Abel 数域的导子计算公式

邓先涛，彭国华
(四川大学数学学院，成都 610064)

摘　要：基于 Kronecker-Weber 定理本文利用素数在 Abel 数域中的分歧指数明确给出 Abel 数域的导子计算公式. 特别地，二次数域的导子公式可以容易地从该公式推导出来.

关键词：导子；Kronecker-Weber 定理；惯性群；分歧指数
中图分类号：O156.2　　**文献标识码**：A　　DOI：10.19907/j.0490-6756.2023.031003

A conductor formula for Abelian number fields

DENG Xian-Tao，*PENG Guo-Hua*
(School of Mathematics，Sichuan University，Chengdu 610064，China)

Abstract：In this article，based on Kronecker-Weber theorem we explicitly give a conductor formula for the Abelian number fields based on the ramification indices. Particularly，the conductor of a quadratic number field can be easily deduced from this formula.

Keywords：Conductor；Kronecker-Weber theorem；Inertia group；Ramification index
(2010 MSC 11D41)

1　Introduction

An Abelian number field is a finite Galois extension over the rational number field whose Galois group is commutative. By Kronecker-Weber theorem，there exists a cyclotomic field $\mathbf{Q}(\zeta_m)$，such that $K\subseteq\mathbf{Q}(\zeta_m)$ for an Abelian number filed K. The *conductor* of K，denoted by $\mathfrak{f}(K)$，is the smallest positive integer m satisfying the above property. If m is odd，then we have $\mathbf{Q}(\zeta_m)=\mathbf{Q}(\zeta_{2m})$. Hence $\mathfrak{f}(K)\not\equiv 2 \pmod 4$.

The conductor is an important arithmetic invariant of an Abelian number field. It is closely related to the class number，the genus field，and the discriminant of a number field and so on. For example，Mäki[1] published some results on the conductor density of Abelian number fields，Johnston[2] gave the trace map between absolutely Abelian fields with the same conductor.

There are also some results on calculating class numbers of Abelian number fields of special conductor. For example，Schoof[3] calculated class numbers of Abelian number fields of prime conductor，Agathocleous[4] calculated class numbers of real cyclotomic fields of conductor pq.

For a quadraticfield $\mathbf{Q}(\sqrt{d})$，where d is a square-free integer，we know that

$$\mathfrak{f}(\mathbf{Q}(\sqrt{d}))=\begin{cases}|d|, & \text{if } d\equiv 1 \pmod 4,\\ |4d|, & \text{if } d\not\equiv 1 \pmod 4.\end{cases}$$

Generally，it is not easy to calculate the conductor. In 1952，Hasse[5] proved the conductor-discriminant formula，which is very useful for com-

收稿日期：2022-02-22
基金项目：国家自然科学基金(12171331)
作者简介：邓先涛(1996－)，男，湖南怀化人，博士研究生，主要从事数论及其应用方向研究. E-mail：xiantaodeng@126.com
通讯作者：彭国华. E-mail：peng@scu.edu.cn

puting the discriminant of an Abelian number field. In 1985, Zhang[6] gave a result on the genus field which is the maximal absolute Abelian number field containing the Abelian number field. The aim of this article is to give an explicit formula on conductor by some methods different from Zhang.

Let p be a prime number, and we fix a prime ideal $\mathfrak{p}$ of K lying above p. Define

$$I_p(K)=\{\sigma\in \mathrm{Gal}(K/\mathbf{Q})\mid \sigma(x)\equiv x(\mathrm{mod}\ \mathfrak{p}),\ \forall x\in O_K\}.$$

Since $\mathrm{Gal}(K/\mathbf{Q})$ is Abelian, $I_p(K)$ is independent of the choice of $\mathfrak{p}$ and hence well-defined. We call $I_p(K)$ the inertia group of p in K, whose order is called the ramification index of p in K, denoted by $e_p(K)$. If $e_p(K)=1$, p is said to be unramified in K, otherwise we say p is ramified. The fixed subfield of $I_p(K)$ in K, denote by K_p^I, is the inertial field of p. A basic fact is that p is unramified in K_p^I.

Theorem 1.1 Let K be an Abelian number field of degree n. Write

$$n=2^{t_0}q_1^{t_1}q_2^{t_2}\cdots q_m^{t_m},$$

where $q_1,q_2,\cdots,q_m$ are distinct odd primes, and $t_0\geqslant 0, t_i\geqslant 1$ for $1\leqslant i\leqslant m$. Let $p_1, p_2,\cdots,p_s$ be all ramified primes in K. For a prime p and an integer k, denote the standard p-adic order of k by $v_p(k)$. Then we have

(i) If 2 is unramified in K, then

$$\mathfrak{f}(K)=p_1p_2\cdots p_s\prod_{i=1}^{m}q_i^{v_{q_i}(e_{q_i}(K))},$$

(ii) If 2 is ramified in K, then

$$\mathfrak{f}(K)=\begin{cases}W_{s,m}, & \text{if } e_2(K(\sqrt{-1}))=e_2(K),\\ 2W_{s,m}, & \text{otherwise},\end{cases}$$

where

$$W_{s,m}=2^{v_2(e_2(K))}p_1p_2\cdots p_s\prod_{i=1}^{m}q_i^{v_{q_i}(e_{q_i}(K))}.$$

Remark 1 Zhang[6] gave a similar result for an Abelian number field K of degree p^r, where p is a prime number. But if p is ramified in K, Zhang's result did not give the explicit power of p in the conductor formula. In Ref. [7], Zhao and Sun gave the conductor formula for an Abelian number field of degree p, where p is a prime number. This article generalizes the above two conclusions. In our formula (Theorem 1.1), we give the explicit power of all primes which are wildly ramified in K, where K is any Abelian number field.

Let K, L and F be Abelian number fields such that $F\subseteq L$, then we define

$$res_K^L:\mathrm{Gal}(L/\mathbf{Q})\to\mathrm{Gal}(F/\mathbf{Q})\ \sigma\to\sigma|_F \tag{1}$$

where $\sigma|_F(\alpha)=\sigma(\alpha)(\forall\alpha\in F)$. Additionally, we also define that

$$\Omega_{\mathbf{Q}}(K,L):\mathrm{Gal}(KL/\mathbf{Q})\to \mathrm{Gal}(K/\mathbf{Q})\otimes\mathrm{Gal}(L/\mathbf{Q}),\ \sigma\to(\sigma|_K,\sigma|_L) \tag{2}$$

Our proof depends on the explicit analysis of the ramification index, and the key idea in our proof is to determine the structure of the inertia groups of an Abelian number field (Proposition 2.1 and Corollary 2.2) by using Kronecker-Weber theorem. In Section 2, we first deal with the case of a cyclic number field of prime power degree (Proposition 2.6), which is the main part of our discussion. The general case is established in Section 3 by viewing an Abelian field as a compositum of cyclic subfields of prime power degree.

2 Cyclicnumber fields of prime power degree

We start with a general result on the inertia group. The following result shows that the inertia group of a number field is determined by the inertia group of its Galois extension.

Proposition 2.1 Let K and L be Abelian number fields with $K\subseteq L$. Then $\mathrm{res}_K^L(I_p(L))=I_p(K)$ holds for every prime number p, where res_K^L is defined in Eq. (1).

Proof Let $\mathfrak{p}$ be a prime ideal in O_K lying above p. By the definition of inertia group, we have $\mathrm{res}_K^L(I_p(L))\subseteq I_p(K)$.

Let $\mathfrak{P}$ be a prime ideal in O_L lying above $\mathfrak{p}$, and $I_{\mathfrak{P}}(L)$ be the inertia group of $\mathfrak{p}$ in L, then $I_{\mathfrak{P}}(L)=\{\sigma\in\mathrm{Gal}(L/K)\mid\sigma(x)\equiv x(\mathrm{mod}\ \mathfrak{P}),\forall x\in O_L\}$. Thus

$$I_p(L)\cap\mathrm{Gal}(L/K)=I_{\mathfrak{P}}(L).$$

Noticing that the restriction map res_K^L is surjective with $\ker(\mathrm{res}_K^L)=\mathrm{Gal}(L/K)$, we have

$$I_p(L)(I_p(L)\cap \mathrm{Gal}(L/K))\cong \mathrm{res}_K^L(I_p(L)).$$

By the transitivity of ramification indices,

$$e_p(K)=\frac{e_p(L)}{e_{\mathfrak{p}}(L)}=|I_p(L)/(I_p(L)\cap \mathrm{Gal}(L/K))|$$
$$=|res_K^L(I_p(L))|.$$

Therefore $\mathrm{res}_K^L(I_p(L))=I_p(L)$. The proof is end.

By using Proposition 2.1 and Kronecker-Weber theorem, we can show that the inertia group of an Abelian number field is determined by the inertia group of a cyclotomic field.

Corollary 2.2 Let K be an Abelian number field, and p be a prime number. Then the inertia group $I_p(K)$ is isomorphic to a subgroup of $(\mathbf{Z}/p^r\mathbf{Z})^\times$ for some $r\geqslant 0$. In particular, $e_2(K)$ is a power of 2, and $I_p(K)$ is cyclic if p is odd.

Proof Let $\mathfrak{f}(K)=m$, then $K\subseteq \mathbf{Q}(\zeta_m)$. For a prime number p, write $m=p^r s$ with $\gcd(p,s)=1$, then $\mathbf{Q}(\zeta_m)=\mathbf{Q}(\zeta_{p^r})\mathbf{Q}(\zeta_s)$, and p is unramified in $\mathbf{Q}(\zeta_s)$. Notice that $\Omega_{\mathbf{Q}}(K,L)$ defined in Eq. (2) is a canonical embedding, thus $\mathrm{Gal}(KL/\mathbf{Q})$ can be regarded as a subgroup of $\mathrm{Gal}(K/\mathbf{Q})\otimes\mathrm{Gal}(L/\mathbf{Q})$. By Proposition 2.1, we have

$$I_p(\mathbf{Q}(\zeta_m))\cong \mathrm{res}_{\mathbf{Q}(\zeta_{p^r})}^{\mathbf{Q}(\zeta_m)}(I_p(\mathbf{Q}(\zeta_m)))\otimes$$
$$\mathrm{res}_{\mathbf{Q}(\zeta_s)}^{\mathbf{Q}(\zeta_m)}(I_p(\mathbf{Q}(\zeta_m)))\cong I_p(\mathbf{Q}(\zeta_{p^r}))=$$
$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q})\cong(\mathbf{Z}/p^r\mathbf{Z})^\times.$$

That is, $I_p(K)=\mathrm{res}_K^{\mathbf{Q}(\zeta_m)}(I_p(\mathbf{Q}(\zeta_m)))$ is isomorphic to a subgroup of $(\mathbf{Z}/p^r\mathbf{Z})^\times$.

If p is an odd prime, then $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is cyclic, and consequently $I_p(K)$ is a cyclic group. If $p=2$, $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is of order 2^{r-1}. The proof is end.

The main approach in this article is to usecompositum of Abelian number fields to explore the correlation between the conductor and the ramification index. The following result shows that the conductor of an Abelian field is determined by those of its subfields.

Lemma 2.3 Let K_1 and K_2 be two Abelian number fields. Then

$$\mathfrak{f}(K_1K_2)=\mathrm{lcm}(\mathfrak{f}(K_1),\mathfrak{f}(K_2)).$$

In general,

$$\mathfrak{f}(K_1\cdots K_r)=\mathrm{lcm}(\mathfrak{f}(K_1),\cdots,\mathfrak{f}(K_r)).$$

Proof Let $\mathfrak{f}(K_1)=m_1$, $\mathfrak{f}(K_2)=m_2$ and $\mathfrak{f}(K_1K_2)=n$. Then $m_1\mid n$ and $m_2\mid n$, thus $\mathrm{lcm}(m_1,m_2)\mid n$. On the other hand, we have

$$K_1K_2\subseteq \mathbf{Q}(\zeta_{m_1})\mathbf{Q}(\zeta_{m_2})=\mathbf{Q}(\zeta_{\mathrm{lcm}(m_1,m_2)}),$$

hence $n\leqslant \mathrm{lcm}(m_1,m_2)$. This implies $n=\mathrm{lcm}(m_1,m_2)$, the first result is proved. On the other hand, we also have that $\mathfrak{f}(K_1\cdots K_r)=\mathrm{lcm}(\mathfrak{f}(K_1),\cdots,\mathfrak{f}(K_r))$ by induction. The proof is end.

In the following, we concentrate on Abelian number fields with prime power degree.

Lemma 2.4 Let p be a prime number, and K be a cyclic number field of degree p^r. Assume that q is a prime number and $q\neq p$. Then we have

(i) The ramification index $e_q(K)\mid q-1$;

(ii) Let L be the unique subfield of $\mathbf{Q}(\zeta_q)$ with $[L:\mathbf{Q}]=e_q(K)$. Then there is $K'\subseteq KL$ in which q is unramified such that $KL=K'L$, and every prime number that is different from p and unramified in K is also unramified in K'.

Proof Notice that $e_q(K)$ is relatively prime to q. The first part follows directly from Corollary 2.2 that $e_q(K)$ is a divisor of $q^{r-1}(q-1)$ for some r. Consequently, there is a unique subfield $L\subseteq\mathbf{Q}(\zeta_q)$ such that $[L:\mathbf{Q}]=e_q(K)$.

If $q=2$ or q is unramified in K, then $e_q(K)=1$, and the second part is clear by taking $K'=K$. So, we may assume q is odd and ramifies in K. Then $I_q(K)$ and $I_q(KL)$ are cyclic by Corollary 2.2, and $I_q(KL)$ is isomorphic to a cyclic subgroup of $I_q(K)\otimes\mathrm{Gal}(L/\mathbf{Q})$ via $\Omega_{\mathbf{Q}}(K,L)$ defined in Eq. (2). Thus $|I_q(KL)|$ is a divisor of $e_q(K)$. On the other hand,

$$|I_q(KL)|\geqslant |I_q(K)|=e_q(K)$$

by Proposition 2.1. Therefore $|I_q(KL)|=e_q(K)$.

Now, taking $K'=(KL)_q^I$, we have $[KL:K']=e_q(K)$ and $L\cap K'=\mathbf{Q}$. Thus q is totally ramified in L and unramified in K' and

$$[K'L:\mathbf{Q}]=[L:\mathbf{Q}][K':\mathbf{Q}]=$$
$$[KL:K'][K':\mathbf{Q}]=[KL:\mathbf{Q}].$$

It follows that $K'L=KL$. If $p'\neq p$ is a prime number that is unramified in K, then $p'\neq q$ and p' is unramified in L. Hence p' is unramified in KL. In particular, p' is unramified in K'. The proof is end.

The following result can be proved in the same way as the above lemma.

Lemma 2.5 Let p be a prime number, and K be a cyclic number field of degree p^r. If $e_p(K)\neq 1$, and L is an Abelian number field such that

$$e_p(L)=e_p(KL)=[L:\mathbf{Q}],$$

then $(KL)_p^I L=KL$.

Proposition 2.6 Let p be a prime number, and K be a cyclic number field of degree p^r. Let q be a prime number that is ramified in K. Then

$$v_q(\mathfrak{f}(K))=\begin{cases}1, \text{ if } q\neq p;\\ v_p(e_p(K))+1, \text{if } q=p \text{ is odd},\\ 2, \text{ if } q=p=2,\ e_2(K(\sqrt{-1}))=2,\\ v_p(e_p(K))+1, \text{ if } q=p=2,\\ \quad e_2(K(\sqrt{-1}))=2.\end{cases}$$

Proof Let $n=v_q(\mathfrak{f}(K))$. Then $\mathfrak{f}(K)=q^n h$ such that $\gcd(q,h)=1$.

Case 1 If $q\neq p$, let L and K_1 be two Abelian number fileds satisfying the properties in Lemma 2.4. Then we have

$$K_1L=KL,\ \mathfrak{f}(L)=q,\ q\mid \mathfrak{f}(K)$$

and $q\nmid \mathfrak{f}(K_1)$. By Lemma 2.3, we have

$$\mathfrak{f}(KL)=\operatorname{lcm}(\mathfrak{f}(K),\mathfrak{f}(L))=q^n h,$$

and $\mathfrak{f}(K_1L)=\operatorname{lcm}(\mathfrak{f}(K_1),\mathfrak{f}(L))=q\mathfrak{f}(K_1)$.

It follows that $n=1$.

Case 2 If $q=p$, we assume that p is ramified in K with ramification index $e_p(K)=p^u$ $(u\geqslant 1)$. Since $e_p(K)\mid e_p(\mathbf{Q}(\zeta_{\mathfrak{f}(K)}))$ and $e_p(\mathbf{Q}(\zeta_{\mathfrak{f}(K)}))=p^{n-1}(p-1)$, we have that $n\geqslant u+1$. Let L_1 be a subfield of $\mathbf{Q}(\zeta_{p^{u+1}})$ such that $[L_1:\mathbf{Q}]=p^u$. Then we obtain that

$$\mathfrak{f}(L_1)=p^{u+1},\ \mathfrak{f}(KL_1)=\mathfrak{f}(K).$$

Subcase 2.1 If p is odd, $I_p(KL_1)$ is cyclic by Corollary 2.2. Notice that $I_p(KL_1)$ can be embedded as a subgroup of $I_p(K)\otimes\mathrm{Gal}(L_1|\mathbf{Q})$ via $\Omega_{\mathbf{Q}}(K,L_1)$ defined in Eq. (2). But both $I_p(K)$ and $\mathrm{Gal}(L_1|\mathbf{Q})$ are cyclic group of order p^u, and $e_p(KL_1)\geqslant e_p(K)=p^u$. It follows $e_p(KL_1)=p^u$.

Let $K_2=(KL_1)_p^I$. Since p is totally ramified in L_1 and $[L_1:\mathbf{Q}]=e_p(KL_1)$, we have $K_2L_1=KL_1$ by Lemma 2.5. Since p is unramified in K_2, we have $p\nmid \mathfrak{f}(K_2)$. Thus

$$\mathfrak{f}(K_2L_1)=p^{u+1}\mathfrak{f}(K_2),\ \mathfrak{f}(K_2L_1)=\mathfrak{f}(K).$$

Consequently $n=v_p(\mathfrak{f}(K))=u+1$.

Subcase 2.2 If $q=p=2$, then $L_1=\mathbf{Q}(\zeta_{2^{u+1}})$, thus we know that $\mathrm{Gal}(L_1|\mathbf{Q})\cong(\mathbf{Z}/2^{u+1}\mathbf{Z})^\times$. Since $\mathfrak{f}(KL_1)=2^n h$, and the inertia group $I_2(\mathbf{Q}(\zeta_{2^n h}))$ is isomorphic to $(\mathbf{Z}/2^n\mathbf{Z})^\times$, $I_2(KL_1)$ is isomorphic to a subgroup of $(\mathbf{Z}/2^n\mathbf{Z})^\times$. Then $I_2(KL_1)$ is cyclic or isomorphic to $(\mathbf{Z}/2^m\mathbf{Z})^\times$ for some $3\leqslant m\leqslant n$.

(i) If $I_2(KL_1)$ is cyclic, then $\mathrm{Gal}(L_1|\mathbf{Q})$ must be cyclic by Proposition 2.1. Consequently $u=1$, and $e_2(L_1)=2$. By Lemma 2.5, we have $K_2L_1=KL_1$ for $K_2=(KL_1)_p^I$. Notice

$$\mathfrak{f}(KL_1)=\mathfrak{f}(K),\ \mathfrak{f}(K_2L_1)=4\mathfrak{f}(K_2).$$

Thus $n=2$.

(ii) If $I_2(KL_1)$ is isomorphic to $(\mathbf{Z}/2^m\mathbf{Z})^\times$ for some $3\leqslant m\leqslant n$, then we obtain that

$$I_2(KL_1)\cong\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2^{m-2}\mathbf{Z}.$$

Notice that $\mathrm{res}_K^{KL_1}(I_2(KL_1))=I_2(K)$ is cyclic of order 2^u, we have $e_2(KL_1)=2^{u+1}$, $m=u+2$. Let $L_2=\mathbf{Q}(\zeta_{2^{u+2}})$, then $e(KL_2)=2^{u+1}$ by Corollary 2.2. Setting $K_3=(KL_2)_2^I$, we have $K_3L_2=KL_2$ by Lemma 2.5. Since $\mathfrak{f}(K_3L_2)=2^{u+2}\mathfrak{f}(K_3)$, we have $\mathfrak{f}(KL_2)=2^n h$. Thus $n=u+2$.

The above discussion shows that $I_2(KL_1)$ is cyclic if and only if $e_2(K(\sqrt{-1}))=2$. The proof is end.

Let K be same as Proposition 2.6, and we assume that $p_1,p_2,\cdots,p_s$ are all prime numbers that are ramified in K. If $p_i\neq p$, then $v_{p_i}(\mathfrak{f}(K))=1$, by Proposition 2.6. If p is ramified or equivalently $p_i=p$ for some i, then we have

$$v_p(\mathfrak{f}(K))=\begin{cases}v_p(e_p(K))+1, \text{ if } p \text{ is odd},\\ 2, \text{ if } p=2,\ e_2(K(\sqrt{-1}))=2,\\ v_p(e_p(K))+2, \text{ if } p=2\\ \quad e_2(K(\sqrt{-1}))\neq 2.\end{cases}$$

Thus

$$\mathfrak{f}(K)=\begin{cases}e_p(K)p_1p_2\cdots p_s, \text{ if all } p_i\neq 2,\\ 2\,p_1p_2\cdots p_s, \text{ if } p_1=2,\\ \quad e_2(K(\sqrt{-1}))=2,\\ 2\,e_2(K)p_1p_2\cdots p_s, \text{ if } p_1=2,\\ \quad e_2(K(\sqrt{-1}))\neq 2.\end{cases}$$

We summarize the result in the following theorem.

Theorem 2.7 Let p be a prime number, and K be a cyclic number field of degree p^r. Let $p_1, p_2, \cdots, p_s$ be all primes which are ramified in K. We have

(i) If 2 is unramified in K, then

$$\mathfrak{f}(K)=e_p(K)p_1p_2\cdots p_s;$$

(ii) If 2 is ramified in K, then

$$\mathfrak{f}(K)=\begin{cases}2\,p_1\cdots p_s, & \text{if } e_2(K(\sqrt{-1}))=2,\\ 2\,p_1\cdots p_2e_2(K), & \text{otherwise.}\end{cases}$$

Based on the conductor formula in Theorem 2.7, we can easily compute the conductor of a quadratic field.

Corollary 2.8 Let d be a square-free integer, and $K=\mathbf{Q}(\sqrt{d})$. Then

$$\mathfrak{f}(\mathbf{Q}(\sqrt{d}))=\begin{cases}|d|, & \text{if } d\equiv1 \pmod 4,\\ |4d|, & \text{if } d\not\equiv1 \pmod 4.\end{cases}$$

Proof Let $d=\pm p_1p_2\cdots p_m$ be the prime decomposition of d, and $d(K)$ be the discriminant of K. Then

$$d(K)=\begin{cases}|d|, & \text{if } d\equiv1 \pmod 4,\\ |4d|, & \text{if } d\not\equiv1 \pmod 4.\end{cases}$$

Notice that a prime number$p$ is ramified in K if and only if $p|d(K)$.

If $d\equiv1 \pmod 4$, then 2 is unramified in K, and $p_1, p_2, \cdots, p_m$ are all primes which are ramified in K. By Theorem 2.7, we have

$$\mathfrak{f}(K)=p_1p_2\cdots p_m=|d|.$$

If $d\equiv2 \pmod 4$, then $p_1, p_2, \cdots, p_m$ are all primes which are ramified in K. Since $K(\sqrt{-1})$ has exactly three quadratic subfields: $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{d})$ and $\mathbf{Q}(\sqrt{-d})$, in which 2 is ramified, then $e_2(K(\sqrt{-1}))=4$. By Theorem 2.7, we have. $\mathfrak{f}(K)=4|d|$.

If $d\equiv3 \pmod 4$, then $2, p_1, p_2, \cdots, p_m$ are all primes which are ramified in K. Since $\mathbf{Q}(\sqrt{-d})\subseteq K(\sqrt{-1})$ and 2 is unramified in $\mathbf{Q}(\sqrt{-d})$, then $e_2(K(\sqrt{-1}))=2$. Again $\mathfrak{f}(K)=|4d|$.

3 The conductor of general Abelian number fields

In this section, we prove the main result for general Abelian number fields.

Proof of Theorem 1.1 Let K be an Abelian number field with Galois group G. By the structure theorem for finite Abelian groups, G is a direct product of cyclic subgroups of prime power order. For each such direct summand H of G, there exists a subgroup H' such that $G=H\otimes H'$. Let M be the fixed field of H' in K. We know that M is Galois over $\mathbf{Q}$ and $\mathrm{Gal}(M/\mathbf{Q})$ is isomorphic to H. Hence M is cyclic number field of prime power order. It follows that there exist cyclic subfields K_i of prime power order such that $K=K_1K_2\cdots K_r$. In other words, K is a compositum of cyclic subfields of prime power degree.

Let $[K:\mathbf{Q}]=2^{t_0}q_1^{t_1}q_2^{t_2}\cdots q_m^{t_m}$, where $q_1, q_2, \cdots, q_m$ are distinct odd primes, and $t_0\geqslant0, t_j\geqslant1$ for $1\leqslant j\leqslant m$. Then $[K_i:\mathbf{Q}]$ is a power of 2 or q_j. Let $p_1, p_2, \cdots, p_s$ be all ramified primes in K. Then, for each K_i, $p_1, p_2, \cdots, p_s$ are the only possible prime divisors of $\mathfrak{f}(K_i)$. Notice that the transitivity of ramification index implies $e_p(K_i)\mid e_p(K)$ for any prime integer p.

Case 1 If 2 is unramified in K, then $e_2(K)=1$, and all p_i are odd. By Theorem 2.7, $\mathfrak{f}(K_i)$ is a divisor of $p_1p_2\cdots p_se_{q_j}(K)$ for some j. In virtue of Lemma 2.3, we have

$$\mathfrak{f}(K)\mid p_1\,p_2\cdots p_s\prod_{j=1}^{m}q_j^{v_{q_j}(e_{q_j}(K))}.$$

Here $v_p(K)$ denotes the standard p-adic valuation of k. Let $L=\mathbf{Q}(\zeta_{\mathfrak{f}(K)})$, we have

$$K\subseteq L,\ e_{q_j}(K)\mid e_{q_j}(L).$$

If $q_j=p_i$ for some i, due to Corollary 2.2, $I_{q_j}(K)$ is cyclic, hence

$$v_{q_j}(e_{q_j}(K))\leqslant v_{q_j}(e_{q_j}(L))=v_{q_j}(\mathfrak{f}(K))-1.$$

If $q_j\neq p_i$ for all i, then $e_{q_j}(K)=0$. It follows

$$p_1\,p_2\cdots p_s\prod_{j=1}^{m}q_j^{v_{q_j}(e_{q_j}(K))}\mid\mathfrak{f}(K).$$

Therefore,

$$\mathfrak{f}(K)=p_1\,p_2\cdots p_s\prod_{j=1}^{m}q_j^{v_{q_j}(e_{q_j}(K))}.$$

Case 2 If 2 is ramified in K, by Lemma 2.4, $[K:\mathbf{Q}]$ must be even. Similarly, based on Corollary 2.2 and Lemma 2.4, we have

$$2^{v_2(e_2(K))}\,p_1\cdots p_s\prod_{j=1}^{m}q_j^{v_{q_j}(e_{q_j}(K))}\mid\mathfrak{f}(K)$$

In particular, $v_2(\mathfrak{f}(K)) \geqslant v_2(e_2(K))+1$. By Theorem 2.7, we can assume that

$$\mathfrak{f}(K) = 2^t p_1 p_2 \cdots p_s \prod_{j=1}^{m} q_j^{v_{q_j}(e_{q_j}(K))},$$

where $t = v_2(e_2(K))$ or $v_2(e_2(K))+1$. We know from Proposition 2.1 that $I_2(K_i) = \mathrm{res}_{K_i}^{K}(I_2(K))$ is always cyclic.

Subcase 2.1 If the inertia group $I_2(K)$ is not cyclic, then $2\,e_2(K_i) \mid e_2(K)$ holds for all i. On the other hand, Theorem 2.7 implies

$$v_2(\mathfrak{f}(K_i)) \leqslant v_2(e_2(K_i))+2.$$

Therefore, $v_2(\mathfrak{f}(K)) \leqslant v_2(e_2(K))+1$, which forces $t = v_2(e_2(K))$. Now

$$e_2(K(\sqrt{-1})) \leqslant e_2(\mathbf{Q}(\zeta_{\mathfrak{f}(K)})) = e_2(K) \leqslant e_2(K(\sqrt{-1})).$$

Hence $e_2(K(\sqrt{-1})) = e_2(K)$ and $t = v_2(e_2(K))$.

Subcase 2.2 If $I_2(K)$ is cyclic, we set $L = \mathbf{Q}(\zeta_n)$, where $n = 2\,e_2(K)$. Notice that $I_2(KL)$ can be embedded as a subgroup of $I_2(K) \otimes \mathrm{Gal}(L/\mathbf{Q})$ via the canonical map $\Omega_{\mathbf{Q}}(K, L)$.

(i) If $I_2(KL)$ is cyclic, then $I_2(K)$ is cyclic by Proposition 2.1. Thus $e_2(K) = 2$ and $L = \mathbf{Q}(\sqrt{-1})$. Eventually $e_2(KL) = 2$. Let $K' = (KL)_2^I$, then $K'L = KL$ and

$$\mathfrak{f}(K) = \mathfrak{f}(KL) = \mathfrak{f}(K'L) = 4\mathfrak{f}(K').$$

Hence $t = v_2(e_2(K)) = 1$.

(ii) If $I_2(KL)$ is not cyclic, then $e_2(KL) = 2\,e_2(K)$ by Corollary 2.2. Thus

$$v_2(\mathfrak{f}(KL)) \geqslant v_2(e_2(K))+2.$$

Therefore $v_2(\mathfrak{f}(K)) \geqslant v_2(e_2(K))+2$. Then we have $t = v_2(e_2(K))+1$.

(iii) We next have a close analysis on the condition that $I_2(KL)$ is not cyclic. If $v_2(e_2(K)) = 1$, one must has

$$e_2(K(\sqrt{-1})) > e_2(K).$$

If $v_2(e_2(K)) > 1$, then we know that

$$K(\sqrt{-1}) = K^R(\sqrt{-1}),$$

and $I_2(K^R)$ is a cyclic group, where K^R denotes the maximal real subfield of $K(\sqrt{-1})$. Thus $\Omega_{\mathbf{Q}}(K^R, \mathbf{Q}(\sqrt{-1}))$ is an isomorphism, which induces an isomorphism:

$$I_2(K(\sqrt{-1})) \cong I_2(K^R) \otimes \mathrm{Gal}(\mathbf{Q}(\sqrt{-1})\mathbf{Q}/)$$

is not a cyclic group. It follows that $I_2(K(\sqrt{-1}))$ is not cyclic and

$$e_2(K) \neq e_2(K(\sqrt{-1})).$$

This shows that $I_2(KL)$ is not cyclic if and only if $e_2(K(\sqrt{-1})) \neq e_2(K)$.

In summary, if 2 is ramified in K, then

$$\mathfrak{f}(K) = \begin{cases} W_{s,m}, & \text{if } e_2(K(\sqrt{-1})) = e_2(K), \\ 2\,W_{s,m}, & \text{otherwise}, \end{cases}$$

where

$$W_{s,m} = 2^{v_2(e_2(K))} p_1 p_2 \cdots p_s \prod_{j=1}^{m} q_j^{v_{q_j}(e_{q_j}(K))}.$$

The proof is end.

References:

[1] Mäki S. The conductor density of Abelian number fields [J]. J London Math Soc, 1993, 47: 18.

[2] Johnston H. On the trace map between absolutely Abelian number fields of equal conductor [J]. Acta Arith, 2006, 122: 63.

[3] Schoof R. Class numbers of real cyclotomic fields of prime conductor [J]. Math Comp, 2003, 72: 913.

[4] Agathocleous E. On the class numbers of real cyclotomic fields of conductor pq [J]. Acta Arith, 2014, 165: 257.

[5] Hasse H. Über die klassenzahl abelscher zahlkörper [M]. Berlin: Springer-Verlag, 1985.

[6] Zhang X K. A simple construction of genus fields of Abelian number fields [J]. Proc Amer Math Soc, 1985, 94: 393.

[7] Zhao Z J, Sun G R. A note on the conductor of cyclic number fields [J]. Acta Math Sin, 2016, 59: 761.

引用本文格式:

中　文: 邓先涛, 彭国华. Abel 数域的导子计算公式[J]. 四川大学学报: 自然科学版, 2023, 60: 031003.

英　文: Deng X T, Peng G H. A conductor formula for Abelian number fields [J]. J Sichuan Univ: Nat Sci Ed, 2023, 60: 031003.