Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Algebra 320 (2008) 1391–1408

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Similar sublattices of the root lattice A_4

Michael Baake [a,*], Manuela Heuer [b], Robert V. Moody [c]

[a] *Fakultät für Mathematik, Universität Bielefeld, Box 100131, 33501 Bielefeld, Germany*
[b] *Department of Mathematics and Statistics, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK*
[c] *Department of Mathematics and Statistics, University of Victoria, Victoria, British Columbia, V8W 3P4, Canada*

Received 15 February 2007

Available online 9 June 2008

Communicated by Efim Zelmanov

Abstract

Similar sublattices of the root lattice A_4 are possible [J.H. Conway, E.M. Rains, N.J.A. Sloane, On the existence of similar sublattices, Can. J. Math. 51 (1999) 1300–1306] for each index that is the square of a non-zero integer of the form $m^2 + mn - n^2$. Here, we add a constructive approach, based on the arithmetic of the quaternion algebra $\mathbb{H}(\mathbb{Q}(\sqrt{5}))$ and the existence of a particular involution of the second kind, which also provides the actual sublattices and the number of different solutions for a given index. The corresponding Dirichlet series generating function is closely related to the zeta function of the icosian ring.

Keywords: Similar sublattices; Icosian ring; Zeta function

1. Introduction

Any lattice Γ in Euclidean space $\mathbb{R}^d$ possesses sublattices that are images of Γ under a non-zero similarity, i.e., under a linear map S of $\mathbb{R}^d$ with $\langle Su|Sv\rangle = c\langle u|v\rangle$ for all $u, v \in \mathbb{R}^d$, where $c > 0$ and $\langle .|.\rangle$ denotes the standard Euclidean scalar product. If $\Gamma' = S\Gamma \subset \Gamma$, Γ' is a *similar sublattice* (or similarity sublattice, SSL) of Γ, with index $[\Gamma : \Gamma'] = c^{d/2}$. If the lattice Γ has a rich point symmetry structure, there are usually interesting SSLs, beyond the trivial ones of the form $m\Gamma$ with $m \in \mathbb{N}$. Several examples have been investigated in the past, compare

* Corresponding author.
E-mail addresses: mbaake@math.uni-bielefeld.de (M. Baake), m.heuer@open.ac.uk (M. Heuer), rmoody@uvic.ca (R.V. Moody).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2008.04.021

[2–4,9] and references given there. Of particular interest are root lattices, due to their interesting geometry and their abundance in mathematics and its applications. In [9], the possible values of c were classified for many root lattices, while more complete information in terms of generating functions is available in dimension $d \leqslant 4$, see [3,4].

One important example that has not yet been solved completely is the root lattice A_4. It is the purpose of this article to close this gap. After a short summary of a more general nature, we review the mathematical setting in 4-space via quaternions. This permits the solution of the problem in Section 4, using the arithmetic of a maximal order of the division algebra $\mathbb{H}(\mathbb{Q}(\sqrt{5}))$. Related results will briefly be summarized afterwards, followed by some details on the underlying algebraic structure that we found along the way.

2. Generalities

A lattice Γ in Euclidean space $\mathbb{R}^d$ is a free $\mathbb{Z}$-module of rank d whose $\mathbb{R}$-span is all of $\mathbb{R}^d$. Two lattices in $\mathbb{R}^d$ are called *similar* if they are related by a non-zero similarity. For a given lattice $\Gamma \subset \mathbb{R}^d$, the similar sublattices (SSLs) form an important class, and one is interested in the possible indices and the arithmetic function $g_\Gamma(m)$ that counts the distinct SSLs of index m. Clearly, $g_\Gamma(1) = 1$. One can show [12] that $g_\Gamma(m)$ is super-multiplicative, i.e., $g_\Gamma(mn) \geqslant g_\Gamma(m) g_\Gamma(n)$ for coprime m, n. It is not always multiplicative, as one can see from considering suitable rectangular lattices in the plane [22], such as the one spanned by $(2,0)$ and $(0,3)$. However, in many relevant cases, and in all cases that will appear below, $g_\Gamma(m)$ is multiplicative. This motivates the use of a Dirichlet series generating function for it,

$$D_\Gamma(s) := \sum_{m=1}^{\infty} \frac{g_\Gamma(m)}{m^s}, \tag{1}$$

which will then have an Euler product expansion as well.

If Γ is a generic lattice in $\mathbb{R}^d$, the only SSLs of Γ will be its integrally scaled versions, i.e., the sublattices of the form $m\Gamma$ with $m \in \mathbb{N}$. In this case, as $m\Gamma$ has index m^d in Γ, the generating function simply reads

$$D_\Gamma(s) = \zeta(ds), \tag{2}$$

where $\zeta(s)$ is Riemann's zeta function. If SSLs other than those of the form $m\Gamma$ exist, each of them can again be scaled by an arbitrary natural number, so that

$$D_\Gamma(s) = \zeta(ds) D_\Gamma^{\mathsf{pr}}(s), \tag{3}$$

where $D_\Gamma^{\mathsf{pr}}(s)$ is the Dirichlet series generating function for the *primitive* SSLs of Γ (we shall define this in more detail below).

Let us first summarize some general properties of the generating functions in this context. The following statement follows from a simple conjugation argument.

Fact 1. *If Γ and Λ are similar lattices in $\mathbb{R}^d$, one has $D_\Gamma(s) = D_\Lambda(s)$.* $\square$

Given a lattice $\Gamma \subset \mathbb{R}^d$, its *dual* lattice Γ^* is defined as

$$\Gamma^* := \{ x \in \mathbb{R}^d \mid \langle x | y \rangle \in \mathbb{Z} \text{ for all } y \in \Gamma \}. \tag{4}$$

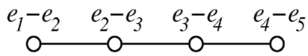

Fig. 1. Standard basis representation of the root lattice A_4.

Fact 2. *If Γ is a lattice in $\mathbb{R}^d$, one has $D_\Gamma(s) = D_{\Gamma^*}(s)$.*

Proof. If S is any (non-zero) linear similarity in $\mathbb{R}^d$, one has

$$S\Gamma \subset \Gamma \quad \Longleftrightarrow \quad S^t\Gamma^* \subset \Gamma^*,$$

which, in view of (4), is immediate from the relation $\langle x|Sy\rangle = \langle S^t x|y\rangle$.

Observing $\det(S) = \det(S^t)$, one thus obtains an index preserving bijection between the SSLs of Γ and those of Γ^*, whence we have $g_\Gamma(m) = g_{\Gamma^*}(m)$ for all $m \in \mathbb{N}$. This gives $D_\Gamma(s) = D_{\Gamma^*}(s)$. □

Remark 1. Defining the transposed similarity via the scalar product makes it transparent that there is a certain scaling degree of freedom to choose the non-degenerate bilinear form without changing the result of Fact 2, which is in line with Fact 1.

3. Mathematical setting in 4-space

As is apparent from the treatment in [9], the usual description of A_4 as a lattice in a 4-dimensional hyperplane of $\mathbb{R}^5$, see Fig. 1, gives access to the possible values of c, and hence to the possible indices, but not necessarily to the actual similarities and the SSLs. Therefore, we use a description in $\mathbb{R}^4$ instead, which will enable us to use quaternions, based on the inclusion of a root system of type A_4 within one of type H_4, see [18, Prop. 2] or [8, Thm. 4.1]. In particular, we shall need the Hamiltonian quaternion algebras $\mathbb{H}(\mathbb{R})$, $\mathbb{H}(\mathbb{Q})$ and $\mathbb{H}(K)$, with the quadratic field $K = \mathbb{Q}(\sqrt{5})$, generated by the basis quaternions $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$. The latter observe Hamilton's relations

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1$$

and will be identified with the canonical Euclidean basis in 4-space. Quaternions are thus also written as vectors, $x = (x_0, x_1, x_2, x_3)$, and the algebra is equipped with the usual conjugation $x \mapsto \bar{x}$, where $\bar{x} = (x_0, -x_1, -x_2, -x_3)$. For later use, we also introduce the reduced trace $\mathrm{tr}(x)$ and the reduced norm $\mathrm{nr}(x)$ in a quaternion algebra via

$$\mathrm{tr}(x) := x + \bar{x}, \qquad \mathrm{nr}(x) := x\bar{x} = |x|^2.$$

If we work over the field $K = \mathbb{Q}(\sqrt{5})$, we shall also need its trace and norm, defined as

$$\mathrm{Tr}(\alpha) := \alpha + \alpha', \qquad \mathrm{N}(\alpha) := \alpha\alpha',$$

where $'$ is the algebraic conjugation in K, defined by $\sqrt{5} \mapsto -\sqrt{5}$.

The first benefit of this setting is the following result.

Fact 3. *All non-zero linear similarities in $\mathbb{R}^4 \simeq \mathbb{H}(\mathbb{R})$ can be written as either $x \mapsto pxq$ (orientation preserving case) or as $x \mapsto p\bar{x}q$ (orientation reversing case), with non-zero quaternions $p, q \in \mathbb{H}(\mathbb{R})$. The determinants of the linear maps defined this way are $\pm|p|^4|q|^4$. Conversely, all mappings of the form $x \mapsto pxq$ and $x \mapsto p\bar{x}q$ are linear similarities.*

Proof. This follows easily from the corresponding result on orthogonal matrices in $\mathbb{R}^4$, as every non-zero similarity is the product of an orthogonal transformation and a non-zero homothety, see [4,13] for details. The result on the determinants is standard. □

For some purposes, it is convenient to refer to the standard matrix representation of the linear map $x \mapsto pxq$, as defined via $(pxq)^t = M(p,q)x^t$. Details can be found in [4,13].

Following [8], we consider the lattice

$$L = \left\langle (1,0,0,0), \frac{1}{2}(-1,1,1,1), (0,-1,0,0), \frac{1}{2}(0,1,\tau-1,-\tau) \right\rangle_{\mathbb{Z}} \tag{5}$$

where $\tau = (1+\sqrt{5})/2$ is the golden ratio. Due to $\mathrm{Tr}(\tau) = 1$ and $\mathrm{N}(\tau) = -1$, τ is an integer in K. In fact, τ is a fundamental unit of $\mathbb{Z}[\tau]$, the ring of integers of K.

The Gram matrix of L, calculated with $\langle .|. \rangle$, reads

$$\frac{1}{2}\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}, \tag{6}$$

which shows that L is a scaled copy of the root lattice A_4 in its standard representation with basis vectors of squared length 2, compare [10] and Fig. 1. Our choice of this particular realization of the A_4 root lattice is motivated by the observation that L is a subset of the so-called *icosian ring* $\mathbb{I}$, which has a powerful arithmetic structure. A concrete representation of $\mathbb{I}$ is obtained via the vectors

$$(\pm 1,0,0,0),\ \frac{1}{2}(\pm 1,\pm 1,\pm 1,\pm 1),\ \frac{1}{2}(\pm\tau', \pm\tau, 0, \pm 1) \tag{7}$$

and all their *even* coordinate permutations. Together, they form a set of 120 vectors (all of length 1) which constitute a non-crystallographic *root system of type* H_4, denoted by Δ_{H_4}, see [4,8] for details. The orthogonal transformations $\{x \mapsto pxq, x \mapsto p\bar{x}q \mid p, q \in \Delta_{H_4}\}$ form the corresponding *Coxeter group* W_{H_4} of all 120^2 point symmetries of Δ_{H_4}.

The icosian ring $\mathbb{I}$ is the $\mathbb{Z}$-span of Δ_{H_4}, $\mathbb{I} := \langle \Delta_{H_4} \rangle_{\mathbb{Z}}$, and has rank 8. At the same time, $\mathbb{I}$ is a $\mathbb{Z}[\tau]$-module of rank 4, and can alternatively be written as

$$\mathbb{I} = \left\langle (1,0,0,0), (0,1,0,0), \frac{1}{2}(1,1,1,1), \frac{1}{2}(1-\tau,\tau,0,1) \right\rangle_{\mathbb{Z}[\tau]}. \tag{8}$$

In this formulation, $\mathbb{I}$ is a maximal order in the quaternion algebra $\mathbb{H}(K)$, which has class number 1, see [21]. Consequently, all ideals of $\mathbb{I}$ are principal, and one has a powerful notion of prime factorization.

Remark 2. The quadratic form $\mathrm{tr}(x\bar{y}) = 2\langle x|y\rangle$ takes only integer values on the icosian ring, and is thus the canonical form on $\mathbb{I}$ in the context of root systems. Relative to this form, L *is* the root lattice A_4, with the weight lattice A_4^* as its dual (defined relative to the trace form) and the index relation $[A_4^* : A_4] = 5$, see [8,10] for details.

The icosian ring $\mathbb{I}$ also contains the $\mathbb{Z}[\tau]$-module

$$\mathcal{L} := \langle 1, \mathrm{i}, \mathrm{j}, \mathrm{k}\rangle_{\mathbb{Z}[\tau]} \simeq \mathbb{Z}[\tau]^4 \tag{9}$$

as a submodule of index 16. The same statement applies to $\mathbb{I}'$, which is another maximal order in $\mathbb{H}(K)$. Note that $\mathcal{L}$ is an index 4 submodule of $\mathbb{I} \cap \mathbb{I}'$, the latter thus being of index 4 both in $\mathbb{I}$ and in $\mathbb{I}'$.

The benefit of this approach will be that we can use the arithmetic of the ring $\mathbb{I}$. Let us recall the following result from [4], which is also immediate from Eqs. (8) and (9).

Fact 4. $2\mathbb{I} \subset \mathcal{L}$, *i.e.*, $x \in \mathbb{I}$ *implies* $2x \in \mathcal{L}$. $\square$

The golden key for solving the SSL problem is the mapping $\widetilde{\cdot} : \mathbb{H}(K) \to \mathbb{H}(K)$, $x \mapsto \widetilde{x}$ (also denoted by η later on), with

$$\widetilde{x} := \left(x_0', x_1', x_3', x_2'\right). \tag{10}$$

The relevance of this map was noticed in [12] as a result of explicit calculations around SSLs with small indices. The rather strange looking combination of a permutation of two coordinates with algebraic conjugation of all coordinates, which we shall call a *twist map* from now on, is an algebra involution of the second kind [14, Ch. I.2]. It has the following important properties (see also Section 6 for more).

Lemma 1. *The twist map* $\widetilde{\cdot}$ *of* (10) *is a* $\mathbb{Q}$*-linear and* K*-semilinear involutory algebra anti-automorphism, i.e., for arbitrary* $x, y \in \mathbb{H}(K)$ *and* $\alpha \in K$*, it satisfies*:

(a) $\widetilde{x+y} = \widetilde{x} + \widetilde{y}$ *and* $\widetilde{\alpha x} = \alpha' \widetilde{x}$,
(b) $\widetilde{xy} = \widetilde{y}\widetilde{x}$ *and* $\widetilde{\widetilde{x}} = x$,
(c) $\widetilde{\bar{x}} = \bar{\widetilde{x}}$ *and thus, for* $x \neq 0$, *also* $(\widetilde{x})^{-1} = \widetilde{x^{-1}}$.

It maps K*, the center of the algebra* $\mathbb{H}(K)$*, onto itself, but fixes only the elements of* $\mathbb{Q}$ *within* K*. Moreover, the icosian ring is mapped onto itself,* $\widetilde{\mathbb{I}} = \mathbb{I}$*, as is its algebraic conjugate,* $\mathbb{I}'$.

Proof. Most of these properties are immediate from the definition, and (b) can be proved by checking the action of the twist map on the basis quaternions $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$. The statements on K, $\mathbb{I}$ and $\mathbb{I}'$ follow easily from the definition in (8). $\square$

Seen as a vector space over $\mathbb{Q}$, $\mathbb{H}(K)$ has dimension 8 and can be split into a direct sum, $\mathbb{H}(K) = V_+ \dot{+} V_-$, where

$$V_\pm := \left\{x \in \mathbb{H}(K) \;\middle|\; \widetilde{x} = \pm x\right\}$$

are the eigenspaces under the twist map, with $V_+ \cap V_- = \{0\}$ and $V_- = \sqrt{5}V_+$. Concretely, one can choose the 4 basis vectors of L from (5) also as a $\mathbb{Q}$-basis for V_+.

Remark 3. Defining $u = \sqrt{5}\mathrm{i}$, $v = \mathrm{j} - \mathrm{k}$ and $w = \sqrt{5}(\mathrm{j}+\mathrm{k})$, one checks that $u^2 = -5$, $v^2 = -2$ and $w = uv = -vu$, so that $D := \langle 1, u, v, w\rangle_{\mathbb{Q}}$ is a quaternion algebra over $\mathbb{Q}$, of type $H(\frac{-5,-2}{\mathbb{Q}})$ in the terminology of [16, Sec. 57]. Extending this algebra by adjoining $\sqrt{5}$ leads to $\mathbb{H}(K)$, so $\mathbb{H}(K) = \mathbb{Q}(\sqrt{5}) \otimes_{\mathbb{Q}} D$. The benefit [17] is that the involution $\tilde{.}$ looks more canonical in this setting. In fact, $\widetilde{u} = -u = \bar{u}$, and analogously for v and w. Consequently, for $\alpha \in K$ and $x \in D$, one has $(\alpha x)^{\sim} = \alpha' \bar{x}$, which clearly shows the nature of the involution. Note, however, that L is a subset of V_+ and is thus not contained in D.

These observations, together with the nature of $\mathbb{I}$ as a maximal order in $\mathbb{H}(K)$, suggest that L might actually be the $\mathbb{Z}$-module of fixed points of the twist map inside $\mathbb{I}$.

Proposition 1. *One has* $\mathbb{I} \cap V_+ = \{x \in \mathbb{I} \mid \widetilde{x} = x\} = L$, *with* L *as in* (5).

Proof. The basis vectors of L in (5) are fixed under the twist map, so $\widetilde{x} = x$ is clear for all $x \in L$. We also know from Lemma 1 that $\widetilde{\mathbb{I}} = \mathbb{I}$. To prove our claim, we have to show that no element of $\mathbb{I} \setminus L$ is fixed under the twist map.

Let $L[\tau]$ be the $\mathbb{Z}[\tau]$-span of L. It is clear that

$$L[\tau] = L + \tau L = L \dot{+} \tau L,$$

where the latter equality follows from $L \cap \tau L = \{0\}$, and also that $\widetilde{L[\tau]} = L[\tau]$. Observe that $|\det_K(\mathbb{I})| = 1/4$ and $|\det_K(L[\tau])| = \sqrt{5}/4$, where the K-determinants are just the ordinary determinants of the bases given in (5) and (8). Using the connection of the corresponding index with the ratio of the $\mathbb{Q}$-determinants, see [6] for details, one concludes that

$$\big[\mathbb{I} : L[\tau]\big] = \big|\mathrm{N}(\sqrt{5})\big| = 5, \tag{11}$$

so that $\mathbb{I}/L[\tau] \simeq C_5$.

Consequently, the twist map, which is an involution, induces an automorphism on the cyclic group C_5. The order of this automorphism must divide 2. Since $0 \neq v = \mathrm{j} - \mathrm{k} \in \mathbb{I} \setminus L[\tau]$, but satisfies $\widetilde{v} = -v$, the induced automorphism on C_5 cannot be the identity. This leaves only inversion (i.e., $k \mapsto -k \bmod 5$), which has no fixed point in C_5 other than 0, so that all fixed points of the twist map inside $\mathbb{I}$ must lie in $L[\tau]$. It is easy to see that a quaternion of the form $x + \tau y$ with $x, y \in L$ is fixed if and only if $y = 0$, which completes the argument. □

Remark 4. An alternative way to prove Proposition 1 would be to use Remark 2 and to show that all potential $x \in \mathbb{I}$ with $\widetilde{x} = x$ are elements of the dual of L (taken with respect to $\mathrm{tr}(x\bar{y})$), but that the coset representative of A_4^*/A_4 cannot be chosen in $\mathbb{I}$. In fact, extending A_4 and A_4^* to lattices over $\mathbb{Z}[\tau]$, compare [19], one sees that $\mathbb{I}$ is intermediate between them, but is still integral for $\mathrm{tr}(x\bar{y})$. When viewed as a $\mathbb{Z}[\tau]$-module, $\mathbb{I}$ has class number 1, see [19, Thm. 3.4]. Moreover, it is a principal ideal domain and a maximal order in $\mathbb{H}(K)$. The intimate relation with quaternion arithmetic is the entry point for our further analysis.

In fact, in the setting of Remarks 2 and 4, we have $L = A_4$ and thus $L[\tau] = \mathbb{Z}[\tau] \otimes_{\mathbb{Z}} A_4$. Then, its dual over $\mathbb{Z}[\tau]$ (relative to $\operatorname{tr}(x\bar{y})$ again) is $\mathbb{Z}[\tau] \otimes_{\mathbb{Z}} A_4^*$, which has K-index 5 over $L[\tau]$, where the K-index (up to units in $\mathbb{Z}[\tau]$) is given by the determinant of the linear mapping that sends a basis of $L[\tau]$ to one of $L[\tau]^*$. The various inclusions can now be summarized as

$$2L[\tau] \overset{16}{\subset} L[\tau] \overset{\sqrt{5}}{\subset} \mathbb{I} \overset{\sqrt{5}}{\subset} L[\tau]^*$$

together with

$$2L[\tau] \overset{\sqrt{5}}{\subset} 2\mathbb{I} \overset{4}{\subset} \mathcal{L} \overset{4}{\subset} \mathbb{I} \overset{\sqrt{5}}{\subset} L[\tau]^*,$$

where the integers on top of the inclusion symbols denote the corresponding K-indices. The indices over $\mathbb{Q}$ are then just the squares of these numbers.

Also, as a result of Proposition 1, we get that

$$\Delta_{A_4} = V_+ \cap \Delta_{H_4} \tag{12}$$

with the root system Δ_{H_4} as described above. Explicitly, observing $\tau' = 1 - \tau$, this leaves us with the 20 roots of the root system Δ_{A_4},

$$\begin{aligned} &\pm(1,0,0,0),\ \pm(0,1,0,0),\ \pm\frac{1}{2}\,(\pm1,\pm1,1,1),\\ &\pm\frac{1}{2}(0,\pm1,\tau-1,-\tau),\ \pm\frac{1}{2}(\pm1,0,-\tau,\tau-1), \end{aligned} \tag{13}$$

which will become important later on, see [18, Prop. 2] and [8] for the relation between the corresponding reflection groups.

4. Similarities for A_4 via quaternions

We are interested in the SSLs of the root lattice A_4. They are in one-to-one relation to those of the lattice L defined in Eq. (5). For convenience, we define $\mathbb{H}(K)^\bullet = \mathbb{H}(K) \setminus \{0\}$, and analogously for other rings.

Lemma 2. *All SSLs of the lattice L, defined as in Eq.* (5)*, are images of L under orientation preserving mappings of the form $x \mapsto pxq$, with $p, q \in \mathbb{H}(K)^\bullet$ and $K = \mathbb{Q}(\sqrt{5})$.*

Proof. As L is invariant under the conjugation map $x \mapsto \bar{x}$, we need not consider orientation reversing similarities. By Fact 3, all SSLs are thus images of L under mappings $x \mapsto pxq$ with $p, q \in \mathbb{H}(\mathbb{R})^\bullet$.

A simple argument with the matrix entries of the linear transformations defined by the mappings $x \mapsto pxq$, compare [4], shows that all products $p_i q_j$ must be in the quadratic field $K = \mathbb{Q}(\sqrt{5})$, which leaves the choice to take $p, q \in \mathbb{H}(K)^\bullet$. □

We need to select an appropriate subset of mappings that reach all SSLs of L. A first step is provided by the following observation.

Lemma 3. *If $p \in \mathbb{I}$, $pL\widetilde{p}$ is an SSL of L.*

Proof. By Fact 3, $pL\widetilde{p}$ is similar to L, so it remains to be shown that $pL\widetilde{p} \subset L$. Observe that $p \in \mathbb{I}$ implies $\widetilde{p} \in \mathbb{I}$, so that $pL\widetilde{p} \subset \mathbb{I}$ is clear. If x is any point of L, we have $\widetilde{x} = x$ by Proposition 1. Using the properties of the twist map from Lemma 1, one gets

$$(px\widetilde{p})^{\sim} = \widetilde{\widetilde{p}}\,\widetilde{x}\,\widetilde{p} = px\widetilde{p}.$$

Consequently, again by Proposition 1, $px\widetilde{p} \in L$, and hence $pL\widetilde{p} \subset L$, as claimed. □

Proposition 2. *If $pLq \subset L$ with $p, q \in \mathbb{H}(K)^{\bullet}$, there is an $\alpha \in \mathbb{Q}$ such that*

$$q = \alpha\widetilde{p}.$$

Proof. If $p, q \in \mathbb{H}(K)^{\bullet}$, the inclusion $pLq \subset L$ implies $pxq = \widetilde{pxq} = \widetilde{q}x\widetilde{p}$ for all $x \in L$, hence also $x\widetilde{p}q^{-1} = (\widetilde{q})^{-1}px = (\widetilde{p}q^{-1})^{\sim}x$. Since $1 \in L$, this implies $\widetilde{p}q^{-1} = (\widetilde{p}q^{-1})^{\sim}$, and we get

$$x\widetilde{p}q^{-1} = \widetilde{p}q^{-1}x,$$

still for all $x \in L$. Noting that $\langle L\rangle_K = \mathbb{H}(K)$, the previous equation implies that $\widetilde{p}q^{-1}$ must be central, i.e., an element of K. Consequently, $q = \alpha\widetilde{p}$ for some $\alpha \in K$.

Since $p \in \mathbb{H}(K)$, we can choose some $0 \neq \beta \in \mathbb{Z}[\tau]$ such that $w = \beta p \in \mathbb{I}$. Observing that $(\beta p)^{\sim} = \beta'\widetilde{p}$, one sees that $\alpha px\widetilde{p} = \frac{\alpha}{\mathrm{N}(\beta)}wx\widetilde{w}$, where $0 \neq \mathrm{N}(\beta) \in \mathbb{Z}$. As $wL\widetilde{w} \subset L$ by Lemma 3, and since $L \cap \tau L = \{0\}$, the original relation $pLq \subset L$ now implies $\frac{\alpha}{\mathrm{N}(\beta)} \in \mathbb{Q}$, hence also $\alpha \in \mathbb{Q}$. □

An element $q \in \mathbb{I}$ is called $\mathbb{I}$-*primitive* when all $\mathbb{Z}[\tau]$-divisors of q are units. Another way to phrase this is to say that the $\mathbb{I}$-content of q,

$$\mathrm{cont}_{\mathbb{I}}(q) := \mathrm{lcm}\big\{\alpha \in \mathbb{Z}[\tau]^{\bullet} \mid q \in \alpha\mathbb{I}\big\}, \tag{14}$$

is a unit in $\mathbb{Z}[\tau]$. Whenever the context is clear, we shall simply speak of primitivity and content of q. Note that the content is unique up to units of $\mathbb{Z}[\tau]$, as $\mathbb{Z}[\tau]$ is Euclidean and hence also a principal ideal domain. More generally, one has to formulate the content via a fractional ideal, see [4] for details.

Corollary 1. *All SSLs of the lattice L are images of L under mappings of the form $x \mapsto \alpha px\widetilde{p}$ with $p \in \mathbb{I}$ primitive and $\alpha \in \mathbb{Q}$.*

Proof. By Proposition 2, we know that mappings of the form $x \mapsto \beta qx\widetilde{q}$ with $q \in \mathbb{H}(K)$ and $\beta \in \mathbb{Q}$ suffice. Since all coordinates of q are in $K = \mathbb{Q}(\sqrt{5})$, there is a natural number m such that $p := mq \in \mathcal{L}$, with $\mathcal{L}$ as in (9). Then, with $\alpha := \beta/m^2$, one has $\alpha px\widetilde{p} = \beta qx\widetilde{q}$ whence the mappings $x \mapsto \alpha px\widetilde{p}$ and $x \mapsto \beta qx\widetilde{q}$ are equal. While α is still in $\mathbb{Q}$, p and $\widetilde{p}$ are now elements of $\mathcal{L} \subset \mathbb{I}$.

If p is primitive in $\mathbb{I}$, we are done. If not, we know that p/c is a primitive element of $\mathbb{I}$ when $c = \mathrm{cont}_{\mathbb{I}}(p)$. Simultaneously, we have $(p/c)^{\sim} = \widetilde{p}/c'$. Since $c \in \mathbb{Z}[\tau]$, we know that $cc' \in \mathbb{Z}$, so that this factor can be absorbed into α. □

At this stage, we recollect an important property of the icosian ring from [4].

Fact 5. *Let $p, q \in \mathbb{H}(K)^{\bullet}$ be such that $p\mathbb{I}q \subset \mathbb{I}$. If one of p or q is an $\mathbb{I}$-primitive icosian, the other must be in $\mathbb{I}$ as well.*

Proof. This follows from [4, Prop. 1 and Remark 1], where this is shown for any maximal order of class number one. In particular, it applies to $\mathbb{I}$. □

As a result of independent interest, we note the following.

Fact 6. *The linear map T defined by $x \mapsto \alpha p x \widetilde{p}$ has trace $\alpha\,\mathrm{N}(\mathrm{tr}(p))$ and determinant $\alpha^4\,\mathrm{N}(|p|^4)$, and its characteristic polynomial reads*

$$X^4 - \mathrm{trace}(T)X^3 + AX^2 - BX + \det(T)$$

where $A = \alpha^2(\mathrm{Tr}((\mathrm{tr}(p))^2(\mathrm{nr}(p))') - 2\,\mathrm{N}(\mathrm{nr}(p)))$ and $B = \alpha^3\,\mathrm{N}(\mathrm{tr}(p)\,\mathrm{nr}(p))$.

Proof. This is a straight-forward calculation, e.g., with the matrix representation from [4,13], taking into account that $\mathrm{nr}(\widetilde{p}) = (\mathrm{nr}(p))'$ and expressing the coefficients in terms of traces and norms. □

In view of Corollary 1, we now need to understand how an SSL of L of the form $pL\widetilde{p}$ with an $\mathbb{I}$-primitive quaternion relates to the primitive sublattices of L. Recall that Λ is a sublattice of Γ if and only if there is a non-singular integer matrix Z that maps a basis of Γ to a basis of Λ, written as $B_\Lambda = B_\Gamma Z$ in terms of basis matrices, compare [7]. The index is then

$$[\Gamma : \Lambda] = \left|\det(Z)\right|$$

which does not depend on the actual choice of the lattice basis. A sublattice Λ of $\Gamma \subset \mathbb{R}^d$ is called *Γ-primitive* (or simply primitive) when

$$\mathrm{cont}_\Gamma(\Lambda) := \mathrm{lcm}\{m \in \mathbb{N} \mid \Lambda \subset m\Gamma\} = 1. \tag{15}$$

This is equivalent to saying that $\gcd(Z) := \gcd\{Z_{ij} \mid 1 \leqslant i, j \leqslant d\} = 1$.

Proposition 3. *If $p \in \mathbb{I}$ is $\mathbb{I}$-primitive, $pL\widetilde{p}$ is an L-primitive sublattice of L.*

Proof. By Lemma 3, we know that $pL\widetilde{p} \subset L$. We thus have to show that $\frac{1}{m}pL\widetilde{p} \subset L$ implies $m = 1$. Note first that $\frac{1}{m}pL\widetilde{p} \subset L$ also implies $\frac{1}{m}pL[\tau]\widetilde{p} \subset L[\tau]$, with $L[\tau] = L \dotplus \tau L$ as before. From (11), we know that $5\mathbb{I} \subset L[\tau]$, so that we get

$$\frac{5}{m}p\mathbb{I}\widetilde{p} \subset \frac{1}{m}pL[\tau]\widetilde{p} \subset L[\tau] \subset \mathbb{I}.$$

Since p is $\mathbb{I}$-primitive by assumption, then so is $\widetilde{p}$. By Fact 5, this forces $5/m$ to be an element of $\mathbb{Z}[\tau]$. With $m \in \mathbb{N}$, this only leaves $m = 1$ or $m = 5$.

Observe next that $2L[\tau] \subset \mathcal{L} = \mathbb{Z}[\tau]^4$. On the other hand, it is easy to check explicitly (e.g., by means of the basis vectors) that $\sqrt{5}\mathcal{L} \subset L[\tau]$. Together with $2\mathbb{I} \subset \mathcal{L}$ from Fact 4, this gives

$$\frac{4\sqrt{5}}{m} p\mathbb{I}\widetilde{p} \subset \frac{2\sqrt{5}}{m} p\mathcal{L}\widetilde{p} \subset \frac{2}{m} pL[\tau]\widetilde{p} \subset 2L[\tau] \subset \mathcal{L} \subset \mathbb{I}.$$

Invoking Fact 5 again, we see that $\frac{4\sqrt{5}}{m} \in \mathbb{Z}[\tau]$, which (with $m \in \mathbb{N}$) is only possible for $m|4$. In combination with the previous restriction, this implies $m = 1$. $\square$

Combining the results of Corollary 1 and Proposition 3, we obtain the following important observation.

Corollary 2. *The L-primitive SSLs of L are precisely the ones of the form $pL\widetilde{p}$ with p an $\mathbb{I}$-primitive icosian.*

Proof. After Proposition 3, it remains to show that every primitive SSL M of L is of the form $pL\widetilde{p}$ for some primitive $p \in \mathbb{I}$. By Corollary 1, $M = \alpha pL\widetilde{p}$ with $\alpha \in \mathbb{Q}$ and $p \in \mathbb{I}$ primitive. By Proposition 3, $pL\widetilde{p}$ is already a primitive sublattice, so $\alpha = \pm 1$. $\square$

Next, we need to find a suitable bijection that permits us to count the primitive SSLs of L of a given index. Recall from [8,15] that the unit group of $\mathbb{I}$ has the form

$$\mathbb{I}^{\times} = \big\{x \in \mathbb{I} \bigm| \mathrm{N}\big(\mathrm{nr}(x)\big) = \pm 1\big\} = \big\{\pm\tau^m \varepsilon \bigm| m \in \mathbb{Z} \text{ and } \varepsilon \in \Delta_{H_4}\big\},$$

where Δ_{H_4} is defined as above via Eq. (7) and satisfies $\Delta_{H_4} = \mathbb{I}^{\times} \cap \mathbb{S}^3 = \mathbb{I} \cap \mathbb{S}^3$, see [4,15] for details.[1]

Lemma 4. *For $p \in \mathbb{I}$, one has $pL\widetilde{p} = L$ if and only if $p \in \mathbb{I}^{\times}$.*

Proof. We have $pL\widetilde{p} \subset L$ for all $p \in \mathbb{I}$ by Lemma 3. The corresponding index is given by the determinant of the mapping $x \mapsto px\widetilde{p}$. By Fact 6, the equality $L = pL\widetilde{p}$ is then equivalent to $\mathrm{N}(|p|^4) = 1$ and hence to $\mathrm{N}(\mathrm{nr}(p)) = \pm 1$, which, in turn, is equivalent to $p \in \mathbb{I}^{\times}$. $\square$

We need one further result to construct a bijective correspondence between primitive SSLs of L and certain right ideals of $\mathbb{I}$, which will then solve our problem.

Lemma 5. *For primitive $r, s \in \mathbb{I}$, one has $r\mathbb{I} = s\mathbb{I}$ if and only if $rL\widetilde{r} = sL\widetilde{s}$.*

Proof. Since $r, s \in \mathbb{I}$, it is clear that $r\mathbb{I} = s\mathbb{I} \Rightarrow \mathbb{I} = r^{-1}s\mathbb{I} \Rightarrow r^{-1}s \in \mathbb{I}$. Similarly, $s^{-1}r \in \mathbb{I}$, so $r^{-1}s \in \mathbb{I}^{\times}$. Lemma 4 now implies $r^{-1}sL(r^{-1}s)^{\sim} = L$, which gives $rL\widetilde{r} = sL\widetilde{s}$.

In the reverse direction, suppose that $rL\widetilde{r} = sL\widetilde{s}$, which gives $yL\widetilde{y} = L$ with $y := r^{-1}s$. Choose $\alpha \in K$ so that αy is a primitive element of $\mathbb{I}$, which is always possible. Then,

$$\alpha yL\widetilde{\alpha y} = \alpha\alpha' yL\widetilde{y} = \alpha\alpha' L$$

[1] Let us take this opportunity to mention that [4], in deviation from other conventions and from the one adopted here, uses the notation $\mathbb{I}^{\times}$ for the $\mathbb{I}$-units on $\mathbb{S}^3$, i.e., for the elements of Δ_{H_4} only.

is a primitive sublattice of L by Proposition 3, whence $\alpha\alpha' = \pm 1$ and $\alpha y L \widetilde{\alpha y} = L$.

This implies $\varepsilon := \alpha y = \alpha r^{-1} s \in \mathbb{I}^{\times}$ by Lemma 4. Then,

$$r = r\varepsilon\varepsilon^{-1} = \alpha s \varepsilon^{-1} \in \alpha\mathbb{I},$$

so that $\alpha' r \in \mathbb{I}$ due to $\alpha\alpha' = \pm 1$, where $\alpha' \in K$ by construction. Since $r \in \mathbb{I}$ is primitive as well, such a relation is only possible with $\alpha \in \mathbb{Z}[\tau]$, in view of the properties of the $\mathbb{I}$-content of r. Consequently, $\alpha\alpha' = \pm 1$ now gives $\alpha \in \mathbb{Z}[\tau]^{\times}$, so that y is an element of $\mathbb{I}$. Lemma 4 now implies $y \in \mathbb{I}^{\times}$, whence $y\mathbb{I} = \mathbb{I}$, and finally $s\mathbb{I} = r\mathbb{I}$. □

In view of our discussion so far, we call a right ideal of $\mathbb{I}$ *primitive* if it is of the form $p\mathbb{I}$ for some primitive $p \in \mathbb{I}$.

Proposition 4. *There is a bijective correspondence between the primitive right ideals of* $\mathbb{I}$ *and the primitive SSLs of L, defined by* $p\mathbb{I} \mapsto pL\widetilde{p}$. *Furthermore, one has the index formula*

$$[\mathbb{I} : p\mathbb{I}] = \mathrm{N}\left(\mathrm{nr}(p)^2\right) = \mathrm{N}\left(|p|^4\right) = [L : pL\widetilde{p}]$$

under this correspondence.

Proof. It is clear from Lemma 5 that the mapping is well defined and injective, while Corollary 2 implies its surjectivity.

The index of $p\mathbb{I}$ in $\mathbb{I}$ derives from the determinant formula in Fact 3 by taking the norm in $\mathbb{Z}[\tau]$. The index relation now follows from Fact 6. □

Remark 5. The results of Lemmas 4 and 5 also show that $\Delta_{H_4} = \mathbb{I}^{\times} \cap \mathbb{S}^3$, which is a subgroup of $\mathbb{I}^{\times}$ of order 120, can be viewed as the standard double cover of the rotation symmetry group of L, which has order 60 and contains the point reflection in the origin (note that -1 is a rotation in 4-space). This is a geometric interpretation of the bijective correspondence. Let us, in this context, also point out that $p\mathbb{I}\widetilde{p} \cap V_+ = pL\widetilde{p}$, but that $p\mathbb{I} \cap V_+$ is generally a much bigger set.

With the representation of a general SSL as an integer multiple of a primitive SSL mentioned earlier, and observing that all possible indices of SSLs are squares, we can now solve our original problem. We need the Dirichlet character

$$\chi(n) = \begin{cases} 0, & n \equiv 0(5), \\ 1, & n \equiv \pm 1(5), \\ -1, & n \equiv \pm 2(5). \end{cases} \tag{16}$$

Note that the corresponding L-series, $L(s,\chi) = \sum_{m=1}^{\infty} \chi(m) m^{-s}$, defines an entire function on the complex plane. Furthermore, we need the zeta functions of the icosian ring,

$$\zeta_{\mathbb{I}}(s) = \zeta_K(2s)\zeta_K(2s-1) \quad \text{and} \quad \zeta_{\mathbb{I}.\mathbb{I}}(s) = \zeta_K(4s), \tag{17}$$

where $\zeta_{\mathbb{I}}(s)$ and $\zeta_{\mathbb{I}.\mathbb{I}}(s)$ denote the Dirichlet series for the one-sided and the two-sided ideals of $\mathbb{I}$, respectively. Here, $\zeta_K(s) = \zeta(s)L(s,\chi)$ is the Dedekind zeta function of the quadratic field K, see [4,6,21] for details.

Theorem 1. *The number of SSLs of a given index is the same for the lattices A_4 and L. The possible indices are the squares of non-zero integers of the form $k^2 + k\ell - \ell^2 = \mathrm{N}(k + \ell\tau)$. Moreover, all possible indices are realized.*

Furthermore, there is an index preserving bijection between the primitive SSLs of A_4 and the primitive right ideals of $\mathbb{I}$. When $f(m)$ denotes the number of SSLs of index m^2 and $f^{\mathsf{pr}}(m)$ the number of primitive ones, the corresponding Dirichlet series generating functions read

$$D_{A_4}(s) := \sum_{m=1}^{\infty} \frac{f(m)}{m^{2s}} = \zeta(4s)\frac{\zeta_{\mathbb{I}}(s)}{\zeta_K(4s)} = \frac{\zeta_K(2s)\zeta_K(2s-1)}{L(4s,\chi)}$$

and

$$D^{\mathsf{pr}}_{A_4}(s) := \sum_{m=1}^{\infty} \frac{f^{\mathsf{pr}}(m)}{m^{2s}} = \zeta^{\mathsf{pr}}_{\mathbb{I}}(s) = \frac{\zeta_{\mathbb{I}}(s)}{\zeta_K(4s)} = \frac{\zeta_K(2s)\zeta_K(2s-1)}{\zeta_K(4s)},$$

with $\zeta_K(s)$ and $L(s,\chi)$ as defined above. In particular, each possible index is thus also realized by a primitive SSL.

Proof. The first claim follows from Fact 1, while the index characterization follows either from [9] or from the index formula in Proposition 4. Recall that $k^2 + k\ell - \ell^2 = \mathrm{N}(k + \ell\tau)$ is the norm the principal ideal $(k + \ell\tau)\mathbb{Z}[\tau]$, and that all $\mathbb{Z}[\tau]$-ideals are of this form. Since the reduced norm as a mapping from icosian right ideals to ideals in $\mathbb{Z}[\tau]$ is surjective, each possible index is realized.

In view of the previous remarks, we have

$$D_{A_4}(s) = \zeta(4s) D^{\mathsf{pr}}_{A_4}(s),$$

where, due to our bijective correspondence and the index formula of Proposition 4, the various formulas for the Dirichlet series are immediate, see [4,6] for a derivation of $\zeta^{\mathsf{pr}}_{\mathbb{I}}(s)$ as the quotient stated above. The last equality then follows from (17). Since $f^{\mathsf{pr}}(m)$ vanishes precisely when $f(m)$ does (see below for an explicit formula), the last claim is clear. □

Inserting the Euler products of $\zeta(s)$ and $\zeta_K(s)$, one finds the expansion of the Dirichlet series $D_{A_4}(s)$ as an Euler product,

$$D_{A_4}(s) = \frac{1}{(1-5^{-2s})(1-5^{1-2s})} \prod_{p\equiv\pm1(5)} \frac{1+p^{-2s}}{1-p^{-2s}} \frac{1}{(1-p^{1-2s})^2} \prod_{p\equiv\pm2(5)} \frac{1+p^{-4s}}{1-p^{-4s}} \frac{1}{1-p^{2-4s}}$$

and similarly for $D^{\mathsf{pr}}_{A_4}(s)$. Consequently, the arithmetic function $f(m)$ (and also $f^{\mathsf{pr}}(m)$) is multiplicative, i.e., $f(mn) = f(m)f(n)$ for m,n coprime, with $f(1) = 1$. The function f is then completely specified by its values at prime powers p^r with $r \geqslant 1$. These are given by

$$f(p^r) = \begin{cases} \frac{5^{r+1}-1}{4}, & \text{if } p = 5, \\ \frac{2(1-p^{r+1})-(r+1)(1-p^2)p^r}{(1-p)^2}, & \text{for primes } p \equiv \pm1(5), \\ \frac{2-p^r-p^{r+2}}{1-p^2}, & \text{for primes } p \equiv \pm2(5) \text{ and } r \text{ even}, \\ 0, & \text{for primes } p \equiv \pm2(5) \text{ and } r \text{ odd}, \end{cases}$$

and similarly for $f^{\mathsf{pr}}(m)$:

$$f^{\mathsf{pr}}(p^r) = \begin{cases} 6 \cdot 5^{r-1}, & \text{if } p = 5, \\ (r+1)p^r + 2rp^{r-1} + (r-1)p^{r-2}, & \text{for } p \equiv \pm 1(5), \\ p^r + p^{r-2}, & \text{for } p \equiv \pm 2(5) \text{ and } r \text{ even}, \\ 0, & \text{for } p \equiv \pm 2(5) \text{ and } r \text{ odd}. \end{cases}$$

The first few terms of the Dirichlet series thus read

$$\begin{aligned} D_{A_4}(s) &= 1 + \frac{6}{4^{2s}} + \frac{6}{5^{2s}} + \frac{11}{9^{2s}} + \frac{24}{11^{2s}} + \frac{26}{16^{2s}} + \frac{40}{19^{2s}} + \frac{36}{20^{2s}} + \frac{31}{25^{2s}} \\ &\quad + \frac{60}{29^{2s}} + \frac{64}{31^{2s}} + \frac{66}{36^{2s}} + \cdots, \\ D^{\mathsf{pr}}_{A_4}(s) &= 1 + \frac{5}{4^{2s}} + \frac{6}{5^{2s}} + \frac{10}{9^{2s}} + \frac{24}{11^{2s}} + \frac{20}{16^{2s}} + \frac{40}{19^{2s}} + \frac{30}{20^{2s}} + \frac{30}{25^{2s}} \\ &\quad + \frac{60}{29^{2s}} + \frac{64}{31^{2s}} + \frac{50}{36^{2s}} + \cdots \end{aligned}$$

where the denominators are the squares of the integers previously identified in [9], see also entry A031363 of [20]. Further details can be found in [12].

These series may now be compared with the zeta functions $\zeta_{\mathbb{I}}(s)$ and $\zeta^{\mathsf{pr}}_{\mathbb{I}}(s)$, which reveals the origin of the various contributions. In particular, the 6 SSLs of index 16 stem from the 5 generators of primitive ideals of $\mathbb{I}$ of index 16 together with the SSL $2A_4$. No such extra solution exists for index 25, while index 81 emerges also from the SSL $3A_4$.

Due to our definition with $f(m)$ being the number of SSLs of A_4 of index m^2, the Dirichlet series generating function of the arithmetic function f is $D_{A_4}(s/2)$, which has nice analytic properties. In particular, it is analytic on the half-plane $\{\sigma > 2\}$, where we write $s = \sigma + \mathrm{i}t$ as usual. Moreover, it is analytic on the line $\{\sigma = 2\}$, except at $s = 2$, where we have a simple pole as the right-most singularity of $D_{A_4}(s/2)$. Consequently, one can derive the asymptotic growth of $f(m)$ from it. Since the value of the arithmetic function $f(m)$ fluctuates heavily, this is done via the corresponding summatory function

$$F(x) := \sum_{m \leqslant x} f(m) \sim \varrho \frac{x^2}{2}, \quad \text{as } x \to \infty,$$

where the growth constant is given by

$$\varrho = \operatorname{res}_{s=2} D_{A_4}(s/2) = \frac{\zeta_K(2) L(1, \chi)}{L(4, \chi)} = \frac{1}{2}\sqrt{5}\log(\tau) \simeq 0.538011.$$

This result relies on Delange's theorem, see [4, Appendix] for details. The corresponding calculations for the asymptotic behavior of $f^{\mathsf{pr}}(m)$ are analogous.

5. Results for related lattices

From previously published results, one can read off or easily derive the generating functions for the root lattices A_d with $d \leqslant 3$.

Theorem 2. *The Dirichlet series generating functions for the number of SSLs of the root lattices A_d with $d \leqslant 3$ are $D_{A_1}(s) = \zeta(s)$, $D_{A_2}(s) = \zeta_{\mathbb{Q}(\xi_3)}$, with $\xi_3 = e^{2\pi i/3}$ and $\zeta_{\mathbb{Q}(\xi_3)}(s)$ the Dedekind zeta function of the cyclotomic field $\mathbb{Q}(\xi_3)$, and $D_{A_3}(s) = \zeta(3s)\Phi_{\mathrm{cub}}(3s)$, where*

$$\Phi_{\mathrm{cub}}(s) = \frac{1-2^{1-s}}{1+2^{-s}} \frac{\zeta(s)\zeta(s-1)}{\zeta(2s)}$$

is the generating function of the related cubic coincidence site lattice problem derived in [1,6].

Proof. A_1 is a scaled version of the integer lattice $\mathbb{Z}$, whence $D_{A_1}(s) = D_{\mathbb{Z}}(s) = \zeta(s)$ follows from Fact 1 together with [3, Prop. 3.1]. The triangular lattice A_2 is a scaled version of the ring of Eisenstein integers in $\mathbb{Q}(\xi_3)$, so that this generating function follows from [2, Prop. 1]. It can also be written as a product of two Dirichlet series,

$$D_{A_2}(s) = \zeta(2s) \frac{\zeta_{\mathbb{Q}(\xi_3)}(s)}{\zeta(2s)},$$

one for the scaling by integers and the other for the primitive SSLs.

For the primitive cubic lattice $\mathbb{Z}^3$, the SSL generating function was previously identified as $\zeta(3s)\Phi_{\mathrm{cub}}(3s)$ in [3, Thm. 5.1]. Noting that A_3 is a version of the face-centered cubic lattice, compare [10], one has to check that the cubic lattices share the same SSL statistics. This is a straight-forward calculation with their basis matrices and the integrality conditions for similarity transforms, similar to the one outlined in [3, Sec. 5], using the Cayley parametrization of matrices in $\mathrm{SO}(3, \mathbb{Q})$ from [1], see also [12] for details. $\square$

Clearly, by Fact 2, one then also has the relation

$$D_{A_3}(s) = D_{A_3^*}(s) = D_{\mathbb{Z}^3}(s). \tag{18}$$

This identity can also be derived [22] by a consideration of the shelling structure of A_3^* relative to $\mathbb{Z}^3$, which bypasses the explicit basis calculations referred to above.

Other completely worked out examples include the square lattice $\mathbb{Z}^2$, with $D_{\mathbb{Z}^2}(s) = \zeta_{\mathbb{Q}(i)}(s)$, see [3], and the cubic lattices in $d = 4$, see [4]. Also, various $\mathbb{Z}$-modules of rank $r > d$ in dimensions $d \leqslant 4$ are solved in [2–5]. Common to all these examples is the rather explicit use of methods from algebraic number theory or quaternions in conjunction with suitable parametrizations of the rotations involved. In higher dimensions, results are sparse, compare [9] and references given there, and we are not aware of any complete solution in terms of generating functions at present.

6. Algebraic afterthoughts

The special twist map $\tilde{.}$ played a crucial role in solving the sublattice problem above. It is an odd looking map at first sight, but has a number of interesting properties that are worth considering in more detail. To do so, we also write $\eta(x) = \widetilde{x}$ from now on, and use both notations in parallel. Moreover, we define inner automorphisms T_a of the quaternion algebra $\mathbb{H}(K)$ via $T_a(x) = axa^{-1}$, for $a \in \mathbb{H}(K)^{\bullet}$. Finally, we call any K-semilinear involutory anti-automorphism of $\mathbb{H}(K)$ a *twist map*.

Lemma 6. *If σ_1 and σ_2 are two twist maps of $\mathbb{H}(K)$ that map $\mathbb{I}$ into itself, their product is an inner automorphism of $\mathbb{I}$, i.e., $\sigma_1\sigma_2 = T_\varepsilon$ for some $\varepsilon \in \mathbb{I}^\times$. In particular, any such twist map is of the form $T_\varepsilon\eta$ for some $\varepsilon \in \mathbb{I}^\times$.*

Proof. Since both σ_i are K-semilinear, their product is K-linear. Also, the product $\sigma_1\sigma_2$ of two anti-automorphisms is an automorphism of $\mathbb{H}(K)$, which must be inner by the Skolem–Noether theorem [14, Thm. I.1.4]. This gives $\sigma_1\sigma_2 = T_a$ with $a \in \mathbb{H}(K)^\bullet$. By construction, T_a is also an automorphism of $\mathbb{I}$, whence we may assume $a \in \mathbb{I}$ without loss of generality. This implies $a\mathbb{I} = \mathbb{I}a$, so that $a\mathbb{I}$ is a two-sided ideal. Within $\mathbb{I}$, this implies $a = \alpha\varepsilon$ with $0 \neq \alpha \in \mathbb{Z}[\tau]$ and $\varepsilon \in \mathbb{I}^\times$. Observing $T_{\alpha\varepsilon} = T_\varepsilon$ establishes the claim. □

For our further arguments, it is advantageous to consider the mapping $\vartheta : \mathbb{H}(K) \to V_+$, defined by $x \mapsto x\eta(x) = x\widetilde{x}$, where $V_+ = \{x \in \mathbb{H}(K) \mid \widetilde{x} = x\}$ as before. Clearly, one has $\vartheta(\mathbb{I}) \subset L$, as a consequence of Proposition 1.

Lemma 7. *The mapping ϑ satisfies $\vartheta(\mathbb{I}^\times) = \vartheta(\Delta_{H_4}) \subset \Delta_{A_4}$. Moreover, the corresponding restriction, $\vartheta_\Delta : \Delta_{H_4} \to \Delta_{A_4}$, is a surjective 6-to-1 mapping.*

Proof. Any $a \in \mathbb{I}^\times$ has the form $a = \pm\tau^m\varepsilon$ for some $m \in \mathbb{Z}$ and $\varepsilon \in \Delta_{H_4}$, so that $a\widetilde{a} = (\tau\tau')^m\varepsilon\tilde{\varepsilon} = (-1)^m\varepsilon\tilde{\varepsilon}$. The identity $\vartheta(\mathbb{I}^\times) = \vartheta(\Delta_{H_4})$ follows from the observation that $\mathrm{i} \in \Delta_{H_4}$, with $\vartheta(\mathrm{i}) = \mathrm{i}^2 = -1$. If $\varepsilon \in \Delta_{H_4}$, $\varepsilon\tilde{\varepsilon}$ lies both in L and in Δ_{H_4}, and thus in $\Delta_{A_4} = L \cap \Delta_{H_4}$, see Eq. (12).

Observe next that the equation $\varepsilon\tilde{\varepsilon} = 1$ has precisely 6 solutions with $\varepsilon \in \Delta_{H_4}$, namely ± 1 together with $\pm\frac{1}{2}(\pm 1, 0, \tau, \tau - 1)$. Under multiplication, they form the cyclic group C_6, generated by the quaternion $\frac{1}{2}(1, 0, \tau, \tau - 1)$. Clearly, one has $\vartheta(a) = \vartheta(b)$ with $a, b \in \Delta_{H_4}$ if and only if $b = a\varepsilon$ with $\varepsilon \in C_6$, so that a coset decomposition of the 120 roots of Δ_{H_4} with respect to C_6 establishes the second claim. □

Define now, for an arbitrary $\varepsilon \in \mathbb{I}^\times$, the mapping $\eta_\varepsilon = T_\varepsilon\eta T_{\varepsilon^{-1}}$. Since $\eta_{\gamma\varepsilon} = \eta_\varepsilon$ for any unit $\gamma \in \mathbb{Z}[\tau]^\times$, all such maps can be obtained from an $\varepsilon \in \Delta_{H_4}$.

Proposition 5. *The twist maps of $\mathbb{H}(K)$ that map $\mathbb{I}$ into itself are precisely the maps $\eta_\varepsilon = T_\varepsilon\eta T_{\varepsilon^{-1}} = T_{\varepsilon\tilde{\varepsilon}}\eta$, with $\varepsilon \in \Delta_{H_4}$. Equivalently, they are precisely the maps $T_a\eta$ with $a \in \Delta_{A_4}$.*

Proof. By Lemma 6, we know that any twist map is of the form $T_a\eta$ for some $a \in \mathbb{I}^\times$. It is easy to check the commutation relation $\eta T_{a^{-1}} = T_{\widetilde{a}}\eta$, which also implies, via left multiplication by T_a, that

$$T_a\eta T_{a^{-1}} = T_{a\widetilde{a}}\eta.$$

A twist map is an involution (in particular, one has $\eta^2 = \mathrm{Id}$), so that $(T_a\eta)^2 = T_{a(\widetilde{a})^{-1}}$ has to be the identity. Since $T_b = \mathrm{Id} = T_1$ with $b \in \mathbb{I}^\times$ implies $b \in \mathbb{I}^\times \cap K = \mathbb{Z}[\tau]^\times$, the previous condition means $\widetilde{a} = \beta a$ for some $\beta \in \mathbb{Z}[\tau]^\times$. Consequently, $a = (\beta a)^\sim = \beta'\widetilde{a} = \beta'\beta a$, whence $\beta'\beta = 1$. This implies $\beta = \pm\tau^{2m}$ for some $m \in \mathbb{Z}$. Observing that $T_{\tau^m a} = T_a$, we may thus, without loss of generality, replace a by $\tau^m a$, so that the involution condition reduces to $\widetilde{a} = \pm a$.

Next, write $a = \gamma\varepsilon$ with $\gamma \in \mathbb{Z}[\tau]^\times$ and $\varepsilon \in \Delta_{H_4}$, which is possible due to the structure of $\mathbb{I}^\times$. Inserting this into $\widetilde{a} = \pm a$ results in $\gamma^{-1}\gamma' = \pm\varepsilon\tilde{\varepsilon}^{-1}$. Observe next that $\mathbb{Z}[\tau]^\times$ and Δ_{H_4} share only ± 1. Within $\mathbb{Z}[\tau]^{\times}$, $\gamma^{-1}\gamma' = -1$ has no solution, while $\tilde{\varepsilon} = -\varepsilon$ has no solution in Δ_{H_4}, meaning that we must have $\gamma^{-1}\gamma' = 1 = \varepsilon\tilde{\varepsilon}^{-1}$. This leaves us with the condition $\widetilde{a} = a$, which is precisely solved by the 20 elements of Δ_{A_4}, see Eq. (12). All possible twist maps are thus of the form $T_a\eta$ with $a \in \Delta_{A_4}$.

Observing $\varepsilon\tilde{\varepsilon} = \vartheta(\varepsilon)$, the first claim now follows from Lemma 7. □

Theorem 3. *There are exactly* 10 *distinct twist maps of* $\mathbb{H}(K)$ *that map* $\mathbb{I}$ *into itself, which may be written as* η_ε *with* ε *running through the* 10 *positive roots of* Δ_{A_4}.

Moreover, the fixed points of η_ε *are precisely the points of the lattice* $T_\varepsilon(L)$*, each of which is a root lattice of type* A_4.

Proof. The twist maps $T_a\eta$ with $a \in \Delta_{A_4}$ from Proposition 5 form precisely 10 distinct maps because $T_b = T_a$ holds here if and only if $b = \pm a$. Consequently, the restriction to the positive roots of Δ_{A_4} suffices.

From Proposition 1, we know that $L = \{x \in \mathbb{I} \mid \widetilde{x} = x\}$ is the lattice of fixed points of $\eta_1 = \eta$. It is an immediate consequence that η_ε fixes the points of $\varepsilon L \varepsilon^{-1} = T_\varepsilon(L)$. □

Remark 6. There are 60 congruent copies of L within the icosian ring $\mathbb{I}$, each of which must be of the form aLb with $a, b \in \Delta_{H_4}$ due to the structure of $\mathbb{I}^{\times}$. Observing $aL\widetilde{a} = L = -L = -aL\widetilde{a}$ for $a \in \Delta_{H_4}$, it is evident that the stabilizer of L, when seen as a subgroup of $\Delta_{H_4} \times \Delta_{H_4}$, has order 240. Since the order of $\Delta_{H_4} \times \Delta_{H_4}$ is 120^2, the length of the orbit of L under the action of this group is 60, which are the congruent copies. Among them, the 10 lattices of Theorem 3 are precisely the ones that contain 1. They are thus special in the sense that they line up with the arithmetic of $\mathbb{I}$.

Consider $T : \Delta_{H_4} \to \mathrm{Aut}(\mathbb{I})$, $\varepsilon \mapsto T_\varepsilon$, which is a group homomorphism. As $T_\varepsilon = T_{-\varepsilon}$, $T(\Delta_{H_4}) \simeq Y$ is the standard icosahedral group of order 60. If c denotes the conjugation map, $x \mapsto c(x) := \bar{x}$, one has $cT_\varepsilon = T_\varepsilon c$ for all $\varepsilon \in \Delta_{H_4}$, so that

$$\big\langle T(\Delta_{H_4}), c\big\rangle \simeq Y \times C_2 = Y_h$$

is the full icosahedral group of order 120. By Lemma 1, c and η commute as well, while $\eta T_\varepsilon \eta = T_{\tilde{\bar{\varepsilon}}}$ shows that

$$\big\langle T(\Delta_{H_4}), c, \eta\big\rangle \simeq Y_h \rtimes \langle\eta\rangle = \big(Y \rtimes \langle\eta\rangle\big) \times \langle c\rangle.$$

Lemma 8. *One has* $Y \rtimes \langle\eta\rangle \simeq S_5$*, with* S_5 *being the full permutation group of* 5 *elements.*

Proof. Note that Y is isomorphic with the alternating group of 5 elements, which is simple. As $\langle\eta\rangle \simeq C_2$, $Y \rtimes \langle\eta\rangle$ is a C_2-extension of Y, where the automorphism on Y induced by η is $T_\varepsilon \mapsto T_{\tilde{\bar{\varepsilon}}}$, hence not the identity. As the automorphism class group of Y is the cyclic group C_2, there are (up to isomorphism) only two C_2-extensions of Y, namely Y_h and S_5. Since $Y_h \simeq Y \times C_2$, the claim follows. □

Let us add some comments on the geometric meaning of the 10 twist maps, in the setting of root systems, where we focus on the interplay between twist maps that map $\mathbb{I}$ into itself and elements of order 3. Here, we use the natural quadratic form $\mathrm{tr}(x\bar{y})$ mentioned in Remark 2.

The intersection of the fixed points of η and the pure icosians $\mathbb{I}_0 = \{x \in \mathbb{I} \mid x + \bar{x} = 0\}$ is the $\mathbb{Z}$-span of a root system of type A_2. The latter consists of the 6 roots

$$\pm(0,1,0,0),\ \pm\frac{1}{2}(0,\pm 1,\tau-1,-\tau),$$

which is also the intersection of $\mathbb{I}_0$ with our original A_4 root system from Eq. (13).

Now, the twist maps are semilinear involutions of $\mathbb{I}$, each of them a conjugate of our given one, η, by an element of the group $\mathbb{I}^\times$. Since all conjugations by elements of $\mathbb{I}^\times$ are orthogonal transformations that stabilize 1 and $\mathbb{I}_0$, each twist map likewise fixes an A_2 root system which lies both inside its own A_4 and inside $\mathbb{I}_0$.

We can easily see the geometric meaning of these 10 root systems of type A_2. We have noted that each $a \in \Delta_{H_4}$ determines, by conjugation, an orthogonal transformation T_a that preserves $\mathbb{I}$, $\mathbb{I}_0$, and Δ_{H_4}, where $\Delta_{H_4} = \mathbb{I} \cap \mathbb{S}^3$ as mentioned above. In particular, T_a preserves $\mathbb{I}_0 \cap \Delta_{H_4}$, which is a root system of type H_3, with 30 elements, that we denote by Δ_{H_3}. Its convex hull is the icosidodecahedron, a semi-regular polytope with the 30 roots as its vertices, 20 triangular faces, and 12 pentagonal faces. It is the dual of Kepler's famous triacontahedron, see [11, Plate I, Figs. 10 and 12] for details. The 20 triangular faces, which come in centrally symmetric pairs, give rise to 10 axes of 3-fold symmetry—which, in fact, correspond to the elements of order 3 in the symmetry group Y_h of the icosahedron. We shall show that each of these axes has a hexagon of roots in the plane orthogonal to it. These hexagons are precisely the root systems of type A_2 that arise from our twist maps.

To see this, recall that the elements of the form T_a, with $a \in \Delta_{H_4}$, give rise to the symmetry group (of order 120) of the root system Δ_{H_3}, via the mappings $x \mapsto T_a(x)$ and $x \mapsto T_a(\bar{x})$. Here, the first type provides the 60 orientation preserving elements (isomorphic to the alternating group on 5 elements), and the second type the 60 orientation reversing elements. Together, they form Y_h, the symmetry group of the icosahedron (and hence also of the icosidodecahedron and the triacontahedron).

Because all our twist maps are conjugate to one another, it suffices to look at the A_2 lattice indicated above. It has the A_2 root basis

$$\left\{(0,-1,0,0), \frac{1}{2}(0,1,\tau-1,-\tau)\right\},$$

and the product of the two reflections generated by these quaternions is the rotation of order 3 that is a Coxeter element of this root system (the only other one being its inverse, which is obtained by multiplying the two elements in the opposite order). It is the inner automorphism determined by

$$-\frac{1}{2}(0,1,0,0)(0,1,\tau-1,-\tau) = \frac{1}{2}(-1,0,\tau,-\tau') =: z.$$

Of course, z is an element of Δ_{H_4}, and it is easy to see that $z^3 = -1$, so T_z has order 3. These inner automorphisms and their inverses give 20 elements of order 3, which then exhaust the elements of order 3 in Y_h. This establishes the connection between the A_2 root systems in Δ_{H_3} and the rotations of order 3 in the icosahedral group.

Each A_2 inside Δ_{H_3} completes uniquely to an A_4 which contains ± 1. This is easy to see from Eq. (5), in which the four icosians displayed are an A_4 basis which includes the A_2 that we have been using in our above argument.

So, in short, geometrically we can locate the A_4 root systems that are the fixed points of the special twist maps as follows. Each of the great circles through 6 vertices of the icosidodecahedron of roots in $\mathbb{I}_0$ is a root system of type A_2, and it extends uniquely to a root system of type A_4 inside Δ_{H_4} that contains 1.

Acknowledgments

It is a pleasure to thank Ulf Rehmann, Rudolf Scharlau, Rainer Schulze-Pillot and Peter Zeiner for helpful discussions, and Peter Pleasants for carefully reading the manuscript. We thank the referee for a number of helpful suggestions to improve the manuscript. This work was supported by the German Research Council (DFG), within the CRC 701, by EPSRC via grant EP/D058465, and by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] M. Baake, Solution of the coincidence problem in dimensions $d \leqslant 4$, in: R.V. Moody (Ed.), The Mathematics of Long-Range Aperiodic Order, in: NATO ASI Ser. C Math. Phys. Sci., vol. 489, Kluwer, Dordrecht, 1997, pp. 9–42, rev. version, arXiv: math.MG/0605222.

[2] M. Baake, U. Grimm, Bravais colourings of planar modules with N-fold symmetry, Z. Krist. 219 (2004) 72–80, arXiv: math.CO/0301021.

[3] M. Baake, R.V. Moody, Similarity submodules and semigroups, in: J. Patera (Ed.), Quasicrystals and Discrete Geometry, in: Fields Inst. Monogr., vol. 10, AMS, Providence, RI, 1998, pp. 1–13.

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

[5] M. Baake, R.V. Moody, Invariant submodules and semigroups of self-similarities for Fibonacci modules, in: M. de Boissieu, J.-L. Verger-Gaugry, R. Currat (Eds.), Aperiodic '97, World Scientific, Singapore, 1998, pp. 21–27, arXiv: math-ph/9809008.

[6] M. Baake, P. Pleasants, U. Rehmann, Coincidence site modules in 3-space, Discrete Comput. Geom. 38 (2007) 111–138, arXiv: math.MG/0609793.

[7] J.W.S. Cassels, Introduction to the Geometry of Numbers, reprint, Springer, 1997.

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

[9] J.H. Conway, E.M. Rains, N.J.A. Sloane, On the existence of similar sublattices, Canad. J. Math. 51 (1999) 1300–1306.

[10] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, third ed., Springer, New York, 1999.

[11] H.S.M. Coxeter, Regular Polytopes, third ed., Dover, New York, 1973.

[12] M. Heuer, Ähnlichkeitsuntergitter des Wurzelgitters A_4, Diplomarbeit, Univ. Bielefeld, 2006.

[13] M. Koecher, R. Remmert, Hamilton's quaternions, in: H.-D. Ebbinghaus, et al. (Eds.), Numbers, Springer, New York, 1991, pp. 189–220.

[14] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, Coll. Publ., vol. 44, AMS, Providence, RI, 1998.

[15] R.V. Moody, A. Weiss, On shelling E_8 quasicrystals, J. Number Theory 47 (1994) 405–412.

[16] O.T. O'Meara, Introduction to Quadratic Forms, corr. third printing, Springer, Berlin, 1973.

[17] U. Rehmann, private communication, 2006.

[18] R. Scharlau, A structure theorem for weak buildings of spherical type, Geom. Dedicata 24 (1987) 77–84.

[19] R. Scharlau, Unimodular lattices over real quadratic fields, Math. Z. 216 (1994) 437–452.

[20] N.J.A. Sloane, The Online Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.

[21] M.-F. Vignéras, Arithmétique des Algèbres de Quaternions, Lecture Notes in Math., vol. 80, Springer, Berlin, 1980.

[22] P. Zeiner, private communication, 2006.