SURJECTIVITY OF TRACE FOR RELATIVE EXTENSIONS

SUDIPA DAS AND R. THANGADURAI

ABSTRACT. Let L/K be a finite extension of number fields and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be its ring of integers respectively. We classify all the finite extensions L/K such that the trace map restricted to $\mathcal{O}_L$ is surjective. When $\mathcal{O}_K$ is a PID, we classify all the finite extensions L/K of number fields such that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = [L:K]\mathcal{O}_K$.

1. INTRODUCTION

Let L/K be a finite extension of number fields and $\mathcal{O}_L$ and $\mathcal{O}_K$ be the ring of integers of L and K respectively. It is easy to see that the trace map $\mathrm{Tr}_{L/K} : L \to K$ is surjective. Since $\mathrm{Tr}(\mathcal{O}_L) \subset \mathcal{O}_K$, we can consider the restricted trace map $\mathrm{Tr}_{L/K} : \mathcal{O}_L \to \mathcal{O}_K$. It is a natural question to ask whether this restricted trace map is surjective or not?.

One can easily hit upon plenty of counter-examples when L is a quadratic extension of $K = \mathbb{Q}$. More precisely, if $L = \mathbb{Q}(\sqrt{m})$ for a square-free integer m with $m \equiv 2, 3 \pmod 4$, it is well-known that the ring of integers $\mathcal{O}_L = \mathbb{Z}[\sqrt{m}]$. If $\alpha \in \mathbb{Z}[\sqrt{m}]$, then $\alpha = a + b\sqrt{m}$ and hence $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha) = a + b\sqrt{m} + a - b\sqrt{m} = 2a \in 2\mathbb{Z}$. Thus, $\mathrm{Tr}_{L|\mathbb{Q}}(\mathbb{Z}[\sqrt{m}]) = 2\mathbb{Z}$ and hence the restricted trace map is not surjective in this case. It is known that when $m \equiv 2$ or 3 modulo 4, the absolute discriminant d_L of L is $4m$.

Suppose the extension L/K is of degree $d \geq 2$. Note that $\mathrm{Tr}_{L/K} : \mathcal{O}_L \to \mathcal{O}_K$ is a homomorphism of abelian groups $\mathcal{O}_L$ and $\mathcal{O}_K$ and hence the image $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is an additive subgroup of $\mathcal{O}_K$. Since $\mathrm{Tr}_{L/K}(k\alpha) = k \cdot \mathrm{Tr}_{L/K}(\alpha)$ for all $k \in \mathcal{O}_K$ and $\alpha \in \mathcal{O}_L$, we conclude that $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is an ideal of $\mathcal{O}_K$. Before we state our results, we define the following terminology.

Definition 1.1. *Let L/K be a finite extension of number fields and $\mathcal{O}_L$ (respectively, $\mathcal{O}_K$) be the ring of integers of L (respectively, K). A non-zero prime ideal $\mathfrak{P}$ in $\mathcal{O}_L$ lying above a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\mathfrak{P}^e$ exactly divides $\mathfrak{p}\mathcal{O}_L$ (we write $\mathfrak{P}^e \| \mathfrak{p}\mathcal{O}_L$) for some natural number $e \geq 1$, is said to be*

- tamely ramified *in L, if e is coprime to the characteristic of the finite field $\mathcal{O}_K/\mathfrak{p}$;*
- wildly ramified *in L, if the characteristic of the finite field $\mathcal{O}_K/\mathfrak{p}$ divides e;*
- totally ramified *in L, if $e = [L:K]$;*

In Galois theory, it is well-known that every finite Galois extension L/K with Galois group G admits a normal basis, that is, there exists an element $\alpha \in L$ such that $\{\sigma(\alpha) \ : \ \sigma \in G\}$ forms an K-basis for L. A related question is whether L admits a normal integral basis or not?. That is, does there exists $\alpha \in \mathcal{O}_L$ such that the set $\{\sigma(\alpha) \ : \ \sigma \in G\}$ forms an integral

2010 *Mathematics Subject Classification.* Primary 11R04, 11R29 .

Key words and phrases. Trace forms, Tame and Wild number fields, ramification indexes.

basis for $\mathcal{O}_L$ as an $\mathcal{O}_K$ module?. It is known, due to S. Ullom [8], that if a finite Galois extension L/K of number fields or $\mathfrak{p}$-adic fields admit a normal integral basis, then L/K must be a tame extension which in turn implies the trace map restricted to $\mathcal{O}_L$ must be a surjective map. See for instance A. Frohlich [3] and E. Aljadeff [1].

In this article, we consider the relative extensions and prove the following.

Theorem 1.1. *Let L/K be a finite extension of number fields of degree d. Then the following statements are equivalent:*

1. $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$;
2. *Let $\mathfrak{p}$ be any prime ideal divisor of $d\mathcal{O}_K$ and $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}$ be the prime ideal factorization of $\mathfrak{p}$ in $\mathcal{O}_L$ for some integers $s \geq 1$ and $e_i \geq 1$. Then, there exists an integer i with $1 \leq i \leq s$ such that $\mathfrak{P}_i$ is tamely ramified in L.*

Theorem 1.2. *Let L/K be a finite extension number fields of degree d. Consider the following three statements:*

1. *$\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is a proper ideal of $\mathcal{O}_K$.*
2. *There is a prime factor $\mathfrak{p}$ in $d\mathcal{O}_K$ such that $\mathfrak{p}^d$ divides disc(L/K).*
3. *L/K is wildly ramified.*

Then (1) $\iff$ (2) $\implies$ (3).

When $K = \mathbb{Q}$, and if $L/\mathbb{Q}$ is any finite extension (not necessarily Galois), then Theorem 1.1 and Theorem 1.2 are proved by F. Battistoni and T. Zaimi [2].

Corollary 1.1. *Let L/K be a finite Galois extension of number fields of degree d. Then the three statements in Theorem 1.2 are equivalent.*

The following Corollary is a rephrasing of the statements (1) and (2) in Theorem 1.2.

Corollary 1.2. *Let L/K be a finite extension of number fields of degree d. If $\mathfrak{p}^d$ does not divide the disc(L/K) for every prime ideal $\mathfrak{p}$ dividing $d\mathcal{O}_K$, then $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$. In other words if for any prime $\mathfrak{p}$ dividing $d\mathcal{O}_K$, the highest power of $\mathfrak{p}$ dividing* $\mathrm{disc}(L/K)$ *is atmost $(d-1)$, then L/K is tamely ramified.*

Corollary 1.3. *Let L/K be a finite extension of number fields of degree d. Let $\mathfrak{p}$ be a maximal ideal in $\mathcal{O}_K$. If $\mathfrak{p}$ is totally and tamely ramified in L, then the highest power of $\mathfrak{p}$ dividing* $\mathrm{disc}(L/K)$ *is equal to $d-1$. Conversely, if the highest power of $\mathfrak{p}$ dividing* $\mathrm{disc}(L/K)$ *is $d-1$, then $\mathfrak{p}$ is totally ramified if and only if it is tamely ramified.*

Though Theorem 1.2 says that for any prime divisor $\mathfrak{p}$ of $d\mathcal{O}_K$, we have $\mathfrak{p}^d$ divides $\mathrm{disc}(L/K)$. However, $v_{\mathfrak{p}}(\mathrm{disc}(L/K))$ can be very large compared to the degree d of the extension. For example, Let L/K be a finite Galois extension of number fields with Galois group G, $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which is wildly ramified in L/K and $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ over $\mathfrak{p}$. Let $G_{i,\mathfrak{P}}$ be the i-th ramification group of G relative to $\mathfrak{P}$. By the Hilbert's formula, we have

$$v_{\mathfrak{P}}(\mathcal{D}_{L/K}) = \sum_{i=0}^{m_0} (|G_{i,\mathfrak{P}}| - 1)$$

for some natural number m_0. Then by applying this formula for a degree p, a prime number wildly ramified Galois extension L/K, we get any prime $\mathfrak{p}$ of $\mathcal{O}_K$ which is wildly ramified (and hence totally ramified) and for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ over $\mathfrak{p}$, we have

$$v_{\mathfrak{P}}(\mathcal{D}_{L/K}) = (p-1)(1+m_0) \implies v_{\mathfrak{p}}(\mathrm{disc}(L/K)) = (p-1)(1+m_0).$$

If $m_o \geq 2$, then we see that $v_{\mathfrak{p}}(\mathrm{disc}(L/K)) = (p-1)(1+m_0) > p$.

Suppose L/K is a finite extension of number fields such that $\mathcal{O}_K$ is a PID and the degree of L/K is $d \geq 2$. Since $\mathcal{O}_K$ is a PID, there exists an algebraic integer $t \in \mathcal{O}_K$ such that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = t\mathcal{O}_K$. Since $\mathrm{Tr}_{L/K}(1) = d$, the degree of L/K, and if $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = t\mathcal{O}_K$ for some algebraic integer $t \in \mathcal{O}_K$, then t is a divisor of d in $\mathcal{O}_K$.

If L/K is a wildly ramified extension of number fields of degree $d \geq 2$ and $\mathcal{O}_K$ is a PID, it is a natural question to ask under what conditions $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = d\mathcal{O}_K$?. For a finite extension L/K of number fields, we can define *the group index*, $I(L/K)$, which is defined to be the index $[\mathcal{O}_K : \mathrm{Tr}_{L/K}(\mathcal{O}_L)]$. When $\mathcal{O}_K$ is a PID, we see that

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L) = d\mathcal{O}_K \iff [\mathcal{O}_K : \mathrm{Tr}_{L/K}(\mathcal{O}_L)] = [\mathcal{O}_K : d\mathcal{O}_K] = d.$$

In 2006, H. Johnston [4], improving the results of Girstmair, proved the following. *Let L/K be a finite extension of absolutely abelian number fields of equal conductor n. Let $e = v_2(n)$ and $m = n/2^e$, and let $\mathbb{Q}(m)$ be the m-th cyclotomic field. Then*

$$I(L/K) = \begin{cases} 2^{[K\cap\mathbb{Q}(m):\mathbb{Q}]}; & \text{if } L/K \text{ is wildly ramified} \\ 1; & \text{otherwise.} \end{cases}$$

We prove the following result.

Theorem 1.3. *Let L/K be a finite extension of number fields of degree d. If there exists an integral basis $\{1, \alpha_1, \alpha_2, \ldots, \alpha_{d-1}\}$ for L/K such that $\mathrm{Tr}_{L/K}(\alpha_i) = 0$ for all $i = 1, 2, \ldots, d-1$, then $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = d\mathcal{O}_K$. Conversely, suppose the ring of integers $\mathcal{O}_K$ is a PID and $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = d\mathcal{O}_K$. Then there exists an integral basis $\{1, \alpha_1, \alpha_2, \ldots, \alpha_{d-1}\}$ for L/K such that $\mathrm{Tr}_{L/K}(\alpha_i) = 0$ for all $i = 1, 2, \ldots, d-1$.*

We also observe the following regarding the generator of a normal integral basis of a finite Galois extension L/K of number fields.

Theorem 1.4. *Let L/K be a finite Galois extension of number fields. Suppose L/K admits a normal integral basis in it and let $\alpha \in \mathcal{O}_L$ be a generator of the normal integral basis. Then $\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K^\times$ where $\mathcal{O}_K^\times$ denotes the unit group of $\mathcal{O}_K$.*

2. Preliminaries

Let L/K be a finite extension of number fields. The inverse *different ideal* $\mathfrak{D}_{L/K}$ of L/K is the fractional ideal of $\mathcal{O}_L$ defined as follows:

$$\mathfrak{D}_{L/K}^{-1} = \left\{x \in L \mid \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K \text{ for all } y \in \mathcal{O}_L\right\}.$$

We have the following basic lemmas.

Lemma 2.1. *(For a proof, see Chapter III, §3, Proposition 7 in* [6]*) Let* $\mathfrak{a}$ *(respectively,* $\mathfrak{b}$*) be a fractional ideal of* K *(respectively,* L*) relative to* $\mathcal{O}_K$ *(respectively,* $\mathcal{O}_L$*). Then* $\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathfrak{a}$ *if and only if* $\mathfrak{b} \subset \mathfrak{a} \cdot \mathfrak{D}_{L/K}^{-1}$.

Remark 2.1. *By Lemma 2.1, we get* $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{a}$ *for some ideal* $\mathfrak{a}$ *in* $\mathcal{O}_K$ *if and only if* $\mathcal{O}_L \subset \mathfrak{a} \cdot \mathfrak{D}_{L/K}^{-1}$ *if and only if* $\mathfrak{D}_{L/K} \subset \mathfrak{a}\mathcal{O}_L$.

Lemma 2.2. *(For a proof, see Chapter III, §2, Theorem 2.6 in* [7]*) A prime ideal* $\mathfrak{P}$ *of* L *is ramified over* K *if and only if* $\mathfrak{P}|\mathfrak{D}_{L/K}$. *Let* $\mathfrak{P}^s$ *be the highest power of* $\mathfrak{P}$ *dividing* $\mathfrak{D}_{L/K}$, *and let* e *be the ramification index of* $\mathfrak{P}$ *over* K. *Then we have*

$$s \begin{cases} = e-1; & \text{if } \mathfrak{P} \text{ is tamely ramified} \\ \in [e, e-1+v_{\mathfrak{P}}(e)]; & \text{if } \mathfrak{P} \text{ is wildly ramified.} \end{cases}$$

Remark 2.2. *Let* $\mathfrak{p}$ *be prime ideal in* $\mathcal{O}_K$ *and* $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} \mathfrak{Q}_1 \cdots \mathfrak{Q}_t$ *be the prime factorization in* $\mathcal{O}_L$ *with* $s \geq 1$, $t \geq 0$ *and* $e_i \geq 2$ *are integers for all* $i = 1, 2, \ldots, s$. *Then Lemma 2.1 implies that* $\mathfrak{Q}_i$ *does not divide* $\mathfrak{D}_{L/K}$ *for all* $i = 1, 2, \ldots, t$.

If a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is tamely ramified in L (means, if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, then the prime ideal $\mathfrak{P}_i$ of $\mathcal{O}_L$ is tamely ramified for every i), then the following lemma estimates the maximum power of $\mathfrak{p}$ dividing the discriminant, $\mathrm{disc}(L/K)$, of L/K.

Lemma 2.3. *Let* $\mathfrak{p}$ *be a prime ideal of* K *and let the factorization be* $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} \mathfrak{Q}_1 \cdots \mathfrak{Q}_t$ *in* L *where* $s \geq 1$ *and* $t \geq 0$ *are integers and the integers* $e_i \geq 2$ *for all* $i = 1, 2, \ldots, s$. *Suppose* $\mathfrak{p}^n \| \mathrm{disc}(L/K)$ *for some natural number* n. *If* $\mathfrak{p}$ *is tamely ramified in* L, *then*

$$n = \sum_{i=1}^{s} (e_i - 1) f_i = [L:K] - (f_1 + \cdots + f_s + g_1 + \cdots + g_t) \leq [L:K] - (s+t),$$

where f_i*'s (respectively,* g_j*'s) are the residue degree of* $\mathfrak{P}_i$ *(respectively,* $\mathfrak{Q}_j$*) over* $\mathfrak{p}$ *for each* i *(respectively, for each* j*).*

Proof. Given that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} \mathfrak{Q}_1 \cdots \mathfrak{Q}_t$ be the prime ideal factorization of $\mathfrak{p}$ in $\mathcal{O}_L$ where $s \geq 1$ and $t \geq 0$ are integers and the integers $e_i \geq 2$ for all $i = 1, 2, \ldots, s$. Let f_i (respectively, g_j's) be the residue degree of $\mathfrak{P}_i$ (respectively, $\mathfrak{Q}_j$) over $\mathfrak{p}$ for each $i \geq 1$ and j. Then we know that $[L:K] = \sum_{i=1}^{s} e_i f_i + \sum_{j=1}^{t} g_j$.

By hypothesis, we know that $\mathfrak{p}$ is tamely ramified in L. Then by Lemma 2.2, if u_i is the exact power of $\mathfrak{P}_i$ dividing $\mathfrak{D}_{L/K}$, then $u_i = e_i - 1$ for all $i = 1, 2, \ldots, s$ and by Remark 2.2, we see that $\mathfrak{Q}_j$ doesn't divide $\mathfrak{D}_{L/K}$. Therefore,

$$\mathcal{N}_{L/K}(\mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_s^{u_s}) = \mathcal{N}_{L/K}(\mathfrak{P}_1^{e_1-1}) \cdots \mathcal{N}_{L/K}(\mathfrak{P}_s^{e_s-1}) = \mathfrak{p}^{(e_1-1)f_1 + \cdots + (e_s-1)f_s}.$$

If $\mathfrak{p}^n \| \mathrm{disc}(L/K)$ is the exact power of $\mathfrak{p}$ dividing the discriminant of L/K, then since $\mathcal{N}_{L/K}(\mathfrak{D}_{L/K}) = \mathrm{disc}(L/K)$, we see that

$$\mathrm{disc}(L/K) = \mathfrak{p}^n \mathfrak{a} = \mathcal{N}_{L/K}(\mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_s^{u_s} \mathfrak{b}) = \mathcal{N}_{L/K}(\mathfrak{D}_{L/K})$$

where $\mathfrak{a}$ is coprime to $\mathfrak{p}$ and $\mathfrak{b}$ is coprime to $\mathfrak{P}_i$'s. Then by unique factorization of ideals, we conclude that

$$\mathfrak{p}^n = \mathcal{N}_{L/K}(\mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_s^{u_s}) = \mathfrak{p}^{(e_1-1)f_1+\cdots+(e_s-1)f_s}$$

and hence we get the exact power of $\mathfrak{p}$ in $\mathrm{disc}(L/K)$ is

$$\begin{aligned} n &= \sum_{i=1}^{s}(e_i-1)f_i = \sum_{i=1}^{s} e_i f_i + \sum_{j=1}^{t} g_j - (f_1 + \cdots + f_s + g_1 + \cdots + g_t) \\ &= [L:K] - (f_1 + \cdots + f_s + g_1 + \cdots + g_t) \leq [L:K] - (s+t), \end{aligned}$$

as each $f_i \geq 1$ and if $t \neq 0$, then each $g_i \geq 1$. □

When L/K is a finite extension of number fields, since $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is an ideal of $\mathcal{O}_K$, we have the following observation.

Lemma 2.4. *Let L/K be a finite extension of number fields. Then $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ in $\mathcal{O}_K$ for some integers $a_i \geq 1$ if and only if for each $i = 1, 2, \ldots, r$, we have $a_i = \min_{\mathfrak{P}_{ij}|\mathfrak{p}_i} \left\lceil \frac{v_{\mathfrak{P}_{ij}}(\mathcal{D}_{L/K})}{v_{\mathfrak{P}_{ij}}(\mathfrak{p}_i)} \right\rceil$ where the prime ideal $\mathfrak{P}_{ij}$ in $\mathcal{O}_L$ dividing $\mathfrak{p}_i$ for every j.*

Proof. Let $i \in \{1, 2, \ldots, r\}$ be a fixed integer and consider prime ideal $\mathfrak{p}_i$ in $\mathcal{O}_K$. Then by Remark 2.1, we see that

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{p}_i^{n_i} \iff v_{\mathfrak{P}_{ij}}(\mathcal{D}_{L/K}) \geq v_{\mathfrak{P}_{ij}}(\mathfrak{p}_i) n_i \iff n_i \leq v_{\mathfrak{P}_{ij}}(\mathcal{D}_{L/K})/v_{\mathfrak{P}_{ij}}(\mathfrak{p}_i)$$

for every prime ideal $\mathfrak{P}_{ij}$ dividing $\mathfrak{p}_i$. Since the exact power of $\mathfrak{p}_i$ dividing $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is equal to a_i, the result follows. □

When $K = \mathbb{Q}$, Lemma 2.4 was proved by Maurer [5]. In the next lemma, we deal with trace zero elements of $\mathcal{O}_L$ which is useful in proving Theorem 1.3.

Lemma 2.5. *Let L/K be a finite extension of number fields and $\mathcal{O}_L$ and $\mathcal{O}_K$ be the ring of integers of L and K respectively. Then the following exact sequences of projective $\mathcal{O}_K$-modules*

$$0 \to \mathcal{O}_L^0 \to \mathcal{O}_L \to \mathrm{Tr}_{L/K}(\mathcal{O}_L) \to 0$$

splits, where $\mathcal{O}_L^0$ is the kernal of the trace map on $\mathcal{O}_L$.

Proof. Since the trace map on $\mathcal{O}_L$ is an additive homomorphism and $\mathcal{O}_K$-linear map, we see that $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is an ideal in $\mathcal{O}_K$ and it is generated by at most 2 elements of $\mathcal{O}_K$. Since $\mathcal{O}_L^0$ is the kernal of the trace map, $\mathcal{O}_L^0$ is an ideal in $\mathcal{O}_L$. Thus, $\mathcal{O}_L, \mathcal{O}_L^0$ and $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ are all finitely generated torsion-free $\mathcal{O}_K$-modules and hence they are all projective $\mathcal{O}_K$-modules. Therefore, we get the above exact sequence splits. □

Corollary 2.1. *Let L/K be a finite extension of number fields of degree d and $\mathcal{O}_L$ and $\mathcal{O}_K$ be the ring of integers of L and K respectively. Then we have*

$$\mathcal{O}_L \cong \mathcal{O}_L^0 \oplus \mathrm{Tr}_{L/K}(\mathcal{O}_L)$$

with rank of $\mathcal{O}_L^0$ as a $\mathcal{O}_K$-module is at least $d-2$.

Proof. By Lemma 2.5, we get the first assertion. Since $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is an ideal in the Dedekind domain, it is generated by at most 2 elements of $\mathcal{O}_K$ and hence the assertion. □

Remark 2.3. *Consider the case when $\mathcal{O}_K$ is a PID. In this case, there exists $t \in \mathcal{O}_K$ such that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = t\mathcal{O}_K$. By the module isomorphism, we see that*

$$\mathcal{O}_L/\mathcal{O}_L^0 \cong \mathrm{Tr}_{L/K}(\mathcal{O}_L) = t\mathcal{O}_K.$$

Therefore, as a free $\mathcal{O}_K$-submodule of $\mathcal{O}_L$, the free rank of $\mathcal{O}_L^0$ is $d-1$. Thus, $\mathcal{O}_L \cong \mathcal{O}_L^0 \oplus \gamma\mathcal{O}_K$ as a $\mathcal{O}_K$-module for some $\gamma \in \mathcal{O}_L$ such that $\mathrm{Tr}_{L/K}(\gamma) = t$. Indeed, if we write $\mathcal{O}_L^0 = \alpha_1\mathcal{O}_K \oplus \cdots \oplus \alpha_{d-1}\mathcal{O}_K$ as $\mathcal{O}_K$-module, then we can get an integral basis $\{\alpha_1, \ldots, \alpha_{d-1}, \gamma\}$ of $\mathcal{O}_L$ with $\mathrm{Tr}_{L/K}(\alpha_i) = 0$ for each i and $\mathrm{Tr}_{L/K}(\gamma) = t$.

We need the following theorem of S. Ullom [8].

Theorem 2.1. *Let L/K be a finite Galois extension of number fields. If L/K admits a normal integral basis, then L/K is tamely ramified.*

The following two observations suggest how the trace map behaves in the intermediate fields and of independent interest.

Lemma 2.6. *Let L/K be any finite extension of number fields such that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$. Then $\mathrm{Tr}_{F/K}(\mathcal{O}_F) = \mathcal{O}_K$ for every intermediate field $K \subset F \subset L$.*

Proof. Since $\mathcal{O}_K = \mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\mathcal{O}_L)) \subset \mathrm{Tr}_{F/K}(\mathcal{O}_F)$, we et $\mathrm{Tr}_{F/K}(\mathcal{O}_F) = \mathcal{O}_K$. □

Proposition 2.1. *Let L/K be any finite extension of number fields and $F_{ii\in I}$ be any family of subfields of L containing K with $\mathrm{Tr}_{F_i/K}(\mathcal{O}_{F_i}) = \mathfrak{a}_i$, an ideal in $\mathcal{O}_K$ for each $i \in I$. Then*

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \bigcap_{i\in I} \mathfrak{a}_i.$$

Proof. Since $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathrm{Tr}_{F_i/K}(\mathrm{Tr}_{L/F_i}(\mathcal{O}_L)) \subset \mathrm{Tr}_{F_i/K}(\mathcal{O}_{F_i}) \subset \mathfrak{a}_i$ for each $i \in I$, we get the assertion. □

3. Proof of Theorem 1.1, 1.2, Corollary 1.1, 1.2 and 1.3

Proof of Theorem 1.1. Suppose $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is a proper ideal $\mathcal{O}_K$. Then there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{p}$. Since $d\mathcal{O}_K \subset \mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{p}$, we see that $\mathfrak{p}$ divides $d\mathcal{O}_K$. Now by Remark 2.1, we get $\mathfrak{D}_{L/K} \subset \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}\mathfrak{Q}_1 \cdots \mathfrak{Q}_t$. Then by Lemma 2.2 and Remark 2.2, we conclude that $t = 0$ and each $\mathfrak{P}_i$ is wildly ramified for $i = 1, 2, \ldots, s$.

Suppose (2) is not true. Then by Lemma 2.2, for each $i = 1, 2, \ldots, s$, we get $\mathfrak{P}_i^{e_i} | \mathfrak{D}_{L/K}$. Since $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are coprime for each $i \neq j$, we get $\mathfrak{D}_{L/K} \subset \mathfrak{p}\mathcal{O}_L$. Again by Remark 2.1, we conclude that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{p}$, which proves the theorem. □

Proof of Theorem 1.2. We prove (1) $\iff$ (2). The first implication follows from Theorem 1.1. For the converse implication, if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}$ is a prime ideal factorization and there exists a prime $\mathfrak{P}_i$ (for some i) of $\mathcal{O}_L$ such that $\mathfrak{P}_i$ is tamely ramified, then, by Lemma 2.3, the highest power of $\mathfrak{p}$ dividing $\mathrm{disc}(L/K)$ would be $d - f_i$, which contradicts our assumption. Thus each $\mathfrak{P}_i$ is wildly ramified for each i and hence $\mathfrak{D}_{L/K}$ is divisible by $\mathfrak{P}_i^{e_i}$ for each i. This implies $\mathfrak{D}_{L/K} \subset \mathfrak{p}\mathcal{O}_L$, and by Lemma 2.1, we get $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{p}$. Thus, $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is a proper ideal in $\mathcal{O}_K$.

(2) $\implies$ (3) follows from Lemma 2.3. □

Proof of Corollary 1.1. It is enough to prove (3) $\implies$ (1). Suppose L/K is wildly ramified. Then there exists a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ such that if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s}$ is the ideal factorization, then there exists at least one i for which $\mathfrak{P}_i^{e_i}$ divides $\mathfrak{D}_{L/K}$. Since L/K is a Galois extension, we get $e_1 = \cdots = e_s$. Then by Lemma 2.2, we get $\mathfrak{P}_i^{e_i}$ divides $\mathfrak{D}_{L/K}$ for each $i = 1, \ldots, s$. This implies that $\mathfrak{D}_{L/K} \subset \mathfrak{p}\mathcal{O}_L$, and hence by Lemma 2.1, we get, $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathfrak{p}$. □

Proof of Corollary 1.2. This follows from Theorem 1.2. □

Proof of Corollary 1.3. Since $\mathfrak{p}$ is totally ramified in L, we get $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^d$ for some prime ideal $\mathfrak{P}$ in L. Hence $e = d$ and $f = 1$. If $\mathfrak{p}^n \| \mathrm{disc}(L/K)$, then as $\mathfrak{p}$ is tamely ramified, by Lemma 2.2, we get $n = e - 1 = d - 1$, as desired.

Conversely, suppose the highest power of $\mathfrak{p}$ dividing $\mathrm{disc}(L/K)$ is $n = d-1$. Assume that $\mathfrak{p}$ is totally ramified. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^d$ and hence we get $e = d$ and $f = 1$. If $\mathfrak{p}$ is wildly ramified, then by Lemma 2.2, we must have $n \geq d$, a contradiction. Hence $\mathfrak{p}$ must be tamely ramified.

Assume that $\mathfrak{p}$ is tamely ramified. If possible, suppose $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s}$ for some integer $s \geq 2$. Then by Lemma 2.2, we get $n \leq d - s \leq d - 2$, a contradiction to $n = d - 1$. Hence we conclude that $s = 1$ and $\mathfrak{p}$ must be totally ramified. □

4. Proof of Theorem 1.3

Suppose $\{1, \alpha_1, \ldots, \alpha_{d-1}\}$ is an integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$ where $\mathrm{Tr}_{L/K}(\alpha_i) = 0$ for each $i = 1, 2, \ldots, d-1$. We prove that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset d\mathcal{O}_K$. For, if $\beta \in \mathcal{O}_L$, then $\beta = c_1 + c_2\alpha_1 + \cdots + c_d\alpha_{d-1}$ for some $c_i \in \mathcal{O}_K$. Hence $\mathrm{Tr}_{L/K}(\beta) = c_1\mathrm{Tr}_{L/K}(1) = c_1 d \in d\mathcal{O}_K$ and we get $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset d\mathcal{O}_K$. Since $1 \in \mathcal{O}_L$, we see that $d = \mathrm{Tr}_{L/K}(1) \in \mathrm{Tr}_{L/K}(\mathcal{O}_L)$, which proves the assertion.

Conversely, suppose the ring of integers $\mathcal{O}_K$ of K is a PID and $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = d\mathcal{O}_K$. By Corollary 2.1, we let $\{\alpha_1, \ldots, \alpha_{d-1}\}$ be an $\mathcal{O}_K$ basis of $\mathcal{O}_L^0$. Again by Corollary 2.1, there exists $\gamma \in \mathcal{O}_L$ such that $\{\alpha_1, \ldots, \alpha_{d-1}, \gamma\}$ forms an integral basis of L/K, where $\mathrm{Tr}_{L/K}(\gamma) = d$. We claim that $\{1, \alpha_1, \ldots, \alpha_{d-1}\}$ is a $\mathcal{O}_K$-basis of $\mathcal{O}_L$ and hence an integral basis.

To prove that $\{1, \alpha_1, \ldots, \alpha_{d-1}\}$ is an integral basis for $\mathcal{O}_L$, we need to prove that if $c_0 + c_1\alpha_1 + \cdots + c_{d-1}\alpha_{d-1} = 0$ with $c_i \in \mathcal{O}_K$, then $c_0 = c_1 = \cdots = c_{d-1} = 0$ and $\gamma = a_0 + a_1\alpha_1 + \cdots + a_{d-1}\alpha_{d-1}$ for some $a_i \in \mathcal{O}_K$.

Suppose $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_{d-1}\alpha_{d-1} + x_d = 0$ for some $x_i \in \mathcal{O}_K$. Then applying trace on both sides, we get $\mathrm{Tr}_{L/K}(x_d) = 0$, and hence we get $dx_d = 0$. Since $\mathcal{O}_K$ is an integral domain, we get $x_d = 0$. Thus the equation now becomes $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_{d-1}\alpha_{d-1} = 0$. Since $\alpha_i \in \mathcal{O}_L^0$'s forms an $\mathcal{O}_K$-basis, we get $x_i = 0$ for all i.

It remains to show that $\gamma \in \mathcal{O}_L$ (as above) can be expressed as an $\mathcal{O}_K$ linear combination of $1, \alpha_1, \ldots, \alpha_{d-1}$. To see this, since $\mathrm{Tr}_{L/K}(\gamma) = \mathrm{Tr}_{L/K}(1) = d$, we get $\mathrm{Tr}_{L/K}(\gamma - 1) = 0$ and

hence $(\gamma - 1) \in \mathcal{O}_L^0$. Therefore, $\gamma - 1 = c_1\alpha_1 + \cdots + c_{d-1}\alpha_{d-1}$ for some $c_i \in \mathcal{O}_K$ which inturn implies that $\gamma = 1 + c_1\alpha_1 + \cdots + c_{d-1}\alpha_{d-1}$, as desired. □

5. Proof of Theorem 1.4

Let L/K be a given Galois extension of number fields of degree d with Galois group $G = \{\sigma_1, \ldots, \sigma_d\}$. Since L/K admits a normal integral basis, there exists $\alpha \in \mathcal{O}_L$ such that $\{\sigma(\alpha) \ : \ \sigma \in G\}$ forms an integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$. Therefore, by Theorem 2.1, L/K is tamely ramified and hence $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.

Since $1 \in \mathcal{O}_K$, there exists $\beta \in \mathcal{O}_L$ such that $\mathrm{Tr}_{L/K}(\beta) = 1$. Also, we can write $\beta = c_1\sigma_1(\alpha) + \cdots + c_d\sigma_d(\alpha)$ for some $c_i \in \mathcal{O}_K$. Then

$$1 = \mathrm{Tr}_{L/K}(\beta) = \mathrm{Tr}_{L/K}\left(\sum_{i=1}^{d} c_i\sigma_i(\alpha)\right) = \sum_{i=1}^{d} c_i\mathrm{Tr}_{L/K}(\sigma_i(\alpha)) = (c_1 + \cdots + c_d)\mathrm{Tr}_{L/K}(\alpha).$$

This implies that $c_1 + \cdots + c_d \in \mathcal{O}_K\backslash\{0\}$ and $\mathrm{Tr}_{L/K}(\alpha)$ are units in $\mathcal{O}_K$ and hence the theorem. □

References

[1] E. Aljadeff, *On the surjectivity of some trace maps*, Israel J. Math., **86** (1994), 221-232.

[2] F. Battistoni and T. Zaimi, *On the trace of the integers of a number field*, arXiv:2110.06614v1 [math.NT] 13 Oct 2021.

[3] A. Frohlich, *Galois module structure of algebraic integers*, Springer-Verlag, New York, Tokyo, 1983.

[4] H. Johnston, *On the trace map between absolutely abelian number fields of equal conductor*, Acta Arith., **122** (1) (2006), 63-74.

[5] D. Maurer, *The trace form of an algebraic number field,* J. Number Theory, **5** (1973), 379-384.

[6] J. P. Serre, *Local fields*, GTM, **67**, Springer-Verlag, New York-Berlin, 1979. (Translated from the French Marvin Jay Greenberg).

[7] J. Neukirch, *Algebraic Number Theory*, GTM, **322**, Springer-Verlag, 1977.

[8] S. Ullom, *Normal bases in Galois extensions of number fields*, Nagoya Math. J., **34** (1969), 153-167.

(Sudipa Das and R. Thangadurai) Harish-Chandra Research Institute, A CI of Homi Bhabha National Institute, Chhatnag Road, Jhunsi, Prayagraj 211019, India.

Email address, Sudipa Das: sudipadas@hri.res.in

Email address, R. Thangadurai: thanga@hri.res.in