# COINCIDENCE SITE MODULES IN 3-SPACE

MICHAEL BAAKE, PETER PLEASANTS, AND ULF REHMANN

Abstract. The coincidence site lattice (CSL) problem and its generalization to $\mathbb{Z}$-modules in Euclidean 3-space is revisited, and various results and conjectures are proved in a unified way, by using maximal orders in quaternion algebras of class number 1 over real algebraic number fields.

## 1. Introduction

A *lattice* in Euclidean space $\mathbb{R}^d$ is a $\mathbb{Z}$-module of rank $d$ whose $\mathbb{R}$-span is $\mathbb{R}^d$. Two lattices $\varGamma$ and $\varGamma'$ in $\mathbb{R}^d$ are called *commensurate*, denoted by $\varGamma \sim \varGamma'$, if their intersection $\varGamma \cap \varGamma'$ has finite index both in $\varGamma$ and in $\varGamma'$. This definition also applies to the commensurability of $\mathbb{Z}$-modules in $\mathbb{R}^d$ of rank $m > d$. The *commensurator* of a lattice $\varGamma$ is the subgroup in $\mathrm{GL}(d,\mathbb{R})$ defined by

$$\mathrm{comm}(\varGamma) \; := \; \{M \in \mathrm{GL}(d,\mathbb{R}) \mid \varGamma \sim M\varGamma\}\,.$$

It is not difficult to see that $\mathrm{comm}(\varGamma) \simeq \mathrm{GL}(d,\mathbb{Q})$, via the map that takes the standard basis of $\mathbb{R}^d$ to a lattice basis. More generally, for a subgroup $G \subset \mathrm{GL}(d,\mathbb{R})$, one defines the commensurator of $\varGamma$ relative to $G$ in an analogous way, denoted by $\mathrm{comm}_G(\varGamma)$. Any commensurator of this form is a function of the equivalence class defined by $\sim$, i.e., commensurate lattices possess the same commensurators. One can extend the definition to the affine group and subgroups thereof, but that is outside our scope here.

Of particular interest in crystallography is the commensurator of a lattice relative to the group of isometries, $\mathrm{O}(d,\mathbb{R})$, or to its rotation subgroup, $\mathrm{SO}(d,\mathbb{R})$. This has been investigated in great detail in connection with the classification of grain boundaries and twins in materials science, compare [8, 13]. The connection with the algebraic problem we are interested in here emerges via the so-called coincidence site lattices (CSLs), see [5, 2, 19] and references therein. These are finite index sublattices of a given lattice $\varGamma$ that are intersections of the form $\varGamma \cap R\varGamma$ with an isometry $R$ from the commensurator. In this context, the notation

$$\mathrm{(S)OC}(\varGamma) \; := \; \mathrm{comm}_{\mathrm{(S)O}(d,\mathbb{R})}(\varGamma)$$

has proved useful, together with the index function $\varSigma\colon\, \mathrm{OC}(\varGamma) \longrightarrow \mathbb{N}$ defined by

$$\varSigma(R) \; := \; [\varGamma : (\varGamma \cap R\varGamma)]\,.$$

The integer $\varSigma(R)$ is the *coincidence index* of the isometry $R$, and the image $\varSigma\big(\mathrm{OC}(\varGamma)\big)$ is called the elementary (or simple) *coincidence spectrum* of $\varGamma$. It refers to indices that emerge from single intersections only.

More generally, one considers multiple intersections of the form $\varGamma \cap R_1\varGamma \cap \ldots \cap R_\ell\varGamma$, with each $R_i \in \mathrm{OC}(\varGamma)$, and defines $\varSigma(R_1,\ldots,R_\ell)$ as the index of this intersection in $\varGamma$. Clearly, the corresponding multiple spectra satisfy

$$\varSigma\big(\mathrm{OC}(\varGamma)^m\big) \;\subseteq\; \varSigma\big(\mathrm{OC}(\varGamma)^n\big) \quad \text{for} \quad m \le n,$$

and $\varSigma_{\mathrm{tot}} := \bigcup_{m\ge 1} \varSigma\big(\mathrm{OC}(\varGamma)^m\big)$ is called the total (or complete) coincidence spectrum of $\varGamma$. In several important examples, compare [3, 27], these spectra are equal or stabilize, in the sense that the total spectrum is reached after finitely many lattice intersections. Usually, there are more multiple CSLs than simple ones with a given index, though this quantity also stabilizes in the examples mentioned.

Following the discovery of quasicrystals in the early 1980s, there was a clear need for generalizing these concepts to accommodate aperiodic situations. A very natural approach consists in extending the setting from lattices to finitely generated $\mathbb{Z}$-modules that are embedded in $\mathbb{R}^d$, such as rings of cyclotomic integers in the plane [19, 3] or similar sets in higher dimensions [2, 25, 26]. In general, such sets are dense, but commensurability and the commensurator are still well defined, all on the basis of group-subgroup indices, see [2] for details. This is the approach we shall use here, too. For a given $\mathbb{Z}$-module $\varGamma$, it leads to the determination of its elementary coincidence spectrum and the corresponding coincidence site modules (CSMs), classified according to their index in $\varGamma$. In this paper, we focus on single intersections, as they permit a rather general solution with algebraic methods based on maximal orders in quaternion algebras over real algebraic number fields. Single intersections are also the most important ones for the applications in physics, as they refer to the grain boundaries of twins, which are more abundant than multiple junctions.

The paper is written in a self-contained way, in order to also reach readers from the applied sciences. For this reason, we have not aimed at maximal generality, and we have tried to give simple proofs, rather than refer to general abstract results (though the latter are also mentioned at several places). The full machinery will be developed in a forthcoming publication [6], together with further examples that are beyond our scope here.

The material is organized as follows. Section 2 reviews the situation of the body centred cubic lattice as a motivating example, hinting at the underlying connection to quaternion arithmetic. The connection with quaternion algebra is summarized in Section 3, followed by the core of the paper in Sections 4 – 6. Here, we develop the precise connection to reduced one-sided ideals in maximal orders and the general solution of the coincidence problem in the case that both the quaternion algebra and the base field have class number 1. Section 7 applies the general findings to three specific cases of interest, which are related to the Hurwitz, the icosian and the octahedral rings, followed by some open questions.

## 2. Example: The body centred cubic lattice in $\mathbb{R}^3$

Let $\mathbb{Z}^3$ be the standard primitive cubic lattice in 3-space, and consider $\varGamma_{\mathrm{bcc}} := \mathbb{Z}^3 \cup (v + \mathbb{Z}^3)$, where $v = \frac{1}{2}(1,1,1)^t$. It is well known [13, 5] that

$$\mathrm{(S)OC}(\varGamma_{\mathrm{bcc}}) \;=\; \mathrm{(S)O}(3,\mathbb{Q})\,,$$

which is clear from $\varGamma_{\mathrm{bcc}} \sim \mathbb{Z}^3$ and the corresponding statement for $\mathbb{Z}^3$, compare [2, 5]. From now on, we shall restrict ourselves to rotations, i.e., to orientation preserving isometries. In 3-space, the orientation reversing isometries are of the form $-R$ with $R$ a rotation. As $-\mathbb{1}_3$

commutes with all isometries and is a symmetry of $\varGamma_{\rm bcc}$ (and, in fact, of all lattices and $\mathbb{Z}$-modules $\varGamma$ in 3-space), it is clear that the consideration of $\mathrm{SOC}(\varGamma_{\rm bcc})$ (or of $\mathrm{SOC}(\varGamma)$) is sufficient to analyze the corresponding coincidence problem completely. Note also that $\mathrm{SO}(3,\mathbb{Q})$ is a dense subgroup of $\mathrm{SO}(3,\mathbb{R})$.

The main interest lies in the classification of the CSLs $\varGamma_{\rm bcc} \cap R\varGamma_{\rm bcc}$ that emerge from $R \in \mathrm{SO}(3,\mathbb{Q})$, grouped according to their index

$$\varSigma(R) \; := \; [\varGamma_{\rm bcc} : (\varGamma_{\rm bcc} \cap R\varGamma_{\rm bcc})] \, .$$

The answer is well known [13, 2] and can be formulated either explicitly in terms of lattices and their bases [13] or in terms of quaternions [2, 25]. In particular, the elementary coincidence spectrum is the set of odd integers,

$$\varSigma\big(\mathrm{SOC}(\varGamma_{\rm bcc})\big) \; = \; 2\mathbb{N}_0 + 1 \; = \; \{1,3,5,\dots\} \, . \tag{1}$$

An interesting quantity is the number of CSLs of $\varGamma_{\rm bcc}$ of index $m$, denoted by $f(m)$. It turns out to be a multiplicative arithmetic function, i.e., $f(mn) = f(m)f(n)$ for $m,n$ coprime, and is thus specified by its values at prime powers (other than 1): $f(2^r) = 0$ and $f(p^r) = (p+1)p^{r-1}$, for odd primes $p$. This results in the Euler factors

$$E_p(s) \; = \; \sum_{r\geq 0} \frac{f(p^r)}{p^{rs}} \; = \; \frac{1+p^{-s}}{1-p^{1-s}} \; = \; \frac{1-p^{-2s}}{(1-p^{-s})(1-p^{1-s})}$$

for odd primes, and in $E_2(s) = 1$. The corresponding Dirichlet series generating function reads

$$\begin{aligned} \varPhi_{\rm cub}(s) \; &= \; \sum_{m=1}^{\infty} \frac{f(m)}{m^s} \; = \; \prod_{p\in\mathcal{P}} E_p(s) \; = \; \frac{1-2^{1-s}}{1+2^{-s}} \cdot \frac{\zeta(s)\,\zeta(s-1)}{\zeta(2s)} \\ &= \; 1 + \frac{4}{3^s} + \frac{6}{5^s} + \frac{8}{7^s} + \frac{12}{9^s} + \frac{12}{11^s} + \frac{14}{13^s} + \frac{24}{15^s} + \frac{18}{17^s} + \frac{20}{19^s} + \dots \, , \end{aligned} \tag{2}$$

where $\mathcal{P} = \{2,3,5,7,11,\dots\}$ is the set of rational primes and $\zeta(s) = \sum_{n\geq 1} n^{-s}$ is Riemann's zeta function. As we shall see later, this generating function applies to all three cubic lattices (primitive, face centred and body centred), which is why we have called it $\varPhi_{\rm cub}$.

This Dirichlet series permits the determination of asymptotic properties of $f(m)$, e.g., by means of Delange's theorem (though we do not need the full strength of it), see [4, Appendix] for a formulation adapted to the situation at hand. The result is formulated via the corresponding summatory function and reads

$$F(x) \; := \; \sum_{m\leq x} f(m) \; \sim \; \frac{3}{\pi^2}\, x^2 \; = \; \frac{1}{\zeta(2)}\, \frac{x^2}{2} \, , \qquad \text{as } x \to \infty,$$

where $1/\zeta(2) = 6/\pi^2$ is the residue of $\varPhi_{\rm cub}(s)$ at its right-most singularity, a simple pole at $s = 2$. This shows that $f(m)$ increases linearly on average and, following [14], see Chapter 18.2 and the footnote on p. 266 of it, one also says that $6m/\pi^2$ is the average size of the arithmetic function $f(m)$.

Moreover, as observed in [2], one can express (2) in terms of the zeta function of the Hurwitz ring $\mathbb{J}$ of integer quaternions [15] in the quaternion algebra $\mathbb{H}(\mathbb{Q})$ as

$$\Phi_{\rm cub}(s) \;=\; \frac{1}{1+2^{-s}}\cdot\frac{\zeta_{\mathbb{J}}(s/2)}{\zeta(2s)} \;=\; \frac{\zeta_{\mathbb{J}}(s/2)}{\zeta_{\mathbb{J}.\mathbb{J}}(s/2)}\,, \tag{3}$$

where $\zeta_{\mathbb{J}}(s)$ and $\zeta_{\mathbb{J}.\mathbb{J}}(s)$ are the Dirichlet series generating functions for the one- and two-sided ideals of $\mathbb{J}$, see Section 7.1 for details. This indicates that one should be able to re-derive the result using the arithmetic structure of the ring $\mathbb{J}$ and to generalize it to other situations. That is what we achieve in this article, with special focus on results and conjectures made in [5, 2]. For first results on multiple CSLs of $\varGamma_{\rm bcc}$, we refer to [26, 27].

## 3. Quaternion algebra and orthogonal groups

Let us first recall some basic results about quaternions and introduce some notation, see [17, Sec. 57] for background material. Let $K$ be a real algebraic number field of finite degree over $\mathbb{Q}$. We consider the corresponding quaternion algebra,

$$\mathbb{H}(K) \;=\; K + {\rm i}K + {\rm j}K + {\rm k}K,$$

which is a skew field, otherwise known as a division algebra. A convenient form of the defining relations for the generating elements 1 (implicit in the above representation) and $\rm i, j, k$ is the original one due to Hamilton [16],

$${\rm i}^2 \;=\; {\rm j}^2 \;=\; {\rm k}^2 \;=\; {\rm ijk} \;=\; -1,$$

together with the requirement that $K$ is central in $\mathbb{H}(K)$. We note that $K$ is the exact centre of the algebra $\mathbb{H}(K)$.

A single quaternion $x = x_0 + {\rm i}x_1 + {\rm j}x_2 + {\rm k}x_3$ is sometimes also written as $x = (x_0, x_1, x_2, x_3)$, i.e., as a row vector, while $x^t$ denotes its column counterpart. The following result is standard, compare [16] and references therein.

**Fact 1.** *$\mathbb{H}(K)$ is canonically equipped with the following structural maps and properties.*

(i) *the* conjugation: *$x \mapsto \bar{x} := x_0 - {\rm i}x_1 - {\rm j}x_2 - {\rm k}x_3$, which is an anti-automorphism on the $K$-algebra $\mathbb{H}(K)$, i.e., one has $\overline{xy} = \bar{y}\,\bar{x}$ for all $x, y \in \mathbb{H}(K)$;*

(ii) *the* reduced norm *and* reduced trace: *${\rm nr}, {\rm tr}\colon \mathbb{H}(K) \longrightarrow K$, defined by*

$${\rm nr}(x) \;=\; x\bar{x} \;=\; \textstyle\sum_i x_i^2 \quad \textit{and} \quad {\rm tr}(x) \;=\; x + \bar{x} \;=\; 2x_0.$$

*They satisfy the identity ${\rm nr}(x+y) = {\rm nr}(x) + {\rm nr}(y) + {\rm tr}(x\bar{y})$, which makes ${\rm nr}$ a quadratic form on the vector space $\mathbb{H}(K)$;*

(iii) *the Euclidean scalar product associated to the reduced norm, $\langle x, y\rangle := \frac{1}{2}\,{\rm tr}(x\bar{y}) = \sum_i x_i y_i$, which defines the Euclidean metric on $\mathbb{H}(K) \cong K^4$ and makes $\{1, {\rm i}, {\rm j}, {\rm k}\}$ an orthonormal basis of $\mathbb{H}(K)$ (a so-called 4-bein);*

(iv) *an orthogonal decomposition $\mathbb{H}(K) = \mathbb{H}_+ \oplus \mathbb{H}_-$ into eigenspaces of the conjugation map, where*

$$\mathbb{H}_+ \;:=\; \{x \in \mathbb{H}(K) \mid \bar{x} = x\} = K \quad \textit{and}$$
$$\mathbb{H}_- \;:=\; \{x \in \mathbb{H}(K) \mid \bar{x} = -x\} \;=\; {\rm i}K \oplus {\rm j}K \oplus {\rm k}K.$$

*The elements of* $\mathbb{H}_+$ *are the* scalar quaternions *and those of* $\mathbb{H}_-$ *are the* pure quaternions*. For* $x \in \mathbb{H}(K)$*, we call the corresponding components* $\mathrm{Re}(x) := \frac{1}{2}(x + \bar{x})$ *the* real part *and* $\mathrm{Im}(x) := \frac{1}{2}(x - \bar{x})$ *the* imaginary part *of* $q$*.* □

For $x \in \mathbb{H}(K)$, the (reduced) characteristic polynomial (and the minimal polynomial for $x \notin K$) is just $X^2 - \mathrm{tr}(x)X + \mathrm{nr}(x)$. It is preserved under each algebra automorphism of $\mathbb{H}(K)$, and the same is true for conjugation, orthogonality, the metric, and the decomposition into scalar and pure part. Therefore, any inner automorphism $i_q \colon x \mapsto qxq^{-1}$ (for $x \in \mathbb{H}(K)$ and $q \in \mathbb{H}(K)^\bullet := \mathbb{H}(K) \setminus \{0\}$ ) leaves both subspaces $\mathbb{H}_+$ and $\mathbb{H}_-$ invariant and induces an isometry on $\mathbb{H}_- \cong K^3$. Hence, $q \mapsto i_q$ defines a homomorphism $\mathbb{H}(K)^\bullet \longrightarrow \mathrm{SO}(\mathbb{H}_-)$ where $\mathrm{SO}(\mathbb{H}_-) \simeq \mathrm{SO}(3, K)$.

The map $i_q$ fixes the elements of the space $K + qK$, which, for $q \notin K$, intersects $\mathbb{H}_-$ in the line $\mathrm{Im}(q)K$, whose orthocomplement $W$ in $\mathbb{H}_-$ is a plane. Hence, $\mathbb{H}_- = \mathrm{Im}(q)K \oplus W$. For $w \in W$, we obtain $0 = 2\langle q, w\rangle = \mathrm{tr}(q\bar{w}) = q\bar{w} + w\bar{q} = -qw + w\bar{q}$. This implies the relation $qwq^{-1} = q\bar{q}^{-1}w$ which shows that $i_q$, restricted to $\mathbb{H}_-$, is a rotation with axis $\mathrm{Im}(q)$ and rotation number $q\bar{q}^{\,-1}$ (whose real part is $\cos(\varphi)$).

If $q \in \mathbb{H}_- \setminus \{0\}$, then $q\bar{q}^{\,-1} = -1$, hence the eigenvalues of $-i_q$ on $\mathbb{H}_-$ are $-1$ on the one-dimensional subspace $qK$, and $+1$ on its two-dimensional complement $W$, i.e., $-i_q$ is the reflection symmetry of $\mathbb{H}_-$ with respect to $qK$. Recall that any rotation of the three-dimensional space $\mathbb{H}_-$ is a product of two reflection symmetries $-i_q$, $-i_{q'}$ for $q, q' \in \mathbb{H}_-$, see [17, Thm. 43.4, p. 105] for details in the generality needed. Consequently, the rotation is induced by $i_{qq'}$, which proves the surjectivity of the homomorphism $\mathbb{H}(K)^\bullet \longrightarrow \mathrm{SO}(\mathbb{H}_-)$ defined by $q \mapsto i_q$.

The above argument also shows that, for any $q \in \mathbb{H}(K)$, one has $qx = xq$ if and only if $x \in K + qK$, i.e., $q$ or $x$ is central, or $\mathrm{Im}(q)$ and $\mathrm{Im}(x)$ are collinear (or parallel).

The homomorphism $q \mapsto i_q$ can be made more explicit as follows: After identifying $K^3 = \mathrm{i}K \oplus \mathrm{j}K \oplus \mathrm{k}K = \mathbb{H}_-$, the general setting permits rotation matrices in $\mathrm{SO}(3, K)$ to be written via Cayley's parametrization (which goes back to Euler for the case $K = \mathbb{R}$, compare [16]) as

$$R(q) \;:=\; R_q \;=\; \frac{1}{\mathrm{nr}(q)} \begin{pmatrix} \kappa^2 + \lambda^2 - \mu^2 - \nu^2 & -2\kappa\nu + 2\lambda\mu & 2\kappa\mu + 2\lambda\nu \\ 2\kappa\nu + 2\lambda\mu & \kappa^2 - \lambda^2 + \mu^2 - \nu^2 & -2\kappa\lambda + 2\mu\nu \\ -2\kappa\mu + 2\lambda\nu & 2\kappa\lambda + 2\mu\nu & \kappa^2 - \lambda^2 - \mu^2 + \nu^2 \end{pmatrix}, \tag{4}$$

where $q = \kappa + \mathrm{i}\lambda + \mathrm{j}\mu + \mathrm{k}\nu \in \mathbb{H}(K)^\bullet$, and where $K^3$ is considered to be represented by the column vectors $(x, y, z)^t$ with $x, y, z \in K$.

This explicit parametrization is useful in practice. The rotation axis (when $R_q$ is not the identity) is given by $(\lambda, \mu, \nu)^t$, while the corresponding rotation angle $\varphi$, using that the trace of $R(q)$ is $1 + 2\cos(\varphi)$ by Euler's theorem, is determined by

$$\cos(\varphi) \;=\; \mathrm{Re}(q/\bar{q}) \;=\; \frac{\mathrm{Re}(q^2)}{\mathrm{nr}(q)} \;=\; \frac{\kappa^2 - \lambda^2 - \mu^2 - \nu^2}{\kappa^2 + \lambda^2 + \mu^2 + \nu^2}\,.$$

**Fact 2.** *If* $K$ *is a real algebraic number field, every rotation matrix* $M \in \mathrm{SO}(3, K)$ *is of the form* $M = R_q$ *for some* $q \in \mathbb{H}(K)^\bullet$*, i.e., the mapping* $\mathbb{H}(K)^\bullet \longrightarrow \mathrm{SO}(3, K)$ *defined by the Cayley parametrization* $q \mapsto R_q$ *from* (4) *is onto.*

*Proof.* This follows from the above arguments. Alternatively, one can use the parametrization (4) for $\mathrm{SO}(3) = \mathrm{SO}(3,\mathbb{R})$, where it is well-known since Euler and emerges from the canonical 2 to 1 map from $\mathrm{SU}(2) \longrightarrow \mathrm{SO}(3)$, combined with the observation that $R(q) = R(\alpha q)$ for arbitrary non-zero $\alpha \in \mathbb{R}$. One can then show that a parametrization of the subgroup $\mathrm{SO}(3,K)$ can be achieved with the quaternions restricted to $\mathbb{H}(K)^{\bullet}$. □

Looking at this matrix setting in 4-space, noting that $K^4 \cong \mathbb{H}(K) = K \oplus \mathrm{i}K \oplus \mathrm{j}K \oplus \mathrm{k}K$ and recalling our convention to write quaternions as row vectors, one has the relation

$$\left(qaq^{-1}\right)^t \; = \; \begin{pmatrix} 1 & 0 \\ 0 & R_q \end{pmatrix} a^t$$

for arbitrary $a \in \mathbb{H}(K)$ and $q \in \mathbb{H}(K)^{\bullet}$, which reflects the orthogonal decomposition into real and imaginary parts mentioned above. In particular, one also has

$$\mathrm{Im}(qaq^{-1}) \; = \; R_q \, \mathrm{Im}(a), \tag{5}$$

which will be crucial for our further development.

## 4. Quaternion arithmetic

Consider the real algebraic number field $K$ and let $\mathcal{O}$ be the ring of integers in $K$, compare [9] for general background material on algebraic number fields.

**Assumption.** *We shall assume throughout this article that $K$ has class number* 1.

The important consequence of this, for our purposes, is that $\mathcal{O}$ is a principal ideal domain (PID) and hence that every $\mathcal{O}$-module we encounter will be free and thus has a basis. Also, our results permit a simpler formulation this way, though many can be generalized to avoid this assumption.

Next, we need to know what 'integral' and 'integer' mean in $\mathbb{H}(K)$. A quaternion $q$ is called *integral* (over $\mathcal{O}$), when both $\mathrm{tr}(q)$ and $\mathrm{nr}(q) =: |q|^2$ are in $\mathcal{O}$, i.e., when it is a root of a monic polynomial with coefficients in $\mathcal{O}$.

The notation $|q|^2$ instead of $\mathrm{nr}(q)$ is quite common and highlights the fact that the reduced norm coincides with the squared Euclidean norm of the quaternion under the standard identification of the generating elements with the Euclidean 4-bein. However, it has to be stressed here that, in spite of the notation, $|q|^2$ is in general not a square in $K$.

Clearly, if $q$ is integral, then so is $\bar{q}$. Note that, because of the invariance of conjugation, this definition is invariant under all automorphisms of $\mathbb{H}(K)$. However, due to non-commutativity, the set of integral quaternions fails to be a ring. This is the origin of various differences from the arithmetic of commutative number fields.

Following [23], we call a finitely generated $\mathcal{O}$-module whose $K$-span is the whole of $\mathbb{H}(K)$ an *ideal*. An *order* is an ideal that is also a ring containing 1, see [20, Sec. 8] and [23, Chap. 1, Sec. 4] for details. It is called *maximal* when it is not contained in any larger order of $\mathbb{H}(K)$. Note that some authors restrict the term 'ideal' to $\mathcal{O}$-modules whose left and right orders are maximal, because their properties are then more similar to those of ideals in algebraic number fields. Another term in use is that of a (full) $\mathcal{O}$-lattice, compare [20, 23].

The following basic properties of an order $L$ are important throughout the article.

**Fact 3.** *All elements of an arbitrary order $L \subset \mathbb{H}(K)$ are integral. Moreover, one has $\bar{L} = L$ and $L \cap K = \mathcal{o}$.*

*Proof.* The first assertion follows from [23, Lemme I.4.1 and Prop. I.4.2] or [20, Thms. 8.6, 9.3 and 1.14]. If $x \in L$, one has $\bar{x} = \mathrm{tr}(x) - x$, so $\bar{x} \in L$ since $\mathrm{tr}(x) \in \mathcal{o}$, and $\bar{L} = L$.

Since $1 \in L$ and $L$ is an $\mathcal{o}$-module, $\mathcal{o} \subseteq L \cap K$ is clear. Conversely, if $x \in L \cap K$, one has $\mathrm{tr}(x) = 2x \in \mathcal{o}$ and $\mathrm{nr}(x) = x^2 \in \mathcal{o}$, which implies that also $x \in \mathcal{o}$. □

An element $a$ of an order $L$ is an *$L$-unit* when $a^{-1} \in L$, and it is a consequence of Fact 3 that $a \in L$ is an $L$-unit if and only if $\mathrm{nr}(a)$ is a unit of $\mathcal{o}$. When it is clear which order is meant we shall omit the prefix $L$ and simply speak of a *unit*. A *left ideal* of $L$ is an ideal $I$ with $aI \subseteq I$ for every $a \in L$ and it is *principal* if it has the form $Lx$ for some $x \in \mathbb{H}(K)$. Right ideals and principal right ideals of $L$ are defined similarly. A *two-sided* ideal of $L$ is an ideal that is simultaneously a left ideal and a right ideal of $L$.

Clearly,

$$\mathcal{L} \;:=\; \mathcal{o} + \mathrm{i}\mathcal{o} + \mathrm{j}\mathcal{o} + \mathrm{k}\mathcal{o} \tag{6}$$

is an order, as is $q\mathcal{L}q^{-1}$ for any $q \in \mathbb{H}(K)^{\bullet}$; but it is not maximal because $\frac{1}{2}(1+\mathrm{i}+\mathrm{j}+\mathrm{k})$ is integral and appending it to $\mathcal{L}$ generates a larger order. For the applications, we are mainly interested in maximal orders that contain $\mathcal{L}$. In the literature, such maximal orders are sometimes simply referred to as rings of integers.

**Fact 4.** *If $q$ is an element of a maximal order $\mathcal{O}$ that contains $\mathcal{L}$, then $2q \in \mathcal{L}$.*

*Proof.* The $\mathcal{o}$-basis of $\mathcal{L}$ is also a $K$-basis of $\mathbb{H}(K)$, so $q = a + \mathrm{i}b + \mathrm{j}c + \mathrm{k}d$ with $a, b, c, d \in K$. Since $q$, $\mathrm{i}q$, $\mathrm{j}q$ and $\mathrm{k}q$ must all be integral (as i, j and k are units of $\mathcal{O}$), their reduced traces must be in $\mathcal{o}$. They are $2a$, $-2b$, $-2c$ and $-2d$, respectively, so that $2q \in \mathcal{L}$. □

Maximal orders $\mathcal{O}$ are certainly not unique, as the application of inner automorphisms results in different maximal orders. They may not even be unique up to inner automorphism. Orders related by an inner automorphism are said to be of the same *type*. The *class number* of a maximal order $\mathcal{O}$ is the number of equivalence classes of left ideals of $\mathcal{O}$ under the equivalence relation of right multiplication by elements of $\mathbb{H}(K)$. Since the conjugation anti-automorphism takes left ideals to right ideals, right multiplication to left multiplication and $\mathcal{O}$ to itself, interchanging the roles of 'left' and 'right' in this definition results in the same value of the class number.

**Fact 5.** *All maximal orders of $\mathbb{H}(K)$ have the same class number, in the sense just defined, which is known as the* class number of $\mathbb{H}(K)$. *Moreover, if the class number is* 1, *all maximal orders are mutual images of one another under inner automorphims.*

*Proof.* This follows from Lemme I.4.10 and Exercise I.4.1 of [23]. □

When $\mathbb{H}(K)$ has class number 1, every left ideal of a maximal order $\mathcal{O}$ has the form $\mathcal{O}q$ for some $q \in \mathcal{O}^{\bullet} := \mathcal{O} \setminus \{0\}$ (and every right ideal has the form $q\mathcal{O}$). In the case of $\mathbb{H}(\mathbb{Q})$, there is only one type of maximal order, and a unique maximal order $\mathcal{O}$ that contains $\mathcal{L}$, see [15]:

$$\mathcal{O} \;=\; \mathbb{J} \;=\; \bigl\langle 1, \mathrm{i}, \mathrm{j}, \tfrac{1}{2}(1+\mathrm{i}+\mathrm{j}+\mathrm{k}) \bigr\rangle_{\mathbb{Z}} \,. \tag{7}$$

This is the so-called Hurwitz ring of integers [15]. It is an index 2 extension of $\mathcal{L} \simeq \mathbb{Z}^4$. In fact, seen as a lattice in 4-space, it is the weight lattice $D_4^*$, the dual of the root lattice $D_4$, the latter in standard representation with roots of squared length 2, compare [11].

Later on, we shall need some information about the relation between $\mathcal{O}$ and $q\mathcal{O}q^{-1}$, for $q \in \mathcal{O}$. It is immediate that

$$\mathcal{O} = q\mathcal{O}q^{-1} \iff q\mathcal{O} = \mathcal{O}q \iff \bar{q}\mathcal{O} = \mathcal{O}\bar{q}\,, \tag{8}$$

the last characterization following from $\overline{\mathcal{O}} = \mathcal{O}$. When this occurs, $q\mathcal{O} = \mathcal{O}q$ is said to be a *two-sided ideal* of $\mathcal{O}$, and $q$ is said to generate a two-sided ideal. All elements of $K$ commute with $\mathcal{O}$, and thus generate two-sided ideals. Another example we shall meet below is $1 + \mathrm{i}$, which generates a two-sided ideal in $\mathbb{J}$, but not in our other explicit examples of Section 7.

Finally, we observe the following counterpart of the relation $L \cap K = \mathcal{o}$ from Fact 3, where we use the set-valued extension of Re, i.e., $\mathrm{Re}(S) := \{\mathrm{Re}(x) \mid x \in S\}$.

**Fact 6.** *If $\mathbb{H}(K)$ has class number 1 and if $\mathcal{O}$ is a maximal order in $\mathbb{H}(K)$, $\mathcal{O}$ has real part $\mathrm{Re}(\mathcal{O}) = \frac{1}{2}\mathcal{o}$.*

*Proof.* Assume first that $\mathcal{O}$ is a maximal order that contains $\mathcal{L}$ of (6) as well as the integral quaternion $\frac{1}{2}(1+\mathrm{i}+\mathrm{j}+\mathrm{k})$. It is clear that such a maximal order exists, and that $\frac{1}{2}\mathcal{o} \subseteq \mathrm{Re}(\mathcal{O})$ in this situation. On the other hand, $2q \in \mathcal{L}$ for all $q \in \mathcal{O}$ by Fact 4 in this case, and we must also have $\mathrm{Re}(\mathcal{O}) \subseteq \frac{1}{2}\mathcal{o}$, hence $\mathrm{Re}(\mathcal{O}) = \frac{1}{2}\mathcal{o}$. By Corollaire I.4.11 and Exercise I.4.1 of [23], all other maximal orders of $\mathbb{H}(K)$ are images of this one under inner automorphisms, and, since the real part is invariant under inner automorphisms, the result follows. □

Below, we shall often meet intersections of two (not necessarily distinct) maximal orders. These are also known as *Eichler orders*, see [23, 21] for details.

In this and the following two sections, we develop some general arguments without using specific properties of the maximal orders we have in mind for the applications. To this end, let $K$ as above be a real algebraic number field with class number 1 whose ring of integers $\mathcal{o}$ is therefore a PID. The class number property implies that every $\mathcal{o}$-module in $\mathbb{H}(K)$ is free (and thus has a basis) [1, Ch. 3, Thm. 6.6], since such modules are torsion-free. In what follows, $L$ will be an arbitrary order in $\mathbb{H}(K)$ and $\mathcal{O}$ a maximal order. Later on, we shall need the assumption that $\mathcal{O}$ has class number 1, i.e., that all ideals of $\mathcal{O}$ are principal. This condition will be formulated as a property of $\mathbb{H}(K)$ and always be mentioned explicitly.

Let us return to the parametrization of the rotations. It is clear that the choice of $q$ in (4) is not unique. In fact, we can always arrange $q \in \mathcal{O}^{\bullet}$ (by multiplying $q$ by a suitable element of $\mathcal{o}$). An element $q \in \mathcal{O}$ is called *$\mathcal{O}$-primitive* if it is not divisible by any non-unit of $\mathcal{o}$. For an arbitrary $q \in \mathcal{O}^{\bullet}$, one can define

$$\mathrm{cont}_{\mathcal{O}}(q) \;:=\; \mathrm{lcm}\{\alpha \in \mathcal{o} \mid q/\alpha \in \mathcal{O}\}\,, \tag{9}$$

which is called the *$\mathcal{O}$-content* of $q$, see [4] for details on this concept in a more general setting. It is well defined up to units of $\mathcal{o}$ due to our assumption that $\mathcal{o}$ is a PID. So, $q$ is $\mathcal{O}$-primitive when $\mathrm{cont}_{\mathcal{O}}(q)$ is a unit in $\mathcal{o}$. Alternatively, one can consider the content to be the principal ideal generated by $\mathrm{cont}_{\mathcal{O}}(q)$, which takes care of the units automatically.

More generally, when $\mathcal{O}$ is a PID as here, primitivity relative to any order $L$ of $\mathbb{H}(K)$ can be defined in an analogous way: $q \in L$ is *$L$-primitive* if it cannot be factorized as $q = \alpha r$, with $r \in L$ and $\alpha$ a non-unit in $\mathcal{O}$. As with units, we shall omit the prefix $L$ when it is clear which order is meant. Also the *$L$-content*, $\mathrm{cont}_L(q)$, for any $q \in L^\bullet$ can be defined analogously to the $\mathcal{O}$-content, and is again unique up to units of $\mathcal{O}$. In particular, primitivity relative to the order $\mathcal{L}$ of (6) is another useful concept. In [15], an element $q \in \mathcal{L}$ that is $\mathcal{L}$-primitive in this sense is often simply called *primitive*, and this property is equivalent to the condition that $\gcd(q) := \gcd(q_0, q_1, q_2, q_3) = 1$, where the gcd is defined as usual, and determined up to a unit of $\mathcal{O}$. More generally, one has $\mathrm{cont}_{\mathcal{L}}(q) = \gcd(q)$.

**Proposition 1.** *Let $L$ be an arbitrary order of $\mathbb{H}(K)$ and let $R\colon\, q \mapsto R(q)$ be Cayley's parametrization of* (4)*. Then, one has $R(L^\bullet) = \mathrm{SO}(3, K)$. Moreover, any rotation matrix $M \in \mathrm{SO}(3, K)$ can be parametrized as $M = R(q)$ with an $L$-primitive element $q \in L$. This gives a multiple cover of $\mathrm{SO}(3, K)$, where the remaining multiplicity is due to $R(\varepsilon q) = R(q)$ with $\varepsilon$ a unit in $\mathcal{O}$.*

*Proof.* Since $R(\mathbb{H}(K)^\bullet) = \mathrm{SO}(3, K)$ by Fact 2, it is clear that, given a matrix $M \in \mathrm{SO}(3, K)$, $q$ can be chosen to satisfy $R(q) = M$ and to be an $L$-primitive quaternion at the same time, the latter condition due to the freedom to multiply $q$ by a suitable non-zero element of $K$, which commutes with $q$ and does not change the matrix $M$.

Clearly, $R(\varepsilon q) = R(q)$ for any unit $\varepsilon \in \mathcal{O}$, and $\varepsilon q$ is $L$-primitive when $q$ is. In view of Eq. (5), and the fact that $\mathrm{Re}(qaq^{-1}) = \mathrm{Re}(a)$, two quaternions $p, q$ parametrize the same matrix $M$ if and only if $p^{-1}q$ is a central element of $\mathbb{H}(K)$, so $q = \alpha p$ with $\alpha \in K$. When $p$ and $q$ are both $L$-primitive, such a relation can only hold when $\alpha$ is a unit in $\mathcal{O}$. □

**Remark 1.** The relevance of Proposition 1 originates in the observation that

$$\mathrm{SOC}\big(\mathrm{Im}(\mathcal{L})\big) \;=\; \mathrm{comm}_{\mathrm{SO}(3,\mathbb{R})}\big(\mathrm{Im}(\mathcal{L})\big) \;=\; \mathrm{SO}(3, K)\,, \tag{10}$$

since $\mathrm{Im}(\mathcal{L})$ is the $\mathcal{O}$-span of the standard Euclidean 3-bein in $\mathbb{R}^3$. Moreover, $\mathrm{SO}(3, K)$ is the SOC-group of $\mathrm{Im}(L)$ for *any* order $L$ of $\mathbb{H}(K)$, because $\mathcal{L}$ and $L$ (and hence also $\mathrm{Im}(\mathcal{L})$ and $\mathrm{Im}(L)$) are commensurate.

## 5. Index calculations

One of our main goals is to compute indices of CSMs. As we shall see below, this will require working out indices of the form $[\mathrm{Im}(L) : \mathrm{Im}(qL)]$ for elements $q \in L^\bullet$. To achieve this in a simple and systematic fashion, it is advantageous along the way, and essential for our later proofs in this concrete approach, to work with indices which take values in $\mathcal{O}$ rather than in $\mathbb{Z}$, and we define these now. In fact, we define these more general indices to be principal ideals in $\mathcal{O}$. In this setting, the coset-counting indices of interest can later be derived as the absolute norms of the corresponding $\mathcal{O}$-indices, see Fact 8 below.

For a vector space $V$ over $K$ and a $K$-linear map $\phi$ of $V$ into itself, we use $\det_K(\phi)$ to denote the usual determinant of $\phi$. It is an element of $K$ and can be calculated using a $K$-basis of $V$. Similarly, $\det_{\mathbb{Q}}(\phi)$ denotes the determinant of $\phi$ when $V$ is regarded as a vector space over

$\mathbb{Q}$ and $\phi$ as a $\mathbb{Q}$-linear map. It is a rational number and can be calculated using a $\mathbb{Q}$-basis of $V$. In both cases, the result is independent of the particular basis chosen.

If $J \subseteq I$ are full $\mathcal{O}$-modules in $V$, we define the *$K$-index* of $J$ in $I$ as

$$[I : J]_K \;:=\; \det_K(\phi)\,\mathcal{O}, \tag{11}$$

where $\phi$ is a linear map that takes an $\mathcal{O}$-basis of $I$ to an $\mathcal{O}$-basis of $J$ and $\det_K(\phi)\,\mathcal{O}$ is the principal ideal of $\mathcal{O}$ generated by $\det_K(\phi)$. The determinant $\det_K(\phi)$ is in $\mathcal{O}$, since $J \subseteq I$, and changing the bases of $I$ and $J$ multiplies it by a unit of $\mathcal{O}$, so the ideal $[I : J]_K$ is independent of the chosen bases. By considering the inverse of $\phi$, it is clear that $I = J$ if and only if $[I : J]_K = \mathcal{O}$. The $K$-index is multiplicative: if $I_1 \supseteq I_2 \supseteq I_3$ are full $\mathcal{O}$-modules in $V$, one has

$$[I_1 : I_3]_K \;=\; [I_1 : I_2]_K\,[I_2 : I_3]_K. \tag{12}$$

We also write $[I : J] = |\det_{\mathbb{Q}}(\phi)|$, a positive integer, which is the index of $J$ in $I$ in the usual sense.

**Lemma 1.** *For any order $L$ in $\mathbb{H}(K)$ and any $q \in L^{\bullet}$, one has $[L : qL]_K = [L : Lq]_K = |q|^4\mathcal{O}$.*

*Proof.* It is sufficient to prove the claim for right ideals $qL$. The linear map $\phi_q \colon x \mapsto qx$ (the left regular representation of $q$ on $\mathbb{H}(K)$) takes an $\mathcal{O}$-basis of $L$ to an $\mathcal{O}$-basis of $qL$, and a straightforward calculation using the basis $\{1, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$ of $\mathbb{H}(K)$ gives $\det_K(\phi_q) = |q|^4$. □

Our next result is an index formula that provides the link to our problem in 3-space by giving the indices of images under the mapping $x \mapsto \mathrm{Im}(x)$ and paves the way to 3-dimensional analogues of Lemma 1.

**Proposition 2.** *If $J \subseteq I$ are ideals in $\mathbb{H}(K)$, one has the index relations*

$$\begin{aligned}
[I : J]_K \;&=\; [I \cap \mathbb{H}_+ : J \cap \mathbb{H}_+]_K\,[\mathrm{Im}(I) : \mathrm{Im}(J)]_K \quad \textit{and}\\
[I : J]_K \;&=\; [\mathrm{Re}(I) : \mathrm{Re}(J)]_K\,[I \cap \mathbb{H}_- : J \cap \mathbb{H}_-]_K\,,
\end{aligned}$$

*where all five indices are principal ideals of $\mathcal{O}$.*

*Proof.* These identities are both instances of the fact that the density of a lattice (being the reciprocal of the absolute value of its determinant) is the density of an orthogonal projection of it multiplied by the density of the kernel of the projection.

For the first identity, choose generators $\alpha_0$ and $\beta_0$ of $I \cap \mathbb{H}_+$ and $J \cap \mathbb{H}_+$ and extend them to $\mathcal{O}$-bases

$$\{\alpha_0, \alpha_1 + u_1, \alpha_2 + u_2, \alpha_3 + u_3\} \quad \text{and} \quad \{\beta_0, \beta_1 + u_1, \beta_2 + u_2, \beta_3 + u_3\}$$

of $I$ and $J$; these operations being possible by [1, Thm. 6.16], since $\alpha_0$ and $\beta_0$ are primitive elements of $I$ and $J$ in the sense of [1]. By construction, $\{\mathrm{Im}(u_1), \mathrm{Im}(u_2), \mathrm{Im}(u_3)\}$ and $\{\mathrm{Im}(v_1), \mathrm{Im}(v_2), \mathrm{Im}(v_3)\}$ are then $\mathcal{O}$-bases of $\mathrm{Im}(I)$ and $\mathrm{Im}(J)$. Note that, due to our convention, each $\mathrm{Im}(u_i)$ is the transpose of the row vector $u_i$ without its first coordinate, and similarly for the row vectors $v_j$. Since $I \cap \mathbb{H}_+$ and $J \cap \mathbb{H}_+$ are 1-dimensional, $[I \cap \mathbb{H}_+ : J \cap \mathbb{H}_+]_K$ is trivially evaluated as $(\beta_0/\alpha_0)\mathcal{O}$. If

$$x \;=\; \mu_0\alpha_0 + \mu_1(\alpha_1 + u_1) + \mu_2(\alpha_2 + u_2) + \mu_3(\alpha_3 + u_3)\,,$$

one has

$$\mathrm{Im}(x) \;=\; \mathrm{Im}\bigl(\mu_1 u_1 + \mu_2 u_2 + \mu_3 u_3\bigr),$$

so the $4\times 4$ matrix of the linear map taking the basis of $I$ to the basis of $J$ has the form

$$M \;=\; \begin{pmatrix} \beta_0/\alpha_0 & m \\ 0 & M_3 \end{pmatrix}^t ,$$

where $M_3$ is the $3\times 3$ matrix of the linear map taking the basis of $\mathrm{Im}(I)$ to the basis of $\mathrm{Im}(J)$. Taking determinants of both sides gives

$$[I:J]_K \;=\; \det(M)\,\mathcal{O} \;=\; (\beta_0/\alpha_0)\det(M_3)\,\mathcal{O} \;=\; [I\cap\mathbb{H}_+ : J\cap\mathbb{H}_+]_K\,[\mathrm{Im}(I):\mathrm{Im}(J)]_K .$$

For the second identity, let $\alpha$ and $\beta$ be generators of the $\mathcal{O}$-ideals $\mathrm{Re}(I)$ and $\mathrm{Re}(J)$, choose $u_0$ and $v_0$ in $\mathbb{H}_-$ with $\alpha+u_0\in I$ and $\beta+v_0\in J$, and choose bases $\{u_1,u_2,u_3\}$ and $\{v_1,v_2,v_3\}$ of $I\cap\mathbb{H}_-$ and $J\cap\mathbb{H}_-$. Then, $\{\alpha+u_0,u_1,u_2,u_3\}$ and $\{\beta+v_0,v_1,v_2,v_3\}$ are bases of $I$ and $J$, and the $4\times 4$ matrix of the linear map taking the former to the latter is

$$M \;=\; \begin{pmatrix} \beta/\alpha & m \\ 0 & M_3^t \end{pmatrix},$$

where $M_3$ is the $3\times 3$ matrix of the linear mapping that takes $\{\mathrm{Im}(u_1),\mathrm{Im}(u_2),\mathrm{Im}(u_3)\}$ to $\{\mathrm{Im}(v_1),\mathrm{Im}(v_2),\mathrm{Im}(v_3)\}$. Hence

$$[I:J]_K \;=\; \det(M)\,\mathcal{O} \;=\; (\beta/\alpha)\det(M_3)\,\mathcal{O} \;=\; [\mathrm{Re}(I):\mathrm{Re}(J)]_K\,[I\cap\mathbb{H}_- : J\cap\mathbb{H}_-]_K\,,$$

which completes the argument. □

Since $\mathbb{H}_+\simeq K$ in our setting, we shall usually write $I\cap K$ instead of $I\cap\mathbb{H}_+$ from now on.

**Fact 7.** *If $L'\subset L$ are orders in $\mathbb{H}(K)$, one has* $[L:L']_K=[\mathrm{Im}(L):\mathrm{Im}(L')]_K$.

*Proof.* This follows from Proposition 2, since $L\cap K=L'\cap K=\mathcal{O}$, by Fact 3. □

**Lemma 2.** *If $L$ is an order of $\mathbb{H}(K)$ and $q\in L$ is $L$-primitive, one has*

$$qL\cap K \;=\; L\bar{q}\cap K \;=\; |q|^2\mathcal{O}.$$

*Proof.* It is sufficient to prove $qL\cap K=|q|^2\mathcal{O}$, as the other claim follows by conjugation. Observe that the inclusions $|q|^2\mathcal{O}\subseteq qL\cap K$ and $qL\cap K\subseteq\mathcal{O}$ are clear. It remains to show that $\alpha\in qL\cap K$ implies $|q|^2\mid\alpha$. We have $\bar{q}\alpha=\alpha\bar{q}=|q|^2r$, where also $\bar{q}$ is $L$-primitive, i.e., $\mathrm{cont}_L(\bar{q})$ is a unit in $\mathcal{O}$. Consequently, we have $|q|^2\mid\mathrm{cont}_L(\alpha\bar{q})=\alpha$. □

**Lemma 3.** *If $L$ is an order of $\mathbb{H}(K)$ and $q\in L$ is $L$-primitive, one has the index formula*

$$[\mathrm{Im}(L):\mathrm{Im}(qL)]_K \;=\; [\mathrm{Im}(L):\mathrm{Im}(L\bar{q})]_K \;=\; |q|^2\mathcal{O}.$$

*Proof.* This follows from Proposition 2 and Lemmas 1 and 2, since $[\mathcal{O}:|q|^2\mathcal{O}]_K=|q|^2\mathcal{O}$. □

In the three lemmas derived so far, and in various places below, there are obvious additional identities, due to the freedom to replace $q$ by $\bar{q}$.

To make the transition from $K$-indices to the usual indices of modules, we need to introduce norms from $K$ to $\mathbb{Q}$. Let $\mathrm{N}:=|\mathrm{N}_{K/\mathbb{Q}}|$ be the absolute norm from $K$ to $\mathbb{Q}$, which is given by $\mathrm{N}(\alpha) = \bigl|\prod \sigma(\alpha)\bigr| \in \mathbb{Q}$, where $\sigma$ runs through the homomorphisms of $K$ into $\mathbb{C}$. It is a non-negative rational number for all $\alpha \in K$, and a non-negative integer for $\alpha \in \mathcal{O}$.

The absolute norm can also be defined for principal ideals of $\mathcal{O}$ by $\mathrm{N}(\alpha\mathcal{O}) = \mathrm{N}(\alpha)$, and is independent of the generator $\alpha$, since the ratio of any two generators is a unit and has absolute norm 1.

**Fact 8.** *With* N *as above and $V$, $\phi$ as in the paragraph preceding Eq.* (11), *we have the identity* $|\det_{\mathbb{Q}}(\phi)| = \mathrm{N}\bigl(\det_K(\phi)\bigr)$. *In particular,* $[I : J] = \mathrm{N}\bigl([I : J]_K\bigr)$ *for any ideals $I, J$ of $\mathbb{H}(K)$ with $J \subseteq I$.*

*Proof.* This is a standard result that can be proved by embedding $V$ in $V_{\mathbb{R}}^r \oplus V_{\mathbb{C}}^s \simeq \mathbb{R}^{nd}$, where $V_{\mathbb{R}}$ is the real vector space $V \otimes_K \mathbb{R}$ (the *realification* of $V$), $V_{\mathbb{C}}$ is the complex vector space $V \otimes_K \mathbb{C}$ (the *complexification* of $V$), $r$ is the number of homomorphisms of $K$ into $\mathbb{R}$, $s$ is the number of complex conjugate pairs of homomorphisms of $K$ into $\mathbb{C}$, $d = r + 2s$ is the degree of $K$ over $\mathbb{Q}$ and $n$ is the dimension of $V$. Then, $\phi$ can be extended to an $\mathbb{R}$-linear map of $\mathbb{R}^{nd}$ into itself and the determinant of the extended linear map is the norm of the determinant of $\phi$. The 1-dimensional case of this construction is given in [9, Ch. II.3.1] and the general case in [18, Sec. 4]. □

This gives the following useful consequences.

**Proposition 3.** *Let $L' \subseteq L$ be arbitrary orders in $\mathbb{H}(K)$ and $q \in L^{\bullet}$. Then, one has*

(i) $[L : L'] = [\mathrm{Im}(L) : \mathrm{Im}(L')]$;

(ii) $[L : qL] = [L : Lq] = \mathrm{N}\bigl(|q|^4\bigr)$;

(iii) $[\mathrm{Im}(L) : \mathrm{Im}(qL)] = [\mathrm{Im}(L) : \mathrm{Im}(Lq)] = \mathrm{N}\bigl(|q|^2\bigr)$, *provided that $q$ is $L$-primitive.*

*Proof.* Part(i) is immediate from Facts 7 and 8. Part (ii) results from combining Fact 8 with Lemma 1, and Part (iii) from combining it with Lemma 3. □

**Remark 2.** Part (ii) of Proposition 3 clearly displays the correct scaling behaviour of the index when $q$ is replaced by $\alpha q$ with $\alpha \in \mathcal{O}$. Taking the scaling behaviour into account in Part (iii), it is almost immediate that its extension to general $q \in L^{\bullet}$ reads

$$[\mathrm{Im}(L) : \mathrm{Im}(qL)] \; = \; [\mathrm{Im}(L) : \mathrm{Im}(Lq)] \; = \; \mathrm{N}\bigl(\mathrm{cont}_L(q)\bigr)\, \mathrm{N}\bigl(|q|^2\bigr). \tag{13}$$

It is possible [24] to derive generalizations of (13) to central simple algebras of dimension $n^2$ over fields with a Dedekind ring $\mathcal{O}$, with $q \mapsto \mathrm{Im}(q)$ replaced by the mapping $q \mapsto q - \frac{1}{n}\mathrm{tr}(q)$. Our formula would then result from taking $n = 2$ and considering only principal ideals.

Let us now look at the coincidence problem for the rank 3 $\mathcal{O}$-module $\Gamma := \mathrm{Im}(L)$, where we want to classify the intersections $\Gamma \cap R\Gamma$ with $R \in \mathrm{SOC}(\Gamma)$ according to their indices. From Proposition 1, we already know that, for finite index, we may restrict to $R = R_q$ with $q \in L^{\bullet}$, and with the identity (5) we have

$$\Gamma \cap R_q \Gamma \; = \; \mathrm{Im}(L) \cap R_q\, \mathrm{Im}(L) \; = \; \mathrm{Im}(L) \cap \mathrm{Im}(qLq^{-1}). \tag{14}$$

**Lemma 4.** *If $L$ is an order of $\mathbb{H}(K)$ and $q \in L^{\bullet}$, one has the relation*

$$\mathrm{Im}(L) \cap \mathrm{Im}(qLq^{-1}) \; = \; \mathrm{Im}(L \cap qLq^{-1}).$$

*Proof.* The inclusion $\supseteq$ is immediate, so we have to prove the converse. Consider an element $u^t \in \mathrm{Im}(L) \cap \mathrm{Im}(qLq^{-1})$, where we write $u^t$ for the transpose of $u$ without its first coordinate. As $\mathrm{Im}(qLq^{-1}) = R_q \mathrm{Im}(L)$, there is some $v^t \in \mathrm{Im}(L)$ with $u^t = R_q v^t$, and we can choose $x = (\alpha, u)$ and $y = (\beta, v)$ in $L$, with $\alpha, \beta \in K$. Assume for a moment that $\alpha - \beta \in \mathcal{O}$. Then, $z = \alpha - \beta + y = (\alpha, v) \in L$ with $\mathrm{Im}(z) = \mathrm{Im}(y)$. Moreover, one has

$$qzq^{-1} \;=\; q(\alpha, v)q^{-1} \;=\; (\alpha, u) \;=\; x \;\in\; L$$

so that $qzq^{-1} \in L \cap qLq^{-1}$ with $\mathrm{Im}(qzq^{-1}) = u^t$.

It remains to show that $\alpha - \beta \in \mathcal{O}$. Observe that, since $x$ and $y$ are integral,

$$\begin{aligned} \mathrm{tr}(x) &= 2\alpha := \gamma \in \mathcal{O}, \\ \mathrm{tr}(y) &= 2\beta := \delta \in \mathcal{O}, \text{ and} \\ \mathrm{nr}(x) - \mathrm{nr}(y) &= \alpha^2 - \beta^2 = (\gamma^2 - \delta^2)/4 \in \mathcal{O}, \end{aligned}$$

the last line because $\mathrm{nr}(y) = \mathrm{nr}(qyq^{-1}) = \mathrm{nr}(\beta, u)$. We now have $4|(\gamma^2 - \delta^2)$ with $\gamma, \delta \in \mathcal{O}$, and the proof will be complete if we can deduce from this that $2|(\gamma - \delta)$. Let $\pi$ be a prime factor of 2 and suppose that $\pi^e \parallel 2$. Now, $\pi^e \nmid (\gamma - \delta)$ would imply $\pi^e \nmid (\gamma + \delta)$, since $\gamma + \delta \equiv \gamma - \delta \pmod 2$, giving $\pi^{2e} \nmid (\gamma^2 - \delta^2)$ and contradicting the fact that $\gamma^2 - \delta^2$ is divisible by 4. Hence every prime factor of 2 divides $\gamma - \delta$ to at least as high a power as it divides 2 and we have established that $2|(\gamma - \delta)$ and thus $\alpha - \beta \in \mathcal{O}$. □

The set of $L$-primitive elements of $L$ is still too big for our purposes. Recall that any $q \in L^\bullet$ with the property that $qL$ is a two-sided ideal also satisfies $qLq^{-1} = L$, and is thus not of interest for the coincidence problem (at least as far as counting the CSMs is concerned). In fact, the elements of $L$ that generate two-sided ideals give, via the parametrization $R$, a multiple cover of the rotation symmetry group of the module $\mathrm{Im}(L)$, the multiplicity being due to units of $\mathcal{O}$. Consider a general element $x \in L^\bullet$ and assume that it is of the form $x = aqb$ with $a, b, q \in L^\bullet$ and $qL = Lq$, so that $q$ generates a 2-sided ideal. Then, there are elements $a', b' \in L^\bullet$ such that $x = qa'b = ab'q$, and $q$ is then both a left and a right divisor of $x$. We can thus simply call $q$ a divisor of $x$ in this case. Now, $x$ is called *$L$-reduced* if no divisor $q$ of $x$ other than the units of $L$ satisfies $qL = Lq$. Again, we shall omit the prefix $L$ when it is clear from the context. Recalling Eq. (5), and thus the identity

$$R_q \,\mathrm{Im}(L) \;=\; \mathrm{Im}(qLq^{-1})\,,$$

the following consequence of Proposition 1 and Lemma 4 is immediate.

**Corollary 1.** *Let $\varGamma = \mathrm{Im}(L)$ and consider a CSM of $\varGamma$, obtained from a rotation matrix $M \in \mathrm{SOC}(\varGamma) = \mathrm{SO}(3, K)$. Then, among the $\mathrm{SOC}(\varGamma)$-matrices that result in the same CSM, there is at least one of the form $R = R(q)$ with $q$ an $L$-reduced element of $L$.* □

Consider now a maximal order $\mathcal{O}$. Our next aim is to relate the conjugate orders $q\mathcal{O}q^{-1}$, which are all of the same type as $\mathcal{O}$, to ideals $q\mathcal{O}$ of $\mathcal{O}$. For this, we shall need to know something about the irreducible factors of elements of $\mathcal{O}$, and the following fact is sufficient for our purpose.

**Fact 9.** *Let $\mathbb{H}(K)$ have class number* 1*, and let $\mathcal{O}$ be a maximal order in $\mathbb{H}(K)$. If $q \in \mathcal{O}$ is primitive and $\pi \in \mathcal{o}$ is a prime factor of $|q|^2$, then $q$ can be factorized as $q = rp$, with $r, p \in \mathcal{O}$ and $|p|^2$ an associate of $\pi$.*

*Proof.* We translate the proof of [12, Ch. 5, Thm. 2] to this more general setting.

Since $\mathbb{H}(K)$ has class number 1, the left ideal $\mathcal{O}q + \mathcal{O}\pi$ has the form $\mathcal{O}p$ for some $p \in \mathcal{O}$ (the *greatest common right divisor* of $q$ and $\pi$, determined up to multiplication by a unit). So $q = rp$ and $\pi = sp$, for some $r, s \in \mathcal{O}$, and $\pi^2 = \mathrm{nr}(\pi) = |s|^2|p|^2$. Since $\pi$ is prime, $|p|^2$ must be an associate of 1, $\pi$ or $\pi^2$. However, $p$ is not a unit because $p = tq + u\pi$, for some $t, u \in \mathcal{O}$, so $\mathrm{nr}(p) = \mathrm{nr}(t)\,\mathrm{nr}(q) + \mathrm{nr}(u)\pi^2 + \pi\,\mathrm{tr}(tq\bar{u})$ is divisible by $\pi$. Also, if $|p|^2$ were an associate of $\pi^2$, then $s$ would be a unit, making $\pi$ an associate of $p$ and therefore a divisor of $q$, which is impossible since $q$ is primitive. Consequently, $|p|^2$ is an associate of $\pi$. □

We now embark on finding a correspondence between $q\mathcal{O}$ and $\mathrm{Im}(q\mathcal{O}q^{-1})$ when $q$ is reduced.

**Lemma 5.** *Let $\mathbb{H}(K)$ have class number* 1 *and let $\mathcal{O}$ be a maximal order. If $q, r \in \mathcal{O}$ are primitive, one has*

$$\mathrm{Im}(q\mathcal{O}) \subseteq \mathrm{Im}(r\mathcal{O}) \implies q\mathcal{O} \subseteq r\mathcal{O} \quad \textit{and} \quad q\mathcal{O} \subseteq r\mathcal{O} \implies \mathcal{O} \cap q\mathcal{O}q^{-1} \subseteq \mathcal{O} \cap r\mathcal{O}r^{-1}.$$

*Proof.* Since $\mathbb{H}(K)$ has class number 1, the right ideal $q\mathcal{O} + r\mathcal{O}$ has the form $d\mathcal{O}$ for some $d \in \mathcal{O}$ (the *greatest common left divisor* of $q$ and $r$). When $\mathrm{Im}(q\mathcal{O}) \subseteq \mathrm{Im}(r\mathcal{O})$, we have

$$\mathrm{Im}(d\mathcal{O}) \;=\; \mathrm{Im}(q\mathcal{O} + r\mathcal{O}) \;=\; \mathrm{Im}(q\mathcal{O}) + \mathrm{Im}(r\mathcal{O}) \;=\; \mathrm{Im}(r\mathcal{O}),$$

so, by Lemma 3 and recalling $|q|^2 = \mathrm{nr}(q)$,

$$\mathrm{nr}(d)\,\mathcal{o} \;=\; [\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(d\mathcal{O})]_K \;=\; [\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(r\mathcal{O})]_K \;=\; \mathrm{nr}(r)\,\mathcal{o},$$

since $d$ (being a left divisor of $r$) is primitive. Hence $\mathrm{nr}(r/d)$ is a unit in $\mathcal{o}$, so $r/d$ is a unit in $\mathcal{O}$ and $r\mathcal{O} = d\mathcal{O} \supseteq q\mathcal{O}$, establishing the first implication.

Now assume that $q\mathcal{O} \subseteq r\mathcal{O}$. Then $q = rp$ for some $p \in \mathcal{O}$. Given any $x \in \mathcal{O} \cap q\mathcal{O}q^{-1}$, put $y = r^{-1}xr$ and define

$$\mathrm{lden}(y) \;:=\; \{a \in \mathcal{O} \mid ay \in \mathcal{O}\}$$

(the *left denominator* of $y$). This is a left ideal of $\mathcal{O}$ and has the form $\mathcal{O}d$ for some $d \in \mathcal{O}$. Clearly, $\mathrm{lden}(y)$ contains $r$, but it also contains $\bar{p}$, as $y = pzp^{-1}$ for some $z \in \mathcal{O}$. Consequently, $r = sd$ and $\bar{p} = td$ with $s, t \in \mathcal{O}$, and hence $q = |d|^2 s\bar{t}$. Since $q$ is primitive, $|d|^2$ is a unit of $\mathcal{o}$ and hence $d$ is a unit of $\mathcal{O}$. Thus $\mathrm{lden}(y) = \mathcal{O}$, so $y \in \mathcal{O}$ and $x = ryr^{-1} \in \mathcal{O} \cap r\mathcal{O}r^{-1}$. This establishes the second implication. □

**Lemma 6.** *If $\mathbb{H}(K)$ has class number* 1*, $\mathcal{O}$ is a maximal order, and $q \in \mathcal{O}$ is reduced, then* $\mathrm{Im}(q\mathcal{O}) = \mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1})$.

We note that, except when $q$ is a unit, it is only the projections into $\mathbb{H}_-$ that are equal: $q\mathcal{O}$ and $\mathcal{O} \cap q\mathcal{O}q^{-1}$ themselves are distinct (because $1 \in q\mathcal{O}$ only for $q$ a unit).

*Proof.* We use induction on the absolute norm $\mathrm{N}\big(|q|^2\big)$. The result is certainly true when $\mathrm{N}\big(|q|^2\big) = 1$, since then $|q|^2$ is a unit in $\mathcal{o}$ so $q$ is a unit in $\mathcal{O}$ and $q\mathcal{O} = \mathcal{O} = \mathcal{O} \cap q\mathcal{O}q^{-1}$. When

$\mathrm{N}(|q|^2) > 1$, $|q|^2$ is divisible by some prime $\pi$ of $\mathcal{o}$, so $q = rp$ for some $r, p \in \mathcal{O}$ with $|p|^2$ an associate of $\pi$, by Fact 9. Moreover, $r$ and $p$ are reduced, because $q$ is. Now

$$q\mathcal{O} \subseteq \mathcal{O} \cap q\mathcal{O}q^{-1} \subseteq \mathcal{O} \cap r\mathcal{O}r^{-1}, \tag{15}$$

where the first inclusion is straightforward and the second is a consequence of Lemma 5. Also $p\mathcal{O}p^{-1} \neq \mathcal{O}$, since $p$ is reduced but not a unit, and hence $q\mathcal{O}q^{-1} \neq r\mathcal{O}r^{-1}$. But $\mathcal{O}$, $q\mathcal{O}q^{-1}$ and $r\mathcal{O}r^{-1}$ are maximal orders, so by Lemma 8 of the Appendix $\mathcal{O} \cap q\mathcal{O}q^{-1} \neq \mathcal{O} \cap r\mathcal{O}r^{-1}$ whence $[\mathcal{O} \cap r\mathcal{O}r^{-1} : \mathcal{O} \cap q\mathcal{O}q^{-1}]_K \neq \mathcal{o}$. On projecting into $\mathbb{H}_-$, (15) gives

$$\mathrm{Im}(q\mathcal{O}) \subseteq \mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1}) \subseteq \mathrm{Im}(\mathcal{O} \cap r\mathcal{O}r^{-1}) = \mathrm{Im}(r\mathcal{O}),$$

where the equation on the right is an application of the induction hypothesis since $r$ is reduced and

$$\mathrm{N}(|r|^2) = \mathrm{N}(|q|^2)/\,\mathrm{N}(|p|^2) < \mathrm{N}(|q|^2).$$

By Lemma 3 and the multiplicativity of $K$-indices, we have

$$[\mathrm{Im}(r\mathcal{O}) : \mathrm{Im}(q\mathcal{O})]_K = \frac{[\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(q\mathcal{O})]_K}{[\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(r\mathcal{O})]_K} = \frac{|q|^2}{|r|^2}\,\mathcal{o} = \pi\mathcal{o}\,,$$

a prime ideal of $\mathcal{o}$, but Fact 7 implies

$$[\mathrm{Im}(\mathcal{O} \cap r\mathcal{O}r^{-1}) : \mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1})]_K = [\mathcal{O} \cap r\mathcal{O}r^{-1} : \mathcal{O} \cap q\mathcal{O}q^{-1}]_K \neq \mathcal{o}\,.$$

Being a divisor of the prime ideal $\pi\mathcal{o}$, this index must therefore be $\pi\mathcal{o}$ itself and, again by the multiplicativity of $K$-indices, $[\mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1}) : \mathrm{Im}(q\mathcal{O})]_K = \mathcal{o}$. Hence $\mathrm{Im}(q\mathcal{O}) = \mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1})$, completing the induction. □

Summing up:

**Proposition 4.** *If $K$ and $\mathbb{H}(K)$ both have class number 1, if $\mathcal{O}$ is a maximal order of $\mathbb{H}(K)$, and if $q, r \in \mathcal{O}$ are $\mathcal{O}$-reduced, the following inclusions are equivalent:*

(i) $\mathrm{Im}(q\mathcal{O}) \subseteq \mathrm{Im}(r\mathcal{O})$;
(ii) $q\mathcal{O} \subseteq r\mathcal{O}$;
(iii) $\mathcal{O} \cap q\mathcal{O}q^{-1} \subseteq \mathcal{O} \cap r\mathcal{O}r^{-1}$;
(iv) $\mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1}) \subseteq \mathrm{Im}(\mathcal{O} \cap r\mathcal{O}r^{-1})$.

*Proof.* Lemma 5 gives (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii), the claim (iii) $\Rightarrow$ (iv) follows by projection into $\mathbb{H}_-$, and (iv) $\iff$ (i) by Lemma 6. □

As a matter of independent interest, we list the following consequences of Lemma 6.

**Proposition 5.** *Let $\mathbb{H}(K)$ be the standard quaternion algebra over the real algebraic number field $K$, and suppose that both $K$ and $\mathbb{H}(K)$ have class number 1. Let $\mathcal{O}$ be a maximal order of $\mathbb{H}(K)$ and $q \in \mathcal{O}$ an $\mathcal{O}$-reduced element. Then, one has the following relations:*

(i) $\mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1}) = \mathrm{Im}(q\mathcal{O}) = \mathrm{Im}(\mathcal{O}\bar{q})$;
(ii) $\mathcal{O} \cap q\mathcal{O}q^{-1} = \mathcal{o} + q\mathcal{O} + \mathcal{O}\bar{q} = \mathcal{o} + q\mathcal{O} = \mathcal{o} + \mathcal{O}\bar{q}$;
(iii) $[\mathcal{O} : \mathcal{O} \cap q\mathcal{O}q^{-1}] = [\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(\mathcal{O} \cap q\mathcal{O}q^{-1})] = \mathrm{N}(|q|^2)$;
(iv) $[\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(\mathcal{O}) \cap \mathrm{Im}(q\mathcal{O}q^{-1})] = \mathrm{N}(|q|^2)$;

(v) $[\mathcal{O}\cap q\mathcal{O}q^{-1} : q\mathcal{O}] \, = \, [\mathcal{o} + q\mathcal{O} : q\mathcal{O}] \, = \, [\mathcal{o} + \mathcal{O}\bar{q} : q\mathcal{O}] \, = \, \mathrm{N}\bigl(|q|^2\bigr).$

*Proof.* Part (i) follows from Lemma 6 together with the observation that $\mathrm{Im}(qx) = \mathrm{Im}(-\bar{x}\bar{q})$ when $x \in \mathcal{O}$. Part (ii) follows from the inclusions

$$\mathcal{o} + q\mathcal{O} \;\subseteq\; \mathcal{o} + q\mathcal{O} + \mathcal{O}\bar{q} \;\subseteq\; \mathcal{O}\cap q\mathcal{O}q^{-1}$$

and the fact that, by Propositions 2 and Lemma 6,

$$[\mathcal{O}\cap q\mathcal{O}q^{-1} : \mathcal{o} + q\mathcal{O}]_K \;=\; [\mathcal{o} : \mathcal{o}]_K \, [\mathrm{Im}(\mathcal{O}\cap q\mathcal{O}q^{-1}) : \mathrm{Im}(q\mathcal{O})]_K \;=\; \mathcal{o}.$$

For Part (iii), we note that

$$[\mathcal{O} : \mathcal{O}\cap q\mathcal{O}q^{-1}]_K \;=\; [\mathcal{o} : \mathcal{o}]_K \, [\mathrm{Im}(\mathcal{O}) : \mathrm{Im}(\mathcal{O}\cap q\mathcal{O}q^{-1})]_K,$$

by Proposition 2, and use Lemmas 6 and 3, and Fact 8. Part (iv) follows from Part (iii) and Lemma 4. Finally, Part (v) is a consequence of Parts (ii) and (iii), Lemma 1, the multiplicativity of $K$-indices and Fact 8. □

## 6. General results

We are finally in a position to state our main result on the connection between coincidence site modules and one-sided ideals.

**Theorem 1.** *Let $\mathbb{H}(K)$ be the standard quaternion algebra over the real algebraic number field $K$, and suppose that both $K$ and $\mathbb{H}(K)$ have class number* 1*. Let $\mathcal{O}$ be a maximal order of $\mathbb{H}(K)$. Then, the CSMs of $\varGamma := \mathrm{Im}(\mathcal{O})$ are in one-to-one correspondence with the one-sided ideals $q\mathcal{O}$ that are generated by the $\mathcal{O}$-reduced elements $q \in \mathcal{O}$. The corresponding coincidence indices are given by $\mathrm{N}(|q|^2)$, so that these right ideals are to be counted according to the square root of their ideal index from Proposition 3* (ii)*.*

*Proof.* Parts (ii) and (iv) of Proposition 4 provide the connection between the CSMs and the right ideals generated by $\mathcal{O}$-reduced elements of $\mathcal{O}$, and Proposition 3 (iii) gives the indices of the CSMs. □

This implies that we may count the CSMs by counting one-sided ideals in $\mathcal{O}$, which can be done by counting *all* ideals of a given index in $\mathcal{O}$ and subtracting off the two-sided ones. While the former is achieved by the zeta function $\zeta_{\mathcal{O}}(s)$, the latter is done by the zeta function of the base field, via $\zeta_K(4s)$, up to finitely many correction factors from ramified primes. The factor 4 in the argument of $\zeta_K$ stems from the index formula of Lemma 1. Let us introduce a Dirichlet series generating function for one-sided ideals that are generated by $\mathcal{O}$-reduced elements as $\zeta_{\mathcal{O}}^{\mathrm{red}}(s)$, and denote the Dirichlet series generating function for the two-sided ideals of $\mathcal{O}$ by $\zeta_{\mathcal{O}.\mathcal{O}}(s)$, see below for examples.

**Lemma 7.** *If $\mathcal{O}$ is a maximal order in the quaternion algebra $\mathbb{H}(K)$ of class number* 1*, one has the identity $\zeta_{\mathcal{O}}(s) = \zeta_{\mathcal{O}}^{\mathrm{red}}(s)\, \zeta_{\mathcal{O}.\mathcal{O}}(s)$.*

*Proof.* Due to the assumption on the class number, each right ideal is principal, and thus of the form $q\mathcal{O}$ for some $q \in \mathcal{O}$. If $q$ has any divisor that generates a two-sided ideal, we can pull that factor out to the right to obtain a unique factorization of $q\mathcal{O}$ into a reduced and a two-sided ideal. Consequently, sorted by their index, we can either count all right ideals together (giving the term on the left), or reduced right ideals and their possible right multiplication by two-sided ideals separately (giving the product of Dirichlet series on the right). □

Now, in view of Theorem 1, counting CSMs is the same as counting reduced right ideals, but with respect to the square root of the ideal index. This results in

**Theorem 2.** *Under the assumptions of Theorem 1, the Dirichlet series generating function* $\varPhi(s)$ *for the number* $f(m)$ *of CSMs of index* $m$ *of the* $\mathcal{O}$*-module* $\varGamma = \mathrm{Im}(\mathcal{O}) \subset \mathbb{R}^3$ *is given by*

$$\varPhi(s) \;=\; \sum_{m\geq 1} \frac{f(m)}{m^s} \;=\; \zeta_{\mathcal{O}}^{\mathrm{red}}(s/2) \;=\; \frac{\zeta_{\mathcal{O}}(s/2)}{\zeta_{\mathcal{O}.\mathcal{O}}(s/2)} \;=\; E(s)\, \frac{\zeta_K(s)\, \zeta_K(s-1)}{\zeta_K(2s)}\,,$$

*where* $\zeta_K(s)$ *is the Dedekind zeta function of the field* $K$ *and* $E(s)$ *is either* $1$ *or an additional analytic factor (with finitely many terms) that takes care of the extra contributions from ramified primes.*

*In particular, the arithmetic function* $f(m)$ *is multiplicative, and the elementary coincidence spectrum of* $\varGamma$ *is* $\varSigma(\mathrm{OC}(\varGamma)) = \varSigma(\mathrm{SOC}(\varGamma)) = \{m \in \mathbb{N} \mid f(m) \neq 0\}$.

*Proof.* The first claim follows from Theorem 1 together with Lemma 7. Since both zeta functions involved, $\zeta_{\mathcal{O}}(s)$ and $\zeta_{\mathcal{O}.\mathcal{O}}(s)$, possess an Euler product decomposition, this applies to $\varPhi(s)$ as well, with their detailed structure following from [23] and [20]. As a consequence, $f(m)$ must be a multiplicative arithmetic function. The claim about the spectrum is obvious. □

**Corollary 2.** *The asymptotic growth of the multiplicative arithmetic function* $f(m)$ *of Theorem 2 is given through its summatory function via*

$$F(x) \;:=\; \sum_{m\leq x} f(m) \;\sim\; \varrho\, \frac{x^2}{2}, \quad \text{as } x \to \infty, \quad \text{with } \varrho = \mathrm{res}_{s=2}\, \varPhi(s).$$

*In particular, the average size of* $f(m)$ *is* $\varrho m$.

*Proof.* Consider the function $\varPhi(s)$ from Theorem 2. By the general structure of the zeta functions involved and the fact that $E(s)$ is an entire function, $\varPhi(s)$ is analytic in the open half-plane $\{s = \sigma + it \mid \sigma > 2\}$, and has a first order pole at $s = 2$, but no other singularity on the line $\{\sigma = 2\}$. In fact, $\varPhi(s)$ is analytic everywhere on this line except at $s = 2$.

Delange's theorem, compare [4, Appendix] for a formulation tailored to this situation, now gives $F(x) \sim \varrho x^2/2$, as $x \to \infty$, with $\varrho$ as claimed. □

**Remark 3.** The residue in Corollary 2 can be calculated as

$$\mathrm{res}_{s=2}\, \varPhi(s) \;=\; \frac{E(2)\, \zeta_K(2)}{\zeta_K(4)}\, \mathrm{res}_{s=1}\, \zeta_K(s). \tag{16}$$

and $\mathrm{res}_{s=1}\, \zeta_K(s)$ can be expressed in terms of values of $L$-series.

## 7. Specific results

There are three explicit cases of particular interest for applications in crystallography, where the ring of integers $\mathcal{O}$ is a principal ideal domain (compare Table 1 on p. 422 of [9]) and the quaternion algebra $\mathbb{H}(K)$ has class number 1 (see [21] and the first table on p. 156 of [23]

| $K$ | $\mathbb{Q}$ | $\mathbb{Q}(\sqrt{5})$ | $\mathbb{Q}(\sqrt{2})$ |
|---|---|---|---|
| $\mathcal{O}$ | $\mathbb{J}$ | $\mathbb{I}$ | $\mathbb{K}$ |
| $\mathcal{o}$ | $\mathbb{Z}$ | $\mathbb{Z}[\tau]$ | $\mathbb{Z}[\sqrt{2}]$ |

TABLE 1. Data for three quaternion algebras $\mathbb{H}(K)$ of class number 1, with maximal order $\mathcal{O}$. Here, $\tau = (\sqrt{5}+1)/2$ is the golden ratio, and the ring of integers $\mathcal{o}$ is a PID in all three cases (see text for details).

for further examples). The basic information is summarized in Table 1. The corresponding zeta functions are the Dirichlet series generating functions for the right ideals,

$$\zeta_{\mathcal{O}}(s) \;=\; \sum_{0\neq\mathfrak{A}\subset\mathcal{O}} \frac{1}{[\mathcal{O}:\mathfrak{A}]^s} \;=\; \sum_{n\geq 1} \frac{f_{\mathcal{O}}(n)}{n^s}\,,$$

where $\mathfrak{A}$ runs through the non-zero right ideals of $\mathcal{O}$ and $f_{\mathcal{O}}(m)$ is the number of such ideals of index $m$. Due to the class number being 1, all ideals are principal, so we have $\mathfrak{A} = a\mathcal{O}$ for some $a \in \mathcal{O}^{\bullet}$, and then $[\mathcal{O} : a\mathcal{O}] = \mathrm{N}\big(|a|^4\big)$ by Proposition 3 (ii). The zeta function for the left ideals is the same, as left and right ideals are in a natural one-to-one relation that preserves the norm. Similarly, $\zeta_{\mathcal{O}.\mathcal{O}}(s)$ is defined as the Dirichlet series that runs over all non-zero two-sided ideals of $\mathcal{O}$, so that $\zeta_{\mathcal{O}.\mathcal{O}}(s) = \sum_{n\geq 1} \frac{f_{\mathcal{O}.\mathcal{O}}(n)}{n^s}$.

In all three cases of Table 1, these zeta functions can be expressed in terms of the Dedekind zeta functions of $K$ as follows, compare [23]:

$$\zeta_{\mathcal{O}}(s) \;=\; \zeta_K(2s)\,\zeta_K(2s-1)\cdot \begin{cases} (1-2^{1-2s}), & \text{if } K=\mathbb{Q}\,,\\ 1, & \text{otherwise,}\end{cases} \tag{17}$$

where the extra factor for $K = \mathbb{Q}$ results from the rational prime 2 being ramified in this case. The Dedekind zeta functions entering are given by

$$\begin{aligned} \zeta_{\mathbb{Q}}(s) &= \zeta(s) = \prod_{p\in\mathcal{P}} \frac{1}{1-p^{-s}}\,,\\ \zeta_{\mathbb{Q}(\sqrt{5})}(s) &= \frac{1}{1-5^{-s}} \prod_{p\equiv\pm 1\,(5)} \frac{1}{(1-p^{-s})^2} \prod_{p\equiv\pm 2\,(5)} \frac{1}{1-p^{-2s}}\,,\\ \zeta_{\mathbb{Q}(\sqrt{2})}(s) &= \frac{1}{1-2^{-s}} \prod_{p\equiv\pm 1\,(8)} \frac{1}{(1-p^{-s})^2} \prod_{p\equiv\pm 3\,(8)} \frac{1}{1-p^{-2s}}\,, \end{aligned} \tag{18}$$

see [4] for further details in this context, including explicit terms and asymptotic properties.

We shall also need the Dirichlet series generating functions for the two-sided ideals of $\mathcal{O}$. By the relation between prime ideals in $\mathcal{O}$ and $\mathcal{o}$ according to [20, Thm. 22.4], it can be expressed by the zeta function of the base field $K$, possibly up to finitely many correction factors for primes that ramify in the extension from $K$ to $\mathbb{H}(K)$. With the examples of Table 1, this happens only for $\mathbb{J}$, where $(1+\mathrm{i})\mathbb{J} = \mathbb{J}(1+\mathrm{i}) = \mathbb{J}(1+\mathrm{i})\mathbb{J}$ is the unique two-sided prime ideal over the rational prime 2. We know from Proposition 3 (ii) that $(1+\mathrm{i})\mathbb{J}$ has index 4 in $\mathbb{J}$, to be compared with index 16 for the ideal $2\mathbb{J}$. In all other cases, if $\mathfrak{P}$ is the unique two-sided prime ideal in $\mathcal{O}$ that lies over the prime ideal $\mathfrak{p} \in \mathcal{o}$, compare [20, Thm. 22.3], one has

$$[\mathcal{O} : \mathfrak{P}] \; = \; [\mathcal{o} : \mathfrak{p}]^4 .$$

Consequently, we obtain for our three examples of Table 1:

$$\zeta_{\mathcal{O}.\mathcal{O}}(s) \; = \; \zeta_K(4s) \cdot \begin{cases} (1+4^{-s}), & \text{if } K = \mathbb{Q}\,, \\ 1, & \text{otherwise.} \end{cases} \tag{19}$$

With these general preparations, we can now apply the results to the three cases of Table 1.

7.1. **The Hurwitz ring $\mathbb{J}$.** Here, we consider $\mathbb{H}(\mathbb{Q})$, with $\mathbb{J}$ as defined in Eq. (7). This is the unique maximal order that contains $\mathcal{L} \simeq \mathbb{Z}^4$ of (6), with $\mathcal{o} = \mathbb{Z}$ and $[\mathbb{J} : \mathcal{L}] = 2$. It is immediate that $\mathrm{Im}(\mathbb{J}) = \Gamma_{\mathrm{bcc}}$, so that we can re-derive the results from Section 2. The characterization of the $\mathbb{J}$-reduced elements of $\mathbb{J}$ follows from the detailed analysis in [15]:

**Fact 10.** *An element $q \in \mathbb{J}$ is $\mathbb{J}$-reduced if and only if $q$ is $\mathbb{J}$-primitive and $|q|^2$ is odd.* □

Theorem 2, applied to $\mathbb{J}$, reproduces all results of Section 2. In particular, we find

**Corollary 3.** *The elementary coincidence spectrum of the lattice $\Gamma_{\mathrm{bcc}} = \mathrm{Im}(\mathbb{J})$ is the set of odd integers. This set is a monoid, generated by the odd rational primes.* □

In view of Fact 10, one can also derive a simple formula for the index of a rotation matrix $R \in \mathrm{SOC}(\Gamma_{\mathrm{bcc}})$. If $R = R_q$ with $q \in \mathbb{J}$ being $\mathbb{J}$-reduced, one simply has $\Sigma_{\mathrm{bcc}}(R_q) = |q|^2$. Otherwise, replace $q$ by $q' = q/\mathrm{cont}_{\mathbb{J}}(q)$, which is $\mathbb{J}$-primitive. If $|q'|^2$ is odd, the quaternion $q'$ is already reduced. If not, one has $q' = q''(1+\mathrm{i})$ with $|q''|^2$ odd. In this case, since $1+\mathrm{i}$ generates a two-sided ideal, $R_{q''}$ defines the same CSL as $R_{q'}$. For a general $q \in \mathbb{J}$, we thus have

$$\Sigma_{\mathrm{bcc}}(R_q) \; = \; \big|q/\mathrm{cont}_{\mathbb{J}}(q)\big|^2 \cdot \begin{cases} 1, & \text{if } |q'|^2 \text{ is odd,} \\ \frac{1}{2}, & \text{otherwise.} \end{cases} \tag{20}$$

This formula is well known and has been derived before [13, 2] by different methods.

The dual lattice of $\Gamma_{\mathrm{bcc}}$ is the so-called face centred cubic lattice, conveniently written as

$$\Gamma_{\mathrm{fcc}} \; = \; \{(\ell, m, n)^t \in \mathbb{Z}^3 \mid \ell + m + n \;\text{ even}\} \; = \; (1+\mathrm{i})\mathbb{J} \cap \mathbb{H}_- \,.$$

It is a sublattice of $\mathbb{Z}^3$ of index 2. Clearly, due to commensurability, all three lattices share the same commensurator subgroup of $\mathrm{SO}(3,\mathbb{R})$, namely $\mathrm{SO}(3,\mathbb{Q})$. More generally, we have

**Theorem 3.** *Let $R \in \mathrm{SO}(3,\mathbb{Q})$. Then, the three cubic lattices in $\mathbb{R}^3$ share the same index formula, i.e., $\Sigma_{\mathrm{bcc}}(R) = \Sigma_{\mathrm{p}}(R) = \Sigma_{\mathrm{fcc}}(R)$. In particular, the coincidence spectrum for all three lattices is the set of odd integers, as given in Eq.* (1)*, and the Dirichlet series generating function for all three cubic lattices is $\Phi_{\mathrm{cub}}(s)$ of Eqs.* (2) *and* (3)*.*

*Proof.* By [2, Thm. 2.2], two mutually dual lattices share the same index formula, which then applies to $\varGamma_{\rm bcc}$ and $\varGamma_{\rm fcc}$. So, we have $\varSigma_{\rm bcc}(R) = \varSigma_{\rm fcc}(R) =: \varSigma(R)$.

Moreover, we have the inclusion

$$\varGamma_{\rm fcc} \overset{2}{\subset} \mathbb{Z}^3 \overset{2}{\subset} \varGamma_{\rm bcc}\,.$$

By [2, Lemma 2.6], this relation implies $\varSigma_{\rm p}(R) \mid 2\varSigma(R)$ and $\varSigma(R) \mid 2\varSigma_{\rm p}(R)$, which tells us that the coincidence index for $\mathbb{Z}^3$ could only differ from $\varSigma(R)$ by a factor of 2.

From our previous arguments, we know that $\varSigma(R)$ is always odd, so that $\varSigma(R) \mid \varSigma_{\rm p}(R)$ On the other hand, also the index $\varSigma_{\rm p}(R)$ is always odd, see [13, 2], which emerges from an independent argument directly on the basis of the rotation matrix $R$. Consequently, we must have $\varSigma_{\rm p}(R) \mid \varSigma(R)$, which gives $\varSigma_{\rm p}(R) = \varSigma(R)$. □

**Remark 4.** Observing that the lattice $\mathbb{Z}^3$ is isomorphic with $\mathbb{J} \cap \mathbb{H}_-$, the index relation $\varSigma_{\rm p}(R) = \varSigma(R)$ in the previous proof can also be derived with an independent argument based upon Fact 6 and an index formula for intersections with $\mathbb{H}_-$, see [6] for more.

Also of interest is the analysis of multiple intersections. Unfortunately, the relation to the arithmetic of $\mathbb{J}$ becomes considerably more involved. First explicit results are available [26, 27], including the observation that the total coincidence spectrum is identical to the elementary one. For a given index, new CSLs appear, but all possibilities are exhausted with triple intersections.

7.2. **The icosian ring $\mathbb{I}$.** Here, we consider $\mathbb{H}\big(\mathbb{Q}(\sqrt{5}\,)\big)$. In this case, there are two maximal orders that contain $\mathcal{L}$ of (6), with $\mathcal{O} = \mathbb{Z}[\tau]$. One choice is

$$\mathbb{I} \;:=\; \big\langle (1,0,0,0), (0,1,0,0), \tfrac{1}{2}(1,1,1,1), \tfrac{1}{2}(1-\tau,\tau,0,1)\big\rangle_{\mathbb{Z}[\tau]}\,,$$

where $\tau = (\sqrt{5}+1)/2$ is the golden ratio. The other choice is $\mathbb{I}'$, where $'$ denotes the algebraic conjugation of $\mathbb{Q}(\sqrt{5}\,)$, defined by $\sqrt{5} \mapsto -\sqrt{5}$. Both have been called the *icosian ring*, see [10, 4, 11] for details on the connection to the root system of type $H_4$. Our choice here matches that of [10, 11], while the roles of $\mathbb{I}$ and $\mathbb{I}'$ are interchanged in comparison to [2, 4]. It is not difficult to check that $\mathcal{L}$ of (6) is an index 16 submodule both of $\mathbb{I}$ and $\mathbb{I}'$. Moreover, one has the relation

$$2(\mathbb{I}+\mathbb{I}') \overset{4}{\subset} \mathcal{L} \overset{4}{\subset} \mathbb{I}\cap\mathbb{I}',$$

where $\mathbb{I}\cap\mathbb{I}' = \mathbb{J}[\tau] := \mathbb{J} + \tau\mathbb{J}$ provides a connection to the Hurwitz ring. Let us mention that, in the icosian case, $2\mathbb{I}$ is the unique prime ideal over $2 \in \mathbb{Z}[\tau]$, and that $(1+\mathrm{i})\mathbb{I} = \mathbb{I}'(1+\mathrm{i})$, so that $(1+\mathrm{i})\mathbb{I}$ is a one-sided, but not a two-sided ideal. This also shows that $\mathbb{I}$ and $\mathbb{I}'$ are related by an inner automorphism, and hence are of the same type, in line with Fact 5. Unlike in the case of the Hurwitz ring, the rational prime 2, which is also a prime of $\mathbb{Z}[\tau]$, does not ramify. More generally, no prime of $\mathbb{Z}[\tau]$ ramifies in the extension step to $\mathbb{I}$. Consequently, one has

**Fact 11.** *An element $q \in \mathbb{I}$ is $\mathbb{I}$-reduced if and only if it is $\mathbb{I}$-primitive.* □

With this definition, the imaginary part satisfies $\mathrm{Im}(\mathbb{I}) = \frac{1}{2}\mathcal{M}_{\mathrm{B}}$, where

$$\begin{aligned} \mathcal{M}_{\mathrm{B}} \; &= \; \bigl\{ \textstyle\sum_{i=1}^{3} \alpha_i e_i \mid \alpha_i \in \mathbb{Z}[\tau], \text{ with } \tau^2\alpha_1 + \tau\alpha_2 + \alpha_3 \equiv 0 \ (\mathrm{mod}\ 2) \bigr\} \\ &= \; \bigl\langle (2,0,0)^t, (1,1,1)^t, (\tau,0,1)^t \bigr\rangle_{\mathbb{Z}[\tau]} \; \subset \; \mathbb{R}^3 \end{aligned}$$

is the standard body centred icosahedral module of quasi-crystallography, see [2] and references therein. Furthermore, $\mathbb{I} \cap \mathbb{H}_- \simeq \mathrm{Im}(\mathbb{I} \cap \mathbb{H}_-) = \frac{1}{2}\mathcal{M}_{\mathrm{F}}$, where

$$\begin{aligned} \mathcal{M}_{\mathrm{F}} \; &= \; \bigl\{ \textstyle\sum_{i=1}^{3} \alpha_i e_i \mid \alpha_i \in \mathbb{Z}[\tau], \text{ with } \alpha_1 \equiv \tau\alpha_2 \equiv \tau^2\alpha_3 \ (\mathrm{mod}\ 2) \bigr\} \\ &= \; \bigl\{ \textstyle\sum_{i=1}^{3} \alpha_i e_i \in \mathcal{M}_{\mathrm{B}} \mid \alpha_1 + \alpha_2 + \alpha_3 \equiv 0 \ (\mathrm{mod}\ 2) \bigr\} \\ &= \; \bigl\langle (2,0,0)^t, (\tau{+}1,\tau,1)^t, (0,0,2)^t \bigr\rangle_{\mathbb{Z}[\tau]} \; \overset{4}{\subset} \; \mathcal{M}_{\mathrm{B}} \; \subset \; \mathbb{R}^3 \end{aligned}$$

is the standard face centred icosahedral module. Both $\mathcal{M}_{\mathrm{B}}$ and $\mathcal{M}_{\mathrm{F}}$ are free $\mathbb{Z}[\tau]$-modules of rank 3, and free $\mathbb{Z}$-modules of rank 6. One quickly checks that

$$[\mathrm{Im}(\mathbb{I}) : \mathrm{Im}(\mathcal{L})] \; = \; [\mathbb{I} : \mathcal{L}] \; = \; 16\,,$$

in line with Fact 7. Note that $\mathrm{Im}(\mathbb{I})$ can be obtained as the projection of the weight lattice $D_6^*$ into a 3-dimensional subspace that is invariant under the symmetry group of the icosahedron. This also relates $\mathcal{M}_{\mathrm{B}}$ to a lattice in 6-space, which is complemented by the corresponding relation between $\mathcal{M}_{\mathrm{F}}$ and the root lattice $D_6$, see [2] for details.

An application of Theorem 2 to $\mathbb{I}$ gives the generating function

$$\begin{aligned} \Phi_{\mathrm{ico}}(s) \; &= \; \frac{1+5^{-s}}{1-5^{1-s}} \prod_{p \equiv \pm 1\ (5)} \left( \frac{1+p^{-s}}{1-p^{1-s}} \right)^2 \prod_{p \equiv \pm 2\ (5)} \frac{1+p^{-2s}}{1-p^{2(1-s)}} \\ &= \; 1 + \frac{5}{4^s} + \frac{6}{5^s} + \frac{10}{9^s} + \frac{24}{11^s} + \frac{20}{16^s} + \frac{40}{19^s} + \frac{30}{20^s} + \frac{30}{25^s} + \frac{60}{29^s} + \dots \end{aligned} \tag{21}$$

**Remark 5.** The generating function $\Phi_{\mathrm{ico}}(s)$ applies to both $\mathcal{M}_{\mathrm{B}}$ and $\mathcal{M}_{\mathrm{F}}$, as well as to any image of either under a linear similarity. The relation between $\mathcal{M}_{\mathrm{B}}$ and $\mathcal{M}_{\mathrm{F}}$ can be understood from the point of view of mutually dual embeddings as lattices into 6-space mentioned before, compare [2].

The asymptotic growth constant $\varrho$ of Corollary 2 takes the form

$$\varrho \; = \; \mathrm{res}_{s=2}\, \Phi_{\mathrm{ico}}(s) \; = \; \frac{45\sqrt{5}\log(\tau)}{\pi^4} \; \simeq \; 0.497\,089\,,$$

and $\varrho m$ is the average size of the arithmetic function $f(m)$; details of the calculation follow from [4, Appendix].

The index of a matrix $R \in \mathrm{SOC}(\mathcal{M}_{\mathrm{B}})$, written as $R = R_q$ with $q \in \mathbb{I}^{\bullet}$, is given by

$$\Sigma(R_q) \; = \; \mathrm{N}\bigl(|q/\mathrm{cont}_{\mathbb{I}}(q)|^2\bigr). \tag{22}$$

It is thus of the form $\mathrm{N}(k + \ell\tau) = k^2 + k\ell - \ell^2$ with $k, \ell \in \mathbb{Z}$. Since each prime $\pi \in \mathbb{Z}[\tau]$ has a decomposition $\pi = p\bar{p}$ in $\mathbb{I}$, one sees that all indices of this form indeed occur.

**Corollary 4.** *The* $\mathbb{Z}[\tau]$*-modules* $\mathcal{M}_{\rm B}$ *and* $\mathcal{M}_{\rm F}$ *have the* SOC*-group* $\mathrm{SO}(3,\mathbb{Q}(\sqrt{5}\,))$ *and share the elementary coincidence spectrum*

$$\begin{aligned}\varSigma\bigl(\mathrm{SO}(3,\mathbb{Q}(\sqrt{5}\,))\bigr) \;&=\; \{m\in\mathbb{N}\mid m=k^2+k\ell-\ell^2\,,\ \textit{with}\ k,\ell\in\mathbb{Z}\}\\ &=\; \{1,4,5,9,11,16,19,20,25,\dots\}\,.\end{aligned}$$

*This spectrum is a monoid and consists of all natural numbers that have all primes congruent to* $\pm 2$ *(mod* 5*) in their factorizations occuring with an even power.*

*Proof.* The claim on $\mathcal{M}_{\rm B}$ is clear by Theorem 2, as is the characterization of the natural numbers representable by the quadratic form $k^2+k\ell-\ell^2$, compare [14].

The SOC-group of $\mathcal{M}_{\rm F}$ is the same because the two modules are commensurate. Also, the index formula is the same because the modules $\mathcal{M}_F$ and $\mathcal{M}_B$ are dual to one another via the embedding into 6-space (as $D_6$ and $D_6^*$, respectively). Consequently, one can use the result from [2] that they share the index formula, thus giving equal spectra. □

A related object of interest is $\mathbb{Z}[\tau]^3 = \mathrm{Im}(\mathcal{L})$, which is a submodule of $\mathrm{Im}(\mathbb{I})$ of index 16 and hence commensurate. Clearly, $\mathrm{OC}\bigl(\mathrm{Im}(\mathcal{L})\bigr) = \mathrm{OC}\bigl(\mathrm{Im}(\mathcal{O})\bigr)$, and they also share the elementary coincidence spectrum [2], though a given index may arise from different sets of rotations. Consequently, one gets different Dirichlet series, too, see [2, Sec. 5.3] for details.

7.3. **The octahedral (or cubian) ring** $\mathbb{K}$**.** Here, we consider $\mathbb{H}\bigl(\mathbb{Q}(\sqrt{2}\,)\bigr)$, with maximal order

$$\mathbb{K} \;:=\; \bigl\langle 1, \tfrac{1+\mathrm{i}}{\sqrt{2}}, \tfrac{1+\mathrm{j}}{\sqrt{2}}, \tfrac{1+\mathrm{i}+\mathrm{j}+\mathrm{k}}{2}\bigr\rangle_{\mathbb{Z}[\sqrt{2}]}\,,$$

see [4] for a more detailed description. Note that $\mathbb{K}$ contains $\mathcal{L}$ of (6), with $\mathcal{O}=\mathbb{Z}[\sqrt{2}\,]$, as an index 16 submodule and that $\mathbb{K}$ is the only maximal order to contain $\mathcal{L}$. In this case, the imaginary part is

$$\mathrm{Im}(\mathbb{K}) \;=\; \tfrac{1}{\sqrt{2}}\bigl\langle (1,0,0)^t, (0,1,0)^t, \tfrac{1}{\sqrt{2}}(1,1,1)^t\bigr\rangle_{\mathbb{Z}[\sqrt{2}]}\,,$$

so that $[\mathrm{Im}(\mathbb{K}):\mathrm{Im}(\mathcal{L})] = [\mathbb{K}:\mathcal{L}] = 16$, in line with Fact 7. In the case of $\mathbb{K}$, the rational prime 2 ramifies in the extension from $\mathbb{Z}$ to $\mathbb{Z}[\sqrt{2}\,]$, but $\sqrt{2}$ does not ramify in the following extension to $\mathbb{K}$. As no other prime ramifies, one finds

**Fact 12.** *An element* $q\in\mathbb{K}$ *is* $\mathbb{K}$*-reduced if and only if it is* $\mathbb{K}$*-primitive.* □

This time, an application of Theorem 2 gives

$$\begin{aligned}\varPhi_{\rm oct}(s) \;&=\; \frac{1+2^{-s}}{1-2^{1-s}} \prod_{p\equiv\pm1\,(8)} \left(\frac{1+p^{-s}}{1-p^{1-s}}\right)^2 \prod_{p\equiv\pm3\,(8)} \frac{1+p^{-2s}}{1-p^{2(1-s)}}\\ &=\; 1+\frac{3}{2^s}+\frac{6}{4^s}+\frac{16}{7^s}+\frac{12}{8^s}+\frac{10}{9^s}+\frac{48}{14^s}+\frac{24}{16^s}+\frac{36}{17^s}+\frac{30}{18^s}+\dots\end{aligned}\tag{23}$$

Here, the asymptotic growth constant $\varrho$ of Corollary 2 reads

$$\varrho \;=\; \mathrm{res}_{s=2}\,\varPhi_{\rm oct}(s) \;=\; \frac{720\sqrt{2}\log(1+\sqrt{2}\,)}{11\,\pi^4} \;\simeq\; 0.837\,559\,,$$

with $\varrho m$ again being the average size of $f(m)$.

The index of a matrix $R = R_q$ with $q \in \mathbb{K}$ is given by

$$\Sigma(R_q) \;=\; \mathrm{N}\big(|q/\mathrm{cont}_{\mathbb{K}}(q)|^2\big). \tag{24}$$

It is thus of the form $\mathrm{N}\big(k+\ell\sqrt{2}\big) = k^2 - 2\ell^2$ with $k,\ell \in \mathbb{Z}$. Since each prime $\pi \in \mathbb{Z}[\sqrt{2}\,]$ has a decomposition $\pi = p\bar{p}$ in $\mathbb{K}$, one sees that all indices of this form indeed occur. This gives

**Corollary 5.** *The elementary coincidence spectrum of the* $\mathbb{Z}[\sqrt{2}\,]$*-module* $\mathrm{Im}(\mathbb{K})$ *is*

$$\begin{aligned}\Sigma\big(\mathrm{SO}(3,\mathbb{Q}\,(\sqrt{2}\,))\big) \;&=\; \{m \in \mathbb{N} \mid m = k^2 - 2\ell^2\,,\ \textit{with } k,\ell \in \mathbb{Z}\} \\ &=\; \{1,2,4,7,8,9,14,16,17,18,23,25,\dots\}\,.\end{aligned}$$

*The spectrum is a monoid and consists of all natural numbers that have all primes congruent to* $\pm 3$ *(mod* $8$*) in their factorizations occuring with an even power.* □

A related module in 3-space is $\mathbb{Z}[\sqrt{2}\,]^3$, realized as $\mathrm{Im}(\mathcal{L})$ with the order $\mathcal{L}$ of (6). The treatment of this module parallels the situation already met with the icosian ring, see above.

## 8. Extensions and outlook

The picture for the coincidence site modules in 3-space that emerge from single intersections seems to be rather clear now. Still, there are several important questions that have not been addressed here at all. First of all, having counted the CSMs, one would like to have a finer classification into Bravais types. Some results in this direction, for the cubic lattices, are presented in [25]. Then, there is no compelling reason to stop at single intersections, and recent developments make an extension to multiple coincidence site modules desirable. While this is rather well understood in the planar case [3], by algebraic means based upon the arithmetic of cyclotomic fields, only first steps exist in 3-space, see [26, 27] for some results.

As we briefly mentioned in passing, several of our above findings can be generalized beyond the class number 1 situation, and we hope to report on that soon [6]. Quaternions are certainly also helpful in 4-space, and further progress in this direction is in sight [7], at least for simple coincidences. More complicated, however, seems the situation in higher dimensions, even for the class of root lattices, and that might be a good problem to solve.

## Appendix

In the proof of Lemma 6, we needed a global version of a uniqueness result on intersecting maximal orders in quaternion division algebras, which is to some extent implicit in [20, 23], but which we could not find in explicit form and which does not seem to have an analogue in the more general context of central simple algebras [20, 24]. For completeness, we sketch here a localization argument for this [22, 24] that was communicated to us by U. Staemmler. For comparison with other work, we recall that the intersection of two (not necessarily distinct) maximal orders is called an *Eichler order*.

**Lemma 8.** [22] *Let* $\mathbb{H}(K)$ *be the quaternion division algebra over the real algebraic number field* $K$*, and let* $M$*,* $N$ *and* $O$ *be three maximal orders of* $\mathbb{H}(K)$ *that satisfy* $O \cap M = O \cap N$*. Then* $M = N$*.*

*Proof.* We write $H = \mathbb{H}(K)$ for this proof. One has $M = N$ if and only if all local completions of $M$ and $N$ at prime ideals $\mathfrak{p}$ of $K$ are equal, i.e., $M_{\mathfrak{p}} = N_{\mathfrak{p}}$, see [23, Prop. III.5.1] and [20, Sec. 3] for details in the present setting. Note that $E := O \cap M = O \cap N$ is an Eichler order. Local completion preserves intersections and the property of being a maximal order, see [23, p. 84]. In particular, $E_{\mathfrak{p}} = O_{\mathfrak{p}} \cap M_{\mathfrak{p}} = O_{\mathfrak{p}} \cap N_{\mathfrak{p}}$ remains an Eichler order in $H_{\mathfrak{p}}$.

Either $H_{\mathfrak{p}}$ is a skew field (when $\mathfrak{p}$ divides the discriminant of $H$ over $K$) or else it is isomorphic to the matrix ring $\mathrm{Mat}(2, K_{\mathfrak{p}})$ by Wedderburn's theorem, see [17, Sec. 52]. In the latter case, $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ by [23, Lemme II.2.4], which states that Eichler orders uniquely specify the two intersecting maximal orders here. In the former case, $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ because $H_{\mathfrak{p}}$ has a unique maximal order by [23, Lemme II.1.5]. So, $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ and hence $M = N$. □

Note that this proof actually shows a slightly stronger statement: if $L, M, N, O$ are maximal orders with $L \cap M = N \cap O$, one has $\{L, M\} = \{N, O\}$. But the lemma as stated is enough for our purposes.

## Acknowledgements

It is a pleasure to express our gratitude to Ute Staemmler, Alfred Weiss and Peter Zeiner for their cooperation and for useful hints on the manuscript. Interesting discussions with Herbert Abels, Robert V. Moody and Claus-Michael Ringel are gratefully acknowledged. M. B. would like to thank the University of Queensland for support in form of a Raybould Visiting Fellowship and the Department of Mathematics for hospitality, where a substantial part of this work was done. It was also supported by the German Research Council (DFG), within the CRC 701.

## References

[1] W. A. Adkins and S. H. Weintraub, *Algebra – An Approach via Module Theory*, corr. 2nd printing, Springer, New York (1999).

[2] M. Baake, Solution of the coincidence problem in dimensions $d \leq 4$, in: *The Mathematics of Long-Range Aperiodic Order*, ed. R.V. Moody, NATO-ASI Series C489, Kluwer, Dordrecht (1997), pp. 9–44; rev. version, `math.MG/0605222`.

[3] M. Baake and U. Grimm, Multiple planar coincidences with $N$-fold symmetry, *Z. Kristallogr.* **221** (2006) 571–581; `math.MG/0511306`.

[4] M. Baake and R. V. Moody, Similarity submodules and root systems in four dimensions, *Can. J. Math.* **51** (1999) 1258–1276; `math.MG/9904028`.

[5] M. Baake and P. A. B. Pleasants, Algebraic solution of the coincidence problem in two and three dimensions, *Z. Naturforschung* **50a** (1995) 711–717.

[6] M. Baake and P. A. B. Pleasants, in preparation.

[7] M. Baake and P. Zeiner, in preparation.

[8] W. Bollmann, *Crystal Defects and Crystalline Interfaces*, Springer, Berlin (1970).

[9] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York (1966).

[10] L. Chen, R. V. Moody and J. Patera, Non-crystallographic root systems, in: *Quasicrystals and Discrete Geometry*, ed. J. Patera, Fields Institute Monographs, vol. 10, AMS, Providence, RI (1998), pp. 135–178.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer, New York (1999).

[12] J. H. Conway and D. A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A. K. Peters, Natick, MA (2003).

[13] H. Grimmer, Coincidence rotations for cubic lattices, *Scripta Met.* **7** (1973) 1295–1300.

[14] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford (1979).

[15] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Springer, Berlin (1919).

[16] M. Koecher and R. Remmert, Hamilton's quaternions, in: *Numbers*, eds. H.-D. Ebbinghaus et al., Springer (1991), pp. 189–220.

[17] O. T. O'Meara, *Introduction to Quadratic Forms*, 3rd corr. printing, Springer, Berlin (1973).

[18] P. A. B. Pleasants, The construction of quasicrystals with arbitrary symmetry group, in: *Proceedings of the* 5*th International Conference on Quasicrystals* (*Avignon, 1995*), eds. C. Janot and R. Mosseri, World Scientific, Singapore (1995), pp. 22–30.

[19] P. A. B. Pleasants, M. Baake and J. Roth, Planar coincidences for $N$-fold symmetry, *J. Math. Phys.* **37** (1996) 1029–1058; corr. version, `math.MG/0511147`.

[20] I. Reiner, *Maximal Orders*, reprint, Clarendon Press, Oxford (2003).

[21] U. Staemmler, *Idealklassenzahlen von Quaternionenalgebren über algebraischen Zahlkörpern*, Diploma thesis, Univ. des Saarlandes, Saarbrücken (2002).

[22] U. Staemmler, private communication (2006).

[23] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, LNM 800, Springer, Berlin (1980).

[24] A. Weiss, private communication (2006).

[25] P. Zeiner, Symmetries of coincidence site lattices of cubic lattices, *Z. Kristallogr.* **220** (2005) 915–925; `math.MG/0605525`.

[26] P. Zeiner, Multiple CSLs for the body centred cubic lattice, in: *Proceedings SSPCM*, (in press); `math.MG/0605521`.

[27] P. Zeiner, Multiple CSLs for cubic lattices, preprint (2006).

Fakultät für Mathematik, Univ. Bielefeld, Box 100131, 33501 Bielefeld, Germany
*E-mail address*: `mbaake@math.uni-bielefeld.de`
*URL*: `http://www.math.uni-bielefeld.de/baake/`

Department of Mathematics, University of Queensland, Brisbane, QLD 4072, Australia
*E-mail address*: `pabp@maths.uq.edu.au`
*URL*: `http://www.maths.uq.edu.au/`

Fakultät für Mathematik, Univ. Bielefeld, Box 100131, 33501 Bielefeld, Germany
*E-mail address*: `rehmann@math.uni-bielefeld.de`
*URL*: `http://www.math.uni-bielefeld.de/rehmann/`