Rendiconti Sem. Mat. Univ. Pol. Torino
Vol. 78, 1 (2020), 13 – 19

F. Battistoni

DISCRIMINANTS OF NUMBER FIELDS AND SURJECTIVITY OF TRACE HOMOMORPHISM ON RINGS OF INTEGERS

Abstract. In this note we give a brief survey of the most elementary criteria used to determine the surjectivity of the trace operator on the ring of integers of a number field K. Furthermore, we introduce an easy to state yet unknown surjectivity criterion depending only on the prime factorization of the degree n of K and on the squarefree part of the discriminant d_K.

1. Preliminaries and trace homomorphism

Let K be a number field of degree $n \in \mathbb{N}$ over the field $\mathbb{Q}$ of rational numbers. It is known that, for $n > 1$, there is not a canonical way to embed K in the field $\mathbb{C}$ of complex numbers; nonetheless, the field K admits exactly n embeddings $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$.
By the Primitive Element Theorem (Theorem 5.1 of [6]) we know that any number field K has the form $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in K$, and if $p(x) \in \mathbb{Z}[x]$ is the minimum polynomial of α, then there is a bijection between the embeddings $\sigma_1, \dots, \sigma_n$ of K and the complex roots of $p(x)$.

Given $\beta \in K$, define its **trace** as the number $\mathrm{Tr}(\beta) := \sum_{i=1}^{n} \sigma_i(\beta)$. By its very definition, the trace is an algebraic number which is invariant for the action of the n embeddings of K, and thus it is a rational number. This allows to define the trace function

$$\mathrm{Tr} : K \to \mathbb{Q}$$

which is immediately seen to be an homomorphism of $\mathbb{Q}$-vector spaces.

If $K = \mathbb{Q}(\alpha)$ and $p(x) := x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Q}[x]$ is the minimum polynomial of α, then $\mathrm{Tr}(\alpha) = -a_1$; this follows immediately from the fact that $p(x)$ splits as $\prod_{i=1}^{n}(x - \sigma_i(\alpha))$ in any algebraic closure of K (Corollary 3.12 of [3]).

Let O_K be the ring of integers of K, i.e. the subring of the algebraic integers contained in K. If $\alpha \in O_K$, then not only $\mathrm{Tr}(\alpha)$ is a rational number but it is also an algebraic integer, and so $\mathrm{Tr}(\alpha) \in \mathbb{Z}$. The restricted map

$$\mathrm{Tr} : O_K \to \mathbb{Z}$$

is an homomorphism of abelian groups.

The ring of integers O_K satisfies the following two important properties:

- Any non-zero ideal $I \subset O_K$ can be written in a unique way as a finite product of prime ideals of O_K (Theorem 3.14, Chapter I of [2]);

– If K has degree n, then $(O_K,+)$ is a free abelian group of rank n (Theorem 1, Chapter I of [4]).

2. Surjectivity of trace operator

Given a number field K of degree n, it is very easy to see that the trace map is a surjective homomorphism: in fact, $\mathrm{Tr}(1) = n$ and so, given $a/b \in \mathbb{Q}$, the element $a/(nb)$ is such that $\mathrm{Tr}(a/(nb)) = a/(nb) \cdot \mathrm{Tr}(1) = a/b$.
Actually, this proves that considering the subfield $\mathbb{Q} \subset K$ is enough to yield a surjection.

Does this surjectivity hold also for the restricted map $\mathrm{Tr} : O_K \to \mathbb{Z}$? Surely the trick of dividing by the degree n of the number field no longer works, because given $\alpha \in O_K$ the element α/n may not be in O_K.
In fact, it is very easy to provide an example of number field for which the trace restricted to the ring of integers is not surjective: consider the field $K = \mathbb{Q}(\sqrt{2})$, which has minimum polynomial $p(x) := x^2 - 2$. The ring of integers O_K is then equal to $\mathbb{Z}[\sqrt{2}]$ (Propostions 1.32 and 1.33, Chapter II of [1]), i.e. any algebraic integer in K has the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. Being $\mathrm{Tr}(m) = 2m$ for any $m \in \mathbb{Z}$ and $\mathrm{Tr}(\sqrt{2}) = 0$ because of $p(x)$, then the trace of any element of O_K is an even rational integer, and so the restricted trace map is not surjective.
The above considerations imply that the restricted trace is not surjective for any quadratic number field $\mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree and $d \equiv 2,3 \bmod 4$ (this last assumption is needed to ensure that the ring of integers is equal to $\mathbb{Z}[\sqrt{d}]$).

One could wonder if there exist any criteria, different from explicitly studying the trace map, to determine whether the restricted trace homomorphism is surjective.
A first try comes from looking at the minimum polynomial of the number field.

PROPOSITION 1. *Let K be a number field with minimum polynomial $p(x) := x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$. If $a_1 = \pm 1$, then the trace map $\mathrm{Tr} : O_K \to \mathbb{Z}$ is surjective.*

Proof. $p(x)$ being a monic irreducible polynomial with integer coefficients, there exists $\alpha \in O_K$ root of $p(x)$ such that $\mathrm{Tr}(\alpha) = -a_1 = \mp 1$. Then, for every $m \in \mathbb{Z}$ it is $m = \mathrm{Tr}(m\alpha)$ or $m = \mathrm{Tr}(-m\alpha)$ depending on the sign of $\mathrm{Tr}(\alpha)$. □

What can be said for number fields K which are defined by polynomials with coefficient $a_1 \neq \pm 1$ and such that it seems not possible to produce elements $\alpha \in O_K$ with $\mathrm{Tr}(\alpha) = \pm 1$ by hands only? One can get further information thanks to the concept of ramification, which is naturally related to the trace homomorphism: this is the subject of the next section.

3. Discriminants and ramification

Let K be a number field and let O_K be its ring of integers. Given a prime number $p \in \mathbb{Z}$, the ideal pO_K is not necessarily prime but has a factorization

$$pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

where the $\mathfrak{p}_i$'s are prime ideals in O_K and $e_i \in \mathbb{N}$ for every $i = 1, \ldots, r$. The prime number p is said to be **ramified in** K if $e_i > 1$ for some index i.

It is a classical problem in Number Theory to detect the prime numbers ramifying in a number field K: its solution depends mainly on the folllowing concepts.
Let $\alpha_1 \ldots, \alpha_n \in O_K$ be independent $\mathbb{Z}$-generators of O_K as abelian group. The **discriminant of** K is defined as

$$d_K := (\det(\sigma_i(\alpha_j))_{i,j=1}^n)^2 = \det(\mathrm{Tr}(\alpha_i\alpha_j))_{i,j=1}^n.$$

One gets $d_K \in \mathbb{Z}$ because of the last equality, and it is obvious from the definition that the value of d_K does not change by considering a new system $\beta_1, \ldots, \beta_n$ of $\mathbb{Z}$-independent generators for O_K.
The importance of the discriminant for the study of the ramified primes relies in the following proposition:

PROPOSITION 2. *A prime number p ramifies in K if and only if p divides d_K.*

Proof. See Corollary III.2.12 of [8]. □

The prime numbers may ramify with different behaviours: the following distinction will be useful to provide criteria for the study of the restricted trace homomorphism.
Let p be a rational prime number ramifying in K and let $pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be its prime ideal factorization in O_K. Then p is said to be **wildly ramified** if there exists $i \in \{1, \ldots, r\}$ such that p divides e_i; otherwise p is said to be **tamely ramified**.
A number field K is said to be **tame** if every ramified prime number is tamely ramified, otherwise K is said to be **wild**.

The last tool needed is the concept of different ideal.
Consider the set $\hat{O}_K := \{\alpha \in K\colon \mathrm{Tr}(\alpha \cdot O_K) \subset \mathbb{Z}\}$. The set $\mathcal{D}_K := \{\beta \in K\colon \beta \cdot \hat{O}_K \subset O_K\}$ is called the **different ideal of** K (or simply the different of K); it is an abelian group with respect to the sum.

LEMMA 1. *The different $\mathcal{D}_K$ satifies the following properties:*

- *$\mathcal{D}_K$ is an ideal of O_K;*
- *If p wildly ramifies in K, $pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and there exists $i \in \{1, \ldots, r\}$ such that p divides e_i, then $\mathfrak{p}_i$ is a factor of $\mathcal{D}_K$ with exponent at least e_i;*

- *If p tamely ramifies in K and $pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, then for any $i \in \{1, \dots, r\}$ the number $e_i - 1$ is the exact exponent of the prime $\mathfrak{p}_i$ as factor of $\mathcal{D}_K$;*

- *The size of the quotient ring $O_K/\mathcal{D}_K$ is equal to $|d_K|$.*

Proof. These results are all proved in Section 4.2 of [7]. □

The distinction between tame and wild number fields and the concept of different ideal have proved to be important in determining the surjectivity of the trace homomorphism restricted to the ring of integers.

THEOREM 1. *Let K be a tame number field. Then* $\mathrm{Tr} : O_K \to \mathbb{Z}$ *is surjective.*

Proof. See Corollary 5, Section 4.2 of [7]. The different ideal has a main role in the setting of the proof. □

One can get an interesting Corollary, from which the surjectivity of the restricted trace can be recovered by looking only at the factorization of the discriminant.

COROLLARY 1. *Let K be a number field with squarefree discriminant d_K. Then* $\mathrm{Tr} : O_K \to \mathbb{Z}$ *is surjective.*

Proof. If $d_K = \pm p_1 \cdots p_r$ is squarefree, then $\mathcal{D}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where the size of every quotient ring $O_K/\mathfrak{p}_i$ is equal to p_i. This implies that, for any fixed factor p_i of the discriminant, $\mathfrak{p}_i$ is the unique factor of $p_i O_K$ which has exponent greater than 1, and the value of this exponent is precisely equal to 2. Thus, any odd p_i is tamely ramified.
If 2 divides d_K and $\mathfrak{Q}$ is the factor of $2O_K$ dividing $\mathcal{D}_K$, then either 2 wildly ramifies with the exponent of $\mathfrak{Q}$ being 1, or 2 tamely ramifies with the exponent of $\mathfrak{Q}$ being 2, and both these options are absurd.
Thus K is a tame number field, and from Theorem 1 the surjectivity on the trace over the ring of integers follows. □

4. A weaker discriminant criterion

Theorem 1 of the previous section proves the surjectivity of the restricted trace for a wide class of number fields, and it also yields a good sufficient criterion depending only on the factorization of the discriminant d_K.
The goal of this section is to present a simple, yet new, criterion for the surjectivity which not only relies on the factorization of d_K, but has the advantage to give a positive answer also for some wild number fields.

THEOREM 2. *Let K be a number field of degree n and assume that, for every prime number p dividing n, the number p^2 does not divide d_K. Then* $\mathrm{Tr} : O_K \to \mathbb{Z}$ *is surjective.*

Proof. Let $T_0(K) := \{\alpha \in O_K \colon \mathrm{Tr}(O_K) = 0\}$ be the kernel of the restricted trace homomorphism. The structure theorem of free abelian groups (Theorem 7.3, Chapter I of [5]) implies that $T_0(K)$ is a free abelian group too, its rank being equal to $n-1$.
The set $\mathrm{Tr}(O_K)$ is an ideal in $\mathbb{Z}$. Let t be the positive generator of this ideal. Since $n = \mathrm{Tr}(1)$ one gets that t divides n.

The previous considerations imply that the ring of integers admits a decomposition $O_K = T_0(K) \oplus \mathbb{Z}\gamma$ as free abelian group, where $\gamma \in O_K$ is such that $\mathrm{Tr}(\gamma) = t$. Let $\alpha_1, \ldots, \alpha_{n-1}$ be a $\mathbb{Z}$-basis for $T_0(K)$: then $\alpha_1, \ldots, \alpha_{n-1}, \gamma$ is a $\mathbb{Z}$-basis for O_K and so the discriminant d_K can be computed by means of this basis.
Let M_K denote the matrix

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \cdots & \cdots & \cdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_n(\alpha_{n-1}) \\ \sigma_1(\gamma) & \cdots & \sigma_n(\gamma) \end{pmatrix}.$$

Since its determinant does not change by replacing the last column with the sum of every other column, we get that

$$\det M_K = \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{n-1}(\alpha_1) & \mathrm{Tr}(\alpha_1) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_{n-1}(\alpha_{n-1}) & \mathrm{Tr}(\alpha_{n-1}) \\ \sigma_1(\gamma) & \cdots & \sigma_{n-1}(\gamma) & \mathrm{Tr}(\gamma) \end{pmatrix}$$

$$= \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{n-1}(\alpha_1) & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_{n-1}(\alpha_{n-1}) & 0 \\ \sigma_1(\gamma) & \cdots & \sigma_{n-1}(\gamma) & t \end{pmatrix}.$$

Consider now the minor given by the first $n-1$ rows and the first $n-1$ columns:

$$N_K := \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{n-1}(\alpha_1) \\ \cdots & \cdots & \cdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_{n-1}(\alpha_{n-1}) \end{pmatrix}.$$

Applying any σ_i which is not the identity embedding on K, one sees that a column of N_K is now formed by elements $\sigma_n(\alpha_j)$ with $j = 1, \ldots, n-1$, while the other columns are permutations of the remaining columns. But for every $j \in \{1, \ldots, n-1\}$ it is $\sigma_n(\alpha_j) = -\sum_{i=1}^{n-1} \sigma_i(\alpha_j)$: this implies that $\det N_K$ is invariant for the action of the embeddings σ_i, up to a possible change of sign due to the permutation of the columns.
Thus it is enough to take the square of $\det N_K$ to get an algebraic integer invariant for any embeddings σ_i, i.e. a rational integer, and so $d_K = (\det M_K)^2 = (\det N_K)^2 \cdot t^2 = C \cdot t^2$, with $C \in \mathbb{Z}$. In other words, it is $d_K/t^2 \in \mathbb{Z}$.
Finally, from the above considerations and the fact that t divides n, the hypothesis of the Theorem force $t = 1$, and so the trace $\mathrm{Tr} : O_K \to \mathbb{Z}$ must be surjective. □

An example of wild number field for which the surjectivity of the restricted trace is not evident without Theorem 2 is given by the cubic field K defined by the polynomial x^3+x-6. In fact, its discriminant is equal to $-2^2 \cdot 61$, so the primes 61 and 2 both ramify. A computation with the computer algebra package PARI/GP [9] shows that the prime 2 wildly ramifies, thus the extension is not tame and Theorem 1 or Corollary 1 do not apply. However, $\mathrm{Tr} : O_K \to \mathbb{Z}$ is surjective, by Theorem 2.

Some final considerations arise looking back at the quadratic fields studied in Section 2: in fact, these are wild fields for which the trace on the ring of integers is not surjective. Moreover, their discriminant is always divided by $4 = 2^2$, and thus they do not satisfy the hypotheses needed for the sufficient criterion introduced by Theorem 2. This suggests a possible conjecture for the complete characterization of the surjectivity of the trace map on the ring of integers:
Given a number field K, then $\mathrm{Tr} : O_K \to \mathbb{Z}$ *is not surjective if and only if K is wild and does not satisfy the hypotheses of Theorem 2.*

References

[1] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[2] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[3] F. Jarvis. *Algebraic number theory*. Springer Undergraduate Mathematics Series. Springer, Cham, 2014.

[4] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[5] S. Lang. *Algebra, Revised Third Edition*. Springer, 2002.

[6] J. S. Milne. Fields and Galois Theory (v4.60), 2018. Available at www.jmilne.org/math/.

[7] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Science & Business Media, 2013.

[8] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[9] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.11.0`, 2018. Available at http://pari.math.u-bordeaux.fr/.

AMS Subject Classification: 11R04, 11R29

Francesco BATTISTONI,
Dipartimento di Matematica, Università degli Studi di Milano
Via Saldini 50, 20133 Milano, Italy
e-mail: `francesco.battistoni@unimi.it`

Lavoro pervenuto in redazione il 26.04.2019.