v_m X'(F) = 0 \); hence \( X'(F) \cong A'_m(F) \). Consequently, from Corollary 2.3, we have

\[
X'(F) \cong X'_\infty(F) \oplus D_\infty(F) \cong A_m(F) \cong A'_m(F) \oplus \mathbb{Z}/2\mathbb{Z}.
\]

Also, from Proposition 2.2, we have \( \text{rk}_2(A_{m-1}(F)) = 2^{m-1} < \text{rk}_2(A_m(F)) = 2^m \), then \( X'_\infty(F) \not\cong A_{m-1}(F) \).

Now, we will prove that \( X'_\infty(F) \) is an elementary abelian 2-group. We will use other notations. For each nonnegative integer \( m \), let \( S_n \) be the set of \( \ell' \)-adic places of \( F_n \), and \( D_{S_n} \) the subgroup of \( A_n(F) \) generated by the classes of places in \( S_n \). Let \( A_{S_n} \) be the group of \( S_n \)-classes, that is, \( A_{S_n} := A_n(F)/D_{S_n} \). Let \( M_n \) be the maximal abelian unramified 2-extension over \( F_n \), in which all places of \( S_n \) split completely. By class field theory, we have

\[
\text{Gal}(M_n/F_n) \cong A_{S_n}.
\]

Since \( F \) contains a unique 2-adic place which is totally ramified in \( F_\infty \) and the \( \ell' \)-adic place of \( F \) splits completely in \( F_{m'} \), then the maximal abelian unramified extension of \( F \) contained in \( M_{m'} \) is \( F_{m'} M_0 \). On the other hand, \( A_{S_{m'}} \) is a finitely generated \( \Lambda = \mathbb{Z}_2[[T]] \)-module and \( A_{S_{m'}}/T \cong A_0^{S_0} \). By the hypotheses, we have \( (\ell/\ell') = -1 \), then \( A_0^{S_0} = 0 \) and by Nakayama’s lemma, \( A_{S_{m'}} = 0 \). It follows that for each nonnegative integers \( n \leq m' \), we have \( A_n(F) \cong D_{S_n} \). But, all classes of places in \( S_n \) are trivial or of order 2, then \( A_n(F) \) is an elementary 2-group, thus \( X'_\infty(F) \) is an elementary group isomorphic to \( (\mathbb{Z}/2\mathbb{Z})^{2^m} \). \( \square \)

**Application to the \( \mathbb{Z}_2 \)-torsion of \( X'_\infty(K) \), for some imaginary biquadratic number fields \( K \).** It is well known from the results of Ferrero and Kida \([2; 7]\) that the \( \mathbb{Z}_2 \)-torsion part \( X_0^0(K) \) of the unramified abelian Iwasawa module \( X'_\infty(K) \) of any imaginary quadratic number field \( K \) is trivial or cyclic of order 2. As an application of the main theorem, we will determine an infinite family of imaginary biquadratic...
number fields $K$, in which the $\mathbb{Z}_2$-torsion part of the Iwasawa module $X_\infty(K)$ is an elementary group of arbitrary large rank.

M. Atsuta [1] studied the minus quotient $X^-_\infty(K)$ of the Iwasawa module $X_\infty(K)$ for CM number fields $K$, that is,

$$X^-_\infty(K) = X_\infty(K)/(1+J)X_\infty(K),$$

where $J$ is the complex conjugation. He determined the maximal finite submodule of $X^-_\infty$ under some mild assumptions. Precisely for a CM number field $K$ such that its totally real maximal subfield $K^+$ is unramified at 2 and contains a unique 2-adic place, then $X^-_\infty(K)$ has no nontrivial finite $\Lambda$-submodule [1, Example 2.8].

So from the exact sequence

$$0 \rightarrow X_\infty(K^+) \rightarrow X_\infty(K) \rightarrow X^-_\infty(K) \rightarrow 0,$$

we have the maximal finite $\Lambda$-submodule of $X_\infty(K)$ which coincides with the maximal finite submodule of $X_\infty(K^+)$:

$$X^0_\infty(K) = X^0_\infty(K^+).$$

We reconsider now, the quadratic number field $F = \mathbb{Q}(\sqrt{\ell\ell'})$ of the main Theorem 1.1. Recall that $\ell$ and $\ell'$ are two prime numbers such that

$$\ell \equiv -\ell' \equiv 1 \pmod{4} \quad \text{and} \quad (\ell/\ell') = -1.$$

The positive integers $m$ and $m'$ are defined as

$$v_2(\ell - 1) - 2 = m \quad \text{and} \quad v_2(\ell' + 1) - 2 = m' \quad (m' \geq m).$$

Then we have:

**Proposition 2.4.** For the imaginary biquadratic number field $K = F(i)$, we have the structure of the unramified abelian Iwasawa module $X_\infty(K)$ of $K$:

$$X_\infty(K) \simeq \mathbb{Z}_2^{\lambda_2(K)} \oplus X^0_\infty(K),$$

where $\lambda_2(K) = 2^m + 2^{m'} - 1$ and $X^0_\infty(K) \simeq X_\infty(F) \simeq (\mathbb{Z}/2\mathbb{Z})^{2^m}$.

**Proof.** From Kida’s formula [7, Theorem 3], we see immediately that

$$\lambda(K) = 2^m + 2^{m'} - 1.$$

On the other hand, since the quadratic extension $K/K^+$ (here $K^+ = F$) is unramified at 2-adic primes, then $X^-_\infty(K)$ has no nontrivial $\Lambda$-submodule [1, Corollary 1.4]. Hence, the $\mathbb{Z}_2$-torsion $X^0_\infty(K)$ of the Iwasawa module $X_\infty(K)$ coincides with the Iwasawa module $X_\infty(F)$:

$$X^0_\infty(K) = X_\infty(F).$$
Consequently from Theorem 1.1, we obtain
\[ X_\infty(K) \simeq \mathbb{Z}_2^{2^m + 2^{m'} - 1} \oplus (\mathbb{Z}/2\mathbb{Z})^{2^m}. \]

Acknowledgement

The author is grateful to the referee for careful reading of the manuscript and for valuable comments and suggestions for the improvement of this article.

References


[8] N. Kumakawa, “On the Iwasawa \( \lambda \)-invariant of the cyclotomic \( \mathbb{Z}_2 \)-extension of \( \mathbb{Q}(\sqrt{pq}) \) and the 2-part of the class number of \( \mathbb{Q}(\sqrt{pq}, \sqrt{2 + \sqrt{2}}) \)”, *Int. J. Number Theory* 17:4 (2021), 931–958. MR Zbl


Received October 25, 2022. Revised February 28, 2023.
ALI MOUHIB
DEPARTMENT OF MATHEMATICS
SCIENCES AND ENGINEERING LABORATORY
POLYDISCIPLINARY FACULTY OF TAZA
SIDI MOHAMED BEN ABDELLAH UNIVERSITY
TAZA-GARE
MOROCCO
ali.mouhib@usmba.ac.ma
Combinatorial properties of nonarchimedean convex sets  
ARTEM CHERNIKOV and ALEX MENNEN  

Generalisations of Hecke algebras from loop braid groups  
CELESTE DAMIANI, PAUL MARTIN and ERIC C. ROWELL  

Backström algebras  
YURIY DROZD  

Rigidity of 3D spherical caps via $\mu$-bubbles  
YUHAO HU, PENG LIU and YUGUANG SHI  

The deformation space of Delaunay triangulations of the sphere  
YANWEN LUO, TIANQI WU and XIAOPING ZHU  

Nonexistence of negative weight derivations of the local $k$-th Hessian algebras associated to isolated singularities  
GUORUI MA, STEPHEN S.-T. YAU and HUAIQING ZUO  

The structure of the unramified abelian Iwasawa module of some number fields  
ALI MOUHIB  

Conjugacy classes of $\pi$-elements and nilpotent/abelian Hall $\pi$-subgroups  
NGUYEN N. HUNG, ATTILA MARÓTI and JUAN MARTÍNEZ  

The classification of nondegenerate uniconnected cycle sets  
WOLFGANG RUMP