Conductor ideals in Galois extensions

Chanwit Prabpayak

ABSTRACT

Let $K$ be an algebraic number field, $O_K$ is its ring of integers. An order $O$ in $K$ is a subring of $O_K$ which contains a $\mathbb{Z}$-basis for the field $K$. The conductor of $O$ is the largest ideal of $O_K$ contained in $O$. This paper showed that $\mathbb{Z} + f$ is the only one order in quadratic number fields having conductor ideal and conductor ideals were characterized in a Galois extension over $\mathbb{Q}$.

Keywords: conductor ideal, order

INTRODUCTION

Throughout this paper, let $\mathbb{Z}$, $\mathbb{Z}^+$ and $\mathbb{Q}$ denote the set of integers, the set of positive integers and the set of rational numbers respectively.

Let $K$ be an algebraic number field. $O_K$ denotes the ring of integers of the field $K$. A subring $O$ of $K$ is called an order if $O$ is a finitely generated $\mathbb{Z}$-module containing a $\mathbb{Z}$-basis for $K$, or equivalently, $O$ is a subring of finite index within the ring of integers of $K$. For each order, there is a special ideal which is called the conductor of the order. In quadratic number fields, it is well known that the conductor ideal is just the principal ideal $(a)$ for some $a \in \mathbb{Z}^+$. Furtwängler (1919) showed how ideals in the ring of integers of an algebraic number field can be conductor ideals. His results were again given in a new variant of proof by Lettl and Prabpayak (2014). Prabpayak (2014) studied orders in pure cubic number fields. He characterized conductor ideals of order and he could determine the number of all orders with the given conductor ideal in such fields.

Let $f$ be a conductor ideal in a quadratic number field. This paper shows that there exists exactly one order in this field with the conductor ideal $f$. Moreover, conductor ideals are characterized in a Galois extension over $\mathbb{Q}$.

MATERIALS AND METHOD

Let $K$ be an algebraic number field. For any non-zero ideal $I$ of $O_K$, let $N(I)$ denote its norm. For any non-maximal order $O$ in $K$, the set $f = \{x \in K \mid xO_K \subset O\}$ is called the conductor of $O$. Then $f$ is an ideal of $O$ and also of $O_K$. So, call $f$ the conductor ideal of $O$. It can be easily shown that $\mathbb{Z} + f$ is the smallest order in $O_K$ containing $f$. Therefore $\mathbb{Z} + f \subset O$.

Theorem 1. Let $K$ be an algebraic number field and $P$ be a rational prime with $(p) = pO_K = P_1^{e_1} \cdots P_g^{e_g}$ where $P_1, \ldots, P_g$ are distinct prime ideals of $O_K$ and $e_1, \ldots, e_g$ are positive integers. Let $r_i$ denote the inertial degree of $P_i$, i.e. $N(P_i) = p^{r_i}$. Let $k$ be a positive integer. Then $P_k$ is a conductor ideal if and only if one of the following two conditions holds:

Faculty of Science and Technology, Rajamangala University of Technology Phra Nakhon, Bangkok 10800, Thailand.

E-mail: chanwit.p@rmutp.ac.th

Received date : 08/01/15 Accepted date : 21/04/15
1. \( r_i \geq 2 \),
2. \( r_i = 1 \) and \( k \) is not congruent to 1 modulo \( e_i \).

**Theorem 2.** Let \( K \) be an algebraic number field and \( p \) be a rational prime with \( (p) = P_1^{r_1} \cdots P_g^{r_g} \) where \( P_1, \ldots, P_g \) are distinct prime ideals of \( O_K \) of norm \( N(P_i) = p^{e_i} \) and \( g, e_1, \ldots, e_g \) are positive integers. Let \( k_i \) be non-negative integers for \( i = 1, \ldots, g \). Put \( f = P_1^{k_1} \cdots P_g^{k_g} \). Then \( f \) is the conductor ideal of some order in \( K \) if and only if for every integer \( 1 \leq i \leq g \) with \( k_i \geq 1 \) then: if \( r_i = 1 \) and \( k_i \equiv 1 \mod e_i \), then there exists some \( j \in \{1, \ldots, g\} \setminus \{i\} \) with \( k_j > \frac{k_i - 1}{e_i} e_j \).

Theorem 1 and Theorem 2 were given by Furtwängler (1919) which show how any ideal in \( \mathbb{Z} \) can be a conductor ideal.

**Theorem 3.** Let \( K \) be an algebraic number field. Let \( f \) be an ideal of \( O_K \) and \( f = f_1 \cdots f_g \) where \( f_i \) are ideals of \( O_K \) of norm \( N(f_i) = p_i^{r_i} \) with positive integers \( r_i \) and pairwise different prime numbers \( p_i \). Then there exists an order in \( K \) with conductor ideal \( f \) if and only if for all non-negative integer \( 1 \leq i \leq g \) there exist orders \( O_i \) in \( K \) with conductor ideal \( f_i \).

Theorem 3 was given by Prabpayak (2014). From this theorem, it suffices to investigate those ideals \( f \) whose norm is a power of some rational prime \( p \), and the characterization of \( f \) depends on how the principal ideal \( (p) \) factors into prime ideals of \( O_K \).

**RESULTS AND DISCUSSION**

Let \( K \) be a quadratic number field. As mentioned above, it suffices to investigate ideals whose norm is a power of some rational prime \( p \), and the characterization of those ideals depends on how the principal ideal \( (p) \) factors into prime ideals of \( O_K \), now let \( p \) be a prime number. Then, there are three possibilities of decomposition of \( p \) that \( p \) factors into prime ideals of \( O_K \). Using the notations in Theorem 2:

**Case 1:** \( p \) ramifies in \( K \). This is \( (p) = P^2 \). It is known that \( n = e_1 r_1 + \cdots + e_g r_g \). Then, \( e_1 = 2 \) and \( r_1 = 1 \). By Theorem 1, for every positive integer \( k \), \( P^k \) is a conductor ideal when \( k \) is not congruent to 1 modulo 2. Thus \( k \) is even, and then there is a positive integer \( d \) such that \( k = 2d \). Now \( P^{kd} = (p^d) \).

**Case 2:** \( p \) splits in \( K \) as \( (p) = P_1 P_2 \) where \( P_1 \) and \( P_2 \) are different prime ideals of \( O_K \). Then \( r_1 = r_2 = e_1 = e_2 = 1 \). Let \( f = P_1^{k_1} P_2^{k_2} \) with positive integers \( k_1, k_2 \). Since \( r_1 = 1 \) and \( k_1 \equiv 1 \mod e_1 \), by Theorem 2, \( f \) is a conductor ideal when \( k_2 > \frac{k_1 - 1}{e_1} e_2 \). But \( e_1 = e_2 = 1 \), then, obtain \( k_1 \leq k_2 \). Also, \( r_2 = 1 \) and \( k_2 \equiv 1 \mod e_2 \), then \( f \) is a conductor ideal when \( k_1 > \frac{k_2 - 1}{e_2} e_1 \), i.e., \( k_2 \leq k_1 \). It follows that \( f \) is a conductor ideal whenever \( k_1 = k_2 \). Therefore \( f = P_1^{k_1} P_2^{k_2} = P_1^{k_1} P_2^{k_1} = (P_1 P_2)^{k_1} = (p)^{k_1} \).

**Case 3:** \( p \) is inert or \( p \) remains prime. Then \( e_1 = 1 \) and \( r_1 = 2 \). By Theorem 1, \( (p)^k \) is a conductor ideal for all positive integers \( k \).

From the three cases it can be concluded that for any positive integer \( k \), \( (p)^k \) is a conductor ideal. Now it can be described how conductor ideals in quadratic number fields can be obtained by using the fact that every positive integer greater than 1 can be expressed as the product of primes and Theorem 3.

Let \( f \) be an ideal of \( O_K \). It is known that all conductor ideals are just of the form \( (p)^k \) for arbitrary \( k \in \mathbb{Z}^+ \). By Theorem 3, the ideal \( f \) is a conductor ideal if and only if there exists \( a \in \mathbb{Z} \) such that \( f = (a) = aO_K \). Suppose \( K = \mathbb{Q} \sqrt{d} \) with a unique square-free integer \( d \in \mathbb{Z} \setminus \{1\} \). Then \( \{1, \omega\} \) is an integral basis for the field \( K \), where

\[
\omega = \begin{cases} 
\frac{1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4, \\
\sqrt{d} & \text{otherwise}.
\end{cases}
\]
The ring of integers of $K$ is given by $O_K = \mathbb{Z} + \omega\mathbb{Z}$. Let $f = (a)$ be a conductor ideal with $a \in \mathbb{Z}^*$. Then $\mathbb{Z} + f$ is an order in $O_K$ with conductor ideal $f$. Since $\mathbb{Z} + f = \mathbb{Z} + aO_K = \mathbb{Z} + a\omega\mathbb{Z}$, $(1, a\omega)$ is a $\mathbb{Z}$-basis for the order $\mathbb{Z} + f$.

Let $A = \mathbb{Z} + f$. If $O$ is another order in $O_K$ with conductor ideal $f$, then one can prove that $A$ is the smallest order in $O_K$ with conductor ideal $f$. Then, $A \subseteq O \subseteq O_K$. There exists $a, b \in \mathbb{Z}^*$ such that $(1, a+b\omega)$ is a $\mathbb{Z}$-basis for $O$. Then $(1, b\omega)$ is also a $\mathbb{Z}$-basis for $O$ and $b \neq 1$. Since $(1, \omega)$ is a $\mathbb{Z}$-basis for $O_K$, $(b, b\omega)$ is a $\mathbb{Z}$-basis for $bO_K$. Hence $(b) \subseteq O$. But $a\omega \in A \subseteq O$, and there exist $m, n \in \mathbb{Z}^*$ such that $a\omega = m + nb\omega$. Thus $a = nb$. Suppose that $n > 1$. Then $a$ is divisible by $b$. It follows that $(a)$ is strictly contained in $(b)$. This is a contradiction to the maximality of $f$ in $O$. Hence $n = 1$, and thus $a = b$. This means $A = O$. Therefore $A$ is the only order in the quadratic number field $K$ with conductor ideal $f$.

Let $K$ be a Galois extension over $\mathbb{Q}$ and $[K : \mathbb{Q}] = n$. Let $p$ be a prime number and $(p) = P_1^{e_1} \cdots P_g^{e_g}$ where $g$ is a positive integer and $P_1, \ldots, P_g$ are distinct prime ideals of $O_K$. Then all ramification indices are equal, $e_1 = e_2 = \cdots = e_g = e$ for some $e \in \mathbb{Z}^*$, and so are the inertial degrees, i.e., $r_1 = r_2 = \cdots = r_g = r$ for some $r \in \mathbb{Z}^*$. Thus, $egr = n$. Let $f = P_1^{k_1} \cdots P_g^{k_g}$ with $k_1, \ldots, k_g \in \mathbb{Z}^*$. Theorem 2 can be used to investigate all ideals $f$ which are conductor ideals.

Suppose $e = 1$. By Theorem 2, if $r \geq 2$, there is no restriction on $k_i$ for all $i$. Then consider the case that $r = 1$. Assume $k_1 \leq k_2 \leq \ldots \leq k_g$. Since $k_i \equiv 1 \mod e_i$ and $k_i < k_g$ always hold for all $i \neq g$, it satisfies conditions of Theorem 2, and thus there is no restriction on $k_i$ for all $i \neq g$. Next conditions on $k_g$ can be determined. Since $e_g = 1$ and $k_g \equiv 1 \mod e_g$ hold, the condition $k_1 \geq k_g$ must hold for some $i \neq g$. Choose the weakest condition $k_{g-1} \geq k_g$ and this implies $k_{g-1} = k_g$. Hence $f = P_1^{k_1} P_2^{k_2} \cdots P_{g-1}^{k_{g-1}} P_g^{k_g}$ is a conductor ideal. Therefore $f$ is a conductor ideal if and only if the largest value of the exponents $k_i$ appears twice.

If $e \geq 2$, then it follows from Theorem 2 that there is no restrictions on $k_i (i = 1, \ldots, g)$ when $r \geq 2$. For $r = 1$, assume $k_1 \leq k_2 \leq \cdots \leq k_g$. For each $j \in \{1, \ldots, g\}$, if $k_j$ is not congruent to 1 modulo $e_j$, then the following condition must hold:

\[ \exists l \neq j : k_l > \frac{k_j - 1}{e_j}. \]

This implies $\exists l \neq j : k_l \geq k_j$. By the assumption, the condition above holds for all $j \neq g$ by taking $k_1 = k_g$. Then there is no restriction on $k_i$ for $i = 1, \ldots, g-1$. If $k_g \equiv 1 \mod e_g$, then $k_g \geq k_g$ must hold for some $l \neq g$. Choose the weakest condition $k_{g-1} \geq k_g$ and then $k_{g-1} = k_g$. Hence $f = P_1^{k_1} P_2^{k_2} \cdots P_{g-1}^{k_{g-1}} P_g^{k_g-1}$ is a conductor ideal. Therefore $f = P_1^{k_1} \cdots P_g^{k_g}$ is a conductor ideal if and only if the largest value of the exponents $k_i$ appears twice.

For $g = 1$, use Theorem 1 directly to investigate all conductor ideals $f$.

**CONCLUSION**

The following theorems arise from the above:

**Theorem 4.** Let $K$ be a quadratic number field. For any conductor ideal $f$ in $O_K$, there is exactly one order in $O_K$ with conductor ideal $f$, namely, $\mathbb{Z} + f$.

**Theorem 5.** Let $K$ be a Galois extension over $\mathbb{Q}$ and let $p$ be a prime number with $(p) = P_1^{e_1} \cdots P_g^{e_g}$ where $P_1, \ldots, P_g$ are distinct prime ideals of $O_K$ and $e_1, \ldots, e_g$ are positive integers. Let $f = P_1^{k_1} \cdots P_g^{k_g}$ with positive integers $k_1, \ldots, k_g$. Then $f$ is a conductor ideal if and only if the inertial degree of $P_i$ is larger than 1 or in case the inertial degree equals 1: If the largest of the exponents $k_i$ is congruent to 1 modulo $e_i$ then the exponents $k_i$ must appear twice.
ACKNOWLEDGEMENT

The author is highly grateful to referees for their valuable comments and suggestions which were helpful in the improvement of this paper.

LITERATURE CITED

