A proof of a conjecture on trace-zero forms and shapes of number fields

Guillermo Mantilla-Soler\textsuperscript{2,3,*} and Carlos Rivera-Guaca\textsuperscript{1}

Abstract

In 2012 the first named author conjectured that totally real quartic fields of fundamental discriminant are determined by the isometry class of the integral trace zero form; such conjecture was based on computational evidence and the analog statement for cubic fields which was proved using Bhargava’s higher composition laws on cubes. Here, using Bhargava’s parametrization of quartic fields we prove the conjecture by generalizing the ideas used in the cubic case. Since at the moment, for arbitrary degrees, there is nothing like Bhargava’s parametrizations we cannot deal with degrees $n > 5$ in a similar fashion. Nevertheless, using some of our previous work on trace forms we generalize this result to higher degrees. We show that if $n$ is an integer bigger than 2 such that $(\mathbb{Z}/n\mathbb{Z})^\ast$ is a cyclic group, the shape is a complete invariant for degree $n$ number fields that are totally real and have fundamental discriminant.

1 Introduction

Let $K$ be a number field of degree $n := [K : \mathbb{Q}]$ and let $O_K$ be its maximal order. The trace zero module of $O_K$ is the $\mathbb{Z}$-submodule of $O_K$ given by the kernel of the trace map, i.e., $O_K^0 = K^0 \cap O_K$ where $K^0 := \{x \in K : \text{tr}_{K/\mathbb{Q}}(x) = 0\}$. The integral trace-zero form of $K$ is the isometry class of the rank $n - 1$ quadratic $\mathbb{Z}$-module $(O_K^0, \text{tr}_{K/\mathbb{Q}})$ given by restricting the trace pairing from $O_K \times O_K$ to $O_K^0 \times O_K^0$. It is clear that the isometry class of the quadratic module $(O_K^0, \text{tr}_{K/\mathbb{Q}})$ determines the field $K$ for $n = 1, 2$. This is not the case for cubic fields, see \cite[Sect. 3]{11}. However, it can be shown, using Delone-Faddeev-Gross parametrization of cubic rings and Bhargava’s higher composition laws on cubes, that for totally real cubic fields of fundamental discriminant $(O_K^0, \text{tr}_{K/\mathbb{Q}})$ determines the field $K$ (see \cite[Theorem 6.5]{11}). In \cite{10} the first named author conjectured that the above property of the trace zero form is not only particular of degrees less than 4 but also works for quartic fields (see \cite[Conjecture 2.10]{10}). In Sect. 4 we prove such conjecture via Bhargava’s parametrization of quartic rings:

Theorem (cf. Sect. 4). 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

$$(O_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (O_L^0, \text{tr}_{L/\mathbb{Q}})$$
exists, then $K \cong L$.

Another quadratic invariant, with a more geometric interpretation and closely related to the trace zero form, that has been studied by several authors is the shape of $K$. Endow $K$ with the real-valued $\mathbb{Q}$-bilinear form $b_K$ whose associated quadratic form is given by

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

The shape of $K$, denoted $\text{Sh}(K)$, is the isometry equivalence class of $(O_K^1, b_K)$ up to scalar multiplication. Here $O_K^1$ is the image of $O_K$ under the projection map, $\alpha \mapsto \alpha_{\perp} := n\alpha - \text{tr}_{K/Q}(\alpha)$, i.e.,

$$O_K^1 := \{\alpha_{\perp} : \alpha \in O_K\} = (\mathbb{Z} + nO_K) \cap O_K^0.$$ 

Thus $\text{Sh}(K) = \text{Sh}(L)$ if and only if $(O_K^1, b_K) \cong (O_L^1, \lambda b_L)$ for some $\lambda \in \mathbb{R}^*$. Equivalently, $\text{Sh}(K)$ can be thought as the $(n - 1)$-dimensional lattice inside $\mathbb{R}^n$, via the Minkowski embedding, that is the orthogonal complement of 1 and that is defined up to reflection, rotations and scaling by $\mathbb{R}^*$. Hence $\text{Sh}(K)$ correspond to an element to the space of shapes

$$S_{n-1} := \text{GL}_{n-1}(\mathbb{Z}) \setminus \text{GL}_{n-1}(\mathbb{R})/\text{GO}_{n-1}(\mathbb{R}).$$

The distribution of shapes of number fields in $S_n$ have been the subject of a lot of interesting current research (see [5,7,8,12]). Our main result about shapes and trace zero forms is the following:

**Theorem** (cf. Theorem 2.13). Let $K$ be a totally real number field of fundamental discriminant and degree $n \geq 3$. If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, then for any number field $L$ the following are equivalent:

(i) $K \cong L$.

(ii) $(O_K^1, \text{tr}_{K/Q}) \cong (O_L^1, \text{tr}_{L/Q}).$

(iii) $\text{Sh}(K) = \text{Sh}(L)$ and $L$ is totally real with fundamental discriminant.

If $(n, \text{Disc}(K)) = 1$ the above are also equivalent to (iv) $(O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q}).$

Based on this theorem, Question 2.18 and the computational evidence given in [10, Table 1] we propose the following conjecture:

**Conjecture 1.1** Let $K$ be a totally real octic number field with fundamental discriminant. If $L$ is a tamely ramified number field such that an isomorphism of quadratic modules

$$(O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q})$$

exists, then $K \cong L$.

1.1 Structure of the paper

In Sect. 2 we prove our main results on trace zero modules and shapes of arbitrary degree. In Sect. 3 we review Casimir invariants and some of their properties. In Sect. 4 we prove [10, Conjecture 2.10] using Bhargava’s parametrization of quartic rings.

2 From $O_K^0$ and $O_K^1$ to $O_K$

In this section we study in detail the structure of the modules $O_K^0$ and $O_K^1$ and layout a strategy to see when an isometry between the trace zero parts (resp. shapes) can be lifted to a full isometry of between the integral traces. By the end of this section we explain what are the limitations of such strategy.
2.1 The discriminants of $O_K^0$ and $O_K^\perp$

We start by finding out what are the values of the determinants of the quadratic modules $O_K^0$ and $O_K^\perp$.

We denote by $\text{Disc}(O_K^0)$ (resp. $\text{Disc}(O_K^\perp)$) the determinant of the quadratic module $(O_K^0, \text{tr}_{K/Q})$ (resp. $(O_K^\perp, \text{tr}_{K/Q})$).

The following lemma will be useful to us.

**Lemma 2.1** Let $n$ be an integer bigger than 1 and let $K$ be a degree $n$ number field. Let $k$ be the positive integer such that $\text{tr}_{K/Q}(O_K) = k\mathbb{Z}$. Then,

$$\text{Disc}(O_K^0) = \frac{n}{K^2} \text{Disc}(K) \text{ and } \text{Disc}(O_K^\perp) = n^{2n-3} \text{Disc}(K).$$

**Proof** Using the surjectivity of trace map in the instances $\text{tr}_{K/Q} : O_K \to k\mathbb{Z}$ and $\text{tr}_{K/Q} : \mathbb{Z} + nO_K \to n\mathbb{Z}$ we observe that

$$(O_K/(\mathbb{Z} + O_K^0)) \cong \mathbb{Z}/(n/k)\mathbb{Z} \text{ and } \mathbb{Z} + nO_K = \mathbb{Z} + O_K^\perp.$$

Since $O_K$ has an integral basis containing 1, there is an isomorphism of $\mathbb{Z}$-modules $O_K/(\mathbb{Z} + nO_K) \cong (\mathbb{Z}/n\mathbb{Z})^{n-1}$. In particular,

$$[O_K : \mathbb{Z} + O_K^0] = n/k \text{ and } [O_K : \mathbb{Z} + O_K^\perp] = n^{n-1}.$$

The result follows from this and from the fact that the decomposition $\mathbb{Z} + O_K^0$ is orthogonal with respect the trace pairing. $\Box$

**Lemma 2.2** (Maurer [14]). Let $K$ be a number field and let $k$ be an integer such that $\text{tr}_{K/Q}(O_K) = k\mathbb{Z}$. A prime $p$ divides $k$ if and only if $p \mid e(p|p)$ for all primes $p$ in $K$ lying over $p$.

**Proof** We will give an alternative proof to the one presented in [14]. In fact, it is not hard to see that the following slightly more general statement holds: Let $\mathcal{D}_{K/Q}$ denote the different ideal of $K/Q$, then for a rational prime $p$ we have

$$v_p(k) = \min_{p \mid p} \left[ \frac{v_p(D_{K/Q})}{e(p|p)} \right].$$

The lemma will follow from the fact $v_p(D_{K/Q}) \geq e(p|p) \iff p \mid e(p|p)$. Since the trace map is $\mathbb{Z}$-linear, and by hypothesis its image is $k\mathbb{Z}$, the result is obtained from the following equivalences. For any $r \in \mathbb{Z}^+ \cup \{0\}$,

$$p^r \mid k \iff \text{tr}_{K/Q}(O_K) \subset p^r\mathbb{Z}$$
$$\iff \text{tr}_{K/Q}(p^{-r}O_K) \subset \mathbb{Z}$$
$$\iff p^{-r} \in \mathcal{D}_{K/Q}^{-1}$$
$$\iff \mathcal{D}_{K/Q} \subset p^rO_K$$
$$\iff rv_p(p) \leq v_p(D_{K/Q}) \text{, for all } p \text{ prime in } K$$
$$\iff re(p|p) \leq v_p(D_{K/Q}) \text{, for all } p \text{ dividing } p$$
$$\iff r \leq \left[ \frac{v_p(D_{K/Q})}{e(p|p)} \right] \text{, for all } p \text{ dividing } p$$
$$\iff r \leq \min_{p \mid p} \left[ \frac{v_p(D_{K/Q})}{e(p|p)} \right].$$

The result follows, since $v_p(k)$ is the largest of such $r$. $\Box$
Corollary 2.3  Let \( n \) be a positive integer and let \( L \) be a degree \( n \) number field. Suppose that any of the following conditions holds:

(i) Every prime \( p \mid n \) satisfies \( p^n \nmid \text{Disc}(L) \).
(ii) The extension \( L/\mathbb{Q} \) is tamely ramified at \( p \), for every \( p \mid n \).
(iii) The field \( L \) has fundamental discriminant and \( n > 2 \).

Then, \( \text{tr}_{L/\mathbb{Q}}(O_L) = \mathbb{Z} \). Moreover, if \( n = 4 \) condition (i) is equivalent to \( \text{tr}_{L/\mathbb{Q}}(O_L) = \mathbb{Z} \) and if \( n \) is prime, conditions (i) and (ii) are equivalent to \( \text{tr}_{L/\mathbb{Q}}(O_L) = \mathbb{Z} \).

Proof  Let \( k \in \mathbb{Z}^+ \) be such that \( \text{tr}_{L/\mathbb{Q}}(O_L) = k\mathbb{Z} \).

- Suppose that (i) holds. By definition of discriminant, as the determinant of a Gram matrix of \((O_L, \text{tr}_{L/\mathbb{Q}})\), we know that \( k^n \mid \text{Disc}(L) \). Since \( n = \text{tr}_{L/\mathbb{Q}}(1) \) we have that \( k \mid n \), hence any prime \( p \) dividing \( k \) would satisfy \( p^n \mid \text{Disc}(L) \) and \( p \mid n \). By hypothesis (i) we conclude that \( k \) has no prime divisor so \( k = 1 \).
- Suppose that (ii) holds. If there is a prime \( p \) dividing \( k \) then \( p \) divides \( n \). By (ii) we have that \( p \mid e(p|p) \) for every prime \( p \) lying over \( p \), contradicting Lemma 2.2 therefore \( k = 1 \).
- Suppose that (iii) holds. The extension \( L/\mathbb{Q} \) 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 the factorization type of 2 in \( L \). Then \( 2 \mid e_i \) for all \( i \), and
  \[
  3 \geq v_2(\text{Disc}(L)) \geq e_1f_1 + e_2f_2 + \cdots = n > 2
  \]
  yields \( n = 3 = e_1f_1 + e_2f_2 + \cdots \equiv 0 \mod 2 \), a contradiction. Thus \( k = 1 \).

To prove the reciprocals suppose first that \( k = 1 \) and that \( n = p \) is prime. Let \( f_1^{e_1} \cdots f_g^{e_g} \) be factorization type of \( p \) in \( L \). If condition (ii) did not hold, there would be an index \( i \) such that \( p \mid e_i \) which we may assume is \( i = 1 \). In that case \( p = e_1f_1 + \cdots \geq p \) implies that there is only one prime \( p \) in \( L \) lying over \( p \) and for that prime \( p \mid e(p|p) = e_1 \), contradicting (2.2). Since condition (ii) always implies condition (i), this proves

\[
\text{tr}_{L/\mathbb{Q}}(O_L) = \mathbb{Z} \iff (ii) \iff (i),
\]

in this case.

Similarly, if \( k = 1, n = 4 \) and condition (i) did not hold, then \( 2^4 \nmid \text{Disc}(L) \). In particular 2 would be wildly ramified in \( L \), so its factorization type would be \( 1^22^1, 1^21^12^1 \) or \( 2^2 \). Since \( k = 1 \), only the first two cases are possible. However, for a prime \( p \) in \( K \) the exact power of \( p \) dividing the different ideal \( D_{L/K} \) is bounded by \( e \cdot (v_p(e) + 1) - 1 \), where \( e = e(p|p) \) and \( p = p \cap \mathbb{Z} \), thus in either case if \( p \) is the prime in \( L \) with \( e(p|2) = 2 \) we would have \( D_{L/K} = p^a \), where \( (a, 2) = 1 \) and \( v \leq 3 \). This yields \( 4 \leq v_2(\text{Disc}(L)) = v \cdot f(p | 2) = v \leq 3 \), a contradiction. 

We say that a number field \( L \) is tame, or tamely ramified, if no rational prime ramifies wildly in \( L \).

Lemma 2.4  Let \( n > 1 \) be an integer and let \( K \) and \( L \) be two degree \( n \) number fields. Suppose that \( K \) has fundamental discriminant and that \( L \) is tame. If

\[
(O_K^n, \text{tr}_{K/\mathbb{Q}}) \cong (O_L^n, \text{tr}_{L/\mathbb{Q}})
\]

then

\[
O_K^n \cong O_L^n
\]
then, \( \text{Disc}(K) = \text{Disc}(L) \) and moreover such discriminant is square free. In particular, a tame number field with fundamental discriminant has square free discriminant.

**Proof** Let us assume first that \( n > 2 \). In such case it follows from Corollary 2.3 that \( \text{tr}_{K/Q}(O_K) = \mathbb{Z} = \text{tr}_{L/Q}(O_L) \). Thus \( \text{Disc}(K) = \text{Disc}(L) \) thanks to Lemma 2.1. Let \( \bar{L} \) be the Galois closure of \( L/Q \). Recall that tame extensions are closed under composition and sub-extensions, see [15, Chapter II, Corollaries 7.8, 7.9]. Hence since \( L \) is tame so is \( \bar{L} \), and so it is any \( E/Q \) sub-extension of \( \bar{L}/Q \). If \( \text{Disc}(L) \) were not square free, and since it is a fundamental discriminant, the extension \( E = Q(\sqrt{\text{Disc}(L)})/Q \) would be a sub-extension \( \bar{L}/Q \) that is not tame; since it has wild ramification at \( p = 2 \). Now suppose \( n = 2 \). If \( \text{Disc}(K) \neq \text{Disc}(L) \) then, by Lemma 2.1, \( \text{Disc}(K) = 4\text{Disc}(L) \) which implies, since \( n = 2 \), that \( K \cong L \) thus \( \text{Disc}(K) = \text{Disc}(L) \) contradicting the initial hypothesis. \( \square \)

### 2.2 A basis for \( O_K^n \) and a condition of an isometry extension

For totally real number fields \( K \) and \( L \) we have that \( (O_K, \text{tr}_{K/Q}) \cong (O_L, \text{tr}_{L/Q}) \) always implies \( (O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q}) \). Moreover:

**Proposition 2.5** Let \( K, L \) be two totally real number fields and suppose

\[
\phi : (O_K, \text{tr}_{K/Q}) \sim (O_L, \text{tr}_{L/Q})
\]

is an isometry. Then, \( \phi(1) = \pm 1 \). In particular, the restriction of \( \phi \) induces an isometry between the integral trace zero parts of \( K \) and \( L \), and also between the shapes of \( K \) and \( L \).

**Proof** Because the fields have isometric integral trace forms, they must have the same degree, say \( n \). Now let \( \alpha := \phi(1) \). By hypothesis \( \alpha^2 \) is a totally positive algebraic integer such that \( \text{tr}_{L/Q}(\alpha^2) = \text{tr}_{L/Q}(\phi(1)^2) = \text{tr}_{K/Q}(1^2) = n \). Hence, from the AM-GM inequality applied to the \( n \) conjugates of \( \alpha^2 \in L \) over \( Q \), we find that the equality in

\[
1 \leq N_{L/Q}(\alpha^2)^{\frac{1}{n}} \leq \frac{\text{tr}_{L/Q}(\alpha^2)}{n} = 1
\]

implies \( \alpha^2 \in Q \) and thus \( \alpha^2 = 1 \). To prove the last claim, note that the isometry \( \phi \) maps the elements in \( O_K \) orthogonal to 1 precisely to the elements in \( \phi(O_K) = O_L \) orthogonal to \( \phi(1) = \pm 1 \), i.e., \( \phi(O_K^0) = O_L^0 \). Similarly, as \( \phi(\mathbb{Z} + nO_K) = \phi(1)\mathbb{Z} + nO_L = \mathbb{Z} + nO_L \), we have that \( \phi(O_K^0) = O_L^0 \).

The following example (found by ‘brute force” using Magma) shows that the converse of Proposition 2.5 is not true.

**Example 2.6** 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. The fields \( K \) and \( L \) are totally real with \( \text{Disc}(K) = 2^6 41^3 = \text{Disc}(L) \) and \( (O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q}) \). However \( (O_K, \text{tr}_{K/Q}) \not\cong (O_L, \text{tr}_{L/Q}) \) and \( (O_K^0, b_K) \not\cong (O_L^0, b_L) \).

In view of such example it is natural to ask under what conditions we could expect to have a reciprocal of Proposition 2.5. To address that question, we note that since \( K = \mathbb{Q} \perp K^0 \), each isometry \( \phi : (K^0, \text{tr}_{K/Q}) \sim (L^0, \text{tr}_{L/Q}) \) has two natural extensions to an isometry \( (K, \text{tr}_{K/Q}) \cong (L, \text{tr}_{L/Q}) \). The one taking 1 to 1 call it \( \phi^+ \) and the one taking 1 to \(-1 \) call it \( \phi^- \). These are in fact the only two possible extensions of \( \phi \). Indeed, given an isometry \( \phi : (K, \text{tr}_{K/Q}) \sim (L, \text{tr}_{L/Q}) \) extending \( \phi \), 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 $\phi(1) \in \mathbb{Q}$. Since $[K : \mathbb{Q}] = \text{tr}_{K/\mathbb{Q}}(1^2) = \text{tr}_{L/\mathbb{Q}}(\phi(1)^2) = [L : \mathbb{Q}]\phi(1)^2$ we obtain that $\phi(1) \in \{-1, +1\}$.

Since $K^0 = O_K^0 \cdot \mathbb{Q} = O_K^1 \cdot \mathbb{Q}$, it follows that an isometry

$$\varphi : (O_K^0, \text{tr}_{K/\mathbb{Q}}) \sim (O_L^0, \text{tr}_{L/\mathbb{Q}}) \text{ resp. } \varphi : (O_K^0, \text{tr}_{K/\mathbb{Q}}) \sim (O_L^1, \text{tr}_{L/\mathbb{Q}})$$

will lift to an isometry $(O_K, \text{tr}_{K/\mathbb{Q}}) \cong (O_L, \text{tr}_{L/\mathbb{Q}})$ if and only if either $\varphi^+(O_K) = O_L$ or $\varphi^-(O_K) = O_L$. But when do we have these equalities? This motivates the following:

**Lemma 2.7** Let $K$ and $L$ be number fields and let $n := [K : \mathbb{Q}]$. Then:

(i) Let $\varphi : (O_K^1, \text{tr}_{K/\mathbb{Q}}) \sim (O_L^1, \text{tr}_{L/\mathbb{Q}})$ be an isometry. Then $\varphi^\pm(O_K) = O_L$ if and only if there exists a basis $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ of $O_K$ such that $t_i \equiv \pm s_i \mod n$ 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 $\varphi(\alpha_i \pm) = n\beta_i - s_i \in O_L^1$, with $\beta_i \in O_L$.

(ii) Suppose that $\text{tr}_{K/\mathbb{Q}}(O_K) = k \mathbb{Z} = \text{tr}_{L/\mathbb{Q}}(O_L)$ with $k \in \mathbb{Z}^+$ and let $\varphi : (O_K^0, \text{tr}_{K/\mathbb{Q}}) \sim (O_L^0, \text{tr}_{L/\mathbb{Q}})$ be an isometry. Then $\varphi^\pm(O_K) = O_L$ if and only if $\varphi(\gamma_0) \equiv \pm 1 \mod n/k$. Here $\gamma_0 := 1 - (n/k)\gamma_K \in O_K^0$ where $\gamma_K$ is any element in $O_K$ such that $\text{tr}_{K/\mathbb{Q}}(\gamma_K) = k$.

**Proof** Note that in both cases the hypotheses and the existence of the respective isometry imply that $n = [L : \mathbb{Q}]$ and that $\text{Disc}(K) = \text{Disc}(L)$. For the degrees this is clear, and for the discriminants it follows from the equalities, see Lemma 2.1, $\text{Disc}(O_K^1) = n^{2n-3}\text{Disc}(K)$ and $\text{Disc}(O_K^0) = k^2\text{Disc}(K)$. Thus in each case $\varphi^\pm(O_K) \subset O_L$ if and only if $\varphi^\pm(O_K) = O_L$.

Now to prove (i) observe that for any basis $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ of $O_K$ we have

\[
\varphi^\pm(O_K) \subset O_L \iff \varphi^\pm(\alpha_i) \in O_L \quad \text{for all } 1 \leq i < n
\]

\[
\iff \varphi^\pm\left(\frac{\alpha_i + t_i}{n}\right) \in O_L \quad \text{for all } 1 \leq i < n
\]

\[
\iff \varphi(\alpha_i) \pm t_i \in \frac{n\beta_i - s_i}{n}O_L \quad \text{for all } 1 \leq i < n
\]

\[
\iff \varphi(\alpha_i) \pm t_i \in \frac{-s_i + t_i}{n}O_L \quad \text{for all } 1 \leq i < n
\]

\[
\iff s_i \equiv \pm t_i \mod n
\]

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

\[
\varphi^\pm(O_K) \subset O_L \iff \varphi^\pm(\gamma_K) \in O_L
\]

\[
\iff (k/n)\varphi^\pm(1 - \gamma_0) \in O_L
\]

\[
\iff (k/n)(\pm 1 - \varphi(\gamma_0)) \in O_L
\]

\[
\iff \varphi(\gamma_0) = \pm 1 \mod n/k
\]

\[\Box\]

To use this lemma, we begin by giving a description of the basis of $O_K^0$ that generalizes [11, Proposition 5.2]
Proposition 2.8 Suppose that $K$ is a number field of degree $n \geq 3$ and $\text{tr}_{K/Q}(O_K) = k\mathbb{Z}$, $k \in \mathbb{Z}^+$. There exists a $\mathbb{Z}$-basis \{1, $\alpha_1$, ..., $\alpha_{n-1}$\} of $O_K$ such that

\[
(\text{tr}_{K/Q}(\alpha_1), \ldots, \text{tr}_{K/Q}(\alpha_{n-2}), \text{tr}_{K/Q}(\alpha_{n-1})) =: (t_1, \ldots, t_{n-2}, t_{n-1}) \equiv (0, \ldots, 0, k) \mod n
\]

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

Remark 2.9 If $n = 2$, for any basis \{1, $\alpha_1$\} of $O_K$ we have that $\text{tr}_{K/Q}(\alpha_1) = t_1 \equiv k \mod 2$ and that \{(2/k)\alpha_1 - t_1/k\} is a basis of $O_K^0$.

The proof is based in the following elementary lemma:

Lemma 2.10 Let $r$ and $m \geq 2$ be integers, then:

(a) Given any sets of integers \{u_1, \ldots, u_m\} and \{s_1, \ldots, s_m\}, there exist integers \{c_1, \ldots, c_m\} such that $\sum_i c_is_i = 0$ and $\gcd(u_1 - c_1, \ldots, u_m - c_m) = 1$.

(b) If $\gcd(r, s_1, \ldots, s_m) = 1$, then there are integers \{h_1, \ldots, h_m\} such that

\[
\gcd(rh_1 + s_1, \ldots, rh_m + s_m) = 1.
\]

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

\[
f : \mathbb{Z}^m \twoheadrightarrow \mathbb{Z}/s\mathbb{Z} \ni (c_1, \ldots, c_m) \mapsto \sum_i c_is_i
\]
since $\mathbb{Z}$ is a PID, there is an exact sequence of $\mathbb{Z}$-modules $\mathbb{Z}^m \xrightarrow{g} \mathbb{Z}^m \xrightarrow{f} \mathbb{Z}/s\mathbb{Z} \rightarrow 0$.

For a prime $p$ denote $\nu \mapsto \nu\overline{p}$ the canonical projection $\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$ and $\overline{g} : \mathbb{F}_p^m \rightarrow \mathbb{F}_p^m$ the map induced by $g$. We claim that $\ker(\overline{g}) \neq \mathbb{F}_p^m$. Indeed, by tensoring with $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{F}_p$ we get an exact sequence of $\mathbb{F}_p$-spaces

\[
\mathbb{F}_p^m \xrightarrow{\overline{g}} \mathbb{F}_p^m \xrightarrow{\tilde{f}} \mathbb{F}_p \rightarrow 0.
\]

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

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

\[
X_p := \{\nu \in \mathbb{F}_p^m : \overline{g}(\nu) = \overline{u}\}.
\]

Then either $X_p = \emptyset$ or $X_p = \overline{v_0} + \ker(\overline{g})$ with $\overline{v_0} \in X_p$. In particular, from this together with the above claim, it follows that $X_p \neq \mathbb{F}_p^m$ so we may pick $\nu_p \in \mathbb{F}_p^m$ such that $\overline{g}(\nu_p) \neq \overline{u}$.

By the Chinese remainder theorem we can choose $\nu \in \mathbb{Z}^m$ such that

\[
\nu \equiv \nu_p \mod p \text{ for all } p \mid N.
\]

If $N = \pm 1$ take $\nu = 0$. Define $c := (c_1, \ldots, c_m) := g(\nu) \in \ker(f)$, then $\sum_i c_is_i = 0$ 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 therefore

\[
u \equiv c = g(\nu) \equiv g(\nu_p) \neq u \mod p
\]

a contradiction. This proves (a) whenever $N \neq 0$. On the other hand, if $N = 0$ pick any non-zero element \{(d_1, \ldots, d_m) \in \text{Ker}(f)\} (which exists because $m \geq 2$) and take $c_i := u_i - d_i/d$, where $d = \gcd(d_1, \ldots, d_m)$. Then, $\sum_i c_is_i = N - \sum_i d_is_i/d = 0$ and $\gcd(u_1 - c_1, \ldots, u_m - c_m) = \gcd(d_1/d, \ldots, d_m/d) = 1$, so (a) also holds in this case.
To prove (b), write $1 = ar + bs$ with $a, b \in \mathbb{Z}$ and write $bs = \sum_i u_is_i$ for some integers $\{u_i\}$. By (a) there are $\{c_i\}$ such that $\sum_i c_is_i = 0$ and that $v_i := u_i - c_i$ are coprime. Let $\{h_i\}$ be such that $\sum_i v_ih_i = a$. Then
\[
\sum_i v_i(\rho h_i + s_i) = r \sum_i v_ih_i + \sum_i v_is_i = ra + bs = 1
\]
and therefore the integers $\{rh_i + s_i\}$ are coprime. \hfill \box

**Proof of Proposition 2.8** Let $\{1, \beta_1, \ldots, \beta_{n-1}\}$ be a basis of $O_K$ and let $s_i := \text{tr}_{K/\mathbb{Q}}(\beta_i)$ for $1 \leq i \leq n - 1$. By hypothesis $(1/k)\text{tr}_{K/\mathbb{Q}}(O_K) = (n/k, s_1/k, \ldots, s_{n-1}/k)\mathbb{Z} = \mathbb{Z}$. By applying Lemma 2.10 (b) to $m := n - 1 \geq 2$ and $r := n/k$ we know that there are integers $\{h_1, \ldots, h_{n-1}\}$ such that $\{rh_1 + s_1/k, \ldots, rh_{n-1} + s_{n-1}/k\}$ are coprime. Therefore we can place those numbers as the last column vector of some matrix $A$ in $\text{GL}_{n-1}(\mathbb{Z})$, that is,
\[
(rh_1 + s_1/k, \ldots, rh_{n-1} + s_{n-1}/k)^t = A (0, \ldots, 0, 1)^t.
\]
Define the basis $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ by the relation
\[
(1, \alpha_1, \ldots, \alpha_{n-1})^t := \begin{bmatrix} 1 & 0 \\ 0 & A^{-1} \end{bmatrix} (1, \beta_1, \ldots, \beta_{n-1})^t
\]
then $(\alpha_1, \ldots, \alpha_{n-1})^t = A^{-1}(\beta_1, \ldots, \beta_{n-1})^t$ and
\[
(1/k) \left( \text{tr}_{K/\mathbb{Q}}(\alpha_1), \ldots, \text{tr}_{K/\mathbb{Q}}(\alpha_{n-1}) \right)^t = A^{-1}(s_1/k, \ldots, s_{n-1}/k)^t
\]
\[
\equiv A^{-1}(rh_1 + s_1/k, \ldots, rh_{n-1} + s_{n-1}/k)^t \mod r
\]
\[
= (0, \ldots, 0, 1)^t \mod r
\]
hence $(\text{tr}_{K/\mathbb{Q}}(\alpha_1), \ldots, \text{tr}_{K/\mathbb{Q}}(\alpha_{n-1})) \equiv (0, \ldots, 0, k) \mod n$.

To prove that $\{\alpha_1 - t_1/n, \ldots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$ is a $\mathbb{Z}$-basis of $O_K^\perp$ note that its $\mathbb{Z}$-span $C$ is clearly contained in $O_K^\perp$ and the $\mathbb{Z}$-span of $\{\alpha_1 - t_1/n, \ldots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$ has index $n/k$. Indeed, the matrix expressing $\{\alpha_1 - t_1/n, \ldots, \alpha_{n-2} - t_{n-2}/n, (n/k)\alpha_{n-1} - t_{n-1}/k\}$ in terms of the integral basis $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ of $K$ is
\[
\begin{bmatrix}
1 & 0 & 0 & \cdots & 0 \\
-t_1/n & 1 & 0 & \cdots & 0 \\
-t_2/n & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
-t_{n-1}/k & 0 & 0 & \cdots & n/k
\end{bmatrix}
\]
so its determinant is $n/k$. It follows that $\text{Disc}(C) = \frac{n}{k^2} \text{Disc}(K) = \text{Disc}(O_K^\perp)$ and therefore $C = O_K^\perp$. \hfill \box

### 2.3 Proofs of the main results

We are now ready to prove the following partial reciprocal of Proposition 2.5.

**Theorem 2.11** Let $n$ be a positive integer and let $K$ be a degree $n$ number field. Suppose that $\text{tr}_{K/\mathbb{Q}}(O_K) = \mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. Then given a number field $L$ we have that:

(i) Every isometry $\varphi : (O_K^\perp, \text{tr}_{K/\mathbb{Q}}) \simto (O_L^\perp, \text{tr}_{L/\mathbb{Q}})$ extends to an isometry
\[
\phi : (O_K, \text{tr}_{K/\mathbb{Q}}) \simto (O_L, \text{tr}_{L/\mathbb{Q}}).
\]
(ii) If \((n, \text{Disc}(K)) = 1\), then every isometry \(\varphi : (O_K^0, \text{tr}_{K/Q}) \sim (O_L^0, \text{tr}_{L/Q})\) also extends to an isometry \(\varphi : (O_K, \text{tr}_{K/Q}) \sim (O_L, \text{tr}_{L/Q})\).

\[\text{Proof}\] In the case \(n = 1\) there is nothing to prove and the case \(n = 2\) is easy to check, so let us suppose that \(n \geq 3\).

(i) Let \(\{1, \alpha_1, \ldots, \alpha_{n-1}\}\) be any basis of \(O_K\). Let \(\alpha_i := \text{tr}_{K/Q}(\alpha_i), 1 \leq i < n\), so that \(\alpha_i \perp n\alpha_1 - t_i\) is a basis of \(O_K^1\) and for each \(1 \leq i < n\) choose \(\beta_i \in O_L\) and \(s_i \in \mathbb{Z}\) such that

\[y_i := \varphi(\alpha_i) = n\beta_i - s_i \in O_L^1.\]

Then \(\text{tr}_{L/Q}(y_iy_j) = n^2\text{tr}_{L/Q}(\beta_i\beta_j) - ns_is_j \equiv -ns_is_j \mod n^2\) and since \(\text{tr}_{L/Q}(y_iy_j) = \text{tr}_{K/Q}(\alpha_i\alpha_j)|\mathbf{L}/\mathbf{Q}|\), we conclude that

\[t_it_j \equiv s_is_j \mod n, \text{ for all } 1 \leq i, j < n.\]

Let \(u_i\) be integers such that \(\sum u_it_i \equiv 1 \mod n\) and let \(u := \sum u_is_i\). Then \(su \equiv ti \mod n\) for all \(1 \leq i < n\), in particular \((u, n) = 1\). If \(v\) is the multiplicative inverse of \(u\) modulo \(n\) then

\[t_it_j \equiv v^2t_i^*t_j \mod n, \text{ for all } 1 \leq i, j < n.\]

Hence \(v^2 \equiv 1 \mod n\), and since \((\mathbb{Z}/n\mathbb{Z})^\times\) is cyclic \(v \equiv \pm 1 \mod n\), thus \(s_i \equiv \pm t_i \mod n\) for all \(1 \leq i < n\). Thanks to Lemma 2.7 either \(\phi = \varphi^+\) or \(\phi = \varphi^-\) extend \(\varphi\) to an isometry \((O_K, \text{tr}_{K/Q}) \sim (O_L, \text{tr}_{L/Q})\).

(ii) First note that we must have \(\text{tr}_{L/Q}(O_L) = \mathbb{Z}\). If \(k\) is a positive integer such that \(\text{tr}_{L/Q}(O_L) = k\mathbb{Z}\) we have, thanks to Lemma 2.1, that the existence of the isometry \(\varphi\) implies \(n\text{Disc}(K) = \frac{n^2}{k^2}\text{Disc}(L)\). Notice that \(\text{tr}_{L/Q}(O_L) = k\mathbb{Z}\) implies that \(k^{n-2} | \text{Disc}(L)\), i.e., \(k^{n-2} | \text{Disc}(K)\). Since \(k | n, n \geq 3\), and \((\text{Disc}(K), n) = 1\) we conclude that \(k = 1\).

Let \(\{1, \alpha_1, \ldots, \alpha_{n-1}\}\) be an integral basis of \(O_K\) and let \(\{t_1, \ldots, t_{n-1}\}\) be as in Proposition 2.8 so that

\[w_1 := \alpha_1 - t_1/n, \ldots, w_{n-2} := \alpha_{n-2} - t_{n-2}/n, w_{n-1} := n\alpha_{n-1} - t_{n-1}\]

is a basis of \(O_K^0\). Note that for all \(1 \leq i < n\) we have

\[\text{tr}_{K/Q}(w_iw_{n-1}) = \text{tr}_{K/Q}(w_i(n\alpha_{n-1} - t_{n-1})) = n\text{tr}_{K/Q}(w_i\alpha_{n-1}) \equiv 0 \mod n\]

and for \(i = n - 1\)

\[\frac{1}{n}\text{tr}_{K/Q}(w_{n-1}^2) = \text{tr}_{K/Q}(mt_{n-1}^2 - t_{n-1}\alpha_{n-1}) = n\text{tr}_{K/Q}(\alpha_{n-1}^2) - t_{n-1}^2 \equiv -1 \mod n.\]

Let us define \(\theta_i := \varphi(w_i), 1 \leq i < n\). Take \(\gamma_L \in O_L\) such that \(\text{tr}_{K/Q}(\gamma_L) = 1\) 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 \(\theta_i \equiv \sum l_i\theta_i \mod n\) we find that the Gram matrix \(G := (\text{tr}_{K/Q}(w_iw_j)) = (\text{tr}_{L/Q}(\theta_i\theta_j))\) satisfies

\[G(l_1, \ldots, l_{n-1})^t \equiv 0 \mod n.\]
Call $G^*$ the matrix obtained from $G$ dividing the last column by $n$, which has integer entries thanks to $(\ast)$. Then
\[ G^* (l_1, \ldots, l_{n-2}, 0)^t \equiv G^* (l_1, \ldots, l_{n-2}, nl_{n-1})^t = G (l_1, \ldots, l_{n-2}, l_{n-1})^t \equiv 0 \pmod{n}. \]

From Lemma 2.1 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 $l_{n-1} = 1 \equiv 0 \pmod{n}$, squaring this congruence and taking traces again we find
\[
\begin{align*}
l_{n-1}^2 & \equiv 2l_{n-1} + 1 \equiv 0 \pmod{n} \\
\Rightarrow l_{n-1}^2 - 2l_{n-1} + 1 & \equiv 0 \pmod{n}
\end{align*}
\]

Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, $l_{n-1} \equiv \pm 1 \pmod{n}$. 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 Lemma 2.7(ii). □

**Corollary 2.12** Let $K$ be a totally real number field of fundamental discriminant and of degree $n \geq 3$. Suppose that $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclic. 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) $(\mathcal{O}_K^+, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^+, \text{tr}_{L/\mathbb{Q}})$.
(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) $(\mathcal{O}_K^0, \text{tr}_{K/\mathbb{Q}}) \cong (\mathcal{O}_L^0, \text{tr}_{L/\mathbb{Q}})$.

**Proof** The equivalences (i) $\iff$ (ii) and (i) $\iff$ (ii) $\iff$ (iv) under the additional conditions follow from Proposition 2.5, Theorem 2.11 and the fact that $\text{tr}_{K/\mathbb{Q}}(\mathcal{O}_K) = \mathbb{Z}$ (since $K$ has fundamental discriminant). It remains to prove (ii) $\iff$ (iii):

$\Rightarrow$ Since $L$ is totally real $b_K = \text{tr}_{K/\mathbb{Q}}$ and $\text{Sh}(K) = \text{Sh}(L)$. Furthermore, $\text{Disc}(L) = \text{Disc}(K)$ is fundamental.

$\Leftarrow$ Let $\lambda \in \mathbb{R}^+$ be such that an isometry $\varphi : (\mathcal{O}_K^+, \text{tr}_{K/\mathbb{Q}}) \to (\mathcal{O}_L^+, \lambda \text{tr}_{L/\mathbb{Q}})$ exists. Let $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis of $\mathcal{O}_K$, take $x_i := \alpha_i + t_i, 1 \leq i < n$ $t_i := \text{tr}_{K/\mathbb{Q}}(\alpha_i)$, as basis of $\mathcal{O}_K^+$ and define $y_i := \varphi(x_i) = n\beta_i - s_i, \beta_i \in \mathcal{O}_L, s_i \in \mathbb{Z}$. Then, $\text{tr}_{K/\mathbb{Q}}(x_iy_i) = \lambda \text{tr}_{L/\mathbb{Q}}(y_i^2)$ for all $1 \leq i, j < n$. In particular $\lambda$ is a positive rational number so we may write $\lambda = r/s$ and $r, s$ are coprime positive integers.

Since $n^{2n-3}\text{Disc}(K) = \text{Disc}(\mathcal{O}_K^+) = \det(\mathcal{O}_L^+, \lambda \text{tr}_{L/\mathbb{Q}}) = \lambda^{n-1}n^{2n-3}\text{Disc}(L)$ we know that
\[
\begin{align*}
r^{n-1}\text{Disc}(K) & = (r/s)^{n-1}\text{Disc}(L)
\end{align*}
\]

Thus $s^2 | \text{Disc}(K)$ 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 $s^2 | \text{Disc}(L)$ 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 \((1/4)\text{tr}_{K/Q}(x_i x_j) \equiv -t_i t_j \mod 4\) and \((1/4)\text{tr}_{L/Q}(y_i y_j) \equiv -s_i s_j \mod 4\), this implies
\[
t_i t_j \equiv -(1/4)\text{tr}_{K/Q}(x_i x_j) = -(1/2)\text{tr}_{K/Q}(y_i y_j) \equiv 2s_i s_j \mod 4
\]
which yields \( t_i t_j \equiv 0 \mod 2 \) for all \( 1 \leq i, j < n \) contradicting \( \text{tr}_{K/Q}(O_K) = \mathbb{Z} \).

• 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 \( \text{Disc}(L) = \text{Disc}(K)/4 \equiv 3 \mod 4 \) or \( v_2(\text{Disc}(K)) = 3 \) and \( v_2(\text{Disc}(L)) = 1 \). Both cases lead to a contradiction since by Stickelberger’s criterion, applied to \( \text{Disc}(L) \), the discriminant of a number field is equal to either 0 or 1 modulo 4.

Thus \( r = 1 \) and by symmetry of the argument \( s = 1 \), therefore \( \lambda = 1 \) and \((O_K^+, \text{tr}_{K/Q}) \cong (O_L^+, \text{tr}_{L/Q})\) as required. \( \square \)

**Theorem 2.13** Let \( K \) be a totally real number field of fundamental discriminant and of degree \( n \geq 3 \). Suppose that \((\mathbb{Z}/n\mathbb{Z})^\times\) is cyclic. For any number field \( L \) the following are equivalent:

(i) \( K \cong L \).

(ii) \((O_K^+, \text{tr}_{K/Q}) \cong (O_L^+, \text{tr}_{L/Q})\).

(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) \( (O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q})\).

**Proof** The result follows from Corollary 2.12 and [13, Theorem 5.3]. \( \square \)

### 2.4 Strategy’s limitations

The following examples try to illustrate the limitations of the strategy employed to prove Theorems 2.11, 2.13 and test the sharpness of the statements. All the examples here have been found by conveniently looking at John Jones tables [9]. The calculations of sizes of orthogonal groups have been carried out with \texttt{Magma}.

Suppose a number field \( K \) is totally real with \( \text{tr}_{K/Q}(O_K) = k\mathbb{Z}, k \in \mathbb{Z}^+ \), then by Proposition 2.5 the restrictions maps

\[
\text{Aut}(O_K, \text{tr}_{K/Q}) \to \text{Aut}(O_K^+, \text{tr}_{K/Q}) \text{ and } \text{Aut}(O_K, \text{tr}_{K/Q}) \to \text{Aut}(O_K^0, \text{tr}_{K/Q})
\]

are well defined homomorphism of groups. Moreover, these maps are injective if \( n \mid k \).

This is because given \( \varphi \) in either codomain, \( \varphi^+ \) and \( \varphi^- \) are the only possible pre-images of \( \varphi \) and they cannot both extend \( \varphi \), otherwise we would have

\[
n\varphi^+(\gamma_K) - k = \varphi^+(n\gamma_K - k) = \varphi^-(n\gamma_K - k) = n\varphi^-(\gamma_K) + k,
\]

where \( \gamma_K \in O_K \) and \( \text{tr}_{K/Q}(\gamma_K) = k \) so \( -k \equiv k \mod n \) and \( n | k \).

It follows that, when \( n \mid k \), every automorphism of \((O_K^+, \text{tr}_{K/Q})\) can be extended to all \( O_K \) if and only if \( \#\text{Aut}(O_K, \text{tr}_{K/Q}) = \#\text{Aut}(O_K^+, \text{tr}_{K/Q}) \) and in general the restriction map will not be surjective if \( \#\text{Aut}(O_K, \text{tr}_{K/Q}) < \#\text{Aut}(O_K^+, \text{tr}_{K/Q}) \), similarly for \((O_K^0, \text{tr}_{K/Q})\).

**Example 2.14** Let \( K \) be the cubic field with defining polynomial \( x^3 + x^2 - 8x + 3 \), then \( K \) is totally real, \( \text{Disc}(K) = 3 \cdot 5^2 \cdot 19 \), \( \text{tr}_{K/Q}(O_K) = \mathbb{Z} \) and

\[
\#\text{Aut}(O_K^+, \text{tr}_{K/Q}) = \#\text{Aut}(O_K, \text{tr}_{K/Q}) = 2 \neq 4 = \#\text{Aut}(O_K^0, \text{tr}_{K/Q})
\]
Recall from Corollary 2.3(i) that \( O_K \) as \( K \) is totally real, \( \text{Disc}(O_K) = 26 \), \( \text{tr}_{K/Q}(O_K) = 2 \mathbb{Z} \) and

\[
\#\text{Aut}(O_K, \text{tr}_{K/Q}) = 8 < 16 = \#\text{Aut}(O_K^l, \text{tr}_{K/Q}).
\]

Thus the restriction map is not surjective and therefore the hypothesis \( \text{tr}_{K/Q}(O_K) = \mathbb{Z} \) in Theorem 2.11(ii) is not superfluous.

**Proposition 2.16** Let \( K \) be a \( \mathbb{Z}/l\mathbb{Z} \)-field with \( l \) prime and let \( L \) be a number field. Every isometry \( (O_K^l, \text{tr}_{K/Q}) \cong (O_L^l, \text{tr}_{L/Q}) \) (resp. \( (O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q}) \)) can be extended to one between the integral trace quadratic modules \( (O_K, \text{tr}_{K/Q}) \cong (O_L, \text{tr}_{L/Q}) \).

**Proof** The case \( l \mid \text{Disc}(K) \) follows directly from Theorem 2.11 and Corollary 2.3(i). If \( l \mid \text{Disc}(K) \) then, thanks to being a prime degree Galois extension, \( l \) is totally ramified. Thanks to Lemma 2.2, and since \( \text{tr}_{K/Q}(1) = l \), we have that \( \text{tr}_{K/Q}(O_K) = l \mathbb{Z} \). We claim that if \( (O_K^l, \text{tr}_{K/Q}) \cong (O_L^l, \text{tr}_{L/Q}) \) this implies \( \text{tr}_{L/Q}(O_L) = l \mathbb{Z} \).

Suppose not. Then \( \text{tr}_{L/Q}(O_L) = \mathbb{Z} \) and by Lemma 2.1 we would have \( \text{Disc}(L) = l^{-2} \text{Disc}(K) \). If \( l = 2 \), then \( L = \mathbb{Q}(\sqrt{\text{Disc}(L)}) = \mathbb{Q}(\sqrt{\text{Disc}(K)}) = K \) and since \( \text{tr}_{K/Q}(O_K) = l \mathbb{Z} \) we would obtain a contradiction, so we may assume that \( l \) is odd. Recall from Corollary 2.3(i) that \( l \leq v_l(\text{Disc}(K)) \). Given that \( l \) is odd and that \( K \) 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, \( l + 1 \leq v_l(\text{Disc}(L)) \). By Corollary 2.3(ii) \( L \) is tamely ramified in \( L \) thus if \( f_1^e_1 \cdots f_g^e_g \) is its factorization type, the inequality

\[
l - 1 \leq v_l(\text{Disc}(L)) = l - (f_1 + \cdots + f_g) \leq l - 1
\]

shows that \( f_1 = 1 \) and that \( g = 1 \) and this yields \( l = e_1 f_1 = e_1 \), a contradiction.

Hence if \( \varphi : (O_K^l, \text{tr}_{K/Q}) \sim (O_L^l, \text{tr}_{L/Q}) \) is an isometry, we have \( \text{tr}_{L/Q}(O_L) = l \mathbb{Z} = \text{tr}_{L/Q}(O_L) \), and taking \( \gamma_K = 1 \) in (2.7)(ii) we conclude that both \( \varphi^+ \) and \( \varphi^- \) extend \( \varphi \). Also if we are given an isometry \( \varphi : (O_K^l, \text{tr}_{K/Q}) \sim (O_L^l, \text{tr}_{L/Q}) \), then \( \text{Disc}(K) = \text{Disc}(L) \) and, as \( l \) is prime, Corollary 2.3 implies \( \text{tr}_{L/Q}(O_L) = l \mathbb{Z} \), thus (2.8) shows \( O_K^l = l O_K^0 \) and \( O_L^l = l O_L^0 \). Therefore \( \varphi(O_K^l) = O_L^l \) (\( \varphi \) considered from \( K^0 \) to \( L^0 \)) and we are back to the above case.

**Example 2.17** 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, \( \text{Disc}(K) = 3^3 \cdot 7^5 \), \( \text{tr}_{K/Q}(O_K) = \mathbb{Z} \) and

\[
\#\text{Aut}(O_K^l, \text{tr}_{K/Q}) = \#\text{Aut}(O_K, \text{tr}_{K/Q}) = 96 \neq 1440 = \#\text{Aut}(O_K^0, \text{tr}_{K/Q}).
\]

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. In particular, it would be interesting to answer the following question.

**Question 2.18** Do there exist totally real octic fields with odd discriminant \( K, L \), and an isometry \( (O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q}) \) which cannot be lifted to an isometry \( (O_K, \text{tr}_{K/Q}) \cong (O_L, \text{tr}_{L/Q}) \)?
3 Casimir invariants

In this section we recall the definition of Casimir invariants and state some of the useful facts about them.

Let $V$ be a finite dimensional vector space over a field $F$ and let $V^* := \text{Hom}_F(V, F)$ be its dual. Let $\Gamma : V \to V^*$ be an isomorphism, for instance the one induced by a nondegenerate bilinear form $B : V \times V \to F$. Now let $R$ be an $F$-algebra and let $\phi, \psi \in \text{Hom}_F(V, R)$. The map

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

is bilinear and $F$-balanced (as $R$ is an $F$-algebra), hence it lifts to a morphism $V^* \otimes_F V \to R$. Identifying $V^* \otimes_F V$ with $\text{End}_F(V)$ we obtain a linear map

$$\rho_{\Gamma, \psi, \phi} : \text{End}_F(V) \to R.$$

**Definition 3.1** Let $\psi, \phi \in \text{Hom}_F(V, R)$. The $\Gamma$-Casimir element of $\psi$ and $\phi$ is the element $c_\Gamma(\psi, \phi) \in R$ given by the image under $\rho_{\Gamma, \psi, \phi}$ of the identity morphism;

$$c_\Gamma(\psi, \phi) := \rho_{\Gamma, \psi, \phi}(1).$$

The $\Gamma$-Casimir element $c_\Gamma(\psi, \phi)$ can be explicitly calculated as follows: Let $\{v_1, \ldots, v_n\}$ be an $F$-basis of $V$, $\{f_1, \ldots, f_n\}$ its dual basis, and $v_i^* \in V$ the elements such that $\Gamma(v_i^*) = f_i$. Then

$$c_\Gamma(\psi, \phi) = \sum_{i=1}^n \psi(v_i^*)\phi(v_i).$$

The above follows from the fact that $\sum_i f_i \otimes v_i$ maps to $1 \in \text{End}_F(V)$ under the canonical identification $V^* \otimes_F V \cong \text{End}_F(V)$. In particular, the above representation of $c_\Gamma(\psi, \phi)$ is independent of the choice of basis $\{v_1, \ldots, v_n\}$.

**Example 3.2** Suppose that $V = F^n$, that $R = F$ and that $\Gamma$ is the isomorphism that takes the standard basis in $F^n$ into its dual basis. If we identify $\text{Hom}_F(F^n, F)$ with $F^n$ via $\Gamma$ then $\langle \cdot, \cdot \rangle_\Gamma$ is the usual dot product in $F^n$.

**Definition 3.3** Let $F$ be a field, $V$ be a finite dimension $F$-space, $\Gamma : V \to V^*$ be an isomorphism and $R$ be an $F$-algebra. The **Casimir pairing** associated to $\Gamma$ is the map

$$\langle \cdot, \cdot \rangle_\Gamma : \text{Hom}_F(V, R) \times \text{Hom}_F(V, R) \to R, \quad (\psi, \phi) \mapsto c_\Gamma(\psi, \phi).$$

Whenever the isomorphism $\Gamma$ is induced by a nondegenerate bilinear form $B$ we denote by $\langle \cdot, \cdot \rangle_B$ the Casimir pairing associated to $\Gamma$.

If $K/F$ is a finite separable field extension the trace pairing

$$\text{tr}_{K/F} : K \times K \to F; \quad (x, y) \mapsto \text{tr}_{K/F}(xy)$$

is a nondegenerate bilinear form. For any $F$-algebra $R$ we denote by $\langle \cdot, \cdot \rangle_{\text{tr}_{K/F}}$ the Casimir pairing on $\text{Hom}_F(K, R)$ associated to the trace pairing $\text{tr}_{K/F}$.

**Lemma 3.4** Let $K/F$ be a finite separable field extension of degree $n$. Suppose that $\Omega/K$ is a field extension that contains a Galois closure of $K/F$. Let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of $F$-embeddings of $K$ into $\Omega$. Then $\{\sigma_1, \ldots, \sigma_n\}$ is an orthonormal $\Omega$-basis of $\text{Hom}_F(K, \Omega)$ with respect to the bilinear form $\langle \cdot, \cdot \rangle_{\text{tr}_{K/F}}$. 
Proof Let \( \{ \alpha_i \} \) be a \( F \)-basis of \( K \), and let \( A := (\sigma_j(\alpha_i)) \) and \( A' := (\sigma_j(\alpha_i^*) \)). Then
\[
A(A')^t = \left( \sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j^*) \right) = (\text{tr}_{K/F}(\alpha_i\alpha_j^*)) = I,
\]
hence \( (\delta_{ij}) = I = (A')^tA = \left( \sum_k \sigma_k(\alpha_i^*)\sigma_k(\alpha_j) \right) = (\langle \sigma_i, \sigma_j \rangle_{\text{tr}}). \) As \( \text{Hom}_F(K, \Omega) \) has dimension \( n \) over \( \Omega \) this proves that the embeddings form an orthonormal basis of this vector space.

It follows from the above that any \( F \)-linear map from \( K \) to \( \Omega \) can be written in terms of Casimir elements:

**Corollary 3.5** Let \( K, F, \Omega, \) and \( \sigma_1, \ldots, \sigma_n \) be as above. Then, for all \( \phi \in \text{Hom}_F(K, \Omega) \)
\[
\phi = \sum_{i=1}^n \langle \phi, \sigma_i \rangle_{\text{tr}} \sigma_i.
\]

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

**Proposition 3.6** Let \( F, V \) and \( R \) be as above and suppose \( B \) is a nondegenerate bilinear form on \( V \). Then,

(i) If \( R \) is commutative and \( B \) is symmetric, then \( \langle \cdot, \cdot \rangle_B \) is symmetric.

(ii) If \( \theta : R \to R' \) 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
\[
\langle \psi \otimes 1, \phi \otimes 1 \rangle_{B \otimes F'} = \langle \psi, \phi \rangle_B \otimes 1 \in R \otimes F'
\]

(iv) Let \( (V, B_V) \) and \( (W, B_W) \) be nondegenerate quadratic \( F \)-spaces. An \( F \)-linear map \( \phi : V \to W \) is an isometry if and only if the induced natural map
\[
\Phi : \text{Hom}_F(W, R) \to \text{Hom}_F(V, R), \quad \tau \mapsto \tau \circ \phi
\]
is an isomorphism of \( R \)-modules which respects the Casimir pairings \( \langle \cdot, \cdot \rangle_{B_V} \) and \( \langle \cdot, \cdot \rangle_{B_W} \).

Proof The only nontrivial part is (iv). First suppose \( \phi : V \to W \) is an isometry. Take \( \{ v_i \} \) any basis of \( V \) with dual basis \( \{ v_i^* \} \); as \( \phi \) is an isometry, it follows that \( \langle \phi(v_i^*) \rangle \) is the dual basis of \( \{ \phi(v_i) \} \) in \( (W, B_W) \). Since \( \phi \) is an isomorphism, \( \Phi \) is also one and
\[
\langle \Phi(\tau_1), \Phi(\tau_2) \rangle_{B_V} = \langle \tau_1 \circ \phi, \tau_2 \circ \phi \rangle_{B_V}
\]
\[
= \sum_i \tau_1(\phi(v_i^*))\tau_2(\phi(v_i))
\]
\[
= \langle \tau_1, \tau_2 \rangle_{B_W}
\]
for all \( \tau_1, \tau_2 \in \text{Hom}_F(W, R) \).
Conversely, suppose \( \Phi \) is an isomorphism which preserves the Casimir pairings. First we prove that \( \phi \) must be bijective. Indeed, we have a commutative diagram
(where the vertical maps are canonical isomorphisms) so \( \Phi^* \otimes 1 \) 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 \( \Phi \) is.

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 \( \tau_i \in \text{Hom}_F(W, R) \) be defined by \( \tau_i(w_j) = \delta_{ij} \). Then, for every \( \tau \in \text{Hom}_F(W, R) \)

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

\[
\langle \tau, \tau_i \rangle_{B_w} = \sum_k \tau(w_k^*) \tau_i(w_k) = \tau(w_i^*).
\]

Since \( \Phi \) preserves the Casimir pairings, it follows that \( \tau(w_i/a_i) = \tau(w_i^*) \) for all \( \tau \in \text{Hom}_F(V, R) \), 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.

**Corollary 3.7** Let \( F \) be a field and let \( K/F \) and \( L/F \) be separable field extensions of the same degree \( n \). Suppose that \( \Omega/F \) is field extension containing a Galois closure of \( KL/F \).

Let \( \phi : K \to L \) be an \( F \)-linear map. Then the following are equivalent

(i) The map \( \phi \) is an isometry between \( (K, \text{tr}_{K/F}) \) and \( (L, \text{tr}_{L/F}) \).

(ii) The map \( \Phi, \) composition by \( \phi \), is an isometry between the spaces \( \text{Hom}_F(L, \Omega) \) and \( \text{Hom}_F(K, \Omega) \) endowed with their Casimir pairings \( \langle \cdot, \cdot \rangle_{L/F} \) and \( \langle \cdot, \cdot \rangle_{K/F} \).

(iii) The matrix \( U = (c_{ij}) \) is orthogonal, where \( c_{ij} := \langle \sigma_i, \tau_j \rangle_{K/F} \), and \( \{ \sigma_i \}, \{ \tau_i \} \) are the sets of \( F \)-embeddings of \( K \) and \( L \) into \( \Omega \).

**Proof** The equivalence of (i) and (ii) is Proposition 3.6(iv), and the equivalence of (ii) and (iii) follows from the fact that \( \{ \sigma_i \} \) and \( \{ \tau_i \} \) are orthonormal bases by Lemma 3.4.

**4 A proof via Bhargava’s parametrization of quartic rings**

The aim of this section is to prove [10, Conjecture 2.10] using Bhargava’s parametrization of quartic rings. Even though the veracity of the conjecture follows from Theorem 2.13 we add the proof coming from Bhargava’s parametrization since it generalizes the ideas involved in the proof of cubic fields, thus showing the close relation existing between parametrization of rings and trace-zero forms on them. A similar, although quite more simple, argument can be carried on for quadratic fields given that there is also a parametrization in degree 2. For the convenience of the reader we recall here the statement of the conjecture

**Conjecture** [10, Conjecture 2.10] 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

\[
(O_K^0, \text{tr}_{K/Q}) \cong (O_L^0, \text{tr}_{L/Q})
\]

exists, then \( K \cong L \).
Thanks to Lemma 2.4 we may assume in the conjecture that $K$ and $L$ have square free discriminant.

### 4.1 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

$$2 \cdot (A, B) = \begin{pmatrix}
a_{11} & a_{12} & a_{13} \\
a_{12} & a_{22} & a_{23} \\
a_{13} & a_{23} & a_{33}
\end{pmatrix}, \quad \begin{pmatrix}
b_{11} & b_{12} & b_{13} \\
b_{12} & b_{22} & b_{23} \\
b_{13} & b_{23} & b_{33}
\end{pmatrix}$$

where $a_{ij}, b_{ij} \in \mathbb{Z}$. The group $G_3 := \text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$ 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

$$g \cdot (A, B) = (r \cdot g_3 A g_3^* + s \cdot g_3 B g_3^* + t \cdot g_3 A g_3^* + u \cdot g_3 B g_3^*)$$

(1)

This action has a fundamental invariant called the discriminant and is given by

$$\text{Disc}(A, B) = \text{Disc}(f_{A,B}(x, y)) = b^2 c^2 - 27 a^2 d^2 + 18 a b c d - 4 a^3 - 4 b^3 d$$

where $f_{A,B}(x, y) = 4 \cdot \det(Ax - By) = ax^2 + bx^2y + cxy^2 + dy^3$ is the cubic resolvent form of $(A, B)$, a covariant for the action of $\text{GL}_2(\mathbb{Z})$.

In [3] Bhargava proved that quartic rings can be parametrized using integral ternary quadratic forms. His main result is the following.

**Theorem 4.1** There is a bijection between the set of $G_3$-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 quadratic resolvent mapping $Q/\mathbb{Z} \to R/\mathbb{Z}$ satisfying certain formal properties whose precise definition can be found in [3, Sect. 3.9]. When $Q$ is the maximal order in a $S_4$-field $K$ the ring $R$ is unique; it is the cubic ring corresponding to $f_{A,B}$ by the Delone–Faddeev–Gross parametrization of cubic rings, an order in the usual cubic resolvent field of $K$.

The space $(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$ has a $\text{SL}_3(\mathbb{Z})$-covariant of degree 4. Namely, let $(A, B) \in (\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*$ and suppose $Q$ is the quartic ring corresponding to $(A, B)$ by Theorem 4.1. Then the covariant denoted $Q_{(A,B)}$ 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 $Q_{(A,B)} = O_K$ is the maximal order in a quartic field $K$, then $Q_{(A,B)}$ corresponds to the isometry class of the quadratic $\mathbb{Z}$-module $(O_K^+, \frac{1}{4} \text{tr}_K/Q)$. The explicit computation of $Q_{(A,B)}$ in terms of the coefficients of $(A, B)$ is in Sect. 2.3.2 of [6] and also in the appendix to Chapter 5 of [4].

Thus if $(\text{Sym}^2 \mathbb{Z}^3)^*$ denotes the set of integral ternary quadratic forms and we let

$$(\text{Sym}^2 \mathbb{Z}^3)^*/\text{SL}_3(\mathbb{Z})$$

to be its set of orbits by the action of $\text{SL}_3(\mathbb{Z})$ we have a map

$$Q : (\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*/G_3 \to (\text{Sym}^2 \mathbb{Z}^3)^*/\text{SL}_3(\mathbb{Z})$$

Thanks to Corollary 2.12, the proof of [10, Conjecture 2.10] amounts to proving that $Q$ is injective when restricted to the orbits of pairs $(A, B)$ coming from totally real quartic fields with square free discriminant.
4.2 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 \( G_\mathbb{Z} = \text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z}) \) 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 [2] 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 4.2** There is a bijection between the set of nondegenerate \( G_\mathbb{Z} \)-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 \( I^2 \subseteq (\delta) \) 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 \( R \) 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 4.2 as

\[
\Phi : W_\mathbb{Z}/G_\mathbb{Z} \longrightarrow \mathcal{R}
\]

where \( W_\mathbb{Z} \) denotes the set of nondegenerate elements in \( \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3 \).

There is also a natural map

\[
T : \mathcal{R} \longrightarrow (\text{Sym}^2 \mathbb{Z}^3)^*/\text{SL}_3(\mathbb{Z})
\]

taking the equivalence class of \((R, I, \delta)\) to equivalent class of the integral quadratic form obtained by restricting the twisted 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 map connecting the two previous theorems. Indeed, let \( V_\mathbb{Z} \) denote the set of nondegenerate elements in \((\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3)^*\). Then we have the natural map

\[
V_\mathbb{Z}/G_\mathbb{Z} \rightarrow W_\mathbb{Z}/G_\mathbb{Z}
\]

taking the orbit of \((A, B) \in V_\mathbb{Z}\) to the orbit of \((2A, 2B) \in W_\mathbb{Z}\).

4.3 Proof of the conjecture

All these maps fit together in the following diagram:
Surprisingly enough we get the following.

**Lemma 4.3** The above diagram is commutative.

**Proof** For the moment we are only able to prove this by a direct computation. Let \((A, B) \in V_{\mathbb{Z}}\) with coefficients given by

\[
2 \cdot (A, B) = \begin{pmatrix}
2a_{11} & a_{12} & a_{13} \\
a_{12} & 2a_{22} & a_{23} \\
a_{13} & a_{23} & 2a_{33}
\end{pmatrix},
\]

and suppose that its class corresponds by Theorem 4.1 to the class of the pair \((Q, R')\).

We need to show that if \((R, I, \delta)\) represents the class corresponding to the image of the class of \((2A, 2B) \in W_{\mathbb{Z}}\) under \(\Phi\), then for some basis of \((\alpha_1, \alpha_2, \alpha_3)\) of \(I\) the matrix \(\text{Tr}(\alpha_i \alpha_j \delta)\) coincides with the matrix \((Q_{ij})\) in [6, pp. 44–45], which is the Gram matrix of \(Q(A, B)\) in an explicit basis of \(Q_{\perp}\).

The ring \(R\) corresponds under the Delone–Faddeev parametrization to the binary cubic form

\[
det(2Ax - 2By) = ax^3 + bx^2y + cxy^2 + dy^3
\]

which means that \(R'\) has a basis \((1, \omega, \theta)\) such that the ring structure of \(R\) is given by

\[
\begin{align*}
\omega \theta &= -ad \\
\omega^2 &= -ac + b\omega - a\theta \\
\theta^2 &= -bd + d\omega - c\theta
\end{align*}
\]

In particular, \(\text{Tr}(\omega) = b\) and \(\text{Tr}(\theta) = -c\). Now the ideal \(I\) has a \(\mathbb{Z}\)-basis \((\alpha_1, \alpha_2, \alpha_3)\) such that

\[
\alpha_i \alpha_j = \delta(c_{ij} + b^*_y \omega + a^*_y \theta),
\]

where \(2A =: (a^*_y)\), \(2B =: (b^*_y)\) and the constants \(c_{ij}\) are uniquely determined from the associative law on triple products \(\delta^{-1} \alpha_i (\delta^{-1} \alpha_j) (\delta^{-1} \alpha_k)\), see [4, Sect. 3.1.4]. More specifically, these constants are given in terms of \((a^*_y)\) and \((b^*_y)\) by [4, Eq. (3.8)]. Alternatively, we can also describe \(C = (c_{ij})\) explicitly as

\[
C := \text{Adj} (\text{Adj}(2A) + \text{Adj}(2B)) - \det(2A)(2A) - \det(2B)(2B),
\]
where $\text{Adj}(X)$ denotes the adjoint of a matrix $X$. Thus in this basis
\[
(\text{tr} \left( \frac{a_i a_j}{\delta} \right)) = 3C + b(2B) - c(2A).
\]

On expanding the right hand side in terms of the $a_{ij}$’s and $b_{ij}$’s, we find that this matrix coincides with the matrix $(Q_{ij})$ in [6, pp. 44–45].

It follows that in order to prove [10, Conjecture 2.10] 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 the conjecture follows from:

**Theorem 4.4** 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, $(R, I, \delta)$ 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 pair $(Q, R')$, where $Q$ is the maximal order 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,

- Since $\text{Disc}(R') = d$ is square-free, the ring $R'$ is the maximal order in the cubic resolvent field of $K$. Also, $R'$ the cubic ring corresponding to $f_{(A,B)}$ and $R$ is 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 $R'$, then $(1, 2\omega, 2\theta)$ is a normalized basis of $R'$. In particular, $R$ is an order of conductor $\epsilon = 2R'$ in $R'$. Note that given $x = r + 2s\omega + 2t\theta \in R$, with $r, s, t \in \mathbb{Z}$; we have $x \in 2R'$ if and only if $r \equiv \text{tr}(x) \equiv 0 \mod 2$, also note that $\text{tr}(x^2) \equiv r^2 \equiv r \equiv \text{tr}(x) \mod 2$.
- 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 [1, Lemma 21]).
- We claim that there is a $\kappa \in R \otimes \mathbb{Q}$, such that $\kappa I$ is an integral ideal in $R$ prime to the conductor $\epsilon = 2R'$. Indeed, take a $\mathbb{Z}$-basis $(1, \gamma_1, \gamma_2, \gamma_3)$ of $Q$ and let $t_i := \text{tr}(\gamma_i)$. Then $(4\gamma_1 - t_i)$ is a basis of $Q^+$ and if $(Q_{ij})$ is the Gram matrix of $\frac{1}{4} \text{tr}(x^2)$ in this basis, then
\[
Q_{ii} \equiv t_i \mod 4.
\]

Since $d$ is square free, then $(4, t_1, t_2, t_3) = \text{tr}(Q) = \mathbb{Z}$ (see Corollary 2.3). Thus at least one of $Q_{ii}$ must be odd, say $Q_{11}$. Next, according to Lemma 4.3, $(Q_{ij})$ 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
\[
\frac{\alpha_1^2}{\delta} = r + s(2\omega) + t(2\theta),
\]
then $1 \equiv Q_{11} = 3r \equiv r \mod 2$, 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 $\frac{a^2}{3} \in \kappa I$ and $1 - \frac{a^2}{3} \in \epsilon = 2R'$.

We have proved that $(R, I, \delta)$ is equivalent to a triple $(R', \delta')$ 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 $a$ 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 $a$.

**Proof of Theorem 4.4** Let $K := R \otimes \mathbb{Q}$ and $L := S \otimes \mathbb{Q}$. Choose $I$ and $J$ to be prime to the conductor of $R$ and $S$, respectively, and to $d$. This implies, thanks to $I$ and $J$ being invertible, that $I^2 = (\delta)$ and $J^2 = (\epsilon)$. The isometry can be extended to a rational isometry

$$\phi : (K, \text{tr}(x^2/\delta)) \sim (L, \text{tr}(x^2/\epsilon))$$

Let $\sigma : K \rightarrow \mathbb{R}$ and $\tau : L \rightarrow \mathbb{R}$ be embeddings (recall that $K$ and $L$ are totally real). We claim that $c_{\sigma, \tau} := \langle \sigma, \tau \phi \rangle_{K/\mathbb{Q}} \sqrt{\frac{\text{tr}(\delta)}{\text{tr}(\epsilon)}}$, see Sect. 3 to recall definition and properties, is an algebraic integer. Replacing $K$ by $\sigma(K)$, $L$ by $\tau(L)$ and $\tau \phi$ by $\tau \phi \sigma^{-1}$ we see, thanks to Proposition 3.6(iv), that it is enough to show that $c_{\sigma, \tau}$ is integral for $\sigma$ and $\tau$ some fixed embeddings $\kappa K : K \rightarrow \mathbb{R}$ and $\kappa L : L \rightarrow \mathbb{R}$. We identify $K$ and $L$ as subsets of $\mathbb{R}$ via the embeddings $\kappa K$ and $\kappa L$, and we will denote by $c$ the element $c_{\kappa K, \kappa L}$. By definition of the Casimir invariant, and of $\delta$ and $\epsilon$, we have that $c^2 \in KL$. Hence, to show that $c$ is algebraic integer it is enough to show that $c^2 \in O_{KL}$. To this end we will show that in $KL \otimes \mathbb{Q}_p$

$$c^2 \otimes 1 \in O_{KL} \otimes \mathbb{Z}_p, \quad (2)$$

for all primes $p$.

Let $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ be a basis of $IO_K$ and let $\langle \alpha_1^*, \alpha_2^*, \alpha_3^* \rangle$ be its dual basis in $K$ with respect to the trace form. Then by definition, and the fact that Casimir invariants are compatible with tensor products (see Proposition 3.6), we have

$$\frac{\epsilon}{\delta} c^2 \otimes 1 = \left( \sum_{i=1}^{3} (\alpha_i^* \otimes 1)(\phi \otimes 1)(\alpha_i \otimes 1) \right)^2. \quad (3)$$

Now $\langle \alpha_1^*, \alpha_2^*, \alpha_3^* \rangle$ generates the dual ideal of $(IO_K)$, i.e, the fractional ideal

$$\{ x \in K : \text{Tr}_{K/\mathbb{Q}}(x(IO_K)) \subset \mathbb{Z} \} = (IO_K)^{-1}D_K^{-1}$$

(here $D_K$ is the different ideal of $K$).

First suppose $p \nmid 2d$. As $p \neq 2$ we have $I \otimes \mathbb{Z}_p = (IO_K) \otimes \mathbb{Z}_p$ and $J \otimes \mathbb{Z}_p = (IO_L) \otimes \mathbb{Z}_p$. Moreover, $p \nmid d = \text{Disc}(K)$ implies that $D_K \otimes \mathbb{Z}_p = O_K \otimes \mathbb{Z}_p$, thus it follows that each $\alpha_1^* \otimes 1$ belongs to $(IO_K)^{-1} \otimes \mathbb{Z}_p$, and since $\phi \otimes 1$ maps $I \otimes \mathbb{Z}_p$ into $J \otimes \mathbb{Z}_p$ we conclude that the right hand side of (3) belongs to

$$(IO_K)^{-1}(IO_L) \otimes \mathbb{Z}_p)^2 \subset (1^{-1}JO_{KL} \otimes \mathbb{Z}_p)^2 = \frac{\epsilon}{\delta} O_{KL} \otimes \mathbb{Z}_p.$$

Therefore $c^2 \otimes 1 \in O_{KL} \otimes \mathbb{Z}_p$.

Next consider the case $p = 2$. Since $\delta, \epsilon$ and $D_K$ are coprime to 2, it would be enough to show that $\phi \otimes 1$ maps $O_K \otimes \mathbb{Z}_2$ into $O_L \otimes \mathbb{Z}_2$. Indeed, we can compute the right hand side of (3) using a fixed $\mathbb{Z}$-basis $\langle \alpha_1, \alpha_2, \alpha_2 \rangle$ of $O_K$ (recall that the Casimir invariant is independent of the choice of the $\mathbb{Q}$-basis of $K$). Then $\alpha_1^* \otimes 1 \in O_K \otimes \mathbb{Z}_2$ and $\phi(\alpha_1 \otimes 1) \in O_L \otimes \mathbb{Z}_2$, showing that $c^2$ is 2-integral. To prove $(\phi \otimes 1)(O_K \otimes \mathbb{Z}_2) \subset O_L \otimes \mathbb{Z}_2$, we will use the fact that given $z \in S \otimes \mathbb{Z}_2$ we have $z \in 2(O_L \otimes \mathbb{Z}_2)$ if and only if $\text{tr}(z^2) \equiv \text{tr}(z) \equiv 0 \mod 2$ (see the first remark before the proof). Let $x \in O_K$, then $2x \otimes 1 \in R \otimes \mathbb{Z}_2 = I \otimes \mathbb{Z}_2$ and so
$y := \phi(2x) \otimes 1 = (\phi \otimes 1)(2x \otimes 1) \in J \otimes \mathbb{Z}_2 = S \otimes \mathbb{Z}_2$. Thus $z := \frac{\phi(2x)^2}{\varepsilon} \otimes 1 = \frac{x^2}{\varepsilon \otimes 1} \in S \otimes \mathbb{Z}_2$, moreover,

$$\text{tr}(z) = \text{tr} \left( \frac{\phi(2x)^2}{\varepsilon} \otimes 1 \right) = \text{tr} \left( \frac{(2x)^2}{\delta} \otimes 1 \right) = 4 \text{tr} \left( \frac{x^2}{\delta} \otimes 1 \right) \equiv 0 \mod 4 \mathbb{Z}_2,$$

because $\frac{x^2}{\delta} \otimes 1 \in O_K \otimes \mathbb{Z}_2$. In particular, $\text{tr}(z) \equiv 0 \mod 2$, and as we already knew that $z \in S \otimes \mathbb{Z}_2$, it follows that $z \in 2(O_L \otimes \mathbb{Z}_2)$. Hence $y^2 \in 2(O_L \otimes \mathbb{Z}_2)$, which implies $y = 2(\phi \otimes 1)(x \otimes 1) \in 2(O_L \otimes \mathbb{Z}_2)$, because $\text{tr}(y) \equiv \text{tr}(y^2) \equiv 0 \mod 2$ and $y \in S \otimes \mathbb{Z}_2$. Hence $(\phi \otimes 1)(x \otimes 1) \in O_L \otimes \mathbb{Z}_2$.

It remains to prove (2) when $p$ is an odd prime such that $p \mid d$. Since in this case $\delta$ and $\varepsilon$ are prime to $p$, $L \otimes \mathbb{Z}_p = R \otimes \mathbb{Z}_p = O_K \otimes \mathbb{Z}_p$ and $J \otimes \mathbb{Z}_p = S \otimes \mathbb{Z}_p = O_L \otimes \mathbb{Z}_p$. Hence $\phi \otimes 1$ takes $p$-integral elements to $p$-integral elements. Moreover, because $K$ is a cubic extension with fundamental discriminant ramified at $p \neq 2$, $p$ must factor in $O_K$ as $p^3 \mathfrak{p}_1^2$. Let us identify $K \otimes \mathbb{Q}_p \cong \mathbb{Q}_p \times K_{\mathfrak{p}_2}$, where $K_{\mathfrak{p}_2} = \mathbb{Q}_p(\pi)$ is one of the two quadratic ramified extensions of $\mathbb{Q}_p$, and $\pi^2 = up, u \in \mathbb{Q}_p^*$. Take $(\alpha_1, \alpha_2, \alpha_3) = ((1, 0), (0, 1, 0), (0, \pi))$ as a $\mathbb{Q}_p$-basis of this space, its dual basis (with respect to $\text{tr}(x^2)$) will be $(\alpha_1^*, \alpha_2^*, \alpha_3^*) = ((1, 0, 0, 1/2, 0, 1/2)), \ldots$, and its Gram matrix with respect to $\text{tr}(x^2/\delta)$ is

$$M := \begin{pmatrix} 1/\delta_1 & 0 & 0 \\ 0 & \text{tr}(1/\delta_2) & \text{tr}(\pi/\delta_2) \\ 0 & \text{tr}(\pi/\delta_2) & \pi^2/\text{tr}(1/\delta_2) \end{pmatrix},$$

where $\delta = (\delta_1, \delta_2) \in \mathbb{Q}_p \times \mathbb{Q}_p(\pi)$. Write $\beta_i := (\phi \otimes 1)(\alpha_i) \in O_L \otimes \mathbb{Z}_p$, $i = 1, 2, 3$. As in (3) we have $c \otimes 1 = \alpha_1^* \beta_1 + \alpha_2^* \beta_2 + \alpha_3^* \beta_3$. The first two terms are clearly in $O_K \otimes \mathbb{Z}_p$, because $\alpha_1^*, \alpha_2^* \in O_K \otimes \mathbb{Z}_p$. As $p \cdot (\alpha_3^*)^2 \in O_K \otimes \mathbb{Z}_p$, we see that to prove $c \otimes 1 \in p$-integral it is enough to show that $\beta_3^* \beta_3$ is zero modulo $p$. This will follow from the fact that the last row of $M$ is zero modulo $p$ (here $\text{tr}(\pi/\delta_2) \equiv 0 \mod p$ because $\delta$ is prime to $p$, so $1/\delta_2 = a + b\pi \in \mathbb{Z}_p[\pi], a, b \in \mathbb{Z}_p$ and thus $\text{tr}(\pi/\delta_2) = 2b\pi^2$). Indeed, since $\phi \otimes 1$ is an isometry, $M$ is also the Gram matrix of $\text{tr}(x^2/\varepsilon)$ in the basis $\langle \beta_1, \beta_2, \beta_3 \rangle$ of $L \otimes \mathbb{Q}_p$, which factors as

$$M = B \cdot \text{diag}(\tau_1(\varepsilon^{-1}), \tau_2(\varepsilon^{-1}), \tau_3(\varepsilon^{-1})) \cdot B^t,$$

where $B = (\tau_i(\beta_i))$ and $\{\tau_1, \tau_2, \tau_3\} = \text{Hom}_{\mathbb{Q}_p-\text{alg}}(L \otimes \mathbb{Q}_p, \mathbb{Q}_p)$. Multiplying on the right by the adjoint of $C := \text{diag}(\tau_1(\varepsilon^{-1}), \tau_2(\varepsilon^{-1}), \tau_3(\varepsilon^{-1}))B^t$, we find that the last row of $\text{det}(C)$ is also zero modulo $p$, but $\text{det}(C)^2 = \text{Disc}(L) = p$ (up to units in $\mathbb{Z}_p$). Hence the last row of $B$ is zero modulo $\text{det}(C)$. This finishes the proof of (2), and thus we have that $c_i, r$ is an algebraic integer.

Now we have two cases:

- $K \not\cong L$. Since $K$ and $L$ are cubic fields, and non-isomorphic, they are linearly disjoint. Let $\{\sigma_1, \sigma_2, \sigma_3\}$ and $\{\tau_1, \tau_2, \tau_3\}$ be the complex embeddings of $K$ and $L$, respectively, with $\sigma_1$ and $\tau_1$ the inclusions $K \hookrightarrow \mathbb{R}$ and $L$. Since $K$ and $L$ are linearly disjoint for each $1 \leq i, j \leq 3$ there exists a unique embedding $\theta_{ij} : KL \hookrightarrow \mathbb{R}$ extending both $\sigma_i$ and $\tau_j$. Let $c_{ij} := \langle \sigma_\nu, \tau_\nu \rangle_{\theta_{ij}(\delta)} \sqrt{\frac{\sigma_j(\delta)}{\sigma_i(\delta)}} \in \mathbb{R}$. Since $\phi$ is an isometry the matrix $U = (c_{ij})$ must be orthogonal. Indeed, let $(\alpha_1, \alpha_2, \alpha_3)$ be any $\mathbb{Q}$-basis of $K$ with dual basis $(\alpha_1^*, \alpha_2^*, \alpha_3^*)$ with respect to the trace form. Let $\beta_i = \phi(\alpha_i), i = 1, 2, 3; A = (\sigma_\nu(\alpha_\nu)), A' := (\sigma_\nu(\alpha_\nu^*)), B = (\tau_i(\beta_i)), \Delta := \text{diag} \left( \frac{1}{\sqrt{\sigma_1(\delta)}}, \frac{1}{\sqrt{\sigma_2(\delta)}}, \frac{1}{\sqrt{\sigma_3(\delta)}} \right)$ and $\mathcal{E} := \text{diag} \left( \frac{1}{\sqrt{\tau_1(\varepsilon)}}, \frac{1}{\sqrt{\tau_2(\varepsilon)}}, \frac{1}{\sqrt{\tau_3(\varepsilon)}} \right)$. 

Then,
\[
A \Delta^2 A^t = \left( \operatorname{tr} \left( \frac{\alpha_i \alpha_j}{\delta} \right) \right) = \left( \operatorname{tr} \left( \frac{\beta_i \beta_j}{\epsilon} \right) \right) = B \mathcal{E}^2 B^t,
\]
shows that \( \Delta^{-1} A^{-1} B \mathcal{E} = \Delta^{-1} A' B \mathcal{E} = U \) is orthogonal.

However, \( \theta_j(c_{ij}^2) = c_{ij}^2 \leq 1 \), 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 \( U = (c_{ij}) = (c_{11}) \) is nonsingular.

- \( K \cong L \). In particular, \( O_K \cong O_L \) thus the integral ternary quadratic forms defining the quartic rings from which \( (R, I, \delta) \) and \( (s, J, \epsilon) \) come from have equivalent cubic resolvent forms \( \mathcal{E} \). Therefore 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 that \( R = S \).

Let \( c_{ij} := (\sigma, \sigma \phi)_{U, K/\mathbb{Q}} \sqrt{\operatorname{tr} K/\mathbb{Q}} \in \mathbb{R} \), as before we have that \( U = (c_{ij}) \) is orthogonal and \( c_{ij}^2 \leq 1 \) for all \( i, j \). Now let \( \overline{K} \) be the Galois closure of \( K \), for every \( \sigma \in \text{Gal}(\overline{K}/\mathbb{Q}) \) and \( i, j \) we have that
\[
\sigma(c_{ij}^2) = c_{ij}^2 \leq 1
\]
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 \( U \). From this and the relation, see Corollary 3.5,
\[
\sigma \phi = \sum_{j} (\sigma, \sigma \phi)_{U, K/\mathbb{Q}} \sigma_j
\]
follows that \( c_{ij}^2 = \delta_{ij} \) (Kronecker delta). In particular, if \( \kappa = (\sigma_1, \sigma_1 \phi)_{U, K/\mathbb{Q}} \in K \)
\[
1 = c_{11}^2 = \kappa^2 \frac{\delta}{\epsilon}
\]
and as \( \phi(x) = \kappa x, f = \kappa I \). Therefore, the triples \( (R, I, \delta) \) and \( (R, J, \epsilon) \) are equivalent.

\[\square\]

**Author details**

1Department of Mathematics, University of Washington, Seattle, USA,
2Department of Mathematics, Universidad Konrad Lorenz, Bogotá, Colombia,
3Department of Mathematics and Systems Analysis, Aalto University, Espoo, Finland.

**Acknowledgements**

We would like to thank the referee for the careful reading of the paper, and for their helpful comments.

Received: 8 January 2020  Accepted: 25 August 2020  Published online: 31 August 2020

**References**

1. Bhargava, M., Varma, I., 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 Math. J. **164**(10), 1911–1933 (2015)
2. Bhargava, M.: Higher composition laws II: on cubic analogues of Gauss composition. Ann. Math. **159**, 865–886 (2004)
3. Bhargava, M.: Higher composition laws III: the parametrization of quartic rings. Ann. Math. **159**, 1329–1360 (2004)
4. Bhargava, M.: Higher composition laws. Ph.D thesis, Princeton University (2001)
5. Bhargava, M., Harron, P.: The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields. Compositio Mathematica **152**(6), 1111–1120 (2016)
6. Harron, P.: The equidistribution of lattice shapes of rings of integers of cubic, quartic, and quintic Number Fields: an artist’s rendering. Ph.D thesis, Princeton Univ (2016)
7. Harron, R.: The shapes of pure cubic fields. Proc. Am. Math. Soc. **145**(2), 509–524 (2017)
8. Harron, R.: Equidistribution of shapes of complex cubic fields of fixed quadratic resolvent. arXiv preprint arXiv:1907.07209 (2019)
9. Jones, J., Roberts, D.: A data base of number fields. LMS J. Comput. Math. 17(1), 595–618 (2014)
10. Mantilla-Soler, G.: On number fields with equivalent integral trace forms. Int. J. Number Theory 8–7, 1569–1580 (2012)
11. Mantilla-Soler, G.: Integral trace forms associated to cubic extensions. Algeb. Number Theory 4–6, 681–699 (2010)
12. Mantilla-Soler, G., Monsurrò, M.: The Shape of $\mathbb{Z}/\ell\mathbb{Z}$-number fields With M. Monsurrò. Ramanujan J. 39(3), 451–463 (2016)
13. Mantilla-Soler, G., Rivera-Guaca, C.: An introduction to Casimir pairings and some arithmetic applications. arXiv:1812.03133v3 (2019)
14. Maurer, D.: The Trace-Form of an algebraic number field. J. Number Theory 5, 379–384 (1973)
15. Neukirch, J.: Algebraische Zahlentheorie. Springer, Berlin (2007)

**Publisher’s Note**
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.