



UNIVERSIDAD NACIONAL DE COLOMBIA

# Characterization of number fields by their integral trace form

Carlos Andrés Rivera Guaca

Universidad Nacional de Colombia  
Facultad de Ciencias, Departamento de Matemáticas  
Bogotá D.C., Colombia  
2018

# Characterization of number fields by their integral trace form

**Carlos Andrés Rivera Guaca**

Thesis submitted as a partial requirement to qualify for the title of:  
**Master of Science in Mathematics**

Director:  
Guillermo Mantilla Soler  
Co-director:  
John Jaime Rodríguez Vega

Research field:  
Algebraic Number Theory

Universidad Nacional de Colombia  
Facultad de Ciencias, Departamento de Matemáticas  
Bogotá D.C., Colombia  
2018

It is always noteworthy that all those who seriously study this science [the theory of numbers] conceive a sort of passion for it.

- Carl Friedrich Gauss

# Abstract

We prove that the integral trace form (the quadratic form obtained by restricting  $x \mapsto \text{Tr}_{K/\mathbb{Q}}(x^2)$  to the ring of integer of a number field  $K$ ) is a complete invariant for totally real number fields of fundamental discriminant, we also study the relations of this invariant with the trace-zero form and the shape of  $K$  (a geometric invariant introduced in [Ter97] and studied in more generality in [BH16]), and give analog results for those invariants. As a consequence, we settle a conjecture from 2012 made in [MS12] about tamely ramified quartic fields of fundamental discriminant. Our method of proof is based on what we call *Casimir elements* and *Casimir pairings*, new tools we introduce in this work, which are related to (and generalize) the Casimir elements from the representation theory of Lie algebras. Additionally, we give an alternative proof of this conjecture via Bhargava's parametrization of quartic rings.

**Keywords:** Trace form, Totally real number fields, Shapes of number fields, Casimir invariant, Higher composition laws.

## Resumen

Probamos que la forma traza entera (la forma cuadrática obtenida a partir de restringir  $x \mapsto \text{Tr}_{K/\mathbb{Q}}(x^2)$  al anillo de enteros de un cuerpo de números  $K$ ) es un invariante completo para cuerpos de números totalmente reales de discriminante fundamental, también estudiamos la relación de este invariante con la forma traza-cero y la forma geométrica de  $K$  (un invariante introducido en [Ter97] y estudiado en más generalidad en [BH16]), y damos resultados análogos para estos invariantes. Como consecuencia, probamos una conjetura del 2012 propuesta en [MS12] sobre cuerpos cuárticos moderadamente ramificados de discriminante fundamental. Nuestro método de prueba se basa en lo que llamamos *elementos de Casimir* y *emparejamientos de Casimir*, herramientas nuevas introducidas en este trabajo, las cuales están relacionadas con (y generalizan) los elementos de Casimir de la teoría de representación de álgebras de Lie. Adicionalmente, damos una prueba alternativa de esta conjetura via la parametrización de anillos cuárticos de Bhargava.

# Table of contents

<b>Abstract</b>	<b>iv</b>
<b>List of symbols</b>	<b>viii</b>
<b>Introduction</b>	<b>1</b>
<b>1 Preliminaries</b>	<b>9</b>
1.1 Quadratic modules . . . . .	9
1.2 Some basic algebraic number theory . . . . .	12
1.2.1 Number fields and rings of integers . . . . .	12
1.2.2 Hilbert ramification theory . . . . .	14
1.2.3 Absolute values and completions . . . . .	17
1.2.4 Different and discriminant . . . . .	20
1.3 Some results from permutation group theory . . . . .	23
<b>2 The quadratic <math>\mathbb{Z}</math>-modules associated to a number field</b>	<b>25</b>
2.1 Definition and some properties . . . . .	25
2.1.1 Definitions . . . . .	25
2.1.2 Discriminants . . . . .	29
2.1.3 Localization . . . . .	29
2.1.4 Signature . . . . .	32
2.2 Interplay of the quadratic modules . . . . .	33
<b>3 Galois theory of fields with fundamental discriminant</b>	<b>43</b>
3.1 Working with one field $K$ . . . . .	43
3.1.1 Ramification . . . . .	43
3.1.2 The Galois group . . . . .	44
3.1.3 Discriminants of intermediate fields . . . . .	46
3.2 Working with a compositum $KL$ . . . . .	48
3.2.1 Linear disjointness . . . . .	48
3.2.2 The Galois group . . . . .	50
3.2.3 Discriminants of intermediate fields . . . . .	53
3.2.4 Lattice of subfield of $KL/\mathbb{Q}$ . . . . .	56

---

<b>4</b>	<b>Casimir pairings and proofs of the mains theorems</b>	<b>58</b>
4.1	Definition and examples . . . . .	58
4.2	Integrality at finite primes . . . . .	62
4.3	Proofs of the theorems . . . . .	68
<b>5</b>	<b>An alternative proof via Bhargava's parametrization of quartic rings</b>	<b>73</b>
5.1	Parametrization of quartic rings . . . . .	73
5.2	Parametrization of order two ideals in cubic rings . . . . .	75
5.3	Proof of the Conjecture . . . . .	76
	<b>Bibliography</b>	<b>79</b>

# List of symbols

Notation	Definition
$\mathbb{Z}_p, \mathbb{Q}_p$	$p$ -adic integers and $p$ -adic rationals
$\mathbb{1}_X$	Identity map on the set $X$ .
$e(\mathfrak{P} \mathfrak{p}), f(\mathfrak{P} \mathfrak{p})$	Ramification index and inertia degree.
$I_{\mathfrak{P}}, D_{\mathfrak{P}}$	Inertia and decomposition groups.
$\text{Tr}_{B/A}, \text{Nm}_{B/A}$	Trace and norm maps $B \rightarrow A$ .
$\text{tr}_{B/A}$	Trace bilinear form $B \times B \rightarrow A$ .
$(M, \text{tr}_{B/A})$	Quadratic module obtained by restricting $\text{tr}_{B/A}$ to $M$ .
$\mathcal{O}_K$	Ring of integers.
$\mathcal{O}_K^0$	Elements in $\mathcal{O}_K$ with trace 0.
$\mathcal{O}_K^\perp$	Elements in $\mathbb{Z} + [K : \mathbb{Q}] \cdot \mathcal{O}_K$ with trace 0.
$\alpha_\perp$	$[K : \mathbb{Q}] \cdot \alpha - \text{Tr}_{K/\mathbb{Q}}(\alpha)$ .
$\text{Sh}(K)$	Shape of a number field.
$\text{disc}(M, B)$	Discriminant of a quadratic module $(M, B)$
$\text{disc}(K), d_K$	Absolute discriminant.
$\mathfrak{d}_K$	Discriminant ideal.
$\mathfrak{d}_{L/K}$	Relative discriminant ideal of $L/K$
$\mathcal{D}_{L/K}$	Different ideal of $L/K$
$K_v, K_{\mathfrak{p}}$	Completion of $K$ at a place $v$ or $\mathfrak{p}$ .
$\tilde{K}$	Galois closure of a number field $K$
$G$ -field	A number field $K$ such that $\text{Gal}(\tilde{K}/\mathbb{Q}) \cong G$ .
$R_3(K)$	Cubic resolvent field of a quartic $S_4$ -field $K$ .
$c_B(\phi, \psi)$	$B$ -Casimir element of $\psi$ and $\phi$
$\langle \cdot, \cdot \rangle_B$	Casimir pairing associated to $B$

# Introduction

The main goal of this thesis is to show how under certain ramification conditions we can completely determine a number field (up to isomorphism) by some associated invariant quadratic form, namely its integral trace form. We begin by giving some motivation and explaining the relevance of the problem, we also state the new results obtained in this work and outline the general structure of the thesis.

## Overview

The discriminant, an integer coming from Minkowski's geometry of numbers, is one of the most natural and important arithmetic invariants we can attach to a number field  $K$ . It tells us, among other things; which primes ramify in  $K$ , the parity of the number  $s_K$  of pairs of complex embeddings of  $K$  and the parity of the Galois group of the Galois closure of  $K$ <sup>1</sup>. Even more astonishingly, by a theorem due to Hermite and Minkowski, we know that (up to isomorphism) only finitely many number fields can share the same discriminant.

This result allows us to study number fields by enumerating (listing) them by the size of their discriminant. Actually, when people want to know “how many” number fields satisfy certain property  $P$ , and there could be infinitely many that do, what they usually do is study the asymptotic behavior of

$$N_P(X) := \#\{K : K \text{ satisfy } P \text{ and } |\text{disc}(K)| < X\} < \infty$$

as  $X \rightarrow \infty$ <sup>2</sup>. Thus we can say that the discriminant is a fairly useful and strong invariant. For instance, it characterizes completely a quadratic field among all other quadratic fields. However, although only finitely many, there can be multiple number fields with the same discriminant, e.g., the fields  $\mathbb{Q}(\sqrt[3]{6})$  and  $\mathbb{Q}(\sqrt[3]{12})$  both have discriminant  $-972$  but they are not isomorphic. Hence we see that the discriminant is in fact not a complete invariant, i.e., it does not specify completely the isomorphism class of a number field.

---

<sup>1</sup>This group, view as a subgroup of  $S_n$  where  $n = [K : \mathbb{Q}]$ , is even if and only if the discriminant of  $K$  is a perfect square. A transitive subgroup  $G$  of  $S_n$  is said to be even if  $G \subset A_n$ .

<sup>2</sup> Even for a simple property like  $P_n :=$  “having degree equal to  $n$ ” the asymptotic behavior of  $N_{P_n}(X)$  is still unknown in general. A conjecture due to Linnik asserts that  $N_{P_n}(X) \sim C_n X$ .

Since the discriminant is an invariant so close to being complete a natural question is

- ♣ Can we find a closely related invariant that refines (improves) the discriminant and that is in fact complete?

Among the several options<sup>3</sup> one candidate seems to be the most natural. The **integral trace form** is the integral quadratic form associated to restriction of the trace pairing

$$\mathrm{tr}_{K/\mathbb{Q}} : K \times K \rightarrow \mathbb{Q}, (x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

to the ring of integers  $\mathcal{O}_K$  of  $K$ . Since the discriminant of  $K$  is the discriminant of the quadratic  $\mathbb{Z}$ -module  $(\mathcal{O}_K, \mathrm{tr}_{K/\mathbb{Q}})$ , we can consider the isometry class of  $(\mathcal{O}_K, \mathrm{tr}_{K/\mathbb{Q}})$  as such a refinement.

This invariant made its first appearance in the 80's in a pioneer work by R. Perlis & P.E. Conner [CP84] where they proved the following theorem

**Theorem 1** ([CP84, Theorem IV.1.1]). *Suppose  $K$  and  $L$  are Galois number fields of odd prime degree  $l$  such that  $\mathrm{disc}(K) = \mathrm{disc}(L)$ . Then, for every isomorphism of groups*

$$h : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q})$$

*There is isometry of quadratic  $\mathbb{Z}$ -modules  $\phi : (\mathcal{O}_K, \mathrm{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L, \mathrm{tr}_{L/\mathbb{Q}})$  such that*

$$\phi\sigma = h(\sigma)\phi \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q})$$

The theorem actually tells us the opposite of what we hoped for. For this type of fields the integral trace forms is just as good invariant as the discriminant itself, there was no improvement. And since there are examples of not isomorphic Galois cubic fields with the same discriminant, we see that this invariant is not complete in general either.

However, when given any invariant we can always ask exactly when two objects that share the same invariant are forced to be isomorphic. And in the case of the integral trace form the question is particularly interesting due to its intimate relation with the discriminant.

## The cubic case

This question was first studied systemically for cubic fields in [MS10]. To state the results established there we need the following definition

**Definition 1.** An integer  $D$  is said to be a **fundamental discriminant** if it is the discriminant of a quadratic field or equivalently if  $1 \neq D$  and  $D$  is either square-free congruent to 1

<sup>3</sup>Other invariants refining the discriminant include its Dedekind zeta function  $\zeta_K$  (see [Per77]), its Brauer equivalent class (see [Lin18]) and its ring of adèles  $\mathbb{A}_K$ .

modulo 4 or of the form  $D = 4m$  where  $m$  is a square-free integer not congruent to 1 modulo 4

The paper [MS10] starts by giving lots of different examples of non-conjugated (not isomorphic) cubic fields  $K$  and  $L$  such that  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ . Here is a summary of the examples found in [MS10] (the polynomials displayed define the corresponding non-conjugated cubic fields  $K$  and  $L$ , i.e., the fields are obtained by adjoining a root of the respective polynomial to  $\mathbb{Q}$ ):

	Galois (square disc.)	non fundamental disc.	fundamental disc.
<b>disc</b> > 0	$x^3 - 6x^2 + 9x + 1$ $2x^3 + 3x^2 - 9x + 2$ disc = $42^2$	$2x^3 + 3x^2 - 21x + 4$ $x^3 + 9x^2 - 18x - 1$ disc = $3^5 \cdot 5^2 \cdot 11$	???
<b>disc</b> < 0	***	$x^3 - 6$ $x^3 - 12$ disc = $-2^2 \cdot 3^5$	$x^3 - 16x + 27$ $x^3 + 2x + 11$ disc = $-3299$

**Table 1:** Examples in the cubic case from [MS10]

Each example actually represents a theorem and whole family of examples, the upper left being Perlis and Conner's theorem in degree  $l = 3$ . This may lead to the conclusion that the integral trace form is not such a good refinement. Nevertheless, observe how in the upper right no example was ever found. In fact, Mantilla-soler in [MS10] obtained a first positive result by showing that the integral trace form is indeed a complete invariant for this type of cubic fields!. More precisely, he proved

**Theorem 2** (Mantilla-Soler, [MS10]). *Let  $K$  be a cubic number field of positive, fundamental discriminant. Let  $L$  be a number field such that there exists an isomorphism of quadratic modules*

$$(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$$

and assume  $9 \nmid \text{disc}(L)$ . Then  $K \cong L$ .

Here  $\mathcal{O}_K^0 = \{x \in \mathcal{O}_K : \text{Tr}_{K/\mathbb{Q}}(x) = 0\}$  is the **trace zero** module. It is easy to see that for totally real number fields<sup>4</sup>  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  always implies  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  (see Proposition 2.10) so the theorem in particular proves what we wanted since  $9 \nmid \text{disc}(L)$  when  $\text{disc}(L)$  is fundamental .

The proof of Theorem 2 given [MS10] is not at all trivial and relies on a clever combination of the law of composition of Bhargava cubes [Bha01] with the Delone-Faddeev parametrization of cubic rings.

<sup>4</sup>A number field is totally real if every embedding  $\sigma : K \hookrightarrow \mathbb{C}$  is real, i.e.,  $\sigma(K) \subset \mathbb{R}$ .

## Totally real vs Nontotally real

The dichotomy of positive versus negative discriminant that we saw in Table 1 for the cubic case is by no means coincidental. It is related to a deep result in the theory of quadratic forms known as Eichler's theorem which implies, for example, that two indefinite regular quadratic forms of dimension  $n \geq 3$  are equivalent if and only if they lie in the same spinor genus. By a theorem due to Olga Taussky (see Theorem 2.9) the trace form of a number field  $K$  is definite precisely when  $K$  is totally real, this corresponds in the cubic case to discriminant being positive. So for non-totally real fields, in order to see if the integral trace forms are equivalent, it is sufficient to prove that they lie in the same spinor genus.

Surprisingly in [MS15] the author was able to completely characterize the spinor genus of the integral trace form in terms of very simple invariants.

**Theorem 3** ([MS15, Proposition 2.9]). *Let  $K, L$  be tamely ramified number fields of the same degree  $n \geq 3$ . The integral trace forms of  $K$  and  $L$  are in the same spinor genus if and only if the following conditions hold:*

- (i)  $\text{disc}(K) = \text{disc}(L)$
- (ii)  $K$  and  $L$  have the same number of complex embeddings.
- (iii) For every finite prime  $p \neq 2$  that ramifies in  $K$  if  $\{\mathfrak{p}_i\}, \{\mathfrak{q}_j\}$  are the primes lying above  $p$  in  $K$  and  $L$ , respectively. Then, the numbers  $\#\left\{i : f(\mathfrak{p}_i|p) \text{ is even or } \left(\frac{e(\mathfrak{p}_i|p)}{p}\right) = 1\right\}$  and  $\#\left\{j : f(\mathfrak{q}_j|p) \text{ is even or } \left(\frac{e(\mathfrak{q}_j|p)}{p}\right) = 1\right\}$  are congruent modulo 2.

In particular, Theorem 3 provides us with a general tool to find examples of non-totally real fields  $K \not\cong L$  with equivalent integral trace forms in higher degrees. Here are the examples with discriminant of minimal absolute value in degrees 4, 5 and 6 found with Magma.

**Example 1.** The polynomials  $x^4 - 2x^2 - x - 2$  and  $x^4 - x^3 - 2x - 3$  define non-conjugated quartic fields of discriminant  $-4027$ . They satisfy the hypothesis of Theorem 3 and since they are not totally real they have equivalent integral trace forms.

**Example 2.** The polynomials  $x^5 + 2x^3 - x + 1$  and  $x^5 + 2x^4 - 2x^2 - 1$  define non-conjugated quintic fields of discriminant  $16757 = 13 \cdot 1289$ . They satisfy the hypothesis of Theorem 3 and since they are not totally real they have equivalent integral trace forms.

**Example 3.** The polynomials  $x^6 - 2x^5 + 4x^4 - 6x^3 + 6x^2 - 5x + 3$  and  $x^6 - 3x^5 + 4x^4 - 3x^3 + x^2 + 1$  define non-conjugated sextic fields of discriminant  $-64387 = -31^2 \cdot 67$ . They satisfy the hypothesis of Theorem 3 and since they are not totally real they have equivalent integral trace forms.

## The Conjecture

Although Theorem 3 gives us a neat description of the trace form in the non-totally real case, it still leaves us with the question of whether or not the analogue of Theorem 2 holds for totally real fields in degree  $n > 3$ . More specifically, the following question was raised in [MS12]

**Question 1.** Are there examples of non-conjugated totally real number fields  $K$  and  $L$  of fundamental discriminant such that their corresponding trace zero forms (resp, integral trace forms) are equivalent?

Mantilla-Soler gave a partial answer by proving computationally that there is no such examples with degree  $\leq 11$  and discriminant  $\leq 10^9$

**Theorem 4** (Mantilla-Soler, [MS12]). *Let  $n$  be a positive integer less than 11, and let  $X_n$  be the quantity described in Table 2. Suppose that  $K$  is a totally real number field of degree  $n$  with fundamental discriminant bounded by  $X_n$ . If  $L$  is a tamely ramified number field such that*

$$(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$$

Then  $K \cong L$ .

$X_n$	$n$
$\infty$	1,2,3
$1.0 \times 10^9$	4,5,6
$8.9 \times 10^{10}$	7
$2.5 \times 10^9$	8
$2.8 \times 10^{10}$	9
$2.8 \times 10^{10}$	10

**Table 2:** Upper bounds

The results were particularly solid in the quartic case. The reason for this, totally real fields with fundamental discriminant (and such that there is at least one more field with the same discriminant) get much more scarce as we increase the degree. For  $5 \leq n \leq 10$  and the values of  $X_n$  described in Table 2 there are only 5, 122 such number fields with discriminant  $\leq X_n$ , all of them for  $n \in \{5, 6, 7\}$ . In contrast, there are a total of 1, 301, 472 quartic fields with this property and discriminant  $\leq 10^9$ . With such a strong evidence for the quartic case the following conjecture was formulated

**Conjecture 1** (Mantilla-Soler, [MS12]). Let  $K$  be a totally real quartic number field with fundamental discriminant. If  $L$  is a tamely ramified number field such that an isomorphism of quadratic modules

$$(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$$

exists. Then  $K \cong L$ .

Since its formulation in 2012 the conjecture has received noticeable attention, see for example

- Jordan Ellengber’s post in Quomodocumque: [Can the trace hear the shape of its field?](#).
- F.O. Odumodu’s thesis from Stellenbosch University [Odu13] (supervised by B.Erez).

However, the problem had remained open up to now.

## New results

The main result of this thesis answers Question 1 for integral trace forms.

**Theorem 5** (cf. Theorem 4.18). *Let  $K$  be a totally real number field with fundamental discriminant. If  $L$  is a number field such that an isomorphism of quadratic modules*

$$(\mathcal{O}_K, tr_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, tr_{L/\mathbb{Q}})$$

*exists. Then  $K \cong L$ .*

The hypothesis of the above theorem can be interpreted in some sense as “having the least possible ramification”. This is because a totally real number field is a field where the infinite prime of  $\mathbb{Q}$  is unramified and a number field of fundamental discriminant is a field such that for each finite rational prime  $p$  that ramifies in  $K$  only one prime  $\mathfrak{p}|p$  in  $K$  is allowed to be ramified over  $\mathbb{Q}$  and for that prime the ramification index and inertia degree are as small as possible  $e(\mathfrak{p}|p) = 2$  and  $f(\mathfrak{p}|p) = 1$ , see (3.1).

This theorem is pretty general but it does not prove Conjecture 1 yet. This is achieved in the next theorem

**Theorem 6** (cf. Theorem 4.19). *Let  $K$  be a totally real number field of fundamental discriminant and degree  $n \geq 3$  such that  $(\mathbb{Z}/n\mathbb{Z})^\times$  is cyclic. Then, for any number field  $L$  the following are equivalent:*

- (i)  $K \cong L$
  - (ii)  $(\mathcal{O}_K, tr_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, tr_{L/\mathbb{Q}})$ .
  - (iii)  $(\mathcal{O}_K^\perp, tr_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^\perp, tr_{L/\mathbb{Q}})$ .
  - (iv)  $Sh(K) = Sh(L)$  and  $L$  is totally real with fundamental discriminant.
- If  $(n, disc(K)) = 1$ , then the four items are also equivalent to*
- (v)  $(\mathcal{O}_K^0, tr_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, tr_{L/\mathbb{Q}})$ .

Here  $\mathcal{O}_K^\perp$  is the set of elements of  $\mathbb{Z} + n\mathcal{O}_K$  with trace zero and  $\text{Sh}(K)$  is the shape of  $K$ , an important geometric invariant that have been greatly studied in recent years, see Chapter 2 for its definition and more details.

Now Conjecture 1 follows from Theorem 6 for  $n = 4$ , by noting that for tamely ramified  $L$  we have  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$  (see (2.6)(ii)), thus  $\text{disc}(L) = \frac{\text{disc}(\mathcal{O}_L^0)}{4} = \frac{\text{disc}(\mathcal{O}_K^0)}{4} = \text{disc}(K)$  (see (2.3)). Also  $2 \nmid \text{disc}(L)$ , otherwise, 2 would ramify in  $L$  and, as we mentioned before, this would imply  $2 = e(\mathfrak{p}|2)$  for a unique  $\mathfrak{p}|2$  in  $L$ , contradicting that  $L$  is tame at 2.

Observe that if we apply Theorem 6 to  $n = 3$  we almost recover Theorem 2, but we would have to change the condition  $9 \nmid \text{disc}(L)$  (which is equivalent to  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$  (2.6)(i)) by the more restrictive condition  $3 \nmid \text{disc}(L)$ . Hence we would like to remove the hypothesis “ $(\text{disc}(K), n) = 1$ ” and “ $(\mathbb{Z}/n\mathbb{Z})^\times$  is cyclic” from our theorem. Even though we were not able to do that (and we are not sure if it is possible at all), we can prove that the theorem with these hypothesis removed holds up to (possibly) finitely many counter examples for each  $n$ .

**Theorem 7** (cf. Theorem 4.20). *Let  $K$  be a totally real number field with fundamental discriminant and degree  $n$ . Then, for a number field  $L$  such that  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$ , the five statements in the above theorem are equivalent up to finitely many counterexamples for each  $n$ . More specifically, they will be equivalent as soon as  $\text{disc}(K) \geq (32n^3)^{\frac{n^2(n+1)}{4}}$ .*

For example, to completely recover Theorem 2 it would be “enough” to check it in a computer for all the cubic fields with positive fundamental discriminant less than

$$864^9 \approx 2.26 \times 10^{26}$$

## Outline of the thesis

- In Chapter 1 we fix some notation and review some of the basic notions and facts that will be used in the rest of the work. From quadratic forms we will not need any deep result, just some basic definitions. Since we will be working with both global and local fields, we chose to make a presentation of the essentials of algebraic number theory via the theory of Dedekind domains. We also work with some properties of permutation group theory that will be useful in Chapter 3.
- The goal of Chapter 2 is to study the interplay of three closely related quadratic invariants that have been introduced in the literature. These are: the integral trace form with associated quadratic  $\mathbb{Z}$ -module  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$ , the trace zero form with associated quadratic  $\mathbb{Z}$ -module  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$  and the shape  $\text{Sh}(K)$  linked to a quadratic  $\mathbb{Z}$ -module  $(\mathcal{O}_K^\perp, b_K)$ .

After giving their definition and describing some of their well-known properties, we show that for totally real fields  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  is the strongest of these invariants and how under certain conditions on  $[K : \mathbb{Q}]$  and  $\text{disc}(K)$  the trace zero and  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$  become stronger than  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$ . We also show that for  $\mathbb{Z}/l\mathbb{Z}$ -fields with  $l$  prime the three invariants  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$ ,  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$  and  $(\mathcal{O}_K^\perp, b_K)$  are essentially the same.

- Chapter 3 deals with Galois theory of field with fundamental discriminant. Most of the chapter is devoted to prove Theorem 3.19 (a key result we need to complete the proof of our main theorem in Chapter 4 in case the prime  $p = 2$  divides the discriminant and also to prove Theorem 7). Another important fact proved in the chapter is Corollary 3.8 (a statement on linear disjointness of fields with fundamental discriminant needed in the proof of Theorem 5).

We also give an alternative proof of the fact that fields with (possibly even) fundamental discriminant of degree  $n$  are  $S_n$ -fields. This result was first proved in [N+88] for odd fundamental discriminant and it was later generalized to any fundamental discriminant in [Kon95]. The proof given here was constructed out of [N+88] without knowing of the existence of [Kon95].

- In Chapter 4 we introduced the most important ingredient in the proof of our main results, the Casimir elements  $c_B(\psi, \phi)$  and the Casimir parings  $\langle \cdot, \cdot \rangle_B$ . We explore some of their nice properties and show how they generalize the Casimir elements from the theory of representation of Lie algebras. We conclude the chapter by putting together all the previous work to prove the main results.
- Finally in Chapter 5 we adapt the proof of Theorem 2 given in [MS10] to obtain a proof of Conjecture 1 via Bhargava's parametrization of quartic rings.

# 1 Preliminaries

In this chapter we review some of the material from algebraic number theory and quadratic forms that will be needed in the rest of the work, the main references are [Mil, Ser79] for algebraic number theory and [Ger08, O'M13] for quadratic forms.

## 1.1. Quadratic modules

**Definition 1.1.** Let  $R$  be an integral domain and  $F$  a field containing  $R$ , a **quadratic  $R$ -module** is a pair  $(M, B)$  where  $M$  is a free  $R$ -module of finite rank and  $B : M \times M \rightarrow F$  is a symmetric bilinear form. When  $R = F$  so that  $M = V$  is an  $F$ -vector space, we call the pair  $(V, B)$  a **quadratic  $F$ -space**. Finally, if  $B$  is a symmetric bilinear form, the mapping  $q : M \rightarrow F$  defined by  $x \mapsto B(x, x)$  is the **quadratic map** associated with  $B$ .

**Definition 1.2.** Let  $(M_1, B_1)$  and  $(M_2, B_2)$  be quadratic  $R$ -modules an **isometry** is an isomorphism of  $R$ -modules

$$\varphi : M_1 \rightarrow M_2$$

such that  $B_2(\varphi(x), \varphi(y)) = B_1(x, y)$  for all  $x, y \in M_1$ . We say that  $M_1$  and  $M_2$  are **isometric** which we write as

$$(M_1, B_1) \cong (M_2, B_2)$$

or simply  $M_1 \cong M_2$  if there exists a isometry between  $M_1$  and  $M_2$ .

Let  $\mathcal{B} := \{v_i\}$  be an  $R$ -basis of the quadratic  $R$ -module  $(M, B)$ , the symmetric matrix

$$A = (B(v_i, v_j)) \in M_n(F)$$

is called the **Gram matrix of  $(M, B)$  with respect to  $\mathcal{B}$** . We write

$$M \cong A \text{ in } \mathcal{B}$$

if  $A$  is the Gram matrix of  $(M, B)$  in the basis  $\mathcal{B}$  and we write  $M \cong A$  (no basis mentioned) if  $A$  is the Gram matrix of  $(M, B)$  in *some* basis. Also, if  $A$  is the diagonal matrix  $\text{diag}(a_1, \dots, a_n)$  we write  $M \cong \langle a_1, \dots, a_n \rangle$ . Remark that the Gram matrix captures completely the isometry class of the quadratic module, i.e., if  $M_1 \cong A$  then  $M_1 \cong M_2$  if and only if  $M_2 \cong A$ .

Suppose  $M \cong A$  in a basis  $\mathcal{B} := \{v_1, \dots, v_n\}$  and take  $\{v'_1, \dots, v'_n\} \subset M$ , then  $v'_i = \sum_j t_{ij}v_j$  for some matrix  $T = (t_{ij}) \in M_n(R)$ , hence if  $A' := (B(v'_i, v'_j))$  then  $A' = TAT^t$  and thus

$$\det(A') = \det(T)^2 \det(A) \quad (1)$$

In particular, if  $\mathcal{B}' := \{v'_1, \dots, v'_n\}$  is another basis, so that  $M \cong A'$  in  $\mathcal{B}'$ , then the  $T$  is an invertible matrix, i.e.,  $\det(T) \in R^\times$ . So

$$\det(A) = \det(A') \pmod{(R^\times)^2}$$

This allows us to give the following definition

**Definition 1.3.** Let  $(M, B)$  be a quadratic  $R$ -module with  $M \cong A$ . The **discriminant** of  $(M, B)$  denoted  $\text{disc}(M, B)$  or  $\text{disc}(M)$  is defined as the class of  $\det(A)$  in  $F/R^{\times 2}$  (quotient of multiplicative monoids).

Another easy but important consequence of the relation (1) is

**Corollary 1.4.** Suppose  $R$  is a principal ideal domain. Let  $(M, B)$  be an  $R$ -quadratic module of rank  $n$  and let  $N \leq M$  be an  $R$ -submodule of the same rank. Write

$$M/N \cong R/d_1R \oplus \dots \oplus R/d_tR$$

then where  $d_1 \mid d_2 \dots \mid d_t$  are the elementary divisor, then

$$\text{disc}(N, B) = (d_1 \cdots d_t)^2 \text{disc}(M, B)$$

where  $(N, B)$  is the quadratic  $R$ -module obtained by restricting  $B$  to  $N$ . In particular, if  $\text{disc}(M, B) \neq 0$ , then  $N = M$  if and only if  $\text{disc}(N, B) = \text{disc}(M, B)$ .

For example if  $R = \mathbb{Z}$ , this relation reads  $\text{disc}(N, B) = [M : N]^2 \text{disc}(M, B)$ .

## Orthogonality

Let  $(M, B)$  be a quadratic  $R$ -module. If  $N$  is a submodule of  $M$  its **orthogonal complement** is

$$N^\perp := \{v \in M : B(v, x) = 0, \text{ for all } x \in N\}$$

Two elements  $x, y \in M$  are said to be **orthogonal** if  $B(x, y) = 0$  and two subsets  $X, Y \subset M$  are orthogonal if  $B(x, y) = 0$  for all  $x \in X$  and  $y \in Y$ . Finally, given submodules  $N_i$  of  $M$  we write

$$M = \perp_i N_i$$

(an **orthogonal sum**) if  $M = \bigoplus_i N_i$  and the  $N_i$  are pairwise orthogonal. Note that if  $N_i \cong A_i$ , then  $N \cong A$  where  $A$  is the matrix diagonal in the blocks  $A_i$ . Thus,

$$\text{disc}(M) = \prod_i \text{disc}(M_i)$$

The following theorem is a consequence of a version of the **Gram-Schmidt** process, proved for  $\mathbb{R}^n$  in a basic linear algebra course, in general quadratic spaces.

**Theorem 1.5** ([Ger08, Theorem 2.11]). *Let  $(V, B)$  be any  $n$ -dimensional quadratic  $F$ -space, then  $V$  has an orthogonal basis, i.e., exists  $\{v_1, \dots, v_n\}$  such that  $V = Fv_1 \perp \dots \perp Fv_n$ .*

Let  $(V, B)$  be a quadratic  $F$ -space we say that  $(V, B)$  is **non-degenerate** or **regular** if its **radical**  $\text{rad}(V) := V^\perp$  is zero.

**Corollary 1.6.** A quadratic space  $V$  is non-degenerate if and only if  $\text{disc}(V) \neq 0$

*Proof.* Let  $\{v_i\}$  be an orthogonal basis of  $V$ , then  $\text{rad}(V) = 0$  if and only if  $q(v_i) \neq 0$  for all  $i$  and  $\text{disc}(V) = \prod_i q(v_i) \pmod{F^{\times 2}}$ .  $\square$

### Dual basis

Let  $F$  be a field and  $V$  be a finite dimensional  $F$ -vector space. Each basis  $\{v_1, \dots, v_n\}$  of  $V$  has an associated dual basis  $\{f_1, \dots, f_n\}$ , a basis of the dual space  $\text{Hom}_F(V, F) =: V^*$  defined by

$$f_i(v_j) = \delta_{ij} \text{ (Kronecker delta)}$$

In particular,  $V \cong V^*$ , as both spaces have the same dimension  $n$ .

Now let  $B : V \times V \rightarrow F$  be an  $F$ -bilinear form, this induces a map

$$\phi_B : V \rightarrow V^*, v \mapsto (w \mapsto B(v, w))$$

Which is injective, and thus an isomorphism, if and only if  $B$  is non-degenerate. In that case, for each  $F$ -basis  $\{v_i\}$  of  $V$ , by taking the inverse image through  $\phi_B$  of the dual basis  $\{f_i\}$  of  $\{v_i\}$  in  $V^*$  we get a unique  $F$ -basis  $\{v_i^*\}$  of  $V$  such that

$$B(v_i, v_j^*) = \delta_{ij}$$

we call  $\{v_i^*\}$  the **dual basis** of  $\{v_i\}$  in  $V$  with respect to  $B$ .

### Scalar extension

Let  $R \subset S$  be commutative rings and  $(M, B)$  be a quadratic  $R$ -module, then we can endow the  $S$ -module  $M \otimes_R S$  with a natural structure of quadratic  $S$ -module  $(M \otimes S, B \otimes S)$  by defining  $B \otimes S$  as the unique  $S$ -bilinear form such that

$$(B \otimes S)(v \otimes 1, w \otimes 1) = B(v, w) \in S$$

for all  $v, w \in M$ .

## Signature

**Theorem 1.7 (Witt Cancellation , [Ger08, Theorem 2.38]).** *If  $V, V_1, V_2$  are non-degenerate quadratic  $F$ -spaces such that*

$$V \perp V_1 \cong V \perp V_2$$

*then  $V_1 \cong V_2$ .*

Since  $\mathbb{R}^\times / \mathbb{R}^{\times 2} = \{-1, +1\}$ , this result together with (1.5) implies the following

**Theorem 1.8 (Sylvester's law of inertia, [Ger08, Theorem 2.40]).** *Let  $(V, B)$  nondegenerate quadratic space over  $\mathbb{R}$  then exists unique  $r$  and  $s$  such that*

$$V \cong \underbrace{\langle 1, 1, \dots, 1 \rangle}_r \underbrace{\langle -1, \dots, -1 \rangle}_s$$

We define the **signature** of a non-degenerate real quadratic space  $(V, B)$  as  $(r, s)$ , we say that  $(V, B)$  is **positive definite** is it has signature  $(r, 0)$  or equivalently if  $q(v) > 0$  for all  $v \neq 0$ . We say that  $(V, B)$  is **indefinite** if neither  $r$  nor  $s$  is 0. If  $(V, B)$  is a non-degenerate quadratic  $\mathbb{Q}$ -space, then the signature of  $(V, B)$  is the signature of  $(V \otimes \mathbb{R}, B \otimes \mathbb{R})$ .

## 1.2. Some basic algebraic number theory

### 1.2.1. Number fields and rings of integers

Let  $A$  be an integral domain, which is not a field. We say that  $A$  is a **Dedekind domain** if any of the following equivalent conditions hold:

- (a) Every non zero proper ideal  $\mathfrak{a}$  of  $A$  factor uniquely (up to order) into a product of prime ideals.
- (b)  $A$  is Noetherian, integrally closed and every nonzero prime ideal is maximal (i.e.,  $A$  has Krull dimension 1).
- (c)  $A$  is Noetherian and for every pair of ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  such that  $\mathfrak{a} \subset \mathfrak{b}$  exists  $\mathfrak{c}$  such that  $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$  (to contain is to divide).

Dedekind domains are a fundamental concept in algebraic number theory, because, as shown in condition (a), they somehow mimic the fundamental theorem of arithmetic in  $\mathbb{Z}$  in arbitrary domains. Another reason why they are important is given by the following theorem

**Theorem 1.9 ([Mil, Theorem 3.29]).** *Let  $A$  be a Dedekind domain with field of fractions  $K$ , and let  $B$  be the integral closure of  $A$  in a finite separable extension  $L$  of  $K$ . Then  $B$  is a Dedekind domain.*

A prototypical example of a Dedekind domain is  $A = \mathbb{Z}$ , since for example clearly satisfies condition (a) in the definition. A **number field**  $K$  is a subfield of  $\mathbb{C}$  of finite degree over  $\mathbb{Q}$ , it follows from the above theorem that the integral closure  $\mathcal{O}_K$  of  $\mathbb{Z}$  in a number field  $K$  (i.e. the set of all elements in  $K$  which are zeros of monic polynomials with coefficients in  $\mathbb{Z}$ ) is also a Dedekind domain, this ring is known as the **ring of algebraic integers** in  $K$ .

Let  $A$  be a Dedekind domain with field of fractions  $K$ , and let  $B$  be the integral closure of  $A$  in a finite separable extension  $L$  of  $K$ . Take a prime ideal<sup>1</sup>  $\mathfrak{p}$  in  $A$ , then according to (a) the ideal  $\mathfrak{p}B$ , generated by  $\mathfrak{p}$  in  $B$ , factors uniquely in  $B$  as

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

where  $g \geq 1$ , the  $\mathfrak{P}_i$  are distinct prime ideals in  $B$  and  $e_i > 0$ . The primes  $\mathfrak{P}_i$ , which by (c) are precisely the primes in  $B$  containing  $\mathfrak{p}$ , are said to lie over  $\mathfrak{p}$  or divide  $\mathfrak{p}$ ; the number  $e_i$  denoted  $e(\mathfrak{P}_i|\mathfrak{p})$  is called the **ramification index** and the number  $f_i := [B/\mathfrak{P}_i : A/\mathfrak{p}]$  denoted  $f(\mathfrak{P}_i|\mathfrak{p})$  is called the **inertia degree**. In this case we use the notation<sup>2</sup>  $f_1^{e_1} f_2^{e_2} \cdots f_g^{e_g}$  and we say that  $\mathfrak{p}$  has **factorization type**  $f_1^{e_1} f_2^{e_2} \cdots f_g^{e_g}$  in  $B$ .

We say that the prime  $\mathfrak{p}$  is **ramified** in  $B$  if there is a prime  $\mathfrak{P}$  in  $B$  lying over  $\mathfrak{p}$  such that  $e(\mathfrak{P}|\mathfrak{p}) > 1$  (in that case we also say that  $\mathfrak{P}$  is ramified over  $K$ ) and we say that  $\mathfrak{p}$  **splits completely** in  $B$  if  $e(\mathfrak{P}|\mathfrak{p}) = 1 = f(\mathfrak{P}|\mathfrak{p})$  for all primes  $\mathfrak{P}$  in  $B$  lying over  $\mathfrak{p}$ .

A fundamental relation between the  $e$ 's and  $f$ 's is the following

**Theorem 1.10** ([Mil, Theorem 3.34]). *Let  $A, K, B$  and  $L$  be as above, and let  $\mathfrak{P}_1 \cdots \mathfrak{P}_g$  be the primes in  $B$  lying over a prime  $\mathfrak{p}$  in  $A$ ; then*

$$\sum_{i=1}^g e(\mathfrak{P}_i|\mathfrak{p}) f(\mathfrak{P}_i|\mathfrak{p}) = [L : K]$$

*If  $L$  is Galois over  $K$ , then all ramification index are equal and all inertia degrees are equal, and thus*

$$efg = [L : K]$$

*where  $e := e(\mathfrak{P}_i|\mathfrak{p})$  and  $f := f(\mathfrak{P}_i|\mathfrak{p})$ .*

A simple fact that is used quite often is that these numbers are multiplicative in towers.

**Proposition 1.11.** Let  $K \subset L \subset M$  be a tower of fields where  $K$  and  $L$  are as above and  $M/L$  is finite and separable. If  $\mathfrak{Q}$  is a prime in the integral closure of  $B$  in  $M$ ,  $\mathfrak{P} := \mathfrak{Q} \cap B$  and  $\mathfrak{p} := \mathfrak{P} \cap A$ . Then,  $e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{P})e(\mathfrak{P}|\mathfrak{p})$  and  $f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P})f(\mathfrak{P}|\mathfrak{p})$ .

<sup>1</sup>As in many texts in algebraic number theory from now on we will assume the convention of ideal meaning a nonzero ideal.

<sup>2</sup>This is Bhargava's notation.

Another useful property of this kind of extensions is the following

**Proposition 1.12** ([Mil, Proposition 2.29]). Let  $A$  be an integrally closed domain with field of fractions  $K$ , and let  $B$  be the integral closure of  $A$  in a separable extension  $L$  of  $K$  of degree  $m$ . There exists free  $A$ -modules  $M$  and  $M'$  of  $L$  such that

$$M \subset B \subset M'$$

Therefore  $B$  is a finitely generated  $A$ -modules if  $A$  is Noetherian, and it is free of rank  $m$  if  $A$  is a principal ideal domain.

## 1.2.2. Hilbert ramification theory

Suppose  $A, B, K$  and  $L$  are as above and suppose  $L/K$  is a Galois extension with Galois group  $G := \text{Gal}(L/K)$ . The group  $G$  acts naturally on the set of all primes  $\mathfrak{P}$  in  $B$  above a given prime  $\mathfrak{p}$  in  $A$  by setting  $\sigma\mathfrak{P} := \sigma(\mathfrak{P})$ ,  $\sigma \in G$ . A key fact that links Galois theory and the decomposition of primes in field extensions is the following

**Proposition 1.13** ([Neu13, I Proposition 9.1]). The above action is transitive.

It follows from the Orbit-Stabilizer theorem that if we fix a prime  $\mathfrak{P}$  in  $L$  over  $\mathfrak{p}$ , then the total number of such primes will be

$$[G : D_{\mathfrak{P}}]$$

where  $D_{\mathfrak{P}} := \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$  is the **decomposition group** of  $\mathfrak{P}$ . This together with (1.10) shows  $|D_{\mathfrak{P}}| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$ .

It is also possible to give a interpretation of the ramification index in terms of groups. To see this let us define the **inertia group** of a prime  $\mathfrak{P}$  in  $B$  as

$$I_{\mathfrak{P}} := \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}, \text{ for all } \alpha \in B\}$$

**Proposition 1.14** ([Neu13, I Proposition 9.4]). Let  $\tilde{G}$  be the Galois group of  $A/\mathfrak{p} \subset B/\mathfrak{P}$ , then there is an exact sequence of groups

$$1 \rightarrow I_{\mathfrak{P}} \hookrightarrow D_{\mathfrak{P}} \rightarrow \tilde{G} \rightarrow 1$$

and hence  $I_{\mathfrak{P}} \triangleleft D_{\mathfrak{P}}$  and  $|I_{\mathfrak{P}}| = e(\mathfrak{P}|\mathfrak{p})$ .

Let us fix a prime  $\mathfrak{P}$  in  $L$  lying over  $\mathfrak{p} := \mathfrak{P} \cap K$  with decomposition and inertia groups  $D$  and  $I$ . According to propositions 1.13 and 1.14 if  $D$  acts by right multiplication on  $G$ , then there is a bijection between the set  $D$ -orbits (or right cosets)  $G/D := \{\sigma D : \sigma \in G\}$  and the set of primes in  $N$  over  $\mathfrak{p}$ , given by

$$\sigma D \longleftrightarrow \sigma(\mathfrak{P})$$

Moreover each  $D$ -orbit  $\sigma D$  has size  $|D| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$  and if we restrict the action to  $I$  then each  $I$ -orbit  $\sigma I$  has size  $|I| = e(\mathfrak{P}|\mathfrak{p})$ .

This generalizes naturally to a (possibly non-Galois extension)  $L/K$ . More precisely, we have the following

**Proposition 1.15.** Let  $A$  be a Dedekind domain with field of fractions  $K$ , let  $B$  be the integral closure of  $A$  in a finite separable extension  $L$  of  $K$  and suppose  $N/K$  is a Galois extension of  $L/K$  with Galois group  $G$ . Fix a prime  $\mathfrak{P}$  in  $N$  with inertia and decomposition groups  $I$  and  $D$ . Let  $H := \text{Gal}(N/L)$  and let  $D$  act on the set of left cosets  $H \backslash G = \{H\sigma : \sigma \in G\}$  by right multiplication, then

- (i) The map taking the  $D$ -orbit of the coset  $H\sigma$  to  $\sigma(\mathfrak{P}) \cap L$  is a well defined bijection between the double quotient  $H \backslash G / D$  and the set of primes in  $L$  lying over  $\mathfrak{p} := \mathfrak{P} \cap K$ .
- (ii) If  $\mathfrak{q} := \sigma(\mathfrak{P}) \cap L$ , then the size of the  $D$ -orbit of  $H\sigma$  in  $H \backslash G$  is given by

$$[\sigma D \sigma^{-1} : \sigma D \sigma^{-1} \cap H] = e(\mathfrak{q}|\mathfrak{p})f(\mathfrak{q}|\mathfrak{p}) = |H\sigma D|/|H|$$

and the size of the  $I$ -orbit of  $H\sigma$  (the orbit of the action restricted to  $I$ ) is given by

$$[\sigma I \sigma^{-1} : \sigma I \sigma^{-1} \cap H] = e(\mathfrak{q}|\mathfrak{p}) = |H\sigma I|/|H|$$

*Proof.* See [Neu13, I §9]. □

**Corollary 1.16.** Let  $L_1/K$  and  $L_2/K$  finite separable extensions of  $K$ , then a prime  $\mathfrak{p}$  is unramified in  $L_1 L_2$  if and only if  $\mathfrak{p}$  is unramified in  $L_1$  and  $L_2$ .

*Proof.* Let  $N$  be a Galois extension containing  $L_1$  and  $L_2$ . By (1.15)(ii) if  $I$  is the inertia group of a prime in  $N$  lying over  $\mathfrak{p}$ , then  $\mathfrak{p}$  is unramified in  $L_i$  if and only if  $\sigma I \sigma^{-1} \subset \text{Gal}(N/L_i)$ , for all  $\sigma \in \text{Gal}(N/K)$ . The claim now follows from the fact  $\text{Gal}(N/L_1 L_2) = \text{Gal}(N/L_1) \cap \text{Gal}(N/L_2)$ . □

**Corollary 1.17.** Let  $\tilde{L}$  be the Galois closure of  $L/K$ , then a prime  $\mathfrak{p}$  is ramified in  $L$  if and only if  $\mathfrak{p}$  is ramified in  $\tilde{L}$ .

*Proof.* The Galois closure  $\tilde{L}$  is the compositum of the conjugates of  $L$  over  $K$  all of which are unramified at  $\mathfrak{p}$  if and only if  $L$  is. □

### Norm and trace

Let  $A \subset B$  be commutative rings such that  $B$  is free of finite rank as an  $A$ -module. Then each  $b \in B$  induces an  $A$ -linear endomorphism of  $B$

$$x \mapsto b \cdot x$$

the **norm** and **trace** of  $b \in B$ , denoted  $\text{Nm}_{B/A}(b)$  and  $\text{Tr}_{B/A}(b)$  are defined as the determinant and trace of this endomorphism.

The following proposition gives us way to compute the norm and trace in finite separable extension of fields

**Proposition 1.18** ([Mil, Corollary 2.20]). Let  $L/K$  be a separable extension of finite degree  $n$ . Fix an extension  $\Omega$  of  $K$  containing the Galois closure of  $L/K$ . If  $\{\sigma_1, \dots, \sigma_r\}$  are the set of embeddings  $L \hookrightarrow \Omega$  fixing  $K$ , then

$$\text{Tr}_{L/K}(\beta) = \sum_{i=1}^n \sigma_i(\beta), \quad \text{Nm}_{L/K}(\beta) = \prod_{i=1}^n \sigma_i(\beta)$$

Note that this in particular imply that if  $B$  is the integral closure in  $L$  of an integrally closed ring  $A \subset K$  with field of fractions  $K$ , then  $\text{Nm}_{L/K}(\beta), \text{Tr}_{L/K}(\beta) \in A$  for all  $\beta \in B$ .

There is also a notion of norms for ideals compatible with this. Namely, suppose  $A$  is a Dedekind domain with field of fractions  $K$  and  $B$  is the integral closure of  $A$  in a finite separable extension  $L$  of  $K$ . Denote  $\text{Id}(A)$  the group of fractional ideals and consider the unique homomorphism of groups

$$\mathcal{N}_{L/K} : \text{Id}(B) \rightarrow \text{Id}(A)$$

defined in primes ideals of  $B$  as  $\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$  where  $\mathfrak{p} := \mathfrak{P} \cap K$ . This generalizes  $\text{Nm}_{L/K}$ , because for principal ideals in  $B$  we have

$$\mathcal{N}_{L/K}(\beta B) = \text{Nm}_{L/K}(\beta)A,$$

see [Mil, Proposition 4.1(c)]. Here are some other properties of  $\mathcal{N}$ .

**Proposition 1.19** ([Mil, §4]). With  $A, K, B$  and  $L$  as above we have:

(i) If  $M/L$  is a finite separable extension, then

$$\mathcal{N}_{M/K} = \mathcal{N}_{L/K} \circ \mathcal{N}_{M/L}$$

(ii) For every ideal  $\mathfrak{a} \subset A$ ,  $\mathcal{N}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^{[L:K]}$ .

(iii) If  $L/K$  is Galois, then

$$\mathcal{N}_{L/K}(\mathfrak{P})B = \prod_{\sigma \in \text{Gal}(L/K)} \sigma \mathfrak{P}$$

(iv) If  $A = \mathbb{Z}$  so that  $K = \mathbb{Q}$  and  $L$  a number field then

$$\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{a}) = (\mathbb{N}(\mathfrak{a}))$$

where  $\mathbb{N}(\mathfrak{a}) := [\mathcal{O}_L : \mathfrak{a}]$ .

### 1.2.3. Absolute values and completions

**Definition 1.20.** Let  $K$  be a field an **absolute value** on  $K$  is a map  $x \mapsto |x| : K \rightarrow \mathbb{R}$  such that for all  $x, y \in K$

- (a)  $|x| \geq 0$  and  $|x| = 0$  if and only if  $x = 0$
- (b)  $|xy| = |x||y|$
- (c)  $|x + y| \leq |x| + |y|$

If in addition the absolute value satisfies

$$(c') \quad |x + y| \leq \max\{|x|, |y|\}$$

we say that  $|\cdot|$  is a **non archimedean absolute value**. The pair  $(K, |\cdot|)$  is called a **valuated field**.

Every absolute value determines a metric on  $K$  by taking

$$d(x, y) := |x - y|$$

as the distance function and thus a topology on  $K$ . We say that two absolute values  $|\cdot|_1$  and  $|\cdot|_2$  on  $K$  are **equivalent** if they define the same topology over  $K$ , this can be seen to be equivalent to say that there exists  $a > 0$  such that  $|\cdot|_2 = |\cdot|_1^a$  or that for all  $x \in K$   $|x|_2 < 1$  implies  $|x|_1 < 1$ , see [Mil, Proposition 7.8].

**Definition 1.21.** Let  $K$  be a field. A **discrete valuation** on  $K$  is a nonzero homomorphism  $v : K^\times \rightarrow \mathbb{Z}$  such that  $v(a + b) \geq \min\{v(a), v(b)\}$ . We say that the valuation is **normalized** if  $v(K^\times) = \mathbb{Z}$ .

Sometimes is convenient to extend  $v$  to all  $K$  by defining  $v(0) = \infty$ .

Let  $v$  be a normalized discrete valuation, then the set

$$A := \{x \in K : v(x) \geq 0\}$$

is a local subring of  $K$  with maximal ideal  $\mathfrak{m} = \{x \in A : v(x) > 0\}$ , which is principal generated by any element  $\pi$  such that  $v(\pi) = 1$  (the element  $\pi$  is called a **uniformizing parameter** or **prime element**). A ring  $A$  arising in this fashion is known as a **discrete valuation ring**, discrete valuation rings are Dedekind domains and in fact a ring  $A$  is a Dedekind domain if and only if every localization  $A_{\mathfrak{p}}$  is a discrete valuation ring.

Let  $e > 1$  be a real number, then every discrete valuation on  $K$  induces a non archimedean absolute value by taking

$$|x| := e^{-v(x)} \tag{2}$$

Conversely, for every nontrivial non archimedean absolute such that

$$\{-\log |x| : x \neq 0\}$$

is a discrete in  $\mathbb{R}$  exists a unique normalized discrete valuation  $v$  on  $K$  and  $e > 1$  such that (2) holds.

We say that a valuated field  $(K, |\cdot|)$  is **complete** if every Cauchy sequence  $(x_n)$  with  $x_n \in K$  converges in  $K$ . A **completion** of  $(K, |\cdot|)$  is a triple  $(\widehat{K}, |\cdot|', \iota)$  such that  $(\widehat{K}, |\cdot|')$  is complete and  $\iota : (K, |\cdot|) \hookrightarrow (\widehat{K}, |\cdot|')$  is a ring homomorphism preserving absolute values such that  $\iota(K)$  is dense in  $\widehat{K}$ .

Given a valuated field  $(K, |\cdot|)$  we can always construct a completion by taking  $\widehat{K}$  to be the set of equivalence classes of Cauchy sequences where

$$(x_n) \sim (y_n) \iff \lim_n |x_n - y_n| = 0$$

with the natural multiplication and addition, absolute value defined by  $|x|' := \lim |x_n|$  and  $\iota : (K, |\cdot|) \hookrightarrow (\widehat{K}, |\cdot|')$ , given by the diagonal embedding mapping  $a \in K$  to the class of the constant sequence  $(x_n)$  with  $x_n = a$  for all  $n$ .

Any completion  $(\widehat{K}, |\cdot|', \iota)$  of  $(K, |\cdot|)$  satisfy the following universal property: Given a complete valuated field  $(L, |\cdot|'')$  and a ring homomorphism  $f : (K, |\cdot|) \rightarrow (L, |\cdot|'')$  preserving absolute values, there exists a unique  $\widetilde{f} : (\widehat{K}, |\cdot|') \rightarrow (L, |\cdot|'')$  ring homomorphism preserving absolute values such that  $f = \widetilde{f} \circ \iota$ .

$$\begin{array}{ccc} (K, |\cdot|) & \xhookrightarrow{\iota} & (\widehat{K}, |\cdot|') \\ f \downarrow & \swarrow \widetilde{f} & \\ (L, |\cdot|'') & & \end{array}$$

Hence a completion of  $(K, |\cdot|)$  always exists and is unique up to isomorphisms preserving absolute values.

**Theorem 1.22** ([Mil, Theorem 7.38]). *Let  $K$  be complete with respect to an absolute value  $|\cdot|_K$  and let  $L$  be a finite separable extension of  $K$  of degree  $n$ . Then  $|\cdot|_K$  extend uniquely to an absolute value  $|\cdot|_L$  and  $L$  is complete for the extended absolute value. For all  $\beta \in L$ ,*

$$|\beta|_L = |\mathrm{Nm}_{L/K} \beta|_K^{1/n}$$

**Corollary 1.23.** *Let  $K$  be as in the theorem, and let  $\Omega$  be a (possibly infinity) separable extension. Then  $|\cdot|_K$  extends in a unique way to an absolute value  $|\cdot|_\Omega$  on  $\Omega$*

### Completions of global fields

Let  $A$  be a Dedekind domain with field of fractions  $K$ . For every  $0 \neq x \in K$ , the fractional ideal  $(x) = \{xa : a \in A\}$  factors uniquely as

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

where the  $v_{\mathfrak{p}}(x) \in \mathbb{Z}$  are all but finitely many equal to zero. Thus, if we fix a prime  $\mathfrak{p}$  in  $A$  we get a map  $v_{\mathfrak{p}} : K^{\times} \rightarrow \mathbb{Z}$ ,  $x \mapsto v_{\mathfrak{p}}(x)$  and it is easy to check that this is a normalized discrete valuation. The completion of  $K$  with respect to the corresponding nonarchimedean absolute value  $|\cdot|_{\mathfrak{p}}$  is denoted as  $K_{\mathfrak{p}}$ .

**Theorem 1.24** ([Ser79, II §3 Theorem 1(i)]). *Suppose  $A$  is a Dedekind domain with field of fractions  $K$  and  $B$  is the integral closure of  $A$  in finite separable extension  $L$  of  $K$ . Let  $\mathfrak{P}$  be a prime in  $B$  dividing a prime  $\mathfrak{p}$  in  $A$ , then*

$$e(\mathfrak{P}|\mathfrak{p}) = e(L_{\mathfrak{P}}/K_{\mathfrak{p}}), \quad f(\mathfrak{P}|\mathfrak{p}) = e(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

**Proposition 1.25** ([Mil, Proposition 8.2]). Let  $K$  be a field,  $|\cdot|$  an absolute value on  $K$  (archimedean or discrete nonarchimedean) and let  $L$  be a finite separable extension of  $K$ . Let  $\widehat{K}$  be the completion of  $K$  with respect to  $|\cdot|$ . Then  $|\cdot|$  has finitely many extensions  $|\cdot|_1, \dots, |\cdot|_g$  to  $L$ . If  $L_i$  denotes the completion of  $L$  with respect to the absolute value  $|\cdot|_i$ ,  $a \mapsto a_i$  denotes the inclusion of  $L$  in  $L_i$  and  $b \mapsto b$  denotes the inclusion  $\widehat{K} \hookrightarrow L_i$ , then the canonical map

$$L \otimes_K \widehat{K} \rightarrow \prod_{i=1}^g L_i$$

induced by the one taking  $a \otimes b$  to  $(a_1b, \dots, a_gb)$  is an isomorphism.

**Corollary 1.26.** For any element of  $a \in L$  we have

$$\mathrm{Nm}_{L/K}(a) = \prod \mathrm{Nm}_{L_i/\widehat{K}}(a_i), \quad \mathrm{Tr}_{L/K}(a) = \sum \mathrm{Tr}_{L_i/\widehat{K}}(a_i)$$

If  $|\cdot|$  is a discrete nonarchimedean (i.e. if  $|\cdot|$  comes from a discrete valuation defined on  $K$ ) we can work directly with the valuation rings.

**Proposition 1.27** ([Ser79, II §3 Proposition 4]). With the same set-up as in (1.25), suppose  $|\cdot|$  is discrete nonarchimedean and  $A \subset K$  is the corresponding valuation ring with completion  $\widehat{A}$  and let  $B$  the integral closure of  $A$  in  $L$ . If  $B_i$  is the valuation ring corresponding to  $|\cdot|_i$ , then the canonical map

$$B \otimes_A \widehat{A} \rightarrow \prod_{i=1}^g B_i$$

is an isomorphism.

### The primes of a number field

Let  $K$  be a number field. An equivalence class of absolute values on  $K$  is called a **prime** or a **place** of  $K$ . The following theorem describes the places of a number field.

**Theorem 1.28** (Ostrowski, [Mil, Theorem 7.14]). *Let  $K$  a number field. Let  $v$  be a place of  $K$ , then  $v$  is the equivalence class of exactly one of the following absolute values*

- (a)  $|a|_{\mathfrak{p}} := (1/\mathbb{N}\mathfrak{p})^{v_{\mathfrak{p}}(a)}$  for  $\mathfrak{p}$  is a prime ideal in  $\mathcal{O}_K$  (nonarchimedean case)
- (b)  $|a| := |\sigma(a)|$  for a real embedding  $\sigma : K \hookrightarrow \mathbb{R}$ .
- (c)  $|a| := |\sigma(a)|$  for pair of complex embeddings  $\{\sigma, \bar{\sigma}\}$ .

We say that the prime  $v$  is **finite** if it correspond to a prime ideal and **infinite** otherwise.

Let  $K \subset L$  be number fields. Given a prime  $w$  in a number field  $L$  we can restrict any absolute value in  $w$  to  $K$  to get a prime  $v$  in  $K$ , we say that the prime  $w$  **divides** or **lies over**  $v$  and write  $v \mid w$ . When  $w$  correspond to prime ideal  $\mathfrak{P}_w$ ,  $v$  correspond to the prime ideal  $\mathfrak{p}_v := \mathfrak{P}_w \cap \mathcal{O}_K$ . So this coincides with our earlier notion. And if  $w$  is an infinite prime corresponding to an embedding  $\sigma_w : L \hookrightarrow \mathbb{C}$ , then  $v$  correspond to the embedding  $\sigma_v := \sigma_w \upharpoonright_K$ .

There is also a notion of ramification for infinite primes. Given an infinite prime  $v$  in a number field  $K$ , we say that  $v$  is **ramified** in a finite extension  $L/K$  if first  $\sigma_v(K) \subset \mathbb{R}$  and there is a prime  $w \mid v$  in  $L$  such that  $\sigma_w(L) \not\subset \mathbb{R}$ .

#### 1.2.4. Different and discriminant

Let  $B \subset A$  be rings such that  $B$  is a free  $A$ -module of degree  $n$  and let  $\{\alpha_1, \dots, \alpha_n\} \subset B$  the **discriminant** of  $\{\alpha_1, \dots, \alpha_n\}$  is defined as

$$D_{B/A}(\alpha_1, \dots, \alpha_n) := \det(\mathrm{Tr}_{B/A}(\alpha_i \alpha_j))$$

If  $S \in M_n(A)$  and  $\beta_i := \sum_{j=1}^n s_{ij} \alpha_j$  then, as  $\mathrm{Tr}_{B/A}$  is  $A$ -linear, we get

$$(\mathrm{Tr}_{B/A}(\beta_i \beta_j)) = S(\mathrm{Tr}_{B/A}(\alpha_i \alpha_j)) S^t$$

hence

$$D_{B/A}(\beta_1, \dots, \beta_n) = \det(S)^2 D_{B/A}(\alpha_1, \dots, \alpha_n)$$

In particular, if  $\{\alpha_i\}$  and  $\{\beta_i\}$  are  $A$ -bases of  $B$ , then their discriminant lie in the same class of  $A/A^{\times 2}$  (quotient of multiplicative monoids). The **discriminant of  $B$  over  $A$**  denoted  $\mathrm{disc}(B/A)$  is the image in  $A/A^{\times 2}$  of the discriminant of any  $A$ -basis of  $B$ . Note that every element  $d \in A$  such that  $dA^{\times 2} = \mathrm{disc}(B/A)$  generates the same ideal in  $A$ .

If  $A = \mathbb{Z}$  (resp.  $\mathbb{Z}_p$ ),  $K$  is number field (resp. a finite extension of  $\mathbb{Q}_p$ ) and  $B = \mathcal{O}_K$ . We define the **absolute discriminant** of  $K$  or simply discriminant of  $K$  as

$$\text{disc}(K) := \text{disc}(B/A) \in A/A^{\times 2}$$

and denote  $\mathfrak{d}_K$  the ideal in  $A$  generated by  $\text{disc}(K)$ . Remark that, since  $\mathbb{Z}^{\times 2} = \{\pm 1\}^2 = \{1\}$ ,  $\text{disc}(K)$  is a well defined integer in the number field case.

Now suppose  $A$  is a Dedekind domain with field of fractions  $K$  and  $B$  is the integral closure of  $A$  in finite separable extension  $L$  of  $K$ . Let  $n := [L : K]$ , then the **relative discriminant** of  $L$  over  $K$  denoted  $\mathfrak{d}_{L/K}$  is the ideal in  $A$  generated by the set

$$\{D_{L/K}(\alpha_1, \dots, \alpha_n) : \{\alpha_i\} \text{ is a } K\text{-basis of } L \text{ contained in } B\}$$

If  $A$  is a principal ideal domain so that  $B$  is free over  $A$  of rank  $n$  (by 1.12), then  $\mathfrak{d}_{L/K}$  is the ideal in  $A$  generated by  $\text{disc}(B/A)$ . In particular, if  $A = \mathbb{Z}$  ( resp.  $\mathbb{Z}_p$ ) the relative discriminant of a number field (resp. a finite extension of  $\mathbb{Q}_p$ )  $K$  over  $\mathbb{Q}$  (resp.  $\mathbb{Q}_p$ ) agrees with our definition of absolute discriminant of  $K$ .

Here are some of the properties of the discriminant

**Proposition 1.29** ([Mil, Proposition 2.40]). Let  $K$  be a number field, then

- (i) If  $s$  is the number pairs of complex embeddings, then the sign of  $\text{disc}(K)$  is  $(-1)^s$ .
- (ii) (Stickelberger's criterion)  $\text{disc}(K) \equiv 0, 1 \pmod{4}$

As a consequence of (1.27) we have

**Proposition 1.30.** Let  $K$  be a number field and  $p$  a rational prime, then

$$\text{disc}(K) \equiv \prod_{\mathfrak{p}|p} \text{disc}(K_{\mathfrak{p}}) \pmod{\mathbb{Z}_p^{\times 2}}$$

### The different ideal

Suppose  $A$  is a Dedekind domain with field of fractions  $K$  and  $B$  is the integral closure of  $A$  in finite separable extension  $L$  of  $K$ . Consider the  $B$ -submodule of  $L$

$$\{x \in L : \text{Tr}_{L/K}(xB) \subset A\}$$

is called **the codifferent of  $L$  over  $K$** . It is easy to see that this is in fact fractional ideal containing  $B$ , hence its inverse denoted  $\mathcal{D}_{L/K}$  is an integral ideal in  $B$  which is known as the **different ideal**. The key relation between the different and the discriminant is the following, see [Ser79, III §3].

**Proposition 1.31.**  $\mathfrak{d}_{L/K} = \mathcal{N}_{L/K}(\mathcal{D}_{L/K})$

Other properties of the different and discriminant that will be useful later are

**Proposition 1.32** (Transitivity). Let  $M/L$  be a finite separable extension, then

- (i)  $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$
- (ii)  $\mathfrak{d}_{M/K} = \mathcal{N}_{L/K}(\mathfrak{d}_{M/L})\mathfrak{d}_{L/K}^{[M:L]}$

**Theorem 1.33** (Ramification). Let  $\mathfrak{P}$  be a prime ideal in  $L$ . The prime  $\mathfrak{P}$  is unramified over  $K$  if and only if  $\mathfrak{P}$  does not divide the different  $\mathcal{D}_{L/K}$ .

**Corollary 1.34.** Let  $\mathfrak{p}$  be a prime in  $A$ , then  $\mathfrak{p}$  ramifies in  $L$  if and only if  $\mathfrak{p}$  divides  $\mathfrak{d}_{L/K}$ .

*Proof.* This follows from (1.33) and the fact that  $\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$ .  $\square$

The following theorem due to Dedekind gives us a sharper version of (1.33).

**Proposition 1.35** ([Ser79, III §6 Proposition 13]). Let  $\mathfrak{P}$  be a prime ideal in  $K$ ,  $\mathfrak{p} = \mathfrak{P} \cap A$ ,  $p = \text{char}(A/\mathfrak{p})$  and  $e := e(\mathfrak{P}|\mathfrak{p})$ , then

- (i) If  $p \nmid e$ , we have  $v_{\mathfrak{P}}(\mathcal{D}_{L/K}) = e - 1$
- (ii) If  $p \mid e$ , then  $e \leq v_{\mathfrak{P}}(\mathcal{D}_{L/K}) \leq e - 1 + ev_p(e)$

We say that the extension  $L/K$  is **tamely ramified at** a prime  $\mathfrak{p}$  in  $K$  if  $p \nmid e(\mathfrak{P}|\mathfrak{p})$  for all primes  $\mathfrak{P}$  lying over  $\mathfrak{p}$ , where  $p := \text{char}(A/\mathfrak{p})$ . The extension  $L/K$  is said to be **wildly ramified at**  $\mathfrak{p}$  if it is not tamely ramified at  $\mathfrak{p}$ . On taking norms we get by (1.31) the following useful fact

**Corollary 1.36.** If  $\mathfrak{p}$  is a prime in  $A$ , then

$$\sum_{\mathfrak{P}} (e(\mathfrak{P}|\mathfrak{p}) - 1) f(\mathfrak{P}|\mathfrak{p}) \leq v_{\mathfrak{p}}(\mathfrak{d}_{L/K})$$

where the sum is over all primes  $\mathfrak{P}$  in  $L$  dividing  $\mathfrak{p}$  and the equality holds if and only if  $L/K$  is tame at  $\mathfrak{p}$ .

Tame ramification behaves well when taking compositum, more specifically, we have the following analogs of (1.16) and (1.17)

**Proposition 1.37.** Let  $L_1/K$  and  $L_2/K$  extensions of number fields, then a prime  $\mathfrak{p}$  is tamely ramified in  $L_1L_2$  if and only if  $\mathfrak{p}$  is tamely ramified in both  $L_1$  and  $L_2$ .

*Proof.* By (1.24) it is enough to prove it in the local case. For a proof of this see [Nar13, Corollary 2, pag. 229]  $\square$

**Corollary 1.38.** Let  $\tilde{L}$  be the Galois closure of a number field extension  $L/K$ , then a prime  $\mathfrak{p}$  is tamely ramified in  $L$  if and only if  $\mathfrak{p}$  is tamely ramified in  $\tilde{L}$ .

*Proof.* The Galois closure  $\tilde{L}$  is the compositum of the conjugates of  $L$  over  $K$  all of which are tame at  $\mathfrak{p}$  if and only if  $L$  is.  $\square$

### 1.3. Some results from permutation group theory

Let  $\Omega$  be a nonempty set. The set  $\text{Sym}(\Omega)$  all of bijections of  $\Omega$  forms a group under composition; a **permutation group** is simply a subgroup of  $\text{Sym}(\Omega)$ . By Cayley's theorem every group is isomorphic to a permutation group on some set, however, seeing the group as a group of permutations allows a more combinatorial approach. In this section we state some result of this theory that will be useful in Chapter 3. Our main reference for this section will be [DM96].

Let  $G$  be a group acting on a nonempty set  $\Omega$ . Given  $\Delta \subset \Omega$  we define the **pointwise-stabilizer** of  $\Delta$  in  $G$  as

$$G_{(\Delta)} := \{g \in G : g \cdot x = x, \text{ for all } x \in \Delta\}$$

and the **setwise-stabilizer** as

$$G_{\{\Delta\}} := \{g \in G : g \cdot \Delta = \Delta\}$$

where  $g \cdot \Delta = \{g \cdot x : x \in \Delta\}$ . Suppose that  $G$  acts transitively on  $\Omega$ , we say that a nonempty subset  $\Delta$  of  $\Omega$  is a **block** if for all  $g \in G$  either  $g \cdot \Delta = \Delta$  or  $(g \cdot \Delta) \cap \Delta = \emptyset$ , or equivalently, if for every  $x, y \in \Delta$  and  $g \in G$  we have  $g \cdot x \in \Delta \iff g \cdot y \in \Delta$ . The importance of the notion of block is reflected in the following correspondence theorem

**Theorem 1.39** ([DM96, Theorem 1.5A]). *Let  $G$  be a group which acts transitively on a set  $\Omega$  and let  $\alpha \in \Omega$ . There is an order-preserving correspondence between subgroups  $H$  of  $G$  containing  $G_\alpha$  (the stabilizer of  $\alpha$  in  $G$ ) and the set of all blocks  $\Delta$  with  $\alpha \in \Delta$ . Given by  $H \mapsto \{h \cdot \alpha : h \in H\}$  and  $\Delta \mapsto G_{\{\Delta\}}$ .*

**Corollary 1.40.** Let  $n \geq 2$ . The group  $\{\sigma \in S_n : \sigma(1) = 1\}$  is maximal in  $S_n$ .

*Proof.* Take  $G = S_n$  with its natural action on  $\Omega = \{1, \dots, n\}$ . This action is transitive and if  $1 \in \Delta \subsetneq \Omega$  is a block, then  $\Delta = \{1\}$ , otherwise, there would exist  $1 \neq j \in \Delta$  and if we take  $i \notin \Delta$ , then  $\sigma := (ij)$  is such that  $\sigma(1) = 1 \in \Delta$  but  $\sigma(i) = j \notin \Delta$ , contradicting that  $\Delta$  is a block. Hence by (1.39) the stabilizer  $G_1 := \{\sigma \in S_n : \sigma(1) = 1\}$  is maximal.  $\square$

#### Automorphisms of $S_n$

Recall that an automorphism  $\varphi$  of a group  $G$  is said to be *inner* if there exists  $g \in G$  such that  $\varphi(x) = gxg^{-1}$  for all  $x \in G$ . The set of inner automorphism  $\text{Inn}(G)$  form a normal subgroup of  $\text{Aut}(G)$  and the quotient  $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$  is known as the group of outer automorphism. The following theorem is a well-known result first proved by Otto Hölder in 1895, see [Mil58].

**Theorem 1.41** (Hölder, [Höl95]). *The group  $\text{Out}(S_n)$  is not trivial if and only if  $n = 6$ . Hence*

$$\text{Aut}(S_n) = \text{Inn}(S_n)$$

whenever  $n \neq 6$ .

**Corollary 1.42.** Let  $n \neq 6$  be an integer, then every subgroup of index  $n$  in  $S_n$  is the stabilizer of a point. In particular, every two subgroups of index  $n$  in  $S_n$  are conjugated.

*Proof.* Let  $H$  be the a subgroup of index  $n$  in  $S_n$  and let  $\Omega := G/H$  be the set of right cosets, the action by right multiplication defines a homomorphism

$$\varphi : S_n \rightarrow \text{Sym}(\Omega), \sigma \mapsto (\tau H \mapsto \sigma \tau H)$$

Since  $\ker(\varphi)$  is normal and is contained in  $H$  then,  $\ker(\varphi) = 1$ . This is because the only normal, proper and non trivial subgroups of  $S_n$  are  $V_4$  and  $A_4$  if  $n = 4$ , and  $A_n$  if  $n \neq 2, 4$ , but none of this has a size dividing  $|H| = (n - 1)!$ . Hence  $\varphi$  is injective and, as  $|\text{Sym}(\Omega)| = n$ , we conclude that  $\varphi$  is an isomorphism. Now if  $\Omega = \{\tau_1 H, \dots, \tau_n H\}$  with  $\tau_1 = 1$ , then the map

$$\psi : S_n \rightarrow \text{Sym}(\Omega), \sigma \mapsto (\tau_i H \mapsto \tau_{\sigma(i)} H)$$

is also an isomorphism. It follows from Hölder's theorem (1.41) that there is  $\rho \in S_n$  such that

$$(\psi^{-1}\varphi)(\sigma) = \rho\sigma\rho^{-1}, \text{ for all } \sigma \in S_n$$

thus

$$(\rho\sigma\rho^{-1})(1) = 1 \iff (\psi^{-1}\varphi)(\sigma)(1) = 1 \iff (\varphi(\sigma))(\tau_1 H) = \tau_1 H \iff \sigma H = H \iff \sigma \in H$$

and therefore  $H$  is the stabilizer of  $\rho^{-1}(1)$ . □

Complementing this corollary for  $n = 6$  we have the following

**Proposition 1.43.** There are exactly two conjugacy classes  $\Delta_1$  and  $\Delta_2$  of subgroups of index 6 in  $S_6$ . Moreover, every pair of representatives  $H_1 \in \Delta_1$  and  $H_2 \in \Delta_2$  satisfy

$$36 = [S_6 : H_1 \cap H_2] = [S_6 : H_1][S_6 : H_2] = 6 \cdot 6$$

*Proof.* See [Sch94, Lemma 7.8.6]. □

## 2 The quadratic $\mathbb{Z}$ -modules associated to a number field

Throughout this chapter  $K$  denotes a number field of degree  $n = [K : \mathbb{Q}]$ .

### 2.1. Definition and some properties

#### 2.1.1. Definitions

Let  $A \subset B$  be rings such that  $A$  is an integral domain and  $B$  is free of finite rank over  $A$ . The ring  $B$ , view as a  $A$ -module, can be naturally endowed with a structure of  $A$ -quadratic module  $(B, \text{tr}_{B/A})$  by taking the trace pairing

$$\text{tr}_{B/A} : B \times B \rightarrow A, (x, y) \mapsto \text{tr}_{B/A}(x, y) := \text{Tr}_{A/B}(xy)$$

as bilinear form.

Let  $A_1 \subset A$  be a ring and  $M \subset B$  a free  $A_1$ -submodule of  $B$  of finite rank, then restricting  $\text{tr}_{B/A}$  to  $M$  gives us an  $A_1$ -quadratic module structure on  $M$  which, to simplify notation, we will denote  $(M, \text{tr}_{B/A})$  instead of  $(M, \text{tr}_{B/A}|_{M \times M})$ , when there is no place for confusion.

For a finite extension of fields  $F_2/F_1$  the  $F_1$ -quadratic module  $(F_2, \text{tr}_{F_2/F_1})$  is nondegenerate if and only if the extension is separable [Mil, Remark 2.28]. In particular,  $(K, \text{tr}_{K/\mathbb{Q}})$  is nondegenerate for any number field  $K$ .

Since, by (1.12),  $\mathcal{O}_K$  is a free  $\mathbb{Z}$ -module of rank  $n$ , the pair  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  is a quadratic  $\mathbb{Z}$ -module of dimension  $n$  which we call the **integral trace quadratic module associated to  $K$** . In  $\mathcal{O}_K$  we have a distinguished  $\mathbb{Z}$ -module given by the elements orthogonal to 1

$$\mathcal{O}_K^0 := \{x \in \mathcal{O}_K : \text{Tr}_{K/\mathbb{Q}}(x) = 0\} = \mathcal{O}_K \cap K^0$$

where  $K^0 := \{x \in K : \text{Tr}_{K/\mathbb{Q}}(x) = 0\}$ . It is free of rank  $n - 1$  (being the kernel of  $\text{Tr}_{K/\mathbb{Q}} : \mathcal{O}_K \rightarrow \mathbb{Z}$ ), thus  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$  is a quadratic  $\mathbb{Z}$ -module of dimension  $n - 1$  which we call the **trace-zero quadratic module associated to  $K$** . The main feature of  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$

is that it allows us to lower the dimension without “loosing too much information”.

A third quadratic invariant, with a more geometric interpretation, that has been studied by several authors is the shape of  $K$ . It can be defined as follows: Endow  $K$  with the real-valued  $\mathbb{Q}$ -bilinear form  $b_K$  whose associated quadratic form is given by

$$b_K(x, x) := \sum_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(x)|^2$$

(note that when  $K$  is totally real  $b_K$  is just  $\text{tr}_{K/\mathbb{Q}}$ ). The orthogonal complement of 1 in  $(K, b_K)$  is still  $K^0$ . Now, project  $K$  onto  $K^0$  by the map  $\alpha \mapsto \alpha_{\perp} := n\alpha - \text{Tr}_{K/\mathbb{Q}}(\alpha)$  the **shape** of  $K$ , denoted  $\text{Sh}(K)$ , is defined as the isometry equivalence class of  $(\mathcal{O}_K^{\perp}, b_K)$  up to scalar multiplication, where  $\mathcal{O}_K^{\perp}$  is the image of  $\mathcal{O}_K$  under this map, i.e.,

$$\mathcal{O}_K^{\perp} := \{\alpha_{\perp} : \alpha \in \mathcal{O}_K\} = \{x \in \mathbb{Z} + n\mathcal{O}_K : \text{Tr}_{K/\mathbb{Q}}(x) = 0\}$$

Thus  $\text{Sh}(K) = \text{Sh}(L)$  if and only if  $(\mathcal{O}_K^{\perp}, b_K) \cong (\mathcal{O}_L^{\perp}, \lambda b_L)$  for some  $\lambda \in \mathbb{R}^{\times}$ .

Equivalently, the shape invariant  $\text{Sh}(K)$  can be defined as the  $(n-1)$ -dimensional lattice in  $\mathbb{R}^n$  given by the image of  $\mathcal{O}_K^{\perp}$  under the Minkowski map

$$j_K : K \hookrightarrow \mathbb{R}^n, \alpha \mapsto \left( \sigma_1(\alpha), \dots, \sigma_r(\alpha), \sqrt{2}\Re(\tau_1(\alpha)), \sqrt{2}\Im(\tau_1(\alpha)), \dots, \sqrt{2}\Im(\tau_s(\alpha)) \right)$$

where  $\sigma_1, \dots, \sigma_r, \tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$  are the embeddings of  $K$  in  $\mathbb{C}$ , up to reflection, rotations and scaling by  $\mathbb{R}^{\times}$ . The  $\sqrt{2}$  factor in the complex embeddings ensures that  $j_K : (K, b_K) \hookrightarrow (\mathbb{R}^n, \langle \cdot, \cdot \rangle)$  is an isometry in its image (where  $\langle \cdot, \cdot \rangle$  is the usual euclidean product of  $\mathbb{R}^n$ ) and that the lattice  $j_K(\mathcal{O}_K)$  has co-volume  $|\text{disc}(K)|^{1/2}$  in  $\mathbb{R}^n$ .

Hence  $\text{Sh}(K)$  correspond to an element of the double quotient

$$\mathcal{S}_{n-1} := \text{GL}_{n-1}(\mathbb{Z}) / \text{GL}_{n-1}(\mathbb{R}) \backslash \text{GO}_{n-1}(\mathbb{R})$$

called the **space of shapes** (the left quotient modules the change of  $\mathbb{Z}$ -basis of the lattice and the right modules the geometric transformations that preserve “shapes”, the orthogonal similitudes). This space and the distribution of the shapes of number fields in it have been the subject of a lot of interesting current research see [BH16, Har17, MSM16].

Remark that for every  $\mathbb{Z}$ -basis of  $\mathcal{O}_K$  of the form<sup>1</sup>  $\{1, \alpha_2, \dots, \alpha_n\}$  we have that  $\{\alpha_{2\perp}, \dots, \alpha_{n\perp}\}$  is a  $\mathbb{Z}$ -basis of  $\mathcal{O}_K^\perp$ .

**Example 2.1.** Let  $K$  be a quadratic field, i.e., such that  $n = 2$ . Since  $n - 1 = 1$ , the shape of  $K$  is the unique 1-dimensional lattice up to scalar multiplication, namely  $\mathbb{Z}$ . More formally, the space of shapes  $\mathcal{S}_1$  consists of a single point, the class of 1.

**Example 2.2.** Let  $K = \mathbb{Q}(\alpha)$ , where  $\alpha$  is a root of  $x^3 - x^2 + 2x + 1$ . The field  $K$  has discriminant  $7^2$ , thus is a cyclic cubic field, i.e.,  $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ , in particular  $K$  is totally real. The set  $\{1, \alpha, \alpha^2\}$  is an integral basis of  $K$  and  $\text{Tr}_{K/\mathbb{Q}}(\alpha) = 1$ ,  $\text{Tr}_{K/\mathbb{Q}}(\alpha^2) = 5$ . Thus  $\{3\alpha - 1, 3\alpha^2 - 5\}$  is a  $\mathbb{Z}$ -basis of  $\mathcal{O}_K^\perp$ . The Gram matrix of  $\text{tr}_{K/\mathbb{Q}} = b_K$  in this basis is

$$3 \cdot 7 \cdot \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Therefore  $(\mathcal{O}_K^\perp, \frac{1}{42}b_K)$  is isometric to the lattice  $L = \mathbb{Z}v_1 + \mathbb{Z}v_2$ , where  $v_1 = (1, 0)$  and  $v_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ . The lattice  $L$  has the property that the set of lattice points that are closest to the origin form an hexagon, hence  $L$  is called the *hexagonal lattice*. It is denoted as  $\mathbb{A}_2$ .

As an element of  $\mathcal{S}_2$ , we have

$$\text{Sh}(K) = \text{GL}_2(\mathbb{Z}) \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix} \text{GO}_2(\mathbb{R}),$$

i.e., the field  $K$  has hexagonal shape. In fact, this is true for every cyclic cubic field. This was first proved by David C. Terr in [Ter97] and in [MSM16] Mantilla-Soler and Marina Monsurrò gave generalizations of this theorem to every  $\mathbb{Z}/l\mathbb{Z}$ -field with  $l$  odd prime.

---

<sup>1</sup>The basis can always be taken in this form. Indeed, take an arbitrary basis  $\{\alpha'_1, \dots, \alpha'_n\}$  of  $\mathcal{O}_K$  and write  $1 = \sum_j m_j \alpha'_j$  for some integers  $\{m_j\}$ , note that these integer are coprime, thus they are the first row of some matrix  $M = (m_{ij})$  in  $\text{GL}_n(\mathbb{Z})$  and the basis  $\alpha_i := \sum_j m_{ij} \alpha'_j$  begins with 1.

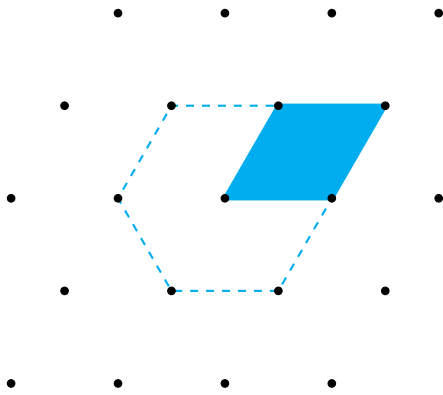
Here are some visual examples of shapes:



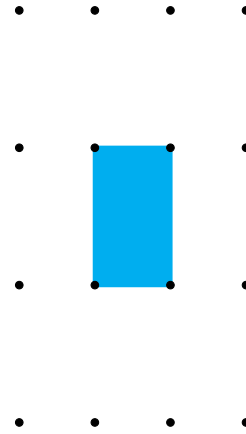
(a) Shape of  $\mathbb{Q}$ .



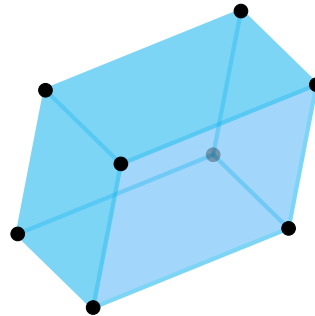
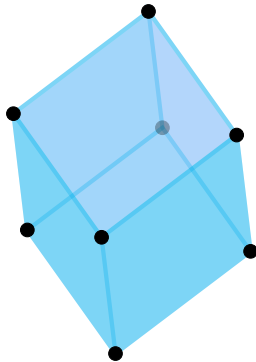
(b) Shape of every quadratic field  $\mathbb{Q}(\sqrt{d})$ .



(c) Shape of every cyclic cubic field. This is the  $A_2$ -hexagonal lattice.



(d) Shape of  $\mathbb{Q}(\sqrt[3]{6})$ .



(e) Fundamental parallelepipeds of LLL-reduced basis<sup>a</sup> for shapes of two different totally real quartic fields with the same fundamental discriminant  $d = 3557$ .

<sup>a</sup> See [Coh13, §2 Section 2.6] for the definition

**Figure 2-1:** Shapes of some number fields

In [Har17] R. Harron showed that every cubic field of the form  $\mathbb{Q}(m^{1/3})$ , where  $m = ab^2$  with  $a$  and  $b$  coprime, square free and positive, such that 3 is wildly ramified has a rectangular shape with sides of ratio  $(a/b)^{1/3}$ . Example (d) is a particular case with  $a = 6$ ,  $b = 1$ . The example (e) corresponds to the quartic fields whose defining polynomials are  $x^4 - x^3 - 8x^2 - 3x + 4$  and  $x^4 - 2x^3 - 9x^2 + 5x + 16$  it was computed using the commands `MinkowskiLattice(R)` and `LLL(Lattice(X))` in `Magma`. By Theorem 6, the fact that we can “see” that they have different shapes implies that they are not isomorphic.

### 2.1.2. Discriminants

Recall that by definition  $\text{disc}(K) = \text{disc}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  (which is precisely the reason why  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  is thought as refinement of  $\text{disc}(K)$ ). The discriminants  $\text{disc}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$  and  $\text{disc}(\mathcal{O}_K^\perp, b_K)$  are also related to  $\text{disc}(K)$ , the former was computed in [MS10, Lemma 2.3] and we state this computation as:

**Lemma 2.3** (Mantilla-Soler, [MS10]). Let  $k$  be the positive integer such that  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = k\mathbb{Z}$ , then  $[\mathcal{O}_K : \mathbb{Z} \perp \mathcal{O}_K^0] = n/k$  and  $\text{disc}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) = \frac{n}{k^2} \text{disc}(K)$ .

*Proof.* Consider the surjective map  $\text{Tr}_{K/\mathbb{Q}} : \mathcal{O}_K \rightarrow k\mathbb{Z}$ . The set  $\mathbb{Z} \perp \mathcal{O}_K^0$  is a submodule of  $\mathcal{O}_K$  containing the kernel of  $\text{Tr}_{K/\mathbb{Q}}$  and whose image by  $\text{Tr}_{K/\mathbb{Q}}$  is  $n\mathbb{Z}$ . Thus  $\text{Tr}_{K/\mathbb{Q}}$  induces an isomorphism

$$\mathcal{O}_K / \mathbb{Z} \perp \mathcal{O}_K^0 \cong k\mathbb{Z} / n\mathbb{Z},$$

it follows that  $\mathbb{Z} \perp \mathcal{O}_K^0$  has index  $n/k$  in  $\mathcal{O}_K$ . Therefore by (1.4)

$$\text{disc}(\mathbb{Z} \perp \mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) = (n/k)^2 \text{disc}(K)$$

as  $\text{disc}(\mathbb{Z} \perp \mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) = \text{disc}(1 \cdot \mathbb{Z}, \text{tr}_{K/\mathbb{Q}}) \text{disc}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) = n \text{disc}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$ , this proves that  $\text{disc}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) = \frac{n}{k^2} \text{disc}(K)$ . □

To compute  $\text{disc}(\mathcal{O}_K^\perp, b_K)$  just note that  $\mathbb{Z} \perp \mathcal{O}_K^\perp$  has index  $n^{n-1}$  in  $\mathcal{O}_K$ , so by (1.4)

$$\text{disc}(\mathbb{Z} \perp \mathcal{O}_K^\perp, b_K) = n^{2(n-1)} \text{disc}(\mathcal{O}_K, b_K) = n^{2(n-1)} |\text{disc}(K)|$$

and  $\text{disc}(\mathcal{O}_K^\perp, b_K) = n^{2n-3} |\text{disc}(K)|$ . It also follows that  $\text{disc}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) = n^{2n-3} \text{disc}(K)$ .

### 2.1.3. Localization

The “local-global” Hasse principle tells us that to solve a global problem it is often very useful to consider its local analog first. Since for a place  $v$  in  $\mathbb{Q}$  Proposition 1.25 gives a decomposition of the underlying vector space in the localization at  $v$  of  $(K, \text{tr}_{K/\mathbb{Q}})$  in terms of local (simpler) fields, one expects that such decomposition would be useful to give a local

description of  $(K, \text{tr}_{K/\mathbb{Q}})$ . A key observation made by D. Maurer in [Mau73] is that a similar decomposition carries over to  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  too, this idea materializes as:

**Proposition 2.4.** (Maurer, [Mau73]) Let  $v$  be a place in  $\mathbb{Q}$ , let  $\{w_i\}$  be the places in  $K$  extending  $v$ , for each  $i$  fix a completion  $K_i$  of  $K$  with respect to  $w_i$ , endow each  $K_i$  with their respective trace forms  $\text{tr}_{K_i/\mathbb{Q}_v}$  and endow  $K_v := K \otimes \mathbb{Q}_v$  with its trace form  $\text{tr}_{K_v/\mathbb{Q}_v}$ . Then

(i) The isomorphism of  $\mathbb{Q}_v$ -algebras

$$f_K : K \otimes \mathbb{Q}_v \xrightarrow{\sim} \prod_i K_i$$

induced by  $a \otimes b \mapsto (a_1b, \dots, a_nb, \dots)$  (where  $a \mapsto a_i$  and  $b \mapsto b$  are the inclusions  $K \hookrightarrow K_i$  and  $\mathbb{Q}_v \hookrightarrow K_i$ ) is also an isometry of quadratic  $\mathbb{Q}_v$ -spaces.

(ii) Suppose  $v = p$  is a finite prime. Let  $(\mathcal{O}_K)_p$  be the  $\mathbb{Z}_p$ -span of  $\{\alpha_1 \otimes 1, \dots, \alpha_n \otimes 1\}$  in  $K \otimes \mathbb{Q}_p$  where  $\{\alpha_1, \dots, \alpha_n\}$  is an integral basis of  $K$ , then  $f_K((\mathcal{O}_K)_p) = \prod_i \mathcal{O}_{K_i}$  and thus  $f_K$  restricts to an isometry of quadratic  $\mathbb{Z}_p$ -spaces

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong (\mathcal{O}_K)_p \xrightarrow{\sim} \prod_i \mathcal{O}_{K_i}$$

*Proof.* The statement (i) is just a reformulation of Proposition 1.25 and Corollary 1.26. To prove (ii) observe that  $f_K((\mathcal{O}_K)_p) \subset \prod_i \mathcal{O}_{K_i}$ , but since both sides have the same discriminant  $\text{disc}(K)$  (because  $\text{disc}(K)$  is the product of the local discriminants, see Proposition 1.30), then the equality must hold by (1.4).  $\square$

This orthogonal decomposition was exploited in [BMP] to compute the genus of  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  (i.e. to compute the Jordan decomposition of  $(\mathcal{O}_K \otimes \mathbb{Z}_v, \text{tr}_{K/\mathbb{Q}} \otimes \mathbb{Z}_v)$  for all primes  $v$ ) for tamely ramified extension  $K/\mathbb{Q}$ . Although, in Chapter 4 we will use some of the ideas involved in their proof, we will not go into the details of the statement here, for we will not need the full power of their result. For an excellent treatment of this theorem and its proof see [MS].

As a consequence of Proposition 2.4, Maurer also deduced the following lemma<sup>2</sup> which combines quite well with Lemma 2.3.

**Lemma 2.5.** (Maurer, [Mau73]). Let  $k$  be an integer such that  $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = k\mathbb{Z}$ , then a prime  $p$  divides  $k$  if and only if  $p \mid e(\mathfrak{p}|p)$  for all primes  $\mathfrak{p}$  in  $K$  lying over  $p$ .

*Proof.* We will give an alternative proof to that presented in [Mau73]. In fact, it is not hard to see that the following slightly more general statement holds: Let  $\mathcal{D}_{K/\mathbb{Q}}$  denote the different ideal of  $K/\mathbb{Q}$ , then for a rational prime  $p$  we have

$$v_p(k) = \min_{\mathfrak{p}|p} \left\lfloor \frac{v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}})}{e(\mathfrak{p}|p)} \right\rfloor$$

and the lemma will follow from the fact  $v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}}) \geq e(\mathfrak{p}|p) \iff p \mid e(\mathfrak{p}|p)$  (1.35). To prove the statement observe that, for any  $r \in \mathbb{Z}^+ \cup \{0\}$ ,

$$\begin{aligned} p^r \mid k &\iff \mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subset p^r \mathbb{Z} \\ &\iff \mathrm{Tr}_{K/\mathbb{Q}}(p^{-r} \mathcal{O}_K) \subset \mathbb{Z} \\ &\iff p^{-r} \in \mathcal{D}_{K/\mathbb{Q}}^{-1} \\ &\iff \mathcal{D}_{K/\mathbb{Q}} \subset (p^r) \\ &\iff rv_{\mathfrak{p}}(p) \leq v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}}), \text{ for all } \mathfrak{p} \text{ prime in } K \\ &\iff re(\mathfrak{p}|p) \leq v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}}), \text{ for all } \mathfrak{p} \text{ dividing } p \\ &\iff r \leq \left\lfloor \frac{v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}})}{e(\mathfrak{p}|p)} \right\rfloor, \text{ for all } \mathfrak{p} \text{ dividing } p \\ &\iff r \leq \min_{\mathfrak{p}|p} \left\lfloor \frac{v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}})}{e(\mathfrak{p}|p)} \right\rfloor \end{aligned}$$

and we are done, since  $v_p(k)$  is the largest of such  $r$ . □

**Corollary 2.6.** Suppose any of the following conditions holds:

- (i) Every  $p \mid n$  satisfies  $p^n \nmid \mathrm{disc}(K)$ .
- (ii) The extension  $K/\mathbb{Q}$  is tamely ramified at  $p$ , for every  $p \mid n$ .
- (iii) The field  $K$  has fundamental discriminant and  $n > 2$ .

Then,  $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$ . Moreover, if  $n = 4$  condition (i) is equivalent to  $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  and if  $n$  is a prime conditions (i) and (ii) are equivalent to  $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$ .

<sup>2</sup>In [Mau73] the lemma is stated for local fields too, but we stated it like this because it suits our purposes.

*Proof.* Let  $k \in \mathbb{Z}^+$  be such that  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = k\mathbb{Z}$ , then:

- If (i) holds, by definition of discriminant as determinant of a Gram matrix of  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$ , we know that  $k^n \mid \text{disc}(K)$ , as  $k \mid n$ , any  $p$  prime dividing  $k$  would satisfy  $p^n \mid \text{disc}(K)$  and  $p \mid n$ , thus no such prime exists and  $k = 1$ .
- If (ii) holds and  $p$  is prime dividing  $k \mid n$ , then  $p \nmid e(\mathfrak{p}|p)$  for every prime  $\mathfrak{p}$  lying over  $p$ , contradicting Lemma 2.5. Therefore  $k = 1$ .
- If (iii) holds, the extension  $K/\mathbb{Q}$  is tame at every odd prime, hence  $p \nmid k$  for all  $p \neq 2$ . Suppose  $2 \mid k$  and let  $f_1^{e_1} f_2^{e_2} \cdots$  be factorization type of 2 in  $K$ , then  $2 \mid e_i$  for all  $i$ , and

$$3 \geq v_2(\text{disc}(K)) \geq e_1 f_1 + e_2 f_2 + \cdots = n > 2$$

yields  $n = 3 = e_1 f_1 + e_2 f_2 + \cdots \equiv 0 \pmod{2}$ , a contradiction. Thus  $k = 1$ .

To prove the reciprocals, suppose  $k = 1$  and  $n = p$  is prime. Let  $f_1^{e_1} \cdots f_g^{e_g}$  be factorization type of  $p$  in  $K$ , if condition (ii) did not hold, there would be an index  $i$  such that  $p \mid e_i$  and we may assume  $i = 1$  but then  $p = e_1 f_1 + \cdots \geq p$  implies that there is only one prime  $\mathfrak{p}$  in  $K$  lying over  $p$  and for that prime  $p \mid e(\mathfrak{p}|p) = e_1$ , contradicting (2.5). Since condition (ii) always implies condition (i), this proves  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z} \iff (ii) \iff (i)$ , in this case.

Similarly, if  $k = 1$ ,  $n = 4$  and condition (i) did not hold, then  $2^4 \mid \text{disc}(K)$ , in particular 2 would be wildly ramified in  $K$ , so its factorization type would be  $1^2 2$ ,  $1^2 1 1$ ,  $1^2 1^2$  or  $2^2$ , as  $k = 1$ , only the first two cases are possible, however, for a prime  $\mathfrak{p}$  in  $K$  the exact power of  $\mathfrak{p}$  dividing the different ideal  $\mathcal{D}_{K/\mathbb{Q}}$  is bounded by  $e \cdot (v_p(e) + 1) - 1$ , where  $e = e(\mathfrak{p}|p)$  and  $p = \mathfrak{p} \cap \mathbb{Z}$  (see (1.35)(ii)), thus in either case if  $\mathfrak{p}$  is the prime in  $K$  with  $e(\mathfrak{p}|2) = 2$  we would have  $\mathcal{D}_{K/\mathbb{Q}} = \mathfrak{p}^v \mathfrak{a}$ , where  $(\mathfrak{a}, 2) = 1$  and  $v \leq 3$ , but this yields  $4 \leq v_2(\text{disc}(K)) = v_2(\mathcal{N}(\mathcal{D}_{K/\mathbb{Q}})) = v \cdot f(\mathfrak{p} | 2) = v \leq 3$ , a contradiction.  $\square$

**Example 2.7.** Let  $K$  be the sextic field with defining polynomial  $x^6 - 2x^5 + 2x^4 + 2x + 1$ , then  $\text{disc}(K) = -2^6 \cdot 3^3 \cdot 31$ , so condition (i) does not hold and yet  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$ . This shows that  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  is weaker than (i) if  $n$  is not 4 or a prime.

**Example 2.8.** For any quartic field  $K$  such that  $\text{disc}(K)$  is fundamental and even, we have that 2 is wildly ramified in  $K$  and yet  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$ . Thus (i) is weaker than (ii) if  $n$  is not prime. This is true for example for the quartic field with defining polynomial  $x^4 - x^3 - 5x^2 + 4x + 2$  and discriminant  $2^2 \cdot 19 \cdot 149$ .

### 2.1.4. Signature

It turns out that the signature of the  $\mathbb{Q}$ -quadratic space  $(K, \text{tr}_{K/\mathbb{Q}})$ , and thus the signature of  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$ , it is completely determined by the signature of  $K$ , this is the content of the following theorem due to Taussky.

**Theorem 2.9.** (Taussky, [Tau68]). Suppose  $K$  has  $r$  real and  $s$  complex pairs of embeddings then the signature of  $(K, \text{tr}_{K/\mathbb{Q}})$  is equal to  $(r + s, s)$ .

*Proof.* By (2.4) there is an orthogonal decomposition

$$(K \otimes \mathbb{R}, \text{tr}_{K/\mathbb{Q}} \otimes \mathbb{R}) \cong \bigoplus_i (K_i, \text{tr}_{K_i/\mathbb{R}})$$

where  $\{K_i\}$  are the  $r + s$  completions of  $K$  at the primes extending the infinite prime of  $\mathbb{Q}$ , thus  $(K_i, \text{tr}_{K_i/\mathbb{R}}) \cong \langle 1 \rangle$  if  $K_i = \mathbb{R}$  and  $(K_i, \text{tr}_{K_i/\mathbb{R}}) \cong \langle 1, -1 \rangle$  if  $K_i = \mathbb{C}$ , hence the result.  $\square$

Note also that as  $K \cong \mathbb{Q} \perp K^0$ , the space  $(K^0, \text{tr}_{K/\mathbb{Q}})$  has signature  $(r + s - 1, s)$  and so do the quadratic modules  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$  and  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$ .

It follows for example that  $(\mathcal{O}_K^\perp, b_K)$ , being by definition positive definite, will be different from  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$  as soon as  $K$  is non-totally real.

## 2.2. Interplay of the quadratic modules

For a general number field  $K$  it might be the case that the quadratic modules we are associating could not be related at all, for example in [Har17] the author exhibited two number fields  $K = \mathbb{Q}(\sqrt[3]{6})$  and  $L = \mathbb{Q}(\sqrt[3]{12})$  such that  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  and yet  $\text{Sh}(K) \neq \text{Sh}(L)$ , by contrast in the totally real case we have the following.

**Proposition 2.10.** Let  $K$  be totally real and let  $L$  be any number field, then every isometry  $\phi : (\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  satisfies  $\phi(1) \in \{+1, -1\}$ . In particular,  $\phi$  restricts to an isometry  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  and to an isometry  $(\mathcal{O}_K^\perp, b_K) \cong (\mathcal{O}_L^\perp, b_L)$ .

*Proof.* Suppose  $\phi : (\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  is an isometry, then both fields must have the same degree  $n$  and, by Taussky's theorem,  $L$  is also totally real. Since  $\phi(1)^2$  is a totally positive<sup>3</sup> algebraic integer and  $\text{Tr}_{K/\mathbb{Q}}(\phi(1)^2) = \text{Tr}_{L/\mathbb{Q}}(1^2) = n$ , by the arithmetic-geometric means inequality applied to the  $n$  conjugates of  $\phi(1)^2$  over  $\mathbb{Q}$ , we have that the equality in

$$1 \leq \text{Nm}_{K/\mathbb{Q}}(\phi(1)^2)^{1/n} \leq \frac{\text{Tr}_{K/\mathbb{Q}}(\phi(1)^2)}{n} = 1$$

implies  $\phi(1)^2$  rational and therefore equal to 1. The relations  $\phi(\mathcal{O}_K^0) = \mathcal{O}_L^0$ , and  $\phi(\mathcal{O}_K^\perp) = \mathcal{O}_L^\perp$  follow from the equivalences

$$\begin{aligned} x \in \mathcal{O}_K^0 &\iff \text{Tr}_{K/\mathbb{Q}}(x \cdot 1) = 0 \\ &\iff \text{Tr}_{L/\mathbb{Q}}(\phi(x)\phi(1)) = 0 \\ &\iff \pm \text{Tr}_{L/\mathbb{Q}}(\phi(x)) = 0 \\ &\iff \phi(x) \in \mathcal{O}_L^0 \end{aligned}$$

<sup>3</sup> An element  $x$  in a number field  $K$  is said to be *totally positive*, denoted  $x \gg 0$ , if  $\sigma(x) > 0$  for every  $\sigma$  real embedding of  $K$

for all  $x$  in  $\mathcal{O}_K$ , and from the fact that  $\phi(\mathbb{Z} + n\mathcal{O}_K) = \phi(1)\mathbb{Z} + n\phi(\mathcal{O}_K) = \mathbb{Z} + n\mathcal{O}_L$ .  $\square$

So for totally real  $K$  we have that  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  always implies  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$ , the following example (found using `Magma` by “brute force”) shows that the converse is not true even under this hypothesis.

**Example 2.11.** Let  $K$  and  $L$  be the quartic fields with defining polynomials  $x^4 + 82x^2 + 656$  and  $x^4 - 2x^3 - 19x^2 + 20x + 18$  respectively, then  $K$  and  $L$  are totally real fields such that  $\text{disc}(K) = 2^6 41^3 = \text{disc}(L)$  and  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  however  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \not\cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  and  $(\mathcal{O}_K^\perp, b_K) \not\cong (\mathcal{O}_L^\perp, b_L)$ .

In view of such example it is natural to ask under what conditions we could expect to have a reciprocal for Proposition 2.10. To address that question, remark that since  $K = \mathbb{Q} \perp K^0$ , each isometry  $\varphi : (K^0, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (L^0, \text{tr}_{L/\mathbb{Q}})$  has two natural extensions to an isometry  $(K, \text{tr}_{K/\mathbb{Q}}) \cong (L, \text{tr}_{L/\mathbb{Q}})$ , namely, the one taking 1 to +1 call it  $\varphi^+$  and the one taking 1 to -1 call it  $\varphi^-$ . These are in fact the only two possible extensions of  $\varphi$ . Indeed, given an isometry  $\phi : (K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (L, \text{tr}_{L/\mathbb{Q}})$  extending  $\varphi$ , we know that  $\phi(1)$  is orthogonal to  $\phi(K^0) = L^0$ , which is the orthogonal complement of  $1 \cdot \mathbb{Q}$  and, as  $(L, \text{tr}_{L/\mathbb{Q}})$  is non degenerate, this implies  $\phi(1) \in \mathbb{Q}$  but then  $n = \text{Tr}_{L/\mathbb{Q}}(\phi(1)^2) = n\phi(1)^2$ , which proves  $\phi(1) \in \{-1, +1\}$ .

Since  $K^0 = \mathcal{O}_K^0 \cdot \mathbb{Q} = \mathcal{O}_K^\perp \cdot \mathbb{Q}$ , it follows that an isometry  $\varphi : (\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$ , respectively  $\varphi : (\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$ , will lift to an isometry  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  if and only if either  $\varphi^+(\mathcal{O}_K) = \mathcal{O}_L$  or  $\varphi^-(\mathcal{O}_K) = \mathcal{O}_L$ . But when do we have this equalities?. This motivates the following

**Lemma 2.12.** Let  $L$  be a number field, then:

- (i) Let  $\varphi : (\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$  be an isometry, then  $\varphi^\pm(\mathcal{O}_K) = \mathcal{O}_L$  if and only if there exists a basis  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  of  $\mathcal{O}_K$  such that  $t_i \equiv \pm s_i \pmod{n}$  for all  $1 \leq i < n$ , where  $t_i := \text{Tr}_{K/\mathbb{Q}}(\alpha_i)$  and the  $s_i$ 's are any integers such that  $\varphi(\alpha_{i\perp}) = n\beta_i - s_i \in \mathcal{O}_L^\perp$ , with  $\beta_i \in \mathcal{O}_L$ .
- (ii) Suppose  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = k\mathbb{Z} = \text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L)$ ,  $k \in \mathbb{Z}^+$  and let  $\varphi : (\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  be an isometry, then  $\varphi^\pm(\mathcal{O}_K) = \mathcal{O}_L$  if and only if  $\varphi(\gamma_0) \equiv \pm 1 \pmod{n/k}$ . Where  $\gamma_0 := 1 - (n/k)\gamma_K \in \mathcal{O}_K^0$  and  $\gamma_K$  is any element in  $\mathcal{O}_K$  such that  $\text{Tr}_{K/\mathbb{Q}}(\gamma_K) = k$ .

*Proof.* Note that in both cases the hypothesis and the existence of the respective isometry imply  $[K : \mathbb{Q}] = n = [L : \mathbb{Q}]$  and  $\text{disc}(K) = \text{disc}(L)$ . This is clear for the degrees and for the discriminants it follows from the equalities  $\text{disc}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) = n^{2n-3} \text{disc}(K)$  and  $\text{disc}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) = \frac{n}{k^2} \text{disc}(K)$ . Thus in each case  $\varphi^\pm(\mathcal{O}_K) \subset \mathcal{O}_L$  if and only if  $\varphi^\pm(\mathcal{O}_K) = \mathcal{O}_L$ . Now to prove (i) observe that for any basis  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  of  $\mathcal{O}_K$  we have

$$\begin{aligned}
\varphi^\pm(\mathcal{O}_K) \subset \mathcal{O}_L &\iff \varphi^\pm(\alpha_i) \in \mathcal{O}_L && \forall 1 \leq i < n \\
&\iff \varphi^\pm\left(\frac{\alpha_{i\perp} + t_i}{n}\right) \in \mathcal{O}_L && \forall 1 \leq i < n \\
&\iff \frac{\varphi(\alpha_{i\perp}) \pm t_i}{n} \in \mathcal{O}_L && \forall 1 \leq i < n \\
&\iff \frac{n\beta_i - s_i \pm t_i}{n} \in \mathcal{O}_L && \forall 1 \leq i < n \\
&\iff \frac{-s_i \pm t_i}{n} \in \mathcal{O}_L && \forall 1 \leq i < n \\
&\iff s_i \equiv \pm t_i \pmod{n} && \forall 1 \leq i < n
\end{aligned}$$

As for (ii) observe that  $\mathcal{O}_K = \gamma_K \mathbb{Z} + \mathcal{O}_K^0$ , thus

$$\begin{aligned}
\varphi^\pm(\mathcal{O}_K) \subset \mathcal{O}_L &\iff \varphi^\pm(\gamma_K) \in \mathcal{O}_L \\
&\iff (k/n)\varphi^\pm(1 - \gamma_0) \in \mathcal{O}_L \\
&\iff (k/n)(\pm 1 - \varphi(\gamma_0)) \in \mathcal{O}_L \\
&\iff \varphi(\gamma_0) = \pm 1 \pmod{n/k}
\end{aligned}$$

□

To see how we could use this lemma, we begin by giving a description of the basis of  $\mathcal{O}_K^0$  that generalizes [MS10, Proposition 5.2]

**Proposition 2.13.** Suppose  $n \geq 3$  and  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = k\mathbb{Z}$ ,  $k \in \mathbb{Z}^+$ , then exists a basis  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  of  $\mathcal{O}_K$  such that

$$(\text{Tr}_{K/\mathbb{Q}}(\alpha_1), \dots, \text{Tr}_{K/\mathbb{Q}}(\alpha_{n-2}), \text{Tr}_{K/\mathbb{Q}}(\alpha_{n-1})) =: (t_1, \dots, t_{n-2}, t_{n-1}) \equiv (0, \dots, 0, k) \pmod{n}$$

and therefore  $\{\alpha_1 - t_1/n, \dots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$  is a basis of  $\mathcal{O}_K^0$ .

**Remark 2.14.** If  $n = 2$ , for any basis  $\{1, \alpha_1\}$  of  $\mathcal{O}_K$  we have  $\text{Tr}_{K/\mathbb{Q}}(\alpha_1) = t_1 \equiv k \pmod{2}$  and  $\{(2/k)\alpha_1 - t_1/k\}$  is a basis of  $\mathcal{O}_K^0$ .

The proof is based in the following elementary lemma:

**Lemma 2.15.** Let  $r$  and  $m \geq 2$  be integers, then:

- (a) Given any sets of integers  $\{u_1, \dots, u_m\}$  and  $\{s_1, \dots, s_m\}$ , there exist integers  $\{c_1, \dots, c_m\}$  such that  $\sum_i c_i s_i = 0$  and  $\text{gcd}(u_1 - c_1, \dots, u_m - c_m) = 1$ .
- (b) If  $\text{gcd}(r, s_1, \dots, s_m) = 1$ , then there are integers  $\{h_1, \dots, h_m\}$  such that

$$\text{gcd}(rh_1 + s_1, \dots, rh_m + s_m) = 1.$$

*Proof.* Let  $s := \gcd(s_1, \dots, s_m)$  and consider the surjective map

$$f : \mathbb{Z}^m \rightarrow s\mathbb{Z}, (c_1, \dots, c_m) \mapsto \sum_i c_i s_i$$

since  $\mathbb{Z}$  is a PID, there is an exact sequence of  $\mathbb{Z}$ -modules  $\mathbb{Z}^m \xrightarrow{g} \mathbb{Z}^m \xrightarrow{f} s\mathbb{Z} \rightarrow 0$ .

For a prime  $p$  denote  $v \mapsto \bar{v}$  the canonical projection  $\mathbb{Z} \rightarrow \mathbb{F}_p$  and  $\bar{g} : \mathbb{F}_p^m \rightarrow \mathbb{F}_p^m$  the map induced by  $g$ . We claim that  $\ker(\bar{g}) \neq \mathbb{F}_p^m$ . Indeed, since the tensor product  $- \otimes_{\mathbb{Z}} \mathbb{F}_p$  is right exact, we get an exact sequence of  $\mathbb{F}_p$ -spaces

$$\mathbb{F}_p^m \xrightarrow{\bar{g}} \mathbb{F}_p^m \xrightarrow{\bar{f}} \bar{s}\mathbb{F}_p \rightarrow 0$$

thus if  $\text{Im}(\bar{g}) = 0$  we would have  $\mathbb{F}_p^m \cong \bar{s}\mathbb{F}_p$ , which contradicts  $m \geq 2$ .

Now set  $N := \sum_i u_i s_i$  and  $u := (u_1, \dots, u_m)$ . First suppose  $N \neq 0$  and for each prime  $p$  dividing  $N$  consider the set

$$X_p := \{\bar{v} \in \mathbb{F}_p^m : \bar{g}(\bar{v}) = \bar{u}\}$$

then either  $X_p = \emptyset$  or  $X_p = \bar{v}_0 + \ker(\bar{g})$  with  $\bar{v}_0 \in X_p$  and from the above paragraph follows that  $X_p \neq \mathbb{F}_p^m$ , so we may pick  $\bar{v}_p \in \mathbb{F}_p^m$  such that  $\bar{g}(\bar{v}_p) \neq \bar{u}$ . By the Chinese remainder theorem we can choose  $v \in \mathbb{Z}^m$  such that

$$v \equiv v_p \pmod{p} \text{ for all } p \mid N$$

(if  $N = \pm 1$  any  $v \in \mathbb{Z}^m$  will satisfy this condition). Define  $c = (c_1, \dots, c_m) := g(v) \in \ker(f)$ , then  $\sum_i c_i s_i = 0$  and the integers  $\{u_i - c_i\}$  are coprime, otherwise there would be a prime  $p$  such that  $p \mid u_i - c_i$  for all  $i \leq m$ , so  $p \mid \sum_i (u_i - c_i) s_i = N$  and we would get

$$u \equiv c = g(v) \equiv g(v_p) \not\equiv u \pmod{p}$$

a contradiction, this proves (a) whenever  $N \neq 0$ . On the other hand, if  $N = 0$  pick any non-zero element  $(d_1, \dots, d_m) \in \text{Ker}(f)$  (which exists because  $m \geq 2$ ) and take  $c_i := u_i - d_i/d$ , where  $d = \gcd(d_1, \dots, d_m)$ . Then,  $\sum_i c_i s_i = N - \sum_i d_i s_i/d = 0$  and  $\gcd(u_1 - c_1, \dots, u_m - c_m) = \gcd(d_1/d, \dots, d_m/d) = 1$ , so (a) also holds in this case.

To prove (b), write  $1 = ar + bs$  with  $a, b \in \mathbb{Z}$  and write  $bs = \sum_i u_i s_i$  for some integers  $\{u_i\}$ , by part (a) exists  $\{c_i\}$  such that  $\sum_i c_i s_i = 0$  and the integers  $v_i := u_i - c_i$  are coprime. Let  $\{h_i\}$  be such that  $\sum_i v_i h_i = a$  then

$$\sum_i v_i (rh_i + s_i) = r \sum_i v_i h_i + \sum_i v_i s_i = ra + bs = 1$$

and therefore the integers  $\{rh_i + s_i\}$  are coprime. □

*Proof of Proposition 2.13.* Let  $\{1, \beta_1, \dots, \beta_{n-1}\}$  be a basis of  $\mathcal{O}_K$  and let  $s_i := \text{Tr}_{K/\mathbb{Q}}(\beta_i)$  for  $1 \leq i \leq n-1$ , by hypothesis  $(1/k)\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \langle n/k, s_1/k, \dots, s_{n-1}/k \rangle_{\mathbb{Z}} = \mathbb{Z}$ , so applying part (b) of the above lemma to  $m := n-1 \geq 2$  and  $r := n/k$ , we find  $\{h_1, \dots, h_{n-1}\}$  such that the integers  $\{rh_1 + s_1/k, \dots, rh_{n-1} + s_{n-1}/k\}$  are coprime and therefore the last column of some matrix  $A$  in  $\text{GL}_{n-1}(\mathbb{Z})$ , that is,

$$(rh_1 + s_1/k, \dots, rh_{n-1} + s_{n-1}/k)^t = A(0, \dots, 0, 1)^t$$

now define the basis  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  by the relation

$$(1, \alpha_1, \dots, \alpha_{n-1})^t := \begin{bmatrix} 1 & 0 \\ 0 & A^{-1} \end{bmatrix} (1, \beta_1, \dots, \beta_{n-1})^t$$

then  $(\alpha_1, \dots, \alpha_{n-1})^t = A^{-1}(\beta_1, \dots, \beta_{n-1})^t$  and

$$\begin{aligned} (1/k)(\text{Tr}_{K/\mathbb{Q}}(\alpha_1), \dots, \text{Tr}_{K/\mathbb{Q}}(\alpha_{n-1}))^t &= A^{-1}(s_1/k, \dots, s_{n-1}/k)^t \\ &\equiv A^{-1}(rh_1 + s_1/k, \dots, rh_{n-1} + s_{n-1}/k)^t \pmod{r} \\ &= (0, \dots, 0, 1)^t \pmod{r} \end{aligned}$$

hence  $(\text{Tr}_{K/\mathbb{Q}}(\alpha_1), \dots, \text{Tr}_{K/\mathbb{Q}}(\alpha_{n-1})) \equiv (0, \dots, 0, k) \pmod{n}$ .

To prove that  $\{\alpha_1 - t_1/n, \dots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$  is a  $\mathbb{Z}$ -basis of  $\mathcal{O}_K^0$  note that its  $\mathbb{Z}$ -span  $C$  is clearly contained in  $\mathcal{O}_K^0$  and the  $\mathbb{Z}$ -span of  $\{1, \alpha_1 - t_1/n, \dots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$  has index  $n/k$ . Indeed, the matrix expressing  $\{1, \alpha_1 - t_1/n, \dots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$  in terms of the integral basis  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  of  $K$  is

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ -t_1/n & 1 & 0 & \dots & 0 \\ -t_2/n & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -t_{n-1}/k & 0 & 0 & \dots & n/k \end{bmatrix}$$

so its determinant is  $n/k$ . As in the proof of (2.3), this implies  $\text{disc}(C) = \frac{n}{k^2} \text{disc}(K) = \text{disc}(\mathcal{O}_K^0)$ , therefore  $C = \mathcal{O}_K^0$ . □

We are now ready to prove the following partial reciprocal of Proposition 2.10.

**Theorem 2.16.** *Suppose  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  and  $(\mathbb{Z}/n\mathbb{Z})^\times$  cyclic, then for any number field  $L$ :*

- (i) *Every isometry  $\varphi : (\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$  extends to an isometry  $\phi : (\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .*

(ii) If  $(n, \text{disc}(K)) = 1$ , then every isometry  $\varphi : (\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  also extends to an isometry  $\phi : (\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .

*Proof.* Case  $n = 1$  is trivial and case  $n = 2$  is easy to check, so let us suppose that  $n \geq 3$ .

(i) Let  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  be any basis of  $\mathcal{O}_K$ . Take  $t_i := \text{Tr}_{K/\mathbb{Q}}(\alpha_i)$ ,  $1 \leq i < n$ , so that  $\alpha_{i\perp} = n\alpha_i - t_i$  is a basis of  $\mathcal{O}_K^\perp$  and for each  $1 \leq i < n$  choose  $\beta_i \in \mathcal{O}_L$  and  $s_i \in \mathbb{Z}$  such that

$$y_i := \varphi(\alpha_{i\perp}) = n\beta_i - s_i \in \mathcal{O}_L^\perp$$

then  $\text{Tr}_{K/\mathbb{Q}}(y_i y_j) = n^2 \text{Tr}_{K/\mathbb{Q}}(\beta_i \beta_j) - ns_i s_j \equiv -ns_i s_j \pmod{n^2}$  and since  $\text{Tr}_{K/\mathbb{Q}}(y_i y_j) = \text{Tr}_{K/\mathbb{Q}}(\alpha_{i\perp} \alpha_{j\perp}) \equiv -nt_i t_j \pmod{n^2}$  we conclude

$$t_i t_j \equiv s_i s_j \pmod{n}, \text{ for all } 1 \leq i, j < n$$

Let  $\{u_i\}$  be integers such that  $\sum_i u_i t_i \equiv 1 \pmod{n}$  and take  $u := \sum_i u_i s_i$ , then  $s_i u \equiv t_i \pmod{n}$  for all  $1 \leq i < n$ , in particular  $(u, n) = 1$  and if  $v$  is its inverse modulo  $n$  then

$$t_i t_j \equiv v^2 t_i t_j \pmod{n}, \text{ for all } 1 \leq i, j < n$$

thus  $v^2 \equiv 1 \pmod{n}$  and as  $(\mathbb{Z}/n\mathbb{Z})^\times$  is cyclic this implies  $v \equiv \pm 1 \pmod{n}$ , thus  $s_i \equiv \pm t_i \pmod{n}$  for all  $1 \leq i < n$  and by (2.12) either  $\phi = \varphi^+$  or  $\phi = \varphi^-$  extend  $\varphi$  to an isometry  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .

(ii) First note that under hypothesis we must have  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$ , because if  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = l\mathbb{Z}$ ,  $l \in \mathbb{Z}^+$  by (2.3), the existence of the isometry  $\varphi$  implies  $n \text{disc}(K) = \frac{n}{l^2} \text{disc}(L)$ , that is,  $\text{disc}(K) = l^{-2} \text{disc}(L)$  thus  $l \mid l^{n-2}$  and  $l^{n-2} \mid l^{-2} \text{disc}(L) = \text{disc}(K)$ , since  $l \mid n$  and  $(\text{disc}(K), n) = 1$ , we conclude  $l = 1$ .

Now, take a basis  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  of  $\mathcal{O}_K$  and  $\{t_1, \dots, t_{n-1}\}$  as in Proposition 2.13 so that

$$w_1 := \alpha_1 - t_1/n, \dots, w_{n-2} := \alpha_{n-2} - t_{n-2}/n, w_{n-1} := n\alpha_{n-1} - t_{n-1}$$

is a basis of  $\mathcal{O}_K^0$ . Note that for all  $1 \leq i < n$  we have

$$\text{Tr}_{K/\mathbb{Q}}(w_i w_{n-1}) = \text{Tr}_{K/\mathbb{Q}}(w_i(n\alpha_{n-1} - t_{n-1})) = n \text{Tr}_{K/\mathbb{Q}}(w_i \alpha_{n-1}) \equiv 0 \pmod{n} \quad (*)$$

and for  $i = n - 1$

$$(1/n) \text{Tr}_{K/\mathbb{Q}}(w_{n-1}^2) = \text{Tr}_{K/\mathbb{Q}}(n\alpha_{n-1}^2 - t_{n-1}\alpha_{n-1}) = n \text{Tr}_{K/\mathbb{Q}}(\alpha_{n-1}^2) - t_{n-1}^2 \equiv -1 \pmod{n}$$

Let us define  $\theta_i := \varphi(w_i)$ ,  $1 \leq i < n$ . Take  $\gamma_L \in \mathcal{O}_L$  such that  $\text{Tr}_{K/\mathbb{Q}}(\gamma_L) = 1$  and write

$$1 - \gamma_L n = \sum_{i=1}^{n-1} l_i \theta_i \text{ with } l_i \in \mathbb{Z}$$

taking traces in the congruences  $\theta_j \equiv \sum_i l_i \theta_i \theta_j \pmod{n}$  we find that the Gram matrix  $G := (\text{Tr}_{K/\mathbb{Q}}(w_i w_j)) = (\text{Tr}_{L/\mathbb{Q}}(\theta_i \theta_j))$  satisfies

$$G(l_1, \dots, l_{n-1})^t \equiv 0 \pmod{n}$$

Call  $G^*$  the matrix obtained from  $G$  dividing the last column by  $n$ , which has integer entries thanks to (\*), then

$$G^*(l_1, \dots, l_{n-2}, 0)^t \equiv G^*(l_1, \dots, l_{n-2}, n l_{n-1})^t = G(l_1, \dots, l_{n-2}, l_{n-1})^t \equiv 0 \pmod{n}$$

from (2.3) we know that  $\det(G^*) = \text{disc}(K)$  which by hypothesis is coprime to  $n$ . It follows that  $l_i \equiv 0 \pmod{n}$  for all  $1 \leq i \leq n-2$  and thus  $l_{n-1} \theta_{n-1} - 1 \equiv 0 \pmod{n}$ , squaring this congruence and taking traces again we find

$$\begin{aligned} l_{n-1}^2 \theta_{n-1}^2 - 2l_{n-1} \theta_{n-1} + 1 &\equiv 0 \pmod{n^2} \Rightarrow l_{n-1}^2 \text{Tr}_{L/\mathbb{Q}}(\theta_{n-1}^2) + n \equiv 0 \pmod{n^2} \\ &\Rightarrow l_{n-1}^2 \text{Tr}_{K/\mathbb{Q}}(w_{n-1}^2) + n \equiv 0 \pmod{n^2} \\ &\Rightarrow l_{n-1}^2(-n) + n \equiv 0 \pmod{n^2} \\ &\Rightarrow l_{n-1}^2(-1) + 1 \equiv 0 \pmod{n} \\ &\Rightarrow l_{n-1}^2 \equiv 1 \pmod{n} \end{aligned}$$

Since  $(\mathbb{Z}/n\mathbb{Z})^\times$  is cyclic, this implies  $l_{n-1} \equiv \pm 1 \pmod{n}$ , now let

$$\gamma_K := \alpha_{n-1} - (t_{n-1} - 1)/n = (1/n)(w_{n-1} + 1) \in \mathcal{O}_K$$

then,  $\text{Tr}_{K/\mathbb{Q}}(\gamma_K) = 1$  and  $\varphi(1 - n\gamma_K) = -\theta_{n-1} \equiv \mp 1 \pmod{n}$ , thus we are done by (2.12)(ii). □

**Corollary 2.17.** Suppose  $K$  totally real,  $\text{disc}(K)$  fundamental and  $(\mathbb{Z}/n\mathbb{Z})^\times$  cyclic,  $n \geq 3$ . Then, for any number field  $L$  the following are equivalent:

- (i)  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .
- (ii)  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$ .
- (iii)  $\text{Sh}(K) = \text{Sh}(L)$  and  $L$  is totally real with fundamental discriminant.

If  $(n, \text{disc}(K)) = 1$ , then the three items are also equivalent to

(iv)  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .

*Proof.* The equivalences (i)  $\iff$  (ii) and (i)  $\iff$  (ii)  $\iff$  (iv) under the additional conditions follow from (2.10), (2.16) and the fact that  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  (by (2.6)(iii)), it remains to prove (ii)  $\iff$  (iii):

$\Rightarrow$ ) By Taussky's theorem,  $L$  is totally real so  $b_K = \text{tr}_{K/\mathbb{Q}}$  and  $\text{Sh}(K) = \text{Sh}(L)$ , also  $\text{disc}(K) = \text{disc}(L)$  is fundamental.

$\Leftarrow$ ) Let  $\lambda \in \mathbb{R}^\times$  be such that an isometry  $\varphi : (\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \rightarrow (\mathcal{O}_L^\perp, \lambda \text{tr}_{L/\mathbb{Q}})$  exists. Let  $\{1, \alpha_1, \dots, \alpha_{n-1}\}$  be a basis of  $\mathcal{O}_K$ , take  $x_i := \alpha_{i\perp} = n\alpha_i - t_i$ ,  $1 \leq i < n$ , as basis of  $\mathcal{O}_K^\perp$  and define  $y_i := \varphi(x_i) = n\beta_i - s_i$ ,  $\beta_i \in \mathcal{O}_L$ ,  $s_i \in \mathbb{Z}$ . Then,  $\text{Tr}_{K/\mathbb{Q}}(x_i x_j) = \lambda \text{Tr}_{L/\mathbb{Q}}(y_i y_j)$  for all  $1 \leq i, j < n$ , in particular  $\lambda \in \mathbb{Q}^{>0}$  so we may write  $\lambda = r/s$  where  $r$  and  $s$  are coprime positive integers.

Since  $n^{2n-3} \text{disc}(K) = \text{disc}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) = \text{disc}(\mathcal{O}_L^\perp, \lambda \text{tr}_{L/\mathbb{Q}}) = \lambda^{n-1} n^{2n-3} \text{disc}(L)$  we know that

$$s^{n-1} \text{disc}(K) = r^{n-1} \text{disc}(L)$$

Thus  $r^2 \mid r^{n-1} \mid \text{disc}(K)$  and if we suppose  $r \neq 1$  then  $r = 2^u$  with

$$n - 1 \leq (n - 1)u \leq v_2(\text{disc}(K)) \leq 3$$

also  $s^2 \mid \text{disc}(L)$  and  $(r, s) = 1$  forces  $s = 1$ . Therefore  $\text{disc}(K) = 2^{u(n-1)} \text{disc}(L)$  and:

- If  $n = 4$ , we would have  $u = 1$  and  $\lambda = 2$ , but since  $(1/4)\text{Tr}_{K/\mathbb{Q}}(x_i x_j) \equiv -t_i t_j \pmod{4}$  and  $(1/4)\text{Tr}_{L/\mathbb{Q}}(y_i y_j) \equiv -s_i s_j \pmod{4}$ , this implies

$$t_i t_j \equiv -(1/4)\text{Tr}_{K/\mathbb{Q}}(x_i x_j) = -(1/2)\text{Tr}_{K/\mathbb{Q}}(y_i y_j) \equiv 2s_i s_j \pmod{4}$$

which yields  $t_i t_j \equiv 0 \pmod{2}$  for all  $1 \leq i, j < n$  contradicting  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$ .

- If  $n = 3$ , we would have  $u = 1$ , so either  $v_2(\text{disc}(K)) = 2$  and  $v_2(\text{disc}(L)) = 0$  in which case  $\text{disc}(L) = \text{disc}(K)/4 \equiv 3 \pmod{4}$  or  $v_2(\text{disc}(K)) = 3$  and  $v_2(\text{disc}(L)) = 1$ , both cases contradict Stickelberger's theorem (1.29)(ii) applied to  $\text{disc}(L)$ .

Thus  $r = 1$  and by symmetry of the argument  $s = 1$ , therefore  $\lambda = 1$  and  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$ , as required.  $\square$

The following examples try to illustrate the limitations of the strategy employed to prove Theorem 2.16 and test the sharpness of the statement:

Suppose  $K$  totally real with  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = k\mathbb{Z}$ ,  $k \in \mathbb{Z}^+$ , then by (2.10) the restrictions maps

$$\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \rightarrow \text{Aut}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \text{ and } \text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \rightarrow \text{Aut}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$$

are well defined homomorphism of groups. Moreover, this maps are injective if  $\frac{n}{k} \nmid 2$ , because by (2.10) given  $\varphi$  in either co-domain,  $\varphi^+$  and  $\varphi^-$  are the only possible preimages of  $\varphi$  and they cannot both extend  $\varphi$ , otherwise, we would have

$$n\varphi^+(\gamma_K) - k = \varphi^+(n\gamma_K - k) = \varphi^-(n\gamma_K - k) = n\varphi^-(\gamma_K) + k, \text{ where } \gamma_K \in \mathcal{O}_K \text{ and } \text{Tr}_{K/\mathbb{Q}}(\gamma_K) = k$$

so  $-k \equiv k \pmod{n}$  and  $\frac{n}{k} \mid 2$ . It follows that, when  $\frac{n}{k} \nmid 2$ , every automorphism of  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$  can be extended to all  $\mathcal{O}_K$  if and only if  $\#\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) = \#\text{Aut}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$  and in general the restriction map will not be surjective if  $\#\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) < \#\text{Aut}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$ , similarly for  $\mathcal{O}_K^0$ .

**Example 2.18.** Let  $K$  be the cubic field with defining polynomial  $x^3 + x^2 - 8x + 3$ , then  $K$  is totally real,  $\text{disc}(K) = 3 \cdot 5^2 \cdot 19$ ,  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  and

$$\#\text{Aut}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) = \#\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) = 2 \neq 4 = \#\text{Aut}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$$

hence there exists an automorphism of  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$  that *cannot* be extended to all  $\mathcal{O}_K$ , so the hypothesis  $(n, \text{disc}(K)) = 1$  in (2.16)(ii) cannot be dropped. By contrast observe that all automorphisms of  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$  can be extended to  $\mathcal{O}_K$ .

**Example 2.19.** Let  $K$  be the field with defining polynomial  $x^4 - 2x^3 - 5x^2 + 6x + 1$ , then  $K$  is totally real,  $\text{disc}(K) = 2^6 \cdot 5^2$ ,  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = 2\mathbb{Z}$  and

$$\#\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) = 8 < 16 = \#\text{Aut}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}})$$

thus the restriction map is not surjective and therefore the hypothesis  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  in (2.16)(i) is not superfluous.

**Proposition 2.20.** Let  $K$  be a  $\mathbb{Z}/l\mathbb{Z}$ -field with  $l$  prime, then for any number field  $L$ , every isometry  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$  (respectively  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$ ) can be extended to one between the integral trace quadratic modules  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .

*Proof.* In the case  $l \nmid \text{disc}(K)$ , this follows directly from (2.16) and (2.6)(i). On the other hand, if  $l \mid \text{disc}(K)$ , we have that  $l$  ramifies in  $K$  and the fact that  $K$  is a  $\mathbb{Z}/l\mathbb{Z}$ -field forces to be only one prime  $\mathfrak{p}$  in  $K$  lying over  $l$  and for that prime  $l = e(\mathfrak{p}|l)$ , so (2.5) tells us  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = l\mathbb{Z}$ . We claim that if  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  this implies  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = l\mathbb{Z}$ .

Suppose not, then  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$  and by (2.3)  $\text{disc}(L) = l^{-2} \text{disc}(K)$ , if  $l = 2$  this contradicts Stickelberger's criterion (1.29)(ii), so we may assume  $l$  odd. Recall from (2.6)(i) that  $l \leq v_l(\text{disc}(K))$ , as  $l$  is odd and  $K$  is a  $\mathbb{Z}/l\mathbb{Z}$ -field, we know that  $\text{disc}(K)$  is perfect square, so in fact  $l + 1 \leq v_l(\text{disc}(K))$ , that is,  $l - 1 \leq v_l(\text{disc}(L))$  but by (2.6)(ii)  $l$  is tamely ramified in  $L$ , thus if  $f_1^{e_1} \dots f_g^{e_g}$  is its factorization type, the inequality

$$l - 1 \leq v_l(\text{disc}(L)) = l - (f_1 + \dots + f_g) \leq l - 1$$

shows  $f_1 = 1$  and  $g = 1$  and this yields  $l = e_1 f_1 = e_1$ , a contradiction.

Hence if  $\varphi : (\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  is an isometry, we have  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = l\mathbb{Z} = \text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L)$  and taking  $\gamma_K = 1$  in (2.12)(ii) we conclude that both  $\varphi^+$  and  $\varphi^-$  extend  $\varphi$ . Also if we are given an isometry  $\varphi : (\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$ , then  $\text{disc}(K) = \text{disc}(L)$  and, as  $l$  is prime, (2.6) implies  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = l\mathbb{Z}$ , thus (2.13) shows  $\mathcal{O}_K^\perp = l\mathcal{O}_K^0$  and  $\mathcal{O}_L^\perp = l\mathcal{O}_L^0$ , therefore  $\varphi(\mathcal{O}_K^0) = \mathcal{O}_L^0$  ( $\varphi$  considered from  $K^0$  to  $L^0$ ) and we are back to the above case.  $\square$

**Example 2.21.** Let  $K$  be the sextic field with defining polynomial  $x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$ , then  $K$  is a totally real  $\mathbb{Z}/6\mathbb{Z}$ -field,  $\text{disc}(K) = 3^3 \cdot 7^5$ ,  $\text{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$  and

$$\#\text{Aut}(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) = \#\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) = 96 \neq 1440 = \#\text{Aut}(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}})$$

As a side note, we did not find any example showing that  $(\mathbb{Z}/n\mathbb{Z})^\times$  being cyclic is really a necessary hypothesis, so there might be some place for improvement there, however, note that any example would require  $n \geq 8$  so it may be possible that the example is just computationally difficult to find. In particular, it would be interesting to answer the following question.

**Question 2.** Do there exist totally real octic fields with odd discriminants  $K, L$  and an isometry  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$  which can not be lifted to an isometry  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ ?

# 3 Galois theory of fields with fundamental discriminant

In this chapter we prove two key results that will be needed in chapter 4. The first, Theorem 3.7, will tell us that when working with number fields of fundamental discriminant and same degree  $n$ , if we suppose that the fields are not isomorphic, then we can say a lot more, they are in fact linearly disjoint. This is a simple consequence of Hölder theorem on the automorphisms of the symmetric group  $S_n$  (1.41).

The second, Theorem 3.19, is the main purpose of this chapter and it basically allows us to lower bound the discriminant

$$|\text{disc}(\mathbb{Q}(c))|$$

for any  $c \in KL$  in terms of  $\text{disc}(K)$ , provided that  $K$  and  $L$  are two non-conjugated fields of the same fundamental discriminant and same degree. It will be useful to deal with even fundamental discriminants in the main result of the thesis and to prove Theorem 7.

For a number field  $K$  we will denote its Galois closure as  $\tilde{K}$  and its corresponding Galois group as  $G_K := \text{Gal}(\tilde{K}/\mathbb{Q})$ . Also,  $d_K$  will denote its discriminant.

## 3.1. Working with one field $K$

### 3.1.1. Ramification

We begin by giving a local description at the ramified primes.

**Lemma 3.1.** Let  $K$  be number field with fundamental discriminant. For rational prime  $p$  ramifying in  $K$ , let  $K_1, \dots, K_g$  be the completions of  $K$  at the primes lying over  $p$ . Then, there is a unique  $i_0$  such that  $K_{i_0}/\mathbb{Q}_p$  is ramified, furthermore,  $[K_{i_0} : \mathbb{Q}_p] = 2$  and  $K_i(\sqrt{d_K})/\mathbb{Q}_p(\sqrt{d_K})$  is unramified for all  $i$ .

*Proof.* Let  $i_0$  be such that  $K_{i_0}/\mathbb{Q}_p$  is ramified, then :

- If  $p \neq 2$ . The relation

$$\sum_i (e(\mathfrak{p}_i|p) - 1)f(\mathfrak{p}_i|p) \leq v_p(\text{disc}(K)) = 1$$

(see (1.36)) shows that  $e(\mathfrak{p}_{i_0}|p) = 2$ ,  $f(\mathfrak{p}_{i_0}|p) = 1$  and  $e(\mathfrak{p}_i|p) = 1$  for all  $i \neq i_0$ .

- If  $p = 2$ , then 2 is wildly ramified in  $K$ . For 2 is wildly ramified in  $F := \mathbb{Q}(\sqrt{d_K})$  (because  $\text{disc}(F) = d_K$ , since  $d_K$  is fundamental) and thus 2 is wildly ramified in  $F \subset \tilde{K}$ , hence wildly ramified in  $K$  by (1.38). Now if  $i_1$  is an index such that  $e(\mathfrak{p}_{i_1}|2) \equiv 0 \pmod{2}$ , then

$$e(\mathfrak{p}_{i_1}|2)f(\mathfrak{p}_{i_1}|2) \leq v_2(d_K) \leq 3$$

implies  $e(\mathfrak{p}_{i_1}|2) = 2$  and  $f(\mathfrak{p}_{i_1}|2) = 1$ , hence there is a unique such  $i_1$  and it must be  $i_0$ , otherwise,  $e(\mathfrak{p}_{i_0}|2) \geq 3$  and we would get

$$2 + 2 \leq (e(\mathfrak{p}_{i_0}|2) - 1)f(\mathfrak{p}_{i_0}|2) + e(\mathfrak{p}_{i_1}|2)f(\mathfrak{p}_{i_1}|2) \leq 3$$

a contradiction. Similarly if  $i \neq i_0$ , then  $e(\mathfrak{p}_i|2) = 1$  (or else  $e(\mathfrak{p}_i|2) \geq 3$ ).

Next we prove that  $K_{i_0}(\sqrt{d_K})/\mathbb{Q}_p(\sqrt{d_K})$  is unramified, let  $d_{K_i} := \text{disc}(K_i)$ . Since  $K_{i_0}/\mathbb{Q}_p$  is a quadratic extension, then  $K_{i_0} = \mathbb{Q}_p(\sqrt{d_{K_{i_0}}})$ . But as  $d_K$  is the product of the local discriminants (1.30), we have

$$d_K \equiv d_{K_{i_0}} u \pmod{\mathbb{Z}_p^{\times 2}}$$

where  $u := \prod_{i \neq i_0} d_{K_i} \in \mathbb{Z}_p^\times$ . Thus in order to prove that  $K_{i_0}(\sqrt{d_K}) = \mathbb{Q}_p(\sqrt{d_K}, \sqrt{u})$  is unramified over  $\mathbb{Q}_p(\sqrt{d_K})$ , it is enough to prove that  $\mathbb{Q}_p(\sqrt{u})$  is unramified over  $\mathbb{Q}_p$ . This is clear for  $p \neq 2$  and for  $p = 2$ , observe that for each  $i \neq i_0$ , as  $K_i/\mathbb{Q}_2$  is unramified, then  $\mathbb{Q}_2(\sqrt{d_{K_i}})$  is unramified (by (1.17)), hence  $d_{K_i} \equiv 1, 5 \pmod{\mathbb{Z}_2^{\times 2}}$  for all  $i \neq i_0$ , thus  $u \equiv 1, 5 \pmod{\mathbb{Z}_2^{\times 2}}$  and therefore  $\mathbb{Q}_2(\sqrt{u})/\mathbb{Q}_2$  is unramified.

The extensions  $K_i(\sqrt{d_K})/\mathbb{Q}_p(\sqrt{d_K})$  with  $i \neq i_0$  are clearly unramified, since  $K_i/\mathbb{Q}_p$  is unramified and  $\mathbb{Q}_p(\sqrt{d_K})$  is not.  $\square$

### 3.1.2. The Galois group

The Galois group of a field with fundamental discriminant of degree  $n$  is always the full symmetric group  $S_n$ . This was proved by J.Nakagawa in [N<sup>+</sup>88] for odd fundamental discriminants (i.e. square free discriminants), here we adapt his proof to any fundamental discriminant (even or odd).

**Theorem 3.2.** (Nakagawa, [N<sup>+</sup>88]) *Let  $K$  be number field with fundamental discriminant and degree  $n$  and let  $\cdot$ . Then,*

(i) *The extension  $\tilde{K}/\mathbb{Q}(\sqrt{d_K})$  is unramified at all finite primes.*

(ii) *Write  $K = \mathbb{Q}(\alpha)$  and let  $\{\alpha_1, \dots, \alpha_n\}$  be the conjugates of  $\alpha_1 := \alpha$  over  $\mathbb{Q}$ . If we identify  $G_K$  with a subgroup of  $S_n$  via its action on  $\{\alpha_1, \dots, \alpha_n\}$ , then for every prime  $\mathfrak{P}$  in  $\tilde{K}$  ramified over  $\mathbb{Q}$  the inertia group  $I_{\mathfrak{P}} \subset G_K \subset S_n$  is generated by a transposition.*

(iii) The field  $K$  is an  $S_n$ -field, i.e.,  $G_K \cong S_n$ .

The proof in [N<sup>+</sup>88] is based in the following two lemmas

**Lemma 3.3.** Let  $L$  be a finite Galois extension of  $\mathbb{Q}$  with Galois group  $G$ . For each prime ideal  $\mathfrak{P}$  of  $\mathcal{O}_K$ , let  $I_{\mathfrak{P}}$  be the inertia group. Then the groups  $I_{\mathfrak{P}}$  generate  $G$ .

**Lemma 3.4.** Let  $H$  be a subgroup of  $S_n$ ; if  $H$  is transitive generated by transpositions then  $H = S_n$ .

*Proof of Theorem 3.2.* Let  $F := \mathbb{Q}(\sqrt{d_K})$ , as  $\tilde{K}/F$  is the Galois closure of  $KF/F$  by (1.17) to prove that  $\tilde{K}/F$  is unramified at finite primes it is enough to prove that so is  $KF/F$ . Let  $\mathfrak{q}$  be a prime in  $F$  and let  $\mathfrak{Q}$  be a prime in  $KF$  over  $\mathfrak{q}$ , let  $\mathfrak{p} = \mathfrak{Q} \cap K$  and  $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$ , then if  $K_{\mathfrak{p}}$  is the completion of  $K$  with respect to  $\mathfrak{p}$  we have that  $K_{\mathfrak{p}}(\sqrt{d_K})$  and  $\mathbb{Q}_p(\sqrt{d_K})$  are the completion of  $KF = K(\sqrt{d_K})$  and  $F$  at  $\mathfrak{Q}$  and  $\mathfrak{q}$ , respectively. In view of Lemma  $K_{\mathfrak{p}}(\sqrt{d_K})/\mathbb{Q}_p(\sqrt{d_K})$  is unramified whenever  $p \mid d_K$ , thus  $e(\mathfrak{Q}|\mathfrak{q}) = 1$ , in this case. If, on the other hand,  $p \nmid d_K$ , then  $p$  is unramified in  $\tilde{K}$  by (1.17), in particular  $e(\mathfrak{Q}|\mathfrak{q}) = 1$ . This proves (i).

Let  $\mathfrak{P}$  be a prime in  $\tilde{K}$  ramified over  $\mathbb{Q}$ ,  $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Q}$  and  $I = I_{\mathfrak{P}}$ ,  $D = D_{\mathfrak{P}}$  be its inertia and decomposition groups. Since  $p \mid d_K$  and  $\tilde{K}/F$  is unramified, then  $\#I = e(\mathfrak{P}|p) = 2$ , thus  $I = \{1, \tau\}$  with  $\tau \in G_K$ . To complete the proof of (ii) we need to show that  $\tau$  is a transposition.

Consider subgroup  $H$  of  $G_K$  corresponding to  $K$ , i.e.,  $H := \text{Gal}(\tilde{K}/K) = \{\sigma : \sigma\alpha_1 = \alpha_1\}$ . By (1.15), if  $\{\sigma_1 \dots \sigma_g\}$  are a set of representatives of the double cosets in  $H \backslash G_K / D$ ; then  $\mathfrak{p}_i := \sigma_i(\mathfrak{P}) \cap K$ ,  $1 \leq i \leq g$  are exactly the primes in  $K$  lying over  $p$  and

$$[\sigma_i D \sigma_i^{-1} : \sigma_i D \sigma_i^{-1} \cap H] = e(\mathfrak{p}_i|p) f(\mathfrak{p}_i|p)$$

$$[\sigma_i I \sigma_i^{-1} : \sigma_i I \sigma_i^{-1} \cap H] = e(\mathfrak{p}_i|p)$$

but by (3.1) there is exactly one index  $i_0$  such that  $e(\mathfrak{p}_{i_0}|p) \neq 1$ , and for that index we have that  $e(\mathfrak{p}_{i_0}|p) = 2$  and  $f(\mathfrak{p}_{i_0}|p) = 1$ . By changing  $\mathfrak{P}$  with a conjugate (if necessary) we may assume  $\mathfrak{p}_{i_0} = \mathfrak{P} \cap K$  so  $\sigma_{i_0} = 1$ . Hence,  $D = I(D \cap H)$  and  $\sigma_i \tau \sigma_i^{-1} \in H$  if and only if  $i \neq i_0$ .

Let  $t \in \{1, \dots, n\}$  be such that  $\tau\alpha_1 = \alpha_t$ , then  $t \neq 1$  since  $\tau \notin H$ . Let  $s \neq t, 1$ , because  $G_K$  is transitive, exists  $\sigma \in G_K$  such that  $\alpha_s = \sigma^{-1}\alpha_1$ ; write  $\sigma = h\sigma_i d$  with  $h \in H$  and  $d \in D$ , then  $\alpha_s = d^{-1}\sigma_i^{-1}\alpha_1$ . Suppose  $i \neq i_0$ , then  $\alpha_s = d^{-1}\alpha_1$  but as  $D = I(D \cap H)$  this contradicts  $s \neq t, 1$ , thus  $i \neq i_0$  and  $\sigma_i \tau \sigma_i^{-1} \in H$ , i.e.,  $\tau\sigma_i^{-1}\alpha_1 = \sigma_i^{-1}\alpha_1$ . It follows that,

$$d^{-1}\tau d\alpha_s = d^{-1}\tau\sigma_i^{-1}\alpha_1 = d^{-1}\sigma_i^{-1}\alpha_1 = \alpha_s$$

but by (1.14) we know that  $I$  is normal in  $D$  so  $d^{-1}\tau d \in I$  and thus  $d^{-1}\tau d = \tau$ . We conclude that  $\tau\alpha_s = \alpha_s$  for all  $s \neq 1, t$  and therefore  $\tau$  is a transposition.

Now (iii) follows directly from (ii) and the above lemmas.  $\square$

### 3.1.3. Discriminants of intermediate fields

The following lemma allows us to compute discriminants of intermediate extension of Galois number fields when they are unramified over a quadratic field.

**Lemma 3.5.** Let  $N/\mathbb{Q}$  be a Galois extension with Galois group  $G$  such that  $\sqrt{d} \in N$  for some  $d \in \mathbb{Q}$  and suppose that a rational prime  $p$  is divisible by a prime  $\mathfrak{P}$  in  $N$  unramified over  $\mathbb{Q}(\sqrt{d}) := F$ . Then, for each intermediate field  $\mathbb{Q} \subset M \subset N$  with Galois group  $H := \text{Gal}(N/M)$  we have

$$v_p(d_M) = v_p(d_F) \cdot [M : \mathbb{Q}] \frac{|C_\tau - H|}{2|C_\tau|}$$

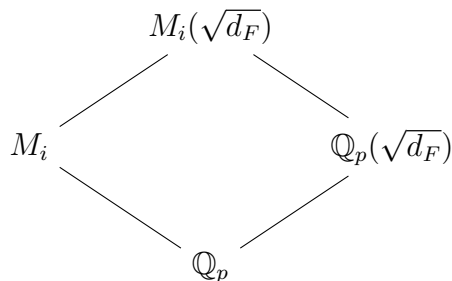
where  $\tau \in G$  is the generator of the inertia group  $I_{\mathfrak{P}}$  (which by hypothesis has order  $\leq 2$ ) and  $C_\tau$  is the conjugacy class of  $\tau$  in  $G$ .

*Proof.* If  $p \nmid d_F$ , then  $p$  is unramified in  $N$ , in particular  $p$  is unramified in  $M$ , thus  $p \nmid d_M$  and the equality holds, so let us suppose  $p \mid d_F$ . As in proof of (3.2) let  $D := D_{\mathfrak{P}}$  be the decomposition group of  $\mathfrak{P}$  and let  $\{\sigma_i\}$  be a set of representatives of the double cosets in  $H \backslash G / D$  so that  $\mathfrak{q}_i = \sigma_i(\mathfrak{P}) \cap M$  are the primes in  $M$  over  $p$ .

Since  $\mathfrak{P}$  is ramified over  $\mathbb{Q}$  and unramified over  $F$ , its inertia group  $I_{\mathfrak{P}} =: I$  has order 2. Let  $\tau \in G$  be its generator, here again by (1.15) we have

$$e(\mathfrak{q}_i|p) = [\sigma_i I \sigma_i^{-1} : \sigma_i I \sigma_i^{-1} \cap H]$$

thus  $e(\mathfrak{q}_i|p)$  is equal to 1 or 2 according to whether or not  $\sigma_i \tau \sigma_i^{-1}$  is in  $H$ . For each  $i$  let  $M_i$  be the completion of  $M$  at  $\mathfrak{q}_i$ . Suppose  $M_i/\mathbb{Q}_p$  is ramified, so that  $e(\mathfrak{q}_i|p) = 2$  and  $[M_i : \mathbb{Q}_p] = 2f(\mathfrak{q}_i|p)$ . Consider the following diagram



by hypothesis the extension  $M_i(\sqrt{d_F})/\mathbb{Q}_p(\sqrt{d_F})$  is unramified and, since the ramification index of the local extension  $\mathbb{Q}_p(\sqrt{d_F})/\mathbb{Q}_p$  is 2, by computing the ramification index of  $M_i(\sqrt{d_F})/\mathbb{Q}_p$  in two different ways we find that  $M_i(\sqrt{d_F})/M_i$  is unramified as well. As  $\text{disc}(\mathbb{Q}_p(\sqrt{d_F})) = \text{disc}(F)$ , applying (1.32)(ii) we get

$$\mathfrak{d}_F^{2f(\mathfrak{q}_i|p)} = \mathfrak{d}_{M_i(\sqrt{d_F})} = \mathfrak{d}_{M_i}^2$$

from which we conclude

$$v_p(d_{M_i}) = v_p(d_F)f(\mathfrak{q}_i|p)$$

Since  $M_i/\mathbb{Q}_p$  is ramified if and only if  $\sigma_i\tau\sigma_i^{-1} \in H$ , then by (1.30) and (1.15) we have

$$\begin{aligned} v_p(d_M) &= \sum_{\substack{i=1 \\ \sigma_i\tau\sigma_i^{-1} \notin H}}^g v_p(d_{M_i}) \\ &= v_p(d_F) \sum_{\substack{i=1 \\ \sigma_i\tau\sigma_i^{-1} \notin H}}^g f(\mathfrak{q}_i|p) \\ &= v_p(d_F) \sum_{\substack{i=1 \\ \sigma_i\tau\sigma_i^{-1} \notin H}}^g \frac{|H\sigma_i D|}{2|H|} \end{aligned}$$

Now let us evaluate this sum in a different way. For each  $\sigma \in G$  there is a unique  $i$  such that  $\sigma \equiv \sigma_i \pmod{(H, D)}$ , moreover, since  $\mathfrak{q}_i := \sigma(\mathfrak{P}) \cap M$ , using again (1.15) we have

$$[\sigma_i I \sigma_i^{-1} : \sigma_i I \sigma_i^{-1} \cap H] = \frac{|H\sigma_i D|}{|H|f(\mathfrak{q}_i)} = \frac{|H\sigma D|}{|H|f(\mathfrak{q}_i)} = [\sigma I \sigma^{-1} : \sigma I \sigma^{-1} \cap H]$$

and thus  $\sigma\tau\sigma^{-1} \in H$  if and only if  $\sigma_i\tau\sigma_i^{-1} \in H$ , hence

$$\begin{aligned} \sum_{\substack{i=1 \\ \sigma_i\tau\sigma_i^{-1} \notin H}}^g |H\sigma_i D| &= \sum_{\substack{i=1 \\ \sigma_i\tau\sigma_i^{-1} \notin H}}^g \sum_{\sigma \equiv \sigma_i \pmod{(H, D)}} 1 \\ &= \sum_{i=1}^g \sum_{\substack{\sigma \equiv \sigma_i \pmod{(H, D)} \\ \sigma_i\tau\sigma_i^{-1} \notin H}} 1 \\ &= \sum_{i=1}^g \sum_{\substack{\sigma \equiv \sigma_i \pmod{(H, D)} \\ \sigma\tau\sigma^{-1} \notin H}} 1 \\ &= \#\{\sigma \in G : \sigma\tau\sigma^{-1} \notin H\} \end{aligned}$$

and therefore

$$v_p(d_M) = v_p(d_F) \cdot \frac{\#\{\sigma \in G : \sigma\tau\sigma^{-1} \notin H\}}{2|H|}$$

For each  $\theta = \sigma_0\tau\sigma_0^{-1} \in C_\tau - H$  we have

$$\{\sigma \in G : \sigma\tau\sigma^{-1} = \theta\} = \{\sigma \in G : (\sigma_0^{-1}\sigma)\tau(\sigma_0^{-1}\sigma)^{-1} = \tau\} = \sigma_0 \text{Stab}_G(\tau)$$

hence  $\#\{\sigma \in G : \sigma\tau\sigma^{-1} = \theta\} = |G|/|C_\tau|$  and

$$\#\{\sigma \in G : \sigma\tau\sigma^{-1} \notin H\} = |G| \cdot |C_\tau - H|/|C_\tau|$$

□

**Proposition 3.6.** Let  $K$  be number field with fundamental discriminant and degree  $n$ . Let  $\mathbb{Q} \subset M \subset \tilde{K}$  is an intermediate extension and identify  $H := \text{Gal}(\tilde{K}/M) \subset G_K$  with a subgroup of  $S_n \cong G_K$ . Then,

$$\mathfrak{d}_M = \mathfrak{d}_K^{c_H}$$

where  $c_H := [M : \mathbb{Q}] \frac{m_H}{n(n-1)}$  and  $m_H$  is the number of transposition not in  $H$ .

*Proof.* Let  $p$  be a rational prime. We will prove that

$$v_p(d_M) = v_p(d_K) \cdot c_H$$

by (3.2)(i) the extension  $\tilde{K}/\mathbb{Q}(\sqrt{d_K})$  is unramified, so  $N := \tilde{K}$ ,  $d = d_K$  and  $p$  satisfy the hypothesis of (3.5). Hence, if  $\tau$  is the generator of  $I_{\mathfrak{p}}$ , to compute  $v_p(d_M)$  it is enough to compute  $|C_\tau - H|/2|C_\tau|$  but since by (3.2)(ii)  $\tau$  is a transposition, then  $C_\tau$  is the set of all transpositions in  $S_n$ . Thus,  $|C_\tau - H| = m_H$ ,  $|C_\tau| = \binom{n}{2}$  and the claim follows. □

This shows for example that if  $K$  is a number field with fundamental discriminant and degree  $n$ , then (possibly up to a sign)  $d_{\tilde{K}} = d_K^{\frac{n!}{2}}$ .

## 3.2. Working with a compositum $KL$

### 3.2.1. Linear disjointness

Recall that two finite field extensions  $K/F$  and  $L/F$  inside a common extension  $\Omega/F$  are linearly disjoint if any of the following equivalent conditions holds (see [FJ08], Section 9.1).

- (a) The map  $K \otimes_F L \rightarrow KL$  induced by  $x \otimes y \mapsto xy$  is injective (and thus is an isomorphism).
- (b)  $K \otimes_F L$  is a field.
- (c)  $[KL : F] = [K : F][L : F]$ .

Moreover, if at least one extension is Galois, this is equivalent to  $L \cap K = F$ .

**Proposition 3.7.** Let  $K, L$  be number fields of the same degree  $n$  such that  $G_K \cong S_n$  and  $L/\mathbb{Q}$  has no intermediate extensions, then

$$K \not\cong L \iff K/\mathbb{Q} \text{ and } L/\mathbb{Q} \text{ are linearly disjoint}$$

*Proof.*  $\Leftarrow$ ): Suppose  $K$  and  $L$  are linearly disjoint, then  $K \not\cong L$ . Otherwise,

$$K \cong L \cong \mathbb{Q}[X]/(p(X))$$

for some  $p(X) \in \mathbb{Q}[X]$ , and tensoring with  $L$ , we get

$$K \otimes_{\mathbb{Q}} L \cong L[X]/(p(X))$$

which is not a field, since  $p(X)$  has a root in  $L$ .

$\Rightarrow$ ): Suppose  $K \not\cong L$ . To prove that  $K$  and  $L$  are linearly disjoint is enough to show that so are  $\tilde{K}$  and  $L$ . Indeed, if  $\tilde{K}$  and  $L$  are linearly disjoint, then the canonical map  $L \otimes_{\mathbb{Q}} \tilde{K} \rightarrow L\tilde{K}$  is an isomorphism and the commutativity of the diagram

$$\begin{array}{ccc} L \otimes_{\mathbb{Q}} K & \longrightarrow & LK \\ \downarrow & & \downarrow \\ L \otimes_{\mathbb{Q}} \tilde{K} & \longrightarrow & L\tilde{K} \end{array}$$

proves that  $L \otimes_{\mathbb{Q}} K \rightarrow LK$  is injective.

Since  $L$  has no intermediate extensions and  $\tilde{K}$  is normal, then  $L$  and  $\tilde{K}$  are linearly disjoint if and only if  $L \cap \tilde{K} = \mathbb{Q}$ , that is, if and only if  $L \not\subset \tilde{K}$ .

Now, if  $n \neq 6$  from the corollary to Hölder theorem (1.42) we know that every group of  $S_n$  of index  $n$  is conjugated to  $H_1 := \{\sigma \in S_n : \sigma(1) = 1\}$ . Therefore, in that case  $L \not\subset \tilde{K}$ , otherwise, the subgroups  $H_L := \text{Gal}(\tilde{K}/L)$  and  $H_K := \text{Gal}(\tilde{K}/K)$  of index  $n$  in  $G_K \cong S_n$  would be conjugated, contrary to our assumption.

On the other hand, if  $n = 6$  and  $L \subset \tilde{K}$ , as  $K \not\cong L$ , from Proposition 1.43 we have that  $H_L$  and  $H_K$  belong to the two different conjugacy classes of subgroups of index 6 in  $S_6$ . Since

$$36 = [G_K : H_K \cap H_L] = [G_K : H_K][G_K : H_L] = 6 \cdot 6$$

This shows that  $K$  and  $L$  are also linearly disjoint in this case.  $\square$

**Corollary 3.8.** Let  $K, L$  be number fields of degree  $n$  and fundamental discriminant, then the following are equivalent

- (i)  $K \not\cong L$
- (ii)  $K/\mathbb{Q}$  and  $L/\mathbb{Q}$  are linearly disjoint
- (iii)  $\tilde{K} \neq \tilde{L}$

*Proof.* From (3.2) we know that  $G_K \cong S_n$ , also  $L$  has no intermediate extensions, as  $G_L \cong S_n$  and  $\{\sigma \in S_n : \sigma(1) = 1\}$  is a maximal subgroup of  $S_n$ . Thus from (3.7) we have (i)  $\iff$  (ii). Clearly (iii)  $\Rightarrow$  (i), so remains to prove (i)  $\Rightarrow$  (iii).

Suppose (i) holds, then as we saw in the proof (3.7), the only case in which  $L \subset \tilde{K}$  is possible is if  $n = 6$  and  $\text{Gal}(\tilde{K}/L)$  and  $\text{Gal}(\tilde{K}/K)$  are the subgroups of  $\text{Gal}(\tilde{K}/\mathbb{Q}) \cong S_6$  corresponding to the two different conjugacy classes  $H_1$  and  $H_2$  of index 6 in  $S_6$ . However if that were the case, since  $d_L$  is fundamental, (3.6) implies  $c_{H_1} = 1 = c_{H_2}$ , and again by (3.6) this would imply that for every sextic field  $K$  with fundamental discriminant there exists a sextic field  $L \not\cong K$  with the same discriminant, which it is not true as example (3.9) shows. Hence  $L \not\subset \tilde{K}$  and in particular  $\tilde{L} \neq \tilde{K}$ .  $\square$

**Example 3.9.** The sextic field  $K$  with defining polynomial  $x^6 - x^5 + x^3 - x^2 + 1$  is the unique sextic field with discriminant  $-14731$ . In fact, the only other sextic field in  $\tilde{K}$  has discriminant  $-14731^3$ , hence, as a curious fact, (3.6) shows that for every sextic field  $K$  of fundamental discriminant there is a "twin" sextic field with the same Galois closure and discriminant  $d_K^3$ .

### 3.2.2. The Galois group

Suppose  $K$  is a field of degree  $n = 4$  such that  $G_K \cong S_4$ , the group  $S_4$  has a unique normal subgroup of order 4, namely,

$$V := \{\iota, (12)(34), (13)(24), (14)(23)\} \cong V_4$$

this group correspond to a unique normal sextic extension  $N/\mathbb{Q}$  inside  $\tilde{K}$ , since  $\text{Gal}(N/\mathbb{Q}) \cong S_4/V \cong S_3$ , there is exactly one cubic field (up to conjugation) inside  $N$  known as the **cubic resolvent** of  $K$  which we will denote  $R_3(K)$ . Remark that  $N$  is the Galois closure of  $R_3(K)$ , i.e.,  $N = \tilde{R}_3(K)$ .

**Lemma 3.10.** Let  $K \not\cong L$  be fields of the same fundamental discriminant and same degree  $n$ . Identify  $G_K \cong S_n$  as in Proposition 3.2. Under this identification the subgroup of  $G_K$  corresponding to  $\tilde{K} \cap \tilde{L}$  maps to

$$T := \begin{cases} V & \text{if } n = 4 \text{ and } R_3(K) \cong R_3(L) \\ A_n & \text{otherwise} \end{cases}$$

*Proof.* Since  $M/\mathbb{Q}$  is Galois,  $T$  is normal in  $S_n$ . Moreover,  $T$  is proper because  $\mathbb{Q}(\sqrt{d_K}) \subset M$  (and thus  $T \subset A_n$ ). Also  $T$  is non trivial, otherwise,  $\tilde{K} \cap \tilde{L} = M = \tilde{K}$  and  $\tilde{L} \subset \tilde{K}$  which, as both fields have the same degree, implies  $\tilde{L} = \tilde{K}$  contradicting (3.8). Hence if  $n \neq 4$  we have  $T = A_n$ . Now if  $n = 4$ , since by definition the field  $\tilde{R}_3(K)$  is the fixed field of the unique normal subgroup of  $G_K$  of order 4, then

$$\begin{aligned} T = V &\iff T \subset V \\ &\iff \tilde{R}_3(K) \subset \tilde{K} \cap \tilde{L} \\ &\iff \tilde{R}_3(K) \subset \tilde{L} \\ &\iff \tilde{R}_3(K) = \tilde{R}_3(L) \\ &\iff R_3(K) \cong R_3(L) \end{aligned}$$

□

**Proposition 3.11.** Let  $K \not\cong L$  be fields of the same fundamental discriminant and same degree  $n$ . Write  $K = \mathbb{Q}(\alpha)$  and  $L = \mathbb{Q}(\beta)$ , then there exists an indexing of the conjugates of  $\alpha$  and  $\beta$ , say  $\{\alpha_1, \dots, \alpha_n\}$  and  $\{\beta_1, \dots, \beta_n\}$ , such that  $\alpha_1 = \alpha$ ,  $\beta_1 = \beta$  and the natural action of  $G_{KL}$  on  $\{\alpha_1, \dots, \alpha_n\}$  and  $\{\beta_1, \dots, \beta_n\}$  induces an isomorphism

$$\Phi : G_{KL} \xrightarrow{\sim} S_n \times_T S_n := \{(\sigma_1, \sigma_2) \in S_n \times S_n : \sigma_1 \sigma_2^{-1} \in T\}$$

where  $T$  is as in (3.10).

*Proof.* Start with an arbitrary indexing,  $\{\alpha_1, \dots, \alpha_n\}$  and  $\{\beta'_1, \dots, \beta'_n\}$ , of the conjugates of  $\alpha$  and  $\beta$  such that  $\alpha_1 := \alpha$  and  $\beta'_1 := \beta$ . This define isomorphisms  $\phi : G_K \xrightarrow{\sim} S_n$  and  $\psi' : G_L \xrightarrow{\sim} S_n$  given by  $\phi(\sigma)(i) = j$  whenever  $\sigma \alpha_i = \alpha_j$  and  $\psi'(\tau)(i) = j$  if  $\tau \beta'_i = \beta'_j$ .

By the above lemma, the map  $\phi$  induces an isomorphism  $\bar{\phi} : \text{Gal}(\tilde{K} \cap \tilde{L}/\mathbb{Q}) \xrightarrow{\sim} S_n/T$ . More specifically, given  $\gamma \in \text{Gal}(\tilde{K} \cap \tilde{L}/\mathbb{Q})$  we have  $\bar{\phi}(\gamma) = \phi(\sigma)T$ . Where  $\sigma \in G_K$  is any extension of  $\gamma$  to all  $\tilde{K}$ . Similarly  $\psi'$  induces an isomorphism  $\bar{\psi}' : \text{Gal}(\tilde{K} \cap \tilde{L}/\mathbb{Q}) \xrightarrow{\sim} S_n/T$ .

Since  $S_n/T$  is isomorphic to either  $S_2$  if  $T = A_n$  or to  $S_3$  if  $T = V$ , by Hölder's theorem (1.41), we have that

$$\text{Aut}(S_n/T) = \text{Inn}(S_n/T),$$

thus there exists  $\pi \in S_n$  such that the automorphism  $\bar{\phi} \circ \bar{\psi}'^{-1} : S_n/T \rightarrow S_n/T$  is conjugation by  $\pi T$ . Moreover, since  $T \leq S_n$  is transitive, there exists  $\nu \in T$  such that  $\nu(1) = \pi^{-1}(1)$ , so by replacing  $\pi$  with  $\pi\nu$  we may assume that  $\pi(1) = 1$ .

Let us reindex the set  $\{\beta'_1, \dots, \beta'_n\}$  as  $\{\beta_1, \dots, \beta_n\}$ , where  $\beta_i = \beta'_{\pi(i)}$ , note that  $\beta_1 = \beta'_1 = \beta$ . This gives us a new isomorphism  $\psi : G_K \xrightarrow{\sim} S_n$  defined as  $\psi(\tau)(i) = j$  if  $\tau \beta_i = \beta_j$ . And by

definition  $\psi(\tau) = \pi\psi'(\tau)\pi^{-1}$ . Hence for each  $\tau \in G_L$ , taking  $\gamma := \tau \upharpoonright_{\tilde{K} \cap \tilde{L}} \in \text{Gal}(\tilde{K} \cap \tilde{L}/\mathbb{Q})$  we get

$$\begin{aligned} \bar{\phi}(\gamma) &= (\pi T)\bar{\psi}'(\gamma)(\pi T)^{-1} \\ &= \pi\psi'(\tau)\pi^{-1}T \\ &= \psi(\tau)T \\ &= \bar{\psi}(\gamma) \end{aligned}$$

from which it follows that  $\bar{\phi} = \bar{\psi}$ .

Now the restriction maps make the diagram

$$\begin{array}{ccc} G_{KL} & \longrightarrow & G_L \\ \downarrow & & \downarrow \\ G_K & \longrightarrow & \text{Gal}(\tilde{K} \cap \tilde{L}/\mathbb{Q}) \end{array}$$

a pullback square. But we just proved that with this indexing of the conjugates of  $\beta$  and  $\alpha$  the maps  $\phi$ ,  $\psi$  and  $\bar{\phi} = \bar{\psi}$ , give an isomorphism between the diagram  $G_K \rightarrow \text{Gal}(\tilde{K} \cap \tilde{L}/\mathbb{Q}) \leftarrow G_L$  and the diagram  $S_n \rightarrow S_n/T \leftarrow S_n$ , therefore the natural map  $\Phi$  is an isomorphism between their respective limits (pullbacks)  $G_{KL}$  and  $S_n \times_T S_n$ . □

An immediate consequence of (3.11) is the following

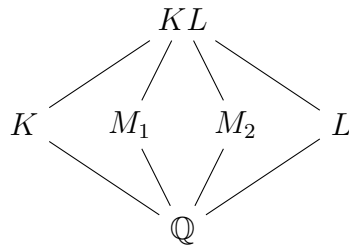
**Corollary 3.12.** Let  $K \not\cong L$  be number fields of the same fundamental discriminant and same degree  $n$ . The structure of the lattice of subfields  $\mathbb{Q} \subset M \subset KL$  depends only on  $n$  and on whether or not  $R_3(K) \cong R_3(L)$  when  $n = 4$ .

*Proof.* Under the isomorphism  $\Phi$  of (3.11) we have that the subgroup of  $G_{KL}$  corresponding to  $KL$  maps to

$$\{(\sigma_1, \sigma_2) \in S_n \times_T S_n : \sigma_1(1) = 1 = \sigma_2(1)\}$$

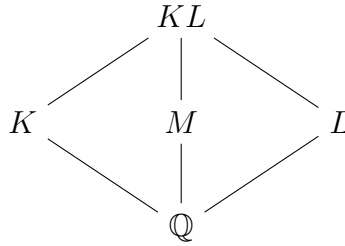
and the lattice of subgroups  $S_n \times_T S_n$  containing this group depends only on  $n$  and  $T$ . □

**Example 3.13.** (a) Let  $K$  and  $L$  be the cubic fields with defining polynomials  $x^3 - 16x - 27$  and  $x^3 - x^2 + 3x + 10$ , respectively. Then  $K \not\cong L$ ,  $d_K = -3299 = d_L$ , and the lattice of subfields of  $KL$  is



where  $M_1$  is the field with defining polynomial  $x^3 + 2x - 11$  and discriminant  $-3299$ , and  $M_2$  is the field with defining polynomial  $x^3 - x^2 + 9x - 8$  and discriminant  $-3299$ . It follows from (3.12) that this is the lattice structure for the compositum of every pair of non isomorphic cubic fields of the same fundamental discriminant.

- (b) Let  $K$  and  $L$  be the quartic fields with defining polynomials  $x^4 - x^3 - 2x^2 + 4x + 1$  and  $x^4 + 4x^2 - 5x + 1$ , respectively. Then  $K \not\cong L$ ,  $d_K = -6571 = d_L$ ,  $R_3(K) \cong R_3(L)$  is the cubic field with defining polynomial  $x^3 - x^2 - 9x - 16$  and the lattice of subfields of  $KL$  is



where  $M$  is the field with defining polynomial  $x^4 - 2x^2 - 3x + 2$  and discriminant  $-6571$ . It follows from (3.12) that this is the lattice structure for the compositum of every pair of non isomorphic quartic fields of the same fundamental discriminant and same cubic resolvent.

### 3.2.3. Discriminants of intermediate fields

**Proposition 3.14.** Let  $K \not\cong L$  be number fields of the same fundamental discriminant and same degree  $n$  and  $\Phi : G_{KL} \xrightarrow{\sim} S_n \times_T S_n$  be as in (3.11). Then,

- (i) The extension  $\widetilde{KL}/\mathbb{Q}(\sqrt{d_K})$  is unramified at all finite primes.
- (ii) Let  $\mathfrak{P}$  be a prime in  $\widetilde{KL}$  ramified over  $\mathbb{Q}$  and let  $\tau$  be the generator of its the inertia group  $I_{\mathfrak{P}}$ , then  $\Phi(\tau) = (\tau_1, \tau_2) \in S_n \times_T S_n$  with  $\tau_1$  and  $\tau_2$  transpositions. Moreover, the conjugacy class  $C$  of  $(\tau_1, \tau_2)$  in the group  $S_n \times_T S_n$  is given by

$$C = \{(\rho_1, \rho_2) \in S_n \times S_n : \rho_1 \text{ and } \rho_2 \text{ are transpositions either equal or disjoint}\}$$

if  $n = 4$  and  $R_3(K) \cong R_3(L)$ , or

$$C = \{(\rho_1, \rho_2) \in S_n \times S_n : \rho_1 \text{ and } \rho_2 \text{ are transpositions}\}$$

in any other case.

*Proof.* The statement (i) is consequence of (1.16) and the fact that both  $\widetilde{K}/\mathbb{Q}(\sqrt{d_K})$  and  $\widetilde{L}/\mathbb{Q}(\sqrt{d_K})$  are unramified at all finite primes. To prove that  $\tau_1$  and  $\tau_2$  are transpositions,

recall that as both  $\mathfrak{P} \cap \tilde{K}$  and  $\mathfrak{P} \cap \tilde{L}$  are ramified over  $\mathbb{Q}$  the groups  $\phi(I_{\mathfrak{P} \cap \tilde{K}})$  and  $\psi(I_{\mathfrak{P} \cap \tilde{L}})$  are generated by transpositions (by (3.2)(ii)). Now

$$(\tau_1, \tau_2) \in \phi(I_{\mathfrak{P} \cap \tilde{K}}) \times \psi(I_{\mathfrak{P} \cap \tilde{L}})$$

so either  $\tau_i = 1$  or  $\tau_i$  is a transposition and, as  $\tau_1 \tau_2^{-1} \in T \subset A_n$ , either they are both transpositions or they are both 1, the latter not being possible since  $\Phi(\tau)$  has order 2.

Next we prove that the conjugacy class  $C$  of  $(\tau_1, \tau_2)$  in  $S_n \times_T S_n$  is as described:

- Suppose  $n = 4$  and  $R_3(K) \cong R_3(L)$ . Let  $(\rho_1, \rho_2) \in C$ , since  $\tau_1$  and  $\tau_2$  are transpositions and every conjugate in  $S_n$  of a transposition is a transposition, we have that both  $\rho_1$  and  $\rho_2$  are transpositions, moreover since

$$\rho_1 \rho_2^{-1} \in \{1, (12)(34), (13)(24), (14)(23)\} = T$$

then  $\rho_1$  and  $\rho_2$  are either equal or disjoint, otherwise,  $\rho_1 \rho_2^{-1}$  would be a three cycle, in particular,  $\tau_1$  and  $\tau_2$  are either equal or disjoint. Conversely, suppose  $\rho_1$  and  $\rho_2$  are transpositions either equal or disjoint, then we claim that  $(\rho_1, \rho_2)$  is conjugated to  $((12), (12))$  in  $S_4 \times_T S_4$ . Indeed, if  $\rho_1 = \rho_2 = \rho$  then taking  $\sigma \in S_n$  such that  $\sigma(12)\sigma^{-1} = \rho$  we find that  $(\sigma, \sigma) \in S_n \times_T S_n$  and  $(\sigma, \sigma)((12), (12))(\sigma, \sigma)^{-1} = (\rho_1, \rho_2)$ ; and if  $\rho_1 = (ij)$  and  $\rho_2 = (kl)$  with  $\{i, j\} \cap \{k, l\} = \emptyset$  then the permutations  $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & k & l \end{pmatrix}$  and  $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ k & l & i & j \end{pmatrix}$  are such that  $\sigma_1 \sigma_2^{-1} = (ik)(jl) \in T$  and  $(\sigma_1, \sigma_2)(12)(\sigma_1, \sigma_2)^{-1} = ((ij), (kl)) = (\rho_1, \rho_2)$ .

- Now suppose  $n \neq 4$  or  $R_3(K) \not\cong R_3(L)$ . Again, as  $\tau_1$  and  $\tau_2$  are transpositions given  $(\rho_1, \rho_2) \in C$  both  $\rho_1$  and  $\rho_2$  are transpositions. Conversely, let  $(\rho_1, \rho_2)$  be a pair of transpositions, then we must find a pair  $(\sigma_1, \sigma_2) \in S_n$  such that  $\text{sgn}(\sigma_1) = \text{sgn}(\sigma_2)$  and

$$(\sigma_1, \sigma_2)(\tau_1, \tau_2)(\sigma_1, \sigma_2)^{-1} = (\rho_1, \rho_2)$$

but this follows from the fact that any pair transpositions  $\rho$  and  $\tau$  in  $S_n$  are conjugated by an element in  $A_n$ , indeed, this can be check directly for  $n = 2, 3$  and if  $n \geq 4$  we can write  $\rho = \sigma \tau \sigma^{-1}$  with  $\sigma \in S_n$ . If  $\sigma \in A_n$  we are done and if  $\sigma \notin A_n$  we can choose  $\pi$  a transposition disjoint from  $\tau$  (since  $n \geq 4$ ), thus  $\sigma \pi \in A_n$  and  $(\sigma \pi) \tau (\sigma \pi)^{-1} = \sigma \tau \sigma^{-1} = \rho$ .

□

**Proposition 3.15.** Let  $K \not\cong L$  be number fields of the same fundamental discriminant and same degree  $n$  and  $\Phi : G_{KL} \xrightarrow{\sim} S_n \times_T S_n$  be as in (3.11). If  $\mathbb{Q} \subset M \subset \tilde{K}\tilde{L}$  is an intermediate extension with Galois group  $\text{Gal}(\tilde{K}/M)$  corresponding to  $H \leq S_n \times_T S_n$  under  $\Phi$ . Then,

$$\mathfrak{d}_M = \mathfrak{d}_K^{c_H}$$

where  $c_H := [M : \mathbb{Q}] \frac{|C - H|}{2|C|}$  and  $C$  is as in (3.14)(ii).

*Proof.* This follows directly from (3.14), since for every rational prime  $p$  we know from (3.14)(i) that  $N := \widetilde{KL}$ ,  $d := \text{disc}(K)$  and  $p$  satisfy the hypothesis of (3.5) combining this the computation in (3.14)(ii) we conclude

$$v_p(d_M) = v_p(d_K) \cdot [M : \mathbb{Q}] \frac{|C - H|}{2|C|}$$

□

**Corollary 3.16.** The discriminant ideal of every intermediate extension  $\mathbb{Q} \subset M \subset KL$  is a perfect power of  $\mathfrak{d}_K$  and the exponent only depends on  $n$  and on whether or not  $R_3(K) \cong R_3(L)$  for  $n = 4$ .

**Corollary 3.17.** With  $K$  and  $L$  as above

$$d_{KL} = d_K^{2(n-1)}$$

*Proof.* In this case  $H = \{(\sigma_1, \sigma_2) \in S_n \times_T S_n : \sigma_1(1) = 1 = \sigma_2(1)\}$  so:

- If  $n = 4$  and  $R_3(K) \cong R_3(L)$ , then  $C \cap H$  is the set of pairs  $(\tau_1, \tau_2)$  such that  $\tau_1$  and  $\tau_2$  are transpositions either equal or disjoint both fixing 1, since there are not any pair of disjoint transpositions in  $S_4$  both fixing 1 and there are  $\binom{3}{2} = 3$  transpositions in  $S_4$  fixing 1, then  $|C \cap H| = 3$ , thus

$$|C - H| = |C| - |C \cap H| = 12 - 3 = 9$$

and therefore  $c_H = [KL : \mathbb{Q}](9/2 \cdot 12) = 4^2(3/8) = 6 = 2 \cdot 3$ .

- If  $n \neq 4$  or  $R_3(K) \not\cong R_3(L)$ , then  $C \cap H$  is the set of pair  $(\tau_1, \tau_2)$  such that  $\tau_1$  and  $\tau_2$  are transpositions fixing 1, hence  $C \cap H = \binom{n-1}{2}^2$ , thus

$$|C - H| = |C| - |C \cap H| = \binom{n}{2}^2 - \binom{n-1}{2}^2 = (n-1)^3$$

and therefore  $c_H = [KL : \mathbb{Q}](n-1)^3/2\binom{n}{2}^2 = 2(n-1)$ . This proves  $\mathfrak{d}_{KL} = \mathfrak{d}_K^{2(n-1)}$ . Since  $d_K^{2(n-1)} > 0$ , it remains to prove that  $d_{KL}$  is positive. As  $K$  and  $L$  are linearly disjoint, then  $s_{KL} = s_K[L : \mathbb{Q}] + s_L[K : \mathbb{Q}] - 2s_K s_L = (s_K + s_L)n - 2s_K s_L$ . Where  $s_K$  denotes the number of complex embeddings of  $K$ . But by hypothesis  $d_K = d_L$ , thus  $s_K \equiv s_L \pmod{2}$  and therefore  $s_{KL} \equiv 0 \pmod{2}$ .

□

### 3.2.4. Lattice of subfield of $KL/\mathbb{Q}$ .

The group  $G := S_n \times_{A_n} S_n$  act naturally on the set  $\Omega := \{1, \dots, n\} \times \{1, \dots, n\}$  by

$$(\sigma_1, \sigma_2) \cdot (i, j) = (\sigma_1(i), \sigma_2(i))$$

this action is clearly transitive, since  $(\tau_1, \tau_2) \in G$  for every pair of transpositions in  $S_n$ .

Now let  $K \not\cong L$  be number fields of the same fundamental discriminant and same degree  $n$ . Remark that, when  $G_{KL} \cong G$ , the stabilizer in  $G$  of  $(1, 1)$  by this action

$$G_{(1,1)} = \{(\sigma_1, \sigma_2) \in G : \sigma_1(1) = 1 = \sigma_2\}$$

is the subgroup of  $G$  corresponding to  $\text{Gal}(\widetilde{KL}/KL)$  under the isomorphism  $\Phi$  of (3.11). Now by (1.39) the subgroups of  $G$  containing  $G_{(1,1)}$  are in one to one correspondence with the blocks of this action on  $\Omega$ , and by Galois theory this are in one to one correspondence to the subfields of  $KL/\mathbb{Q}$ , thus, when  $n \neq 4$  or  $R_3(K) \not\cong R_3(L)$ , to describe the lattice of subfields of  $KL/\mathbb{Q}$  equivalent to describe the blocks of the action. This is done for  $n \geq 4$  in the following lemma.

**Lemma 3.18.** Suppose  $n \geq 4$ . The blocks of the natural action of  $S_n \times_{A_n} S_n$  in  $\Omega$  containing  $(1, 1)$  are  $\Delta_0 := \{(1, 1)\}$ ,  $\Delta_1 := \{1\} \times \{1, \dots, n\}$ ,  $\Delta_2 := \{1, \dots, n\} \times \{1\}$  and  $\Omega$ .

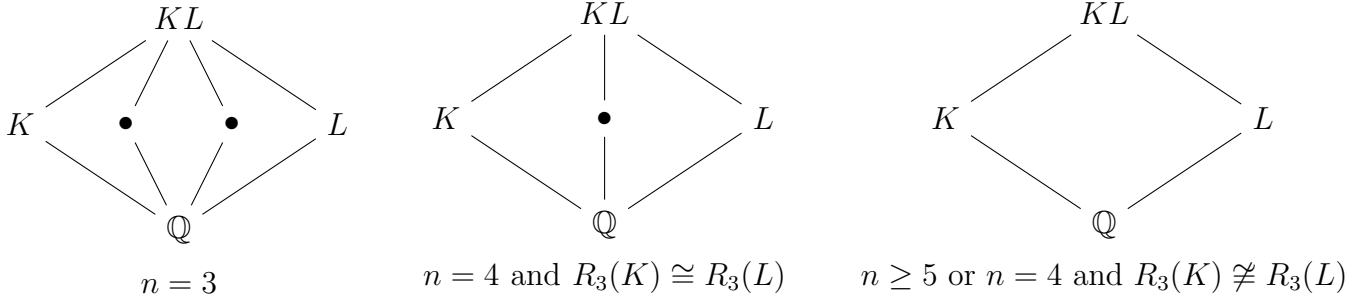
*Proof.* First we observe that  $\Delta_1$  and  $\Delta_2$  are indeed blocks because if  $(\sigma_1, \sigma_2) \cdot \Delta_1 \cap \Delta_1 \neq \emptyset$ , then  $\sigma_1(1) = 1$  and thus  $(\sigma_1, \sigma_2) \cdot \Delta_1 = \Delta_1$  (similarly we see that  $\Delta_2$  is a block). Moreover,  $\Delta_1$  and  $\Delta_2$  are maximal blocks, since for example if  $\Delta_1 \subset \Delta \subsetneq \Omega$  and  $(r, s) \notin \Delta$ , then given  $(i, j) \in \Delta$  we must have  $i = 1$ , otherwise, we may take  $\sigma_1 \in S_n$  such that  $\sigma_1(i) = r$  and  $\sigma_1(1) = 1$  (note that  $r \neq 1$ ), also we can choose  $\sigma_2 \in S_n$  such that  $\sigma_2(j) = s$  with  $\text{sgn}(\sigma_2) = \text{sgn}(\sigma_1)$  (since  $n \geq 3$ ), but then  $(\sigma_1, \sigma_2) \cdot (1, 1) = (1, \sigma_2(1)) \in \Delta_1 \subset \Delta$  and  $(\sigma_1, \sigma_2) \cdot (i, j) = (r, s) \notin \Delta$ , contradicting that  $\Delta$  is a block.

Let  $\Delta \neq \Omega, \Delta_1, \Delta_2$  be a block we need to prove that  $\Delta = \Delta_0$ . As  $\Delta_1$  and  $\Delta_2$  are maximal, then  $\Delta \not\supset \Delta_1, \Delta_2$ , that is, exists  $(1, k) \notin \Delta$  and  $(i, 1) \notin \Delta$ . We claim this implies that for  $(a, b) \in \Delta$  we have  $a \neq 1 \iff b \neq 1$ : Suppose  $a \neq 1$  and  $b = 1$ , then  $a \neq i$  and  $\tau = (ai)$  fixes 1, hence  $(\tau, \tau) \cdot (1, 1) = (1, 1) \in \Delta$  but  $(\tau, \tau)(a, 1) = (i, 1) \notin (\tau, \tau) \cdot \Delta$ , contradicting that  $\Delta$  is a block, by symmetry of the argument  $b \neq 1$  also implies  $a \neq 1$ .

Now let  $(a, b) \in \Delta$  and suppose  $(a, b) \neq (1, 1)$ , then by the above claim  $a \neq 1$  and  $b \neq 1$ . Let  $\pi$  be transposition disjoint form  $(1a)$  (which exists as  $n \geq 4$ ) and let  $c \notin \{b, 1\}$ , then  $\sigma := ((1a)\pi, (1bc)) \in S_n \times_{A_n} S_n$  and  $\sigma \cdot (1, 1) = (a, b) \in \Delta$  but  $\sigma \cdot (a, b) = (1, c) \notin \Delta$  (since  $c \neq 1$ ), a contradiction. Thus,  $\Delta = \{(1, 1)\} = \Delta_0$ .  $\square$

We conclude with the main result of the chapter.

**Theorem 3.19.** *Let  $K \not\cong L$  be number fields of the same fundamental discriminant and same degree  $n$ . Then, the Hasse diagram of the lattice of subfields of  $KL/\mathbb{Q}$  is given by*



where  $\bullet$  stands for a field of degree  $n$  and discriminant of absolute value  $|\text{disc}(K)|$ . Moreover,  $\text{disc}(KL) = \text{disc}(K)^{2(n-1)}$ .

*Proof.* As mention before in (3.12) and (3.16) both the lattice structure and the discriminants ideals of the intermediate fields depend only on  $n$  and on whether or not  $R_3(K) \not\cong R_3(L)$ ; thus for  $n = 3$  or  $n = 4$  and  $R_3(K) \cong R_3(L)$  it is enough to check the theorem in a particular case, this was done in Example 3.13. So let us suppose  $n \geq 5$  or  $n = 4$  and  $R_3(K) \not\cong R_3(L)$ , then we have the following order-preserving correspondences (except for the first one which is order-reversing)

$$\begin{aligned}
 \{\text{subfields } M : \mathbb{Q} \subset M \subset KL\} &\longleftarrow \{\text{subgroups } H : \text{Gal}(\widetilde{KL}/\mathbb{Q}) \supset H \supset \text{Gal}(\widetilde{KL}/KL)\} \\
 &\xleftarrow{\Phi} \{\text{subgroups } H : S_n \times_{A_n} S_n \supset H \supset G_{(1,1)}\} \\
 &\xleftarrow{(1.39)} \{\text{blocks } \Delta : \Omega \supset \Delta \supset \{(1,1)\}\}
 \end{aligned}$$

Now the theorem follows from (3.18), as these blocks have the desired lattice structure. The claim about  $\text{disc}(KL)$  is Corollary 3.17. □

# 4 Casimir pairings and proofs of the mains theorems

The Casimir element or Casimir invariant of a Lie algebra  $\mathfrak{g}$  is a powerful tool in the theory of representation of Lie algebras. It is named after Hendrik Casimir a physicist who discovered the concept in the context of rigid body dynamics. One of the reasons this invariant is so important is the crucial role that plays in the algebraic proof of Weyl's theorem on complete reducibility and in the proof of the Weyl character formula, see [Hal15, Chapter 10]. Weyl's original proof of the theorem on complete reducibility was of analytical nature and it only applied to complex Lie algebras. The introduction of the Casimir element greatly simplified the proof and generalized the theorem to any field of characteristic 0.

The concept can be defined in a more general setting. And in this chapter we see how we can use it in the context of trace forms of fields to answer the questions that were presented in the introduction.

## 4.1. Definition and examples

Let  $V$  be a finite dimensional vector space over a field  $F$  and let  $V^* := \text{Hom}_F(V, F)$  be its dual. Since  $V$  has finite dimension, we have  $V \cong V^*$ , moreover, each non degenerated bilinear form  $B : V \times V \rightarrow F$  induces an isomorphism

$$\Gamma : V \rightarrow V^*, v \mapsto B(v, \cdot)$$

and every such isomorphism is obtained in this way.

Now let  $R$  be an  $F$ -algebra and let  $\phi, \psi \in \text{Hom}_F(V, R)$ . The map

$$V^* \times V \rightarrow R, (f, v) \mapsto (\psi \circ \Gamma^{-1})(f)\phi(v)$$

is bilinear and  $F$ -balanced (as  $R$  is an  $F$ -algebra), hence it lifts to a morphism  $V \otimes_F V^* \rightarrow R$ . If we compose this with the inverse of the canonical isomorphism

$$V^* \otimes V \xrightarrow{\sim} \text{End}_F(V), f \otimes v \mapsto (u \mapsto f(u)v) \tag{1}$$

we get an  $F$ -linear map  $\rho_{B, \psi, \phi} : \text{End}_F(V) \rightarrow R$ .

**Definition 4.1.** The  $B$ -Casimir element of  $\psi$  and  $\phi$  is the element  $c_B(\psi, \phi) \in R$  given by the image under  $\rho_{B, \psi, \phi}$  of the identity morphism;

$$c_B(\psi, \phi) := \rho_{B, \psi, \phi}(1).$$

The element  $c_B(\psi, \phi)$  turns out to be very useful in many contexts and is the key in the proofs of our results. To write it more explicitly let  $\{v_1, \dots, v_n\}$  be an  $F$ -basis of  $V$ , then

$$c_B(\psi, \phi) = \sum_{i=1}^n \psi(v_i^*) \phi(v_i) \quad (2)$$

where  $\{v_1^*, \dots, v_n^*\} \subset V$  is the dual basis of  $\{v_1, \dots, v_n\}$  with respect to  $B$ , i.e, the inverse image through  $\Gamma$  of the basis  $\{f_1, \dots, f_n\}$  of  $V^*$  defined by  $f_i(v_j) = \delta_{ij}$ . To prove this, observe that  $\sum_i f_i \otimes v_i$  maps to  $1 \in \text{End}_F(V)$  under the isomorphism (1). Notice that this representation is independent on the choice of the basis  $\{v_i\}$ .

**Example 4.2.** Let  $\mathfrak{g}$  be an  $n$ -dimensional Lie algebra over a field  $F$  with  $\text{char}(F) = 0$ , by Cartan criterion, the Killing form  $B$  on  $\mathfrak{g}$  is non degenerate if and only if  $\mathfrak{g}$  is semisimple. In that case, if we take  $V = \mathfrak{g}$ ,  $R = U(\mathfrak{g})$  its universal enveloping algebra and  $\iota : \mathfrak{g} \hookrightarrow U(\mathfrak{g})$  the canonical inclusion, then

$$C := c_B(\iota, \iota) \in U(\mathfrak{g})$$

is the well known **quadratic Casimir element** or **Casimir invariant** of  $\mathfrak{g}$ .

**Definition 4.3.** Let  $F$  be a field  $V$  an  $F$ -vector space of finite dimension,  $R$  an  $F$ -algebra and  $B : V \times V \rightarrow F$  a nondegenerate bilinear form. The **Casimir pairing** associated to  $B$  is the map

$$\langle \cdot, \cdot \rangle_B : \text{Hom}_F(V, R) \times \text{Hom}_F(V, R) \rightarrow R, \quad (\psi, \phi) \mapsto \langle \psi, \phi \rangle_B := c_B(\psi, \phi)$$

**Remark 4.4.** Notice that  $\langle \cdot, \cdot \rangle_B$  is  $D$ -bilinear where  $D = Z(R)$  is the center of  $R$ .

We gather some of the properties of the Casimir pairing, which follow immediately from its definition, as

**Proposition 4.5.** Let  $F, V, R$  and  $B$  be as above

- (i) If  $R$  is commutative and  $B$  is symmetric, then  $\langle \cdot, \cdot \rangle_B$  is also symmetric.
- (ii) If  $\theta : R \rightarrow R'$  is a homomorphism of  $F$ -algebras then

$$\theta(\langle \psi, \phi \rangle_B) = \langle \theta \circ \psi, \theta \circ \phi \rangle_B$$

- (iii) If  $F \subset F'$  is a field extension, then

$$\langle \psi \otimes \mathbf{1}_{F'}, \phi \otimes \mathbf{1}_{F'} \rangle_{B \otimes F'} = \langle \psi, \phi \rangle_B \otimes 1 \in R \otimes F'$$

*Proof.* The only non trivial part is (i). Let  $\{v_i\}$  be a basis of  $V$ . Recall that the dual basis  $\{v_i^*\}$  of  $\{v_i\}$  with respect to  $B$  is uniquely defined by the relation  $B(v_i^*, v_j) = \delta_{ij}$ . Hence if  $B$  is symmetric then  $\{v_i\}$  is the dual basis of  $\{v_i^*\}$ , and thus, as the representation in (2) was independent of the basis, we obtain

$$\langle \psi, \phi \rangle_B = \sum_{i=1}^n \psi(v_i^*)\phi(v_i) = \sum_{i=1}^n \psi(v_i)\phi(v_i^*) = \sum_{i=1}^n \phi(v_i^*)\psi(v_i) = \langle \phi, \psi \rangle_B$$

□

Let  $V$  be an  $F$ -vector space of dimension  $n$  and  $R$  an  $F$ -algebra, then just as in (1) we have a canonical isomorphism

$$\mathrm{Hom}_F(V, R) \cong V^* \otimes_F R \cong F^n \otimes_F R \cong R^n$$

In particular, if  $R$  is an integral domain and  $(V, B)$  is a nondegenerate quadratic space, then according to point (i) of the above proposition  $\mathrm{Hom}_F(V, R)$  becomes a quadratic  $R$ -module, when endowed with the symmetric bilinear form  $\langle \cdot, \cdot \rangle_B$ . The following proposition shows that this assignation is functorial.

**Proposition 4.6.** Let  $(V, B_V)$  and  $(W, B_W)$  be non degenerated quadratic  $F$ -spaces, then an  $F$ -linear map  $\phi : V \rightarrow W$  is an isometry if and only if

$$\mathrm{Hom}_F(\phi, R) : \mathrm{Hom}_F(W, R) \rightarrow \mathrm{Hom}_F(V, R), \quad \tau \mapsto \tau \circ \phi$$

is an isomorphism of  $R$ -modules which respects the Casimir pairings  $\langle \cdot, \cdot \rangle_{B_V}$  and  $\langle \cdot, \cdot \rangle_{B_W}$ . Therefore, when  $R$  is an integral domain,  $\phi$  is an isometry of quadratic  $F$ -spaces if and only if  $\mathrm{Hom}_F(\phi, R)$  is an isometry of  $R$ -quadratic modules.

*Proof.* First suppose  $\phi : V \rightarrow W$  is an isometry. Take  $\{v_i\}$  any basis of  $V$  with dual basis  $\{v_i^*\}$  with respect to  $B_V$ . As  $\phi$  is an isometry, it follows that  $\{\phi(v_i^*)\}$  is the dual basis of  $\{\phi(v_i)\}$  with respect to  $B_W$ . Let  $\Phi := \mathrm{Hom}_F(\phi, R)$ , as  $\phi$  is an isomorphism, so is  $\Phi$  and

$$\begin{aligned} \langle \Phi(\tau_1), \Phi(\tau_2) \rangle_{B_V} &= \langle \tau_1 \circ \phi, \tau_2 \circ \phi \rangle_{B_V} \\ &= \sum_i \tau_1(\phi(v_i^*))\tau_2(\phi(v_i)) \\ &= \langle \tau_1, \tau_2 \rangle_{B_W} \end{aligned}$$

for all  $\tau_1, \tau_2 \in \mathrm{Hom}_F(W, R)$ , i.e.,  $\Phi$  preserves the Casimir pairings.

Conversely suppose  $\Phi$  is an isomorphism preserving the Casimir pairings. First we prove that  $\phi$  must be bijective. Indeed, we have a commutative diagram

$$\begin{array}{ccc}
\mathrm{Hom}_F(W, R) & \xrightarrow{\Phi} & \mathrm{Hom}_F(V, R) \\
\downarrow & & \downarrow \\
W^* \otimes R & \xrightarrow{\phi^* \otimes \mathbf{1}_R} & V^* \otimes R
\end{array}$$

(where the vertical maps are canonical isomorphisms) so  $\phi^* \otimes \mathbf{1}_R$  is bijective, but  $R$  is faithfully flat as an  $F$ -module (being free), thus  $\phi^*$  is bijective and it is well known that the dual map  $\phi^*$  is bijective if and only if so is  $\phi$ .

Now let  $\{e_i\}$  be an orthogonal basis of  $V$  with  $a_i := B_V(e_i, e_i)$  so that  $e_i^* = e_i/a_i$ , let  $w_i := \phi(e_i)$  and let  $\tau_i \in \mathrm{Hom}_F(W, R)$  be defined by  $\tau_i(w_j) = \delta_{ij}$ . Then, for every  $\tau \in \mathrm{Hom}_F(W, R)$

$$\langle \tau \circ \phi, \tau_i \circ \phi \rangle_{B_V} = \sum_k \tau(\phi(e_k^*)) \tau_i(\phi(e_k)) = \tau(w_i/a_i)$$

$$\langle \tau, \tau_i \rangle_{B_W} = \sum_k \tau(w_k^*) \tau_i(w_k) = \tau(w_i^*)$$

since  $\Phi$  preserves the Casimir pairings, it follows that  $\tau(w_i/a_i) = \tau(w_i^*)$  for all  $\tau \in \mathrm{Hom}_F(V, R)$ , therefore  $w_i^* = w_i/a_i$ , i.e.,  $B_W(w_i, w_j) = a_i \delta_{ij} = B_V(e_i, e_j)$  which proves that  $\phi$  is an isometry.  $\square$

If we specialize this down to our case of interest things get much more interesting. Recall that if  $K/F$  is a finite extension of fields, then the trace form

$$\mathrm{tr}_{K/F} : K \times K \mapsto F, \quad x \mapsto \mathrm{Tr}_{K/F}(xy)$$

is nondegenerate (and thus  $\langle \cdot, \cdot \rangle_{\mathrm{tr}_{K/F}}$  will be well defined) if and only if  $K/F$  is separable. In this setting we found a nice relationship between  $\langle \cdot, \cdot \rangle_{\mathrm{tr}_{K/F}}$  and the set of  $F$ -embeddings of  $K$ .

**Proposition 4.7.** Let  $K/F$  be a finite separable field extension of degree  $n$  and let  $\{\sigma_1, \dots, \sigma_n\}$  be the set of  $F$ -embeddings of  $K$  into a field  $\Omega$  containing a Galois closure of  $K/F$ . Then  $\{\sigma_1, \dots, \sigma_n\}$  is an orthonormal  $\Omega$ -basis of  $\mathrm{Hom}_F(K, \Omega)$  with respect to the Casimir bilinear form  $\langle \cdot, \cdot \rangle_{\mathrm{tr}_{K/F}}$ .

*Proof.* Let  $\{\alpha_i\}$  be a  $F$ -basis of  $K$ , and let  $A := (\sigma_j(\alpha_i))$ ,  $A' := (\sigma_j(\alpha_i^*))$  then

$$A(A')^t = \left( \sum_k \sigma_k(\alpha_i) \sigma_k(\alpha_j^*) \right) = (\mathrm{Tr}_{K/F}(\alpha_i \alpha_j^*)) = I$$

hence  $(\delta_{ij}) = I = (A')^t A = \left( \sum_k \sigma_i(\alpha_k^*) \sigma_j(\alpha_k) \right) = \left( \langle \sigma_i, \sigma_j \rangle_{\mathrm{tr}_{K/F}} \right)$ . As  $\mathrm{Hom}_F(K, \Omega)$  has dimension  $n$  over  $\Omega$  this proves that the embeddings form an orthonormal basis of this vector space.  $\square$

**Corollary 4.8.** Let  $K, F$  and  $\Omega$  be as above

(i) For any  $\phi \in \text{Hom}_F(K, \Omega)$  there is a Fourier representation

$$\phi = \sum_{i=1}^n \langle \phi, \sigma_i \rangle_{\text{tr}_{K/F}} \sigma_i$$

(ii) Given  $\psi, \phi \in \text{Hom}_F(K, \Omega)$ , we have the Parseval identities

$$\begin{aligned} \langle \psi, \psi \rangle_{\text{tr}_{K/F}} &= \sum_{k=1}^n \langle \psi, \sigma_k \rangle_{\text{tr}_{K/F}}^2 \\ \langle \psi, \phi \rangle_{\text{tr}_{K/F}} &= \sum_{k=1}^n \langle \psi, \sigma_k \rangle_{\text{tr}_{K/F}} \cdot \langle \phi, \sigma_k \rangle_{\text{tr}_{K/F}} \end{aligned}$$

**Corollary 4.9.** Let  $K/F$  and  $L/F$  be separable field extensions of the same degree  $n$ , and  $\Omega$  be field containing a Galois closure of  $KL/F$ . Given an  $F$ -linear map  $\phi : K \rightarrow L$ , the following are equivalent

- (i) The map  $\phi$  is an isometry between  $(K, \text{tr}_{K/F})$  and  $(L, \text{tr}_{L/F})$ .
- (ii)  $\text{Hom}_F(\phi, \Omega)$  is an isometry between the spaces  $\text{Hom}_F(L, \Omega)$  and  $\text{Hom}_F(K, \Omega)$  endowed with their Casimir pairings  $\langle \cdot, \cdot \rangle_{\text{tr}_{L/F}}$  and  $\langle \cdot, \cdot \rangle_{\text{tr}_{K/F}}$
- (iii) The matrix  $U = (c_{ij})$  is orthogonal, where  $c_{ij} := \langle \sigma_i, \tau_j \phi \rangle_{\text{tr}_{K/F}}$ , and  $\{\sigma_i\}, \{\tau_i\}$  are the sets of  $F$ -embeddings of  $K$  and  $L$  into  $\Omega$ .

*Proof.* The equivalence (i)  $\iff$  (ii) is a particular case of Proposition 4.6 and (ii)  $\iff$  (iii) follows from the fact that  $\{\sigma_i\}$  and  $\{\tau_i\}$  are orthonormal bases by (4.7). □

## 4.2. Integrality at finite primes

For a  $\mathbb{Q}$ -linear map between number fields  $\phi : K \rightarrow L$ , we call the smallest positive integer  $m$  such that  $m\phi(\mathcal{O}_K) \subset \mathcal{O}_L$  the **index of  $\phi$** , thus  $m$  is the unique positive integer such that  $m\mathbb{Z} = (\mathcal{O}_L : \phi(\mathcal{O}_K))$ .

**Proposition 4.10.** Let  $K, L$  be number fields, let  $p$  be a rational prime such that  $v_p(\text{disc}(K)) \leq 1$ . Suppose that  $\phi : (K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (L, \text{tr}_{L/\mathbb{Q}})$  is an isometry of index 1 and let

$$c := \langle \iota_K, \iota_L \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \in KL$$

where  $\iota_K : K \hookrightarrow \mathbb{C}$  and  $\iota_L : L \hookrightarrow \mathbb{C}$  are the canonical inclusions  $x \mapsto x$ . Then,  $v_{\mathfrak{p}}(c) \geq 0$  for every prime  $\mathfrak{p} \mid p$  in  $E$ .

Before we begin with the proof, let us fix some notation and review some facts:

- (a) Let  $p$  be a rational prime and fix an algebraic closure  $\overline{\mathbb{Q}_p}^{\text{al}}$  of  $\mathbb{Q}_p$ , by (1.23) the absolute value  $|\cdot|_p$  extends uniquely to an absolute value on all  $\overline{\mathbb{Q}_p}^{\text{al}}$  which we will still denote by  $|\cdot|_p$ .
- (b) Let  $K$  be a number field and let  $\{\mathfrak{p}_i\}$  be the primes in  $K$  lying over  $p$ . For each  $i$ , there is a completion  $K_i$  inside  $\overline{\mathbb{Q}_p}^{\text{al}}$  (unique up to conjugation) of  $K$  with respect to the absolute value  $|\cdot|_{\mathfrak{p}_i}$  in  $K$ , corresponding to  $\mathfrak{p}_i$ , extending  $|\cdot|_p$  in  $\mathbb{Q}$ . Once we fix  $K_i$ , we get a canonical inclusion  $K \hookrightarrow K_i$ , which we denote  $a \mapsto a_i$ , such that  $|a|_{\mathfrak{p}_i} = |a_i|_p$  for all  $a \in K$ .
- (c) Let  $(K)_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p$  and let  $(\mathcal{O}_K)_p := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ . The canonical isomorphism of  $\mathbb{Q}_p$ -algebras

$$(K)_p \rightarrow \prod_i K_i$$

$$a \otimes b \mapsto (a_1 b, \dots, a_i b, \dots)$$

where  $b \mapsto b$  is the inclusion  $\mathbb{Q}_p \hookrightarrow K_i$ , gives an orthogonal decomposition of the  $\mathbb{Q}_p$ -quadratic space  $((K)_p, \text{tr}_{(K)_p/\mathbb{Q}_p}) \cong \perp_i (K_i, \text{tr}_{K_i/\mathbb{Q}_p})$ . Moreover such a decomposition is also valid, see Proposition 2.4, at the integral level i.e., under the above map we have that  $((\mathcal{O}_K)_p, \text{tr}_{(K)_p/\mathbb{Q}_p}) \cong \perp_i (\mathcal{O}_{K_i}, \text{tr}_{K_i/\mathbb{Q}_p})$ .

- (d) Using the isometry above as an identification we denote by  $\pi_i^K : (K)_p \rightarrow K_i$  the natural projection and by  $\mu_i^K : K_i \rightarrow (K)_p$  the natural inclusion of quadratic spaces. Notice that  $\pi_i^K((\mathcal{O}_K)_p) = \mathcal{O}_{K_i}$  and that  $(\mathcal{O}_K)_p$  is the  $\mathbb{Z}_p$ -module generated by the  $\mu_i^K(\mathcal{O}_{K_i})$ 's.

*Proof.* Let  $E := KL$  and let  $\{\mathfrak{p}_i\}$ ,  $\{\mathfrak{q}_j\}$  and  $\{\mathfrak{P}_r\}$  be the primes in  $K$ ,  $L$  and  $E$ , respectively, lying over  $p$ , with completions  $\{K_i\}$ ,  $\{L_j\}$  and  $\{E_r\}$ . By (4.5)(iii) we know that

$$c \otimes 1 = \langle \iota_K \otimes \mathbf{1}_{\mathbb{Q}_p}, \iota_L \phi \otimes \mathbf{1}_{\mathbb{Q}_p} \rangle_{\text{tr}_{(K)_p/\mathbb{Q}_p}} \in (E)_p$$

Since for each  $r$  we have  $|c_r|_p \leq 1 \iff v_{\mathfrak{P}_r}(c) \geq 0$ , the conclusion of the proposition is equivalent to say that  $c_r$  is integral for all  $r$ . This will be the strategy of the proof.

For each  $i$ , let us fix an integral basis  $\mathcal{B}_i := \{\alpha_{i,s} : 1 \leq s \leq n_i := [K_i : \mathbb{Q}_p]\}$  of  $K_i$ , then

$$\mathcal{B} := \bigcup_i \mu_i^K(\mathcal{B}_i)$$

is a  $\mathbb{Z}_p$ -basis of  $(\mathcal{O}_K)_p$  (and thus a  $\mathbb{Q}_p$ -basis of  $(K)_p$ ). Moreover, since the decomposition of  $(K)_p$  is orthogonal, if we take the dual basis  $\mathcal{B}_i^*$  of  $\mathcal{B}_i$  in the space  $(K_i, \text{tr}_{K_i/\mathbb{Q}_p})$ , then

$$\mathcal{B}^* = \bigcup_i \mu_i^K(\mathcal{B}_i^*)$$

is the corresponding dual basis of  $\mathcal{B}$  in the space  $((K)_p, \text{tr}_{(K)_p/\mathbb{Q}_p})$ . Therefore setting

$$\beta_{i,s} := (\phi \otimes 1) (\mu_i^K(\alpha_{i,s})) \in (L)_p$$

we have that

$$c \otimes 1 = \sum_{i,s} (\iota_K \otimes 1) (\mu_i^K(\alpha_{i,s}^*)) (\iota_L \otimes 1)(\beta_{i,s}).$$

Notice that since  $\mu_i^K(\alpha_{i,s}) \in (\mathcal{O}_K)_p$  then  $\beta_{i,s} \in (\mathcal{O}_L)_p$ .

Fix an index  $r$  corresponding to the prime  $\mathfrak{P}_r$  in  $E$  and define  $i_r$  and  $j_r$  by the relations  $\mathfrak{p}_{i_r} = \mathfrak{P}_r \cap K$  and  $\mathfrak{q}_{j_r} = \mathfrak{P}_r \cap L$ . Since the diagram

$$\begin{array}{ccc} (K)_p & \xrightarrow{\iota_K \otimes 1} & (E)_p \\ \downarrow \pi_{i_r}^K & & \downarrow \pi_r^E \\ K_{i_r} & \longrightarrow & E_r \end{array}$$

is commutative (similarly for  $L$ ) then

$$\begin{aligned} c_r &= \pi_r^E(c \otimes 1) \\ &= \pi_r^E \left( \sum_{i,s} (\iota_K \otimes 1) (\mu_i^K(\alpha_{i,s}^*)) (\iota_L \otimes 1)(\beta_{i,s}) \right) \\ &= \sum_{i,s} \pi_r^E ((\iota_K \otimes 1) (\mu_i^K(\alpha_{i,s}^*))) \pi_r^E ((\iota_L \otimes 1)(\beta_{i,s})) \\ &= \sum_{i,s} \pi_{i_r}^K (\mu_i^K(\alpha_{i,s}^*)) \pi_{j_r}^L (\beta_{i,s}) \\ &= \sum_{s=1}^{n_{i_r}} \alpha_{i_r,s}^* \pi_{j_r}^L (\beta_{i_r,s}) \end{aligned}$$

Hence, it suffices to show that  $\alpha_{i_r,s}^* \pi_{j_r}^L (\beta_{i_r,s})$  is in  $\mathcal{O}_{E_r}$  for all  $1 \leq s \leq n_{i_r}$ .

**Claim:** We may assume that  $\alpha_{i_r,s}^*$  is not integral, and moreover that the extension  $K_{i_r}/\mathbb{Q}_p$  is ramified.

*Proof of claim.* Suppose that  $\alpha_{i_r,s}^* \in \mathcal{O}_{K_{i_r}}$ . Here the result follows immediately since

$$\alpha_{i_r,s}^* \pi_{j_r}^L (\beta_{i_r,s}) \in \mathcal{O}_{K_{i_r}} \mathcal{O}_{L_{j_r}} \subseteq \mathcal{O}_{E_r}.$$

If the extension  $K_{i_r}/\mathbb{Q}_p$  is unramified then  $\text{disc}(K_{i_r})$  is a unit in  $\mathbb{Z}_p$  and the codifferent ideal  $\mathcal{D}_{K_{i_r}}^{-1}$  is just  $\mathcal{O}_{K_{i_r}}$ , hence  $\alpha_{i_r,s}^* \in \mathcal{D}_{K_{i_r}}^{-1} = \mathcal{O}_{K_{i_r}}$  for all  $1 \leq s \leq n_{i_r}$ .  $\square$

It remains to verify the ramified case  $K_{i_r}/\mathbb{Q}_p$ . Notice that in this case  $\text{disc}(K)$  is equal to  $p$  modulo units. By the local decomposition of the trace we have that for each  $x \in (L)_p$  that

$$\text{Tr}_{(L)_p/\mathbb{Q}_p}(x) = \sum_j \text{Tr}_{L_j/\mathbb{Q}_p}(\pi_j^L(x)).$$

Hence, if for  $\theta \in L_j$  we denote by  $\theta = \theta^{(1)}, \dots, \theta^{(m_j)}$  the  $m_j := [L_j : \mathbb{Q}_p]$  conjugates of  $\theta$  over  $\mathbb{Q}_p$  then

$$\text{Tr}_{(L)_p/\mathbb{Q}_p}(x) = \sum_j \sum_{t=1}^{m_j} \pi_j^L(x)^{(t)} \quad (3)$$

Consider the square matrix  $B := (\pi_j^L(\beta_{i,s})^{(t)})$  whose rows and columns are index by  $(i, s)$  with  $1 \leq s \leq n_i$  and  $(j, t)$  with  $1 \leq t \leq m_j$ , respectively, in lexicographic order. Taking  $x = \beta_{i,s}\beta_{i',s'}$  in (3) we find that

$$BB^t =: M$$

is the Gram matrix of  $\text{tr}_{(L)_p/\mathbb{Q}_p}$  in the basis  $\bigcup_i \{\beta_{i,s} : 1 \leq s \leq n_i\}$  of  $(L)_p$ . Since  $\phi$  is an isometry,  $M$  is the Gram matrix of  $\text{tr}_{(K)_p/\mathbb{Q}_p}$  in the basis  $\mathcal{B}$  of  $(K)_p$ , i.e,  $M$  is a matrix diagonal in blocks, each block corresponding to the Gram matrix of  $\text{tr}_{K_i/\mathbb{Q}_p}$  in the basis  $\mathcal{B}_i$ . Let  $A$  be the adjoint of  $B^t$ , then

$$\det(B)B = MA.$$

In particular,

$$\begin{aligned} \pi_{j_r}^L(\beta_{i_r,s}) &= \frac{1}{\det(B)} ((i_r, s)\text{-th row of } M) \times ((j_r, 1)\text{-th column of } A) \\ &= \sum_{s_1=1}^{n_{i_r}} \frac{\text{Tr}_{K_r/\mathbb{Q}_p}(\alpha_{i_r,s}\alpha_{i_r,s_1})A_{(i_r,s_1)(j_r,1)}}{\det(B)} \end{aligned} \quad (4)$$

Note that the matrix  $A$ , being the adjoint of  $B^t$ , has integral entries. It follows from the claim above and from the previous equation that to show that  $\alpha_{i_r,s}^* \pi_{j_r}^L(\beta_{i_r,s})$  is integral it is enough to show that

$$\frac{\alpha_{i_r,s}^* \text{Tr}_{K_r/\mathbb{Q}_p}(\alpha_{i_r,s}\alpha_{i_r,s_1})}{\det(B)}$$

is integral for all  $1 \leq s, s_1 \leq n_r$  such that  $\alpha_{i_r,s}^*$  is not integral. Since  $\text{disc}(K) = \det(M) = \det(B)^2$  (up to elements in  $\mathbb{Z}_p^{\times 2}$ ) the integrality of the above is equivalent to

$$(\alpha_{i_r,s}^* \text{Tr}_{K_r/\mathbb{Q}_p}(\alpha_{i_r,s}\alpha_{i_r,s_1}))^2 \in \text{disc}(K)\mathcal{O}_{K_{i_r}} = p\mathcal{O}_{K_{i_r}}. \quad (5)$$

Since  $\sum_i (e(\mathfrak{p}_i|p) - 1)f(\mathfrak{p}_i|p) \leq v_p(\text{disc}(K)) = 1$ , where the first inequality is given by (1.36), we have that exactly one ramification index can be different from 1, and such index must be equal to 2. Since we are assuming that  $K_{i_r}$  is ramified then  $e(\mathfrak{p}_{i_r}|p) = 2$ . Thus  $K_{i_r}/\mathbb{Q}_p$  is a

quadratic ramified extension and, given that  $p \neq 2$  thanks to Stickelberger's criterion (1.29), we have that  $K_{i_r} \in \{\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{up})\}$  where  $u \in \{1, \dots, p-1\}$  is quadratic non-residue modulo  $p$ . Thus an integral basis for  $\mathcal{O}_{K_{i_r}}$  is given by  $\{1, \pi\}$  where  $\pi = \sqrt{\epsilon p}$  and  $\epsilon$  is some unit in  $\mathbb{Z}_p$ .

Let  $\alpha_{i_r,1} := 1, \alpha_{i_r,2} := \pi$ . The dual basis in  $(K_{i_r}, \text{tr}_{K_{i_r}/\mathbb{Q}_p})$  is given by  $\alpha_{i_r,1}^* = 1/2$  and  $\alpha_{i_r,2}^* = 1/2\pi$ . Since  $\alpha_{i_r,1}^* = 1/2$  is integral we are only left to check the values

$$(\alpha_{i_r,2}^* \text{Tr}_{K_r/\mathbb{Q}_p}(\alpha_{i_r,2} \alpha_{i_r,s_1}))^2 = \left( \frac{1}{2\pi} \text{Tr}_{K_r/\mathbb{Q}_p}(\pi \alpha_{i_r,s_1}) \right)^2 = \begin{cases} 0 & \text{if } s_1 = 1. \\ p\epsilon & \text{otherwise.} \end{cases}$$

□

**Theorem 4.11.** *Let  $K, L$  and  $c$  be as above. Write  $d_K = \text{disc}(K) = d_s d_f$  where  $d_f$  is the product of the primes dividing the discriminant exactly once. Then,  $d_s c$  is an algebraic integer. Moreover, if  $K$  tamely ramified then  $\text{rad}(d_s)c$  is an algebraic integer.*

*Proof.* Let  $\{\alpha_1, \dots, \alpha_n\}$  be an integral basis of  $K$ . Recall that by definition

$$c = \sum_{i=1}^n \alpha_i^* \phi(\alpha_i),$$

since each  $\alpha_i^*$  belongs to the codifferent ideal  $\mathcal{D}_K^{-1}$  and  $[\mathcal{D}_K^{-1} : \mathcal{O}_K] = d_K$ , we have  $d_K c \in \mathcal{O}_{KL}$ .

Let  $\mathfrak{P}$  be a prime in  $KL$ , let  $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Q}$  and  $\mathfrak{p} = \mathfrak{P} \cap K$ , then if  $p \mid d_f$  by Proposition 4.10 we have

$$v_{\mathfrak{P}}(d_s c) = v_{\mathfrak{P}}(c) \geq 0$$

and if  $p \nmid d_f$ , then

$$v_{\mathfrak{P}}(d_s c) = v_{\mathfrak{P}}(d_K c) \geq 0$$

this for every prime  $\mathfrak{P}$  in  $KL$ , thus  $d_s c \in \mathcal{O}_{KL}$ .

To prove the last part, suppose that  $K$  is tame at  $p$ , then

$$v_{\mathfrak{p}}(p\mathcal{D}_K^{-1}) = e(\mathfrak{p}|p) - (e(\mathfrak{p}|p) - 1) = 1 \geq 0$$

it follows that  $v_{\mathfrak{P}}(pc) \geq 0$  whenever  $p \mid d_s$  and therefore  $v_{\mathfrak{P}}(\text{rad}(d_s)c) \geq 0$  for all  $\mathfrak{P}$ .

□

**Corollary 4.12.** *Suppose  $K$  has square free discriminant, then  $c$  is an algebraic integer.*

*Proof.* In this case  $d_s = 1$ .

□

It is not hard to generalize a bit (4.12) to even fundamental discriminant and maps  $\phi : K \rightarrow L$  with arbitrary index  $m$ , this is done in

**Lemma 4.13.** Let  $K, L$  be number fields and suppose  $K$  has fundamental discriminant  $d_K$ , then given an isometry  $\phi : (K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (L, \text{tr}_{L/\mathbb{Q}})$  of index  $m$ , we have that  $N(m, d_K) \cdot c$  is an algebraic integer. Where  $N(m, d_K)$  is given by

$$N(m, d_K) := d_2 m \prod_{\substack{p|(m, d_K) \\ p \neq 2}} p$$

and

$$d_2 = \begin{cases} 1, & \text{if } 2 \nmid d_K \\ 2, & \text{if } 2 \mid d_K, 2 \nmid m \\ 4, & \text{if } v_2(d_K) = 3, 2 \mid m \end{cases}$$

*Proof.* The proof follows the same lines as that of (4.11), only in this case  $\mu_i^K(\alpha_{i,s}) \in (\mathcal{O}_K)_p$  just implies  $\beta_{i,s} \in m^{-1}(\mathcal{O}_L)_p$ , thus we get for example

$$|c_{r_0}|_p \leq |m|_p^{-1} \quad (6)$$

for unramified  $K_{i_0}/\mathbb{Q}_p$ . If  $K_{i_0}/\mathbb{Q}_p$  is ramified and  $p \neq 2$ , then, as  $A_{(i,s)(j,t)}$  is polynomial of degree  $n - 1$  in the entries of  $B$ , equation (4) now shows

$$|c_{r_0}|_p \leq \min\{p^{1/2} |m|_p^{-1}, |m|_p^{-(n-1)}\} \quad (7)$$

On the other hand, suppose  $p = 2$  and  $K_{i_0}/\mathbb{Q}_2$  is ramified, then  $K_{i_0}/\mathbb{Q}_2$  is quadratic ramified by (3.1). Which leads us to the following cases<sup>1</sup>

- $v_2(d_K) = 2$ , which implies that  $\mathcal{O}_{K_{i_0}}$  has a basis  $\{1, \pi\}$  where  $\pi \in \{\sqrt{-1}, \sqrt{-5}\}$  thus  $|\pi|_2 = 1$  and

$$|c_{r_0}|_2 \leq 2|m|_2^{-1} \quad (8)$$

in this case (note that we did not use that  $\phi$  was an isometry here).

- $v_2(d_K) = 3$ , in this case  $\mathcal{O}_{K_{i_0}}$  has a basis  $\{1, \pi\}$  where  $\pi \in \{\sqrt{2}, \sqrt{-2}, \sqrt{2 \cdot 5}, \sqrt{-2 \cdot 5}\}$ . In this case equation (4) gives us

$$|c_{r_0}|_2 \leq \min\{2^{3/2} |m|_2^{-1}, 2|m|_2^{-(n-1)}\} \quad (9)$$

Bounds (6),(7),(8) and (9) imply that  $|N(m, d_K)c_{r_0}|_p \leq 1$  in all cases and the lemma follows.  $\square$

<sup>1</sup>As  $K_{i_0}/\mathbb{Q}_2$  is the only ramified extension (3.1) and  $d_K$  is the product of the local discriminants (1.30), we have  $|d_K|_2 = |\text{disc}(K_{i_0})|_2$ , hence the cases.

**Remark 4.14.** Theorem 4.11 remains true if we replace  $c$  with

$$\langle \sigma, \tau \phi \rangle_{\text{tr}_{K/\mathbb{Q}}}$$

where  $\sigma : K \hookrightarrow \mathbb{C}$ ,  $\tau : L \hookrightarrow \mathbb{C}$  are arbitrary embeddings. To see this, apply the theorem to  $\phi' := \tau \phi \sigma^{-1} : K' \rightarrow L'$  where  $K' = \sigma(K)$  and  $L' := \tau(L)$ , and notice that if  $\{\alpha_i\}$  is a basis of  $K$  then

$$\begin{aligned} \langle \sigma, \tau \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} &= \sum_i \sigma(\alpha_i^*)(\tau \phi)(\alpha_i) \\ &= \sum_i \beta_i^* \phi'(\beta_i) \\ &= \langle \iota_{K'}, \iota_{L'} \phi' \rangle_{\text{tr}_{K'/\mathbb{Q}}} \end{aligned}$$

where the  $\beta_i := \sigma(\alpha_i)$  form a basis of  $K'$  with dual basis  $\beta_i^* = \sigma(\alpha_i^*)$ .

### 4.3. Proofs of the theorems

With this tools at hand we can prove our first main result

**Proposition 4.15.** Let  $K, L$  be number fields such that  $K$  is totally real with square free discriminant, then

$$(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$$

if and only if  $K \cong L$ .

*Proof.* The proof is by contradiction. Let  $\phi : (\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  be an isometry and suppose  $K \not\cong L$ . We know from Taussky's theorem that the existence of  $\phi$  implies that  $L$  is also totally real and so is  $E := KL$ . Consider the map

$$\{\theta : E \hookrightarrow \mathbb{R}\} \rightarrow \{\sigma : K \hookrightarrow \mathbb{R}\} \times \{\tau : L \hookrightarrow \mathbb{R}\}, \theta \mapsto (\theta \upharpoonright_K, \theta \upharpoonright_L)$$

this is always injective, but since  $\text{disc}(K) = \text{disc}(L)$  is fundamental and  $K \not\cong L$ , Corollary (3.8) shows that  $K$  and  $L$  are linearly disjoint. Hence both domain and codomain have the same cardinal and the map is also surjective.

It follows that, if we list the embeddings of  $K$  and  $L$  into  $\mathbb{R}$  as  $\{\sigma_1, \dots, \sigma_n\}$  and  $\{\tau_1, \dots, \tau_n\}$ , then for each  $1 \leq i, j \leq n$  exists a unique  $\theta_{ij} : E \hookrightarrow \mathbb{R}$  extending both  $\sigma_i$  and  $\tau_j$ . Thus, fixing a basis  $\{\alpha_i\}$  of  $K$  and setting  $c := \langle \iota_K, \iota_L \phi \rangle_{\text{tr}_{K/\mathbb{Q}}}$ , we find

$$\theta_{ij}(c) = \langle \theta_{ij} \iota_K, \theta_{ij} \iota_L \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} = \langle \sigma_i, \tau_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}}$$

and from (4.9)(iii) we conclude that  $U = (\theta_{ij}(c))$  is orthogonal, in particular  $|\theta_{ij}(c)| \leq 1$  for all  $1 \leq i, j \leq n$ .

But from Corollary 4.12  $c$  is an algebraic integer and since every conjugate of  $c$  has absolute value  $\leq 1$ , then  $c$  is either 0 or a root of the unity, as  $c \in \mathbb{R}$  this shows that  $c \in \{\pm 1, 0\}$ . In particular  $c \in \mathbb{Q}$  and thus all the entries of  $U$  are equal to  $c$ , which contradicts  $U$  being orthogonal (except in the trivial case  $n = 1$ ). The contradiction came from assuming  $K \not\cong L$ , therefore, we conclude  $K \cong L$  as required.  $\square$

As a byproduct of the above proof we obtain following fact

**Corollary 4.16.** Let  $K$  be a totally real number field of degree  $n$  and square free discriminant, then

$$\text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})/\{\pm 1\} = \begin{cases} \{\mathbb{1}_K\} & \text{if } n > 2 \\ \text{Gal}(K/\mathbb{Q}) & \text{if } n = 2 \end{cases}$$

*Proof.* Let  $\phi \in \text{Aut}(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}})$  and  $\{\sigma_i\}$  be the embeddings of  $K$  with  $\sigma_1 = \iota_K$ , then each entry of the orthogonal matrix

$$U = \left( \langle \sigma_i, \sigma_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \right)$$

is an algebraic integer, by (4.14). Also for every  $\sigma \in \text{Gal}(\tilde{K}/\mathbb{Q})$  and  $i, j$  we have

$$\sigma \left( \langle \sigma_i, \sigma_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \right) = \langle \sigma_{i'}, \sigma_{j'} \phi \rangle_{\text{tr}_{K/\mathbb{Q}}}$$

for some  $i', j'$ , i.e., every conjugated of an entry of  $U$  is an entry of  $U$ . Since they are all real and its absolute value is bounded by 1, we find that each one is either 0 or a real root of the unity, i.e.,  $\langle \sigma_i, \sigma_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \in \{0, \pm 1\}$  for all  $i, j$ . Furthermore,  $U$  being orthogonal implies that there is only one  $\langle \sigma_i, \sigma_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}}$  equal to  $\pm 1$  on each row and on each column. If  $j$  is the index such that  $\langle \sigma_1, \sigma_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \neq 0$ , then by the Fourier representation (4.8)(i) we have

$$\iota_K \phi = \sigma_1 \phi = \pm \sigma_j$$

thus  $\mp \phi \in \text{Aut}(K)$ , but since  $K$  is an  $S_n$ -field (3.2), then its group of multiplicative automorphisms  $\text{Aut}(K)$  is trivial if  $n > 2$  and  $\text{Gal}(K/\mathbb{Q})$  if  $n = 2$ .  $\square$

**Lemma 4.17.** Let  $\{r_1, \dots, r_k\}$  be real numbers, then

$$\prod_{u < v} (r_u - r_v)^2 \leq \left( \frac{kS_2 - S_1^2}{\binom{k}{2}} \right)^{\binom{k}{2}}$$

where  $S_1 = \sum_{u=1}^k r_u$  and  $S_2 = \sum_{u=1}^k r_u^2$ .

*Proof.* This is an application of the arithmetic-geometric means inequality, since

$$\left( \prod_{u < v} (r_u - r_v)^2 \right)^{1/\binom{k}{2}} \leq \sum_{u < v} \frac{(r_u - r_v)^2}{\binom{k}{2}}$$

and

$$\begin{aligned}
\sum_{u<v} (r_u - r_v)^2 &= \sum_{u<v} r_u^2 + r_v^2 - 2 \sum_{u<v} r_u r_v \\
&= \sum_{u \neq v} r_u^2 - 2 \sum_{u<v} r_u r_v \\
&= (k-1)S_2 - (S_1^2 - S_2) \\
&= kS_2 - S_1^2
\end{aligned}$$

□

**Theorem 4.18.** *Let  $K, L$  be number fields such that  $K$  is totally real with fundamental discriminant, then*

$$(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$$

if and only if  $K \cong L$ .

*Proof.* Suppose  $K \not\cong L$  and keep the notation as in the proof of (4.15). Since  $\text{disc}(K)$  is fundamental, from (4.13) we know that  $2c$  is an algebraic integer. Let  $M := \mathbb{Q}(c)$  and  $k = [M : \mathbb{Q}]$ , since  $\mathcal{O}_M \supset \mathbb{Z}[2c]$ , if  $\{r_1, \dots, r_k\}$  are the conjugates of  $c$  over  $\mathbb{Q}$ , then by the above lemma we have

$$\text{disc}(M) \leq \text{disc}(\mathbb{Z}[2c]) = \prod_{u<v} (2r_u - 2r_v)^2 \leq 4^{\binom{k}{2}} \left( \frac{k \text{Tr}_{M/\mathbb{Q}}(c^2) - \text{Tr}_{M/\mathbb{Q}}(c)^2}{\binom{k}{2}} \right)^{\binom{k}{2}} \quad (10)$$

Recall that  $U = (c_{ij})$  is an orthogonal matrix, where  $c_{ij} := \theta_{ij}(c)$ , in particular

$$\text{Tr}_{E/\mathbb{Q}}(c^2) = \sum_{i,j} c_{ij}^2 = n$$

also (2.10) tells us that  $\varphi(1) = \pm 1$ , hence  $(\tau_j \circ \phi)(1) = \pm 1$ , which translates by the Fourier representation (4.8)(i) to  $\pm 1 = (\tau_j \circ \varphi)(1) = \sum_i c_{ij}$ , thus

$$\text{Tr}_{E/\mathbb{Q}}(c) = \sum_{i,j} c_{ij} = \pm n$$

and  $\text{Tr}_{E/\mathbb{Q}}(c)^2 = n^2$ . Remark that  $M \neq \mathbb{Q}, K, L$ , since for example  $c \in L$  would imply that every column of  $U$  is a multiple of  $(1, \dots, 1)^t$ , contradicting that  $U$  is orthogonal (hence non-singular).

It follows from Theorem 3.19 that, at least when  $n \geq 5$ , we must have  $M = E$ ,  $k = n^2$  and  $\text{disc}(M) = \text{disc}(K)^{2(n-1)}$ . Because,  $\mathbb{Q}, K$  and  $L$  are the only other subfields of  $E$ . Hence (10) becomes

$$\text{disc}(K)^{2(n-1)} \leq \left( \frac{8}{n+1} \right)^{\binom{n^2}{2}} \quad (11)$$

This is already a contradiction if  $n \geq 7$  and for  $3 \leq n < 7$  inequality (11) gives us the following upper bounds on  $\text{disc}(K)$

Bound	$n$
512	3
$12.1 \times 10^3$	4
$4.9 \times 10^4$	5
$4.6 \times 10^3$	6

as these bounds are below the ones given in Theorem 4 and since by Proposition 2.10  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$  is stronger than  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$ , this proves the theorem whenever  $n \geq 5$  or  $M = E$ .

Now suppose,  $n = 3, 4$  and  $M \neq E$ , in this case Theorem 3.19 tells us that  $k = n$  and  $\text{disc}(M) = \text{disc}(K)$ . From  $\text{Tr}_{E/\mathbb{Q}} = \text{Tr}_{M/\mathbb{Q}} \circ \text{Tr}_{E/M}$  we know that  $\text{Tr}_{M/\mathbb{Q}}(c^2) = 1 = \text{Tr}_{M/\mathbb{Q}}(c)^2$ , hence (10) becomes

$$\text{disc}(K) \leq (4(1 - 1/n))^{\binom{n}{2}}$$

i.e., if  $n = 3$  we get  $\text{disc}(K) \leq 19$  and if  $n = 4$  we get  $\text{disc}(K) \leq 729$ , again this bounds are below the ones given by Theorem 4, so no counterexample to the theorem exists.  $\square$

**Theorem 4.19.** *Let  $K$  be a totally real number field of fundamental discriminant and degree  $n \geq 3$  such that  $(\mathbb{Z}/n\mathbb{Z})^\times$  is cyclic. Then, for any number field  $L$  the following are equivalent:*

- (i)  $K \cong L$
- (ii)  $(\mathcal{O}_K, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L, \text{tr}_{L/\mathbb{Q}})$ .
- (iii)  $(\mathcal{O}_K^\perp, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^\perp, \text{tr}_{L/\mathbb{Q}})$ .
- (iv)  $\text{Sh}(K) = \text{Sh}(L)$  and  $L$  is totally real with fundamental discriminant.

*If  $(n, \text{disc}(K)) = 1$ , then the four items are also equivalent to*

- (v)  $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$ .

*Proof.* This is Corollary 2.17 together with Theorem 4.18.  $\square$

**Theorem 4.20.** *Let  $K$  be a totally real number field with fundamental discriminant and degree  $n$ . Then, for a number field  $L$  such that  $\text{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$ , the five statements in theorem (4.19) are equivalent up to finitely many counterexamples for each  $n$ . More specifically, they will be equivalent as soon as  $\text{disc}(K) \geq (32n^3)^{\frac{n^2(n+1)}{4}}$ .*

*Proof.* Since  $\mathrm{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L) = \mathbb{Z}$  from section 2.1.2 we have that if any of the conditions hold, then  $\mathrm{disc}(K) = \mathrm{disc}(L)$ , also by Taussky's theorem under any of the conditions,  $L$  must be totally real. Hence  $K$  and  $L$  are totally real of the same degree  $n$  and same fundamental discriminant  $d_K = \mathrm{disc}(K)$ .

First we prove that both (v) and (iii) imply (i): Suppose that (v) holds and let  $\varphi : (\mathcal{O}_K^0, \mathrm{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^0, \mathrm{tr}_{L/\mathbb{Q}})$  be isometry, then as we saw in the proof of (2.3) we can write  $\mathcal{O}_K = \gamma_K \cdot \mathbb{Z} + \mathcal{O}_K^0$ , where  $\gamma_K$  is any integer in  $K$  such that  $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_K) = 1$ . Hence, as  $\gamma_0 := 1 - n\gamma \in \mathcal{O}_K^0$ , we have  $n\varphi^+(\gamma_K) = 1 - \varphi(\gamma_0) \in \mathcal{O}_L$  and thus

$$n\varphi^+(\mathcal{O}_K) \subset \mathcal{O}_L$$

(recall that  $\varphi^+$  is the unique extension of  $\varphi$  to a rational isometry between  $K$  and  $L$  such that  $\varphi^+(1) = 1$ ). Similarly, if (iii) hold and  $\varphi : (\mathcal{O}_K^\perp, \mathrm{tr}_{K/\mathbb{Q}}) \xrightarrow{\sim} (\mathcal{O}_L^\perp, \mathrm{tr}_{L/\mathbb{Q}})$  is the respective isometry, then

$$n\varphi^+(x) = \varphi^+(nx) = \varphi^+(\mathrm{Tr}_{K/\mathbb{Q}}(x) + x_\perp) = \mathrm{Tr}_{K/\mathbb{Q}}(x) + \varphi(x_\perp) \in \mathcal{O}_L$$

for all  $x$  in  $\mathcal{O}_K$ . Therefore, in either case we find a rational isometry  $\phi$  of index dividing  $n$ . Suppose  $K \not\cong L$ , again keeping the notation in the proof of (4.15), by (4.13) we have that  $N(n, d_K) \cdot c$  is an algebraic integer. As  $N(n, d_K) \mid 4n^2$ , then  $4n^2 \cdot c$  is an algebraic integer, thus  $\mathcal{O}_M \supset \mathbb{Z}[4n^2c]$ ,  $M = \mathbb{Q}[c]$ , and bounding  $\mathrm{disc}(M)$  as in the proof of (4.18) we find

$$\mathrm{disc}(K) \leq \left( \frac{32n^4}{n+1} \right)^{\frac{n^2(n+1)}{4}} < (32n^3)^{\frac{n^2(n+1)}{4}}$$

if  $n \geq 5$  or  $M = E$  and

$$\mathrm{disc}(K) \leq (16n^3(n-1))^{\frac{n(n-1)}{2}} < (32n^3)^{\frac{n^2(n+1)}{4}}$$

if  $n = 3, 4$  and  $M \neq E$ , contrary to our assumption. Hence,  $K \cong L$ .

The equivalence (iii)  $\iff$  (iv) was proven in (2.17), (ii)  $\Rightarrow$  (iii), (v) is (2.10) and clearly (i)  $\Rightarrow$  (ii), (iii), (iv), (v), this closes the equivalences and finishes the proof.  $\square$

# 5 An alternative proof via Bhargava's parametrization of quartic rings

The proof we gave of Conjecture 1, seems completely unrelated to the proof of the cubic case given in [MS10], which uses a combination of the Delone-Fadaved parametrization cubic rings with Bhargava's composition law of cubes. Since in his P.h.D. thesis [Bha01] Bhargava also generalized both concepts to quartic rings and  $3 \times 3 \times 2$  boxes of integers, respectively, it seems natural too seek a proof of the quartic case using the same method. This is indeed possible and in this chapter we present a brief sketch of such proof.

## 5.1. Parametrization of quartic rings

Let  $(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  denote the set of pairs  $(A, B)$  of *integral* ternary quadratic forms. We can write a pair  $(A, B) \in (\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  as

$$2 \cdot (A, B) = \left( \begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right)$$

where  $a_{ij}, b_{ij} \in \mathbb{Z}$ . The group  $\text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$  acts naturally on  $(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$ . Namely, if  $g = (g_2, g_3) \in \text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$  with  $g_2 = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ , then  $g$  acts on  $(A, B)$  by

$$g \cdot (A, B) = (r \cdot g_3 A g_3^t + s \cdot g_3 B g_3^t, t \cdot g_3 A g_3^t + u \cdot g_3 B g_3^t) \quad (1)$$

This action has a fundamental invariant called the **discriminant** and is given by

$$\text{disc}((A, B)) = \text{disc}(f_{(A,B)}(x, y)) = b^2 c^2 - 27a^2 d^2 + 18abcd - 4ac^3 - 4b^3 d$$

where  $f_{(A,B)}(x, y) = 4 \cdot \det(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$  is the **cubic resolvent form** of  $(A, B)$ , a covariant for the action of  $\text{GL}_2(\mathbb{Z})$ .

A **quartic ring** is a ring that is isomorphic to  $\mathbb{Z}^4$  as a  $\mathbb{Z}$ -module. For example an order<sup>1</sup> in a quartic field is a quartic ring. In [Bha04b] Bhargava proved that we can parametrize quartic rings using integral ternary quadratic forms, his main result is the following.

**Theorem 5.1.** *There is a bijection between the set of  $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ -orbits on the space  $(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  and isomorphism classes of pairs  $(Q, R)$ , where  $Q$  is a quartic ring and  $R$  is a cubic resolvent of  $Q$ . Moreover, this correspondence is discriminant preserving  $\text{disc}((A, B)) = \text{disc}(Q) = \text{disc}(R)$ .*

A cubic resolvent of a quartic ring  $Q$  is a cubic ring  $R$  equipped with a certain quadratic resolvent mapping  $Q \rightarrow R$ , whose precise definition can be found in [Bha04b]. When  $Q$  is the maximal order in a  $S_4$ -field  $K$ , then  $R$  is the maximal order in the usual cubic resolvent field of  $K$ , as we defined it in the beginning of Section 3.2.2 and is the cubic ring corresponding to  $f_{(A,B)}$  by the Delone-Faddeev-Gross parametrization of cubic rings. Let us denote the correspondence given by Theorem 5.1 as

$$\Psi : \text{Cl}((\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*) \longrightarrow \mathcal{K}_4.$$

The space  $(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  has a unique  $SL_3$ -covariant of degree 4. Namely, let  $(A, B) \in (\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  and suppose  $Q$  is a quartic ring corresponding to  $(A, B)$  by  $\Psi$ , then the covariant denoted  $\mathcal{Q}_{(A,B)}$  is the integral ternary quadratic form obtained by restricting the trace form  $\frac{1}{4}\text{Tr}(x^2)$  to  $\{x \in \mathbb{Z} + 4Q : \text{Tr}(x) = 0\}$ . For example, if  $Q_{(A,B)} = \mathcal{O}_K$  is the maximal order in a quartic field  $K$ , then  $\mathcal{Q}_{(A,B)}$  corresponds to the isometry class of the quadratic  $\mathbb{Z}$ -module  $(\mathcal{O}_K^\perp, \frac{1}{4}\text{tr}_{K/\mathbb{Q}})$ . The explicit computation of  $\mathcal{Q}_{(A,B)}$  in terms of the coefficients of  $(A, B)$  is in the appendix to Chapter 5 of [Bha01].

Thus if  $(\text{Sym}^2 \mathbb{Z}^3)^*$  denotes the set of integral ternary quadratic forms and  $\text{Cl}((\text{Sym}^2 \mathbb{Z}^3)^*)$  its orbits by the action of  $SL_3(\mathbb{Z})$ , this gives us a map

$$\mathcal{Q} : \text{Cl}((\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*) \longrightarrow \text{Cl}((\text{Sym}^2 \mathbb{Z}^3)^*)$$

And by Corollary 2.17, the proof of Conjecture 1 amounts to proving that  $\mathcal{Q}$  is injective when restricted to the orbits of pairs  $(A, B)$  coming from totally real quartic fields with square free discriminant.

---

<sup>1</sup> An order in a number field  $K$  is a subring  $1 \in \mathcal{O} \subset \mathcal{O}_K$  such that  $\mathcal{O} \cong \mathbb{Z}^{[K:\mathbb{Q}]}$  (as  $\mathbb{Z}$ -modules). For example  $\mathcal{O}_K$  is an order, in fact is the maximal order in  $K$

## 5.2. Parametrization of order two ideals in cubic rings

There is another arithmetic object that is parametrized by pairs of ternary quadratic forms. Let  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$  be the set of pairs  $(A, B)$  of symmetric  $3 \times 3$  integer matrices. Again the group  $\text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$  acts naturally on this set as described in the equation (1), the only difference is that in the space  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$  the **cubic resolvent form** is now

$$F_{(A,B)} = \det(Ax - By)$$

(without the 4 factor) and the **discriminant** is defined as  $\text{disc}((A, B)) = \text{disc}(F_{(A,B)})$ . The following theorem, obtained by Bhargava in [Bha04a] imposing symmetry on a more general result about  $3 \times 3 \times 2$  boxes of integers (a higher dimensional analog of Bhargava's cubes), shows how the orbits in this space parametrize order two ideals in cubic rings.

**Theorem 5.2.** *There is a bijection between the set of nondegenerate  $\text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$ -orbits on the space  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$  and the set of equivalence classes of triples  $(R, I, \delta)$ , where  $R$  is a nondegenerate cubic ring,  $I$  is an ideal of  $R$ , and  $\delta$  is an invertible element of  $R \otimes \mathbb{Q}$  such that  $I^2 \subset (\delta)$  and  $N(\delta) = N(I)^2$ . (Here two triples  $(R, I, \delta)$  and  $(R', I', \delta')$  are equivalent if there exists an isomorphism  $\phi : R \rightarrow R'$  and an element  $\kappa \in R' \otimes \mathbb{Q}$  such that  $I' = \kappa\phi(I)$  and  $\delta' = \kappa^2\phi(\delta)$ ). Under this bijection,  $\text{disc}((A, B)) = \text{disc}(R)$ .*

The ring  $R$  is associated to the pair  $(A, B)$  is the one corresponding by the Delone-Faddeev-Gross parametrization of cubic rings to  $F_{(A,B)}$ . Let us denote the correspondence from Theorem 5.2 as

$$\Phi : \text{Cl}(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3) \longrightarrow \mathcal{R}$$

Now there is also a natural map

$$T : \mathcal{R} \longrightarrow \text{Cl}((\text{Sym}^2 \mathbb{Z}^3)^*)$$

taking the equivalence class of  $(R, I, \delta)$  to equivalent class of the integral quadratic form obtained by restricting of the trace form  $\text{Tr}(x^2/\delta)$  to  $I$ . It is easy to check that  $T$  is discriminant preserving, i.e.,  $\text{disc}(R) = \text{disc}(I, \text{Tr}(x^2/\delta))$ .

Finally, notice that there is a natural map connecting the two previous theorems, the map

$$\text{Cl}((\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*) \rightarrow \text{Cl}(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)$$

taking the orbit of  $(A, B) \in (\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  to the orbit of  $(2A, 2B) \in \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$ .

### 5.3. Proof of the Conjecture

All these maps fit together in the following diagram

$$\begin{array}{ccc}
 \mathcal{K}_4 & \xrightarrow{\Psi^{-1}} & \text{Cl}((\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*) \\
 & & \downarrow \\
 & & \text{Cl}(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3) \\
 & & \downarrow \Phi \\
 \mathcal{R} & \xrightarrow{T} & \text{Cl}((\text{Sym}^2 \mathbb{Z}^3)^*)
 \end{array}
 \quad \begin{array}{l}
 \nearrow \mathcal{Q} \\
 \searrow
 \end{array}$$

and a direct computation shows

**Lemma 5.3.** The above diagram is commutative.

It follows that in order to prove Conjecture 1 all we have to do is prove that  $T$  is injective when restricted to the equivalence classes of triples coming from totally real quartic fields of some fixed square free discriminant, say  $d$ . Denote this subset of  $\mathcal{R}$  as  $\mathcal{R}(d)$ , then Conjecture 1 follows from.

**Theorem 5.4.** *Let  $(R, I, \delta)$ ,  $(S, J, \epsilon)$  be triples representing classes in  $\mathcal{R}(d)$ . If an isomorphism of quadratic modules*

$$(I, \text{Tr}(x^2/\delta)) \cong (J, \text{Tr}(x^2/\epsilon))$$

*exists. Then,  $(R, I, \delta)$  and  $(S, J, \epsilon)$  are equivalent.*

It is convenient to identify some properties of the elements in  $\mathcal{R}(d)$ , before we give the proof. Start with a pair of integral ternary quadratic forms  $(A, B) \in (\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$  corresponding under  $\Psi$  to the maximal order  $Q$  in a totally real quartic field  $K$  of discriminant  $d$ , and let  $(R, I, \delta)$  be a triple corresponding under  $\Phi$  with  $(2A, 2B)$ . Then,

- The maximal order  $\mathcal{O}$  in the cubic resolvent field of  $K$  is the cubic ring corresponding to  $f_{(A,B)}$ , thus  $R$  will be the cubic ring corresponding to  $F_{(2A,2B)} = 2f_{(A,B)}$ . This means that if  $\{1, \omega, \theta\}$  is a normalized  $\mathbb{Z}$ -basis of  $\mathcal{O}$ , then  $R = \langle 1, 2\omega, 2\theta \rangle$ . In particular,  $R$  is an order of conductor  $\mathfrak{c} = 2\mathcal{O}$  in the cubic resolvent field of  $K$ . Note that given  $x \in R$ , then  $x \in 2\mathcal{O} \iff \text{Tr}(x) \equiv 0 \pmod{2}$ .
- Since  $Q$  is totally real, the pair  $(A, B)$  possesses 4 zeros in  $\mathbb{P}^2(\mathbb{R})$  and so does  $(2A, 2B)$ , which means that  $\delta$  is totally positive (see [BV<sup>+</sup>15, Lemma 21]).

- There is a  $\kappa \in R \otimes \mathbb{Q}$ , such that  $\kappa I$  is an integral ideal in  $R$  ideal prime to the conductor  $\mathfrak{c} = 2\mathcal{O}$ . To prove this, take a  $\mathbb{Z}$ -basis  $\{1, \gamma_1, \gamma_2, \gamma_3\}$  of  $Q$  and let  $t_i := \text{Tr}(\gamma_i)$ , then  $\{4\gamma_i - t_i\}$  is a basis of  $Q^\perp$  and if  $(\mathcal{Q}_{ij})$  is the Gram matrix of  $\frac{1}{4}\text{Tr}(x^2)$  in this basis, then

$$\mathcal{Q}_{ii} \equiv t_i \pmod{4}$$

Since  $d$  is square free, then  $(4, t_1, t_2, t_3) = \text{Tr}(Q) = \mathbb{Z}$  (see (2.6)). Thus at least one of  $\mathcal{Q}_{ii}$  must be odd, say  $\mathcal{Q}_{11}$

Next, according to Lemma 5.3,  $(\mathcal{Q}_{ij})$  is the Gram matrix of  $\text{Tr}(x^2/\delta)$  in some basis  $\{\alpha_1, \alpha_2, \alpha_3\}$  of  $I$  and so  $\kappa := \alpha_1/\delta$  is the constant we are looking for. This is because if

$$\frac{\alpha_1^2}{\delta} = f + b(2\omega) + a(2\theta),$$

then  $1 \equiv \mathcal{Q}_{11} = 3f \equiv f \pmod{2}$ , so  $\kappa I \subset \delta^{-1}I^2 \subset R$  is an integral ideal such that

$$1 = \frac{\alpha_1^2}{\delta} + \left(1 - \frac{\alpha_1^2}{\delta}\right)$$

with  $\frac{\alpha_1^2}{\delta} \in \kappa I$  and  $1 - \frac{\alpha_1^2}{\delta} \in \mathfrak{c} = 2\mathcal{O}$ . We have proved that  $(R, I, \delta)$  is equivalent to a triple  $(R, I', \delta')$  where  $I'$  is an integral ideal prime to the conductor. This implies, by the same proof given for maximal orders, that if we fix any ideal  $\mathfrak{a}$  in  $R$  prime to the conductor, then  $(R, I, \delta)$  is equivalent to a triple  $(R, I'', \delta'')$  where  $I''$  is integral prime to the conductor and prime to  $\mathfrak{a}$ .

*Proof of Theorem A.4.* Let  $K := R \otimes \mathbb{Q}$  and  $L := S \otimes \mathbb{Q}$ . Choose  $I$  and  $J$  to be prime the conductor of  $R$  and  $S$ , respectively, and to  $d$ . The isometry can be extended to a rational isometry

$$\phi : (K, \text{Tr}(x^2/\delta)) \xrightarrow{\sim} (L, \text{Tr}(x^2/\epsilon))$$

Let  $\sigma : K \hookrightarrow \mathbb{R}$  and  $\tau : L \hookrightarrow \mathbb{R}$  be embeddings (recall that  $K$  and  $L$  are totally real). We claim that  $c := \langle \tau, \sigma\phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \sqrt{\frac{\sigma(\delta)}{\tau(\epsilon)}}$  is an algebraic integer. Similarly to Remark 4.14, we see that it is enough to prove it when  $\sigma$  and  $\tau$  are the inclusions  $x \mapsto x$ . The strategy is the same as in Proposition 4.10. We prove that

$$c^2 \otimes 1 \in \mathcal{O}_{KL} \otimes \mathbb{Z}_p$$

for all  $p$ . This is already clear when  $p \nmid 2d$ . The case  $p \mid d$  is a straight forward adaptation of the proof of (4.10) (just use that  $I \otimes \mathbb{Z}_p = R \otimes \mathbb{Z}_p = \mathcal{O}_K \otimes \mathbb{Z}_p$ ), so we omit the details. It remains to prove this when  $p = 2$ . Since  $\delta, \epsilon$  and  $d$  are coprime to 2, it would be enough to show that  $\phi \otimes \mathbf{1}$  maps  $\mathcal{O}_K \otimes \mathbb{Z}_2$  into  $\mathcal{O}_L \otimes \mathbb{Z}_2$ : Let  $\omega \in \mathcal{O}_K$ , then  $2\omega \in R$ , and so  $\phi(2\omega) \in S$ , moreover,

$$\text{Tr} \left( \frac{\phi(2\omega)^2}{\epsilon} \right) = \text{Tr} \left( \frac{(2\omega)^2}{\delta} \right) \equiv 0 \pmod{2\mathbb{Z}_2}$$

and thus  $\phi(2\omega) \otimes 1 \equiv 0 \pmod{2(\mathcal{O}_L \otimes \mathbb{Z}_2)}$ , i.e.,  $\phi(\omega) \otimes 1 \in \mathcal{O}_L \otimes \mathbb{Z}_2$ .

Now we have two cases:

- If  $K \not\cong L$ , by (3.8),  $K$  and  $L$  are linearly disjoint, and if  $\{\sigma_1, \sigma_2, \sigma_3\}$  and  $\{\tau_1, \tau_2, \tau_3\}$  are the embeddings of  $K$  and  $L$ , respectively, with  $\sigma_1$  and  $\tau_1$  the inclusions  $x \mapsto x$ ; then for each  $1 \leq i, j \leq 3$  exists a unique embedding  $\theta_{ij} : KL \hookrightarrow \mathbb{R}$  extending both  $\sigma_i$  and  $\tau_j$ . Let  $c_{ij} := \langle \sigma_i, \tau_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \sqrt{\frac{\sigma_i(\delta)}{\tau_j(\epsilon)}} \in \mathbb{R}$ , since  $\phi$  is an isometry one check easily that

$$U = (c_{ij})$$

must be orthogonal. But  $\theta_{ij}(c_{11}^2) = c_{ij}^2 \leq 1$ , so  $c_{11}^2$  is a positive real algebraic integer all whose conjugates are bounded by 1 and thus  $c_{11}^2 \in \{0, 1\}$ , this contradicts that  $U$  is orthogonal.

- If  $K \cong L$ , then  $\mathcal{O}_K \cong \mathcal{O}_L$ . So the integral ternary quadratic forms defining the quartic rings form which  $(R, I, \delta)$  and  $(s, J, \epsilon)$  come from have equivalent cubic resolvent forms  $f$ , hence the corresponding cubic forms  $F = 2f$  are equivalent and thus  $R \cong S$ . By changing  $S, J$  and  $\epsilon$  by their images in  $R$  under this isomorphism if necessary, we may assume  $R = S$ .

Let  $c_{ij} := \langle \sigma_i, \sigma_j \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \sqrt{\frac{\sigma_i(\delta)}{\sigma_j(\epsilon)}} \in \mathbb{R}$ , as before we have that  $U = (c_{ij})$  is orthogonal and  $c_{ij}^2 \leq 1$  for all  $i, j$ . Now let  $\tilde{K}$  be the Galois closure of  $K$ , for every  $\sigma \in \text{Gal}(\tilde{K}/\mathbb{Q})$  and  $i, j$  we have that

$$\sigma(c_{ij}^2) = c_{i'j'}^2 \leq 1$$

for some  $i', j'$ , thus here again we find  $c_{ij}^2 \in \{0, 1\}$ , moreover, since  $U$  is orthogonal exactly one of the  $c_{ij}^2$  is 1 on each column and row of  $U$  and from the relation

$$\sigma_i \phi = \sum_j \langle \sigma_j, \sigma_i \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \sigma_j$$

follows that  $c_{ij}^2 = \delta_{ij}$  (Kronecker delta). In particular, if  $\kappa = \langle \sigma_1, \sigma_1 \phi \rangle_{\text{tr}_{K/\mathbb{Q}}} \in K$

$$1 = c_{11}^2 = \kappa^2 \frac{\delta}{\epsilon}$$

hence  $\epsilon = \kappa^2 \delta$  and, as  $\phi(x) = \kappa x$ ,  $J = \kappa I$ . Therefore, the triples  $(R, I, \delta)$  and  $(R, J, \epsilon)$  are equivalent.

□

# Bibliography

- [BH16] Manjul Bhargava and Piper Harron. The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields. *Compositio Mathematica*, 152(6):1111–1120, 2016.
- [Bha01] Manjul Bhargava. Higher composition laws. *PhD thesis, Princeton Univ.*, 2001.
- [Bha04a] Manjul Bhargava. Higher composition laws ii: On cubic analogues of gauss composition. *Annals of mathematics*, pages 865–886, 2004.
- [Bha04b] Manjul Bhargava. Higher composition laws iii: The parametrization of quartic rings. *Annals of mathematics*, 159(3):1329–1360, 2004.
- [BMP] B.Erez, J. Morales, and R. Perlis. Sur le genre de la form trace. *Seminaire de Théorie des Nombre de Bordeaux*.
- [BV<sup>+</sup>15] Manjul Bhargava, Ila Varma, et al. On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. *Duke Mathematical Journal*, 164(10):1911–1933, 2015.
- [Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.
- [CP84] Pierre E Conner and Rivka Perlis. *A survey of trace forms of algebraic number fields*, volume 2. World scientific, 1984.
- [DM96] John D Dixon and Brian Mortimer. *Permutation groups*, volume 163. Springer Science & Business Media, 1996.
- [FJ08] Michael D Fried and Moshe Jarden. Field arithmetic. a series of modern surveys in mathematics, 11, 2008.
- [Ger08] Larry J Gerstein. *Basic quadratic forms*, volume 90. American Mathematical Soc., 2008.
- [Hal15] Brian Hall. *Lie groups, Lie algebras, and representations: an elementary introduction*, volume 222. Springer, 2015.

- 
- [Har17] Robert Harron. The shapes of pure cubic fields. *Proceedings of the American Mathematical Society*, 145(2):509–524, 2017.
- [Höl95] Otto Hölder. Bildung zusammengesetzter gruppen. *Mathematische Annalen*, 46(3):321–422, 1895.
- [Kon95] Takeshi Kondo. Algebraic number fields with the discriminant equal to that of a quadratic number field. *Journal of the Mathematical Society of Japan*, 47(1):31–36, 1995.
- [Lin18] Benjamin Linowitz. Brauer equivalent number fields and the geometry of quaternionic shimura varieties. *arXiv preprint arXiv:1804.07367*, 2018.
- [Mau73] Donald Maurer. The trace-form of an algebraic number field. *Journal of Number theory*, 5(5):379–384, 1973.
- [Mil] James S Milne. Algebraic number theory (v3. 03), 2011. URL: [www.jmilne.org/math](http://www.jmilne.org/math).
- [Mil58] Donald W Miller. On a theorem of hölder. *American Mathematical Monthly*, pages 252–254, 1958.
- [MS] Guillermo Mantilla-Soler. The genus of the integral trace form. *Authors webpage*.
- [MS10] Guillermo Mantilla-Soler. Integral trace forms associated to cubic extensions. *Algebra & Number Theory*, 4(6):681–699, 2010.
- [MS12] Guillermo Mantilla-Soler. On number fields with equivalent integral trace forms. *International Journal of Number Theory*, 8(07):1569–1580, 2012.
- [MS15] Guillermo Mantilla-Soler. On the arithmetic determination of the trace. *Journal of Algebra*, 444:272–283, 2015.
- [MSM16] Guillermo Mantilla-Soler and Marina Monsurrò. The shape of  $\mathbb{Z}/l\mathbb{Z}$ -number fields. *The Ramanujan Journal*, 3(39):451–463, 2016.
- [N<sup>+</sup>88] Jin Nakagawa et al. On the galois group of a number field with square free discriminant. *Rikkyo Daigaku sugaku zasshi*, 37(1):95–98, 1988.
- [Nar13] Wladyslaw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Science & Business Media, 2013.
- [Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

- 
- [Odu13] Frances Ogochukwu Odumodu. *Do Trace Forms Characterise Number Fields?* PhD thesis, Stellenbosch University, 2013.
- [O'M13] Onorato Timothy O'Meara. *Introduction to quadratic forms*, volume 117. Springer, 2013.
- [Per77] Robert Perlis. On the equation  $\zeta_k(s) = \zeta_{K'}(s)$ . *Journal of number theory*, 9(3):342–360, 1977.
- [Sch94] Roland Schmidt. *Subgroup lattices of groups*, volume 14. Walter de Gruyter, 1994.
- [Ser79] Jean-Pierre Serre. *Local fields. Translated from the French by Marvin Jay Greenberg*, volume 67. 1979.
- [Tau68] Olga Taussky. The discriminant matrices of an algebraic number field. *Journal of the London Mathematical Society*, 1(1):152–154, 1968.
- [Ter97] David C. Terr. *The distribution of shapes of cubic orders*. Ph.d. thesis, University of California, Berkeley, 1997.