Pacific Journal of Mathematics

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

ALI MOUHIB

Volume 323 No. 1 March 2023

PACIFIC JOURNAL OF MATHEMATICS
Vol. 323, No. 1, 2023
https://doi.org/10.2140/pjm.2023.323.173

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 $(\mathbb{Z}/2\mathbb{Z})^{2^m}$.

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_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K, and for each nonnegative integer n, K_n be the n-th layer of K_∞. 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

$$X_\infty(K) := \varprojlim A_n(K),$$

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_∞/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 $X_\infty(K) \simeq A_n(K)$?

MSC2020: 11R23, 11R29, 11R32, 11R37.
Keywords: class group, unit group, capitulation problem, 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 $\mathrm{rk}_p(G)$ 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 $\mathrm{rk}_p(X_\infty(K))$ 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 ℓ and ℓ', the quadratic number fields $F = \mathbb{Q}(\sqrt{\ell\ell'})$ has been studied intensively, where ℓ and ℓ' 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 ℓ and ℓ' be prime numbers such that $\ell \equiv -\ell' \equiv 1 \pmod 4$, $F = \boldsymbol{Q}(\sqrt{\ell\ell'})$. 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*

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

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 $A_n(K) \simeq \mathrm{Gal}(L_n/K_n)$ and the subgroup $D_n(K)$ of $A_n(K)$ generated by the classes of p-adic primes fixes L'_n, in order that $\mathrm{Gal}(L_n/L'_n) \simeq D_n(K)$. 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

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

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 γ be a topological generator of $\mathrm{Gal}(K_\infty/K)$, let $w_0 = T = \gamma - 1$, and for each positive integer n, we denote by $w_n = \gamma^{p^n} - 1 = (1+T)^{p^n} - 1$, $\nu_n = w_n/w_0$ 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_∞. Suppose there exists a nonnegative integer m such that* $\mathrm{rk}_p(A'_m(K)) < p^m$. *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_∞, then the maximal abelian extension of K_n contained in L'_∞ is $K_\infty L'_n$, and hence $w_n X'_\infty(K)$ fixes $K_\infty L'_n$ [6]. We obtain

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

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

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

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

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

where n_i are positive integers. Clearly we have

$$\mathrm{rk}_p(X'_\infty(K)) = \sum_{i=1}^{r} n_i.$$

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

$$\mathrm{rk}_p(A'_m(K)) = \sum_{i=1}^{r}\big(\min(\deg(w_m), n_i)\big) = \sum_{i=1}^{r}\big(\min(p^m, n_i)\big).$$

The hypothesis, $\mathrm{rk}_p(A'_m(K)) < p^m$, implies $n_i < p^m$ for each $i = 1, \ldots, r$. We conclude that

$$\mathrm{rk}_p(X'_\infty(K)) = \sum_{i=1}^{r} n_i = \mathrm{rk}_p(A'_m(K). \qquad \square$$

Below we consider the quadratic number field $F = \boldsymbol{Q}(\sqrt{\ell\ell'})$, where ℓ and ℓ' 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 $\boldsymbol{Q}$, we have $\boldsymbol{Q}_m$ and $\boldsymbol{Q}_{m'}$ respectively the decomposition fields of ℓ and ℓ'.

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 $\boldsymbol{Q}$ is $\boldsymbol{Q}_n = \boldsymbol{Q}(\alpha_n)$. One can verify that $\alpha_{n+1} = \sqrt{2+\alpha_n}$. We have $N_{\boldsymbol{Q}_n/\boldsymbol{Q}}(2+\alpha_n) = 2$ and $(2+\alpha_n)o_{\boldsymbol{Q}_n}$ is the unique prime ideal of $\boldsymbol{Q}_n$ lying over 2, and hence

$$2o_{\boldsymbol{Q}_n} = (2+\alpha_n)^{2^n} o_{\boldsymbol{Q}_n}.$$

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

$$\boldsymbol{Q}_n = \boldsymbol{Q}(\beta_n) \quad \text{and} \quad \boldsymbol{Q}_{n+1} = \boldsymbol{Q}_n(\sqrt{\beta_n}).$$

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

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*

(2-1) $$\tfrac{1}{2}A_n(F) \simeq \tfrac{1}{2}A'_n(F) \simeq \mathbb{Z}/2\mathbb{Z}^{\oplus 2^n} \quad \textit{for all } n \leq m-1,$$

(2-2) $D_n \simeq \mathbb{Z}/2\mathbb{Z}$, $\frac{1}{2}A'_n(F) \simeq \mathbb{Z}/2\mathbb{Z}^{\oplus 2^m - 1}$, $\frac{1}{2}A_n(F) \simeq \mathbb{Z}/2\mathbb{Z}^{\oplus 2^m}$ *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 ℓ is inert in $\boldsymbol{Q}_1$, which is equivalent to $(2/\ell) = -1$. Hence, the 2-adic place of F is inert in $\boldsymbol{Q}(\sqrt{\ell}, \sqrt{\ell'})$ 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 ℓ splits in $\boldsymbol{Q}_1$, so the 2-adic place of F splits in $\boldsymbol{Q}(\sqrt{\ell}, \sqrt{\ell'})$, thus $A'(F)$ is cyclic nontrivial.

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

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

where $G = \mathrm{Gal}(F_n/\boldsymbol{Q}_n)$.

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

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

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

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

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

$$\left(\frac{u, \ell}{\mathcal{L}'}\right) = \sqrt{\ell}^{\left(\frac{\boldsymbol{Q}_m(\sqrt{\beta_m})/\boldsymbol{Q}_m}{\mathcal{L}'}\right)^{-v_{\mathcal{L}'}((u))}-1} = 1, \quad \left(\frac{u, \ell'}{\mathcal{L}}\right) = \sqrt{\ell'}^{\left(\frac{\boldsymbol{Q}_m(\sqrt{\beta_m})/\boldsymbol{Q}_m}{\mathcal{L}}\right)^{-v_{\mathcal{L}}((u))}-1} = 1,$$

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

Hence, since for each prime ideal $\mathcal{P}$ dividing $\ell\ell'$, we have $\left(\frac{u, \ell\ell'}{\mathcal{P}}\right) = \left(\frac{u, \ell}{\mathcal{P}}\right)\left(\frac{u, \ell'}{\mathcal{P}}\right)$, then u is a norm in the extension $F_n/\boldsymbol{Q}_n$ if and only if u is a norm in the extensions

$\boldsymbol{Q}_n(\sqrt{\ell})/\boldsymbol{Q}_n$ and $\boldsymbol{Q}_n(\sqrt{\ell'})/\boldsymbol{Q}_n$. Thus, we have the following surjective maps:

$$\begin{aligned} f: E'_{\boldsymbol{Q}_n}/E'_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}F_n^* &\twoheadrightarrow E'_{\boldsymbol{Q}_n}/E'_{\boldsymbol{Q}_n}\cap N_{\boldsymbol{Q}_n(\sqrt{\ell'})/\boldsymbol{Q}_n}\boldsymbol{Q}_n(\sqrt{\ell'})^*,\\ E_{\boldsymbol{Q}_n}/E_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}F_n^* &\twoheadrightarrow E_{\boldsymbol{Q}_n}/E_{\boldsymbol{Q}_n}\cap N_{\boldsymbol{Q}_n(\sqrt{\ell'})/\boldsymbol{Q}_n}\boldsymbol{Q}_n(\sqrt{\ell'})^*.\end{aligned}$$

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

$$[E'_{\boldsymbol{Q}_n}:E'_{\boldsymbol{Q}_n}\cap N_{\boldsymbol{Q}_n(\sqrt{\ell'})/\boldsymbol{Q}_n}\boldsymbol{Q}_n(\sqrt{\ell'})^*]=\begin{cases}2^{2^n} & \text{for all } n\le m',\\ 2^{2^{m'}} & \text{for all } n\ge m'.\end{cases}$$

Similarly, we obtain the maximality of the following unit index for $n\le m'$:

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

It follows from the above maps that

$$[E'_{\boldsymbol{Q}_n}:E'_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}F_n^*]\ge\begin{cases}2^{2^n} & \text{for all } n\le m',\\ 2^{2^{m'}} & \text{for all } n\ge m',\end{cases}$$

$$[E_{\boldsymbol{Q}_n}:E_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}F_n^*]\ge\begin{cases}2^{2^n} & \text{for all } n\le m',\\ 2^{2^{m'}} & \text{for all } n\ge m'.\end{cases}$$

Therefore, since $[E_{\boldsymbol{Q}_n}:E_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}F_n^*]\le 2^{2^n}$, we obtain the maximality of the following unit index:

$$[E_{\boldsymbol{Q}_n}:E_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}F_n^*]=2^n \quad \text{for all } n\le m'.$$

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

$$\left(\frac{\beta_n,\ell\ell'}{\mathcal{P}}\right)=\left(\frac{\ell\ell',\beta_n}{\mathcal{P}}\right)=\sqrt{\beta_n}^{\left(\frac{\boldsymbol{Q}_n(\sqrt{\beta_n})/\boldsymbol{Q}_n}{\mathcal{P}}\right)^{-v_{\mathcal{P}}((\ell\ell'))}-1}=\frac{\left(\frac{\boldsymbol{Q}_{n+1}/\boldsymbol{Q}_n}{\mathcal{P}}\right)^{-1}(\sqrt{\beta_n})}{\sqrt{\beta_n}}=1,$$

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

$$[E'_{\boldsymbol{Q}_n}:E'_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}(F_n^*)]=[E_{\boldsymbol{Q}_n}:E_{\boldsymbol{Q}_n}\cap N_{F_n/\boldsymbol{Q}_n}(F_n^*)]=2^{2^n}.$$

It follows from the ambiguous class number formula that

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

Hence we obtain (2-1) of Proposition 2.2.

Suppose now that $n \geq m$, especially when $n = m$, we have

$$|A'_m(F)^G| = 2^{2^{m+1}}[E'_{\boldsymbol{Q}_m} : E'_{\boldsymbol{Q}_m} \cap N_{F_m/\boldsymbol{Q}_m}(F_m^*)]^{-1}.$$

We will prove that the unit index $[E'_{\boldsymbol{Q}_m} : E'_{\boldsymbol{Q}_m} \cap N_{F_m/\boldsymbol{Q}_m}(F_m^*)]$ is maximal equal to 2^{2^m+1}. If we denote by U a fundamental system of units of $\boldsymbol{Q}_m$, it suffices to look if the system of the classes of units

$$\{\overline{-1}, \bar{\beta}_m, \bar{u} \mid u \in U\}$$

is a base of the $\mathbb{F}_2$-vectorial space $E'_{\boldsymbol{Q}_m}/E'_{\boldsymbol{Q}_m} \cap N_{F_n/\boldsymbol{Q}_m}(F_m^*)$. From the equalities

$$[E'_{\boldsymbol{Q}_m} : E'_{\boldsymbol{Q}_m} \cap N_{\boldsymbol{Q}_m(\sqrt{\ell'})/\boldsymbol{Q}_m}\boldsymbol{Q}_m(\sqrt{\ell'})^*] = [E_{\boldsymbol{Q}_m} : E_{\boldsymbol{Q}_m} \cap N_{\boldsymbol{Q}_m(\sqrt{\ell'})/\boldsymbol{Q}_m}\boldsymbol{Q}_m(\sqrt{\ell'})^*] = 2^m,$$

it is clear that $\{\overline{-1}, \bar{u} \mid u \in U\}$ is a base of the $\mathbb{F}_2$-vectorial space

$$E'_{\boldsymbol{Q}_m}/E'_{\boldsymbol{Q}_m} \cap N_{\boldsymbol{Q}_m(\sqrt{\ell'})/\boldsymbol{Q}_m}\boldsymbol{Q}_m(\sqrt{\ell'})^*.$$

Therefore, $\{\overline{-1}, \bar{u} \mid u \in U\}$, is a free system of the $\mathbb{F}_2$-vectorial space

$$E'_{\boldsymbol{Q}_m}/E'_{\boldsymbol{Q}_m} \cap N_{F_n/\boldsymbol{Q}_m}(F_m^*).$$

On the other hand, from the hypotheses, the ℓ-adic places of $\boldsymbol{Q}_m$ are inert in $\boldsymbol{Q}_{m+1}$. Hence β_m is not norm in the extension $F_m/\boldsymbol{Q}_m$, precisely for each ℓ-adic place $\mathcal{L}$ of $\boldsymbol{Q}_m$, we have

$$\left(\frac{\beta_m, \ell\ell'}{\mathcal{L}}\right) = \left(\frac{\ell\ell', \beta_m}{\mathcal{L}}\right) = \sqrt{\beta_m}^{\left(\frac{\boldsymbol{Q}_m(\sqrt{\beta_m})/\boldsymbol{Q}_m}{\mathcal{L}}\right)^{-v_{\mathcal{L}}((\ell\ell'))}-1} = \sqrt{\beta_m}^{\left(\frac{\boldsymbol{Q}_{m+1}/\boldsymbol{Q}_m}{\mathcal{L}}\right)^{-1}-1} = -1.$$

Hence β_m is not norm in the extension $F_m/\boldsymbol{Q}_m$.

Also, the ℓ'-adic places of $\boldsymbol{Q}_m$ are inert in $\boldsymbol{Q}_{m+1}$ 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 ℓ'-adic place $\mathcal{L}'$ of $\boldsymbol{Q}_m$, we have

$$\left(\frac{\beta_m, \ell'}{\mathcal{L}'}\right) = \left(\frac{\ell', \beta_m}{\mathcal{L}'}\right) = \sqrt{\beta_m}^{\left(\frac{\boldsymbol{Q}_m(\sqrt{\beta_m})/\boldsymbol{Q}_m}{\mathcal{L}'}\right)^{-v_{\mathcal{L}'}((\ell'))}-1} = \sqrt{\beta_m}^{\left(\frac{\boldsymbol{Q}_{m+1}/\boldsymbol{Q}_m}{\mathcal{L}'}\right)^{-1}-1} = 1.$$

Hence, β_m is norm in the extension $\boldsymbol{Q}_m(\sqrt{\ell'})/\boldsymbol{Q}_m$, 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 ℓ'-adic place $\mathcal{L}'$ of $\boldsymbol{Q}_m$, we have

$$\left(\frac{\beta_m, \ell'}{\mathcal{L}'}\right) = \left(\frac{\ell', \beta_m}{\mathcal{L}'}\right) = \sqrt{\beta_m}^{\left(\frac{\boldsymbol{Q}_m(\sqrt{\beta_m})/\boldsymbol{Q}_m}{\mathcal{L}'}\right)^{-v_{\mathcal{L}'}((\ell'))}-1} = \sqrt{\beta_m}^{\left(\frac{\boldsymbol{Q}_{m+1}/\boldsymbol{Q}_m}{\mathcal{L}'}\right)^{-1}-1} = -1.$$

Thus β_m is not norm in the extension $\boldsymbol{Q}_m(\sqrt{\ell'})/\boldsymbol{Q}_m$, so $\bar{\beta}_m \notin \ker(f)$.

Also, for each ℓ-adic place $\mathcal{L}$ and ℓ'-adic place $\mathcal{L}'$ of $\boldsymbol{Q}_m$, 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 $F_m/\boldsymbol{Q}_m$, but norm in the extension $\boldsymbol{Q}_m(\sqrt{\ell'})/\boldsymbol{Q}_m$. Hence the kernel of f is nontrivial:

$$\ker(f)=-\bar{\beta}_m\mathbb{F}_2.$$

Consequently, we conclude that the system $\{\overline{-1},\bar{\beta}_m,\bar{u}\mid u\in U\}$ is free. Thus, we find

$$\left|\tfrac{1}{2}A'_m(F)\right|=|A'_m(F)^G|=2^{2^m+2^m}[E'_{\boldsymbol{Q}_m}:E'_{\boldsymbol{Q}_m}\cap N_{F_m/\boldsymbol{Q}_m}(F_m^*)]^{-1}=2^{2^m-1}.$$

So clearly, $D_m(F)$ is nontrivial. Moreover, since the 2-adic place of F_m is totally ramified in F_∞, 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 $\mathrm{rk}_2(A'_m(F))=2^m-1<2^m$, it follows from Proposition 2.1 that

$$\tfrac{1}{2}X'_\infty(F)\simeq\tfrac{1}{2}A'_m(F)\simeq\tfrac{1}{2}A'_n(F)\simeq\mathbb{Z}/2\mathbb{Z}^{\oplus 2^m-1}\quad\text{for all } n\geq m.$$

In addition, by the ambiguous class number formula we conclude that for each $n\geq m$,

$$\mathrm{rk}_2(A_n(F))=\mathrm{rk}_2(A_n(F)^G)=2^m. \qquad \square$$

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

$$D_n(F)\simeq\mathbb{Z}/2\mathbb{Z},\quad \mathrm{rk}_2(A'_n(F))=2^m-1 \quad\text{and}\quad \mathrm{rk}_2(A_n(F))=2^m.$$

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. $\square$

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 ℓ-adic place. By Proposition 2.2, we have $\mathrm{rank}(A'_m(F))<2^m$, then $A'(F)$ capitulates in F_m [15, Lemma 7]. Consider the commutative diagram [6, Theorems 6 and 7]:

$$\begin{array}{ccc} A'(F) & \xrightarrow{\sim} & X'_\infty(F)/w_0X'_\infty(F) \\ \downarrow & & \downarrow \nu_m \\ A'_m(F) & \xrightarrow{\sim} & X'_\infty(F)/w_mX'_\infty(F) \end{array}$$

Since $A'(F)$ capitulates in F_m, then the left vertical map is trivial, thus

$$\nu_m X'_\infty(F) \subset w_m X'_\infty(F).$$

Hence we obtain

$$w_m X'_\infty(F) = \nu_m X'_\infty(F) = w_0(\nu_m X'_\infty(F)).$$

On the other hand, since $\nu_m X'_\infty(F)$ is a finitely generated Λ-module and w_0 is contained in (p, T), then by Nakayama's lemma we obtain $w_m X'_\infty(F) = \nu_m X'_\infty(F) = 0$; hence $X'_\infty(F) \simeq A'_m(F)$. Consequently, from Corollary 2.3, we have

$$X_\infty(F) \simeq X'_\infty(F) \oplus D_\infty(F) \simeq A_m(F) \simeq A'_m(F) \oplus \mathbb{Z}/2\mathbb{Z}.$$

Also, from Proposition 2.2, we have $\mathrm{rk}_2(A_{m-1}(F)) = 2^{m-1} < \mathrm{rk}_2(A_m(F)) = 2^m$, then $X_\infty(F) \not\simeq A_{m-1}(F)$.

Now, we will prove that $X_\infty(F)$ is an elementary abelian 2-group. We will use other notations. For each nonnegative integer $n \le m'$, let S_n be the set of ℓ'-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 $A_n^{S_n}$ be the group of S_n-classes, that is, $A_n^{S_n} := A_n(F)/D_{S_n}$. 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

$$\mathrm{Gal}(M_n/F_n) \simeq A_n^{S_n}.$$

Since F contains a unique 2-adic place which is totally ramified in F_∞ and the ℓ'-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, $A_{m'}^{S_{m'}}$ is a finitely generated $\Lambda = \mathbb{Z}_2[[T]]$-module and $A_{m'}^{S_{m'}}/T \simeq A_0^{S_0}$. By the hypotheses, we have $(\ell/\ell') = -1$, then $A_0^{S_0} = 0$ and by Nakayama's lemma, $A_{m'}^{S_{m'}} = 0$. It follows that for each nonnegative integers $n \le m'$, we have $A_n(F) \simeq D_{S_n}$. 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 $(\mathbb{Z}/2\mathbb{Z})^{2^m}$. □

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 $X^0_\infty(K)$ 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_∞^- 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 Λ-submodule [1, Example 2.8]. So from the exact sequence

$$0 \to X_\infty(K^+) \to X_\infty(K) \to X_\infty^-(K) \to 0,$$

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

$$X_\infty^0(K) = X_\infty^0(K^+).$$

We reconsider now, the quadratic number field $F = \boldsymbol{Q}(\sqrt{\ell\ell'})$ of the main Theorem 1.1. Recall that ℓ and ℓ' 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

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

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:*

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

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

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 Λ-submodule [1, Corollary 1.4]. Hence, the $\mathbb{Z}_2$-torsion $X_\infty^0(K)$ of the Iwasawa module $X_\infty(K)$ coincides with the Iwasawa module $X_\infty(F)$:

$$X_\infty^0(K) = X_\infty(F).$$

Consequently from Theorem 1.1, we obtain

$$X_\infty(K) \simeq \mathbb{Z}_2^{2^m+2^{m'}-1} \oplus (\mathbb{Z}/2\mathbb{Z})^{2^m}. \qquad \square$$

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

[1] M. Atsuta, "Finite Λ-submodules of Iwasawa modules for a CM-field for $p = 2$", *J. Théor. Nombres Bordeaux* **30**:3 (2018), 1017–1035. MR Zbl

[2] B. Ferrero, "The cyclotomic $\mathbf{Z}_2$-extension of imaginary quadratic fields", *Amer. J. Math.* **102**:3 (1980), 447–459. MR Zbl

[3] B. Ferrero and L. C. Washington, "The Iwasawa invariant μ_p vanishes for abelian number fields", *Ann. of Math.* (2) **109**:2 (1979), 377–395. MR Zbl

[4] T. Fukuda and K. Komatsu, "On the Iwasawa λ-invariant of the cyclotomic $\mathbf{Z}_2$-extension of a real quadratic field", *Tokyo J. Math.* **28**:1 (2005), 259–264. MR Zbl

[5] R. Greenberg, "On the Iwasawa invariants of totally real number fields", *Amer. J. Math.* **98**:1 (1976), 263–284. MR Zbl

[6] K. Iwasawa, "On $\mathbf{Z}_l$-extensions of algebraic number fields", *Ann. of Math.* (2) **98** (1973), 246–326. MR Zbl

[7] Y. Kida, "Cyclotomic $\mathbf{Z}_2$-extensions of J-fields", *J. Number Theory* **14**:3 (1982), 340–352. MR Zbl

[8] N. Kumakawa, "On the Iwasawa λ-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

[9] Y. Mizusawa, "On unramified Galois 2-groups over $\mathbb{Z}_2$-extensions of real quadratic fields", *Proc. Amer. Math. Soc.* **138**:9 (2010), 3095–3103. MR Zbl

[10] A. Mouhib, "Sur la 2-extension maximale non ramifiée de la $\mathbf{Z}_2$-extension cyclotomique de certains corps quadratiques", *An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat.* **22**:1 (2014), 207–214. MR

[11] A. Mouhib and A. Movahhedi, "Cyclicity of the unramified Iwasawa module", *Manuscripta Math.* **135**:1-2 (2011), 91–106. MR Zbl

[12] Y. Nishino, "On the Iwasawa invariants of the cyclotomic $\mathbf{Z}_2$-extensions of certain real quadratic fields", *Tokyo J. Math.* **29**:1 (2006), 239–245. MR Zbl

[13] M. Ozaki, "Construction of real abelian fields of degree p with $\lambda_p = \mu_p = 0$", *Int. J. Open Probl. Comput. Sci. Math.* **2**:3 (2009), 342–351. MR Zbl

[14] M. Ozaki and H. Taya, "On the Iwasawa λ_2-invariants of certain families of real quadratic fields", *Manuscripta Math.* **94**:4 (1997), 437–444. MR Zbl

[15] M. Ozaki and G. Yamamoto, "Iwasawa λ_3-invariants of certain cubic fields", *Acta Arith.* **97**:4 (2001), 387–398. 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

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2023 is US $605/year for the electronic version, and $820/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 323 No. 1 March 2023