ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 47, Number 1, 2017

THE DISCRIMINANT OF ABELIAN NUMBER FIELDS

VICTOR BAUTISTA-ANCONA AND JOSE UC-KUK

ABSTRACT. For an abelian number field K, the discriminant can be obtained from the conductor m of K, the degree of K over $\mathbb{Q}$, and the degrees of extensions $K \cdot \mathbb{Q}(\zeta_{m/p^\alpha})/\mathbb{Q}(\zeta_{m/p^\alpha})$, where p runs through the set of primes that divide m, and p^α is the greatest power that divides m. In this paper, we give a formula for computing the discriminant of any abelian number field.

1. Introduction. Let K be an algebraic number field over $\mathbb{Q}$. We say that K is abelian if the extension field $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K/\mathbb{Q})$ is an abelian group. From the Kronecker-Weber theorem, if K is an abelian number field, then K is contained in some cyclotomic field $\mathbb{Q}(\zeta_m)$ [**4**]. The smallest m for which this holds is called the *conductor* of K. The discriminant of a number field K, denoted $\mathrm{disc}\,(K)$, is one of the most important invariants of an algebraic number field.

In the early 2000s, Interlando, Dantas Lopes and da Nóbrega Neto presented a formula for computing the discriminant of subfields of $K = \mathbb{Q}(\zeta_{p^r})$, where p is an odd prime and r is a positive integer, see [**3**]. This formula depends only on p and $[K : \mathbb{Q}]$. Later, in [**1**], Dantas Lopes extends the result of [**3**] to the case where $p = 2$, obtaining a formula that splits into two expressions depending on whether K is cyclotomic or not. Both expressions depend only on $[K : \mathbb{Q}]$.

In a third work, Interlando et al., obtained a formula for computing the discriminant of an abelian number field K; this formula is presented as a function of the conductor m of K, the degree $[K : \mathbb{Q}]$ and the degrees of the fields $K \cap \mathbb{Q}(\zeta_{m/p^\alpha})$ over $\mathbb{Q}$, where p runs through the set of primes that divide m, and p^α runs through all powers of p that

2010 AMS *Mathematics subject classification.* Primary 11R18, 11R29.
Keywords and phrases. Cyclotomic fields, abelian number fields, conductors, discriminant.
The second author was supported by Consejo Nacional de Ciencia y Tecnología (CONACyT).
Received by the editors on February 13, 2015, and in revised form on April 13, 2015.
DOI:10.1216/RMJ-2017-47-1-39

divide m, see [**2,** Theorem 1]. In fact, they showed in their paper that it is not necessary to know all the powers of p that divide m but only the greatest power of p which divides m, see [**2,** Theorem 2].

Unfortunately, [**2,** Theorem 2] is incorrect, since this result only applies to the case where m is odd or a power of 2. The main purpose of this work is to correct this theorem. We present a formula when $m = 2^\alpha n$ with α, $n \geq 2$ and n odd. Furthermore, we show that, in [**2,** Theorem 1], the conductor can be omitted and, therefore, we can conclude that this result is a generalization of [**1,** Theorem 3.1] and [**3,** Theorem 4.1].

The paper is organized as follows. In Section 2, we briefly review the main theorems of [**2**] and show that, under certain conditions, the only subfields of $\mathbb{Q}(\zeta_{mp^n})$ are cyclotomic (Proposition 2.3). In Section 3, we show that, in [**2,** Theorem 1], the conductor can be omitted (Theorem 3.1), and this result is used to show that Theorem 2 of [**2**] is wrong. Finally, in Section 4, we give a corrected version of [**2,** Theorem 2] (Theorem 4.1).

2. Preliminaries. In this section, we present the main theorems of [**2**], proofs are omitted.

Theorem 2.1 ([**2,** Theorem 1])**.** *Let*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}$$

and K be an abelian number field of conductor m. Then,

$$|\mathrm{disc}\,(K)| = \frac{m^{[K:\mathbb{Q}]}}{\prod_{i=1}^{k} p_i^{\sum_{r=1}^{\alpha_i}[K\cap\mathbb{Q}(\zeta_{m/p_i^r}):\mathbb{Q}]}}.$$

Theorem 2.2 ([**2,** Theorem 2])**.** *Let K be an abelian number field of conductor*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Then, the discriminant of K is equal to

$$
|\mathrm{disc}\,(K)| = \begin{cases} \left(\dfrac{m}{\prod_{i=1}^{k} p_i^{\left(p_i^{\alpha_i - 1} - 1 + (p_i - 1)/u_i\right)/\left(p_i^{\alpha_i - 1}(p_i - 1)\right)}} \right) & \textit{if } m \neq 2^n \\ & \textit{for all } n \in \mathbb{N}; \\ 2^{(n-1)2^{n-1}} & \textit{if } K = \mathbb{Q}(\zeta_{2^n}); \\ 2^{n2^{n-1} - 1} & \textit{if } m = 2^{n+1} \\ & \textit{for some } n \in \mathbb{N}, \\ & \textit{but } K \neq \mathbb{Q}(\zeta_{2^{n+1}}), \end{cases}
$$

where $u_i = [K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}}) : \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})]/p_i^{\alpha_i - 1}$.

In the proof of Theorem 2.2, Interlando et al. claim that,

> if m, n, $p \in \mathbb{N}$ with p a prime such that $(m, p^n) = 1$, then, the only subfields of $\mathbb{Q}(\zeta_{mp^n})$ containing $\mathbb{Q}(\zeta_{mp})$ are the cyclotomic ones.

However, this claim is false when $p = 2$, see Figures 1 and 2. Next, we give the correct statement and its proof.

Proposition 2.3. *Let m, n, $p \in \mathbb{N}$ with p a prime such that $(m, p^n) = 1$. Then,*

(1) *if p is odd, the only subfields containing $\mathbb{Q}(\zeta_{mp})$ and contained in $\mathbb{Q}(\zeta_{mp^n})$ are cyclotomic.*
(2) *If $p = 2$, the only subfields containing $\mathbb{Q}(\zeta_{m2^2})$ and contained in $\mathbb{Q}(\zeta_{m2^n})$ are cyclotomic.*

Proof. We know that $\mathbb{Q}(\zeta_{mp^n}) = \mathbb{Q}(\zeta_m)(\zeta_{p^n})$, so that $\mathrm{Gal}(\mathbb{Q}(\zeta_{mp^n})/\mathbb{Q}(\zeta_m))$ is isomorphic to a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Moreover, $\mathbb{Q}(\zeta_{mp^n})/\mathbb{Q}(\zeta_m)$ is a Galois extension, and therefore,

$$|\,\mathrm{Gal}(\mathbb{Q}(\zeta_{mp^n})/\mathbb{Q}(\zeta_m))| = [\mathbb{Q}(\zeta_{mp^n}) : \mathbb{Q}(\zeta_m)] = \phi(p^n) = |(\mathbb{Z}/p^n\mathbb{Z})^\times|.$$

This implies that $\mathrm{Gal}(\mathbb{Q}(\zeta_{mp^n})/\mathbb{Q}(\zeta_m)) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus, we have two cases:

(1) If p is odd, $\mathbb{Q}(\zeta_{mp^n})/\mathbb{Q}(\zeta_m)$ is a cyclic extension of degree $\phi(p^n)$. It follows that, for each divisor d of $\phi(p^n)$ there is only one subfield of $\mathbb{Q}(\zeta_{mp^n})$ of degree d over $\mathbb{Q}(\zeta_m)$. Furthermore, if E_i is a subfield such that

$$\mathbb{Q}(\zeta_{mp}) \subset E_i \subset \mathbb{Q}(\zeta_{mp^n}),$$

then

$$[E_i : \mathbb{Q}(\zeta_m)] = [E_i : \mathbb{Q}(\zeta_{mp})][\mathbb{Q}(\zeta_{mp}) : \mathbb{Q}(\zeta_m)] = (p-1)p^i$$

for some $i \in \{0, 1, \dots, n-1\}$. On the other hand,

$$\left[\mathbb{Q}(\zeta_{mp^{i+1}}) : \mathbb{Q}(\zeta_m)\right] = (p-1)p^i$$

for each $i \in \{0, 1, \dots, n-1\}$. Then, the uniqueness for degrees implies that $E_i = \mathbb{Q}(\zeta_{mp^{i+1}})$.

(2) If $p = 2$, the result is trivial when $n = 2$. Suppose $n \geq 3$. We consider the automorphism $\sigma_5 \in \mathrm{Gal}(\mathbb{Q}(\zeta_{m2^n})/\mathbb{Q}(\zeta_m))$, given for $\sigma_5(\zeta_{2^n}) = \zeta_{2^n}^5$. Then, we have

$$\sigma_5(\zeta_{2^n}^{2^{n-2}}) = \zeta_{2^n}^{5\cdot 2^{n-2}} = \zeta_{2^n}^{(1+2^2)2^{n-2}} = \zeta_{2^n}^{2^{n-2}},$$

that is, σ_5 fixed to $\zeta_{2^n}^{2^{n-2}} = \zeta_{2^2}$, so that

$$\langle \sigma_5 \rangle < \mathrm{Gal}(\mathbb{Q}(\zeta_{m2^n})/\mathbb{Q}(\zeta_{m2^2})).$$

On the other side, the extension $\mathbb{Q}(\zeta_{m2^n})/\mathbb{Q}(\zeta_{m2^2})$ is Galois, so that

$$|\langle \sigma_5 \rangle| = 2^{n-2} = [\mathbb{Q}(\zeta_{m2^n}) : \mathbb{Q}(\zeta_{m2^2})] = |\,\mathrm{Gal}(\mathbb{Q}(\zeta_{m2^n})/\mathbb{Q}(\zeta_{m2^2}))|.$$

Hence, $\mathbb{Q}(\zeta_{m2^n})/\mathbb{Q}(\zeta_{m2^2})$ is a cyclic extension of degree 2^{n-2}. It follows that a unique subfield E_i of $\mathbb{Q}(\zeta_{m2^n})$ exists such that $[E_i : \mathbb{Q}(\zeta_{m2^2})] = 2^i$ for each $i \in \{0, 1, \dots, n-2\}$. But, for $i \in \{0, 1, \dots, n-2\}$, $\mathbb{Q}(\zeta_{m2^{2+i}})$ is a subfield with such properties. Then $E_i = \mathbb{Q}(\zeta_{m2^{2+i}})$. □

Corollary 2.4. *Let K be an abelian number field of conductor $m = 2^{n+1}$. Then $[K : \mathbb{Q}] = 2^n$ or 2^{n-1}.*

Proof. If $m = 2^2$, then $K = \mathbb{Q}(\zeta_{2^2})$. Thus, we consider the case $m = 2^{n+1}$ with $n \geqslant 2$ and assume that $K \neq \mathbb{Q}(\zeta_{2^{n+1}})$, i.e., $[K : \mathbb{Q}] \neq 2^n$ so that $K \neq \mathbb{Q}(\zeta_{2^i})$ for each $i \in \{2, 3, \dots, n\}$ since the conductor of K is $m = 2^{n+1}$. Proposition 2.3 guarantees that $K \cap \mathbb{Q}(\zeta_{2^2}) = \mathbb{Q}$ since only the cyclotomics contain $\mathbb{Q}(\zeta_{2^2})$; also, $K \cdot \mathbb{Q}(\zeta_{2^2})$ is a cyclotomic subfield of $\mathbb{Q}(\zeta_{2^{n+1}})$ containing K. It follows that $K\cdot\mathbb{Q}(\zeta_{2^2})=\mathbb{Q}(\zeta_{2^{n+1}})$. Thus, if $[K:\mathbb{Q}]=2^r$, then

$$\begin{aligned}2^{n-r}&=[\mathbb{Q}(\zeta_{2^{n+1}}):K]\\&=[K\cdot\mathbb{Q}(\zeta_{2^2}):K]\\&=[\mathbb{Q}(\zeta_{2^2}):K\cap\mathbb{Q}(\zeta_{2^2})]\\&=[\mathbb{Q}(\zeta_{2^2}):\mathbb{Q}]\\&=2,\end{aligned}$$

and therefore, $r=n-1$. □

3. Removing the condition over the conductor. We generalize Theorem 2.1 to note that we can eliminate the condition over the conductor.

Theorem 3.1. *Let K be a subfield of $\mathbb{Q}(\zeta_n)$ with $n=\prod_{j=1}^s p_j^{\beta_j}$. Then,*

$$|\mathrm{disc}\,(K)|=\frac{n^{[K:\mathbb{Q}]}}{\prod_{j=1}^s p_j^{\sum_{l=1}^{\beta_j}[K\cap\mathbb{Q}(\zeta_{n/p_j^l}):\mathbb{Q}]}}.$$

Proof. If K is a subfield of $\mathbb{Q}(\zeta_n)$ with $n=\prod_{j=1}^s p_j^{\beta_j}$ and conductor $m=\prod_{i=1}^k p_i^{\alpha_i}$ with $m\neq n$, then $k<s$ or $\alpha_i<\beta_i$ for some $i\in\{1,2,\ldots,k\}$. We claim that

$$\sum_{l=1}^{\beta_j}[K\cap\mathbb{Q}(\zeta_{n/p_j^l}):\mathbb{Q}]=(\beta_j-\alpha_j)[K:\mathbb{Q}]+\sum_{i=1}^{\alpha_j}[K\cap\mathbb{Q}(\zeta_{m/p_j^i}):\mathbb{Q}] \tag{3.1}$$

for $1\le j\le k$, and

$$\sum_{l=1}^{\beta_j}[K\cap\mathbb{Q}(\zeta_{n/p_j^l}):\mathbb{Q}]=\beta_j[K:\mathbb{Q}] \tag{3.2}$$

for $k+1\le j\le s$. To see this, we consider the following two cases.

(i) For $1\le j\le k$, we have:
  (a) if $1\le l\le\beta_j-\alpha_j$, then $m\mid n/p_j^l$, and, therefore,

$$K\subset\mathbb{Q}(\zeta_m)\subset\mathbb{Q}(\zeta_{n/p_j^l}),$$

so that

$$[K \cap \mathbb{Q}(\zeta_{n/p_j^l}) : \mathbb{Q}] = [K : \mathbb{Q}].$$

(b) If $\beta_j - \alpha_j + 1 \leq l \leq \beta_j$, then we have $m/p_j^{l-\beta_j+\alpha_j} \mid n/p_j^l$. Thus, $\mathbb{Q}(\zeta_{m/p_j^{l-\beta_j+\alpha_j}}) \subset \mathbb{Q}(\zeta_{n/p_j^l})$, and, therefore,

$$K \cap \mathbb{Q}(\zeta_{m/p_j^{l-\beta_j+\alpha_j}}) \subset K \cap \mathbb{Q}(\zeta_{n/p_j^l}).$$

Conversely, observe that

$$\begin{aligned} K \cap \mathbb{Q}(\zeta_{n/p_j^l}) \subset \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{n/p_j^l}) &= \mathbb{Q}(\zeta_{(m,n/p_j^l)}) \\ &= \mathbb{Q}(\zeta_{m/p_j^{l-\beta_j+\alpha_j}}). \end{aligned}$$

Then, $K \cap \mathbb{Q}(\zeta_{n/p_j^l}) \subset K \cap \mathbb{Q}(\zeta_{m/p_j^{l-\beta_j+\alpha_j}})$, and, therefore,

$$K \cap \mathbb{Q}(\zeta_{n/p_j^l}) = K \cap \mathbb{Q}(\zeta_{m/p_j^{l-\beta_j+\alpha_j}}).$$

In conclusion,

$$\begin{aligned} \sum_{l=1}^{\beta_j} [K \cap \mathbb{Q}(\zeta_{n/p_j^l}) : \mathbb{Q}] &= \sum_{l=1}^{\beta_j-\alpha_j} [K \cap \mathbb{Q}(\zeta_{n/p_j^l}) : \mathbb{Q}] \\ &\quad + \sum_{l=\beta_j-\alpha_j+1}^{\beta_j} [K \cap \mathbb{Q}(\zeta_{n/p_j^l}) : \mathbb{Q}] \\ &= \sum_{l=1}^{\beta_j-\alpha_j} [K : \mathbb{Q}] \\ &\quad + \sum_{l=\beta_j-\alpha_j+1}^{\beta_j} [K \cap \mathbb{Q}(\zeta_{m/p_j^{l-\beta_j+\alpha_j}}) : \mathbb{Q}] \\ &= (\beta_j - \alpha_j)[K : \mathbb{Q}] \\ &\quad + \sum_{i=1}^{\alpha_j} [K \cap \mathbb{Q}(\zeta_{m/p_j^i}) : \mathbb{Q}]. \end{aligned}$$

(ii) For $k+1 \leq j \leq s$, similarly to case (ia), we have

$$[K \cap \mathbb{Q}(\zeta_{n/p_j^l}) : \mathbb{Q}] = [K : \mathbb{Q}] \quad \text{for } 1 \leq l \leq \beta_j.$$

Thus,

$$\sum_{l=1}^{\beta_j}[K \cap \mathbb{Q}(\zeta_{n/p_j^l}) : \mathbb{Q}] = \sum_{l=1}^{\beta_j}[K : \mathbb{Q}] = \beta_j[K : \mathbb{Q}].$$

From equations (3.1), (3.2) and Theorem 2.1, we obtain

$$\begin{aligned}\frac{n^{[K:\mathbb{Q}]}}{\prod_{j=1}^{s} p_j^{\sum_{l=1}^{\beta_j}[K\cap\mathbb{Q}(\zeta_{n/p_j^l}):\mathbb{Q}]}} &= \prod_{j=1}^{k} p_j^{\beta_j[K:\mathbb{Q}]-\sum_{l=1}^{\beta_j}[K\cap\mathbb{Q}(\zeta_{n/p_j^l}):\mathbb{Q}]} \\ &= \prod_{j=1}^{k} p_j^{\beta_j[K:\mathbb{Q}]-(\beta_j-\alpha_j)[K:\mathbb{Q}]-\sum_{i=1}^{\alpha_j}[K\cap\mathbb{Q}(\zeta_{m/p_j^i}):\mathbb{Q}]} \\ &= |\mathrm{disc}\,(K)|. \qquad \square\end{aligned}$$

Remark 3.2. From Theorem 3.1, we conclude that Theorem 2.1 is, indeed, a generalization of previous works **[1, 3]**.

Next, we compute the discriminant of two particular abelian number fields; these examples show that Theorem 2.2 is incorrect.

Example 3.3. The cyclotomic field $\mathbb{Q}(\zeta_{24})$ has degree 8 over $\mathbb{Q}$ and a Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q}) \cong (\mathbb{Z}/24\mathbb{Z})^{\times}$. We have

$$G = \{\sigma_1, \sigma_5, \sigma_7, \sigma_{11}, \sigma_{13}, \sigma_{17}, \sigma_{19}, \sigma_{23}\},$$

where $\sigma_i(\zeta_{24}) = \zeta_{24}^i$. We consider the following subgroups of G:

$$\begin{aligned}H_J &= \{\sigma_1, \sigma_7, \sigma_{17}, \sigma_{23}\},\\ H_K &= \{\sigma_1, \sigma_7\},\\ H_L &= \{\sigma_1, \sigma_7, \sigma_{13}, \sigma_{19}\},\\ H_N &= \{\sigma_1, \sigma_{17}\},\\ H_O &= \{\sigma_1, \sigma_{13}\},\end{aligned}$$

where J, K, L, N and O are the subfields of $\mathbb{Q}(\zeta_{24})$ fixed by H_J, H_K, H_L, H_N and H_O, respectively. We observe that $L = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$, since $\sigma_i(\zeta_3) = \sigma_i(\zeta_{24}^8) = \zeta_{24}^8 = \zeta_3$ for all $\sigma_i \in H_L$; in a similar way, it is easily verified that $N = \mathbb{Q}(\zeta_8)$ and $O = \mathbb{Q}(\zeta_{12})$. For the subfield

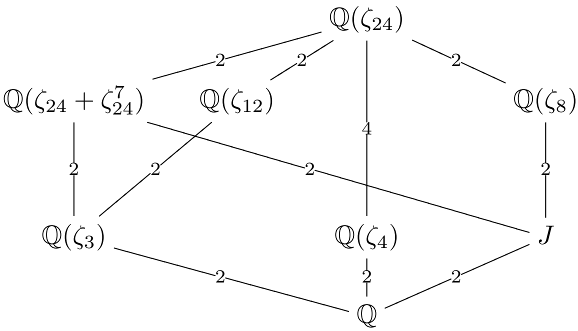

FIGURE 1. Partial lattice of subfields of $\mathbb{Q}(\zeta_{24})$.

$K = \mathbb{Q}(\zeta_{24} + \zeta_{24}^7)$, we have that

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta_{24})]/|H_K| = 4,$$

and also

$$\begin{aligned}
\langle H_K, H_N\rangle = H_J &\Longrightarrow K \cap \mathbb{Q}(\zeta_8) = J,\\
\langle H_K, H_O\rangle = H_L &\Longrightarrow K \cap \mathbb{Q}(\zeta_{12}) = L = \mathbb{Q}(\zeta_3),\\
\langle H_K, H_L\rangle = H_L &\Longrightarrow K \cap \mathbb{Q}(\zeta_6) = K \cap \mathbb{Q}(\zeta_3) = L = \mathbb{Q}(\zeta_3).
\end{aligned}$$

Figure 1 illustrates the partial lattice of subfields of $\mathbb{Q}(\zeta_{24})$. Then, by Theorem 3.1, we have that $|\mathrm{disc}\,(K)| = 2^6 \cdot 3^2$. On the other hand, from Figure 1, we have that

$$[K \cdot \mathbb{Q}(\zeta_8) : \mathbb{Q}(\zeta_8)] = 2$$

and

$$[K \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}(\zeta_3)] = 2;$$

so, Theorem 2.2 says that $|\mathrm{disc}\,(K)| = 2^7 \cdot 3^2$, a different answer to that obtained via Theorem 3.1.

Example 3.4. The cyclotomic field $\mathbb{Q}(\zeta_{40})$ has degree 16 over $\mathbb{Q}$ and a Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{40})/\mathbb{Q}) \cong (\mathbb{Z}/40\mathbb{Z})^\times$. We have

$$G = \{\sigma_1, \sigma_3, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{17}, \sigma_{19}, \sigma_{21}, \sigma_{23}, \sigma_{27}, \sigma_{29}, \\ \sigma_{31}, \sigma_{33}, \sigma_{37}, \sigma_{39}\},$$

where $\sigma_i(\zeta_{40}) = \zeta_{40}^i$. We consider the following subgroups of G:

$$\begin{aligned} H_J &= \{\sigma_1, \sigma_{21}\}, \\ H_K &= \{\sigma_1, \sigma_{31}\}, \\ H_L &= \{\sigma_1, \sigma_{11}, \sigma_{21}, \sigma_{31}\}, \\ H_M &= \{\sigma_1, \sigma_9, \sigma_{17}, \sigma_{33}\}, \\ H_N &= \{\sigma_1, \sigma_7, \sigma_9, \sigma_{17}, \sigma_{23}, \sigma_{31}, \sigma_{33}, \sigma_{39}\}, \end{aligned}$$

where J, K, L, M and N are the subfields of $\mathbb{Q}(\zeta_{40})$ fixed by H_J, H_K, H_L, H_M and H_N, respectively. We observe that $L = \mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5)$, $J = \mathbb{Q}(\zeta_{20})$, and $M = \mathbb{Q}(\zeta_8)$. For the subfield $K = \mathbb{Q}(\zeta_{40} + \zeta_{40}^{31})$ we have that $[K : \mathbb{Q}] = 8$, and also

$$\begin{aligned} \langle H_K, H_J\rangle = H_L &\Longrightarrow K \cap \mathbb{Q}(\zeta_{20}) = L, \\ \langle H_K, H_M\rangle = H_N &\Longrightarrow K \cap \mathbb{Q}(\zeta_8) = N, \\ \langle H_K, H_L\rangle = H_L &\Longrightarrow K \cap \mathbb{Q}(\zeta_{10}) = K \cap \mathbb{Q}(\zeta_5) = L = \mathbb{Q}(\zeta_5). \end{aligned}$$

Figure 2 illustrates the partial lattice of subfields of $\mathbb{Q}(\zeta_{40})$. Then, by Theorem 3.1, we have that $|\mathrm{disc}\,(K)| = 2^{12} \cdot 5^6$. On the other hand, from Figure 2, we have

$$[K \cdot \mathbb{Q}(\zeta_8) : \mathbb{Q}(\zeta_8)] = 4$$

and

$$[K \cdot \mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5)] = 2;$$

so, Theorem 2.2 says that $|\mathrm{disc}\,(K)| = 2^{14} \cdot 5^6$, a different answer to that obtained via Theorem 3.1.

Abelian number fields presented in Examples 3.3 and 3.4 have the particularity that their conductor has the form $2^\alpha n$ with $\alpha, n \geq 2$ and n odd. These examples suggest that Theorem 2.2 is incorrect. Other examples showed that similar problems arise when calculating

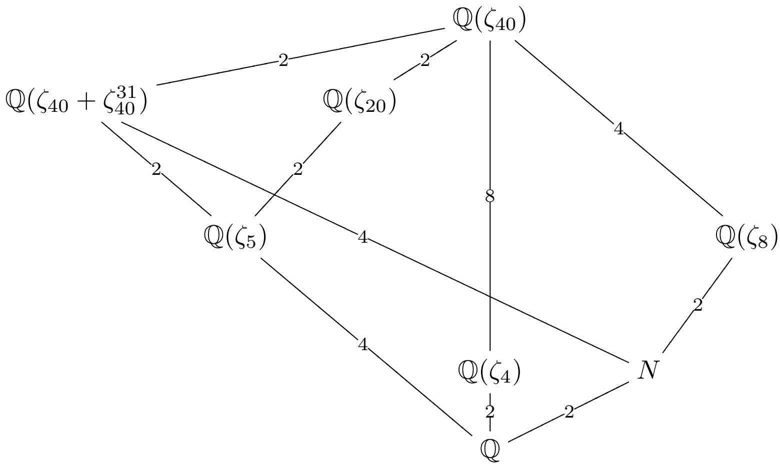

FIGURE 2. Partial lattice of subfields of $\mathbb{Q}(\zeta_{40})$.

the discriminant of an abelian number field whose conductor is in the above-mentioned form.

4. Main result. In this section, we give a corrected version of Theorem 2.2 that works in general, including abelian number fields which have a conductor of form $m = 2^\alpha n$ with $\alpha, n \geq 2$, where n is odd.

Theorem 4.1. *Let K be an abelian number field of conductor $m = \prod_{i=1}^{l} p_i^{\alpha_i}$. Then,*

$$|\mathrm{disc}\,(K)| = \left(\prod_{i=1}^{l} p_i^{\alpha_i - \lambda_i}\right)^{[K:\mathbb{Q}]},$$

where

$$\lambda_i = \frac{p_i^{\alpha_i-(p_i,2)} - 1 + (p_i-1)/u_i}{p_i^{\alpha_i-(p_i,2)}(p_i-1)}$$

and

$$u_i = \frac{[K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}}) : \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})]}{p_i^{\alpha_i - 1}}.$$

Proof. From Theorem 2.1, it is sufficient to calculate the degrees $[K \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}]$ for all $i \in \{1, 2, \ldots, l\}$ and $1 \leq j \leq \alpha_i$. We have that $\mathrm{Gal}(K/K \cap \mathbb{Q}(\zeta_{m/p_i^j})) \cong \mathrm{Gal}(K \cdot \mathbb{Q}(\zeta_{m/p_i^j})/\mathbb{Q}(\zeta_{m/p_i^j}))$, and thus, $[K : K \cap \mathbb{Q}(\zeta_{m/p_i^j})] = [K \cdot \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}(\zeta_{m/p_i^j})]$. It follows that

$$[K \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K : K \cap \mathbb{Q}(\zeta_{m/p_i^j})]} = \frac{[K : \mathbb{Q}]}{[K \cdot \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}(\zeta_{m/p_i^j})]}.$$

We have two cases:

(1) If p_i is odd, Proposition 2.3 says that the only intermediate subfields in extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p_i^{\alpha_i - 1}})$ are cyclotomic. For $1 \leq j < \alpha_i$, $K \cdot \mathbb{Q}(\zeta_{m/p_i^j})$ is a cyclotomic subfield of $\mathbb{Q}(\zeta_m)$ containing K. It follows that $K \cdot \mathbb{Q}(\zeta_{m/p_i^j}) = \mathbb{Q}(\zeta_m)$, so that

$$[K \cdot \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}(\zeta_{m/p_i^j})] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_{m/p_i^j})] = \frac{\phi(m)}{\phi(m/p_i^j)} = p_i^j,$$

and consequently,

$$[K \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{p_i^j}.$$

If $j = \alpha_i$, then $K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})$ has conductor m and

$$\begin{aligned}[K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}}) : \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})] &= \frac{[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})]}{[\mathbb{Q}(\zeta_m) : K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})]} \\ &= \frac{(p_i - 1)p_i^{\alpha_i - 1}}{[\mathbb{Q}(\zeta_m) : K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})]};\end{aligned}$$

also, the extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})$ is cyclic and, therefore, $p_i \nmid [\mathbb{Q}(\zeta_m) : K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})]$. Otherwise, we have $K \subset K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}}) \subset \mathbb{Q}(\zeta_{m/p_i})$. Then

$$[K \cdot \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}}) : \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}})] = u_i p_i^{\alpha_i - 1},$$

and it follows that

$$[K \cap \mathbb{Q}(\zeta_{m/p_i^{\alpha_i}}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{u_i p_i^{\alpha_i - 1}}.$$

Next,

$$\begin{aligned}
\sum_{j=1}^{\alpha_i} [K \cap \mathbb{Q}(\zeta_{m/p_i^j}) : \mathbb{Q}] &= [K : \mathbb{Q}]\left(\frac{1}{u_i p_i^{\alpha_i - 1}} + \sum_{j=1}^{\alpha_i - 1} \frac{1}{p_i^j}\right) \\
&= [K : \mathbb{Q}]\left(\frac{1}{u_i p_i^{\alpha_i - 1}} + \frac{1 - (1/p_i^{\alpha_i})}{1 - (1/p_i)} - 1\right) \\
&= [K : \mathbb{Q}]\left(\frac{p_i^{\alpha_i - 1} - 1 + (p_i - 1)/u_i}{p_i^{\alpha_i - 1}(p_i - 1)}\right) \\
&= [K : \mathbb{Q}]\left(\frac{p_i^{\alpha_i - (p_i, 2)} - 1 + (p_i - 1)/u_i}{p_i^{\alpha_i - (p_i, 2)}(p_i - 1)}\right).
\end{aligned}$$

(2) If $p_i = 2$, then $\alpha_i \geq 2$ and Proposition 2.3 say that only intermediate subfields in extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/2^{\alpha_i - 2}})$ are cyclotomic. For $1 \leq j < \alpha_i - 2$, $K \cdot \mathbb{Q}(\zeta_{m/2^j})$ is a cyclotomic subfield of $\mathbb{Q}(\zeta_m)$ containing K. It follows that $K \cdot \mathbb{Q}(\zeta_{m/2^j}) = \mathbb{Q}(\zeta_m)$, so that

$$[K \cdot \mathbb{Q}(\zeta_{m/2^j}) : \mathbb{Q}(\zeta_{m/2^j})] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_{m/2^j})] = \frac{\phi(m)}{\phi(m/2^j)} = 2^j,$$

and, consequently,

$$[K \cap \mathbb{Q}(\zeta_{m/2^j}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{2^j}.$$

If $\alpha_i - 1 \leq j \leq \alpha_i$, then $\mathbb{Q}(\zeta_{m/2^{\alpha_i - 1}}) = \mathbb{Q}(\zeta_{m/2^{\alpha_i}})$ and, therefore,

$$[K \cap \mathbb{Q}(\zeta_{m/2^{\alpha_i - 1}}) : \mathbb{Q}] = [K \cap \mathbb{Q}(\zeta_{m/2^{\alpha_i}}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K \cdot \mathbb{Q}(\zeta_{m/2^{\alpha_i}}) : \mathbb{Q}(\zeta_{m/2^{\alpha_i}})]}.$$

Then,

$$\begin{aligned}
&\sum_{j=1}^{\alpha_i} [K \cap \mathbb{Q}(\zeta_{m/2^j}) : \mathbb{Q}] \\
&\qquad = [K : \mathbb{Q}]\left(\frac{2}{[K \cdot \mathbb{Q}(\zeta_{m/2^{\alpha_i}}) : \mathbb{Q}(\zeta_{m/2^{\alpha_i}})]} + \sum_{j=1}^{\alpha_i - 2} \frac{1}{2^j}\right)
\end{aligned}$$

$$= [K:\mathbb{Q}]\left(\frac{2^{\alpha_i-2}-1+2^{\alpha_i-1}/[K\cdot\mathbb{Q}(\zeta_{m/2^{\alpha_i}}):\mathbb{Q}(\zeta_{m/2^{\alpha_i}})]}{2^{\alpha_i-2}}\right)$$
$$= [K:\mathbb{Q}]\left(\frac{p_i^{\alpha_i-(p_i,2)}-1+(p_i-1)/u_i}{p_i^{\alpha_i-(p_i,2)}(p_i-1)}\right).$$

The result follows from Theorem 3.1. □

We review Examples 3.3 and 3.4 and recalculate the discriminant of these abelian numbers fields using Theorem 4.1.

Example 4.2. In Example 3.3, we consider the abelian number field $K=\mathbb{Q}(\zeta_{24}+\zeta_{24}^7)$; from Figure 1 and Theorem 4.1, it follows that

$$|\mathrm{disc}\,(K)| = \left(\prod_{i=1}^{l} p_i^{\alpha_i-\lambda_i}\right)^{[K:\mathbb{Q}]} = (2^{3-(3/2)})^4(3^{1-(1/2)})^4 = 2^6\cdot 3^2.$$

This result is consistent with that obtained via Theorem 3.1.

In a similar way,

Example 4.3. In Example 3.4, we consider the abelian number field $K=\mathbb{Q}(\zeta_{40}+\zeta_{40}^{31})$; from Figure 2 and Theorem 4.1, it follows that

$$|\mathrm{disc}\,(K)| = \left(\prod_{i=1}^{l} p_i^{\alpha_i-\lambda_i}\right)^{[K:\mathbb{Q}]} = (2^{3-(3/2)})^8(5^{1-(1/4)})^8 = 2^{12}\cdot 5^6.$$

This result is consistent with that obtained via Theorem 3.1.

The last two expressions in the formula of Theorem 2.2 can be derived from Theorem 4.1, as shown next.

Corollary 4.4. *Let K be an abelian number field of conductor $m=2^{n+1}$. Then,*

$$|\mathrm{disc}\,(K)| = \begin{cases} 2^{n2^n} & \text{if } K=\mathbb{Q}(\zeta_{2^{n+1}}); \\ 2^{n2^{n-1}-1} & \text{otherwise.} \end{cases}$$

Proof. Since $[K\cdot\mathbb{Q}(\zeta_{m/2^{n+1}}):\mathbb{Q}(\zeta_{m/2^{n+1}})]=[K:\mathbb{Q}]$, from Theorem 4.1 we obtain

$$\begin{aligned}|\mathrm{disc}\,(K)| &= \left(2^{n+1-[2^{n-1}-1+(2^n/[K:\mathbb{Q}])]/2^{n-1}}\right)^{[K:\mathbb{Q}]}\\ &= 2^{[K:\mathbb{Q}]\left((n2^{n-1}+1)/2^{n-1}\right)-2}.\end{aligned}$$

Moreover, from Corollary 2.4, we have

$$[K:\mathbb{Q}]=\begin{cases}2^n & \text{if } K=\mathbb{Q}(\zeta_{2^{n+1}});\\ 2^{n-1} & \text{otherwise,}\end{cases}$$

and the result follows. □

Acknowledgments. The second author gratefully acknowledges the support given by CONACyT (Consejo Nacional de Ciencia y Tecnología) for the realization of this article. Finally, we thank the referee for his corrections and remarks.

REFERENCES

1. José Othon Dantas Lopes, *The discriminant of subfields of* $\mathbb{Q}(\zeta_{2^r})$, J. Alg. Appl. **2** (2003), 463–469.

2. J. Carmelo Interlando, José Othon Dantas Lopes and Trajano Pires da N. Neto, *The discriminant of abelian numbers fields*, J. Alg. Appl. **5** (2006), 35–41.

3. Trajano Pires Da N. Neto, J. Carmelo Interlando and José Othon Dantas Lopes, *On computing discriminants of subfields of* $\mathbb{Q}(\zeta_{p^r})$, J. Num. Th. **96** (2002), 319–325.

4. L.C. Washington, *Introduction to cyclotomic fields*, Second edition, Grad. Texts Math. **83**, Springer-Verlag, New York, 1997.

Universidad Autónoma de Yucatán, Periférico Norte, Tablaje 13615, Mérida, Yucatán, Mexico
Email address: **vbautista@uady.mx**

Universidad Autónoma de Yucatán, Periférico Norte, Tablaje 13615, Mérida, Yucatán, Mexico
Email address: **jmanueluk87@gmail.com**