Coincidence site lattices and coincidence site modules

Habilitationsschrift

Peter Zeiner

Fakultät für Mathematik, Universität Bielefeld, Box 100131, 33501 Bielefeld, Germany

E-mail address: `pzeiner@math.uni-bielefeld.de`

Contents

Preface 5

Chapter 1. Introduction 7
1.1. Motivation and brief historical overview 7
1.2. Scope and Outline of the present work 9
1.3. Preliminaries and notation 11

Chapter 2. Similar sublattices and similar submodules 13
2.1. Basic notions and properties 13
2.2. Similar submodules of related modules 20
2.3. Counting similar sublattices and submodules 21

Chapter 3. Coincidence site lattices and modules 27
3.1. Basic notions and properties 27
3.2. Connection between similar submodules and coincidence site modules 31
3.3. Multiple coincidences 33
3.4. Counting coincidence site lattices and modules 34
3.5. Coincidences of the cubic lattices 42

Chapter 4. Coincidences of the 4-dimensional hypercubic lattices 47
4.1. Centred hypercubic lattice 47
4.2. Primitive hypercubic lattice 58

Chapter 5. Coincidences of the lattice A_4 and the icosian ring 63
5.1. Similar sublattices of A_4 63
5.2. Coincidence site lattices of A_4 67
5.3. Some coincidences of $L[\tau]$ and $\mathbb{I}$ 72
5.4. Coincidences of $\mathbb{I}$ 74
5.5. Equal CSLs for L 84

Chapter 6. Multiple CSLs of the cubic lattices 89
6.1. Basic results 89
6.2. Intersection of two CSLs of the body-centred cubic lattice 91
6.3. Intersection of three CSLs of the body-centred cubic lattice 97
6.4. General MCSLs of the body-centred cubic lattices 102
6.5. Other cubic lattices 104

6.6. Triple Junctions 105

Bibliography 107

Chapter 7. Well-rounded sublattices of planar lattices 111
7.1. Introduction 111
7.2. Tools from the geometry of planar lattices 114
7.3. Well-rounded sublattices of $\mathbb{Z}[\mathrm{i}]$ 116
7.4. Well-rounded sublattices of $\mathbb{Z}[\rho]$ 122
7.5. The general case 124
Appendix 7.A. Some useful results from analytic number theory 132
Appendix 7.B. Asymptotics of similar sublattices 135
Appendix 7.C. The index of BRS sublattices 136
Appendix 7.D. Epstein's ζ-function 138
Acknowledgements 140

Bibliography 141

Chapter 8. Supplement to "Well-rounded sublattices of planar lattices" 143
8.1. Explicit expressions for BRS lattices 143
8.2. Asymptotic behaviour — Introduction 144
8.3. Similar Sublattices 145
8.4. Well-rounded sublattices 148
Appendix 8.A. Some formulas 157

Bibliography 175

Preface

Coincidence site lattices (CSLs) are an important tool in crystallography to describe grain boundaries in crystals. Hence, CSLs of 3-dimensional lattices were intensively studied by crystallographers in the sixties and seventies of the last century.

After the discovery of quasicrystals by D. Shechtman in 1982, it became necessary to generalise this concept, and the notion of coincidence site modules (CSMs) was introduced. Mathematicians got interested in the subject in the nineties and CSMs and CSLs were investigated not only in dimensions $d \leq 3$, but also in higher dimensions.

The scope of the present work is to summarise part of the contributions of the author to this field. It includes some general results on CSLs and CSMs and their relationship to similar sublattices and submodules, respectively. Another topic are results on concrete lattices in dimensions $d = 3$ and 4, including the coincidence problem for the 4-dimensional hypercubic lattices and the root lattice A_4 and the icosian ring as well as the problem of multiple coincidences for the 3-dimensional cubic lattices. This is complemented by an article on well-rounded sublattices of planar lattices, which have a lot of connections to planar CSLs.

The author wants to thank all people who have helped to improve the present work. In particular, he wants to thank M. Baake, R. Scharlau, C.Huck, M.J. Loquias, M. Heuer, and S. Glied for interesting discussions on various subjects.

Finally, he acknowledges support by the German Research Foundation (DFG), within the CRC 701.

CHAPTER 1

Introduction

1.1. Motivation and brief historical overview

The study of coincidence site lattices – and more generally – coincidence site modules, is motivated by its use in crystallography. Single crystals can be idealised as periodic arrangements of atoms or molecules. They can be modelled in various ways, the simplest one is to model them as periodic point sets. This view is enough for our purposes, but it is not enough for describing physical properties. Hence, crystals are often modelled as periodic functions or periodic measures. In any case, the symmetry of (ideal) crystals is described by space groups, whose subgroup of translations are lattices in $\mathbb{R}^3$.

However, real crystals are neither infinite nor perfectly periodic. They may have various defects, atoms may be missing or additional atoms may be present, an atom may be replaced by an atom of a different chemical element, they may be distorted - just to name a few. But it is not these imperfections we are interested in. Real crystals are very often not single crystals, but consist of several crystal grains, each of which is more or less periodic. Typically, these crystal grains have the same chemical composition, but they are rotated with respect to each other. Hence, each grain has to be described by its own symmetry group and its own lattice.

But these lattices are not independent of each other, in fact, they are rotated copies of each other. Moreover, it turns out that certain angles between different grains are preferred, namely those which correspond to rotations such that the lattices of the two grains involved have a common sublattice of small index. This gave rise to the notion of a coincidence site lattice (CSL), which is the intersection of a lattice with a rotated copy of itself such that the resulting lattice is a lattice of full rank. Thus, CSLs are used to characterise the relative orientation of crystal grains and to analyse the so-called grain boundaries, which are the planes at which two grains meet.

It was Friedel in 1911 who first recognised the usefulness of coincidence site lattices in describing and classifying grain boundaries of crystals [**28**]. Later on, in 1949, analogous ideas were used by Kronberg and Wilson [**48**]. But it was not until the mid sixties that CSLs became more popular. In fact, the widespread use of CSLs was triggered by a famous paper by Ranganathan in 1966 [**58**]. Here, the famous formula for the coincidence index for cubic lattices was derived.

A lot of papers followed in the later sixties and seventies, mainly concentrating on the cubic lattices, including the important contributions by H. Grimmer [**35, 36, 37, 39**]. Later on, other lattices with high symmetry were analysed as well, including certain hexagonal lattices [**40, 38**]. The activities of these days culminated in the two monographs of W. Bollmann [**18, 19**].

The discovery of quasicrystals in 1982 by D. Shechtman [**64**] gave rise to a renewed interest in CSLs, generalising the concept of CSLs for the needs of quasicrystals [**59, 67, 68, 56, 57, 69**], which led to the concept of coincidence site modules (CSMs); for more information on the mathematical theory of quasicrystals see [**7**]. The more complex situation of quasicrystals made a rigorous mathematical formulation of the coincidence problem necessary [**4**] and triggered a series of mathematical papers on this subject. Coincidences of several prominent modules were analysed, including planar modules with n-fold symmetry [**55**] and certain modules in 3-dimensional space [**11**].

Interest was no longer restricted to the 3-dimensional space. The 4-dimensional hypercubic lattices [**4, 74, 72, 16**], and the A_4-lattice [**8, 16, 43, 42**] have been studied in detail. Results in n dimensions are still sparse, but there are some results on the possible coincidence indices for the n-dimensional hypercubic lattices [**79**]. In addition, there are some results on the structure of the group of coincidence isometries for rational lattices. In particular, an analogue of the Cartan-Dieudonné theorem was proved for lattices [**80**] and later for modules [**44**].

Most of the explicit results for lattices and modules in dimensions $d \leq 4$ are obtained by number theoretical methods involving quadratic number fields (in dimension $d = 2$) and quaternion algebras (in dimension $d = 3$ and 4). An alternative approach using Clifford algebras has lead to some results in the Euclidean plane [**61**] and the hyperbolic plane [**62**].

So far, we have discussed only CSLs that are the intersection of two lattices. More generally, one can consider the intersection of an arbitrary number of rotated lattices – the so-called multiple CSLs. This problem is, in general, more difficult than the corresponding problem for (ordinary) CSLs. Nevertheless, it has been analysed for planar modules with n-fold symmetry [**6**] and for cubic lattices [**75, 15**]. Multiple CSLs have an application in crystallography as well, in connection with so-called triple, or more generally, multiple junctions [**30, 29, 31**]. These are lines or points where three or more crystal grains meet.

Applications of CSLs are not confined to crystallography. In fact, they were also applied in coding theory in connection with so-called lattice quantizers [**24, 65**]. Here, the idea is to express complicated high dimensional lattices as intersections of simpler lattices, e.g. hypercubic lattices or direct sums of low dimensional lattices. Moreover, similar sublattices and CSLs of the hexagonal lattice and the A_4 lattice have been applied to algorithms in practice [**2, 1, 3**].

The concept of CSLs has been generalised in several other ways. We have motivated the CSLs by grains that are rotated with respect to each other, i.e., they are linked by a linear isometry. More generally, one may consider grains that are linked by an affine isometry. This has been done in [**32, 26**]. Correspondingly, affine coincidences, as well as coincidences of shifted lattices and crystallographic point packings have been studied in [**49, 52, 50**].

Furthermore, coincidences of coloured lattices have been considered [**51, 50, 53**]. They occur naturally if one wants to compare the coincidence problem of two lattices, where one is a sublattice of the other one.

Coincidence site lattices are connected to various other special sublattices. In two dimensions, there exist connections to well-rounded sublattices [**77, 13**]. Furthermore, there exists an important connection between similar sublattices and CSLs. In particular, the group of coincidence isometries is a normal subgroup of the group of similarity rotations; compare [**34**] for lattices and [**33, 78**] for modules.

1.2. Scope and Outline of the present work

The aim of the present work is to present part of the contributions of the author to the topic of coincidence site lattices in a uniform framework. It is partly based on articles that have been published already, extends some of them and adds new material that is so far unpublished.

We start with a chapter on similar submodules. Its aim is not to give an exhaustive treatment of this subject, but rather to provide the necessary tools to prove the connections with coincidence site modules in Chapter 3. Thus, we do not include the various results obtained for special lattices here. In particular, we do not mention the important results on the existence of similar sublattices for rational lattices obtained in [**46**]. Similarly, we omit the explicit results for planar lattices and modules that can be found in [**5, 12**]. Results on the similar sublattices of A_4 and the similar submodules of the icosian ring are summarised briefly in Chapter 5, as far as we need them for the discussions of the CSLs. For further details we refer to [**9**] and [**10**], respectively.

In Chapter 3 we discuss the general properties of coincidence site modules. Some of them are straightforward generalisations of the corresponding results obtained in [**4**], whereas other ones need different techniques to handle them. As an example, we mention the proof of the fact that the coincidence indices of an isometry and its inverse are the same, which can be carried out by a simple geometric argument in the case of lattices, whereas we need arguments from algebra and number theory to prove the corresponding statement for modules. This chapter also includes the generalisations of [**76**] and extends results from [**78**]. One of the highlights is the connection between similar submodules and coincidence site modules as expressed in Theorem 3.2.2. The corresponding results for lattices had been proven in [**34**] and for a special class of modules in [**33**]. The chapter ends with a summary of the main results of the CSLs of the cubic lattices [**4, 73**], which we rephrase in a way which is most suited for our analysis of the multiple CSLs in Chapter 6.

In Chapter 4 and Chapter 5 we discuss the coincidence problem for several examples in 4 dimensions, including the 4-dimensional hypercubic lattices, the lattice A_4 and the icosian ring. For all these examples we can calculate the coincidence index explicitly and express it in terms of quaternions. We determine an explicit expression for the CSLs and CSMs, respectively, which allows us to formulate a criterion when two CSLs (CSMs) are equivalent.

We count the number of coincidence isometries and CSLs (CSMs) of a given index, for which explicit formulas exist. We construct the generating functions for these counting functions in the form of a Dirichlet series. These Dirichlet series turn out to have nice analytic properties, which allows us to find the asymptotic growth rates for the number of coincidence isometries and CSLs via Delange's theorem 7.A.1.

The methods in both chapters are very similar. In both cases a principal ideal ring of quaternions is employed to get the results. For the hypercubic lattices, we use the Hurwitz ring of integers, whereas we make use of the icosian ring to study the A_4-lattice. Some of the results of Chapter 4 have already been published in [**74**]. However, Chapter 4 is not just an extension of (part of) the results of [**74**], but we have opted to completely change the presentation so that it matches the discussion of the A_4-lattice and the icosian ring in Chapter 5.

Chapter 5 extends the results of [**8**] and [**43**] on the A_4-lattice and adds the missing proofs. For some of the details, we refer to [**42**].

In Chapter 6 we discuss the multiple CSLs of cubic lattices. This chapter extends results of [**75**] and [**15**]. In particular, we count all double and multiple CSLs and express the results in terms of Dirichlet series, which allows us to calculate the asymptotic behaviour for the counting function also in these cases. Moreover, we get the remarkable result that any multiple CSL is in fact a double or triple CSL. We conclude this chapter with an application of the multiple CSLs to triple junctions; compare [**30**].

Chapters 7 and 8 are a reprint of [**13**] and its supplementary material [**71**]. Thus, both chapters have their own list of references, whereas all other chapters share a common list of references, which can be found at the end of Chapter 6. In Chapter 7, we discuss and count well-rounded sublattices of planar lattices. Here, a lattice in $\mathbb{R}^d$ is called well-rounded if the non-zero lattice vectors of minimal length span $\mathbb{R}^d$. In the case of planar lattices, this is equivalent to the property that the non-zero lattice vectors of minimal length span the lattice.

We have included this paper in the present work since there are many connections between CSLs and well-rounded sublattices in the planar case. First, a planar lattice has well-rounded sublattices if and only if there exists a coincidence reflection, i.e., if there exists a CSL that is generated by a reflection. Moreover, the problem of finding all well-rounded sublattices can be reduced to finding all coincidence reflections and their corresponding CSLs. If a lattice has only one CSL, the asymptotic growth rate of the number of well-rounded sublattices does not depend on the details of the lattice, but only depends on the coincidence index of this particular CSL.

Although counting well-rounded sublattices is more difficult than counting CSLs, and the corresponding expressions are less explicit, we still can determine the asymptotic growth rates. In case of the square lattice and the hexagonal lattice, we are even able to calculate the first error term explicitly. This cannot be achieved by an application of Delange's theorem, but by methods involving the Dirichlet hyperbola method. The explicit calculations are rather lengthy and are presented in Chapter 8. The same methods allow to calculate the first order corrections for the asymptotic behaviour of the number of CSLs for the square lattice and the hexagonal lattice, whose result will be published in [**14**].

1.3. Preliminaries and notation

The basic objects of the present work are lattices and modules. By a lattice we mean a discrete, cocompact subgroup $\varGamma$ of $\mathbb{R}^d$. As any lattice has a basis $\{b_1, \dots, b_d\}$, the lattice $\varGamma$ is the $\mathbb{Z}$-span of these basis vectors, denoted as $\varGamma = \langle b_1, \dots, b_d \rangle_{\mathbb{Z}}$. A sublattice $\varGamma'$ is a subgroup of $\varGamma$ that is a lattice itself. This means that we consider only (sub)lattices of full rank, i.e., lattices, whose $\mathbb{R}$-span is $\mathbb{R}^d$.

If we do not specify otherwise, a module M is always to be understood to be a finitely generated free $\mathbb{Z}$-module embedded in $\mathbb{R}^d$, such that its $\mathbb{R}$-span is $\mathbb{R}^d$, in other words, $\mathbb{R} \otimes_{\mathbb{Z}} M = \mathbb{R}^d$. The rank of M is the cardinality of any basis of M. In other words, by a module of rank k in dimension $d \leq k$, we mean the $\mathbb{Z}$-span $M = \langle b_1, \dots, b_k \rangle_{\mathbb{Z}}$ of $k \geq d$ vectors $b_i \in \mathbb{R}^d$ that span $\mathbb{R}^d$ and are independent over $\mathbb{Q}$. If not stated otherwise, a submodule is to be understood as a submodule of full rank, i.e., we consider only submodules $N \subseteq M$ such that M and N have the same rank. In this terminology, a lattice $\varGamma$ in $\mathbb{R}^d$ is a module of rank $k = d$.

Occasionally, we will need modules $M \subseteq \mathbb{R}^d$ over more general rings $R \subseteq \mathbb{R}$. In this case, we always specify the ring R and we call M an R-module. Here, we do not require M to be a free R-module. Nevertheless, they usually are embedded in $\mathbb{R}^d$, they are finitely generated and span $\mathbb{R}^d$.

As a special variant of a module we will sometimes use the notion of an $\mathcal{S}$-lattice. Let $\mathcal{S} \subset \mathbb{R}$ be a ring with identity that is also a finitely generated, free $\mathbb{Z}$-module. Then we call $M \subset \mathbb{R}^d$ an $\mathcal{S}$-lattice, if there exist d linearly independent vectors $b_i \in \mathbb{R}^d$ such that M is the $\mathcal{S}$-span of $\{b_1, \dots, b_d\}$, i.e., $M = \langle b_1, \dots, b_d \rangle_{\mathcal{S}}$.

The symmetry group of a module M shall be called $\mathrm{O}(M)$. This is the group of all $R \in \mathrm{O}(d, \mathbb{R})$ such that $RM = M$. Clearly, we have $\mathrm{O}(M) \subset \mathrm{O}(d, \mathbb{R})$.

In our discussion of lattices in dimensions 3 and 4, quaternions will play a crucial role. We will introduce them together with their most important properties in Section 3.5. Additional properties may be introduced later, wherever it seems appropriate. Nevertheless, we want to make some remarks here.

Two rings of quaternions will be of crucial importance, namely the ring of Hurwitz quaternions $\mathbb{J}$ and the icosian ring $\mathbb{I}$. Both rings are principal ideal rings, i.e., all right (left) ideals are principal right (left) ideals. Thus, for any two right ideals $a\mathbb{J}$ and $b\mathbb{J}$ there exist quaternions g and m such that $g\mathbb{J} = a\mathbb{J} + b\mathbb{J}$ and $m\mathbb{J} = a\mathbb{J} \cap b\mathbb{J}$. These two quaternions g and m are unique up to multiplication by a unit quaternion from the right. We call g a greatest common left divisor of a and b, and m a least common right multiple of a and b, in symbols $g = \mathrm{gcld}(a, b)$ and $m = \mathrm{lcrm}(a, b)$. As g and m are unique only up to a unit, these equations only make sense as a shorthand notation for the corresponding equation of ideals $g\mathbb{J} = \mathrm{gcld}(a, b)\mathbb{J}$ or as equations of quaternions that hold only up to a multiplication by a unit quaternion from the right. In some cases, we may choose a particular g or m. In these cases, the equations involving them are considered to hold exactly.

In principal, we could write all equations involving a greatest common left divisor or a least common right multiple as equations of ideals. Nevertheless, we prefer the short hand notation $g = \operatorname{gcld}(a, b)$. The reason is that we sometimes need a particular choice of a gcld or lcrm. In particular, we use quaternions to parametrise rotations, and the rotations depend on the actual quaternion rather than on the corresponding ideal.

Clearly, all considerations are also valid for the greatest common right divisor gcrd and the least common left multiple lclm.

CHAPTER 2

Similar sublattices and similar submodules

2.1. Basic notions and properties

Since coincidence site lattices are closely related to similar sublattices (SSLs for short), it is worthwhile to consider similar sublattices first. We start by recalling some important notions.

Two modules $M_1, M_2 \subseteq \mathbb{R}^d$ are called commensurate (in symbols $M_1 \sim M_2$) if their intersection $M_1 \cap M_2$ has finite index in both M_1 and M_2. Clearly, M_1 and M_2 can only be commensurate if they have the same rank. Once we know that two modules in $\mathbb{R}^d$ have the same rank, the situation becomes easier as we can characterise commensurateness in several ways, which we will use freely in the following:

Lemma 2.1.1. *Let $M_1, M_2 \subseteq \mathbb{R}^d$ be modules of rank k. Then the following are equivalent:*

(1) *M_1, M_2 are commensurate.*
(2) *$M_1 \cap M_2$ has finite index in both M_1 and M_2.*
(3) *$M_1 \cap M_2$ has finite index in M_1 or in M_2.*
(4) *There exist (positive) integers m_1 and m_2 such that $m_1 M_1 \subseteq M_2$ and $m_2 M_2 \subseteq M_1$.*
(5) *There exists an integer m such that $mM_1 \subseteq M_2$ or $mM_2 \subseteq M_1$.*
(6) *$M_1 \cap M_2$ has rank k.*

As an immediate consequence we obtain by applying (4) several times:

Lemma 2.1.2. *Commensurateness is an equivalence relation.*

An important example of commensurate modules are similar submodules. Recall that a linear map $f : \mathbb{R}^d \to \mathbb{R}^d$ is called a *similarity transformation* if it is of the form $f = \alpha R$, where R is an isometry and $\alpha \in \mathbb{R}^+$. Two modules are called *similar* if there exists a similarity transformation mapping one module onto the other. Clearly, similarity of modules is an equivalence relation.

Definition 2.1.1. A similarity transformation mapping a module $M \in \mathbb{R}^d$ onto a submodule of M is called a *similarity transformation of M*. A submodule $M_1 \subseteq M$ is called a *similar submodule (SSM)* of M if it is similar to M.

The similarity transformations of M form a monoid. In fact, as similarity transformations are invertible, they canonically generate a group, which is precisely the group of all similarity transformations mapping M onto a module commensurate to M. However, we are less interested in the similarity transformations $f = \alpha R$ themselves, but rather on their rotational parts R and their inflation factors α. We first mention

THEOREM 2.1.3. *Let*

$$\mathrm{OS}(M) := \{R \in \mathrm{O}(d,\mathbb{R}) \mid \exists \alpha \in \mathbb{R}^+ \textit{ such that } \alpha RM \subseteq M\} \tag{2.1}$$

be the set of all similarity isometries *of M. Then* $\mathrm{OS}(M) \subseteq \mathrm{O}(d,\mathbb{R})$ *is a group.*

PROOF. For any $R_1, R_2 \in \mathrm{OS}(M)$ there exist $\alpha_1, \alpha_2 \in \mathbb{R}^+$ such that $\alpha_1 R_1 M \subseteq M$ and $\alpha_2 R_2 M \subseteq M$, hence $\alpha_1\alpha_2 R_1 R_2 M \subseteq \alpha_1 R_1 M \subseteq M$, which proves $R_1R_2 \in \mathrm{OS}(M)$. It remains to show that $R^{-1} \in \mathrm{OS}(M)$ for any $R \in \mathrm{OS}(M)$. There exists an $\alpha \in \mathbb{R}^+$ such that $\alpha RM \subseteq M$ and hence $M \subseteq \frac{1}{\alpha}R^{-1}M$. As M and $\frac{1}{\alpha}R^{-1}M$ are commensurate, by Lemma 2.1.1 there exists a positive integer m such that $\frac{m}{\alpha}R^{-1}M \subseteq M$, which indeed shows $R^{-1} \in \mathrm{OS}(M)$. □

Similar modules have isomorphic OS-groups, in particular their OS-groups are conjugated subgroups of $\mathrm{O}(d,\mathbb{R})$:

LEMMA 2.1.4. *Let M and N be similar modules with $N = \alpha RM$. Then*

$$\mathrm{OS}(N) = R\ \mathrm{OS}(M)R^{-1}. \tag{2.2}$$

Let us take a look at the scaling factors α. We first define

$$\mathrm{Scal}_M(R) := \{\alpha \in \mathbb{R} \mid \alpha RM \subseteq M\} \tag{2.3}$$

and

$$\mathrm{scal}_M(R) := \{\alpha \in \mathbb{R} \mid \alpha RM \sim M\}, \tag{2.4}$$

where we have allowed nonpositive values for α to get "nicer" sets. $\mathrm{Scal}_M(R)$ is nonempty for all R as $0 \in \mathrm{Scal}_M(R)$. More importantly, $\mathrm{Scal}_M(R)$ is non-trivial if and only if $R \in \mathrm{OS}(M)$, i.e. $\mathrm{Scal}_M(R) \neq \{0\}$ if and only if $R \in \mathrm{OS}(M)$.

Clearly, we expect that the sets of scaling factors are intimately related for similar modules. In fact, we immediately get the following result.

LEMMA 2.1.5. *Let M and N be similar modules with $N = \alpha RM$. Then*

$$\mathrm{Scal}_N(S) = \mathrm{Scal}_M(R^{-1}SR) \tag{2.5}$$

$$\mathrm{scal}_N(S) = \mathrm{scal}_M(R^{-1}SR). \tag{2.6}$$

For a lattice Γ, we immediately see $\alpha^d \in \mathbb{Z}$ for any $\alpha \in \mathrm{Scal}_\Gamma(R)$, as the index $[\Gamma : \alpha R\Gamma]$ is given by $[\Gamma : \alpha R\Gamma] = |\det(\alpha R)| = \alpha^d$, if α is non-zero. Furthermore, an application of Lemma 2.1.1 gives $\alpha^d \in \mathbb{Q}$ for any $\alpha \in \mathrm{scal}_\Gamma(R)$. These results can be generalised for $\mathcal{S}$-lattices, see [**33**] for details. Note that $\mathcal{S}$-lattices have been called $\mathcal{S}$-lattices in [**33**]. In particular, for any $\alpha \in \mathrm{Scal}_M(R)$, we have $\alpha^d \in \mathcal{S}$, which follows from the fact that αR is similar to a matrix with entries in $\mathcal{S}$ only. Likewise, for any $\alpha \in \mathrm{scal}_M(R)$, we have $\alpha^d \in K$, where K is the field of fractions of $\mathcal{S}$.

Our first goal is to show that every $\alpha \in \mathrm{Scal}_M(R)$ is some algebraic integer. To this end, we consider $\mathrm{Scal}_M(R)$ for the identity operation $R = E$ first. For any lattice $\mathit{\Gamma}$, we have $\mathrm{Scal}_{\mathit{\Gamma}}(E) = \mathbb{Z}$, and if M is an $\mathcal{S}$-lattice, we get $\mathrm{Scal}_M(E) = \mathcal{S}$. In both cases, $\mathrm{Scal}_M(E)$ is a ring of algebraic integers and, indeed, this is a general property of $\mathrm{Scal}_M(E)$.

THEOREM 2.1.6. *Let $M \subseteq \mathbb{R}^d$ be a module of rank k. $\mathrm{Scal}_M(E)$ is a ring of algebraic integers. In particular, $\mathrm{Scal}_M(E)$ is a ring with identity and it is a finitely generated free $\mathbb{Z}$-module, whose rank is a divisor of k and is at most $\frac{k}{d}$.*

PROOF. If $\alpha, \beta \in \mathrm{Scal}_M(E)$, then $\alpha M \subseteq M$ and $\beta M \subseteq M$. It follows $(\alpha+\beta)M \subseteq \alpha M + \beta M \subseteq M$ and $(\alpha\beta)M \subseteq \alpha M \subseteq M$, hence $\alpha+\beta$ and $\alpha\beta$ are in M, which proves that $\mathrm{Scal}_M(E)$ is a ring. Due to $M \subseteq M$ we have $1 \in \mathrm{Scal}_M(E)$. Clearly, $\mathrm{Scal}_M(E)$ is also a $\mathbb{Z}$-module. Let $v_1, \dots v_d$ be d linearly independent vectors in M. For each fixed i, $M_i := \{\alpha v_i \mid \alpha \in \mathrm{Scal}_M(E)\}$ is a $\mathbb{Z}$-submodule of M, which is isomorphic to $\mathrm{Scal}_M(E)$. As M_i is a submodule of M, it is a finitely generated free $\mathbb{Z}$-module, and so is $\mathrm{Scal}_M(E)$. Thus $\mathrm{Scal}_M(E)$ is a ring of algebraic integers. All M_i have the same rank, and as the direct sum $M_1 \oplus \ldots \oplus M_d$ is a submodule of M, each M_i has rank at most $\frac{k}{d}$, and so has $\mathrm{Scal}_M(E)$.

Let m be the rank of $\mathrm{Scal}_M(E)$ over $\mathbb{Q}$ and let K be the field of fractions of $\mathrm{Scal}_M(E)$. Then K is a vector space over $\mathbb{Q}$ with dimension m. The vector space $\mathbb{Q} \otimes_{\mathbb{Z}} M$ has dimension k over $\mathbb{Q}$, and viewed as vector space over K it has dimension $\frac{k}{m}$, which finally shows that m indeed divides k. □

In the proof, we encountered the module $\alpha M + \beta M$. In general, this is not a similar submodule. As an example consider a ring of algebraic integers $S \subseteq \mathbb{R}$ that is not a PID. Then the similar submodules of $M = S$ are exactly the principal ideals of S, but the sum of two principal ideals is in general not a principal ideal. However, if $M = \mathit{\Gamma}$ is a lattice, then $\alpha\mathit{\Gamma} + \beta\mathit{\Gamma} = \gcd(\alpha,\beta)\mathit{\Gamma}$ is a similar sublattice.

Clearly, M can be also viewed as a $\mathrm{Scal}_M(E)$-module, and as such it is still finitely generated, but it is not necessarily a free $\mathrm{Scal}_M(E)$-module, unless $\mathrm{Scal}_M(E)$ is a PID. As an example, consider $M = \mathbb{Z}[2\sqrt{2}] \oplus \mathrm{i}\mathcal{A} \subseteq \mathbb{C}$, where $\mathcal{A} = 2\mathbb{Z}[2\sqrt{2}] + (2\sqrt{2})\mathbb{Z}[2\sqrt{2}]$ is an ideal of $\mathbb{Z}[2\sqrt{2}]$ with index $\left[\mathbb{Z}[2\sqrt{2}] : \mathcal{A}\right] = 2$, but it is not a principal ideal. Here, $\mathrm{Scal}_M(E) = \mathbb{Z}[2\sqrt{2}]$, but M is not a free $\mathbb{Z}[2\sqrt{2}]$-module.

Since $\alpha M \sim M$ if and only if there is a positive integer m such that $m\alpha M \subseteq M$ we obtain

COROLLARY 2.1.7. *Let $M \subseteq \mathbb{R}^d$ be a free $\mathbb{Z}$-module of finite rank. Then $\mathrm{scal}_M(E) \cup \{0\}$ is the field of fractions of $\mathrm{Scal}_M(E)$.*

An immediate consequence of this result is the following lemma, which was first proved for the special case of $\mathcal{S}$-lattices in [**33**].

THEOREM 2.1.8. *Let α be an arbitrary element of $\mathrm{scal}_M(R)$. Then*

$$\mathrm{scal}_M(R) = \alpha\,\mathrm{scal}_M(E). \tag{2.7}$$

Proof. Let $\alpha, \beta \in \operatorname{scal}_M(R)$. Hence $\alpha RM \sim \beta RM$, which is equivalent to $\frac{\beta}{\alpha}M \sim M$. But the latter is equivalent to $\frac{\beta}{\alpha} \in \operatorname{scal}_M(E)$, hence $\operatorname{scal}_M(R) \subseteq \alpha \operatorname{scal}_M(E)$. The reverse inclusion follows from $\alpha\gamma RM \sim \gamma M \sim M$ for all $\gamma \in \operatorname{scal}_M(E)$. □

The situation is different for $\operatorname{Scal}_M(R)$. We have the following result.

Theorem 2.1.9. $\operatorname{Scal}_M(R)$ *is a finitely generated, free* $\mathbb{Z}$*-module for any similarity isometry* R *of* M*. Moreover,* $\beta \operatorname{Scal}_M(R) \subseteq \operatorname{Scal}_M(R)$ *for any* $\beta \in \operatorname{Scal}_M(E)$ *and, hence,* $\operatorname{Scal}_M(R)$ *is also a finitely generated* $\operatorname{Scal}_M(E)$*-module.*

If $\operatorname{Scal}_M(E)$ *is a PID,* $\operatorname{Scal}_M(R)$ *is a free* $\operatorname{Scal}_M(E)$*-module of rank* 1*, i.e. there exists an* $\alpha \in \operatorname{Scal}_M(R)$ *such that* $\operatorname{Scal}_M(R) = \alpha \operatorname{Scal}_M(E)$*.*

Proof. Let $\alpha, \beta \in \operatorname{Scal}_M(R)$, $n \in \mathbb{Z}$. Then $(\alpha + \beta)RM \subseteq \alpha RM + \beta RM \subseteq M$ and $n\alpha RM \subseteq \alpha RM \subseteq M$ show that $\operatorname{Scal}_M(R)$ is closed under addition and scalar multiplication, whence it is a $\mathbb{Z}$-module. Let $x \in M$. Then $\operatorname{Scal}_M(R)$ is isomorphic to $\operatorname{Scal}_M(R)x$, which is a finitely generated free $\mathbb{Z}$-module, since it is a submodule of M.

Let $\alpha \in \operatorname{Scal}_M(R)$ and $\beta \in \operatorname{Scal}_M(E)$. Then $\alpha\beta RM \subseteq \beta M \subseteq M$ shows $\alpha\beta \in \operatorname{Scal}_M(R)$. Since α was arbitrary, this means $\beta \operatorname{Scal}_M(R) \subseteq \operatorname{Scal}_M(R)$. Thus $\operatorname{Scal}_M(R)$ can be viewed as a $\operatorname{Scal}_M(E)$-module, which is finitely generated as it is already finitely generated over $\mathbb{Z}$.

Assume $\operatorname{Scal}_M(E)$ is a PID. Let $0 \neq \gamma \in \operatorname{Scal}_M(R)$. Then $\frac{1}{\gamma} \operatorname{Scal}_M(R) \subseteq \operatorname{scal}_M(E)$, and as it is a finitely generated $\operatorname{Scal}_M(E)$-module, it is a fractional ideal of $\operatorname{Scal}_M(E)$. Since $\operatorname{Scal}_M(E)$ is a PID, there exits a $\beta \in \operatorname{scal}_M(E)$ such that $\frac{1}{\gamma} \operatorname{Scal}_M(R) = \beta \operatorname{Scal}_M(E)$, i.e., $\operatorname{Scal}_M(R) = \alpha \operatorname{Scal}_M(E)$, where $\alpha = \beta\gamma$. □

Let us consider our previous example $M = \mathbb{Z}[2\sqrt{2}] \oplus \mathrm{i}\mathcal{A} \subseteq \mathbb{C}$ again. Let R be the counterclockwise rotation through $\frac{\pi}{2}$, which is represented by $R = \mathrm{i}$. Here, $\operatorname{Scal}_M(\mathrm{i}) = \mathcal{A}$ is an ideal of $\operatorname{Scal}_M(E) = \mathbb{Z}[2\sqrt{2}]$, but not a principal ideal of $\operatorname{Scal}_M(E)$, which shows that in general $\operatorname{Scal}_M(R)$ cannot be written as $\alpha \operatorname{Scal}_M(E)$. In particular, $\operatorname{Scal}_M(\mathrm{i})$ is not free over $\operatorname{Scal}_M(E)$. In fact, $\operatorname{Scal}_M(R)$ is in general not an ideal (nor a fractional ideal) of $\operatorname{Scal}_M(E)$. Indeed, we can modify our example a little and consider $M = \mathbb{Z}[2\sqrt{2}] \oplus \mathrm{i}\sqrt{n}\,\mathcal{A} \subseteq \mathbb{C}$ instead, where n is some odd positive integer. Then $\operatorname{Scal}_M(\mathrm{i}) = \sqrt{n}\,\mathcal{A}$ and $\operatorname{Scal}_M(\mathrm{i}) \cap \operatorname{Scal}_M(E) = \varnothing$.

Theorem 2.1.10. *Any* $\alpha \in \operatorname{Scal}_M(R)$ *is an algebraic integer. If* M *has rank* $k \geq 2$*, then* α *has degree at most* $k(k-1)$*.*

Proof. As R is an orthogonal matrix, its eigenvalues are unimodular numbers $e^{\mathrm{i}\varphi}$. Hence the eigenvalues of αR are of the form $\alpha e^{\mathrm{i}\varphi}$, and thus it is sufficient to show that the eigenvalues of αR are algebraic integers. As αR maps the module M of rank k into itself, there exists a monic polynomial P of degree k with integral coefficients such that $P(\alpha R) = 0$ (just take the characteristic polynomial of its k-dimensional integral representation). Hence $P(\alpha e^{\mathrm{i}\varphi}) = 0$ and $\alpha e^{\mathrm{i}\varphi}$ is indeed an algebraic integer. In fact, its degree is at most k, from which we infer that α has degree at most $k(k-1)$. □

As mentioned above, $\alpha \in \mathrm{Scal}_M(R)$ is a d-th root of an integer in case of a lattice, and it is a d-th root of an element of $\mathcal{S}$ in case of $\mathcal{S}$-lattices. For general modules M, however, Theorem 2.1.10 is the best we can get. This is illustrated by the following example.

EXAMPLE 2.1.1. Let $\eta = e^{\frac{\mathrm{i}\pi}{3}} \sqrt[3]{\tau} - e^{-\frac{\mathrm{i}\pi}{3}} \frac{1}{\sqrt[3]{\tau}}$, where $\tau = \frac{1+\sqrt{5}}{2}$ is the golden mean. Then $M = \mathbb{Z}[\eta]$ is a free $\mathbb{Z}$-module of rank 3, as η satisfies $\eta^3 + 3\eta - 1 = 0$. Here, $\mathrm{Scal}_M(E) = \mathbb{Z}$. Clearly, $\eta = |\eta| \frac{\eta}{|\eta|}$ is a similarity transformation with $\mathrm{Scal}_M(\frac{\eta}{|\eta|}) = |\eta| \,\mathrm{Scal}_M(E) = |\eta|\mathbb{Z}$. Since $|\eta| = \sqrt{\tau^{2/3} + \tau^{-2/3} + 1}$ has the minimal polynomial $x^6 - 3x^4 - 1$, it is not an n-th root of a rational integer. In particular, $|\eta|$ has degree $6 = 3 \cdot 2$, which shows that the upper bound on the degree of α in Theorem 2.1.10 is optimal. Finally, we mention that η is a symmetry operation of M as $\eta M = M$.

As $\mathrm{OS}(M)$ is a group, we expect that there should be some multiplication law for the set of scaling factors as well. Indeed, using the fact that commensurateness is an equivalence relation once again, we obtain

LEMMA 2.1.11. *For any $R, S \in \mathrm{OS}(M)$*

$$\mathrm{scal}_M(R)\,\mathrm{scal}_M(S) = \mathrm{scal}_M(RS). \tag{2.8}$$

For further reference we also mention the special case $S = R^{-1}$.

LEMMA 2.1.12. *For any $R \in \mathrm{OS}(M)$*

$$\mathrm{scal}_M(R^{-1})\,\mathrm{scal}_M(R) = \mathrm{scal}_M(E) \tag{2.9}$$

The previous lemmas together with $\mathrm{scal}_M(R)\,\mathrm{scal}_M(E) = \mathrm{scal}_M(R)$ show that $\{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$ carries a natural group structure. In addition, these lemmas show that there exists a natural group homomorphism from $\mathrm{OS}(M)$ onto $\{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$. Moreover, Theorem 2.1.8 shows that there is a isomorphism from $\{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$ to a subgroup of $\mathbb{R}^+/(\mathrm{scal}_M(E) \cap \mathbb{R}^+)$, hence $\{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$ is Abelian. Let us summarise this:

THEOREM 2.1.13. *Let $M \subseteq \mathbb{R}^d$ be a free $\mathbb{Z}$-module of finite rank.*

1. $\{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$ *is an Abelian group, where the product* $\mathrm{scal}_M(R)\,\mathrm{scal}_M(S)$ *is defined as the set* $\{\alpha\beta \mid \alpha \in \mathrm{scal}_M(R), \beta \in \mathrm{scal}_M(S)\}$. *Its neutral element is* $\mathrm{scal}_M(E)$ *and the inverse element of* $\mathrm{scal}_M(R)$ *is* $\mathrm{scal}_M(R^{-1})$.
2. $\{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$ *is isomorphic to a subgroup of* $\mathbb{R}^+/(\mathrm{scal}_M(E) \cap \mathbb{R}^+)$.
3. *There exists a natural homomorphism* $\phi : \mathrm{OS}(M) \to \{\mathrm{scal}_M(R) \mid R \in \mathrm{OS}(M)\}$ *via* $R \mapsto \mathrm{scal}_M(R)$.

The corresponding statements for $\mathrm{Scal}_M(R)$ are weaker.

THEOREM 2.1.14. *For any $R, S \in \mathrm{OS}(M)$, one has*

$$\mathrm{Scal}_M(R)\,\mathrm{Scal}_M(S) \subseteq \mathrm{Scal}_M(RS). \tag{2.10}$$

Proof. Let $\alpha \in \operatorname{Scal}_M(R), \beta \in \operatorname{Scal}_M(S)$. Then

$$\alpha\beta M = (\alpha R)(\beta S)M \subseteq \alpha R^{-1} M \subseteq M$$

shows $\alpha\beta \in \operatorname{Scal}_M(RS)$. □

As the connection between the scaling factors of R and R^{-1} will be important later, we mention for further reference the special case $S = R^{-1}$.

Lemma 2.1.15. *For any* $R \in \operatorname{OS}(M)$

$$\operatorname{Scal}_M(R^{-1}) \operatorname{Scal}_M(R) \subseteq \operatorname{Scal}_M(E). \tag{2.11}$$

In addition we have

Lemma 2.1.16. *Let* $\alpha \in \operatorname{Scal}_M(R) \setminus \{0\}$ *and let* $m = [M : \alpha RM]$ *be the index of* αRM *in* M*. Then*

$$\frac{m}{\alpha} \in \operatorname{Scal}_M(R^{-1}). \tag{2.12}$$

Proof. From $mM \subseteq \alpha RM$ we infer $\frac{m}{\alpha} R^{-1} M \subseteq M$, which proves the lemma. □

For a lattice $\Gamma \in \mathbb{R}^d$ we immediately get the following corollary, since $[\Gamma : \alpha R \Gamma] = \alpha^d$.

Corollary 2.1.17. *Let* $\Gamma \in \mathbb{R}^d$ *be a lattice and* $\alpha \in \operatorname{Scal}_\Gamma(R) \setminus \{0\}$*. Then* $\alpha^{d-1} \in \operatorname{Scal}_\Gamma(R^{-1})$.

If $\operatorname{Scal}_M(E)$ is a PID we know that $\operatorname{Scal}_M(R)$ has the form $\operatorname{Scal}_M(R) = \alpha \operatorname{Scal}_M(R)$ for some suitable α. Here, α characterises $\operatorname{Scal}_M(R)$ completely and thus it makes sense to introduce the following definition.

Definition 2.1.2. Let $\operatorname{Scal}_M(E)$ be a PID and $R \in \operatorname{OS}(M)$. Then

$$\operatorname{Den}_M(R) := \{\alpha \in \operatorname{Scal}_M(R) \mid \alpha \operatorname{Scal}_M(E) = \operatorname{Scal}_M(R)\} \tag{2.13}$$

is called the set of denominators of R.

An immediate consequence of this definition is the following lemma.

Lemma 2.1.18. *Let* $\operatorname{Scal}_M(E)$ *be a PID and* $R \in \operatorname{OS}(M)$*, and let* $\operatorname{Scal}^*_M(E)$ *be the set of units of* $\operatorname{Scal}_M(E)$*. Then*

$$\operatorname{Den}_M(R) \operatorname{Scal}^*_M(E) = \operatorname{Den}_M(R). \tag{2.14}$$

Moreover, if $\alpha, \beta \in \operatorname{Den}_M(R)$*, then* $\frac{\alpha}{\beta} \in \operatorname{Scal}^*_M(E)$.

Lemma 2.1.15 can be reformulated in terms of $\operatorname{Den}_M(R)$.

Theorem 2.1.19. *Let* $\operatorname{Scal}_M(E)$ *be a PID and* $R \in \operatorname{OS}(M)$*, and let* $\operatorname{Scal}^*_M(E)$ *be the set of units of* $\operatorname{Scal}_M(E)$*. Then there exists an* $\alpha \in \operatorname{Scal}_M(E)$ *such that*

$$\operatorname{Den}_M(R) \operatorname{Den}_M(R^{-1}) = \alpha \operatorname{Scal}^*_M(E). \tag{2.15}$$

Moreover, α *is a divisor of* $[M : \beta RM]$ *for all* $\beta \in \operatorname{Den}_M(R)$.

PROOF. Lemma 2.1.15 tells us $\mathrm{Den}_M(R)\,\mathrm{Den}_M(R^{-1}) \subseteq \mathrm{Scal}_M(E)$ and Lemma 2.1.18 guarantees that the denominators are unique up to a unit, whence there exists an α as claimed. The divisibility property follows from Lemma 2.1.16. □

A very important case is $\mathrm{Scal}_M(E) = \mathbb{Z}$, in which $\mathrm{Scal}^*_M(E) = \{1, -1\}$ is particularly simple. Here, it is convenient to introduce a special notation for the unique positive element of $\mathrm{Den}_M(R)$.

DEFINITION 2.1.3. Let $\mathrm{Scal}_M(E) = \mathbb{Z}$. The unique positive element of $\mathrm{Den}_M(R)$ is called the denominator of $R \in \mathrm{OS}(M)$ and is denoted by $\mathrm{den}_M(R)$.

We can reformulate Lemmas 2.1.15 and 2.1.16 in terms of the denominator.

THEOREM 2.1.20. *Let* $\mathrm{Scal}_M(E) = \mathbb{Z}$ *and* $R \in \mathrm{OS}(M)$. *Then*

$$\mathrm{den}_M(R)\,\mathrm{den}_M(R^{-1}) \in \mathbb{N} \tag{2.16}$$

and with $m = [M : \mathrm{den}_M(R)RM]$

$$\frac{m}{\mathrm{den}_M(R)\,\mathrm{den}_M(R^{-1})} \in \mathbb{N} \tag{2.17}$$

If $\varGamma \subseteq \mathbb{R}^d$ *is a lattice, then*

$$\frac{\mathrm{den}_\varGamma(R)^{d-1}}{\mathrm{den}_\varGamma(R^{-1})} \in \mathbb{N}. \tag{2.18}$$

The last formula gives an upper bound for $\mathrm{den}_\varGamma(R^{-1}) \le \mathrm{den}_\varGamma(R)^{d-1}$. In fact, this upper bound may be assumed. As an example, we consider the $\mathbb{Z}$-span of the vectors $\xi^{i-1}e_i$, where ξ is the d-th root of a positive integer and $\{e_1, \dots, e_d\}$ is an orthonormal basis of $\mathbb{R}^d$. Let R be the rotation that maps e_i onto e_{i+1} for $i \in \{1, \dots, d-1\}$ and e_d onto e_1. Then $\mathrm{den}_\varGamma(R) = \xi$ and $\mathrm{den}_\varGamma(R^{-1}) = \xi^{d-1}$.

We stress that $\mathrm{den}_M(R)$ and $\mathrm{den}_M(R^{-1})$ are in general not equal, not even if $M = \varGamma$ is a lattice. However, we have the following remarkable result in 2 dimensions.

COROLLARY 2.1.21. *Let* $\varGamma \subseteq \mathbb{R}^2$ *be a lattice. Then* $\mathrm{den}_\varGamma(R^{-1}) = \mathrm{den}_\varGamma(R)$.

PROOF. From Theorem 2.1.20 we infer

$$\frac{\mathrm{den}_\varGamma(R)}{\mathrm{den}_\varGamma(R^{-1})} \in \mathbb{N}, \tag{2.19}$$

and by symmetry

$$\frac{\mathrm{den}_\varGamma(R^{-1})}{\mathrm{den}_\varGamma(R)} \in \mathbb{N}, \tag{2.20}$$

which together imply $\mathrm{den}_\varGamma(R^{-1}) = \mathrm{den}_\varGamma(R)$. □

Let us finally mention that we can reformulate Theorem 2.1.14 in terms of the denominator as well. It reads as follows:

Lemma 2.1.22. *Let* $\operatorname{Scal}_M(E) = \mathbb{Z}$ *and* $R, S \in \operatorname{OS}(M)$. *Then*

$$\frac{\operatorname{den}_M(R)\operatorname{den}_M(S)}{\operatorname{den}_M(RS)} \in \mathbb{N}.$$

2.2. Similar submodules of related modules

We have already seen that similar modules have conjugated OS-groups. We want to go a step further and have a look on commensurate modules. As commensurateness is an equivalence relation, we get

Lemma 2.2.1. *Let* M *and* N *be commensurate. Then* $\operatorname{OS}(M) = \operatorname{OS}(N)$.

Proof. Let αRM be a similar submodule of M. Thus αRM and M are commensurate. As M and N are commensurate, so are αRM and αRN, from which we infer that αRN and N are commensurate, hence by Lemma 2.1.1 there exists an integer m such that $(m\alpha)RN \subseteq N$. Hence $\operatorname{OS}(M) \subseteq \operatorname{OS}(N)$, and by symmetry, $\operatorname{OS}(M) = \operatorname{OS}(N)$. □

Actually, we have proved even more:

Lemma 2.2.2. *Let* M *and* N *be commensurate. Then*

$$\operatorname{scal}_N(R) = \operatorname{scal}_M(R) \tag{2.21}$$

for any $R \in \operatorname{OS}(M) = \operatorname{OS}(N)$.

However, the sets $\operatorname{Scal}_M(R)$ and $\operatorname{Scal}_N(R)$ are different in general. By virtue of Lemma 2.1.1, it is sufficient to consider the more special case that N is a submodule of M.

Theorem 2.2.3. *Let* N *be a submodule of* M *with index* m. *Then*

$$m\operatorname{Scal}_M(R) \subseteq \operatorname{Scal}_N(R) \subseteq \frac{1}{m}\operatorname{Scal}_M(R). \tag{2.22}$$

Proof. From $\alpha RM \subseteq M$ we infer $\alpha RN \subseteq \alpha RM \subseteq M \subseteq \frac{1}{m}N$. On the other hand, $\alpha RN \subseteq N$ implies $m\alpha RM \subseteq \alpha RN \subseteq N \subseteq M$. □

One can reformulate this in terms of denominators, but, in general, this is not very useful since $\operatorname{Scal}_N(E)$ need not be a PID if $\operatorname{Scal}_M(E)$ is. But even if both $\operatorname{Scal}_N(E)$ and $\operatorname{Scal}_M(E)$ are PIDs they need not be equal. However, as $\operatorname{Scal}_N(E)$ and $\operatorname{Scal}_M(E)$ are commensurate, we have $\operatorname{Scal}_N(E) = \operatorname{Scal}_M(E)$ whenever $\operatorname{Scal}_M(E) = \mathbb{Z}$. In this case, which includes the lattice case, we have

Theorem 2.2.4. *Let* $\operatorname{Scal}_M(E) = \mathbb{Z}$ *and let* N *be a submodule of* M *with index* m. *Then*

$$\frac{m\operatorname{den}_M(R)}{\operatorname{den}_N(R)} \in \mathbb{N} \quad \textit{and} \quad \frac{m\operatorname{den}_N(R)}{\operatorname{den}_M(R)} \in \mathbb{N}. \tag{2.23}$$

If $\Gamma \subseteq \mathbb{R}^d$ is a lattice, its dual lattice is defined as

$$\Gamma^* := \{x \in \mathbb{R}^d \mid \forall y \in \Gamma : \langle x, y\rangle \in \mathbb{Z}\}, \tag{2.24}$$

where $\langle\cdot,\cdot\rangle$ denotes the usual inner product in $\mathbb{R}^d$.

Lemma 2.2.5. *Let $\varGamma \subseteq \mathbb{R}^d$ be a lattice. Then* $\operatorname{OS}(\varGamma) = \operatorname{OS}(\varGamma^*)$ *and*

$$\operatorname{Scal}_{\varGamma^*}(R) = \operatorname{Scal}_{\varGamma}(R^{-1}). \tag{2.25}$$

In particular, $\operatorname{den}_{\varGamma(R)^*} = \operatorname{den}_{\varGamma}(R^{-1})$.

Proof. $\alpha\langle Rx, y\rangle = \alpha\langle x, R^{-1}y\rangle$ shows $\alpha R\varGamma^* \subseteq \varGamma^*$ if and only if $\alpha R^{-1}\varGamma \subseteq \varGamma$, from which all claims follow immediately. □

2.3. Counting similar sublattices and submodules

It is one of our goals to count the number of similar submodules of a given module M. As we consider only free $\mathbb{Z}$-modules of finite rank, the number of submodules with a given index is finite. As any similar submodule is generated by some similarity transformation, we may count the number of similarity transformation instead. However, this number may be infinite, so we have to be careful here and find a useful subset of similarity transformations.

Let $\operatorname{O}(M)$ be the symmetry group of M, i.e. the subgroup of $\operatorname{O}(d, \mathbb{R})$ that leaves M invariant. In addition, let $\operatorname{S}(M)$ be the group of all similarity transformations in $\mathbb{R}^d$ that leave M invariant. Clearly, $\operatorname{O}(M)$ is a normal subgroup of $\operatorname{S}(M)$. If M is some lattice $\varGamma$, then the discreteness guarantees $\operatorname{O}(\varGamma) = \operatorname{S}(\varGamma)$, which can be also inferred from the fact that the index of a SSL is given by $[\varGamma : \alpha R\varGamma] = \alpha^d$.

However, $\operatorname{S}(M)$ is much larger than $\operatorname{O}(M)$ in general. In fact, $\operatorname{S}(M)/\operatorname{O}(M)$ may be infinite. This is easily seen if we consider any ring $M \subset \mathbb{R}$ of algebraic integers that has an infinite group of units. Here, M is a module in $\mathbb{R}$ with $\operatorname{Scal}_M(E) = \mathbb{Z}$ and $\operatorname{S}(M)$ is exactly the group of units of M, whereas the symmetry group $\operatorname{O}(M)$ is given by $\operatorname{O}(M) = \{1, -1\}$. Clearly, both $\operatorname{O}(M)$ and the group of scaling operations corresponding to $\operatorname{Scal}^*_M(E)$ are both subgroups of $\operatorname{S}(M)$, but in general they do not generate $\operatorname{S}(M)$. We refer to Example 2.1.1 here. Recall that $\eta = e^{\frac{i\pi}{3}}\sqrt[3]{\tau} - e^{-\frac{i\pi}{3}}\frac{1}{\sqrt[3]{\tau}}$ is a similarity transformation leaving M fixed. But neither is $|\eta|$ an element of $\operatorname{Scal}^*_M(E) = \mathbb{Z}^* = \{1, -1\}$ nor is $\frac{\eta}{|\eta|}$ contained in $\operatorname{O}(M)$.

Note that two similar submodules αRM and βSM are equal if and only if $(\alpha R)^{-1}\beta S \in \operatorname{S}(M)$, i.e. if and only if αR and βS differ only by a similarity transformation contained in $\operatorname{S}(M)$. Hence our task of counting similar submodules is reduced to count all similarity transformations modulo $\operatorname{S}(M)$. The number of all similar submodules of a given index n shall henceforward be called $b_M(n)$.

Often it is very useful to restrict considerations to a useful subclass of similar submodules.

Definition 2.3.1. A similar submodule αRM of a free $\mathbb{Z}$-module M of finite rank is called primitive, if $\frac{\alpha}{\beta}RM \subseteq M$ implies $\beta \in \operatorname{Scal}^*_M(E)$.

In other words, a primitive similar submodule αRM is the largest similar submodule in the corresponding orientation. Hence any similar submodule of M is a primitive one scaled by a factor $\beta \in \operatorname{Scal}_M(E)$. The number of all primitive similar submodules of a given index n shall be denoted by $b^{\mathsf{pr}}_M(n)$.

If $\mathrm{Scal}_M(E)$ is a PID we can establish an easy connection between $b_M(n)$ and $b_M^{\mathsf{pr}}(n)$. Here, the primitive similar sublattices are precisely those sublattices of the form $\mathrm{den}_M(R)RM$. Let $b_M^E(n)$ be the number of similar sublattices of M that are just a scaled version of M, i.e. those sublattices of the form αM with $\alpha \in \mathrm{Scal}_M(E)$. Then we have the following result.

Lemma 2.3.1. *Let* $\mathrm{Scal}_M(E)$ *be a PID. The arithmetic functions* $b_M(n)$ *and* $b_M^{\mathsf{pr}}(n)$ *that count the number of similar and primitive similar submodules of* M*, respectively, are connected via the formula*

$$b_M(n) = \sum_{m|n} b_M^{\mathsf{pr}}\left(\frac{n}{m}\right) b_M^E(m), \tag{2.26}$$

where $b_M^E(n)$ *is the number of sublattices of* M *of the form* αM*.*

Proof. As $\mathrm{Scal}_M(E)$ is a PID, any $\alpha \in \mathrm{Scal}_M(R)$ can be written as $\mathrm{den}_M(R)\beta$ with $\beta \in \mathrm{Scal}_M(E)$. Hence any similar submodule of M is of the form $\beta\,\mathrm{den}_M(R)RM$, whose index in M is given by $[M : \mathrm{den}_M(R)M][M : \beta M]$. Since the representation $\beta\,\mathrm{den}_M(R)RM$ is essentially unique – β and $\mathrm{den}_M(R)$ are unique up to units – the index of any similar submodule factors uniquely into the factor $[M : \mathrm{den}_M(R)M]$ originating from a primitive similar submodule and a second factor $[M : \beta M]$ due to scaling. A standard combinatorial argument finishes the proof. □

Lemma 2.3.2. *Let* $M \subseteq \mathbb{R}^d$ *be a free* $\mathbb{Z}$*-module of rank* k *and let* $\mathrm{Scal}_M(E)$ *be a PID, whose rank as a* $\mathbb{Z}$*-module is* ℓ*. Then* $b_M^E(n) = 0$ *unless* n *is of the form* $n = m^{k/\ell}$ *with* $m \in \mathbb{N}$*, in which case*

$$b_M^E(n) = a(n^{\ell/k}), \tag{2.27}$$

where $a(m)$ *is the number of ideals of* $\mathrm{Scal}_M(E)$ *of index* m*.*

Proof. This result follows immediately from the fact that M is a free $\mathrm{Scal}_M(E)$-module of rank $\frac{k}{\ell}$. □

In case of a lattice Γ we have $k = d$ and $\ell = 1$ since $\mathrm{Scal}_\Gamma(E) = \mathbb{Z}$. Thus we have

Corollary 2.3.3. *Let* $\Gamma \subseteq \mathbb{R}^d$ *be a lattice. Then*

$$b_\Gamma^E(n) = \begin{cases} 1, & \text{if } \sqrt[d]{n} \in \mathbb{Z} \\ 0, & \text{otherwise.} \end{cases} \tag{2.28}$$

Corollary 2.3.4. *Let* $\Gamma \subseteq \mathbb{R}^d$ *be a lattice. The arithmetic functions* $b_\Gamma(n)$ *and* $b_\Gamma^{\mathsf{pr}}(n)$ *that count the number of similar and primitive similar sublattices of* Γ*, respectively, are connected via the formula*

$$b_\Gamma(n) = \sum_{m : m^d | n} b_M^{\mathsf{pr}}\left(\frac{n}{m^d}\right). \tag{2.29}$$

In many interesting examples the arithmetic functions $b_M(n)$ and $b_M^{\mathsf{pr}}(n)$ are multiplicative. It is thus natural to consider generating functions of a Dirichlet series type. An advantage of this approach is that their analytic properties determine the asymptotic growth behaviour of $b_M(n)$ and $b_M^{\mathsf{pr}}(n)$. Lemma 2.3.2 can be easily reformulated in terms of the Dirichlet series

$$\Phi_M(s) = \sum_{n\in\mathbb{N}} \frac{b_M(n)}{n^s} \tag{2.30}$$

and

$$\Phi_M^{\mathsf{pr}}(s) = \sum_{n\in\mathbb{N}} \frac{b_M^{\mathsf{pr}}(n)}{n^s}. \tag{2.31}$$

They are connected via the zeta-function of $\mathcal{S} = \mathrm{Scal}_M(E)$, which is given by

$$\zeta_{\mathcal{S}}(s) = \sum_{\mathcal{A}} \frac{1}{[\mathcal{S}:\mathcal{A}]^s}, \tag{2.32}$$

where the summation runs over all ideals $\mathcal{A}$ of $\mathcal{S}$. In particular, we have

Theorem 2.3.5. *Let $M \subseteq \mathbb{R}^d$ be a free $\mathbb{Z}$-module of rank k and let $\mathcal{S} = \mathrm{Scal}_M(E)$ be a PID, whose rank as a $\mathbb{Z}$-module is ℓ. Then we have*

$$\Phi_M(s) = \Phi_M^{\mathsf{pr}}(s)\zeta_{\mathcal{S}}\left(\tfrac{k}{\ell}s\right), \tag{2.33}$$

where $\zeta_{\mathcal{S}}(s)$ is the ζ-function of $\mathcal{S} = \mathrm{Scal}_M(E)$.

In the special case of a lattice $\varGamma$, we have the well-known result [**10**]

Corollary 2.3.6. *Let $\varGamma \subseteq \mathbb{R}^d$ be a lattice. Then we have*

$$\Phi_\varGamma(s) = \Phi_\varGamma^{\mathsf{pr}}(s)\zeta(ds), \tag{2.34}$$

where $\zeta(s)$ is Riemann's ζ-function.

The situation is particularly nice if $b_M(n)$ is multiplicative. However, in general $b_M(n)$ is not multiplicative, see [**12**] for several examples. Nevertheless, $b_M(n)$ has a weaker property called supermultiplicativity. An arithmetic function $f(n)$ is called supermultiplicative, if $f(nm) \geq f(n)f(m)$ whenever m, n are coprime.

Theorem 2.3.7. *$b_M(n)$ is supermultiplicative.*

Proof. Let αRM and βSM be similar submodules of M of index m and n, respectively. Then $\alpha\beta RSM$ is a similar submodule of αRM with index n and hence it is a similar submodule of M of index mn. Obviously $M_1 = \alpha RM$ has exactly $b_M(n)$ similar submodules M_{1j} of index n, and so has any similar submodule M_i of index m. Calling these submodules M_{ij}, we see that it suffices to show that the submodules M_{ij} are all different. Assume that two of them are equal, say $N = M_{1i} = M_{2j}$. Then the second isomorphism theorem implies $[M_1 + M_2 : M_1] = [M_2 : M_1 \cap M_2] =: \ell$, which in turn gives $\ell = 1$ as ℓ divides the coprime integers m and n, as is illustrated in Fig. 2.1. But this is a contradiction, as M_1 and M_2 are different. □

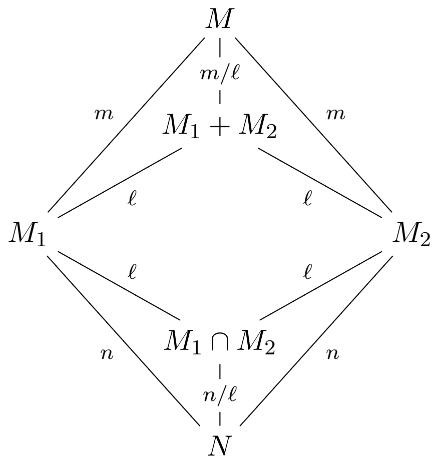

FIGURE 2.1. Diagram of submodule relationships to illustrate the proof of Theorem 2.3.7. The letters beside the lines indicate the corresponding index.

This theorem was initially proved for similar sublattices in [**9**]. We stress that this theorem holds for all modules M and does not depend on whether $\mathrm{Scal}_M(E)$ is a PID or not. The corresponding question for $b_M^{\mathsf{pr}}(n)$ is more difficult. The situation simplifies if $\mathrm{Scal}_M(E)$ is a PID.

COROLLARY 2.3.8. *Let* $\mathrm{Scal}_M(E)$ *be a PID. Then* $b_M^{\mathsf{pr}}(n)$ *is supermultiplicative.*

PROOF. We can proceed in the same way as above. There is only one additional thing to check: We must make sure that for two primitive similar submodules αRM and βSM with index m and n, respectively, the similar submodule $\alpha\beta RSM$ is primitive, as long as m and n are coprime. Assume $\frac{\alpha\beta}{\gamma}RSM$ is still a submodule of M for some $\gamma \in \mathrm{Scal}_M(E)$. Then $N(\gamma)$ divides mn. As $\mathrm{Scal}_M(E)$ is a PID, γ can be written as a product $\gamma = \xi\eta$ with $\xi, \eta \in \mathrm{Scal}_M(E)$ such that $N(\xi)$ divides m and $N(\eta)$ divides n. In addition, $\frac{\alpha\beta}{\eta}RSM$ is a similar submodule of M of index mn', where n' divides n. Similarly, $\frac{\alpha\beta}{\xi}RSM$ is a similar submodule of M of index $m'n$, where m' is a divisor of m. The diagrams of Fig. 2.2 show that the indices ℓ and j both divide m and n, hence $j = \ell = 1$, which implies $\frac{\beta}{\eta}SM \subseteq M$ and $\frac{\alpha}{\xi}RM \subseteq M$. As αRM and βSM are primitive by assumption, ξ and η and thus $\gamma = \xi\eta$ are units, which proves that $\alpha\beta RSM$ is a primitive submodule. □

Moreover, as the Dirichlet convolution of an arithmetic function $f(n)$ with a multiplicative function $g(n)$ is multiplicative if and only if $f(n)$ is multiplicative, we get

LEMMA 2.3.9. *Let* $\mathrm{Scal}_M(E)$ *be a PID. Then* $b_M(n)$ *is multiplicative if and only if* $b_M^{\mathsf{pr}}(n)$ *is multiplicative.*

The condition that $\mathrm{Scal}_M(E)$ is a PID is necessary in general. For if $\mathcal{S}$ is some ring of algebraic integers with $1 \in \mathcal{S}$, then $M = \mathcal{S}$ is a one-dimensional module, which has exactly one primitive similar submodule, namely M itself. Hence $b_M^{\mathsf{pr}}(n) = \delta_{n1}$ is multiplicative, whereas

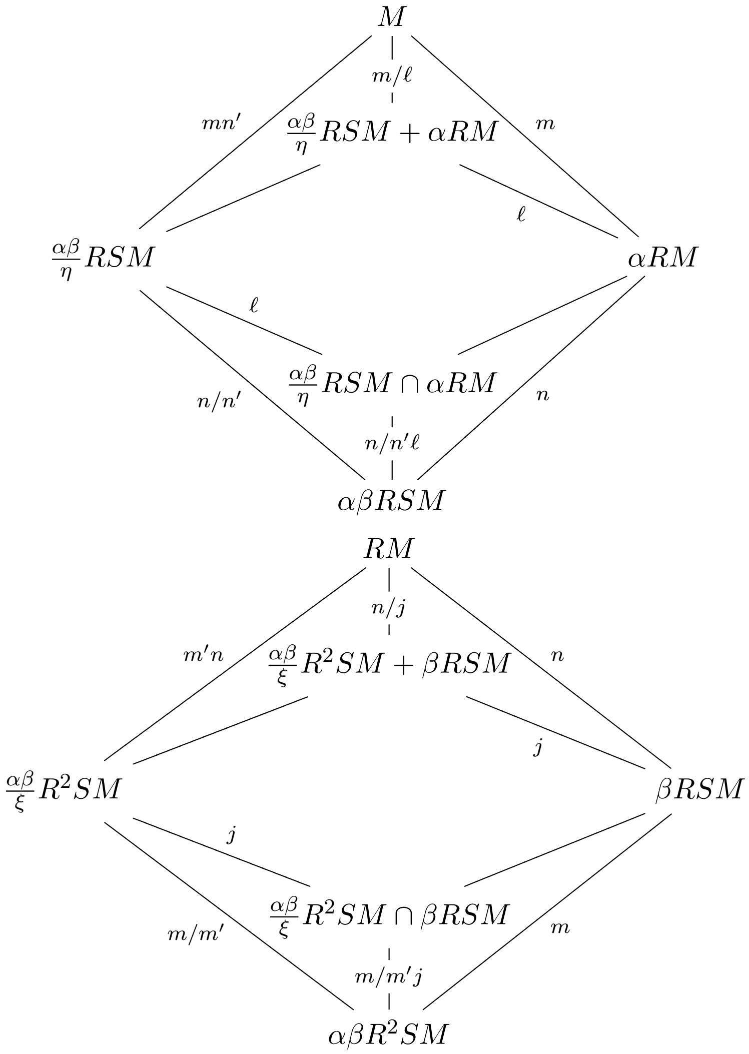
M
m/ℓ
mn'
$\frac{\alpha\beta}{\eta}RSM + \alpha RM$
m
ℓ
$\frac{\alpha\beta}{\eta}RSM$
αRM
ℓ
n/n'
$\frac{\alpha\beta}{\eta}RSM \cap \alpha RM$
n
$n/n'\ell$
$\alpha\beta RSM$
RM
n/j
$m'n$
$\frac{\alpha\beta}{\xi}R^2SM + \beta RSM$
n
j
$\frac{\alpha\beta}{\xi}R^2SM$
βRSM
j
m/m'
$\frac{\alpha\beta}{\xi}R^2SM \cap \beta RSM$
m
$m/m'j$
$\alpha\beta R^2SM$

FIGURE 2.2. Diagrams of submodule relationships to illustrate the proof of Corollary 2.3.8. The letters beside the lines indicate the index.

$b_M(n)$ is the number of principal ideals of $\mathcal{S}$ with index n. However, this function is in general not multiplicative, unless $\mathcal{S}$ is a PID.

Let us summarise these results for the special case of lattices.

THEOREM 2.3.10. *Let $\varGamma \subseteq \mathbb{R}^d$ be a lattice. Then $b^{\mathsf{pr}}_{\varGamma}(n)$ and $b_{\varGamma}(n)$ are supermultiplicative arithmetic functions. Moreover, $b_{\varGamma}(n)$ is multiplicative if and only if $b^{\mathsf{pr}}_{\varGamma}(n)$ is multiplicative.*

We conclude this section by a comparison of generating functions for closely related modules. It follows from the previous sections that modules in the same similarity class possess the same number of (primitive) submodules and thus have the same generating function. Moreover, if $\varGamma$ is a lattice, then $\varGamma$ and $\varGamma^*$ have the same number of sublattices of a given index – recall that $[\varGamma : \alpha R\varGamma] = [\varGamma^* : \alpha R^{-1}\varGamma^*]$. Hence

LEMMA 2.3.11. *For any lattice $\mathit{\Gamma} \subseteq \mathbb{R}^d$*

$$\Phi_{\mathit{\Gamma}^*}(s) = \Phi_{\mathit{\Gamma}}(s) = \Phi_{\mathit{\Gamma}}^{\mathsf{pr}}(s)\zeta(ds). \tag{2.35}$$

More important is the connection between the generating functions of commensurate modules.

THEOREM 2.3.12. *Let M be a module of rank k and let N be a submodule of M with index m. Then $\Phi_M(s)$ and $\Phi_N(s)$ have the same abscissa of convergence $\sigma \leq k$, and for all real $s > \sigma$ one has the inequalities*

$$\frac{1}{m^{ks}}\Phi_M(s) \leq \Phi_N(s) \leq m^{ks}\Phi_M(s). \tag{2.36}$$

PROOF. From Theorem 2.2.3 we know $m\,\mathrm{Scal}_M(R) \subseteq \mathrm{Scal}_N(R) \subseteq \frac{1}{m}\,\mathrm{Scal}_M(R)$. The chain of inclusions $m\alpha RM \subseteq \alpha RN \subseteq N \subseteq M$ tells us $[N : \alpha RN] = m^{-k}[M : m\alpha RM]$ for any $\alpha \in \mathrm{Scal}_N(R)$ and similarly $[M : \beta RM] = m^{-k}[N : m\beta RN]$ for any $\beta \in \mathrm{Scal}_M(R)$. Now we make use of the fact that $\Phi_M(s)$ can be expressed as a sum over all similar submodules of M:

$$\Phi_M(s) = \sum_{L \text{ SSM of } M} \frac{1}{[M : L]^s} \tag{2.37}$$

For sufficiently large $\mathrm{Re}(s)s$ the series converges and if, in addition, s is real, all terms are positive. Hence

$$\Phi_N(s) = \sum_{L \text{ SSM of } N} \frac{1}{[N : L]^s} \leq m^{ks} \sum_{L' \text{ SSM of } M} \frac{1}{[M : L']^s} = m^{ks}\Phi_M(s). \tag{2.38}$$

A similar calculation gives the other inequality. Together they show that both functions have the same abscissa of convergence σ. The bound on σ follows from the fact that the Dirichlet series counting all sublattices of a free $\mathbb{Z}$-module of rank k has abscissa of convergence k. □

For lattices, an analogous theorem holds for the generating function counting the primitive sublattices.

COROLLARY 2.3.13. *Let $\mathit{\Gamma} \subseteq \mathbb{R}^d$ be a lattice and let $\mathit{\Lambda}$ be a sublattice of $\mathit{\Gamma}$ with index m. Then $\Phi_{\mathit{\Gamma}}(s)$ and $\Phi_{\mathit{\Lambda}}(s)$ have the same abscissa of convergence $\sigma \leq d$ and for all real $s > \sigma$*

$$\frac{1}{m^{ds}}\Phi_{\mathit{\Gamma}}(s) \leq \Phi_{\mathit{\Lambda}}(s) \leq m^{ds}\Phi_{\mathit{\Gamma}}(s). \tag{2.39}$$

CHAPTER 3

Coincidence site lattices and modules

3.1. Basic notions and properties

In crystallography, the intersection $\Gamma \cap R\Gamma$ plays an important role in describing grain boundaries. If $\Gamma \cap R\Gamma$ is a lattice of full rank, it is called a *coincidence site lattice* (CSL). As we have seen, the intersection $\Gamma \cap R\Gamma$ has full rank if and only if Γ and $R\Gamma$ are commensurate. This motivates the following definition.

DEFINITION 3.1.1. Let $M \subseteq \mathbb{R}^d$ be a free $\mathbb{Z}$-module of finite rank, and let $R \in \mathrm{O}(d, \mathbb{R})$. If M and RM are commensurate, $M(R) := M \cap RM$ is called a *coincidence site module* (CSM). In this case, R is called a *coincidence isometry.* The corresponding index $\Sigma_M(R) := [M : M(R)]$ is called its *coincidence index.*

Here, we follow closely the notation of [**4**] and adapt it to modules where appropriate. As commensurateness is an equivalence relation, we find

THEOREM 3.1.1. *The set of all coincidence isometries*

$$\mathrm{OC}(M) := \{R \in \mathrm{O}(d, \mathbb{R}) \mid \textit{ M and RM are commensurate}\} \tag{3.1}$$

forms a group, a subgroup of $\mathrm{O}(d, \mathbb{R})$*.*

Note that $\mathrm{OC}(M)$ contains the symmetry group $\mathrm{O}(M)$ of M as a subgroup. In particular, $\mathrm{O}(M)$ is exactly the group of all coincidence isometries of index $\Sigma_M(R) = 1$. We will also use the notation

$$\mathrm{SOC}(M) := \{R \in \mathrm{OC}(M) \mid \det R = 1\} \tag{3.2}$$

for the group of all orientation preserving coincidence isometries (coincidence rotations).

As commensurateness is an equivalence relation, we immediately get

LEMMA 3.1.2. *The* OC*-groups are equal for commensurate modules. In particular, all sublattices of a lattice Γ have the same group of coincidence isometries.*

We have seen that similar modules have conjugated OS-groups. An analogous result is valid for coincidence isometries as well.

LEMMA 3.1.3. *Similar modules have conjugated* OC*-groups. In particular,*

$$\mathrm{OC}(\alpha RM) = R\ \mathrm{OC}(M) R^{-1}. \tag{3.3}$$

Moreover,

$$\Sigma_{\alpha RM}(S) = \Sigma_M(R^{-1}SR). \tag{3.4}$$

Unsurprisingly, there is also a close connection between a lattice and its dual lattice.

LEMMA 3.1.4. *Let $\varGamma^*$ be the dual lattice of a lattice $\varGamma \subseteq \mathbb{R}^d$. Then $\mathrm{OC}(\varGamma^*) = \mathrm{OC}(\varGamma)$ and $\varSigma_{\varGamma^*}(R) = \varSigma_{\varGamma}(R)$ for all $R \in \mathrm{OC}(\varGamma)$.*

PROOF. As two lattices are commensurate if and only if their duals are commensurate, $\varGamma^*$ and $R\varGamma^*$ are commensurate if and only if $\varGamma$ and $R\varGamma$ are commensurate. Hence it follows immediately from its definition that $\mathrm{OC}(\varGamma^*) = \mathrm{OC}(\varGamma)$. The equality of indices follows from

$$[\varGamma^* : \varGamma^*(R)] = [\varGamma^* : (\varGamma + R\varGamma)^*] = [\varGamma + R\varGamma : \varGamma] = [\varGamma : \varGamma(R)]. \tag{3.5}$$

□

An interesting observation is that the coincidence indices of a coincidence isometry and its inverse are the same. For lattices, this fact can be proved by geometric arguments [**4**], which we will repeat here.

LEMMA 3.1.5. *Let $\varGamma \subseteq \mathbb{R}^d$ be a lattice. For any $R \in \mathrm{OC}(\varGamma)$*

$$\varSigma_{\varGamma}(R) = \varSigma_{\varGamma}(R^{-1}). \tag{3.6}$$

PROOF. Here, the key is the fact that $[\varGamma : \varGamma(R)]$ can be interpreted geometrically, i.e. it is the ratio of the volume of fundamental cells of $\varGamma(R)$ and $\varGamma$. As isometries preserve the volume, we have

$$\varSigma_{\varGamma}(R) = [\varGamma : \varGamma(R)] = [R\varGamma : \varGamma(R)] = [R\varGamma : \varGamma \cap R\varGamma] = [\varGamma : R^{-1}\varGamma \cap \varGamma] = \varSigma_{\varGamma}(R^{-1}). \tag{3.7}$$

□

This idea does not work for the module case due to the lack of a suitable fundamental domain. Hence we use a more algebraic way to prove the next result.

THEOREM 3.1.6. *Let $M \subseteq \mathbb{R}^d$ be a free $\mathbb{Z}$-module of finite rank. For any $R \in \mathrm{OC}(M)$*

$$\varSigma_M(R) = \varSigma_M(R^{-1}). \tag{3.8}$$

PROOF. Any module $M \subseteq \mathbb{R}^d$ of rank k is isomorphic to some lattice $\varGamma \subseteq \mathbb{R}^k$, and R induces a linear transformation A in $\mathbb{R}^k$. Clearly, $\varSigma_M(R) = [M : M \cap RM] = [\varGamma : \varGamma \cap A\varGamma]$, and R^{-1} induces the linear map A^{-1}, so $\varSigma_M(R^{-1}) = [\varGamma : \varGamma \cap A^{-1}\varGamma] = [A\varGamma : \varGamma \cap A\varGamma]$. However, A is in general not orthogonal, hence we cannot immediately infer $[\varGamma : \varGamma \cap A\varGamma] = [A\varGamma : \varGamma \cap A\varGamma]$. Nevertheless, this equation holds: Let $P(A)$ be the characteristic polynomial of A. As $\varGamma$ and $A\varGamma$ are commensurate, $P(A)$ has rational coefficients. Our aim is to show that the constant term is ±1, as this means $\det A = \pm 1$ and hence $[\varGamma : \varGamma \cap A\varGamma] = [A\varGamma : \varGamma \cap A\varGamma]$. We do this by proving that P is either a polynomial with symmetric coefficients, i.e. $P(x) = x^k P\left(\left(\frac{1}{x}\right)\right)$, or satisfies $P(x) = -x^k P\left(\left(\frac{1}{x}\right)\right)$. Let λ be an eigenvalue of R. Then λ is a root of P, and hence the minimal polynomial p_λ of λ over $\mathbb{Q}$ divides P. As $|\lambda| = 1$ and p_λ has real coefficients, $\bar{\lambda}$ is a root of p_λ and thus p_λ is the minimal polynomial of $\bar{\lambda} = \frac{1}{\lambda}$. Denoting the degree of p_λ by ℓ, we see that $x^\ell p_\lambda\left(\frac{1}{x}\right) = c p_\lambda(x)$ for some $c \in \mathbb{Q}$. But $c = \pm 1$, since ξ^{-1} is a root of p_λ for any root ξ of p_λ. Let Q be the product of all different p_λ, so $Q(x) = \pm x^m Q\left(\frac{1}{x}\right)$, where m is the degree of Q. Clearly, Q divides P. Moreover, $Q(R) = 0$, and hence $Q(A) = 0$. Thus P is a product of powers of p_λ, whence $P(x) = \pm x^k P(\left(\frac{1}{x}\right)$ as claimed. □

We have seen that a module M and a submodule of M have the same group of coincidence isometries. However, we cannot expect their coincidence indices to be the same. Nevertheless, their coincidence indices are closely related. In particular, there exist certain upper and lower bounds. Our first result reads as follows

LEMMA 3.1.7. *Let N be a submodule of M of index m. Then $\Sigma_M(R)$ divides $m\Sigma_N(R)$.*

PROOF. As $N(R) \subseteq M(R) \subseteq M$, the coincidence index $\Sigma_M(R)$ divides

$$[M : N(R)] = [M : N][N : N(R)] = m\Sigma_N(R).$$

□

The reverse inequality is true as well. There is a particularly short proof for the case of lattices, so we state this case first.

LEMMA 3.1.8. *Let Λ be a sublattice of $\Gamma \subseteq \mathbb{R}^d$ of index m. Then $\Sigma_\Lambda(R)$ divides $m\Sigma_\Gamma(R)$ and $\Sigma_\Gamma(R)$ divides $m\Sigma_\Lambda(R)$.*

PROOF. It is a well-known property of dual lattices that $\Lambda \subseteq \Gamma$ implies $\Gamma^* \subseteq \Lambda^*$. Since $\Sigma_\Gamma(R) = \Sigma_{\Gamma^*}(R)$ for any lattice Γ, the result now follows immediately from Lemma 3.1.7. □

For general modules we have to find an alternative proof, since we lack a comparable notion of dual module. The proof will be of an algebraic nature.

THEOREM 3.1.9. *Let N be a submodule of M of index m. Then $\Sigma_M(R)$ divides $m\Sigma_N(R)$ and $\Sigma_N(R)$ divides $m\Sigma_M(R)$.*

PROOF. It remains to show that $\Sigma_N(R)$ divides $m\Sigma_M(R)$. To this end we use the coset decomposition

$$M = \bigcup_{i=1}^{m} t_i + N,$$

where $t_1, \ldots, t_m$ is a set of coset representatives with $t_1 = 0$. Then

$$M(R) = \bigcup_{i=1}^{m} \bigcup_{j=1}^{m} (t_i + N) \cap R(t_j + N). \tag{3.9}$$

Now one can show that $(t_i + N) \cap R(t_j + N)$ is either empty or a coset of $N(R)$, which we write as $v_{ij} + N(R)$, see [**49, 50**] for details. Clearly, the cosets $v_{ij} + N(R)$ are pairwise disjoint. Let I be the set of all pairs (i, j) such that $(t_i + N) \cap R(t_j + N)$ is non-empty. Now let $(i, j), (k, \ell) \in I$ and let (p, q) be the index pair defined by

$$t_p + N = t_i + t_k + N \quad \text{and} \quad t_q + N = t_j + t_\ell + N.$$

Then $(t_p+N) \cap R(t_q+N) = v_{ij}+v_{k\ell}+N(R)$ shows $\{p, q\} \in I$, and in particular, $v_{pq}+N(R) = v_{ij}+v_{k\ell}+N(R)$. This shows that $J := \{(t_i+N, t_j+N) \mid (i, j) \in I\}$ forms a group, a subgroup of $(M/N)\times(M/N)$. This means that the order of J divides m^2, i.e. $|J| = \frac{m^2}{n}$ for some integer n. Now $|J| = \frac{m^2}{n}$ is also the number of nonempty intersections $(t_i{+}N)\cap R(t_j{+}N)$ in Eq. (3.9), or in other words, $[M(R) : N(R)] = |J| = \frac{m^2}{n}$. Now

$$\varSigma_M(R) = [M : M(R)] = \frac{[M : N][N : N(R)]}{[M(R) : N(R)]} = \frac{m}{|J|}\varSigma_N(R) = \frac{n}{m}\varSigma_N(R) \tag{3.10}$$

shows that $\varSigma_N(R)$ divides $m\varSigma_M(R)$. □

An alternative proof of this theorem, which gives a more detailed expression for $\varSigma_M(R)$ in terms of $\varSigma_N(R)$, can be found in [**50**]. This proof is closely related to the theory of colour groups and thus allows an interpretation in terms of coincidences of coloured lattices, see [**50, 51**] for more on this topic.

In the previous proof intersections of the form $(t_i{+}N)\cap R(t_j{+}N)$ have occurred. These are special cases of expression occurring in connection with affine coincidences and coincidences of multilattices, see [**50, 49, 52**] for more on these topics.

Theorem 3.1.9 gives us some bounds on the coincidence index of a submodule. In certain cases we can even get sharper bounds.

THEOREM 3.1.10. *Let N be a submodule of M of index m. Let $R \in \mathrm{OC}(M)$ be such that $N \cap R(t+N) = \varnothing$ for all $t \in M \setminus N$. Then $\varSigma_N(R)$ divides $\varSigma_M(R)$.*

PROOF. Let I and J be as above. Now I contains exactly one pair of the form $(1, j)$, namely $(1, 1)$. The group properties guarantee that I contains at most one pair (i, j) for any i. Hence J is isomorphic to a subgroup of M/N, which means that $|J|$ divides m in this case, and an application of Eq. (3.10) yields the result. □

For an interpretation of this result in terms of colourings we refer again to [**50, 51**]. In fact, this result corresponds to the notion of "colour coincidence".

This theorem is only useful in practice, if it is reasonably easy to check the condition $N \cap R(t+N) = \varnothing$ for all $t \in M \setminus N$. This is possible if the points of N and $M \setminus N$ lie on different shells, i.e. if the sets $\{|x| \mid x \in N\}$ and $\{|x| \mid x \in M\setminus N\}$ are disjoint. By this means, it is possible to show that the three classes of cubic lattices have the same coincidence indices.

Indeed, let $\varGamma_{pc} = \mathbb{Z}^3$, where the index *pc* indicates that this lattice is a primitive cubic lattice, and let us consider the body-centred cubic lattice $\varGamma_{bcc} = \mathbb{Z}^3 + (u + \mathbb{Z}^3)$, where $u = \frac{1}{2}(1, 1, 1)$. Here, $\varGamma_{pc} \subset \varGamma_{bcc}$ is a sublattice of index 2 and one easily verifies that $|x|^2$ is an integer for all $x \in \varGamma_{pc}$ and $4|x|^2 \equiv 3 \pmod 4$ for all $x \in \varGamma_{bcc}\setminus\varGamma_{pc}$. Hence an application of the theorem shows that $\varSigma_{pc}(R)$ divides $\varSigma_{bcc}(R)$. The reverse divisibility property can be obtained by considering the dual lattice $\varGamma_{bcc}^*$, which is a face centred cubic lattice. In particular, $|x|^2$ is even for all $x \in \varGamma_{bcc}^*$ and odd for all $x \in \varGamma_{pc} \setminus \varGamma_{bcc}^*$. Hence, we have proved the following result.

THEOREM 3.1.11. *Let $\varGamma_{pc}, \varGamma_{bcc}, \varGamma_{fcc}\mathbb{R}^3$ be primitive, body centred, and face centred cubic lattices. Then*

$$\varSigma_{pc}(R) = \varSigma_{bcc}(R) = \varSigma_{fcc}(R) \tag{3.11}$$

for all $R \in \operatorname{OC}(\mathit{\Gamma}_{pc}) = \operatorname{OC}(\mathit{\Gamma}_{bcc}) = \operatorname{OC}(\mathit{\Gamma}_{fcc})$.

Note that this result was already proved in [**39**]. For more on cubic lattices see Section 3.5 and the references mentioned there.

3.2. Connection between similar submodules and coincidence site modules

We expect interesting relations between similar submodules and coincidence site submodules, since the notion of commensurateness plays an important role in both cases. Indeed, there is a close relationship between both types of submodules.

LEMMA 3.2.1. *Let* $M \subseteq \mathbb{R}^d$ *be a finitely generated free* $\mathbb{Z}$*-module. Then*

(1) $R \in \operatorname{OC}(M)$ *if and only if* $1 \in \operatorname{scal}_M(R)$.
(2) $R \in \operatorname{O}(M)$ *if and only if* $1 \in \operatorname{Scal}_M(R)$.

PROOF. By definition, $R \in \operatorname{OC}(M)$ if and only if M and RM are commensurate, which in turn is equivalent to $1 \in \operatorname{scal}_M(R)$. For the second statement, note that $R \in \operatorname{O}(M)$ is equivalent to $M = RM$, which is equivalent to $1 \in \operatorname{Scal}_M(R)$. □

By virtue of Theorem 2.1.8, the condition $1 \in \operatorname{scal}_M(R)$ is equivalent to $\operatorname{scal}_M(R) = \operatorname{scal}_M(E)$. This means that $\operatorname{OC}(M)$ is the kernel of the homomorphism ϕ mentioned in Theorem 2.1.13. Thus we have

THEOREM 3.2.2. *The kernel of the homomorphism*

$$\begin{aligned} \phi : \operatorname{OS}(M) &\to \mathbb{R}^+/(\operatorname{scal}_M(E) \cap \mathbb{R}^+), \\ R &\mapsto \operatorname{scal}_M(R) \cap \mathbb{R}^+ \end{aligned} \tag{3.12}$$

is the group $\operatorname{OC}(M)$. *Thus* $\operatorname{OC}(M)$ *is a normal subgroup of* $\operatorname{OS}(M)$ *and* $\operatorname{OS}(M)/\operatorname{OC}(M)$ *is Abelian.*

This theorem was first proved for lattices in [**34**] and later generalised for $\mathcal{S}$-lattices in [**33**].

If $M \subseteq \mathbb{R}^d$ is a lattice or an $\mathcal{S}$-lattice, all elements of $\operatorname{OS}(M)/\operatorname{OC}(M)$ have finite order. In particular, their order is a divisor of d, see [**34, 33**]:

THEOREM 3.2.3. *Let* $M \subseteq \mathbb{R}^d$ *be a lattice or an* $\mathcal{S}$*-lattice. Then the factor group* $\operatorname{OS}(M)/\operatorname{OC}(M)$ *is the direct sum of cyclic groups of prime power orders that divide d.*

This does not hold in general – recall Example 2.1.1. There $\operatorname{scal}_M(E) = \mathbb{Q}^*$, but $|\eta|^n \notin \mathbb{Q}$ for all $n \in \mathbb{N}$.

EXAMPLE 3.2.1. $\operatorname{OC}(M)$ may be very small compared to $\operatorname{OS}(M)$. Let us consider Example 2.1.1 further. $Z[\eta]$ is the ring of integers of the number field $\mathbb{Q}(\eta)$. It is a Euclidean domain and hence a PID [**21**, Table B.3]. Its discriminant is -135, and hence only 3 and 5 are ramifying primes. In particular, we have $3 = \eta^{-2}(1-\eta)^3$ and $5 = \eta^{-2}(1+\eta)(1-2\eta)^2$, where $\eta^{-1} = 3 + \eta^2$ is a fundamental unit. Hence $\operatorname{SOS}(Z[\eta])$ is an infinite Abelian group isomorphic to $C_2 \times C_3 \times \mathbb{Z}^{(\aleph_0)}$, where the factor C_2 is due to the roots ± 1 of unity and C_3

corresponds to the prime $(-1+\eta)$. Note that the primes over 5 do not give rise to a finite factor but contribute a factor $\mathbb{Z}$.

On the other hand, $\operatorname{SOC}(Z[\eta])$ consists of all $z \in \mathbb{Q}(\eta)$ such that $|z|^2 = 1$. But as $\mathbb{Q}(\eta)$ is a cubic field, the only numbers that satisfy $|z|^2 = 1$ must be rational, i.e. $z = \pm 1$. Thus, $\operatorname{SOC}(Z[\eta]) = \{\pm 1\}$, i.e. $\operatorname{SOC}(Z[\eta])$ contains only the symmetry rotations and there are no further coincidence rotations. This shows that $\operatorname{SOS}(Z[\eta])/\operatorname{SOC}(Z[\eta]) \sim C_3 \times \mathbb{Z}^{(\aleph_0)}$. Hence apart from a finite number of exceptions all elements of the factor group have infinite order.

Lemma 3.2.4. *For any* $R \in \operatorname{OC}(M)$

$$\varSigma_M(R) \in \operatorname{Scal}_M(R) \cap \operatorname{Scal}_M(R^{-1}). \tag{3.13}$$

Moreover, $\operatorname{Scal}_M(R)$ *is an ideal of* $\operatorname{Scal}_M(E)$.

Proof. As $\varSigma_M(R) = [M : M(R)] = [RM : M(R)]$, we infer

$$\varSigma_M(R) RM \subseteq M(R) \subseteq M, \tag{3.14}$$

which proves $\varSigma_M(R) \in \operatorname{Scal}_M(R)$. As $\varSigma_M(R) = \varSigma_M(R^{-1})$, we obtain $\varSigma_M(R) \in \operatorname{Scal}_M(R^{-1})$, and Eq. (3.13) follows. □

If $\operatorname{Scal}_M(E) = \mathbb{Z}$, we can characterise $\operatorname{Scal}_M(R)$ by the denominator $\operatorname{den}_M(R)$. In fact, an immediate consequence of Lemma 3.2.4 is

Corollary 3.2.5. *If* $\operatorname{Scal}_M(E) = \mathbb{Z}$*, then* $\operatorname{den}_M(R)$ *is a positive integer for any* $R \in \operatorname{OC}(M)$.

On the other hand, to each $R \in \operatorname{OC}(M)$ there corresponds another positive integer, namely $\varSigma_M(R)$. Hence we can expect that there are some connections between $\varSigma_M(R)$ and $\operatorname{den}_M(R)$. In order to explore this connection, we need a variant of Theorem 2.1.20.

Lemma 3.2.6. *Let* $M \subseteq \mathbb{R}^d$ *be a free* $\mathbb{Z}$*-module of rank* k *such that* $\operatorname{Scal}_M(E) = \mathbb{Z}$*. For any* $R \in \operatorname{OC}(M)$*, the denominator* $\operatorname{den}_M(R^{-1})$ *divides* $\operatorname{den}_M(R)^{k-1}$*. If* $\varGamma \subseteq \mathbb{R}^d$ *is a lattice, then* $\operatorname{den}_\varGamma(R^{-1})$ *divides* $\operatorname{den}_\varGamma(R)^{d-1}$.

Proof. Since $R \in \operatorname{OC}(M)$, we have $[RM : M(R)] = [M : M(R)]$ by Theorem 3.1.6. Thus

$$[M : \operatorname{den}_M(R) RM] = \frac{[M : \operatorname{den}_M(R) M(R)]}{[\operatorname{den}_M(R) RM : \operatorname{den}_M(R) M(R)]} = \operatorname{den}_M(R)^k, \tag{3.15}$$

and now an application of Theorem 2.1.20 gives the result. □

Note that the requirement $R \in \operatorname{OC}(M)$ is essential, since Eq. (3.15) does not hold in general. As a counterexample we recall Example 2.1.1, where $[M : \eta M] = 1 \neq |\eta|^3$.

Theorem 3.2.7. *If* M *is a free* $\mathbb{Z}$*-module of rank* k *with* $\operatorname{Scal}_M(E) = \mathbb{Z}$*, then for any* $R \in \operatorname{OC}(M)$

1. $\operatorname{lcm}\big(\operatorname{den}_M(R), \operatorname{den}_M(R^{-1})\big)$ *divides* $\varSigma_M(R)$;
2. $\varSigma_M(R)$ *divides* $\gcd\big(\operatorname{den}_M(R), \operatorname{den}_M(R^{-1})\big)^k$.

PROOF. Part 1 is an immediate consequence of Lemma 3.2.4. For part 2, we use

$$\operatorname{den}_M(R)RM \subseteq M \cap RM = M(R), \tag{3.16}$$

where $\operatorname{den}_M(R)RM \subseteq RM$ is due to the fact that $\operatorname{den}_M(R)$ is a positive integer. Calculating the respective indices shows that $\varSigma_M(R)$ divides $\operatorname{den}_M(R)^k$. Since $\varSigma_M(R) = \varSigma_M(R^{-1})$, $\varSigma_M(R)$ divides $\operatorname{den}_M(R^{-1})^k$ as well, which yields (2). □

THEOREM 3.2.8. *If M is a free $\mathbb{Z}$-module of rank k with* $\operatorname{Scal}_M(E) = \mathbb{Z}$, *then $\varSigma_M(R)^2$ divides* $\operatorname{lcm}\big(\operatorname{den}_M(R), \operatorname{den}_M(R^{-1})\big)^k$ *for any $R \in \operatorname{OC}(M)$.*

PROOF. Let $m := \operatorname{lcm}\big(\operatorname{den}_M(R), \operatorname{den}_M(R^{-1})\big)$. Then

$$mM + mRM \subseteq M \cap RM \subseteq M \tag{3.17}$$

shows that $\varSigma_M(R)$ divides $[M : mM + mRM] = \frac{m^k}{\varSigma_M(R)}$. □

Combining Theorem 3.2.7 and 3.2.8 we get

THEOREM 3.2.9. *Let $\varGamma$ be a lattice in $\mathbb{R}^2$. Then*

$$\varSigma_\varGamma(R) = \operatorname{den}_\varGamma(R). \tag{3.18}$$

3.3. Multiple coincidences

So far we only have considered intersections of two commensurate lattices, but there is no reason to restrict the discussion to this case. In fact, intersections of more than two isometric commensurate copies of a lattice or a module have been discussed already in [**6, 75, 15**]. There are various reasons to do so. On the one hand, they naturally occur in the discussion of the counting functions for CSMs, see Section 3.4 and compare [**76**]. On the other hand, they are important in crystallography in connection with multiple junctions [**30, 29, 31**]. Another interesting application arises in the theory of lattice quantizers where one usually deals with rather complex lattices. There one hopes to simplify the problem by representing a complex lattice as the intersection of simpler lattices [**24, 65**].

DEFINITION 3.3.1. Let $M \subseteq \mathbb{R}^d$ be a free $\mathbb{Z}$-module of finite rank and let R_i, $i \in \{1, \ldots m\}$ be coincidence isometries of M. Then the module

$$M(R_1, \ldots, R_m) := M \cap R_1 M \cap \ldots \cap R_m M = M(R_1) \cap \ldots \cap M(R_m) \tag{3.19}$$

is called a *multiple CSM* (MCSM). Its index in M is denoted by $\varSigma(R_1, \ldots, R_m)$.

In order to distinguish CSMs of the type $M(R) = M \cap RM$ from multiple CSMs, we will occasionally use the term simple or ordinary CSM for $M(R)$.

Note that $\varSigma(R_1, \ldots, R_m)$ is finite since $M(R_1, \ldots, R_m)$ is a finite intersection of mutually commensurate modules [**4**]. In particular, an immediate consequence of the second isomorphism theorem is

Lemma 3.3.1.

$$\Sigma(R_1, R_2) = \frac{\Sigma(R_1)\Sigma(R_2)}{\Sigma_+(R_1, R_2)}, \tag{3.20}$$

where $\Sigma_+(R_1, R_2)$ is the index of the direct sum $M_+(R_1, R_2) = M(R_1) + M(R_2)$ in M.

More generally, we have the following relation.

Lemma 3.3.2.

$$\Sigma(R_1, \ldots, R_m) = \frac{\Sigma(R_1, \ldots, R_{m-1})\Sigma(R_m)}{\Sigma_+(R_1, \ldots, R_{m-1}; R_m)}, \tag{3.21}$$

where $\Sigma_+(R_1, \ldots, R_{m-1}; R_m)$ is the index of $M_+(R_1, \ldots, R_{m-1}; R_m) = M(R_1, \ldots, R_{m-1}) + M(R_m)$ in M. In particular, $\Sigma(R_1, \ldots, R_m)$ divides $\Sigma(R_1) \cdot \ldots \cdot \Sigma(R_m)$.

3.4. Counting coincidence site lattices and modules

We have already considered the problem of counting similar submodules. We have been able to reduce this problem to the problem of determining a certain factor group of similarity isometries. This was possible since there was a bijection between similarity isometries (up to a certain group) and similar submodules. Unfortunately, the same approach does not work in the case of CSMs, as different coincidence isometries may generate the same CSM.

We first observe that isometries related by a symmetry operation yield the same coincidence site module:

Lemma 3.4.1. *Let $R \in \mathrm{OC}(M)$, and let S be a symmetry operation, i.e. $S \in \mathrm{O}(M)$. Then $M(R) = M(RS)$.*

The converse is not true. As an example, we consider the orthorhombic lattice Γ, which is spanned by the vectors $e_1, 2e_2, 2e_3$, where $e_1, \ldots, e_3$ is an orthonormal basis of $\mathbb{R}^3$. Let R be the isometry that interchanges e_1 and e_3 and leaves e_2 fixed, whereas S shall be the reflection that interchanges e_1 and e_2 and leaves e_3 fixed. We find $\Gamma(R) = \Gamma(S) = (2\mathbb{Z})^3$, but R and S are not related by a symmetry operation, as RS^{-1} is a rotation that permutes all three basis vectors. To make things even worse, consider the dual lattice Γ^*, which is the $\mathbb{Z}$-span of the vectors $e_1, \frac{1}{2}e_2, \frac{1}{2}e_3$. We know that it has the same OC-group as Γ, and the coincidence indices are the same as well. However, in this case, the two CSLs differ. In particular, $\Gamma^*(R)$ is the lattice spanned by $e_1, \frac{1}{2}e_2, e_3$, whereas $\Gamma^*(S)$ is a lattice that has the basis vectors $e_1, e_2, \frac{1}{2}e_3$.

Nevertheless, there are several important lattices and modules for which there *is* a bijection between $\mathrm{OC}(M)/\,\mathrm{O}(M)$ and the set of coincidence modules. This includes the square and triangular lattice and several modules with N-fold symmetry in the plane, and the cubic lattices in three-dimensional space.

Although we do not know, in general, whether two coincidence isometries generate the same CSM, we can give some necessary conditions. Clearly, a necessary condition for equality is that the coincidence indices are the same. In the case of lattices, we can formulate another necessary condition.

Lemma 3.4.2. *Let $\varGamma$ be a lattice. Assume that the two coincidence isometries R_1 and R_2 generate the same CSL, i.e., $\varGamma(R_1) = \varGamma(R_2)$. Then $\varSigma(R_1) = \varSigma(R_2)$ and* $\operatorname{den}(R_1^{-1}) = \operatorname{den}(R_2^{-1})$.

Proof. The statement about $\varSigma$ is trivial. For the denominator observe that

$$\operatorname{den}(R_1^{-1})\varGamma \subseteq \varGamma(R_1) = \varGamma(R_2) \subseteq R_2\varGamma. \tag{3.22}$$

Thus

$$\operatorname{den}(R_1^{-1})R_2^{-1}\varGamma \subseteq \varGamma, \tag{3.23}$$

which shows that $\operatorname{den}(R_1^{-1})$ is a multiple of $\operatorname{den}(R_2^{-1})$. By symmetry, $\operatorname{den}(R_2^{-1})$ is a multiple of $\operatorname{den}(R_1^{-1})$ as well, and the claim follows. □

We stress that the condition $\operatorname{den}(R_1^{-1}) = \operatorname{den}(R_2^{-1})$ involves the denominators of R_1^{-1} and R_2^{-1} and not R_1 and R_2 themselves. In fact, the corresponding condition $\operatorname{den}(R_1) = \operatorname{den}(R_2)$ does not hold in general, as is shown by the following example.

Let us consider the lattice $\varGamma$ spanned by the vectors $e_1, 2e_2, 4e_3, 4e_4$, where the e_i form an orthonormal basis. Then $R_1 : e_i \mapsto e_{i+1 \pmod 4}$ and $R_2 : e_1 \mapsto e_3, e_2 \mapsto e_2, e_3 \mapsto e_1, e_4 \mapsto e_4$ generate the same CSL of index 4, spanned by the vectors $4e_1, 2e_2, 4e_3, 4e_4$, but their denominators are different: $\operatorname{den}(R_1) = 2 \neq 4 = \operatorname{den}(R_2)$.

As we have seen, we have two distinct counting problems, so we have to introduce two different counting functions. Let $c_M(n)$ be the number of coincidence site modules of index n, and let $c_M^{\mathsf{iso}}(n)$ be the function counting the coincidence isometries up to symmetry operations, i.e. the number of elements of $\operatorname{OC}(M)/\operatorname{O}(M)$ that have index n. For lattices, $\operatorname{O}(\varGamma)$ is finite, so the number of coincidence isometries is given by $|\operatorname{O}(\varGamma)|c_\varGamma^{\mathsf{iso}}(n)$ in this case. Likewise, we use the notation $c_M^{\mathsf{rot}}(n)$ if we want to count orientation preserving isometries only. Note that $c_M^{\mathsf{iso}}(n) = c_M^{\mathsf{rot}}(n)$, whenever $\operatorname{O}(M)$ contains an orientation reversing isometry.

Correspondingly, we introduce the generating functions

$$\Psi_M(s) = \sum_{n\in\mathbb{N}} \frac{c_M(n)}{n^s} \tag{3.24}$$

and

$$\Psi_M^{\mathsf{iso}}(s) = \sum_{n\in\mathbb{N}} \frac{c_M^{\mathsf{iso}}(n)}{n^s}. \tag{3.25}$$

Obviously, $c_M^{\mathsf{iso}}(n)$ is an upper bound for $c_M(n)$, in other words

$$c_M(n) \leq c_M^{\mathsf{iso}}(n). \tag{3.26}$$

We have seen that the counting functions for similar submodules are supermultiplicative, so we might expect that $c_M(n)$ and $c_M^{\mathsf{iso}}(n)$ are supermultiplicative as well, which they are. To prove this, we first need a theorem about the coincidence index of a product R_1R_2. We start with a lemma on arbitrary products R_1R_2.

Lemma 3.4.3. *$\varSigma_M(R_1R_2)$ divides $\varSigma_M(R_1)\varSigma_M(R_2)$.*

Proof. The relations between the CSMs $M(R_1), M(R_2)$ and $M(R_1R_2)$ are shown in Fig. 3.1, where we have set $m := \varSigma_M(R_1)$ and $n := \varSigma_M(R_2)$. Clearly, $M(R_1) + R_1M(R_2)$ is a submodule of R_1M with index p, say. Likewise, $M(R_1R_2) \supseteq M \cap R_1M \cap R_1R_2M$, with index q, say. It follows immediately from the diagram that $\varSigma_M(R_1R_2)$ divides $mn = \varSigma_M(R_1)\varSigma_M(R_2)$. □

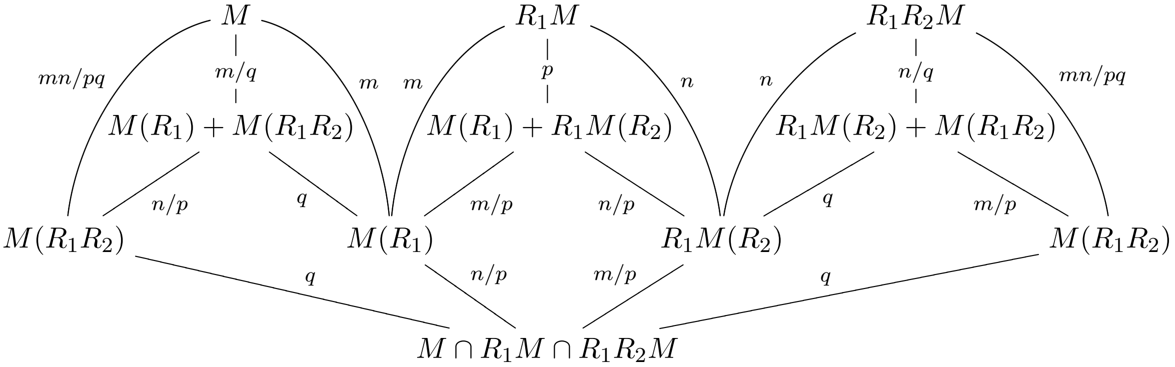

Figure 3.1. Relations between CSMs and their indices

If $\varSigma_M(R_1)$ and $\varSigma_M(R_2)$ are coprime, the diagram simplifies and we get the stronger result

Theorem 3.4.4. *If $\varSigma_M(R_1)$ and $\varSigma_M(R_2)$ are coprime, then*

$$\varSigma_M(R_1R_2) = \varSigma_M(R_1)\varSigma_M(R_2). \tag{3.27}$$

Proof. It is clear from Fig. 3.1 that p and q divide both m and n. Since m and n are coprime this implies $p = q = 1$, and Fig. 3.1 simplifies considerably, the result is shown in Fig. 3.2. In particular, we read off $M(R_1R_2) = M \cap R_1M \cap R_1R_2M$ and $\varSigma_M(R_1R_2) = mn = \varSigma_M(R_1)\varSigma_M(R_2)$. □

Note that the condition that $\varSigma_M(R_1)$ and $\varSigma_M(R_2)$ are coprime is essential. In general we cannot expect equality. A simple counter example is given by $R_2 = R_1^{-1}$, if $\varSigma_M(R_1) > 1$, since $\varSigma_M(R) = \varSigma_M(R^{-1})$ holds for any R by Theorem 3.1.6 and $\varSigma_M(E) = 1$.

A byproduct of the previous proof is

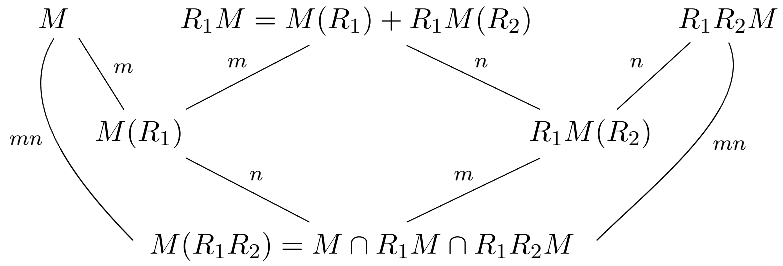
M
$R_1M = M(R_1) + R_1M(R_2)$
R_1R_2M
m
m
n
n
mn
$M(R_1)$
$R_1M(R_2)$
mn
n
m
$M(R_1R_2) = M \cap R_1M \cap R_1R_2M$

Figure 3.2. Relations between CSMs with $\varSigma_M(R_1)$ and $\varSigma_M(R_2)$ coprime

Corollary 3.4.5. *If $\Sigma_M(R_1)$ and $\Sigma_M(R_2)$ are coprime, then*

$$M(R_1R_2) = M \cap R_1M \cap R_1R_2M = M(R_1) \cap R_1M(R_2). \tag{3.28}$$

This result is rather technical but plays an important role in the following, since it relates $M(R_1R_2)$ with some kind of multiple CSMs and provides the basis for something like a "prime decomposition" of CSMs. In fact, it is the analogue of the similar submodule $\alpha R\beta SM$ that we have encountered in the proof of Theorem 2.3.7.

Since the proof of the supermultiplicativity of $c^{\mathsf{iso}}_M(n)$ is simpler than that of $c_M(n)$, we start with the former.

Theorem 3.4.6. *The arithmetic function $c^{\mathsf{iso}}_M(m)$ is supermultiplicative, i.e. $c^{\mathsf{iso}}_M(mn) \geq c^{\mathsf{iso}}_M(m)c^{\mathsf{iso}}_M(n)$ if m and n are coprime.*

Proof. Given isometries R, S with coprime indices m, n, respectively, we know that $\Sigma_M(RS) = mn$ by Theorem 3.4.4. Thus, if $R_i, i \in \{1, \ldots, c^{\mathsf{iso}}_M(m)\}$ and $S_k, k \in \{1, \ldots, c^{\mathsf{iso}}_M(n)\}$ are complete sets of not symmetry related coincidence isometries, it suffices to show that R_iS_k and R_jS_ℓ are not symmetry related unless both $i = j$ and $k = \ell$. I.e., we want to show that $R_iS_k = R_jS_\ell Q$ for some $Q \in \mathrm{O}(M)$ if and only if both $R_j^{-1}R_i = E$ and $S_k^{-1}S_\ell = E$ (which implies even$Q = E$). Lemma 3.4.3 guarantees that the indices of $\tilde{R} := R_j^{-1}R_i$ and $\tilde{S} := S_\ell QS_k^{-1}$ are divisors of m^2 and n^2, respectively. Hence they are coprime. But this implies $1 = \Sigma_M(E) = \Sigma_M(\tilde{R}\tilde{S}) = \Sigma_M(\tilde{R})\Sigma_M(\tilde{S})$, which can be only satisfied for $\Sigma_M(\tilde{R}) = \Sigma_M(\tilde{S}) = 1$. Since R_i and R_j are not symmetry related unless $i = j$, we obtain $R_i = R_j$. This in turn means $S_k = S_\ell Q$, proving that S_k and S_ℓ are symmetry related, which implies $k = \ell$ as claimed. □

To prepare for the more complicated case of $c_M(m)$, we need the following lemma.

Lemma 3.4.7. *Assume that $\Sigma_M(R) =: m$ and $\Sigma_M(S) =: n$ are coprime. Then*

$$nM \cap M(RS) = nM(R) \quad \textit{and} \quad mRM \cap M(RS) = mRM(S). \tag{3.29}$$

Proof. We start with the first equality. First note that $nM \subseteq M(S)$. Hence using Corollary 3.4.5, we see

$$nM \cap M(RS) = nM \cap M \cap RM \cap RSM = nM \cap RM(S) \supseteq nM \cap nRM = nM(R). \tag{3.30}$$

We assume that M is a module of rank k. Since $[M : nM] = n^k$ and $\Sigma_M(RS) = [M : M(RS)] = mn$ the index $[M : nM \cap M(RS)]$ must be a multiple of $n^k m$. On the other hand, $[M : nM(R)] = n^k m$ must be a multiple of $[M : nM \cap M(RS)]$, which shows that both indices are the same and we must have equality in Eq. (3.30).

The proof of the second equality is similar. First note that $\Sigma_M(R) = \Sigma_M(R^{-1}) = m$ guarantees $mRM \subseteq M$. Hence another application of Corollary 3.4.5 gives

$$mRM \cap M(RS) = mRM \cap RSM \supseteq mRM(S).$$

Again, index considerations show that equality must hold, which establishes our claim. □

This lemma does not only tell us that we can recover $M(R)$ and $M(S)$ from $M(RS)$ alone but it also tells us how to do so: just by taking the intersection of $M(RS)$ with a suitable similar submodule of M. Now supermultiplicativity of $c_M(m)$ is almost immediate.

THEOREM 3.4.8. *The arithmetic function $c_M(m)$ is supermultiplicative, i.e. $c_M(mn) \geq c_M(m)c_M(n)$ if m and n are coprime.*

PROOF. We proceed as in the proof of Theorem 3.4.6 and replace the considerations on symmetry related isometries by an application of Lemma 3.4.7. Taking a complete set of $c_M(m)$ isometries R_i that generate all different CSMs of index m and likewise a complete set of $c_M(n)$ isometries S_k we only need to show that R_iS_k and R_jS_ℓ generate different CSMs unless $i = j$ and $k = \ell$. Assume $M(R_iS_k) = M(R_jS_\ell)$. Now Lemma 3.4.7 tells us $M(R_i) = M(R_j)$ and hence $R_i = R_j$. Another application of it gives $R_iM(S_k) = R_iM(S_\ell)$, hence $k = \ell$, which proves our claim. □

There are several mechanisms that could destroy multiplicativity. First, there may be isometries Q of index $\varSigma_M(RS) = mn$ that cannot be written as a product $Q = RS$ with $\varSigma_M(R) = m$ and $\varSigma_M(S) = n$. As an example, we mention $\varGamma = 2\mathbb{Z} \times 3\mathbb{Z}$. Here $c_\varGamma^{\mathsf{iso}}(6) = c_\varGamma^{\mathsf{rot}}(6) = c_\varGamma(6) = 1$, but $c_\varGamma^{\mathsf{iso}}(2) = c_\varGamma^{\mathsf{rot}}(2) = c_\varGamma(2) = 0 = c_\varGamma^{\mathsf{iso}}(3) = c_\varGamma^{\mathsf{rot}}(3) = c_\varGamma(3)$. Further examples can be found in [**27**].

Secondly, two isometries R,R' that generate the same CSM $M(R) = M(R')$ may give rise to different CSMs $M(RS)$ and $M(R'S)$. This is no problem as long as R and R' are symmetry related. In this case, the set $\{M(R'S_k)\}$ is just a permutation of $\{M(RS_k)\}$, if S_k runs over a complete set of S_k. However, if R and R' are not symmetry related, additional CSMs might occur.

Given the close relationship of similar submodules and coincidence site modules, one might be tempted to assume that the counting functions $b_M^{\mathsf{pr}}(n)$ and $b_M(n)$ for similar submodules are multiplicative if and only if the corresponding counting functions $c_M(n)$ and $c_M^{\mathsf{iso}}(n)$ are multiplicative. However, this is not true, not even for the special case of lattices. In fact, similar sublattices seem to be more sensitive to violation of multiplicativity than CSMs. E.g., for $\Gamma = \mathbb{Z} \times 5\mathbb{Z}$, multiplicativity is violated for $b_\varGamma^{\mathsf{pr}}(n)$ and $b_\varGamma(n)$ while $c_\varGamma(n)$ and $c_\varGamma^{\mathsf{iso}}(n)$ are still multiplicative [**12, 27**].

We now know that $c_M(n)$ and $c_M^{\mathsf{iso}}(n)$ are in general supermultiplicative, and we have seen examples, where they are not multiplicative. Nevertheless, $c_M(n)$ and $c_M^{\mathsf{iso}}(n)$ are multiplicative for many important examples.

An interesting question is whether there exist some criteria for multiplicativity and the answer is positive. A first hint is given by known examples in $d \leq 4$. For root lattices in $d \leq 4$, the multiplicity functions $f(m)$ and $f^{\mathsf{iso}}(m)$ are usually multiplicative. The reason is that these lattices are related to principal ideal domains (and thus unique factorisation domains) of algebraic integers or quaternions. So we expect that some kind of unique factorisation property is essential. In fact, we can prove the following criterion.

THEOREM 3.4.9. *The following statements are equivalent:*

(1) *The arithmetic function $c_M(m)$ is multiplicative.*

(2) *Every (ordinary) CSM $M(R)$ can be written (uniquely) as $M(R) = M(R_1) \cap \ldots \cap M(R_n)$, where the indices $\varSigma_M(R_i)$ are powers of distinct primes.*

(3) *Every MCSM $M(R_1, \ldots, R_n)$ of order n can be written (uniquely) as $M(R_1, \ldots, R_n) = M_1 \cap \ldots \cap M_k$, where the M_k are MCSMs of order at most n and whose indices $\varSigma_k$ are powers of distinct primes.*

Note that Lemma 3.4.7 guarantees the uniqueness of the decomposition $M(R) = M(R_1) \cap \ldots \cap M(R_n)$, if it exists.

PROOF. We prove the equivalence of (1) and (2) first and show the equivalence of (2) and (3) afterwards.

(1)⇒(2) It is sufficient to show that every CSM $M(Q)$ with $\varSigma_M(Q) = mn$ for m, n coprime can be written as $M(Q) = M(R) \cap M(S)$, where $\varSigma_M(R) = m$ and $\varSigma_M(S) = n$. There are $c_M(m)$ distinct CSMs $M(R_i)$ of index m and correspondingly $c_M(n)$ distinct CSMs $M(S_j)$ of index n. We know from the proof of Theorem 3.4.8 that they give rise to $c_M(m)c_M(n)$ distinct CSMs $M(R_iS_j)$. Multiplicativity guarantees that $M(Q)$ is one of them, so there exist R, S' such that $M(Q) = M(RS')$ with $\varSigma_M(R) = m$ and $\varSigma_M(S') = n$. Correspondingly there exist S, R' with $M(Q) = M(SR')$ and $\varSigma_M(R') = m$, $\varSigma_M(S) = n$. From Corollary3.4.5 we infer $M(Q) = M(RS') \subset M(R)$ and $M(Q) = M(SR') \subset M(S)$, which gives $M(Q) \subseteq M(R) \cap M(S)$. Comparing the indices shows that equality must hold.

(2)⇒(1) It is sufficient to prove (a version of) submultiplicativity. Let $m = p_1^{s_1} \cdots p_n^{s_n}$ be the prime decomposition of m. By assumption, every CSM of index m can be written as intersection $M(R) = M(R_1) \cap \ldots \cap M(R_n)$ with $\varSigma_M(R_i) = p_i^{s_i}$. But there are at most $c_M(p_1^{s_1}) \cdots c_M(p_n^{s_n})$ such intersections, hence $c_M(m) \leq c_M(p_1^{s_1}) \cdots c_M(p_n^{s_n})$. Together with supermultiplicativity this gives multiplicativity.

(2)⇒(3) $M(R_1, \ldots, R_n)$ is the intersection of n ordinary CSMs, which can be written as $M(R_i) = M(R_i^{(1)}) \cap \ldots \cap M(R_i^{(K_i)})$, where the indices $\varSigma_M(R_i^{(j)})$ are powers of distinct primes for every fixed i. Hence, $M(R_1, \ldots, R_n)$ is an intersection of ordinary CSMs of prime power index, and for every prime p there are at most n CSMs which have an index a power of p. Thus combining them appropriately gives the result.

(3)⇒(2) This is trivial, since (2) is just a special case of (3). □

A corresponding criterion for the coincidence isometries exists as well. The formulation of it is a bit more intricate, since isometries usually do not commute. For CSMs, the decomposition into its prime power constituents is unique (up to permutation); for isometries, a decomposition will depend strongly on how the factors are ordered.

First notice that if the coincidence isometry R with $\varSigma_M(R) = mn$ can be factored as $R = R_1R_2$ with $\varSigma_M(R_1) = m$ and $\varSigma_M(R_2) = n$ coprime, then R_1 and R_2 are uniquely determined up to elements of the symmetry group $\mathrm{O}(M)$, i.e. all other decompositions are of the form $R = (R_1Q)(Q^{-1}R_2)$ with $Q \in \mathrm{O}(M)$. This can be proved by the same argument we used in the proof of Theorem 3.4.6. Note that R_2 and $Q^{-1}R_2$ are usually not symmetry related, whereas R_1 and R_1Q are.

At this point, it is not clear whether the existence of a decomposition $R = R_1R_2$ implies a decomposition $R = R_2'R_1'$, where $\varSigma_M(R_1) = \varSigma_M(R_1') = m$ and $\varSigma_M(R_2) = \varSigma_M(R_2') = n$. This motivates the following definitions.

We call a bijection $\pi = \{p_1, p_2 \ldots\}$ from the positive integers onto the prime numbers an ordering of the prime numbers. We call a decomposition of a coincidence isometry $R = R_1 \cdots R_n$ a π–decomposition of R if $\varSigma_M(R_i)$ is a power of p_i for any i (we allow $\varSigma_M(R_i) = p_i^0 = 1$). It is clear that any π–decomposition is unique up to point group elements.

Theorem 3.4.10. *The following statements are equivalent:*

(1) *The arithmetic function $c_M^{\mathsf{iso}}(m)$ is multiplicative.*
(2) *There exists an ordering π of the prime numbers such that any coincidence isometry R has a (unique) π–decomposition.*
(3) *For any ordering π of the prime numbers there exists a π–decomposition of every coincidence isometry R.*

Proof. It is sufficient to prove the following three implications.

(1)⇒(3) Let R be a coincidence isometry of index $m = p_1^{s_1} \cdots p_n^{s_n}$. By assumption, there are $c_M^{\mathsf{iso}}(m) = c_M^{\mathsf{iso}}(p_1^{s_1}) \cdots c_M^{\mathsf{iso}}(p_n^{s_n})$ inequivalent coincidence isometries of index m. Here, we call two isometries R and S inequivalent, if there does not exist an isometry $Q \in \mathrm{O}(M)$ such that $R = SQ$. But there are also $c_M^{\mathsf{iso}}(p_1^{s_1}) \cdots c_M^{\mathsf{iso}}(p_n^{s_n})$ inequivalent products of the form $R_1 \cdots R_n$ with $\varSigma_M(R_i) = p_i^{s_i}$. Hence R must be one of them. Since the order of the prime factors does not matter, our claim is proved.

(3)⇒(2) Statement (2) is a trivial logical implication of (3).

(2)⇒(1) We use again submultiplicativity. It is not difficult to check that there are at most $c_M^{\mathsf{iso}}(p_1^{s_1}) \cdots c_M^{\mathsf{iso}}(p_n^{s_n})$ inequivalent products $R_1 \cdots R_n$ with $\varSigma_M(R_i) = p_i^{s_i}$ for a given ordering π, hence there are at most and hence exactly $c_M^{\mathsf{iso}}(p_1^{s_1}) \cdots c_M^{\mathsf{iso}}(p_n^{s_n})$ inequivalent coincidence isometries of index $m = p_1^{s_1} \cdots p_n^{s_n}$. □

Given these two quite similar criteria we may expect that there is some connection between the multiplicativity of $c_M(n)$ and $c_M^{\mathsf{iso}}(n)$. In fact, we can prove

Theorem 3.4.11. *The arithmetic function $c_M(m)$ is multiplicative if $c_M^{\mathsf{iso}}(m)$ is.*

Proof. The multiplicativity of $c_M^{\mathsf{iso}}(m)$ guarantees a π–decomposition of R for every π. In particular, if $m = q_1^{s_1} \cdots q_n^{s_n}$ is the prime decomposition of m, we can find orderings $\pi_i = \{p_1^{(i)}, p_2^{(i)}, \ldots\}$ such that $p_1^{(i)} = q_i$. Now let R_i be the first factor of the π_i–decomposition of R. Then $M(R) = M(R_1) \cap \ldots \cap M(R_n)$ by familiar arguments. □

It is worth to comment on the various decompositions that occur here. For simplicity we assume that only two prime powers are involved, say $\Sigma(R) = p_1^{r_1} p_2^{r_2}$. Then the multiplicativity of $f^{\mathsf{iso}}(m)$ guarantees the existence of two decompositions $R = R_1S_1$ and $R = R_2S_2$ with $\Sigma(R_1) = p_1^{r_1} = \Sigma(S_2)$ and $\Sigma(R_2) = p_2^{r_2} = \Sigma(S_1)$. In this case, the unique decomposition of

$M(R)$ reads $M(R) = M(R_1) \cap M(R_2)$. So given the decompositions of R we immediately get the decomposition of $M(R)$. However, it does not work the other way round. So given a decomposition of $M(R)$ we do not get any information on the decompositions of R, even if we would know that they exist. It is thus not surprising that it is still an open question whether the converse of Theorem 3.4.11 is true or not.

Actually, our proofs on the criteria for multiplicativity show a bit more. Even if $c_M(m)$ and $c_M^{\mathsf{iso}}(m)$ are not multiplicative, the multiplicativity property might be satisfied for some integer combinations. In these situations the following results may be useful. The analogue of Theorem 3.4.9 reads

LEMMA 3.4.12. *Let m and n be coprime. The following are equivalent:*

1. $c_M(mn) = c_M(m)c_M(n)$.
2. *Every CSM $M(R)$ of index $\Sigma_M(R) = mn$ can be written as $M(R) = M(R_1) \cap M(R_2)$ with $\Sigma_M(R_1) = m$, $\Sigma_M(R_2) = n$.*
3. *Every MCSM $M(R_1, \ldots, R_\ell)$ of order ℓ can be written (uniquely) as $M(R_1, \ldots, R_\ell) = M_1 \cap M_2$, where the M_1 and M_2 are MCSMs of order at most ℓ and whose indices are $\Sigma_1 = m$ and $\Sigma_2 = n$, respectively.*

Similarly, we can generalize Theorem 3.4.10.

LEMMA 3.4.13. *Let m and n be coprime. The following are equivalent:*

1. $c_M^{\mathsf{iso}}(mn) = c_M^{\mathsf{iso}}(m)c_M^{\mathsf{iso}}(n)$.
2. *Every coincidence rotation R of index $\Sigma_M(R) = mn$ can be written as $R = R_1R_2$ with $\Sigma_M(R_1) = m$, $\Sigma_M(R_2) = n$.*

If multiplicativity is present for some integer combinations, it is quite common that it holds true for certain primes and all its powers. Thus it makes sense to generalize Lemma 3.4.12 further. In fact, the following lemma is an immediate consequence of Lemma 3.4.12.

LEMMA 3.4.14. *Let μ and ν be coprime. Let $\langle\mu\rangle$ be the set of all m that divide some power of μ. Then the following are equivalent:*

1. *$c_M(mn) = c_M(m)c_M(n)$ for all $m \in \langle\mu\rangle$ and $n \in \langle\nu\rangle$.*
2. *Every (ordinary) CSM $M(R)$ of index $\Sigma_M(R) = k$ with $k \in \langle\mu\nu\rangle$ can be written (uniquely) as $M(R) = M(R_1) \cap M(R_2)$, such that $\Sigma_M(R_1) \in \langle\mu\rangle$ and $\Sigma_M(R_2) \in \langle\nu\rangle$.*
3. *Every MCSM $M(R_1, \ldots, R_\ell)$ of order ℓ and index k with $k \in \langle\mu\nu\rangle$ can be written (uniquely) as $M(R_1, \ldots, R_\ell) = M_1 \cap M_2$, where M_1 and M_2 are MCSMs of order at most ℓ and indices $\Sigma_1 \in \langle\mu\rangle$ and $\Sigma_2 \in \langle\nu\rangle$, respectively.*

In a similar way we can generalize Lemma 3.4.13.

LEMMA 3.4.15. *Let μ and ν be coprime. Let $\langle\mu\rangle$ be the set of all m that divide some power of μ. The following are equivalent:*

1. *$c_M^{\mathsf{iso}}(mn) = c_M^{\mathsf{iso}}(m)c_M^{\mathsf{iso}}(n)$ for all $m \in \langle\mu\rangle$ and $n \in \langle\nu\rangle$.*
2. *Every coincidence rotation R of index $\Sigma_M(R) = k$ with $k \in \langle\mu\nu\rangle$ can be written as $R = R_1R_2$, where $\Sigma_M(R_1) \in \langle\mu\rangle$, $\Sigma_M(R_2) \in \langle\nu\rangle$.*

3.5. Coincidences of the cubic lattices

The three-dimensional cubic lattices are among the most important lattices in crystallography. Thus their coincidences have been studied for a long time by crystallographers [**58, 36, 39, 17, 37**]. Later, they have been studied in a mathematical context [**4, 73**]. Here, the key tool is the ring of Hurwitz quaternions, since it turns out that any coincidence rotation of a three-dimensional cubic lattice can be parametrised by Hurwitz quaternions; see also [**10**] and references therein for some background.

Traditionally, one starts with primitive cubic lattices, partly due to the fact that these lattices allow the easiest treatment with elementary methods. We will deviate from this tradition here, as the body centred lattice allows for the nicest description of its coincidence site lattices.

We have introduced the cubic lattices at the end of Section 3.1 already. Let us recall that we have defined $\varGamma_{pc} = \mathbb{Z}^3$ and $\varGamma_{bcc} = \mathbb{Z}^3 + (u + \mathbb{Z}^3)$, where $u = \frac{1}{2}(1,1,1)$. Furthermore, $\varGamma_{fcc} := \varGamma_{bcc}^{*}$ is the root lattice A_3.

As the quaternions are pivotal in the following, we want to sum up their most important properties here. For details we refer to the literature [**47, 23, 45, 41**].

Let $\{\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ be the standard basis of $\mathbb{R}^4$, where $\mathbf{e} = (1,0,0,0)^T$, $\mathbf{i} = (0,1,0,0)^T$, $\mathbf{j} = (0,0,1,0)^T$, and $\mathbf{k} = (0,0,0,1)^T$. The *quaternion algebra over* $\mathbb{R}$ is the associative division algebra $\mathbb{H} := \mathbb{H}(\mathbb{R}) = \mathbb{R}\mathbf{e} + \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k} \cong \mathbb{R}^4$, where multiplication is defined by the relations

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{e}.$$

Elements of $\mathbb{H}$ are called quaternions, and a quaternion q is written as either $q = q_0\mathbf{e} + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$ or $q = (q_0, q_1, q_2, q_3)$. Given two quaternions q and p, their *inner product* is defined by the standard scalar product of q and p as vectors in $\mathbb{R}^4$.

The *conjugate* of a quaternion $q = (q_0, q_1, q_2, q_3)$ is $\overline{q} = (q_0, -q_1, -q_2, -q_3)$, and its *norm* is $|q|^2 = q\,\overline{q} = q_0^2 + q_1^2 + q_2^2 + q_3^2 \in \mathbb{R}$. It is easy to verify that $\overline{q\,p} = \overline{p}\,\overline{q}$ and $|q\,p|^2 = |q|^2|p|^2$ for any $q, p \in \mathbb{H}$. A quaternion whose components are all integers is called a *Lipschitz quaternion.* The set $\mathbb{L}$ of Lipschitz quaternions shall be denoted by

$$\mathbb{L} = \{(q_0, q_1, q_2, q_3) \in \mathbb{H} : q_0, q_1, q_2, q_3 \in \mathbb{Z}\}\,. \tag{3.31}$$

A *primitive Lipschitz quaternion* q is a quaternion in $\mathbb{L}$ whose components are relatively prime. On the other hand, a *Hurwitz quaternion* is a quaternion whose components are all integers or all half-integers. The set $\mathbb{J}$ of Hurwitz quaternions is given by

$$\mathbb{J} = \big\{(q_0, q_1, q_2, q_3) \in \mathbb{H} : q_0, q_1, q_2, q_3 \in \mathbb{Z} \text{ or } q_0, q_1, q_2, q_3 \in \tfrac{1}{2} + \mathbb{Z}\big\} = \mathbb{L} \cup [(\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}) + \mathbb{L}]. \tag{3.32}$$

We call $q \in \mathbb{J}$ a *primitive Hurwitz quaternion* (or $\mathbb{J}$-primitive or primitive for short), if $\frac{1}{n}q \in \mathbb{J}$ with $n \in \mathbb{N}$ implies $n = 1$. We note that the norm $|q|^2$ of any Hurwitz quaternion is an integer. If $|q|^2$ is odd, we call q an odd quaternion, otherwise an even one.

Given a quaternion $q = (q_0, q_1, q_2, q_3)$, its *real part* and *imaginary part* are defined as $\operatorname{Re} q = q_0$ and $\operatorname{Im} q = q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$, respectively. The *imaginary space of* $\mathbb{H}$ is the three-dimensional subspace $\operatorname{Im}\mathbb{H} = \{\operatorname{Im} q : q \in \mathbb{H}\} \cong \mathbb{R}^3$ of $\mathbb{H}$. For ease of notation, we will identify $\operatorname{Im}\mathbb{H}$ and $\mathbb{R}^3$ and, in addition, also the elements $(q_1, q_2, q_3) \in \operatorname{Im}\mathbb{H}$ with the elements $(0, q_1, q_2, q_3) \in \mathbb{H}$.

Similarly, $\varGamma_{bcc} \cong \operatorname{Im}\mathbb{J}$ and $\varGamma_{pc} \cong \operatorname{Im}\mathbb{L}$, which indicates that $\varGamma_{bcc}$ may be easier to deal with, since $\mathbb{J}$ is a maximal order and a principal ideal ring, whereas $\mathbb{L}$ is not.

Any rotation in $\mathbb{R}^3$ can be parametrised by a quaternion $q \in \mathbb{H}$ with $q = (\kappa, \lambda, \mu, \nu)$ via

$$R(q) = \frac{1}{|q|^2}\begin{pmatrix} \kappa^2+\lambda^2-\mu^2-\nu^2 & -2\kappa\nu+2\lambda\mu & 2\kappa\mu+2\lambda\nu \\ 2\kappa\nu+2\lambda\mu & \kappa^2-\lambda^2+\mu^2-\nu^2 & -2\kappa\lambda+2\mu\nu \\ -2\kappa\mu+2\lambda\nu & 2\kappa\lambda+2\mu\nu & \kappa^2-\lambda^2-\mu^2+\nu^2 \end{pmatrix}. \tag{3.33}$$

In particular, we have $R(q)x = \frac{1}{|q|^2} q x \bar{q}$ for any $x \in \mathbb{R}^3$. Clearly, this parametrisation – which is called Cayley's parametrisation – is not unique, but one can prove that it is unique up to a scaling factor.

The first step in determining the CSLs of $\varGamma$ is the determination of $\operatorname{OC}(\varGamma)$. Since the point reflection $I : x \mapsto -x$ is a symmetry operation of all three-dimensional lattices, it is actually sufficient to determine $\operatorname{SOC}(\varGamma)$.

THEOREM 3.5.1. *Let $\varGamma$ be any of the three cubic lattices $\varGamma_{pc}, \varGamma_{bcc}, \varGamma_{fcc}$. Then*

$$\operatorname{OC}(\varGamma) = \operatorname{OS}(\varGamma) = \operatorname{O}(3, \mathbb{Q}). \tag{3.34}$$

PROOF. It follows from Theorem 3.2.3 that all elements of $\operatorname{OS}(\varGamma)/\operatorname{OC}(\varGamma)$ have an order that divides 3. On the other hand, the cubic lattices are rational lattices, which implies that all elements of $\operatorname{OS}(\varGamma)/\operatorname{OC}(\varGamma)$ have an order at most 2. Thus we have indeed $\operatorname{OC}(\varGamma) = \operatorname{OS}(\varGamma)$. Moreover, as $\varGamma$ is commensurate to $\mathbb{Z}^3$, the elements of $\operatorname{OC}(\varGamma)$ are exactly the rational orthogonal matrices. □

As any rotation in $\operatorname{O}(3, \mathbb{Q})$ can be parametrised by a rational quaternion, we can parametrise the coincidence rotations by primitive Lipschitz or Hurwitz quaternions. Contrary to the traditional approach, we opt for primitive Hurwitz quaternions here; compare [**4**]. Using Eq. (3.33) we get

LEMMA 3.5.2. *For any cubic lattice $\varGamma$, we have $\operatorname{den}_{\varGamma}(R(q)) = \frac{|q|^2}{2^\ell}$, where q is a primitive Hurwitz quaternion and ℓ is the maximal exponent such that $2^\ell \big| |q|^2$.*

Note that ℓ is either 0 or 1, depending on whether $|q|^2$ is odd or even. If one chooses to use primitive Lipschitz quaternions, one gets $\ell \in \{0, 1, 2\}$ instead.

THEOREM 3.5.3. *For any cubic lattice $\varGamma$, we have*

$$\varSigma_{\varGamma}(R(q)) = \operatorname{den}_{\varGamma}(R(q)) = \frac{|q|^2}{2^\ell}, \tag{3.35}$$

where q is a primitive Hurwitz quaternion and ℓ is the maximal exponent such that $2^\ell \big| |q|^2$.

PROOF. From Theorem 3.2.7, we know that $\Sigma_\Gamma(R(q))$ is a multiple of $\mathrm{den}_\Gamma(R(q)) = \frac{|q|^2}{2^\ell}$ and a divisor of $\mathrm{den}_\Gamma(R(q))^2$. As the latter is odd, so is $\Sigma_\Gamma(R(q))$, and it is therefore sufficient to show that $\Sigma_\Gamma(R(q))$ divides $|q|^2$. By Theorem 3.1.11, the coincidence indices are the same for all cubic lattices. Hence it suffices to prove $\Sigma_{bcc}(R(q))$ divides $|q|^2$. Since $R(q)\,\mathrm{Im}(xq) = \mathrm{Im}(qx)$ it follows that $\mathrm{Im}(q\mathbb{J}) \subseteq \Gamma_{bcc}(R(q))$. Hence $\Gamma_{bcc}(R(q))$ divides $[\mathrm{Im}\,\mathbb{J} : \mathrm{Im}(q\mathbb{J})]$. The index $[\mathbb{J} : q\mathbb{J}] = |q|^4$ can be easily calculated, as well as $[\mathbb{J} \cap \mathrm{Re}\,\mathbb{H} : (q\mathbb{J}) \cap \mathrm{Re}\,\mathbb{H}] = |q|^2$, where $\mathrm{Re}\,\mathbb{H}$ has to be understood as the real axis. Hence $[\mathrm{Im}\,\mathbb{J} : \mathrm{Im}(q\mathbb{J})] = \frac{[\mathbb{J}:q\mathbb{J}]}{[\mathrm{Re}\,\mathbb{J}:\mathrm{Re}(q\mathbb{J})]} = |q|^2$, and thus $\Gamma_{bcc}(R(q))$ divides $|q|^2$. □

If $\mathrm{den}_\Gamma(R(q))$ is square-free, then there exists a very simple alternative proof. As $\mathrm{den}_\Gamma(R) = \mathrm{den}_\Gamma(R^{-1})$ for the cubic lattices, Theorem 3.2.8 tells us that $\Sigma_\Gamma(R)^2$ divides $\mathrm{den}_\Gamma(R)^3$, and as $\mathrm{den}_\Gamma(R)$ is square-free, we infer $\Sigma_\Gamma(R) = \mathrm{den}_\Gamma(R)$.

The previous proof shows even more. If $|q|^2$ is odd, then $\Gamma_{bcc}(R(q)) = |q|^2 = [\mathrm{Im}\,\mathbb{J} : \mathrm{Im}(q\mathbb{J})]$ and hence $\mathrm{Im}(q\mathbb{J}) = \Gamma_{bcc}(R(q))$.

THEOREM 3.5.4. *If q is a primitive Hurwitz quaternion with $|q|^2$ odd, then*

$$\Gamma_{bcc}(R(q)) = \mathrm{Im}(q\mathbb{J}). \tag{3.36}$$

If $|q|^2$ is not odd, then q can be written as $q = rs$ with $r, s \in \mathbb{J}$, where $|r|^2$ is odd and $|s|^2 = 2^\ell$. As $R(s)$ is a symmetry operation of Γ_{bcc}, we see $\Gamma_{bcc}(R(q)) = \Gamma_{bcc}(R(r)) = \mathrm{Im}(r\mathbb{J})$.

An analogous result exists for the primitive cubic lattice $\mathbb{Z}^3$.

THEOREM 3.5.5. *If q is a primitive Lipschitz quaternion with $|q|^2$ odd, then*

$$\Gamma_{pc}(R(q)) = \mathrm{Im}(q\mathbb{L}). \tag{3.37}$$

Again, we can find a quaternion $r \in \mathbb{L}$ such that $\Gamma_{pc}(R(q)) = \mathrm{Im}(r\mathbb{J})$ if $|q|^2$ is even.

This shows that any CSL of $\mathbb{Z}^3$ is the projection $\mathrm{Im}(q\mathbb{J})$ of an ideal $q\mathbb{J}$ of $\mathbb{J}$. On the other hand, whenever q is an odd primitive Lipschitz quaternion, $\mathrm{Im}(q\mathbb{J})$ is a CSL of $\mathbb{Z}^3$. If we can show that there is a bijection between the set of ideals $\{q\mathbb{J} \mid q \text{ is primitive and odd}\}$ and the set of CSLs, then we can easily count the CSLs of a given index, as the number of ideals of a fixed index is well-known [**66**]. The first step into this direction is the following result.

LEMMA 3.5.6. *Let $q, r \in \mathbb{J}$ such that $|q|^2$ and $|r|^2$ are odd. Then $\mathrm{Im}(q\mathbb{J}) \subseteq \mathrm{Im}(r\mathbb{J})$ if and only if $q\mathbb{J} \subseteq r\mathbb{J}$.*

PROOF. Only the "only if" part is non-trivial. $\mathrm{Im}(q\mathbb{J}) \subseteq \mathrm{Im}(r\mathbb{J})$ implies that $|r|^2$ divides $|q|^2$. Now

$$\mathrm{Im}(r\mathbb{J}) = \mathrm{Im}(r\mathbb{J}) + \mathrm{Im}(q\mathbb{J}) = \mathrm{Im}(r\mathbb{J} + q\mathbb{J}) = \mathrm{Im}(s\mathbb{J}),$$

shows that $|r|^2 = |s|^2$, where s is the greatest common left divisor of r and q. Hence $s^{-1}r \in \mathbb{J}$, but as $|s^{-1}r| = 1$, it must be a unit. Thus $q\mathbb{J} \subseteq s\mathbb{J} = r\mathbb{J}$. □

From this we infer

COROLLARY 3.5.7. *Let $q, r \in \mathbb{J}$ such that $|q|^2$ and $|r|^2$ are odd. Then $\mathrm{Im}(q\mathbb{J}) = \mathrm{Im}(r\mathbb{J})$ if and only if $q\mathbb{J} = r\mathbb{J}$.*

In other words, we have proved

Lemma 3.5.8. *The map $q\mathbb{J} \mapsto \mathit{\Gamma}_{bcc}(R(q))$, which maps the set of right ideals generated by primitive quaternions with $|q|^2$ odd onto the set of CSLs of $\mathit{\Gamma}_{bcc}$, is a bijection.*

We can now write down the counting function for the number of CSLs explicitly. However, before doing so let us mention that analogous results can be proved for the other cubic lattices as well. In case of the primitive cubic lattice we observe that $\mathrm{Im}(q\mathbb{L}) = \mathrm{Im}(q\mathbb{J}) \cap \mathrm{Im}\,\mathbb{L}$ for any primitive Lipschitz quaternion q with $|q|^2$ odd. Using Theorem 3.5.5 the following fact is an immediate consequence of Lemma 3.5.8:

Lemma 3.5.9. *The map $q\mathbb{L} \mapsto \mathit{\Gamma}_{pc}(R(q)) = \mathrm{Im}(q\mathbb{L})$, which maps the set of right ideals generated by primitive Lipschitz quaternions with $|q|^2$ odd onto the set of CSLs of $\mathit{\Gamma}_{bcc}$, is a bijection.*

Actually, we can reformulate these results to stress the common features of the three types of cubic lattices:

Theorem 3.5.10. *Let $\mathit{\Gamma}_a$ be a cubic lattice, $a \in \{bcc, pc, fcc\}$. The map $q\mathbb{J} \mapsto \mathit{\Gamma}_a(R(q)) = \mathrm{Im}(q\mathbb{J}) \cap \mathit{\Gamma}_a$, which maps the set of right ideals generated by primitive quaternions with $|q|^2$ odd onto the set of CSLs of $\mathit{\Gamma}_a$, is a bijection.*

Proof. From $\mathit{\Gamma}_a(R(q)) \subseteq \mathit{\Gamma}_a$ and $\mathit{\Gamma}_a(R(q)) \subseteq \mathit{\Gamma}_{bcc}(R(q)) = \mathrm{Im}(q\mathbb{J})$ we see $\mathit{\Gamma}_a(R(q)) \subseteq \mathrm{Im}(q\mathbb{J}) \cap \mathit{\Gamma}_a$. Index considerations show that we have even $\mathit{\Gamma}_a(R(q)) = \mathrm{Im}(q\mathbb{J}) \cap \mathit{\Gamma}_a$. Now the theorem is a consequence of the bijection in Lemma 3.5.8, where index considerations confirm that $\mathrm{Im}(q\mathbb{J}) = \mathrm{Im}(q'\mathbb{J})$ holds if and only if $\mathrm{Im}(q\mathbb{J}) \cap \mathit{\Gamma}_a = \mathrm{Im}(q'\mathbb{J}) \cap \mathit{\Gamma}_a$. □

We return now to the arithmetic functions counting the number of CSLs and coincidence isometries, where we use $c_{bcc}(n) := c_{\mathit{\Gamma}_{bcc}}(n)$ for sake of simplicity. Using the bijections from above between ideals and CSLs we get the following results:

Corollary 3.5.11. $c^{\mathsf{iso}}_{bcc}(n) = c_{bcc}(n) = c^{\mathsf{iso}}_{pc}(n) = c_{pc}(n) = c^{\mathsf{iso}}_{fcc}(n) = c_{fcc}(n)$.

As $\mathbb{J}$ is a principal ideal ring and thus has an essentially unique prime factorisation, $c_{\mathit{\Gamma}}(n)$ is multiplicative [**66**]. In particular, we have

$$c_{\mathit{\Gamma}}(p^r) = (p+1)p^{r-1} \tag{3.38}$$

if p is prime. Hence, we obtain an explicit expression for the generating function; see also [**4**].

Theorem 3.5.12. *For any cubic lattice $\mathit{\Gamma} \subseteq \mathbb{R}^3$, we have $\Psi_{\mathit{\Gamma}}(s) = \Psi^{\mathsf{iso}}_{\mathit{\Gamma}}(s) = \Psi_{cub}(s)$, which is given by the equation*

$$\begin{aligned}\Psi_{cub}(s) &= \sum_{m=1}^{\infty} \frac{c_{\mathit{\Gamma}}(n)}{m^s} = \prod_{p \neq 2} \frac{1+p^{-s}}{1-p^{1-s}} = \frac{1}{1+2^{-s}} \cdot \frac{\zeta_{\mathbb{J}}(s/2)}{\zeta(2s)} = \frac{1-2^{1-s}}{1+2^{-s}} \frac{\zeta(s)\zeta(s-1)}{\zeta(2s)} \\ &= 1 + \tfrac{4}{3^s} + \tfrac{6}{5^s} + \tfrac{8}{7^s} + \tfrac{12}{9^s} + \tfrac{12}{11^s} + \tfrac{14}{13^s} + \tfrac{24}{15^s} + \tfrac{18}{17^s} + \tfrac{20}{19^s} + \tfrac{32}{21^s} + \tfrac{24}{23^s} + \cdots\end{aligned} \tag{3.39}$$

Here, we have made use of

$$\zeta_{\mathbb{J}}(s) = \sum_{I \subseteq \mathbb{J}} \frac{1}{[\mathbb{J} : I]^s} = (1 - 2^{1-2s})\zeta(2s)\zeta(2s-1), \tag{3.40}$$

which is the ζ-function of the algebra $\mathbb{J}$ of Hurwitz quaternions [**66, 60**], which counts the right ideals of $\mathbb{J}$. As two-sided ideals only generate the trivial CSL $\varGamma(R) = \varGamma$, they do not contribute to $\Psi_{\varGamma}(s)$. This is reflected by the factors $\frac{1}{1+2^{-s}}$ and $\frac{1}{\zeta(2s)}$, which correspond to the two-sided ideals generated by $(1,1,0,0)$ and $(n,0,0,0)$, respectively.

It follows from the properties of the Riemann ζ-function that $\Psi_{\varGamma}(s)$ is a meromorphic function of s. In particular, $\Psi_{\varGamma}$ is analytic in the half plane $\mathrm{Re}(s) \geq 2$, and its right-most pole is located at $s = 2$. Using the theorem of Delange (see Theorem 7.A.1), we get the asymptotic growth behaviour

$$\sum_{n \leq x} c_{\varGamma}(n) = \frac{3x^2}{\pi^2} + \mathcal{O}(x^2). \tag{3.41}$$

In contrast to the CSLs of the square and triangular lattice in the plane, the CSLs of the cubic lattice usually are no similar sublattices, and usually have lower symmetries, see [**73**] for details.

We finally mention that our discussion of the cubic lattices can be generalised to certain modules related to cubic lattices [**11**].

CHAPTER 4

Coincidences of the 4-dimensional hypercubic lattices

So far, we have discussed examples in dimensions 2 and 3 only. In the next chapters we want to discuss some examples in dimension 4 explicitly, in particular, we want to focus on the hypercubic lattices, the A_4-lattice and some modules including the icosian ring.

The key tool are again quaternions. In contrast to the 3-dimensional case, where a single quaternion is sufficient to parametrise a rotation, we need a pair of quaternions in 4 dimensions [**47, 25**]. Again, we identify vectors in $\mathbb{R}^4$ and quaternions. Now,

$$R(p,q) : \mathbb{R}^4 \to \mathbb{R}^4, \quad x \mapsto R(p,q)x = \frac{1}{|pq|} px\bar{q} \tag{4.1}$$

defines a rotation in $\mathbb{R}^4$, whose matrix representation – in abuse of notation it is also noted as $R(p,q) = \frac{1}{|pq|} M(p,q)$ – is explicitly given by

(4.2)

$$M(p,q) = \begin{pmatrix} \langle p,q\rangle & \langle p\mathbf{i},q\rangle & \langle p\mathbf{j},q\rangle & \langle p\mathbf{k},q\rangle \\ \langle p,\mathbf{i}q\rangle & \langle p\mathbf{i},\mathbf{i}q\rangle & \langle p\mathbf{j},\mathbf{i}q\rangle & \langle p\mathbf{k},\mathbf{i}q\rangle \\ \langle p,\mathbf{j}q\rangle & \langle p\mathbf{i},\mathbf{j}q\rangle & \langle p\mathbf{j},\mathbf{j}q\rangle & \langle p\mathbf{k},\mathbf{j}q\rangle \\ \langle p,\mathbf{i}q\rangle & \langle p\mathbf{i},\mathbf{k}q\rangle & \langle p\mathbf{j},\mathbf{k}q\rangle & \langle p\mathbf{k},\mathbf{k}q\rangle \end{pmatrix}$$

$$= \begin{pmatrix} ak+b\ell+cm+dn & -a\ell+bk+cn-dm & -am-bn+ck+d\ell & -an+bm-c\ell+dk \\ a\ell-bk+cn-dm & ak+b\ell-cm-dn & -an+bm+c\ell-dk & am+bn+ck+d\ell \\ am-bn-ck+d\ell & an+bm+c\ell+dk & ak-b\ell+cm-dn & -a\ell-bk+cn+dm \\ an+bm-c\ell-dk & -am+bn-ck+d\ell & a\ell+bk+cn+dm & ak-b\ell-cm+dn \end{pmatrix},$$

where $\mathbf{e} = (1,0,0,0)^T$, $\mathbf{i} = (0,1,0,0)^T$, $\mathbf{j} = (0,0,1,0)^T$, $\mathbf{k} = (0,0,0,1)^T$ are the unit quaternions introduced in Section 3.5 and, furthermore, $p = (k,\ell,m,n)^T$ and $q = (a,b,c,d)^T$. Here, $\langle\cdot,\cdot\rangle$ denotes the standard inner product in $\mathbb{R}^4$.

4.1. Centred hypercubic lattice

In 4 dimensions there are only two types of hypercubic lattices, namely $\mathbb{Z}^4$, the primitive hypercubic lattice, and D_4 the centred hypercubic lattice [**22**]. Note that the dual lattice D_4^* is similar to D_4, which is a special feature of $d = 4$ — in all other dimensions D_n^* and D_n are not similar and hence there are three types of hypercubic lattices.

We start with the centred hypercubic lattice D_4, which we can identify with the Hurwitz ring $\mathbb{J}$ of integer quaternions. The coincidence isometries of hypercubic lattices have already been discussed in [**74**] by some explicit calculations with quaternions. Here, we want to use a different approach. The main idea is to express the CSLs as a sum of certain ideals of $\mathbb{J}$. This has two advantages: on the one hand, it gives us an explicit expression for the CSLs, which makes it easier to determine the number of CSLs, a goal that has not been achieved in [**74**], and on the other hand, it yields a method that can be easily adapted for the case of the A_4 lattice and the icosian ring.

As the symmetry group of D_4 contains a reflection, the number of coincidence isometries is twice the number of coincidence rotations of a given index, and all CSLs are generated by rotations. Hence, we can restrict our discussion to coincidence rotations.

We first observe that $R = R(p,q)$ is a coincidence rotation of $\mathbb{J}$ if and only if $R \in \mathrm{SO}(4,\mathbb{Q})$. Taking the trace of $R(p,q)$ yields $\frac{ak}{|pq|} \in \mathbb{Q}$ and similar sums give $\frac{a\ell}{|pq|}, \frac{am}{|pq|}, \frac{an}{|pq|} \in \mathbb{Q}$, which proves that p is a multiple of an integral quaternion. As $R(p,q)$ is independent of any scaling factor of p, we may assume w.l.o.g. that $p \in \mathbb{J}$. Similarly, it follows that q may be chosen as $q \in \mathbb{J}$. However, not every pair $(p,q) \in \mathbb{J} \times \mathbb{J}$ yields a matrix $R(p,q) \in \mathrm{SO}(4,\mathbb{Q})$. In fact, $R(p,q) \in \mathrm{SO}(4,\mathbb{Q})$ if and only if $|pq| \in \mathbb{N}$. A pair $(p,q) \in \mathbb{J} \times \mathbb{J}$ with $|pq| \in \mathbb{N}$ is called *admissible*. Thus $R(p,q)$ is a coincidence rotation of $\mathbb{J}$ if and only if $R(p,q)$ can be parametrised by an admissible pair of primitive integral quaternions.

However, it turns out that primitive quaternions are not the optimal choice in this case, and we prefer a suitably scaled pair. First note that $|pq|^2$ is a square in $\mathbb{N}$ for an admissible pair, and so is $\frac{|pq|^2}{\gcd(|p|^2,|q|^2)^2}$. As the two factors $\frac{|q|^2}{\gcd(|p|^2,|q|^2)}$ and $\frac{|p|^2}{\gcd(|p|^2,|q|^2)}$ are coprime, they must be squares as well. Hence, we can define the (coprime) integers

$$\alpha_p := \sqrt{\frac{|q|^2}{\gcd(|p|^2,|q|^2)}} \qquad \text{and} \qquad \alpha_q := \sqrt{\frac{|p|^2}{\gcd(|p|^2,|q|^2)}}. \tag{4.3}$$

Of course $(x,y) = (\alpha_p p, \alpha_q q)$ defines the same rotation as (p,q). However, we can deal more easily with (x,y) since $|x|^2 = |y|^2$. Moreover, the octuple $(x,y) = (\alpha_p p, \alpha_q q)$ is primitive for primitive p and q, in the sense that $\frac{1}{n}(\alpha_p p, \alpha_q q) \in \mathbb{J} \times \mathbb{J}$ if and only if $n \in \{\pm 1\}$. This guarantees that there exist quaternions $v, w \in \mathbb{J}$ such that $\langle x, v\rangle + \langle y, w\rangle = 1$. We shall call a pair of quaternions with these two properties an *extended admissible pair*, and denote it by $(p_\alpha, q_\alpha) = (\alpha_p p, \alpha_q q)$.

Clearly, scaling quaternions does not change the rotation $R(p,q)$. On the other hand, there are a lot of rotations that yield the same CSL, namely all rotations that differ by a symmetry operation of $\mathbb{J}$ only. Let us denote the corresponding group by $\mathrm{SO}(\mathbb{J}) := \{R \in \mathrm{SO}(4,\mathbb{R}) \mid R\mathbb{J} = \mathbb{J}\}$, which is of order $24^2 = 576$. Recall that we call two coincidence rotations R, R' symmetry related, if there exists an $S \in \mathrm{SO}(\mathbb{J})$ such that $R' = RS$.

Let us have a closer look on which rotations are symmetry related. It follows from $R(p,q)\mathbb{J} = \frac{1}{|pq|} p\mathbb{J}\bar{q}$ that $R(p,q)\mathbb{J} = R(p',q')\mathbb{J}$ if and only if

$$\frac{1}{|pp'|}\bar{p}p'\mathbb{J} = \frac{1}{|qq'|}\mathbb{J}\bar{q}q'.$$

This means that (p,q) and (pr, qr) are symmetry related if and only if r is a quaternion such that $r\mathbb{J}$ is a two-sided ideal. Apart from scaling factors and units, the only such non-trivial quaternion is $r = (1,1,0,0)$, see [**66, 47, 25, 45**]. Thus $R(p,q)\mathbb{J} = R(pr,qr)\mathbb{J}$, and as $r = (1,1,0,0)$ is the only prime quaternion of norm $|r|^2 = 2$, we can find for any rotation $R \in \mathrm{SOC}(\mathbb{J})$ a pair of quaternions (p,q) with $|p|^2$ and $|q|^2$ odd such that R is symmetry related to $R(p,q)$. Thus we can confine our considerations to latter rotations and we will call an extended admissible pair (p,q) with $|p|^2$ and $|q|^2$ odd an *odd extended admissible* pair. In addition, we will call a quaternion $q \in \mathbb{J}$ with odd norm $|q|^2$ an odd quaternion; compare [**45**].

In fact, we can express all coincidence cite lattices in terms of odd extended admissible pairs. Our first step in this direction is the following lemma.

LEMMA 4.1.1. *Let (p,q) be an odd extended admissible pair. Then*

$$p\mathbb{J} + \mathbb{J}\bar{q} \subseteq \mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}. \tag{4.4}$$

PROOF. Clearly $p\mathbb{J} \subseteq \mathbb{J}$ and $\mathbb{J}\bar{q} \subseteq \mathbb{J}$, thus giving $p\mathbb{J} + \mathbb{J}\bar{q} \subseteq \mathbb{J}$. On the other hand (recall $|p|^2 = |q|^2$)

$$p\mathbb{J} = \frac{p\mathbb{J}q\bar{q}}{|q|^2} \subseteq \frac{p\mathbb{J}\bar{q}}{|q|^2} = \frac{p\mathbb{J}\bar{q}}{|pq|}, \tag{4.5}$$

and a similar argument for $\mathbb{J}\bar{q}$ yields $p\mathbb{J} + \mathbb{J}\bar{q} \subseteq \frac{p\mathbb{J}\bar{q}}{|pq|}$. □

The first step for the converse inclusion is the following result, where we return to the more general case of extended admissible pairs for a moment.

LEMMA 4.1.2. *Let (p,q) be an extended admissible pair. Then*

$$2\left(\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}\right) \subseteq p\mathbb{J} + \mathbb{J}\bar{q}. \tag{4.6}$$

PROOF. Let $x \in \mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}$. Then there exists a $y \in \mathbb{J}$ such that $x = \frac{py\bar{q}}{|pq|}$. Since (p,q) is an extended admissible pair there exist quaternions $v, w \in \mathbb{J}$ such that $\langle p, v\rangle + \langle q, w\rangle = 1$. Hence

$$\begin{aligned} 2x &= 2(\langle p,v\rangle + \langle q,w\rangle)x = 2\langle p,v\rangle x + 2x\langle q,w\rangle = p\bar{v}x + v\bar{p}x + xq\bar{w} + xw\bar{q} \\ &= p\bar{v}x + vy\bar{q} + py\bar{w} + xw\bar{q} \in p\mathbb{J} + \mathbb{J}\bar{q}, \end{aligned}$$

where we have made use of the identity $\langle a,b\rangle = \frac{1}{2}(a\bar{b} + b\bar{a})$. □

Trivially,

$$|p|^2\left(\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}\right) = |p|^2\mathbb{J} \cap p\mathbb{J}\bar{q} \subseteq p\mathbb{J} + \mathbb{J}\bar{q}. \tag{4.7}$$

If we restrict again to odd extended admissible pairs, we get

$$\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|} = 2\left(\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}\right) + |p|^2\left(\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}\right) \subseteq p\mathbb{J} + \mathbb{J}\bar{q}, \tag{4.8}$$

since $|p|^2$ is odd. Hence we have proved

THEOREM 4.1.3. *Let (p, q) be an odd extended admissible pair. Then*

$$\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|} = p\mathbb{J} + \mathbb{J}\bar{q}, \tag{4.9}$$

i.e. each CSL of the centred hypercubic lattice is of the form $p\mathbb{J} + \mathbb{J}\bar{q}$ for a suitable odd extended admissible pair.

As we have an explicit expression for our CSLs now, we can explicitly calculate their indices. So our task is to find the index of $p\mathbb{J} + \mathbb{J}\bar{q}$ for any odd extended admissible pair (p, q).

We start with the following observation.

LEMMA 4.1.4. *Let (p, q) be an odd extended admissible pair. Then $\Sigma(R(\bar{p}, q))\Sigma(R(p, q)) = |p|^4$.*

PROOF. First note

$$p\mathbb{J} \subseteq p\mathbb{J} + \mathbb{J}\bar{q} = \mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|} \subseteq \mathbb{J}. \tag{4.10}$$

$p\mathbb{J}$ is a similar sublattice of $\mathbb{J}$ with index $[\mathbb{J} : p\mathbb{J}] = |p|^4$. On the other hand $[\mathbb{J} : \mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}] = \Sigma(R(p, q))$ is the coincidence index of $R(p, q)$. Moreover

$$[p\mathbb{J} + \mathbb{J}\bar{q} : p\mathbb{J}] = \left[\mathbb{J} + \frac{\bar{p}\mathbb{J}\bar{q}}{|pq|} : \mathbb{J}\right] = \left[\mathbb{J} : \mathbb{J} \cap \frac{\bar{p}\mathbb{J}\bar{q}}{|pq|}\right] = \Sigma(R(\bar{p}, q)), \tag{4.11}$$

where we have used the well known trick of applying the second isomorphism theorem. Thus

$$\Sigma(R(\bar{p}, q))\Sigma(R(p, q)) = |p|^4. \tag{4.12}$$

□

Our next aim is to prove $\Sigma(R(\bar{p}, q)) = \Sigma(R(p, q))$, which gives us the explicit value of $\Sigma(R(p, q))$. Note that it is sufficient to prove that $\Sigma(R(p, q))$ divides $|p|^2$, as the result then follows from the lemma.

LEMMA 4.1.5. *Let (p, q) be a primitive admissible pair of odd quaternions and (p_α, q_α) its extension. Then $[\mathbb{J} : p_\alpha\mathbb{J} + \mathbb{J}\bar{q}_\alpha]$ divides $|p_\alpha|^2$.*

PROOF. We start with the case $\alpha_p = \alpha_q = 1$, i.e., $|p_\alpha|^2 = |p|^2 = |q|^2 = |q_\alpha|^2$. As the result is trivial if p and q are units, we may assume $|p|^2 = |q|^2 > 1$.

Since $[\mathbb{J} : p\mathbb{J}] = [\mathbb{J} : \mathbb{J}\bar{q}]$ we cannot have $p\mathbb{J} \supseteq \mathbb{J}\bar{q}$ unless $p\mathbb{J} = \mathbb{J}\bar{q}$. But the latter would imply that $p\mathbb{J}$ is a two-sided ideal, which is ruled out by the requirement that p is primitive and odd (and not a unit). Thus there exists a minimal integer $1 < m \in \mathbb{N}$ such that $m\mathbb{J}\bar{q} \subseteq p\mathbb{J}$. As $|p|^2\mathbb{J}\bar{q} = p(\bar{p}\mathbb{J}\bar{q}) \subseteq p\mathbb{J}$, the integer m must divide $|p|^2$. Our aim is to show $m = |p|^2$. Let $g = \operatorname{gcld}(m, p)$ be the greatest common left divisor of m and p. Clearly, gcld is defined only up to units, but this does not matter. We can write $p = gh$, where $h \in \mathbb{J}$ is primitive since p is primitive. Note that $m = |g|^2$ and hence h is a unit if and only if $m = |p|^2$. Now, $m\mathbb{J}\bar{q} \subseteq p\mathbb{J}$ implies $\bar{g}\mathbb{J}\bar{q} \subseteq h\mathbb{J}$ and hence $\bar{g}\mathbb{J}\bar{q} + h\mathbb{J}\bar{q} \subseteq h\mathbb{J}$. As h and $\bar{g}$ have no common left divisor – otherwise p would not be primitive – we infer $h\mathbb{J} \supseteq \bar{g}\mathbb{J}\bar{q} + h\mathbb{J}\bar{q} = \mathbb{J}\bar{q}$. Right multiplication by $\mathbb{J}$ yields $h\mathbb{J} \supseteq \mathbb{J}\bar{q}\mathbb{J}$. Since the latter is a two-sided ideal, and q is primitive and odd, we must have $\mathbb{J}\bar{q}\mathbb{J} = \mathbb{J}$. But this implies $\mathbb{J} \subseteq h\mathbb{J}$, form which we infer that h must be a unit and hence $m = |p|^2$ as claimed.

Now, $m = |p|^2$ is the smallest integer such that $m\mathbb{J}\bar{q} \subseteq p\mathbb{J}$. This means that there exists a quaternion $x \in \mathbb{J}\bar{q}$ such that $kx \notin p\mathbb{J}$ for any $0 < k < m$. Hence the index $[p\mathbb{J} + \mathbb{J}\bar{q} : p\mathbb{J}]$ is a multiple of $m = |p|^2$, which in turn yields that $[\mathbb{J} : p\mathbb{J} + \mathbb{J}\bar{q}]$ must be a divisor of $|p|^2$. This settles the case $\alpha_p = \alpha_q = 1$.

Let us turn to the general case. The idea is to reduce the problem to the case $\alpha_p = \alpha_q = 1$. First we define the greatest common left divisor $g_p = \operatorname{gcld}(p, \alpha_q) = \operatorname{gcld}(p_\alpha, \alpha_q)$, where the last equation holds because α_p and α_q are coprime. Similarly, we define the greatest common left divisor $g_q = \operatorname{gcld}(q, \alpha_p) = \operatorname{gcld}(q_\alpha, \alpha_p)$ and use the decompositions $p = g_p h_p$ and $q = g_q h_q$. As p and q are primitive, so are g_p and g_q. Together with α_q being a divisor of $|p|^2$ this implies $|g_p|^2 = \alpha_q$, and analogously we get $|g_q|^2 = \alpha_p$. Hence

$$\begin{aligned} p_\alpha\mathbb{J} + \mathbb{J}\bar{q}_\alpha &= p_\alpha\mathbb{J} + p_\alpha\mathbb{J}\bar{q} + p\mathbb{J}\bar{q}_\alpha + \mathbb{J}\bar{q}_\alpha = p(\mathbb{J}\alpha_p + \mathbb{J}\bar{q}_\alpha) + (\alpha_q\mathbb{J} + p_\alpha\mathbb{J})\bar{q} \\ &= p\mathbb{J}\bar{g}_q + g_p\mathbb{J}\bar{q} = g_p(h_p\mathbb{J} + \mathbb{J}\bar{h}_q)\bar{g}_q. \end{aligned} \tag{4.13}$$

Thus

$$[\mathbb{J} : (p_\alpha\mathbb{J} + \mathbb{J}\bar{q}_\alpha)] = \alpha_p^2\alpha_q^2[\mathbb{J} : (h_p\mathbb{J} + \mathbb{J}\bar{h}_q)]. \tag{4.14}$$

Note that $|h_p|^2 = \frac{|p|^2}{\alpha_q} \neq |h_q|^2 = \frac{|q|^2}{\alpha_p}$, so we cannot apply our known result yet. To circumvent this problem, we define the greatest common divisors $k_p := \operatorname{gcld}(h_p, |h_q|^2) = \operatorname{gcld}(h_p, |h_p|^2, |h_q|^2) = \operatorname{gcld}(h_p, \operatorname{gcd}(|p|^2, |q|^2)$ and $k_q := \operatorname{gcld}(h_q, |h_p|^2)$. Now we can write

$$\begin{aligned} h_p\mathbb{J} + \mathbb{J}\bar{h}_q &= h_p\mathbb{J} + |h_p|^2\mathbb{J} + \mathbb{J}|h_q|^2 + \mathbb{J}\bar{h}_q = \\ &= (h_p\mathbb{J} + |h_q|^2\mathbb{J}) + (\mathbb{J}\bar{h}_q + \mathbb{J}|h_p|^2) = k_p\mathbb{J} + \mathbb{J}\bar{k}_q, \end{aligned} \tag{4.15}$$

Note that both k_p and k_q have the same norm, in particular,

$$|k_p|^2 = |k_q|^2 = \operatorname{gcd}(|h_p|^2, |h_q|^2) = \frac{|p|^2}{\alpha_q^2} = \frac{|q|^2}{\alpha_p^2} = \operatorname{gcd}(|p|^2, |q|^2). \tag{4.16}$$

Thus we can apply the results of part 1 and obtain that

$$[\mathbb{J} : (p_\alpha\mathbb{J} + \mathbb{J}\bar{q}_\alpha)] = \alpha_q^2\alpha_p^2[\mathbb{J} : (k_p\mathbb{J} + \mathbb{J}\bar{k}_q)]$$

is a divisor of $\alpha_q^2\alpha_p^2\frac{|p|^2}{\alpha_q^2} = |p_\alpha|^2$, which proves the theorem also for the general case. □

Combining the last two lemmas we have proved:

Theorem 4.1.6. *Let (p, q) be an odd extended admissible pair. Then $\Sigma(R(p, q)) = |p|^2$.*

Remark 4.1.1. It may be useful to formulate the index in terms of primitive admissible pairs. Let p, q be primitive odd quaternions with extended pair $(p_\alpha, q_\alpha) = (\alpha_p p, \alpha_q q)$. Then

$$\Sigma(R(p, q)) = \alpha_p^2|p|^2 = \alpha_q^2|q|^2 = \alpha_p\alpha_q|pq| = \operatorname{lcm}(|p|^2, |q|^2) = \alpha_p^2\alpha_q^2\operatorname{gcd}(|p|^2, |q|^2). \tag{4.17}$$

Note that $|pq|$ is the denominator of $R(p,q)$. This shows that in general $\mathrm{den}(R)$ and $\varSigma(R)$ do not coincide for the lattice D_4, which is in contrast to the three-dimensional cubic latices. In fact, $\mathrm{den}(R)=\varSigma(R)$ holds if and only if $\alpha_p=\alpha_q=1$.

Our next task is to count the number of coincidence isometries of D_4. Since the point group of D_4 contains $24^2=576$ rotations, the number of coincidence rotations of a given index n can be written as $576\,c^{rot}_{D_4}(n)$. As mentioned above, the number of coincidence isometries is twice this number, i.e. $1152\,c^{rot}_{D_4}(n)$.

By the previous theorem, counting the number of coincidence rotations is equivalent to counting the number of odd extended admissible pairs. We first observe that $c^{rot}_{D_4}(n)$ is a multiplicative function, which follows from the essentially unique prime decomposition in $\mathbb{J}$. Indeed, if (p,q) and (r,s) are odd extended admissible pairs with $|p|^2=m$ and $|r|^2=n$ and m,n coprime, then (pr,qs) is an odd extended admissible pair with $|pr|^2=mn$. On the other hand, any odd extended admissible pair (p,q) with $|p|^2=mn$ can be decomposed into odd extended admissible pairs with index m and n, respectively. As this decomposition is unique up to units, multiplicativity follows.

Thus we need to compute $c^{rot}_{D_4}(n)$ only for prime powers π^r. As odd extended admissible pairs consist of odd quaternions only, $c^{rot}_{D_4}(2^r)=0$. It is now a purely combinatorial task to determine $c^{rot}_{D_4}(\pi^r)$. The number of primitive quaternions p with norm $|p|^2=\pi^r$ is given by $24f(\pi^r)$ with $f(\pi^r)=(\pi+1)\pi^{r-1}$ for $r\geq 1$, compare Eq.(3.38). Any odd extended admissible pair (p,q) with $|p|^2=\pi^r$ can be obtained from a primitive admissible pair (p_1,q_1) with $|p_1|^2=\pi^{r'}$, $|q_1|^2=\pi^{r''}$, $r=\max(r',r'')$, $r'-r''$ even. Hence

$$c^{rot}_{D_4}(\pi^r)=f(\pi^r)^2+2\sum_{s=1}^{[r/2]}f(\pi^r)f(\pi^{r-2s})=\frac{\pi+1}{\pi-1}\pi^{r-1}(\pi^{r+1}+\pi^{r-1}-2). \tag{4.18}$$

We can summarise this as follows:

Theorem 4.1.7. *The number of coincidence rotations of D_4 of a given index n is given by $576\,c^{rot}_{D_4}(n)$, where $c^{rot}_{D_4}(n)$ is a multiplicative arithmetic function, which is completely determined by $c^{rot}_{D_4}(2^r)=0$ for $r\geq 1$ and*

$$c^{rot}_{D_4}(p^r)=\frac{p+1}{p-1}p^{r-1}(p^{r+1}+p^{r-1}-2)\quad \textit{if } p \textit{ is an odd prime, } r\geq 1. \tag{4.19}$$

The multiplicativity of $c^{rot}_{D_4}(n)$ guarantees that the corresponding Dirichlet series generating function can be written as an Euler product:

$$\begin{aligned}\Psi^{rot}_{D_4}(s)=\sum_{n=1}^{\infty}\frac{c^{rot}_{D_4}(n)}{n^s}&=\prod_{p\neq 2}\frac{(1+p^{-s})(1+p^{1-s})}{(1-p^{1-s})(1-p^{2-s})}\\&=1+\frac{16}{3^s}+\frac{36}{5^s}+\frac{64}{7^s}+\frac{168}{9^s}+\frac{144}{11^s}+\frac{196}{13^s}+\frac{576}{15^s}+\frac{324}{17^s}+\frac{400}{19^s}+\frac{1024}{21^s}+\cdots.\end{aligned} \tag{4.20}$$

It is remarkable that $\Psi^{rot}_{D_4}(s)$ can be expressed in terms of the cubic generating function $\Psi_{\Gamma}(s)$ from Eq.(3.39) and thus in terms of Riemann ζ-functions:

$$\Psi^{rot}_{D_4}(s) = \Psi_{cub}(s)\Psi_{cub}(s-1) = \frac{1-2^{1-s}}{1+2^{-s}}\,\frac{1-2^{2-s}}{1+2^{1-s}}\,\frac{\zeta(s)\zeta(s-1)^2\zeta(s-2)}{\zeta(2s)\zeta(2s-2)} \tag{4.21}$$

This explicit expression shows that $\Psi^{rot}_{D_4}(s)$ is a meromorphic function in the complex plane. Its rightmost pole is at $s=3$ with residue $\frac{630}{\pi^6}\zeta(3)$. Using the theorem of Delange 7.A.1 we obtain the asymptotic behaviour

$$\sum_{n\leq x} c^{rot}_{D_4}(n) \sim \frac{210}{\pi^6}\zeta(3)\,x^3 \approx 0.26257\,x^3 \tag{4.22}$$

as x goes to infinity.

Next, we want to calculate the number $c_{D_4}(n)$ of different CSLs of a given index n. In contrast to the three-dimensional cubic lattices, where we have found $c^{iso}(n) = c(n)$, it turns out that $c_{D_4}(n)$ and $c^{iso}_{D_4}(n)$ are in general different. Clearly, we have the upper bound $c_{D_4}(n) \leq c^{rot}_{D_4}(n)$. To determine $c_{D_4}(n)$ we must find out which coincidence rotations generate the same CSL.

We start with finding necessary conditions. We know from Lemma 3.4.2 that two CSLs can be the same only if the corresponding coincidence indices are the same. In addition, the denominators of the inverses must be equal, but as $\mathrm{den}(R) = \mathrm{den}(R^{-1})$, we infer that the denominators must be the same as well. We want to formulate these conditions in terms of quaternions. Recall from Eq. (4.17) that $\Sigma(R(p,q)) = \mathrm{lcm}(|p|^2,|q|^2)$ and $\mathrm{den}(R(p,q)) = |pq|$, if (p,q) is a primitive admissible pair of odd quaternions. Thus, we have the following result.

Lemma 4.1.8. *Let (q_1,p_1) and (q_2,p_2) be two primitive admissible pairs of odd quaternions. Then,*

$$\mathbb{J} \cap \frac{p_1\mathbb{J}\bar{q}_1}{|p_1q_1|} = \mathbb{J} \cap \frac{p_2\mathbb{J}\bar{q}_2}{|p_2q_2|} \tag{4.23}$$

holds only if $|p_1q_1| = |p_2q_2|$ *and* $\mathrm{lcm}(|p_1|^2,|q_1|^2) = \mathrm{lcm}(|p_2|^2,|q_2|^2)$.

Although equal coincidence indices and denominators are necessary for two CSLs to be equal, these conditions are not sufficient. In fact, we have additional necessary conditions, which are a bit technical. We have seen above that $|pq|\mathbb{J} \subseteq \mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|}$, which implies

$$\mathbb{J} \cap \frac{p\mathbb{J}\bar{q}}{|pq|} = p_\alpha\mathbb{J} + \mathbb{J}\bar{q}_\alpha + |pq|\mathbb{J} = p_r\mathbb{J} + \mathbb{J}\bar{q}_r\,, \tag{4.24}$$

where

$$p_r := \mathrm{gcld}(p_\alpha, |pq|) = \alpha_p\,\mathrm{gcld}\left(p, \frac{|pq|}{\alpha_p}\right) = \alpha_p\,\mathrm{gcld}(p,|pq|) \tag{4.25}$$

$$q_r := \mathrm{gcld}(q_\alpha, |pq|) = \alpha_q\,\mathrm{gcld}\left(q, \frac{|pq|}{\alpha_q}\right) = \alpha_q\,\mathrm{gcld}(q,|pq|). \tag{4.26}$$

Note that $|\operatorname{gcld}(p, \frac{|pq|}{\alpha_p})|^2 = \frac{|pq|}{\alpha_p} = \frac{|p|^2}{\alpha_q}$, which means that $\frac{|p|^2}{|\operatorname{gcld}(p,\frac{|pq|}{\alpha_p})|^2} = \alpha_q$ is coprime to α_p. This explains the last equation in Eq. (4.25). A simple consequence is

$$|\operatorname{gcld}(p,|pq|)|^2 = \frac{|pq|}{\alpha_p} = \frac{|p|^2}{\alpha_q} \quad \text{and} \quad |p_r|^2 = \alpha_p|pq| = \frac{\alpha_p^2|p|^2}{\alpha_q}, \tag{4.27}$$

which we mention for later reference here.

Using the notation we have introduced in the proof of lemma 4.1.5 this means $\operatorname{gcld}(p,|pq|) = g_p k_p$. These equations suggest that $\operatorname{gcld}(p,|pq|)$ and $\operatorname{gcld}(q,|pq|)$ play an important role in deciding whether two CSLs are equal. In fact we have the following result:

Lemma 4.1.9. *Let (q_1, p_1) and (q_2, p_2) be two primitive admissible pairs of odd quaternions with $|p_1 q_1| = |p_2 q_2|$ and $\operatorname{lcm}(|p_1|^2, |q_1|^2) = \operatorname{lcm}(|p_2|^2, |q_2|^2)$. Then,*

$$\mathbb{J} \cap \frac{p_1 \mathbb{J} \bar{q}_1}{|p_1 q_1|} = \mathbb{J} \cap \frac{p_2 \mathbb{J} \bar{q}_2}{|p_2 q_2|} \tag{4.28}$$

holds only if $\operatorname{gcld}(p_1,|p_1q_1|) = \operatorname{gcld}(p_2,|p_2q_2|)$ *and* $\operatorname{gcld}(q_1,|p_1q_1|) = \operatorname{gcld}(q_2,|p_2q_2|)$ *(up to units).*

The idea of the proof is to show that $p_{1r}\mathbb{J} + \mathbb{J}\bar{q}_{1r} = p_{2r}\mathbb{J} + \mathbb{J}\bar{q}_{2r}$ is only possible if $p_{1r} = p_{2r}$ and $q_{1r} = q_{2r}$ (up to units). This involves sets of the form $r\mathbb{J} + \mathbb{J}\bar{s}$, with $r = \operatorname{gcld}(p_{1r}, p_{2r})$ and $s = \operatorname{gcld}(q_{1r}, q_{2r})$. This requires some knowledge on the index of $r\mathbb{J} + \mathbb{J}\bar{s}$. As we cannot guarantee that r and s form an odd extended admissible pair, we cannot apply Lemma 4.1.5. Instead, we need some generalisations of it. For simplicity, we start with two primitive odd quaternions r and s.

Lemma 4.1.10. *If $r, s \in \mathbb{J}$ are primitive and odd, then $[\mathbb{J} : (r\mathbb{J} + \mathbb{J}\bar{s})]$ divides $\gcd(|r|^2, |s|^2)$.*

Proof. The proof is similar to the first part of the proof of Lemma 4.1.5, so we can keep the proof short and omit the details, which can be looked up above. First note that the index $[\mathbb{J} : (r\mathbb{J} + \mathbb{J}\bar{s})]$ certainly divides $|r|^4$, since $(r\mathbb{J} + \mathbb{J}\bar{s}) \supseteq r\mathbb{J}$. Next we determine the minimal m such that $r\mathbb{J} \supseteq m\mathbb{J}\bar{s}$ is satisfied. As above, we find that this minimal m is given by $m = |r|^2$. Note that in this step it is crucial that r and s are primitive and odd. Hence there is an element $x \in \mathbb{J}\bar{s}$ of order $|r|^2$ in $\mathbb{J}\bar{s}/(r\mathbb{J} \cap \mathbb{J}\bar{s})$. This implies that $[(r\mathbb{J} + \mathbb{J}\bar{s}) : r\mathbb{J}]$ is at least $m = |r|^2$, i.e. $[\mathbb{J} : (r\mathbb{J} + \mathbb{J}\bar{s})]$ must divide $\frac{[\mathbb{J}:r\mathbb{J}]}{|r|^2} = |r|^2$. Similarly, $[\mathbb{J} : (r\mathbb{J} + \mathbb{J}\bar{s})]$ must divide $|s|^2$, and hence $[\mathbb{J} : (r\mathbb{I} + \mathbb{J}\bar{s})]$ divides $\gcd(|r|^2, |s|^2)$, as claimed. □

As $\operatorname{gcld}(p_{1r}, p_{2r})$ and $\operatorname{gcld}(q_{1r}, q_{2r})$ are not primitive in general, we need the following more general lemma.

Lemma 4.1.11. *Let $r, s \in \mathbb{J}$ be primitive and odd. Furthermore, let $\beta, \gamma \in \mathbb{Z}$ be coprime. Then $[\mathbb{J} : (\beta r\mathbb{J} + \mathbb{J}\gamma\bar{s})]$ divides $\beta_s^2 \gamma_r^2 \gcd\left(\frac{|r|^2}{\gamma_r}, \frac{|s|^2}{\beta_s}\right)$, where $\beta_s := |\operatorname{gcld}(\beta, s)|^2$ and $\gamma_r := |\operatorname{gcld}(\gamma, r)|^2$.*

Proof. Let us define $g_r := \mathrm{gcld}(\gamma, r) = \mathrm{gcld}(\gamma, \beta r)$ and $g_s := \mathrm{gcld}(\beta, s) = \mathrm{gcld}(\beta, \gamma s)$ and decompose $r = g_r k_r$, $s = g_s k_s$. Then

$$\beta r\mathbb{J} + \mathbb{J}\gamma\bar{s} = r\mathbb{J}(\beta + \gamma\bar{s}) + (\gamma + \beta r)\mathbb{I}\bar{s} = r\mathbb{J}\bar{g}_s + g_r\mathbb{J}\bar{s} = g_r(k_r\mathbb{I} + \mathbb{I}\bar{k}_s)\bar{g}_s. \tag{4.29}$$

Hence

$$[\mathbb{J} : (\beta r\mathbb{J} + \mathbb{J}\gamma\bar{s})] = |g_r|^4|g_s|^4[\mathbb{J} : (k_r\mathbb{J} + \mathbb{J}\bar{k}_s)] = \beta_s^2\gamma_r^2[\mathbb{J} : (k_r\mathbb{J} + \mathbb{J}\bar{k}_s)] \tag{4.30}$$

divides $\beta_s^2\gamma_r^2 \gcd(|k_r|^2, |k_s|^2)$ by the previous lemma, as $K - r$ and k_s are primitive and odd. Observing $|k_r|^2 = \frac{|r|^2}{\gamma_r}$ and $|k_s|^2 = \frac{|s|^2}{\beta_s}$) proves the claim. □

We are ready to prove Lemma 4.1.9 now.

Proof of Lemma 4.1.9. As mentioned above, the idea is to show $p_{1r} = p_{2r}$ and $q_{1r} = q_{2r}$ (up to units), where $p_{ir} = \alpha_{p_i}\,\mathrm{gcld}(p_i, |p_1q_1|)$ and $q_{ir} := \alpha_{q_i}\,\mathrm{gcld}(q_i, |p_1q_1|)$. This proves even more, as this yields $\alpha_{p_1} = \alpha_{p_2}$ and $\alpha_{q_1} = \alpha_{q_2}$ in addition.

By assumption, we have

$$p_{1r}\mathbb{J} + \mathbb{J}\bar{q}_{1r} = p_{2r}\mathbb{J} + \mathbb{J}\bar{q}_{2r} = p'\mathbb{J} + \mathbb{J}\bar{q}', \tag{4.31}$$

where $p' = \mathrm{gcld}(p_{1r}, p_{2r})$ and $q' = \mathrm{gcld}(q_{1r}, q_{2r})$. As p' and q' are in general not primitive, we write them as $p' = \beta r$ and $q' = \gamma s$, where r and s are primitive. This fixes r and s up to a sign, which can be chosen such that $\beta, \gamma \in \mathbb{N}$. Note that $\beta = \gcd(\alpha_{p_1}, \alpha_{p_2})$ and $\gamma = \gcd(\alpha_{q_1}, \alpha_{q_2})$ are coprime, as α_{p_1} and α_{q_1} are. Thus we can apply Lemma 4.1.11 to see that the index $[\mathbb{J} : (p'\mathbb{J} + \mathbb{J}\bar{q}')]$ divides $\beta_s^2\gamma_r^2 \gcd\left(\frac{|r|^2}{\gamma_r}, \frac{|s|^2}{\beta_s}\right)$ and hence divides $\beta_s^2\gamma_r^2 \gcd\left(|r|^2, |s|^2\right)$. Actually, we know the index $[\mathbb{J} : (p'\mathbb{J} + \mathbb{J}\bar{q}')]$ explicitly, as this is the coincidence index $\Sigma(p_1, p_2)$, a fact that we will exploit later. For the moment, we just use the upper bound given above.

By Eq. (4.27), $|p_{ir}|^2 = \alpha_{p_i}|p_iq_i| = \alpha_{p_i}|p_1q_1|$, hence $|p'|^2$ divides $\gcd(\alpha_{p_1}|p_1q_1|, \alpha_{p_2}|p_1q_1|) = \beta|p_1q_1|$, which in turn shows that $|r|^2$ divides $\frac{|p_1q_1|}{\beta}$. Similarly, we see that $|s|^2$ divides $\frac{|p_1q_1|}{\gamma}$. Thus $\gcd\left(|r|^2, |s|^2\right)$ divides $\gcd\left(\frac{|p_1q_1|}{\beta}, \frac{|p_1q_1|}{\gamma}\right) = \frac{|p_1q_1|}{\beta\gamma}$ since β and γ are coprime. As β_s divides β and γ_r divides γ, this shows that $[\mathbb{J} : (p'\mathbb{J} + \mathbb{J}\bar{q}')]$ divides $\beta_s\gamma_r|p_1q_1|$.

On the other hand, $[\mathbb{J} : (p'\mathbb{J} + \mathbb{J}\bar{q}')]$ is just the the coincidence index $\Sigma(R(p_1, q_1))$, which, according to Eq (4.17), is given by

$$\Sigma(R(p_1, q_1)) = \alpha_{p_1}\alpha_{q_1}|p_1q_1| = \alpha_{p_2}\alpha_{q_2}|p_1q_1|$$

– note that $\gcd(|p_1|^2, |q_1|^2) = \gcd(|p_2|^2, |q_2|^2)$ follows from $|p_1q_1| = |p_2q_2|$ and $\mathrm{lcm}(|p_1|^2, |q_1|^2) = \mathrm{lcm}(|p_2|^2, |q_2|^2)$. Hence $\alpha_{p_i}\alpha_{q_i}|p_1q_1|$ must divide $\beta_s\gamma_r|p_1q_1|$. But β_s divides $\beta = \gcd(\alpha_{p_1}, \alpha_{p_2})$ and γ_r divides $\gamma = \gcd(\alpha_{q_1}, \alpha_{q_2})$. Hence we infer $\beta_s = \beta = \alpha_{p_1} = \alpha_{p_2}$ and $\gamma_r = \gamma = \alpha_{q_1} = \alpha_{q_2}$.

Inserting these equations into the arguments above, we see that $\frac{|p_1q_1|}{\alpha_{p_i}\alpha_{q_i}}$ must divide $\gcd\left(\frac{|r|^2}{\alpha_{q_i}}, \frac{|s|^2}{\alpha_{p_i}}\right)$ and hence $\frac{|r|^2}{\alpha_{q_i}}$. As $|r|^2$ divides $\frac{|p_1q_1|}{\alpha_{p_i}}$ this yields $|r|^2 = \frac{|p_1q_1|}{\alpha_{p_i}} = |\,\mathrm{gcld}(p_i, |p_1q_1|)|^2$ by Eq. (4.27). As $\alpha_{p_1} = \alpha_{p_2}$ we see $r = \mathrm{gcld}\left(\mathrm{gcld}(p_1, |p_1q_1|), \mathrm{gcld}(p_2, |p_1q_1|)\right)$ and as the norms are equal we must have $r = \mathrm{gcld}(p_1, |p_1q_1|) = \mathrm{gcld}(p_2, |p_2q_2|)$ (up to units), as claimed. An analogous argument for $s = \mathrm{gcld}(q_1, |p_1q_1|) = \mathrm{gcld}(q_2, |p_2q_2|)$ finishes the proof. □

Remark 4.1.2. The previous proof shows that $\alpha_{p_1} = \alpha_{p_2}$ and $\alpha_{q_1} = \alpha_{q_2}$ are necessary conditions for the equality of CSLs as well. We have not included these conditions in the lemma as they follow from the other conditions. We will prove this claim in the proof of Theorem 4.1.12 below.

In fact, the necessary conditions we have found so far are also sufficient. We summarise this as follows; compare [**16**].

Theorem 4.1.12. *Let (q_1, p_1) and (q_2, p_2) be two primitive admissible pairs of odd quaternions. Then,*

$$\mathbb{J} \cap \frac{p_1 \mathbb{J} \bar{q}_1}{|p_1 q_1|} = \mathbb{J} \cap \frac{p_2 \mathbb{J} \bar{q}_2}{|p_2 q_2|} \tag{4.32}$$

holds if and only if $|p_1 q_1| = |p_2 q_2|$, $\operatorname{lcm}(|p_1|^2, |q_1|^2) = \operatorname{lcm}(|p_2|^2, |q_2|^2)$, $\operatorname{gcld}(p_1, |p_1 q_1|) = \operatorname{gcld}(p_2, |p_2 q_2|)$ and $\operatorname{gcld}(q_1, |p_1 q_1|) = \operatorname{gcld}(q_2, |p_2 q_2|)$ (up to units) hold.

Proof. Of course, the greatest common left divisors are only defined up to multiplication by a unit from the right. W.l.o.g. we will assume throughout the proof that we have chosen the units appropriately so that all equations hold exactly.

We know from Theorem 4.1.3 and the proof of Lemma 4.1.5 that the CSLs can be written as

$$\mathbb{J} \cap \frac{p \mathbb{J} \bar{q}}{|pq|} = p_\alpha \mathbb{J} + \mathbb{J} \bar{q}_\alpha = g_p (k_p \mathbb{J} + \mathbb{J} \bar{k}_q) \bar{g}_q, \tag{4.33}$$

where we have used the notation from Lemma 4.1.5.

As we have shown that the conditions are necessary in Lemma 4.1.8 and Lemma 4.1.9, it remains to show that the conditions are sufficient. We will do this by checking that they imply $g_{p_1} = g_{p_2}, g_{q_1} = g_{q_2}$ and $k_{p_1} = k_{p_2}, k_{q_1} = k_{q_2}$, which will prove our claim via Eq. (4.33).

By definition, we have $g_p = \operatorname{gcld}(p, \alpha_q)$ and $k_p = \operatorname{gcld}(h_p, \gcd(|p|^2, |q|^2))$, which can be used to verify $\operatorname{gcld}(p, |pq|) = \operatorname{gcld}(p, \alpha_p \alpha_q \gcd(|p|^2, |q|^2)) = g_p k_p$, and likewise $\operatorname{gcld}(q, |pq|) = g_q k_q$. By assumption, $\operatorname{gcld}(p_1, |p_1 q_1|) = \operatorname{gcld}(p_2, |p_2 q_2|)$, which yields $g_{p_1} k_{p_1} = g_{p_2} k_{p_2}$, and similarly $\operatorname{gcld}(q_1, |p_1 q_1|) = \operatorname{gcld}(q_2, |p_2 q_2|)$ gives $g_{q_1} k_{q_1} = g_{q_2} k_{q_2}$. These equations will give $g_{p_1} = g_{p_2}, g_{q_1} = g_{q_2}$ and $k_{p_1} = k_{p_2}, k_{q_1} = k_{q_2}$ via the unique prime factorisation in $\mathbb{J}$, if we can prove $|k_{p_1}|^2 = |k_{p_2}|^2$ and $|k_{q_1}|^2 = |k_{q_2}|^2$ (recall that we have the freedom to choose the units appropriately).

So it remains to prove $|k_{p_1}|^2 = |k_{p_2}|^2$ and $|k_{q_1}|^2 = |k_{q_2}|^2$. We know $|k_{p_i}|^2 = |k_{q_i}|^2 = \gcd(|p_i|^2, |q_i|^2)$ from Eq. (4.16). Hence it is sufficient to show $\gcd(|p_1|^2, |q_1|^2) = \gcd(|p_2|^2, |q_2|^2)$. By assumption, $\operatorname{lcm}(|p_1|^2, |q_1|^2) = \operatorname{lcm}(|p_2|^2, |q_2|^2)$ and $|p_1 q_1| = |p_2 q_2|$. By Eq. (4.17) we have $\operatorname{lcm}(|p_i|^2, |q_i|^2) = \alpha_{p_i} \alpha_{q_i} |p_i q_i|$, which gives $\alpha_{p_1} \alpha_{q_1} = \alpha_{p_2} \alpha_{q_2}$. Now, we can invoke $\operatorname{lcm}(|p_i|^2, |q_i|^2) = \alpha_{p_i}^2 \alpha_{q_i}^2 \gcd(|p_i|^2, |q_i|^2)$ to prove $\gcd(|p_1|^2, |q_1|^2) = \gcd(|p_2|^2, |q_2|^2)$, which concludes this part of the proof.

Let us remark here that $g_{p_1} = g_{p_2}, g_{q_1} = g_{q_2}$ implies $\alpha_{p_1} = \alpha_{p_2}$ and $\alpha_{q_1} = \alpha_{q_2}$, which gives $|p_1|^2 = |p_2|^2$ and $|q_1|^2 = |q_2|^2$ in addition. □

REMARK 4.1.3. A more technical but equivalent set of conditions for two CSLs to be equal is $|p_1|^2 = |p_2|^2$, $|q_1|^2 = |q_2|^2$, $\operatorname{gcld}(p_1, |p_1q_1|) = \operatorname{gcld}(p_2, |p_2q_2|)$ and $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$. It is obvious that the two conditions $|p_1|^2 = |p_2|^2$ and $|q_1|^2 = |q_2|^2$ imply that the denominators $|p_1q_1| = |p_2q_2|$ and coincidence indices $\operatorname{lcm}(|p_1|^2, |q_1|^2) = \operatorname{lcm}(|p_2|^2, |q_2|^2)$ are the same. The reverse direction is more complicated as the two conditions $|p_1q_1| = |p_2q_2|$ and $\operatorname{lcm}(|p_1|^2, |q_1|^2) = \operatorname{lcm}(|p_2|^2, |q_2|^2)$ alone only yield $\gcd(|p_1|^2, |q_1|^2) = \gcd(|p_2|^2, |q_2|^2)$ but not $|p_1|^2 = |p_2|^2$ and $|q_1|^2 = |q_2|^2$ directly. In fact we need the other two conditions $\operatorname{gcld}(p_1, |p_1q_1|) = \operatorname{gcld}(p_2, |p_2q_2|)$ and $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ to establish $|p_1|^2 = |p_2|^2$ and $|q_1|^2 = |q_2|^2$ as well, as we have seen in the proof above.

We are ready to count the number $c_{D_4}(n)$ of CSLs now. It follows from Theorem 3.4.11 that $c_{D_4}(n)$ is multiplicative, since $c^{iso}_{D_4}(n)$ is multiplicative. As there are no CSLs of even index, $c_{D_4}(n)$ is completely determined by $c_{D_4}(\pi^r)$ for rational primes π. The latter can be calculated by counting the number of odd primitive admissible pairs satisfying the conditions in Theorem 4.1.12 or in Remark 4.1.3. Thus

$$c_{D_4}(\pi^r) = f(\pi^r)^2 + 2\sum_{s=1}^{[r/2]} f(\pi^{r-s}) f(\pi^{r-2s}), \tag{4.34}$$

where $f(\pi^r) = (\pi+1)\pi^{r-1}$ for $r \geq 1$, as above. Note that this expression is very similar to Eq. (4.18), the only difference is that a factor $f(\pi^r)$ is replaced by $f(\pi^{r-s})$, where the latter counts the number of different $\operatorname{gcld}(p, |pq|)$ with $|p|^2 = \pi^r$ and $|q|^2 = \pi^{r-2s}$.

Evaluating the sum yields the following result:

THEOREM 4.1.13. *The number of different CSLs of D_4 of a given index n is given by $c_{D_4}(n)$, where $c_{D_4}(n)$ is a multiplicative arithmetic function, which is completely determined by $c_{D_4}(2^r) = 0$ for $r \geq 1$ and*

$$c_{D_4}(p^r) = \begin{cases} \frac{(p+1)^2}{p^3-1}\left(p^{2r+1} + p^{2r-2} - 2p^{(r-1)/2}\right), & \text{if } r \geq 1 \text{ is odd,} \\ \frac{(p+1)^2}{p^3-1}(p^{2r+1} + p^{2r-2} - 2p^{r/2-1}\frac{1+p^2}{1+p}), & \text{if } r \geq 2 \text{ is even,} \end{cases} \tag{4.35}$$

for odd primes p. The corresponding Dirichlet series reads

$$\begin{aligned} \Psi_{D_4}(s) = \sum_{n=1}^{\infty} \frac{c_{D_4}(n)}{n^s} &= \prod_{p\neq 2} \frac{1 + p^{-s} + 2p^{1-s} + 2p^{-2s} + p^{1-2s} + p^{1-3s}}{(1-p^{2-s})(1-p^{1-2s})} \\ &= 1 + \frac{16}{3^s} + \frac{36}{5^s} + \frac{64}{7^s} + \frac{152}{9^s} + \frac{144}{11^s} + \frac{196}{13^s} + \frac{576}{15^s} + \frac{324}{17^s} + \frac{400}{19^s} + \frac{1024}{21^s} + \cdots . \end{aligned} \tag{4.36}$$

Unfortunately, there is no nice representation of $\Psi_{D_4}(s)$ as a product of Riemann ζ-functions. Nevertheless, we can use Delange's theorem 7.A.1 to calculate the asymptotic behaviour.

Note that $\Psi_{D_4}(s)$ is quite similar to $\Psi^{rot}_{D_4}(s)$, see Eq. (4.21). In fact, differences between them occur only for those integers that are divisible by the square of an odd prime. Thus the rightmost pole of $\Psi_{D_4}(s)$ is at $s = 3$, which is the same as for $\Psi^{rot}_{D_4}(s)$. This implies the asymptotic behaviour $\sum_{n\leq x} c_{D_4}(n) \sim cx^3$ as x goes to infinity for some positive constant c. To be more specific, we consider the ratio

$$\frac{\Psi_{D_4}(s)}{\Psi^{rot}_{D_4}(s)} = \prod_{p\neq 2}\left(1-2\frac{(p^2-1)p^{-2s}}{(1+p^{-s})(1+p^{1-s})(1-p^{1-2s})}\right), \tag{4.37}$$

where the right hand side is an analytic function in the half plane $\{\mathrm{Re}(s) > \frac{3}{2}\}$ with

$$\gamma := \lim_{s\to 3}\frac{\Psi_{D_4}(s)}{\Psi^{rot}_{D_4}(s)} = \prod_{p\neq 2}\left(1-2\frac{(p^2-1)p^{-6}}{(1+p^{-2})(1+p^{-3})(1-p^{-5})}\right) \approx 0.976966 < 1. \tag{4.38}$$

Hence $\sum_{n\leq x} c_{D_4}(n)$ grows by a factor γ slower than $\sum_{n\leq x} c^{rot}_{D_4}(n)$. In particular, we obtain

$$\sum_{n\leq x} c_{D_4}(n) \sim \frac{210}{\pi^6}\zeta(3)\gamma\, x^3 \approx 0.25652x^3, \tag{4.39}$$

as x goes to infinity. This shows that $\sum_{n\leq x} c^{rot}_{D_4}(n)$ and $\sum_{n\leq x} c_{D_4}(n)$ differ by less than 2.5% asymptotically, which means that it is quite rare that two coincidence rotations that are not symmetry related generate the same CSL.

As we have determined the number of different CSLs, we might ask the question how many non-equivalent CSLs there are, where we call two CSLs Λ_1 and Λ_2 equivalent if there is an $R \in \mathrm{O}(\mathbb{J})$ such that $\Lambda_2 = R\Lambda_1$. This question is not completely answered yet, but some partial answers can be found in [**74**].

4.2. Primitive hypercubic lattice

Let us consider the primitive hypercubic lattice now, which we will identify with $\mathbb{Z}^4$, or in terms of quaternions, with the ring of Lipschitz quaternions $\mathbb{L}$. As $\mathbb{Z}^4$ and D_4 are commensurate, they have the same group of coincidence rotations, i.e. $\mathrm{SOC}(\mathbb{Z}^4) = \mathrm{SOC}(D_4) = \mathrm{SO}(4,\mathbb{Q})$.

Moreover, we have $D_4^* \subset \mathbb{Z}^4 \subset D_4$, where $\mathbb{Z}^4$ is a sublattice of D_4 of index 2. Thus the coincidence indices of the two lattices can differ at most by a factor 2 by Theorem 3.1.9. This means that we have either $\Sigma_{\mathbb{Z}^4} = \Sigma_{D_4}(R)$ or $\Sigma_{\mathbb{Z}^4} = 2\Sigma_{D_4}(R)$ for a given coincidence rotation R. Actually, both cases do occur.

This becomes clear immediately, if we recall that the primitive hypercubic lattice $\mathbb{Z}^4$, has a smaller symmetry group than D_4, containing only 192 rotations, so that $[\mathrm{SO}(D_4) : \mathrm{SO}(\mathbb{Z}^4)] = [\mathrm{O}(D_4) : \mathrm{O}(\mathbb{Z}^4)] = 3$. As a consequence, every class of symmetry related coincidence rotations of D_4 splits into three classes of $\mathbb{Z}^4$. In particular, all rotations in $\mathrm{SO}(D_4) \setminus \mathrm{SO}(\mathbb{Z}^4)$ are coincidence rotations of $\mathbb{Z}^4$ of index 2, so we have one class with coincidence index 1 and two classes with index 2.

The same pattern emerges for all the other coincidence rotations – and more generally, for coincidence isometries as well. In particular, every class of symmetry related coincidence rotations of D_4 splits into three classes, one of which has the same coincidence index as before, $\Sigma_{\mathbb{Z}^4}(R) = \Sigma_{D_4}(R)$, while the other two classes have index $\Sigma_{\mathbb{Z}^4}(R) = 2\Sigma_{D_4}(R)$. To see this, we recall that $\mathrm{den}_{\mathbb{Z}^4}(R)$ divides $\varSigma_{\mathbb{Z}^4}(R)$ and $\varSigma_{\mathbb{Z}^4}(R)$ divides $\mathrm{den}_{\mathbb{Z}^4}(R)^4$ by Theorem 3.2.7. So $\varSigma_{\mathbb{Z}^4}(R)$ is even if and only if $\mathrm{den}_{\mathbb{Z}^4}(R)$ is, or in other words,

$$\varSigma_{\mathbb{Z}^4}(R) = \mathrm{lcm}\left(\varSigma_{D_4}(R), \mathrm{den}_{\mathbb{Z}^4}(R)\right), \tag{4.40}$$

compare [**4**]. If (p, q) is an odd primitive admissible pair, then we have

$$\mathrm{den}_{\mathbb{Z}^4}(R(p,q)) = \begin{cases} |pq| & \text{if } \langle p,q\rangle \in \mathbb{Z} \\ 2|pq| & \text{if } \langle p,q\rangle \notin \mathbb{Z}, \end{cases} \tag{4.41}$$

and if (p, q) is an even primitive admissible pair, then

$$\mathrm{den}_{\mathbb{Z}^4}(R(p,q)) = \begin{cases} \frac{|pq|}{2} & \text{if } \langle p,q\rangle \text{ is even} \\ |pq| & \text{if } \langle p,q\rangle \text{ is odd.} \end{cases} \tag{4.42}$$

Checking for all possible combinations of units, we see that indeed every class of symmetry related coincidence rotations of D_4 splits into three classes, one of which has odd denominator and coincidence index $\varSigma_{\mathbb{Z}^4}(R) = \varSigma_{D_4}(R)$, while the other two classes have even denominator and coincidence index $\varSigma_{\mathbb{Z}^4}(R) = 2\varSigma_{D_4}(R)$.

In order to get an explicit expression for the CSLs we consider the following chain of inclusions

$$D_4^* \cap RD_4^* \subseteq \mathbb{Z}^4 \cap R\mathbb{Z}^4 \subseteq D_4 \cap RD_4 \cap \mathbb{Z}^4 \subset D_4 \cap RD_4 \tag{4.43}$$

for any $R \in \mathrm{SOC}(D_4)$. As $\varSigma_{D_4^*}(R) = \varSigma_{D_4}(R)$ by Lemma 3.1.4 and $[D_4 : D_4^*] = 4$, we conclude that $[(D_4 \cap RD_4) : (D_4^* \cap RD_4^*)] = 4$. Moreover, as $[D_4 : \mathbb{Z}^4] = 2$, this shows $[(D_4 \cap RD_4 \cap \mathbb{Z}^4) : (D_4^* \cap RD_4^*)] = 2$, as $\varSigma_{D_4}(R)$ is always odd. Thus, we are left with two possibilities, $\mathbb{Z}^4 \cap R\mathbb{Z}^4 = D_4 \cap RD_4 \cap \mathbb{Z}^4 = \mathbb{Z}^4 \cap RD_4$, in which case we have $\varSigma_{\mathbb{Z}^4}(R) = \varSigma_{D_4}(R)$, or $\mathbb{Z}^4 \cap R\mathbb{Z}^4 = D_4^* \cap RD_4^*$, where we have $\varSigma_{\mathbb{Z}^4}(R) = 2\varSigma_{D_4}(R)$ instead.

Let us summarise these results as follows:

PROPOSITION 4.2.1. *For any coincidence rotation* $R \in \mathrm{SOC}(\mathbb{Z}^4)$ *the coincidence index is given by*

$$\varSigma_{\mathbb{Z}^4}(R) = \mathrm{lcm}\left(\varSigma_{D_4}(R), \mathrm{den}_{\mathbb{Z}^4}(R)\right), \tag{4.44}$$

which is even if and only if $\mathrm{den}_{\mathbb{Z}^4}(R)$ *is even. The corresponding CSL is given by*

$$\mathbb{Z}^4 \cap R\mathbb{Z}^4 = \begin{cases} (D_4 \cap RD_4) \cap \mathbb{Z}^4 = \mathbb{Z}^4 \cap RD_4 & \textit{if } \varSigma_{\mathbb{Z}^4}(R) \textit{ is even,} \\ D_4^* \cap RD_4^* & \textit{if } \varSigma_{\mathbb{Z}^4}(R) \textit{ is odd.} \end{cases} \tag{4.45}$$

This allows us to determine the number of coincidence rotations, which is given by $192 c^{rot}_{\mathbb{Z}^4}(n)$, as the symmetry group $\mathrm{SO}(\mathbb{Z}^4)$ has order 192. By the considerations above, each class of symmetry related coincidence rotations splits into three classes, one with coincidence index $\varSigma_{\mathbb{Z}^4}(R) = \varSigma_{D_4}(R)$, and two with index $\varSigma_{\mathbb{Z}^4}(R) = 2\varSigma_{D_4}(R)$. This gives

$$c^{rot}_{\mathbb{Z}^4}(n) = \begin{cases} c^{rot}_{D_4}(n) & \text{if } n \text{ is odd,} \\ 2c^{rot}_{D_4}\left(\frac{n}{2}\right) & \text{if } n \text{ is even.} \end{cases} \tag{4.46}$$

As $c^{rot}_{D_4}(n)$ is multiplicative, so is $c^{rot}_{\mathbb{Z}^4}(n)$, and the corresponding Dirichlet series admits again an Euler product. In particular, we have the following result (compare also [**4, 74**]):

THEOREM 4.2.2. *The generating function for the number $c^{rot}_{\mathbb{Z}^4}(n)$ of coincidence rotations of $\mathbb{Z}^4$ is given by*

$$\Psi^{rot}_{\mathbb{Z}^4}(s) = \sum_{n=1}^{\infty} \frac{c^{rot}_{\mathbb{Z}^4}(n)}{n^s} = (1+2^{1-s})\Psi^{rot}_{D_4}(s) = (1+2^{1-s}) \prod_{p\neq 2} \frac{(1+p^{-s})(1+p^{1-s})}{(1-p^{1-s})(1-p^{2-s})}$$
$$= 1 + \frac{2}{2^s} + \frac{16}{3^s} + \frac{36}{5^s} + \frac{32}{6^s} + \frac{64}{7^s} + \frac{168}{9^s} + \frac{72}{10^s} + \frac{144}{11^s} + \frac{196}{13^s} + \frac{128}{14^s} + \frac{576}{15^s} + \frac{324}{17^s} + \cdots$$

It is a meromorphic function in the complex plane, whose rightmost pole is located at $s = 3$ with residue $\frac{1575}{2\pi^6}\zeta(3)$. Consequently, we have the asymptotic behaviour

$$\sum_{n\leq x} c^{rot}_{\mathbb{Z}^4}(n) \sim \frac{525}{2\pi^6}\zeta(3)\, x^3 \approx 0.32821\, x^3, \tag{4.47}$$

as x goes to infinity.

PROOF. It follows from Eq. (4.46) that $\Psi^{rot}_{\mathbb{Z}^4}(s)$ is obtained from $\Psi^{rot}_{D_4}(s)$ by adding a factor $1 + 2^{1-s}$. As the latter is analytic, the analytic behaviour of $\Psi^{rot}_{\mathbb{Z}^4}(s)$ is the same as that of $\Psi^{rot}_{D_4}(s)$ (see Theorem 4.1.7 and the comments thereafter), except for some poles on the line $\mathrm{Re}(s) = 1$ which are cancelled by the factor $1 + 2^{1-s}$. An application of Delange's theorem 7.A.1 finally yields the asymptotic behaviour. □

In a similar way we can determine the number of CSLs. It follows from Proposition 4.2.1 that each CSL of D_4 corresponds to exactly one pair of CSLs of Z^4, one of which has odd index and the other one has even index. Note that the explicit expressions for the CSLs in Proposition 4.2.1 guarantee that two CSLs of $\mathbb{Z}^4$ are only equal if the corresponding CSLs of D_4 are equal. This implies that the number of CSLs is given by

$$c_{\mathbb{Z}^4}(n) = \begin{cases} c_{D_4}(n) & \text{if } n \text{ is odd,} \\ c_{D_4}\left(\frac{n}{2}\right) & \text{if } n \text{ is even.} \end{cases} \tag{4.48}$$

This yields the following result:

THEOREM 4.2.3. *The generating function for the number $c_{\mathbb{Z}^4}(n)$ of CSLs of $\mathbb{Z}^4$ is given by*

$$\Psi_{\mathbb{Z}^4}(s) = (1+2^{-s})\Psi_{D_4}(s) = (1+2^{-s}) \prod_{p\neq 2} \frac{1+p^{-s}+2p^{1-s}+2p^{-2s}+p^{1-2s}+p^{1-3s}}{(1-p^{2-s})(1-p^{1-2s})}$$
$$= 1 + \frac{1}{2^s} + \frac{16}{3^s} + \frac{36}{5^s} + \frac{16}{6^s} + \frac{64}{7^s} + \frac{152}{9^s} + \frac{36}{10^s} + \frac{144}{11^s} + \frac{196}{13^s} + \frac{64}{14^s} + \frac{576}{15^s} + \frac{324}{17^s} + \cdots .$$

It is a meromorphic function in the half plane $\{\mathrm{Re}(s) > \frac{3}{2}$, whose rightmost pole is located at $s = 3$ with residue $\frac{2835}{4\pi^6}\zeta(3)\gamma$, where γ is the constant given in Eq. (4.38). Consequently, we *have the asymptotic behaviour*

$$\sum_{n\leq x} c_{\mathbb{Z}^4}(n) \sim \frac{945}{4\pi^6}\zeta(3)\gamma\, x^3 \approx 0.28859\, x^3, \tag{4.49}$$

as x goes to infinity.

CHAPTER 5

Coincidences of the lattice A_4 and the icosian ring

Our next aim is to discuss the coincidence problem of the A_4-lattice, which is another root lattice in $\mathbb{R}^4$. It plays an important role in the theory of quasicrystals, as it is used to construct the well-known Penrose patterns [**7**]. Throughout this chapter, we shall denote it by L. As the A_4-lattice is closely related to the icosian ring $\mathbb{I}$, we will discuss $\mathbb{I}$ as well. In fact, as $\mathbb{I}$ is a ring but L is not, some results are more easily obtained for $\mathbb{I}$ than for L. Thus it makes sense to derive some results for the CSLs of L from the corresponding results for $\mathbb{I}$. Nevertheless, we will treat the A_4-lattice first and defer some proofs to the discussion of $\mathbb{I}$ wherever it is appropriate.

Usually, the A_4 lattice – we will denote it by L in the following – is embedded in $\mathbb{R}^5$ as a lattice plane. However, this is inconvenient for our purposes and we prefer to look at it in $\mathbb{R}^4$, since we want to exploit the useful parametrisation by quaternions, which we do not have at hand in 5 dimensions. A possible basis for L consists of the 4 vectors (compare [**9**])

$$(1,0,0,0),\ \frac{1}{2}(-1,1,1,1),\ (0,-1,0,0),\ \frac{1}{2}(0,1,\tau-1,-\tau), \tag{5.1}$$

where $\tau = \frac{1+\sqrt{5}}{2}$ is the golden mean whose algebraic conjugate τ' can be written as $\tau' = -\frac{1}{\tau} = 1-\tau$. The lattice L cannot be identified with a ring of quaternions. However, if we interpret the basis vectors as quaternions, they relate to the icosian ring $\mathbb{I}$, which is the $\mathbb{Z}[\tau]$-span of the 4 quaternions

$$(1,0,0,0),\ (0,1,0,0),\ \frac{1}{2}(1,1,1,1),\ \frac{1}{2}(1-\tau,\tau,0,1). \tag{5.2}$$

In addition to $\mathbb{I}$, we will frequently use the $\mathbb{Z}[\tau]$-span of the vectors in (5.1), which we call $L[\tau]$. Algebraically, it is the tensor product $\mathbb{Z}[\tau]\otimes_{\mathbb{Z}} L$ and can be written as the direct sum $L+\tau L$, compare [**9**]. We have $L[\tau]\subset\mathbb{I}$ with index $[\mathbb{I} : L[\tau]] = 5$.

We know from Section 3.2 that there are close connections between the SSLs and CSLs. In particular, $\mathrm{OC}(L)$ is a normal subgroup of $\mathrm{OS}(L)$. Thus, it is useful to recall the basic results for the SSLs of A_4, which have been discussed in [**9**] by M. Baake and M. Heuer. We will closely follow their notation here.

5.1. Similar sublattices of A_4

Let us discuss some properties of the A_4 lattice first. Both L and $\mathbb{I}$ are invariant under conjugation, i.e., $L=\bar{L}$ and $\mathbb{I}=\bar{\mathbb{I}}$, but neither of them is invariant under algebraic conjugation $\tau\mapsto\tau'$. Combining the algebraic conjugation with a permutation of the last two components yields an involution of the second kind $\tilde{x} := (x_0', x_1', x_3', x_2')$, which was called twist map in [**9, 8**]. Note that $L = \tilde{L}$ is invariant under the twist map, which, in addition, is an antiautomorphism of $\mathbb{I}$. It is worth to recall the following properties [**9**, Lemma 1] for any $x, y \in \mathbb{I}$ and $\alpha \in \mathbb{Q}(\tau)$

(1) $\widetilde{x+y} = \tilde{x} + \tilde{y}$ and $\widetilde{\alpha x} = \alpha' \tilde{x}$,
(2) $\widetilde{xy} = \tilde{y}\tilde{x}$ and $\tilde{\tilde{x}} = x$,
(3) $\tilde{\bar{x}} = \bar{\tilde{x}}$ and, for $x \neq 0$, $(\tilde{x})^{-1} = \widetilde{x^{-1}}$.

The twist map is the key to our analysis as it gives us a convenient parametrisation of the similarity rotations – and thus the coincidence rotations. Furthermore, it provides us with the following characterisation of the lattice L (see [**9**, Proposition 1])

$$L = \{x \in \mathbb{I} \mid x = \tilde{x}\}. \tag{5.3}$$

By Cayley's parametrisation (4.1), we know that any rotation in 4 dimensions can be written as $R(p,q)x = \frac{1}{|pq|} pxq$. Using the properties of the twist map and the characterisation of L from above, we immediately see that $qL\tilde{q} \subseteq L$ is a similar sublattice of L for any $q \in \mathbb{I}$. In fact, any SSL of L is of the form $\alpha qL\tilde{q} \subseteq L$, with $q \in \mathbb{I}$ and $\alpha \in \mathbb{Q}(\tau)^*$, see [**9**, Corollary 1]).

In order to fully characterise the SSLs, it is convenient to introduce the notion of an $\mathbb{I}$-primitive quaternion, which is the complete analogue of primitive quaternions we have used in the discussion of the 3-dimensional cubic and 4-dimensional hypercubic lattices. We call a quaternion $q \in \mathbb{I}$ $\mathbb{I}$-*primitive* (or primitive for short) if $\alpha q \in \mathbb{I}$ with $\alpha \in \mathbb{Q}(\tau)$ implies $\alpha \in \mathbb{Z}[\tau]$. Equivalently, $q \in \mathbb{I}$ is $\mathbb{I}$-primitive if the $\mathbb{I}$-content of q,

$$\mathrm{cont}_{\mathbb{I}}(q) := \mathrm{lcm}\{\alpha \in \mathbb{Z}[\tau] \setminus \{0\} \mid q \in \alpha\mathbb{I}\} \tag{5.4}$$

is a unit in $\mathbb{Z}[\tau]$. Note that the definition of lcm makes sense as $\mathbb{Z}[\tau]$ is a Euclidean domain. Of course, $\mathrm{cont}_{\mathbb{I}}(q)$ is defined only up to a unit in $\mathbb{Z}[\tau]$. We can now fully characterise the SSLs [**9**, Corollary 2].

Lemma 5.1.1. *The primitive SSLs of L are precisely the the sublattices of the form $qL\tilde{q}$, where $q \in \mathbb{I}$ is $\mathbb{I}$-primitive.*

More generally, the SSLs of L are precisely those lattices of the form $nqL\tilde{q}$ with $n \in \mathbb{N}$ and $q \in \mathbb{I}$ primitive.

As we want to determine the number of different SSLs, we must make sure that we do not count the same SSL twice. In general, different quaternions may generate the same SSL, so we need a criterion, when two SSLs $qL\tilde{q}$ and $pL\tilde{p}$ are equal. One first observes that $L = qL\tilde{q}$ for an $\mathbb{I}$-primitive quaternion q if and only if $q \in \mathbb{I}^{\times}$, where $\mathbb{I}^{\times}$ is the group of unit quaternions in $\mathbb{I}$. From this, one can infer the following result [**9**, Lemma 5].

Lemma 5.1.2. *For $\mathbb{I}$-primitive quaternions $p, q \in \mathbb{I}$ one has $qL\tilde{q} = pL\tilde{p}$ if and only if $q\mathbb{I} = p\mathbb{I}$.*

This lemma reduces the problem of counting SSLs of L to the problem of counting primitive right ideals of $\mathbb{I}$. Here, we call a right ideal $q\mathbb{I}$ primitive, if q is $\mathbb{I}$-primitive.

The index of a primitive SSL can be determined by explicit calculations. We mention that $|\tilde{q}|^2 = (|q|^2)'$ holds for any $q \in \mathbb{I}$. Recall that the norm in $\mathbb{Q}(\tau)$ is defined as

$$\mathrm{Nr}(\alpha) = \alpha\alpha' \tag{5.5}$$

for any $\alpha \in \mathbb{Q}(\tau)$. Therefore, the index of a primitive SSL $qL\tilde{q}$ is given by $[L : qL\tilde{q}] = \mathrm{Nr}(|q|^4)$. As $q\mathbb{I}$ has index $\mathrm{Nr}(|q|^4)$ in $\mathbb{I}$ as well, we have established the following result [**9**, Proposition 4].

LEMMA 5.1.3. *There is a bijective correspondence between the primitive right ideals of* $\mathbb{I}$ *and the primitive SSLs of* L*, defined by* $q\mathbb{I} \mapsto qL\tilde{q}$*. This bijection preserves the indices, i.e., we have*

$$[\mathbb{I} : q\mathbb{I}] = \mathrm{Nr}(|q|^4) = [L : qL\tilde{q}]. \tag{5.6}$$

As a consequence, all possible indices are squares of integers of the form $k^2 + k\ell - \ell^2 = \mathrm{Nr}(k + \ell\tau)$. In fact, all of those indices are realised, compare [**9, 46**]. As the numbers of right ideals $\mathbb{I}$ of a given index are well known, we can deduce the numbers $b_{A_4}(m)$ and $b^{\mathsf{pr}}_{A_4}(m)$ of SSLs and primitive SSLs of index m, respectively. This can be done most efficiently by using the corresponding Dirichlet series generating functions. To explicitly state them, we need to introduce some notation. We first define the Dirichlet character

$$\chi_5(n) = \begin{cases} 0, & \text{if } n \equiv 0 \pmod 5 \\ 1, & \text{if } n \equiv \pm 1 \pmod 5 \\ -1, & \text{if } n \equiv \pm 2 \pmod 5. \end{cases} \tag{5.7}$$

Its corresponding L-series $L(s, \chi_5) = \sum_{n=1}^{\infty} \chi_5(n) n^{-s}$ can be analytically continued to the complete complex plane and thus defines an entire function. The Dedekind zeta function of $K = \mathbb{Q}(\tau)$ is given by $\zeta_K(s) = \zeta(s) L(s, \chi_5)$, which is a meromorphic function. Likewise, the zeta function $\zeta_{\mathbb{I}}$ of the icosian ring counting the right (or left) ideals of $\mathbb{I}$ is meromorphic in the entire complex plane and reads

$$\zeta_{\mathbb{I}}(s) = \zeta_K(2s)\zeta_K(2s-1). \tag{5.8}$$

As the Dirichlet series of the two-sided ideals is given by $\zeta_K(4s)$, we obtain the zeta function $\zeta^{\mathsf{pr}}_{\mathbb{I}}$ of the primitive ideals as

$$\zeta^{\mathsf{pr}}_{\mathbb{I}}(s) = \frac{\zeta_K(2s)\zeta_K(2s-1)}{\zeta_K(4s)}. \tag{5.9}$$

This leads to the following result [**9**, Theorem 1].

THEOREM 5.1.4. *The Dirichlet series generating functions for the numbers* $b_{A_4}(n)$ *and* $b^{\mathsf{pr}}_{A_4}(n)$ *of SSLs and primitive SSLs of the* A_4*-lattice read as follows*

$$\Phi_{A_4}(s) = \sum_{n \in \mathbb{N}} \frac{b_{A_4}(n)}{n^s} = \zeta(4s) \frac{\zeta_{\mathbb{I}}(s)}{\zeta_K(4s)} = \frac{\zeta_K(2s)\zeta_K(2s-1)}{L(4s, \chi_5)} \tag{5.10}$$

and

$$\Phi^{\mathsf{pr}}_{A_4}(s)=\sum_{n\in\mathbb{N}}\frac{b^{\mathsf{pr}}_{A_4}(n)}{n^s}=\zeta^{\mathsf{pr}}_{\mathbb{I}}(s)=\frac{\zeta_K(2s)\zeta_K(2s-1)}{\zeta_K(4s)}. \tag{5.11}$$

As the Euler products of these functions are known, we get the following Euler products for Φ_{A_4} and $\Phi^{\mathsf{pr}}_{A_4}$, compare [**9**]

(5.12)

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

and

$$\Phi^{\mathsf{pr}}_{A_4}(s)=\frac{1+5^{-2s}}{1-5^{1-2s}}\prod_{p\equiv\pm1(5)}\frac{(1+p^{-2s})^2}{(1-p^{1-2s})^2}\prod_{p\equiv\pm2(5)}\frac{1+p^{-4s}}{1-p^{2-4s}} \tag{5.13}$$

From these formulas we get the following explicit values for $b_{A_4}(n)$ and $b^{\mathsf{pr}}_{A_4}(n)$, which are both multiplicative functions. Thus they are both determined by there values for prime powers. As $b_{A_4}(p^{2r+1})=b^{\mathsf{pr}}_{A_4}(p^{2r+1})=0$, we only need to state their values for even prime powers $2r\geq 2$. They read [**9**]

$$b_{A_4}(p^{2r})=\begin{cases}\frac{5^{r+1}-1}{4}, & \text{if } p=5,\\ \frac{2(1-p^{r+1})-(r+1)(1-p^2)p^r}{(1-p)^2}, & \text{if } p\equiv\pm1 \pmod 5,\\ \frac{2-p^r-p^{r+2}}{1-p^2} & \text{if } p\equiv\pm2 \pmod 5 \text{ and } r \text{ even},\\ 0, & \text{if } p\equiv\pm2 \pmod 5 \text{ and } r \text{ odd},\end{cases} \tag{5.14}$$

and

$$b^{\mathsf{pr}}_{A_4}(p^{2r})=\begin{cases}6\cdot5^{r-1}, & \text{if } p=5,\\ (r+1)p^r+2rp^{r-1}+(r-1)p^{r-2}, & \text{if } p\equiv\pm1 \pmod 5,\\ p^r+p^{r-2}, & \text{if } p\equiv\pm2 \pmod 5 \text{ and } r \text{ even},\\ 0, & \text{if } p\equiv\pm2 \pmod 5 \text{ and } r \text{ odd}.\end{cases} \tag{5.15}$$

It follows from these formulas that all possible indices are not only realised for some SSL, but even realised for some primitive SSL. In fact, most SSLs of a given index are primitive. This can be illustrated by mentioning the first few terms of Φ_{A_4} and $\Phi^{\mathsf{pr}}_{A_4}$, respectively

$$\Phi_{A_4}(s)=1+\frac{6}{4^{2s}}+\frac{6}{5^{2s}}+\frac{11}{9^{2s}}+\frac{24}{11^{2s}}+\frac{26}{16^{2s}}+\frac{40}{19^{2s}}+\frac{36}{20^{2s}}+\frac{31}{25^{2s}}+\frac{60}{29^{2s}}+\cdots, \tag{5.16}$$

and

$$\Phi^{\mathsf{pr}}_{A_4}(s)=1+\frac{5}{4^{2s}}+\frac{6}{5^{2s}}+\frac{10}{9^{2s}}+\frac{24}{11^{2s}}+\frac{20}{16^{2s}}+\frac{40}{19^{2s}}+\frac{30}{20^{2s}}+\frac{30}{25^{2s}}+\frac{60}{29^{2s}}+\cdots. \tag{5.17}$$

As all these Dirichlet series are meromorphic functions, we can apply Delange's theorem 7.A.1 to obtain the asymptotic behaviour of $b_{A_4}(n)$ and $b^{\mathsf{pr}}_{A_4}(n)$. In particular, we get the following result [**9**].

COROLLARY 5.1.5. *The asymptotic behaviour of the summatory functions of* $b_{A_4}(n)$ *is as follows*

$$\sum_{m\leq x} b_{A_4}(m) \sim \rho x, \text{ as } x \to \infty, \tag{5.18}$$

where ρ *is given by*

$$\rho = \frac{\zeta_K(2)L(1,\chi_5)}{L(4,\chi_5)} = \frac{1}{2}\sqrt{5}\log(\tau) \approx 0.538011. \tag{5.19}$$

The asymptotic behaviour for $b^{\mathsf{pr}}_{A_4}(n)$ *is analogous with*

$$\rho^{\mathsf{pr}} = \frac{\zeta_K(2)L(1,\chi_5)}{\zeta(4)L(4,\chi_5)} = \frac{45}{\pi^4}\sqrt{5}\log(\tau) \approx 0.497089. \tag{5.20}$$

5.2. Coincidence site lattices of A_4

Let us discuss the CSLs of the A_4-lattice now. We first recall that $L = \bar{L}$, i.e., L is invariant under conjugation, which is an orientation reversing symmetry operation. Hence, it is sufficient to restrict our analysis to coincidence rotations, as they generate all CSLs already.

We know from Section 3.2 that any coincidence rotation is a similarity rotation as well. In fact, a similarity rotation is a coincidence rotation of a lattice if and only if its denominator is an integer.

Now, it follows from the previous section that every similarity rotation can be parametrised by a primitive quaternion $q \in \mathbb{I}$. In particular, every similarity rotation is of the form $x \mapsto \frac{1}{|q\tilde{q}|}qx\tilde{q}$. From Lemma 5.1.1 we infer that its denominator is $|q\tilde{q}|$. Hence, $x \mapsto \frac{1}{|q\tilde{q}|}qx\tilde{q}$ is a coincidence rotation if and only if $|q\tilde{q}| \in \mathbb{N}$. Therefore, we are only interested in those primitive quaternions $q \in \mathbb{I}$ which satisfy $|q\tilde{q}| \in \mathbb{N}$ or, equivalently, $|q\tilde{q}|^2 = \mathrm{Nr}(|q|^2)$ is a square in $\mathbb{N}$. Paralleling our approach to the discussion of the hypercubic lattices in the previous chapter, we call such a quaternion a *primitive admissible* quaternion. More generally, we call a (not necessarily primitive) quaternion $q \in \mathbb{I}$ *admissible*, if $|q\tilde{q}|^2 = \mathrm{Nr}(|q|^2)$ is a square in $\mathbb{N}$.

In the case of the hypercubic lattices it turned out that it is useful to deal with an extended pair of primitive quaternions instead of primitive ones. The same is valid here as well, and we first define the notion of an extended primitive admissible quaternion.

To this end, let $q \in \mathbb{I}$ be primitive and admissible. Then $\frac{|q\tilde{q}|^2}{\gcd(|q|^2,|\tilde{q}|^2)^2}$ is a square in $\mathbb{Z}[\tau]$. Here, gcd means the greatest common divisor in $\mathbb{Z}[\tau]$, which is well defined up to a unit as $\mathbb{Z}[\tau]$ is a Euclidean domain. Now $\frac{|q|^2}{\gcd(|q|^2,|\tilde{q}|^2)} \in \mathbb{Z}[\tau]$ and $\frac{|\tilde{q}|^2}{\gcd(|q|^2,|\tilde{q}|^2)} \in \mathbb{Z}[\tau]$ are relatively prime in $\mathbb{Z}[\tau]$. Since their product is a square, they must be squares (up to units) in $\mathbb{Z}[\tau]$, too (we have unique prime factorisation). Hence, if the units have been chosen appropriately, we may assume that $\frac{|q|^2}{\gcd(|q|^2,|\tilde{q}|^2)} \in \mathbb{Z}[\tau]$ and $\frac{|\tilde{q}|^2}{\gcd(|q|^2,|\tilde{q}|^2)} \in \mathbb{Z}[\tau]$ are squares in $\mathbb{Z}[\tau]$. Hence we may take the root (we may choose the positive one) and define

$$\alpha_q := \sqrt{\frac{|\tilde{q}|^2}{\gcd(|q|^2,|\tilde{q}|^2)}}, \qquad \alpha_{\tilde{q}} := \alpha_q' = \sqrt{\frac{|q|^2}{\gcd(|q|^2,|\tilde{q}|^2)}}, \tag{5.21}$$

which are unique up to a unit. Note that the last equation only holds up to a unit.

DEFINITION 5.2.1. Let $q \in \mathbb{I}$ be a primitive admissible quaternion. Then $\alpha_q q$ is called extended admissible quaternion (corresponding to q).

Of course, this definition is unique only up to a unit in $\mathbb{Z}[\tau]$, but this does not matter as units of $\mathbb{Z}[\tau]$ cancel out in the definition of the coincidence rotations.

Clearly, we have $\widetilde{\alpha_q q} = \alpha_{\tilde{q}}\tilde{q}$ and $|\alpha_q q|^2 = |\alpha_{\tilde{q}}\tilde{q}|^2 \in \mathbb{N}$, i.e. $\alpha_q q$ and $\widetilde{\alpha_q q}$ have the same norm, which makes calculations easier. Although $\alpha_q q$ is not primitive in general, the pair $(\alpha_q q, \alpha_{\tilde{q}}\tilde{q})$ is primitive in the following sense: Let $(x, y) \in \mathbb{I} \times \mathbb{I}$ and define its content

$$\text{cont}_{\mathbb{I}}(x, y) := \text{lcm}\{\alpha \in \mathbb{Z}[\tau] \setminus \{0\} \mid (x, y) \in (\alpha\mathbb{I}) \times (\alpha\mathbb{I})\}. \tag{5.22}$$

Now (x, y) is called primitive if its content $\text{cont}_{\mathbb{I}}(x, y)$ is a unit in $\mathbb{Z}[\tau]$.

Recall that the twist map provided us with the characterisation of L in terms of $\mathbb{I}$ as $L = \{x \in \mathbb{I} \mid x = \tilde{x}\}$, which was very useful in the determination of the SSLs. Here, we need another formula.

LEMMA 5.2.1. $L = \{x + \tilde{x} | x \in \mathbb{I}\} = \{x + \tilde{x} | x \in L[\tau]\}$

PROOF. Clearly, for any $x \in \mathbb{I}$ we have $x + \tilde{x} \in L$. On the other hand, for any $x \in L$ we have $\tau x + \widetilde{\tau x} = \tau x + \tau' \tilde{x} = (\tau + \tau')x = x$. □

The key for characterising the CSLs will be the lattice $L_q := \{qx + \tilde{x}\tilde{q} | x \in \mathbb{I}\}$ for $q \in \mathbb{I}$. Clearly, L_q is a sublattice of L and it is invariant under the twist map $L_q = \widetilde{L_q}$. Our aim is to prove that each CSL is of the form L_q for a suitable quaternion q. The first step in this direction is the following result.

LEMMA 5.2.2. *Let $q \in \mathbb{I}$ be a primitive admissible quaternion and q_α its extension. Then*

$$L_{q_\alpha} \subseteq L \cap \frac{qL\tilde{q}}{|q\tilde{q}|}. \tag{5.23}$$

PROOF. As mentioned above, $L_{q_\alpha} \subseteq L$. On the other hand, if $x \in L_{q_\alpha}$ there is a $y \in \mathbb{I}$ such that $x = q_\alpha y + \tilde{y}\tilde{q_\alpha}$. Recall $|q_\alpha|^2 = |\tilde{q_\alpha}|^2 = |q_\alpha\tilde{q_\alpha}|$ we obtain

$$x = q_\alpha y + \tilde{y}\tilde{q_\alpha} = q_\alpha y \frac{\tilde{\bar{q}}_\alpha \tilde{q_\alpha}}{|\tilde{q_\alpha}|^2} + \frac{q_\alpha \bar{q_\alpha}}{|q_\alpha|^2}\tilde{y}\tilde{q_\alpha} = \frac{1}{|q_\alpha\tilde{q_\alpha}|} q_\alpha (y\tilde{\bar{q}}_\alpha + \bar{q_\alpha}\tilde{y})\tilde{q_\alpha} \in \frac{q_\alpha L_{\bar{q_\alpha}} \tilde{q_\alpha}}{|q_\alpha\tilde{q_\alpha}|} \subseteq \frac{q_\alpha L \tilde{q_\alpha}}{|q_\alpha\tilde{q_\alpha}|} = \frac{qL\tilde{q}}{|q\tilde{q}|},$$

which finishes the proof. □

The converse statement requires some preparation. Although we will be mostly interested in L_q for extended admissible quaternions, we start with some properties for arbitrary quaternions in $\mathbb{I}$. Let $\langle x, y\rangle$ denote the standard inner product in $\mathbb{R}^4$ or $\mathbb{H}$. This can be expressed as $2\langle x, y\rangle = \text{tr}(x\bar{y})$, where $\text{tr}(x) = x + \bar{x}$ is the reduced trace.

Note that $\mathbb{I}$ is a 4-dimensional $\mathbb{Z}[\tau]$-lattice. Thus, it is possible to define its dual. To expand on that, we need to introduce the quaternion algebra $\mathbb{H}(K) := K\mathbf{e} + K\mathbf{i} + K\mathbf{j} + K\mathbf{k}$, where $K = \mathbb{Q}(\tau)$. This is a 4-dimensional K-vector space. We define the dual of a $\mathbb{Z}[\tau]$-lattice Λ as

$$\Lambda^* := \{y \in \mathbb{H}(K) \mid 2\langle x, y\rangle \in \mathbb{Z}[\tau] \text{ for all } x \in \Lambda\}. \tag{5.24}$$

Clearly, Λ^* is again a 4-dimensional $\mathbb{Z}[\tau]$-lattice. For us, the important fact is that $\mathbb{I}$ is self-dual, i.e., $\mathbb{I} = \mathbb{I}^*$, compare [**63, 54, 20**].

Lemma 5.2.3. *Let $q \in \mathbb{I}$. Then $\{2\langle q, x\rangle \mid x \in \mathbb{I}\}$ is an ideal of $\mathbb{Z}[\tau]$. It is generated by $\mathrm{cont}_{\mathbb{I}}(q)$.*

Proof. Let $\mathcal{A} = \{2\langle q, x\rangle \mid x \in \mathbb{I}\}$. As $2\langle y, x\rangle \in \mathbb{Z}[\tau]$ for all $x, y \in \mathbb{I}$, $\mathcal{A}$ is a subset of $\mathbb{Z}[\tau]$. As $\mathbb{I}$ is a $\mathbb{Z}[\tau]$-lattice and $\langle y, x\rangle$ is $\mathbb{Z}[\tau]$-linear, $\mathcal{A}$ is closed under addition and multiplication by elements of $\mathbb{Z}[\tau]$, hence it is an ideal. Let a be a generator of $\mathcal{A}$. As $\mathrm{cont}_{\mathbb{I}}(q)$ divides $2\langle q, x\rangle$ for all $x \in \mathbb{I}$, $\mathrm{cont}_{\mathbb{I}}(q)$ divides a. Conversely, a dividing $2\langle q, x\rangle$ for all $x \in \mathbb{I}$ implies $q \in (\frac{1}{a}\mathbb{I})^* = a\mathbb{I}^* = a\mathbb{I}$ because of self-duality, whence a divides $\mathrm{cont}_{\mathbb{I}}(q)$. □

An immediate consequence is the following criterion.

Corollary 5.2.4. *Let $q \in \mathbb{I}$. Then q is primitive if and only if $\{2\langle q, x\rangle \mid x \in \mathbb{I}\} = \mathbb{Z}[\tau]$. Equivalently, q is primitive, if and only if there exists an $x \in \mathbb{I}$ such that $2\langle q, x\rangle = \mathrm{tr}(q\bar{x}) = 1$.*

For our purposes, the existence of an $x \in \mathbb{I}$ with $2\langle q, x\rangle = \mathrm{tr}(q\bar{x}) = 1$ is the important result. For primitive admissible quaternions there exists the following generalisation.

Lemma 5.2.5. *Let $q \in \mathbb{I}$ be primitive and admissible and let q_α be the corresponding extended quaternion. Then there exists a quaternion $z \in \mathbb{I}$ such that $2\langle q_\alpha, z\rangle + 2\langle \tilde{q}_\alpha, \tilde{z}\rangle = 1$.*

Proof. By the previous corollary there exists a $z \in \mathbb{I}$ such that $2\langle q, z\rangle = 1$, hence $2\langle q_\alpha, z\rangle = \alpha_q$. As $\langle \tilde{u}, \tilde{v}\rangle = \langle u, v\rangle'$ for all $u, v \in \mathbb{I}$ (or, more generally, for all $u, v \in \mathbb{H}(K)$) we conclude $2\langle \tilde{q}_\alpha, \tilde{z}\rangle = \alpha'_q$.

But since α_q and α'_q are relatively prime, there exist $\beta, \gamma \in \mathbb{Z}[\tau]$ such that $\alpha_q\beta + \alpha'_q\gamma = 1$, hence $2\langle q_\alpha, \beta z\rangle + 2\langle \tilde{q}_\alpha, \gamma\tilde{z}\rangle = 1$, i.e. to each extended primitive pair $(q_\alpha, \tilde{q}_\alpha)$ there exists a pair $(x, y) \in \mathbb{I} \times \mathbb{I}$ such that $2\langle q_\alpha, x\rangle + 2\langle \tilde{q}_\alpha, \tilde{y}\rangle = 1$.

Finally, we define $z = \tau x + (1 - \tau)y = \tau x + \tau'$. Making use of $\langle \tilde{u}, \tilde{v}\rangle = \langle u, v\rangle'$ again, we get by recalling $2\langle q_\alpha, x\rangle + 2\langle \tilde{q}_\alpha, \tilde{y}\rangle = 1$

$$2\langle q_\alpha, z\rangle + 2\langle \tilde{q}_\alpha, \tilde{z}\rangle = 2\tau(\langle q_\alpha, x\rangle + \langle \tilde{q}_\alpha, \tilde{y}\rangle) + 2(1-\tau)(\langle q_\alpha, y\rangle + \langle \tilde{q}_\alpha, \tilde{x}\rangle) = \tau + (1-\tau) = 1.$$

□

We are now prepared to prove that every CSL of L is of the form L_q.

Theorem 5.2.6. *Let $q \in \mathbb{I}$ be a primitive admissible quaternion and q_α its extension. Then*

$$L \cap \frac{qL\tilde{q}}{|q\tilde{q}|} = L_{q_\alpha} = (q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}) \cap L. \tag{5.25}$$

Proof. The inclusion $L_{q_\alpha} \subseteq L \cap \frac{qL\tilde{q}}{|q\tilde{q}|}$ was proved in Lemma 5.2.2. To prove the converse inclusion, we assume $x \in L \cap \frac{qL\tilde{q}}{|q\tilde{q}|}$. As mentioned above there exists a quaternion $z \in \mathbb{I}$ such that $2\langle q_\alpha, z\rangle + 2\langle \tilde{q_\alpha}, \tilde{z}\rangle = 1$. Thus

$$\begin{aligned} x &= 2(\langle q_\alpha, z\rangle + \langle \tilde{q_\alpha}, \tilde{z}\rangle)x = 2\langle q_\alpha, z\rangle x + 2\tilde{x}\langle \tilde{q_\alpha}, \tilde{z}\rangle \\ &= (q_\alpha \bar{z} + z\bar{q_\alpha})x + \tilde{x}(\bar{\tilde{z}}\tilde{q_\alpha} + \bar{\tilde{q_\alpha}}\tilde{z}) \end{aligned}$$

Since $x \in L \cap \frac{q_\alpha L\tilde{q_\alpha}}{|q_\alpha \tilde{q_\alpha}|}$ there is a $y \in L$ such that $x = \frac{q_\alpha y\tilde{q_\alpha}}{|q_\alpha \tilde{q_\alpha}|}$. Hence

$$x = q_\alpha \bar{z}x + zy\tilde{q_\alpha} + \tilde{x}\bar{\tilde{z}}\tilde{q_\alpha} + q_\alpha \tilde{y}\tilde{z} = q_\alpha(\bar{z}x + \tilde{y}\tilde{z}) + (\tilde{x}\bar{\tilde{z}} + zy)\tilde{q_\alpha} \in L_{q_\alpha}.$$

It remains to prove the second equality. Clearly $L_{q_\alpha} \subseteq q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}$ and $L_{q_\alpha} \subseteq L$, i.e. $L_{q_\alpha} \subseteq (q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}) \cap L$. On the other hand, if $q_\alpha x + y\tilde{q_\alpha} \in L$, then $q_\alpha x + y\tilde{q_\alpha} = \tau(q_\alpha x + y\tilde{q_\alpha}) + (1-\tau)(q_\alpha\tilde{y} + \tilde{x}\tilde{q_\alpha}) = q_\alpha z + \tilde{z}\tilde{q_\alpha} \in L_{q_\alpha}$, where $z = \tau x + (1-\tau)\tilde{y}$. □

The next step is to calculate the coincidence indices. As one can infer them from the corresponding coincidence indices for the $\mathbb{Z}[\tau]$-lattices $L[\tau]$ and $\mathbb{I}$, we state just the result here and defer the proof to later sections – it follows from Lemma 5.3.6 and Theorem 5.4.4.

Theorem 5.2.7. *Let $q \in \mathbb{I}$ be a primitive admissible quaternion and q_α its extension. Then the coincidence index $\varSigma_{A_4}(q)$ of the corresponding coincidence rotation is given by*

$$\varSigma_{A_4}(q) = |q_\alpha|^2 = |\tilde{q_\alpha}|^2 = \frac{|q\tilde{q}|^2}{\gcd(|q|^2, |\tilde{q}|^2)} = |q\tilde{q}|\alpha_q\alpha_{\tilde{q}} = \operatorname{lcm}(|q|^2, |\tilde{q}|^2). \tag{5.26}$$

Our main goal is the counting of the CSLs. It follows from Lemma 5.1.2 that two primitive admissible quaternions $r, s \in \mathbb{I}$ generate the same CSL, compare [**8**, Lemma 5]. However, the converse is not true, and additional properties are needed to characterise those $r, s \in \mathbb{I}$ that generate the same CSLs. We will deal with this problem in later sections.

For the moment, we just count the number of coincidence rotations. This amounts to counting the right ideals generated by primitive admissible quaternions. Observe that two primitive admissible quaternions $r, s \in \mathbb{I}$ generate the same rotation if and only if they differ only by a unit in $\mathbb{Z}[\tau]$, whereas $r, s \in \mathbb{I}$ with $r = s\varepsilon$ generate different coincidence rotations, whenever ε is a unit in $\mathbb{I}$ that is not in $\mathbb{Z}[\tau]$.

Recall that the rotation symmetry group of A_4 has 120 elements [**22**]. Hence the number of coincidence rotations of a given index m is given by $120c^{\mathsf{rot}}_{A_4}(m)$, and $c^{\mathsf{rot}}_{A_4}(m)$ is the number of right ideals generated by primitive admissible quaternions q with $m = \varSigma_{A_4}(q)$. The (essentially) unique prime factorisation in $\mathbb{I}$ guarantees that $c^{\mathsf{rot}}_{A_4}(m)$ is a multiplicative arithmetic function. Hence, it is sufficient to calculate $c^{\mathsf{rot}}_{A_4}(m)$ for prime powers.

The values of $c^{\mathsf{rot}}_{A_4}(m)$ are related to the values $b^{\mathsf{pr}}_{A_4}(m)$ counting the number of primitive sublattices, but they are not identical for two reasons. First, we do not count all primitive right ideals, but only admissible ones, and secondly, the indices of the respective sublattices differ.

Let us start with $p = 5$, which is a ramifying prime in $\mathbb{Z}[\tau]$, i.e. $p = 5 = (\sqrt{5})^2$. Primitive quaternions q with $|q|^2 = \sqrt{5}^{\,s}\varepsilon$, with ε a unit in $\mathbb{Z}[\tau]$, are admissible if and only if $s = 2r$

is even. In this case, $\Sigma_{A_4}(q) = 5^r$, and we get $c^{\mathsf{rot}}_{A_4}(5^r) = b^{\mathsf{pr}}_{A_4}(5^{4r})$. As the primes $p \equiv \pm 2 \pmod 5$ are inert in $\mathbb{Z}[\tau]$, similar arguments show $c^{\mathsf{rot}}_{A_4}(p^r) = b^{\mathsf{pr}}_{A_4}(p^{4r})$.

The case $p \equiv \pm 1 \pmod 5$ is more difficult as p splits in $\mathbb{Z}[\tau]$ as $p = \pi\pi'$, with π a prime in $\mathbb{Z}[\tau]$. Here, a primitive quaternion q with $|q|^2 = \pi^r(\pi')^s\varepsilon$ is admissible if and only if $r+s$ is even. In this case $\Sigma_{A_4}(q) = p^{(r+s)/2}$. This situation reminds us of the hypercubic case, where we have had a similar condition. The unique factorisation guarantees that q can be written as $q = q_1q_2$ with $|q_1|^2 = \pi^r\varepsilon_1$ and $|q_2|^2 = (\pi')^s\varepsilon_2$. The number of primitive ideals $q\mathbb{I}$ with $|q|^2 = \pi^r\varepsilon$ is given by $f(p) = (p+1)p^{r-1}$, which can be read off from the corresponding Euler factor

$$\frac{1+p^{-2s}}{1-p^{1-2s}} = 1 + \sum_{r\in\mathbb{N}} (p+1)p^{r-1}p^{-2rs} \tag{5.27}$$

of $\zeta^{\mathsf{pr}}_{\mathbb{I}}(s)$, see Eqs. 5.11 and 5.13 and compare [**8**]. In analogy with Eq. 4.18 we can calculate (see [**42**] for a detailed calculation)

$$c^{\mathsf{rot}}_{A_4}(p^r) = f(p^r)^2 + 2\sum_{s=1}^{[r/2]} f(p^r)f(p^{r-2s}) = \frac{p+1}{p-1}p^{r-1}(p^{r+1}+p^{r-1}-2). \tag{5.28}$$

Hence, $c^{\mathsf{rot}}_{A_4}(p^r)$ is given by

$$c^{\mathsf{rot}}_{A_4}(p^r) = \begin{cases} 6\cdot 5^{2r-1}, & \text{if } p=5,\\ \frac{p+1}{p-1}p^{r-1}(p^{r+1}+p^{r-1}-2), & \text{if } p\equiv \pm 1 \pmod 5,\\ p^{2r}+p^{2r-2}, & \text{if } p \equiv \pm 2 \pmod 5. \end{cases} \tag{5.29}$$

This allows us to write down the generating function for the number of coincidence rotations.

THEOREM 5.2.8. *Let $120c^{\mathsf{rot}}_{A_4}(m)$ be the number of coincidence rotations of the lattice A_4. Then the Dirichlet series generating function for $c^{\mathsf{rot}}_{A_4}(m)$ reads a follows*

$$\begin{aligned}\Psi^{\mathsf{rot}}_{A_4}(s) = \sum_{n\in\mathbb{N}} \frac{c^{\mathsf{rot}}_{A_4}(n)}{n^s} &= \frac{\zeta_K(s-1)}{1+5^{-s}}\,\frac{\zeta(s)\zeta(s-2)}{\zeta(2s)\zeta(2s-2)}\\ &= \frac{1+5^{1-s}}{1-5^{2-s}} \prod_{p\equiv\pm1(5)} \frac{(1+p^{-s})(1+p^{1-s})}{(1-p^{1-s})(1-p^{2-s})} \prod_{p\equiv\pm2(5)} \frac{1+p^{-s}}{1-p^{2-s}}\\ &= 1 + \frac{5}{2^s} + \frac{10}{3^s} + \frac{20}{4^s} + \frac{30}{5^s} + \frac{50}{6^s} + \frac{50}{7^s} + \frac{80}{8^s} + \frac{90}{9^s} + \frac{150}{10^s} + \frac{144}{11^s} + \frac{200}{12^s} + \frac{170}{13^s} + \cdots .\end{aligned}$$

This shows that any positive integer occurs as a coincidence index. In other words, the coincidence spectrum, i.e., the set of all possible coincidence indices, is $\mathbb{N}$.

$\Psi^{\mathsf{rot}}_{A_4}$ is a meromorphic function in the entire complex plane, and its rightmost pole is a simple pole located at $s = 3$, with residue

$$\rho^{\mathsf{rot}}_{A_4} = \operatorname{Res}_{s=3} \Psi^{\mathsf{rot}}_{A_4}(s) = \frac{125}{126}\,\frac{\zeta_K(2)\zeta(3)}{\zeta(6)\zeta(4)} = \frac{450\sqrt{5}}{\pi^6}\zeta(3) \approx 1.258124, \tag{5.30}$$

where the last equation follows from inserting the special values

$$\zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945}, \qquad \zeta_K(2) = \frac{2\pi^4}{75\sqrt{5}}, \qquad L(1,\chi_5) = \frac{2\log(\tau)}{\sqrt{5}} \tag{5.31}$$

and Apéry's constant $\zeta(3) = 1.2020569$; compare [**10, 8**] and references therein. A familiar argument based on Delange's theorem 7.A.1 gives us the asymptotic growth rate of $c^{\mathsf{rot}}_{A_4}(m)$.

COROLLARY 5.2.9. *With the residue $\rho^{\mathsf{rot}}_{A_4}$ from above, the asymptotic behaviour of $c^{\mathsf{rot}}_{A_4}(m)$ is given by*

$$\sum_{m\leq x} c^{\mathsf{rot}}_{A_4}(m) \sim \rho^{\mathsf{rot}}_{A_4}\frac{x^3}{3} \approx 0.419375\, x^3, \quad \textit{as } x \to \infty. \tag{5.32}$$

Note that the number of coincidence rotations and the number of CSLs (as we shall see later in Corollary 5.5.7) grows much faster than the number of SSLs. This is due to the fact that the index of a primitive SSL is $\operatorname{den}_{A_4}(q)^4$, whereas the coincidence index $\varSigma_{A_4}(q)$ is much smaller and satisfies the condition $\operatorname{den}_{A_4}(q) \leq \varSigma_{A_4}(q) \leq \operatorname{den}_{A_4}(q)^2$.

5.3. Some coincidences of $L[\tau]$ and $\mathbb{I}$

We have mentioned the formula for the coincidence index in the previous section, but we still have to prove it. The aim of this section is to find a relationship between the coincidence indices of L and the corresponding coincidence indices of $L[\tau]$ and $\mathbb{I}$. In this way, we will be able to express $\varSigma_{A_4}(q)$ in terms of the corresponding coincidence index for $\mathbb{I}$. The final calculation of this coincidence index will then be left to yet another section.

Clearly, the coincidence rotations of L are also coincidence rotations of $L[\tau]$ and $\mathbb{I}$. The group of coincidence rotations for these groups is, of course, much bigger, but we restrict our discussion to these special coincidence rotations for the moment. Since these coincidence rotations do not mix vectors of L and τL we immediately get the following result.

LEMMA 5.3.1. *Let $q \in \mathbb{I}$ be a primitive admissible quaternion and q_α its extension. Then we have*

$$L[\tau] \cap \frac{qL[\tau]\tilde{q}}{|q\tilde{q}|} = L_{q_\alpha} + \tau L_{q_\alpha}. \tag{5.33}$$

Thus the index for $L[\tau]$ is just the square of the corresponding index for L, in other words

$$\left[L[\tau] : L[\tau] \cap \frac{qL[\tau]\tilde{q}}{|q\tilde{q}|}\right] = \varSigma_{A_4}(q)^2. \tag{5.34}$$

LEMMA 5.3.2. *Let $q \in \mathbb{I}$ be a primitive admissible quaternion and q_α its extension. Then*

$$\mathbb{I} \cap \frac{q\mathbb{I}\tilde{q}}{|q\tilde{q}|} = q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}. \tag{5.35}$$

PROOF. Clearly, $q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha} \subseteq \mathbb{I}$. Similarly, $\bar{q}_\alpha\mathbb{I} + \mathbb{I}\tilde{\bar{q}}_\alpha \subseteq \mathbb{I}$ and hence, we have

$$q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha} = \frac{q_\alpha(\bar{q}_\alpha\mathbb{I} + \mathbb{I}\tilde{\bar{q}}_\alpha)\tilde{q_\alpha}}{|q_\alpha\tilde{q_\alpha}|} \subseteq \frac{q_\alpha\mathbb{I}\tilde{q_\alpha}}{|q_\alpha\tilde{q_\alpha}|} = \frac{q\mathbb{I}\tilde{q}}{|q\tilde{q}|}.$$

Thus we obtain the first inclusion

$$\mathbb{I} \cap \frac{q\mathbb{I}\tilde{q}}{|q\tilde{q}|} \supseteq q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}. \tag{5.36}$$

To prove the converse inclusion, we make again use of the existence of a $z \in \mathbb{I}$ such that $2\langle q_\alpha, z\rangle + 2\langle \tilde{q_\alpha}, \tilde{z}\rangle = 1$, compare 5.2.5. Now, for any $x \in \mathbb{I} \cap \frac{q\mathbb{I}\tilde{q}}{|q\tilde{q}|}$ there is a $y \in \mathbb{I}$ such that $x = \frac{qy\tilde{q}}{|q\tilde{q}|} = \frac{q_\alpha y\tilde{q_\alpha}}{|q_\alpha\tilde{q_\alpha}|}$ and hence, we see

$$x = (q_\alpha\bar{z} + z\bar{q}_\alpha)x + x(\bar{\tilde{z}}\tilde{q_\alpha} + \bar{\tilde{q}}_\alpha\tilde{z}) = q_\alpha(\bar{z}x + y\tilde{z}) + (zy + x\bar{\tilde{z}})\tilde{q_\alpha} \in q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}. \tag{5.37}$$

Thus,

$$\mathbb{I} \cap \frac{q\mathbb{I}\tilde{q}}{|q\tilde{q}|} \subseteq q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha} \tag{5.38}$$

and the result follows. □

The next aim is to compare the indices. Denote the coincidence indices of $L[\tau]$ and $\mathbb{I}$ by $\varSigma_{L[\tau]}$ and $\varSigma_{\mathbb{I}}$, respectively. Since $[\mathbb{I} : L[\tau]] = 5$ Lemma 3.1.9 tells us that there are only finitely many possibilities for $\varSigma_{\mathbb{I}}$, namely $\varSigma_{\mathbb{I}} \in \{\frac{\varSigma_{L[\tau]}}{5}, \varSigma_{L[\tau]}, 5\varSigma_{L[\tau]}\}$. We want to show $\varSigma_{\mathbb{I}} = \varSigma_{L[\tau]}$.

First, we want to characterise $L[\tau]$ in a similar way we have characterised L in Lemma 5.2.1.

Lemma 5.3.3. *$L[\tau] = \{x \in \mathbb{I} | x - \tilde{x} \in (2\tau - 1)\mathbb{I}\}$.*

Proof. Recall $L[\tau] = L + \tau L$, i.e. every quaternion $q \in L[\tau]$ can be written as $q = x + \tau y$ with $x, y \in L$. Hence, using $x = \tilde{x}, y = \tilde{y}$ we see that

$$q - \tilde{q} = \tau y - (1 - \tau)\tilde{y} = (2\tau - 1)y = \sqrt{5}y \in (2\tau - 1)L \subseteq (2\tau - 1)\mathbb{I} \tag{5.39}$$

for all $q \in L[\tau]$. On the other hand, any quaternion $r \in \mathbb{I}$ can be written as $r = q + ku$, where $q \in L[\tau]$, $u = \frac{1}{2}(1 - \tau, \tau, 0, 1)$ and $k \in \{0, \dots, 4\}$. Now

$$u - \tilde{u} = \frac{1}{2}(1 - 2\tau, 2\tau - 1, 1, 1) \notin (2\tau - 1)\mathbb{I}, \tag{5.40}$$

which gives the result. □

A simple consequence of this characterisation is the following well-known result (see [**9**]), which will prove useful throughout the next sections.

Corollary 5.3.4. *$\sqrt{5}\mathbb{I} = (2\tau - 1)\mathbb{I} \subseteq L[\tau]$.*

Since $2\langle x, y\rangle \in \mathbb{Z}[\tau]$ for all $x, y \in \mathbb{I}$ and $|u - \tilde{u}|^2 = 3$ is not divisible by 5, an alternative characterisation is the following

Lemma 5.3.5. *$L[\tau] = \{x \in \mathbb{I}$ such that $5 \big| |x - \tilde{x}|^2\}$.*

Since any rotation leaves the norm unchanged, this implies that $\frac{qL[\tau]\tilde{q}}{|q\tilde{q}|} \cap \mathbb{I} = \frac{qL[\tau]\tilde{q}}{|q\tilde{q}|} \cap L[\tau]$, i.e., the conditions of lemma 3.1.9 are satisfied and hence the case $\varSigma_{\mathbb{I}} = \frac{\varSigma_{L[\tau]}}{5}$ is ruled out, i.e., there remain only two possible values for $\varSigma_{\mathbb{I}}$, namely $\varSigma_{\mathbb{I}} \in \{\varSigma_{L[\tau]}, 5\varSigma_{L[\tau]}\}$.

Now assume $\varSigma_{\mathbb{I}} = 5\varSigma_{L[\tau]}$. This is equivalent to

$$L[\tau] \cap \frac{qL[\tau]\tilde{q}}{|q\tilde{q}|} = \mathbb{I} \cap \frac{q\mathbb{I}\tilde{q}}{|q\tilde{q}|} = q_\alpha\mathbb{I} + \mathbb{I}\tilde{q_\alpha}. \tag{5.41}$$

Hence $L[\tau] \supseteq q_\alpha\mathbb{I}$. Furthermore $L[\tau] \supseteq \sqrt{5}\mathbb{I} = (2\tau-1)\mathbb{I}$ (recall Corollary 5.3.4). Hence $L[\tau] \supseteq g\mathbb{I}$, where g is the greatest common left divisor of q_α and $2\tau - 1 = \sqrt{5}$. Since q_α is the extension of a primitive admissible quaternion, q_α cannot be contained in $(2\tau-1)\mathbb{I}$, as $(2\tau-1) = -(2\tau-1)'$ cannot be a divisor of α_q. This implies $g \neq 2\tau - 1$. Obviously, $g = 1$ is absurd, since this would imply $L[\tau] \supseteq \mathbb{I}$. Thus, we have $|g|^2\mathbb{Z}[\tau] = (2\tau-1)\mathbb{Z}[\tau]$, which implies that g is a prime quaternion and, hence, g is not a central element of $\mathbb{I}$. Now, $L[\tau] \supseteq g\mathbb{I}$ implies $gr - \tilde{r}\tilde{g} \in (2\tau-1)\mathbb{I}$ by Lemma 5.3.3. From this we infer that g divides $\tilde{r}\tilde{g}$ for all r, or in other words, $g\mathbb{I} \supseteq \mathbb{I}\tilde{g}$. As both ideals have the same index in $\mathbb{I}$, they must be equal. Hence, $g\mathbb{I} = \mathbb{I}\tilde{g}$ is a two-sided ideal, which implies that g is a central element; compare [**10**]. But this gives a contradiction, which rules out the case $\varSigma_{\mathbb{I}} = 5\varSigma_{L[\tau]}$ as well. Hence we have proved the following result.

Lemma 5.3.6. *For all $R \in \mathrm{SOC}(L)$ we have $\varSigma_{\mathbb{I}}(R) = \varSigma_{L[\tau]}(R) = \varSigma_{A_4}(R)^2$.*

Now, it remains to calculate $\varSigma_{\mathbb{I}}$ to prove Theorem 5.2.7. This will be done in the next section.

5.4. Coincidences of $\mathbb{I}$

There are at least two reasons to consider the CSMs of the icosian ring $\mathbb{I}$. First, they will provide us with a formula for the coincidence index of the A_4-lattice and they will give us the necessary tools to decide under which conditions two CSLs of the A_4-lattice are equal. Secondly, the CSMs of $\mathbb{I}$ are also interesting in their own right, as we can exploit the algebraic properties of $\mathbb{I}$ to completely solve the coincidence problems. It is one of the few examples of a $\mathbb{Z}$-module in 4 dimensions where this is possible.

The methods we use are generalisations of the tools we have used for the A_4-lattice and for the hypercubic lattices in Chapter 4, so we will keep the presentation short and skip some details.

It follows from [**10**] that every similarity rotation of $\mathbb{I}$ can be parametrised by a pair of $\mathbb{I}$-primitive quaternions $(p,q) \in \mathbb{I} \times \mathbb{I}$ as $R(q,p)x = qxp/|pq|$. Moreover, we have $\mathrm{scal}_{\mathbb{I}}(E) = \mathbb{Q}(\tau)^*$, which means that $R(q,p)$ is a coincidence rotation if and only if $\mathrm{scal}_{\mathbb{I}}(R(p,q)) = \mathbb{Q}(\tau)^*$ by Lemma 3.2.1. Thus, $R(p,q))$ is a coincidence rotation if and only if $|pq| \in \mathbb{Z}[\tau]$.

This motivates us to call a pair $(p,q) \in \mathbb{I} \times \mathbb{I}$ *primitive admissible* if p,q are primitive and $|pq| \in \mathbb{Z}[\tau]$. Along the same lines as before we can define

$$\alpha_q := \sqrt{\frac{|p|^2}{\gcd(|q|^2,|p|^2)}}, \qquad \alpha_p := \sqrt{\frac{|q|^2}{\gcd(|q|^2,|p|^2)}} \tag{5.42}$$

for any primitive admissible pair (q,p), where α_q and α_p are again defined up to a unit. Similarly, we can define the extension of a primitive admissible pair $(q_\alpha, p_\alpha) = (\alpha_q q, \alpha_p p)$.

This guarantees

$$|q_\alpha|^2 = |p_\alpha|^2 = |q_\alpha p_\alpha|. \tag{5.43}$$

It is straightforward to generalise Lemma 5.2.5.

LEMMA 5.4.1. *Let (q_α, p_α) be an extension of a primitive admissible pair. Then there exist quaternions $u, v \in \mathbb{I}$ such that $2\langle q_\alpha, u\rangle + 2\langle p_\alpha, v\rangle = 1$.*

We apply this result to obtain the following representation of the CSMs of $\mathbb{I}$.

THEOREM 5.4.2. *Let (q_α, p_α) be an extension of a primitive admissible pair. Then*

$$\mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} = q_\alpha\mathbb{I} + \mathbb{I}p_\alpha. \tag{5.44}$$

PROOF. Clearly, $q_\alpha\mathbb{I} + \mathbb{I}p_\alpha \subseteq \mathbb{I}$. Similarly, $\bar{q}_\alpha\mathbb{I} + \mathbb{I}\bar{p}_\alpha \subseteq \mathbb{I}$ and, hence, applying Eq. (5.43) we get

$$q_\alpha\mathbb{I} + \mathbb{I}p_\alpha = \frac{q_\alpha(\bar{q}_\alpha\mathbb{I} + \mathbb{I}\bar{p}_\alpha)p_\alpha}{|q_\alpha p_\alpha|} \subseteq \frac{q_\alpha\mathbb{I}p_\alpha}{|q_\alpha p_\alpha|} = \frac{q\mathbb{I}p}{|qp|},$$

which gives us the first inclusion

$$\mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} \supseteq q_\alpha\mathbb{I} + \mathbb{I}p_\alpha. \tag{5.45}$$

To prove the converse inclusion, we make use of Lemma 5.4.1 and choose u, v such that $2\langle q_\alpha, u\rangle + 2\langle p_\alpha, v\rangle = 1$. Now, for any $x \in \mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|}$ there is a $y \in \mathbb{I}$ such that $x = \frac{qyp}{|qp|} = \frac{q_\alpha y p_\alpha}{|q_\alpha p_\alpha|}$ and hence

$$x = (q_\alpha\bar{u} + u\bar{q}_\alpha)x + x(\bar{v}p_\alpha + \bar{p}_\alpha v) = q_\alpha(\bar{u}x + yv) + (uy + x\bar{v})p_\alpha \in q_\alpha\mathbb{I} + \mathbb{I}p_\alpha. \tag{5.46}$$

Thus

$$\mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} \subseteq q_\alpha\mathbb{I} + \mathbb{I}p_\alpha \tag{5.47}$$

and the claim follows. □

Our next aim is the calculation of the coincidence index. The first step in this direction is the following lemma, which gives us the product of two coincidence indices.

LEMMA 5.4.3. *Let (q, p) be a primitive admissible pair and (q_α, p_α) its extension. Then*

$$\varSigma_{\mathbb{I}}(R(q,p))\varSigma_{\mathbb{I}}(R(\bar{q},p)) = \mathrm{Nr}(|q_\alpha|^4). \tag{5.48}$$

PROOF. From the inclusions

$$q_\alpha\mathbb{I} \subseteq q_\alpha\mathbb{I} + \mathbb{I}p_\alpha = \mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} \subseteq \mathbb{I}. \tag{5.49}$$

we infer

$$[(q_\alpha\mathbb{I} + \mathbb{I}p_\alpha) : q_\alpha\mathbb{I}] = [(\mathbb{I} + \frac{\bar{q}_\alpha}{|q_\alpha|^2}\mathbb{I}p_\alpha) : \mathbb{I}] = [\mathbb{I} : (\mathbb{I} \cap \frac{\bar{q}_\alpha}{|q_\alpha p_\alpha|}\mathbb{I}p_\alpha)] = \varSigma_{\mathbb{I}}(R(\bar{q},p)) \tag{5.50}$$

and the assertion follows. □

If we can prove $\varSigma_{\mathbb{I}}(R(q,p)) = \varSigma_{\mathbb{I}}(R(\bar{q},p))$, taking the square root of Eq. 5.48 will give us a formula for the coincidence index. This is possible, indeed.

THEOREM 5.4.4. *Let (q,p) be a primitive admissible pair and (q_α, p_α) its extension. Then*

$$\varSigma_{\mathbb{I}}(R(q,p)) = \mathrm{Nr}(\mathrm{lcm}(|q|^2, |p|^2)) = \mathrm{Nr}(|q_\alpha|^2) = \mathrm{Nr}(|p_\alpha|^2). \tag{5.51}$$

PROOF. We have to show $[\mathbb{I} : (q_\alpha \mathbb{I} + \mathbb{I} p_\alpha)] = \mathrm{Nr}(|q_\alpha|^2)$. Due to the previous lemma it is sufficient to show that $[\mathbb{I} : (q_\alpha \mathbb{I} + \mathbb{I} p_\alpha)]$ divides $\mathrm{Nr}(|q_\alpha|^2)$. If p and q are units, the result is trivial. So assume that at least one of p, q is not a unit.

Assume, first, that $\alpha_p = \alpha_q = 1$, i.e., $p_\alpha = p$ and $q_\alpha = q$, which implies $|q|^2 = |p|^2$. Thus, neither p nor q is a unit. Clearly, $[\mathbb{I} : q\mathbb{I}] = \mathrm{Nr}(|q|^4)$. Of course, $q\mathbb{I} \not\supseteq \mathbb{I}p$, since, otherwise, $q\mathbb{I} = \mathbb{I}p$ would be a two-sided ideal, which is impossible, because q is not a unit and primitive by assumption. We consider the set $\{\mu \in \mathbb{Z}[\tau] \mid q\mathbb{I} \supseteq \mu \mathbb{I} p\}$, which is an ideal in $\mathbb{Z}[\tau]$. Let m be a generator of it. Clearly, m divides $|q|^2$. We want to show $m = |q|^2$ (up to a unit).

Assume, on the contrary, that m were a proper divisor of $|q|^2$. Then $g = \mathrm{gcld}(m, q)$ is a proper left divisor of $q = gh$, where h is not a unit. Hence, $h\mathbb{I} \supseteq \bar{g}\mathbb{I}p$, and $h\mathbb{I} \supseteq (h\mathbb{I}p + \bar{g}\mathbb{I}p) = \mathbb{I}p$, since h and $\bar{g}$ have common divisor 1 (otherwise q would not be primitive). Multiplying by $\mathbb{I}$ from the right gives $h\mathbb{I} \supseteq \mathbb{I}p\mathbb{I}$. The latter is a two-sided ideal containing the primitive icosian p, hence we have $\mathbb{I}p\mathbb{I} = \mathbb{I}$. This gives the contradiction $h\mathbb{I} \supseteq \mathbb{I}$. This proves $m = |q|^2$ (up to a unit).

This means that there is an icosian $x \in \mathbb{I}p$ of $\mathbb{Z}[\tau]$-order $|q|^2$ in $\mathbb{I}/q\mathbb{I}$. The latter is a generalisation of the usual notion of the order of an element in a group. It is defined as follows: Let $\mathcal{A}$ be a $\mathbb{Z}[\tau]$-submodule of $\mathbb{I}$ and $x \in \mathbb{I}$. Any element that generates the ideal $\{\mu \in \mathbb{Z}[\tau] \mid \mu x \in \mathcal{A}\}$ is called a $\mathbb{Z}[\tau]$-order of x in $\mathbb{I}/\mathcal{A}$. Now, x having $\mathbb{Z}[\tau]$-order $|q|^2$ in $\mathbb{I}/q\mathbb{I}$ means that there are $\mathrm{Nr}(|q|^2)$ different cosets of $q\mathbb{I}$ of the form $\lambda x + q\mathbb{I}$, $\lambda \in \mathbb{Z}[\tau]$ in $q\mathbb{I} + \mathbb{I}p$. Hence, $[\mathbb{I} : (q\mathbb{I} + \mathbb{I}p)]$ is a divisor of $[\mathbb{I} : q\mathbb{I}]/\mathrm{Nr}(|q|^2) = \mathrm{Nr}(|q|^2)$. But this implies $[\mathbb{I} : (q\mathbb{I} + \mathbb{I}p)] = \mathrm{Nr}(|q|^2)$, as mentioned above.

For the general case the idea is to reduce the problem to the case $\alpha_q = \alpha_p = 1$. First, define the greatest left and common right divisors $g_q = \mathrm{gcld}(q, \alpha_p) = \mathrm{gcld}(q_\alpha, \alpha_p)$ and $g_p = \mathrm{gcrd}(p, \alpha_q) = \mathrm{gcrd}(p_\alpha, \alpha_q)$ with decompositions $q = g_q h_q$ and $p = h_p g_p$. Note that $|g_q|^2 = \alpha_p$ and $|g_p|^2 = \alpha_q$. Hence, we have

$$\begin{aligned} q_\alpha \mathbb{I} + \mathbb{I} p_\alpha &= q_\alpha \mathbb{I} + q\mathbb{I}p_\alpha + q_\alpha \mathbb{I} p + \mathbb{I} p_\alpha = q\mathbb{I}(\alpha_q + p_\alpha) + (\alpha_p + q_\alpha)\mathbb{I}p \\ &= q\mathbb{I}g_p + g_q \mathbb{I} p = g_q(h_q \mathbb{I} + \mathbb{I} h_p) g_p. \end{aligned}$$

This gives us the following formula for the index

$$[\mathbb{I} : (q_\alpha \mathbb{I} + \mathbb{I} p_\alpha)] = \mathrm{Nr}(\alpha_p^2 \alpha_q^2)[\mathbb{I} : (h_q \mathbb{I} + \mathbb{I} h_p)]. \tag{5.52}$$

Note that $|h_q|^2 = \frac{|q|^2}{\alpha_p} \neq |h_p|^2 = \frac{|p|^2}{\alpha_q}$, so we cannot apply our known result yet. To circumvent this problem, we rewrite $h_q \mathbb{I} + \mathbb{I} h_p$ as follows

$$\begin{aligned} h_q \mathbb{I} + \mathbb{I} h_p &= h_q \mathbb{I} + |h_q|^2 \mathbb{I} + \mathbb{I}|h_p|^2 + \mathbb{I} h_p = \\ &= (h_q + |h_p|^2)\mathbb{I} + \mathbb{I}(h_p + |h_q|^2) = k_q \mathbb{I} + \mathbb{I} k_p, \end{aligned} \tag{5.53}$$

where we have introduced the greatest common divisors $k_q := \mathrm{gcld}(h_q, |h_p|^2)$ and $k_p := \mathrm{gcrd}(h_p, |h_q|^2)$, respectively. Both have the norm

$$|k_q|^2 = |k_p|^2 = \gcd(|h_q|^2, |h_p|^2) = \frac{|q|^2}{\alpha_p^2} = \frac{|p|^2}{\alpha_q^2} = \gcd(|p|^2, |q|^2). \tag{5.54}$$

Now, we can apply the results of part 1 and obtain

$$[\mathbb{I} : (q_\alpha \mathbb{I} + \mathbb{I} p_\alpha)] = \mathrm{Nr}(\alpha_p^2 \alpha_q^2)[\mathbb{I} : (k_q \mathbb{I} + \mathbb{I} k_p)] = \mathrm{Nr}(\alpha_p^2 \alpha_q^2 \frac{|q|^2}{\alpha_p^2}) = \mathrm{Nr}(|q_\alpha|^2). \tag{5.55}$$

This finishes the proof. □

We are ready now to calculate the number of coincidence rotations. Note that the order of the rotation symmetry group of $\mathbb{I}$ is 7200, whence the number of coincidence rotations is given by $7200 c_{\mathbb{I}}^{\mathsf{rot}}(m)$, where $c_{\mathbb{I}}^{\mathsf{rot}}(m)$ is an integral arithmetic function. To determine $c_{\mathbb{I}}^{\mathsf{rot}}(m)$ we need the number of primitive icosians q of a given norm $|q|^2 = \mu \in \mathbb{Z}[\tau]$ (up to a unit), which is given by $240 f(\mu)$, where 240 is the number of unit icosians and $f(\mu)$ is a multiplicative function, which is determined by its values for prime powers $r \geq 1$ in $\mathbb{Z}[\tau]$

$$f(\pi^r) = \begin{cases} 6 \cdot 5^{r-1} & \text{if } \pi = \sqrt{5}, \\ (p+1)p^{r-1} & \text{if } \pi\pi' = p \equiv \pm 1 \pmod 5, \\ (p^2+1)p^{2r-2} & \text{if } \pi = p \equiv \pm 2 \pmod 5. \end{cases} \tag{5.56}$$

The multiplicativity of $f(\mu)$ is inherited by $c_{\mathbb{I}}^{\mathsf{pr}}(m)$, so it is sufficient to calculate $c_{\mathbb{I}}^{\mathsf{pr}}(m)$ for prime powers.

We start with $\pi = \sqrt{5}$. A primitive pair (q, p) with $|q|^2 = \sqrt{5}^r \varepsilon_1$, $|p|^2 = \sqrt{5}^s \varepsilon_2$ is admissible if and only if $r + s$ is even. From this, we infer that $c_{\mathbb{I}}^{\mathsf{pr}}(5^r)$ is given by

$$c_{\mathbb{I}}^{\mathsf{rot}}(5^r) = f(5^r)^2 + 2\sum_{s=1}^{[r/2]} f(5^r) f(5^{r-2s}) = 3 \cdot 5^{r-1}(13 \cdot 5^{r-1} - 1). \tag{5.57}$$

Similarly, if $p \equiv \pm 2 \pmod 5$, a primitive pair (q_1, q_2) with $|q_1|^2 = p^r \varepsilon_1$, $|q_2|^2 = p^s \varepsilon_2$ is admissible, if and only if, $r + s$ is even. The corresponding coincidence index is given by $p^{2\max(r,s)}$. Thus $c_{\mathbb{I}}^{\mathsf{rot}}(p^{2r-1}) = 0$. For even powers a similar calculation as above gives

$$c_{\mathbb{I}}^{\mathsf{rot}}(p^{2r}) = f(p^r)^2 + 2\sum_{s=1}^{[r/2]} f(p^r) f(p^{r-2s}) = \frac{p^2+1}{p^2-1} p^{2r-2}\left(p^{2r+2} + p^{2r-2} - 2\right). \tag{5.58}$$

The case $p \equiv \pm 1 \pmod 5$ is again more complicated, as p splits as $p = \pi\pi'$. Just as before, a primitive pair (q_1, q_2) with $|q_1|^2 = \pi^r \varepsilon_1$, $|q_2|^2 = \pi^s \varepsilon_2$ is admissible, if and only if, $r + s$ even. Thus, there are

$$g^{\mathsf{rot}}(\pi^r) = f(\pi^r)^2 + 2\sum_{s=1}^{[r/2]} f(\pi^r) f(\pi^{r-2s}) = \frac{p+1}{p-1} p^{r-1}(p^{r+1} + p^{r-1} - 2) \tag{5.59}$$

primitive admissible pairs to be considered. In addition, we get a contribution of those primitive admissible pairs with $|q_1|^2 = (\pi')^r\varepsilon_1$, $|q_2|^2 = (\pi')^s\varepsilon_2$. In total, this leads to

(5.60)
$$\begin{aligned}
c_{\mathbb{I}}^{\mathsf{rot}}(p^r) &= \sum_{s=0}^{r} g^{\mathsf{rot}}(\pi^{r-s})g^{\mathsf{rot}}((\pi')^s)\\
&= (p+1)p^{r-2}\left(2p^r(p+1) - 2\frac{p^{r-1}-1}{p-1}\left(6 + \frac{12}{p-1} + \frac{8}{(p-1)^2}\right)\right.\\
&\qquad \left. +(r-1)p^{r-2}\left(p^3+3p^2+7p+13+\frac{20}{p-1}+\frac{8}{(p-1)^2}\right) + (r-1)\frac{4(p+1)}{(p-1)^2}\right).
\end{aligned}$$

Actually, we do not need this explicit expression for $c_{\mathbb{I}}^{\mathsf{rot}}(p^r)$. Since $c_{\mathbb{I}}^{\mathsf{rot}}(p^r)$ is a Dirichlet convolution of $g^{\mathsf{rot}}(\pi^r)$ with itself, its corresponding Euler product is just the square of the Euler product corresponding to $g^{\mathsf{rot}}(\pi^r)$.

Putting everything together we get the following result.

Theorem 5.4.5. *Let $7200c_{\mathbb{I}}^{\mathsf{rot}}(m)$ be the number of coincidence rotations of the icosian ring $\mathbb{I}$. Then the Dirichlet series generating function for $c_{\mathbb{I}}^{\mathsf{rot}}(m)$ reads a follows*

$$\begin{aligned}
\Psi_{\mathbb{I}}^{\mathsf{rot}}(s) &= \sum_{n\in\mathbb{N}} \frac{c_{\mathbb{I}}^{\mathsf{rot}}(n)}{n^s} = \frac{\zeta_K(s)\zeta_K(s-1)}{\zeta_K(2s)}\frac{\zeta_K(s-1)\zeta_K(s-2)}{\zeta_K(2s-2)} = \zeta_{\mathbb{I}}^{\mathsf{pr}}(s)\zeta_{\mathbb{I}}^{\mathsf{pr}}(s-1)\\
&= \frac{(1+5^{-s})(1+5^{1-s})}{(1-5^{1-s})(1-5^{2-s})}\prod_{p\equiv\pm1(5)}\left(\frac{(1+p^{-s})(1+p^{1-s})}{(1-p^{1-s})(1-p^{2-s})}\right)^2\prod_{p\equiv\pm2(5)}\frac{(1+p^{-2s})(1+p^{2-2s})}{(1-p^{2-2s})(1-p^{4-2s})}\\
&= 1 + \frac{25}{4^s} + \frac{36}{5^s} + \frac{100}{9^s} + \frac{288}{11^s} + \frac{440}{16^s} + \frac{400}{19^s} + \frac{900}{20^s} + \frac{960}{25^s} + \frac{1800}{29^s} + \frac{2048}{31^s} + \cdots .
\end{aligned}$$

This shows that the possible coincidence indices are exactly those numbers that can be represented as $k^2 + k\ell - \ell^2 = \mathrm{Nr}(k+\ell\tau)$.

$\Psi_{\mathbb{I}}^{\mathsf{rot}}(s)$ is a meromorphic function in the entire complex plane, whose rightmost pole is a simple pole at $s=3$ with residue

(5.61)
$$\rho_{\mathbb{I}}^{\mathsf{rot}} := \mathrm{Res}_{s=3}\,\Psi_{\mathbb{I}}^{\mathsf{rot}}(s) = \frac{\zeta_K(2)^2\zeta_K(3)}{\zeta_K(4)\zeta_K(6)}L(1,\chi_5) = \frac{3^5\cdot5^7\cdot7\sqrt{5}}{268\pi^{12}}\log(\tau)\zeta_K(3) \approx 0.593177.$$

Here, we have inserted the explicit formulas for $\zeta_K(2)$ and $L(1,\chi_5)$ as given in Eq. 5.31. In addition, we have used the numerical value $\zeta_K(3) \approx 1.027548$ as well as the formulas

$$\zeta_K(4) = \frac{4\pi^8}{16875\sqrt{5}} \qquad \text{and} \qquad \zeta_K(6) = \frac{536\pi^{12}}{3^4\cdot5^8\cdot7\sqrt{5}}, \tag{5.62}$$

which can be derived from [**70**, Proposition 1, Theorem 4.2] as outlined in the appendix of [**10**].

Using Delange's theorem 7.A.1 we get the asymptotic behaviour of $c_{\mathbb{I}}^{\mathsf{rot}}(n)$.

COROLLARY 5.4.6. *The asymptotic behaviour of the summatory functions of* $c_{\mathbb{I}}^{\mathsf{rot}}(n)$ *reads as follows*

$$\sum_{m\leq x} c_{\mathbb{I}}^{\mathsf{rot}}(m) \sim \rho_{\mathbb{I}}^{\mathsf{rot}} \frac{x^3}{3} \approx 0.197726\, x^3, \;\; \textit{as } x \to \infty, \tag{5.63}$$

with $\rho_{\mathbb{I}}^{\mathsf{rot}}$ *as given above.*

The proof of Theorem 5.4.4 provides us with the tools to determine which CSMs are equal. In particular, Eq. (5.53) shows that

$$q_\alpha \mathbb{I} + \mathbb{I} p_\alpha = g_q(k_q\mathbb{I} + \mathbb{I}k_p)g_p \tag{5.64}$$

depends only on g_q, g_p, k_q and k_p. Recalling the definitions of g_q and k_q we see immediately that $g_q k_q$ divides q and $g_q|h_p|^2$. Since g_q divides α_p we infer that $g_q k_q$ divides $\alpha_p|h_p|^2 = \frac{\alpha_p}{\alpha_q}|p|^2 = |pq|$. Thus $g_q k_q$ divides $\operatorname{gcld}(q, |pq|)$. We claim that even $g_q k_q = \operatorname{gcld}(q, |pq|)$. Indeed, $|\operatorname{gcld}(q, |pq|)|^2 = |\operatorname{gcld}(q, \alpha_p\alpha_q \gcd(|p|^2, |q|^2)|^2 = \alpha_q \gcd(|p|^2, |q|^2) = |g_q|^2|k_q|^2$, which is only possible if $g_q k_q = \operatorname{gcld}(q, |pq|)$ up to units. Thus, we get the following alternative representation of the CSMs of $\mathbb{I}$.

THEOREM 5.4.7. *Let* (q, p) *be a primitive admissible pair. Decompose* $q = g_q k_q r_q$ *and* $p = r_p k_p q_p$ *such that* $|g_q|^2 = |r_q|^2 = \alpha_p$, $|g_p|^2 = |r_p|^2 = \alpha_q$, *and* $|k_q|^2 = |k_p|^2 = \gcd(|q|^2, |p|^2)$. *Then*

$$\mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} = g_q(k_q\mathbb{I} + \mathbb{I}k_p)g_p. \tag{5.65}$$

An immediate consequence is a sufficient condition for two CSMs to be equal.

COROLLARY 5.4.8. *Let* (q_1, p_1) *and* (q_2, p_2) *be two primitive admissible pairs such that* $|q_1p_1| = |q_2p_2|$ *and* $\alpha_{q_1} = \alpha_{q_2}$ *and* $\alpha_{p_1} = \alpha_{p_2}$. *Then*

$$\mathbb{I} \cap \frac{q_1\mathbb{I}p_1}{|q_1p_1|} = \mathbb{I} \cap \frac{q_2\mathbb{I}p_2}{|q_2p_2|} \tag{5.66}$$

holds if $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ *and* $\operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$.

PROOF. Since $\alpha_{p_1} = \alpha_{p_2}$ divides $|q_1p_1| = |q_2p_2|$, the condition $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ gives $g_{q_1} = \operatorname{gcld}(q_1, \alpha_{p_1}) = \operatorname{gcld}(q_2, \alpha_{p_2}) = g_{q_2}$, where we can guarantee by an appropriate choice of units that the equation holds exactly. Together with $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ this implies $k_{q_1} = k_{q_2}$ (up to units). Similarly, we can show $g_{p_1} = g_{p_2}$ and $k_{p_1} = k_{p_2}$, and an application of the theorem gives the result. □

If two coincidence rotations have the same denominator and the same coincidence index, their α's need not be the same, only their product is fixed. However, the conditions $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ and $\operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$ guarantee that we have indeed $\alpha_{p_1} = \alpha_{p_2}$ and $\alpha_{q_1} = \alpha_{q_2}$. Thus, we can reformulate the corollary as follows.

Corollary 5.4.9. *Let (q_1,p_1) and (q_2,p_2) be two primitive admissible pairs such that $|q_1p_1| = |q_2p_2|$ and $\operatorname{lcm}(|q_1|^2,|p_1|^2) = \operatorname{lcm}(|q_2|^2,|p_2|^2)$. Suppose that $\operatorname{gcld}(q_1,|p_1q_1|) = \operatorname{gcld}(q_2,|p_2q_2|)$ and $\operatorname{gcrd}(p_1,|p_1q_1|) = \operatorname{gcrd}(p_2,|p_2q_2|)$ hold. Then*

$$\mathbb{I} \cap \frac{q_1\mathbb{I}p_1}{|q_1p_1|} = \mathbb{I} \cap \frac{q_2\mathbb{I}p_2}{|q_2p_2|}. \tag{5.67}$$

Our aim is to prove the converse statement. To achieve this, we need some further lemmas. But first, we want to understand the theorem and its corollaries a bit better. In fact, it is not really necessary, but it improves the understanding of what is going on. Note that the denominator of our rotation is just $|pq|$, as well as for the inverse rotation. Hence, we have $|pq|\mathbb{I} \subseteq \frac{q\mathbb{I}p}{|qp|}$ and thus, $|pq|\mathbb{I} \subseteq \mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|}$. In particular,

$$\mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} = \mathbb{I} \cap \frac{q\mathbb{I}p}{|qp|} + |pq|\mathbb{I} = q_\alpha\mathbb{I} + \mathbb{I}p_\alpha + |pq|\mathbb{I} = q_r\mathbb{I} + \mathbb{I}p_r, \tag{5.68}$$

where $q_r = \operatorname{gcld}(q_\alpha,|pq|) = \alpha_q \operatorname{gcld}(q,|pq|)$ and $p_r = \operatorname{gcrd}(p_\alpha,|pq|) = \alpha_p \operatorname{gcld}(p,|pq|)$. Observing $g_q = \operatorname{gcld}(q_r,\alpha_p)$ and $g_p = \operatorname{gcrd}(p_r,\alpha_q)$ we could extend these considerations to an alternative proof of theorem 5.4.7.

As a first step in proving the converse of Corollary 5.4.9 we note that there is an analogue of Lemma 3.4.2 for $\mathbb{I}$.

Lemma 5.4.10. *If*

$$\mathbb{I} \cap \frac{q_1\mathbb{I}p_1}{|q_1p_1|} = \mathbb{I} \cap \frac{q_2\mathbb{I}p_2}{|q_2p_2|}. \tag{5.69}$$

then $|q_1p_1| = |q_2p_2|$ and $\operatorname{lcm}(|q_1|^2,|p_1|^2) = \operatorname{lcm}(|q_2|^2,|p_2|^2)$ (up to $\mathbb{Z}[\tau]$-units), i.e. denominator and coincidence index must be the same.

Here, $\operatorname{lcm}(|q_1|^2,|p_1|^2)$ can be interpreted as the $\mathbb{Q}(\tau)$-index of $\mathbb{I} \cap \frac{q_1\mathbb{I}p_1}{|q_1p_1|}$ in $\mathbb{I}$. Without going into details, we mention that one can define a so-called $\mathbb{Q}(\tau)$-index for a $\mathbb{Z}[\tau]$-sublattice $\mathcal{L}$ in a $\mathbb{Z}[\tau]$-lattice $\mathcal{G}$, compare [**11, 42**]. Just as the ordinary index $[\Gamma : \Lambda]$ equals $|\det(\phi)|$, where ϕ is a linear mapping which maps a basis of Γ onto a basis of Λ, one can define the $\mathbb{Q}(\tau)$-index $[\mathcal{G} : \mathcal{L}]_{\mathbb{Q}(\tau)}$ as the determinant of a linear mapping ϕ which maps a $\mathbb{Z}[\tau]$-basis of $\mathcal{G}$ onto a $\mathbb{Z}[\tau]$-basis of $\mathcal{L}$. This index is well-defined up to a unit in $\mathbb{Z}[\tau]$. The connection between the ordinary index $[\mathcal{G} : \mathcal{L}]$ and $[\mathcal{G} : \mathcal{L}]_{\mathbb{Q}(\tau)}$ is given by $[\mathcal{G} : \mathcal{L}] = |\operatorname{Nr}([\mathcal{G} : \mathcal{L}]_{\mathbb{Q}(\tau)})|$. In fact, one can prove that $\operatorname{lcm}(|q_1|^2,|p_1|^2)$ is the $\mathbb{Q}(\tau)$-index of $\mathbb{I} \cap \frac{q_1\mathbb{I}p_1}{|q_1p_1|}$ in $\mathbb{I}$ by adapting the proof of Theorem 5.4.4 to the $\mathbb{Q}(\tau)$-index.

Proof of Lemma 5.4.10. The statement $\operatorname{lcm}(|q_1|^2,|p_1|^2) = \operatorname{lcm}(|q_2|^2,|p_2|^2)$ just says that the $\mathbb{Q}(\tau)$-indices of $\mathbb{I} \cap \frac{q_1\mathbb{I}p_1}{|q_1p_1|}$ and $\mathbb{I} \cap \frac{q_2\mathbb{I}p_2}{|q_2p_2|}$ in $\mathbb{I}$ must be the same, which is trivial.

So it remains to show the claim for the denominator. We proceed as in the case of lattices. First, we see

$$|q_1p_1|\mathbb{I} \subseteq \mathbb{I} \cap \frac{q_2\mathbb{I}p_2}{|q_2p_2|}, \tag{5.70}$$

i.e. $|q_1p_1|$ is a $\mathbb{Z}[\tau]$-multiple of the denominator of the rotation $R(\bar{q}_2, \bar{p}_2)$, i.e. $|q_1p_1|$ is a $\mathbb{Z}[\tau]$–multiple of $|q_2p_2|$ and vice versa, so $\frac{|q_1p_1|}{|q_2p_2|}$ is a $\mathbb{Z}[\tau]$-unit. □

We need some additional information on the index $[\mathbb{I} : (r\mathbb{I} + \mathbb{I}s)]$. Theorem 5.4.4 only covers the case that (r, s) is the extension of an admissible pair, which is too restrictive here. We first consider the case that r and s are both primitive.

LEMMA 5.4.11. *If $r, s \in \mathbb{I}$ are primitive, then $[\mathbb{I} : (r\mathbb{I} + \mathbb{I}s)]$ divides $\mathrm{Nr}(\gcd(|r|^2, |s|^2))$.*

PROOF. The proof is similar to the first part of the proof of Theorem 5.4.4, so we just mention the main steps here. The details can be looked up above. First, note that the $\mathbb{Q}(\tau)$-index $[\mathbb{I} : (r\mathbb{I} + \mathbb{I}s)]_{\mathbb{Q}(\tau)}$ certainly divides $|r|^4$, since $(r\mathbb{I} + \mathbb{I}s) \supseteq r\mathbb{I}$. Next we determine a generator m of the ideal $\{\mu \in \mathbb{Z}[\tau] \mid r\mathbb{I} \supseteq \mu\mathbb{I}s\}$. It turns out that $m = |r|^2$ (up to units). Hence, we have an element $x \in \mathbb{I}s$ of $\mathbb{Z}[\tau]$-order $|r|^2$. But this implies that the $\mathbb{Q}(\tau)$-index $[(r\mathbb{I} + \mathbb{I}s) : r\mathbb{I}]_{\mathbb{Q}(\tau)}$ is a multiple of $m = |r|^2$, i.e. $[\mathbb{I} : (r\mathbb{I} + \mathbb{I}s)]_{\mathbb{Q}(\tau)}$ must divide $[\mathbb{I} : r\mathbb{I}]_{\mathbb{Q}(\tau)}/|r|^2 = |r|^2$. Similarly, $[\mathbb{I} : (r\mathbb{I}+\mathbb{I}s)]_{\mathbb{Q}(\tau)}$ must divide $|s|^2$, and hence $[\mathbb{I} : (r\mathbb{I}+\mathbb{I}s)]_{\mathbb{Q}(\tau)}$ divides $\gcd(|r|^2, |s|^2)$. Taking the norm finishes the proof. □

Primitive quaternions are not enough, since q_α and p_α are in general not primitive. However, α_q and α_p are relatively prime, so the following lemma is sufficient.

LEMMA 5.4.12. *If $r, s \in \mathbb{I}$ are primitive quaternions and $\beta, \gamma \in \mathbb{Z}[\tau]$ are relatively prime, then $[\mathbb{I} : (\beta r\mathbb{I} + \mathbb{I}\gamma s)]$ divides $\mathrm{Nr}(\beta_s^2\gamma_r^2 \gcd(\frac{|r|^2}{\gamma_r}, \frac{|s|^2}{\beta_s}))$, where $\beta_s := |\operatorname{gcrd}(\beta, s)|^2$ and $\gamma_r := |\operatorname{gcld}(\gamma, r)|^2$.*

In case of an admissible extension pair $\beta r = q_\alpha = \alpha_q q$, $\gamma s = p_\alpha = \alpha_p p$, we have $\beta_s = \beta = \alpha_q$, $\gamma_r = \gamma = \alpha_p$ and hence, $[\mathbb{I} : (q_\alpha\mathbb{I} + \mathbb{I}p_\alpha)]$ divides

$$\mathrm{Nr}\left(\alpha_q^2\alpha_p^2 \gcd\left(\frac{|q|^2}{\alpha_p}, \frac{|p|^2}{\alpha_q}\right)\right) = \mathrm{Nr}\left(\alpha_q^2\alpha_p^2 \gcd(|q|^2, |p|^2)\right) = \mathrm{Nr}(\alpha_q^2|q|^2) = \mathrm{Nr}(|q_\alpha|^2)$$

in agreement with theorem 5.4.4.

PROOF. We define $g_r := \operatorname{gcld}(\gamma, r)$ and $g_s := \operatorname{gcrd}(\beta, s)$ and use the decompositions $r = g_r k_r$, $s = k_s g_s$. This gives

$$\beta r\mathbb{I} + \mathbb{I}\gamma s = r\mathbb{I}(\beta + s) + (\gamma + r)\mathbb{I}s = r\mathbb{I}g_s + g_r\mathbb{I}s = g_r(k_r\mathbb{I} + \mathbb{I}k_s)g_s. \tag{5.71}$$

Hence, we see that

$$[\mathbb{I} : (\beta r\mathbb{I} + \mathbb{I}\gamma s)] = \mathrm{Nr}(|g_r|^4)\,\mathrm{Nr}(|g_s|^4)[\mathbb{I} : (k_r\mathbb{I} + \mathbb{I}k_s)] = \mathrm{Nr}(\beta_s^2\gamma_r^2)[\mathbb{I} : (k_r\mathbb{I} + \mathbb{I}k_s)] \tag{5.72}$$

divides $\mathrm{Nr}(\beta_s^2\gamma_r^2)\,\mathrm{Nr}(\gcd(|k_r|^2, |k_s|^2))$ by the previous lemma. Observing $|k_r|^2 = \frac{|r|^2}{\gamma_r}$ and $|k_s|^2 = \frac{|s|^2}{\beta_s}$ proves the assertion. □

Now we have everything at hand to prove the following criterion for two CSMs to be equal.

Theorem 5.4.13. *Let (q_1, p_1) and (q_2, p_2) be two primitive admissible pairs. Then*

$$\mathbb{I} \cap \frac{q_1 \mathbb{I} p_1}{|q_1 p_1|} = \mathbb{I} \cap \frac{q_2 \mathbb{I} p_2}{|q_2 p_2|} \tag{5.73}$$

holds if and only if $|q_1p_1| = |q_2p_2|$, $\operatorname{lcm}(|q_1|^2, |p_1|^2) = \operatorname{lcm}(|q_2|^2, |p_2|^2)$, $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ *and* $\operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$ *hold (up to units).*

Proof. Corollary 5.4.9 proves the if-statement, Lemma 5.4.10 guarantees that the denominator and the coincidence index (and its $\mathbb{Q}(\tau)$-variant) are equal. Hence it remains to show that two CSMs are only equal if $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ and $\operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$ hold. That means, we have to show that

$$q_{1\alpha}\mathbb{I} + \mathbb{I}p_{1\alpha} = q_{2\alpha}\mathbb{I} + \mathbb{I}p_{2\alpha} \tag{5.74}$$

implies $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ and $\operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$. We make use of Eq. (5.68) and assume that

$$q_{1r}\mathbb{I} + \mathbb{I}p_{1r} = q_{2r}\mathbb{I} + \mathbb{I}p_{2r} \tag{5.75}$$

holds, where $q_{ir} = \operatorname{gcld}(q_{i\alpha}, |p_1q_1|) = \alpha_{q_i} \operatorname{gcld}(q_i, |p_1q_1|)$ and $p_{ir} = \operatorname{gcrd}(p_{i\alpha}, |p_1q_1|) = \alpha_{p_i} \operatorname{gcld}(p_i, |p_1q_1|)$. This equation can be used to rewrite $q_{1r}\mathbb{I} + \mathbb{I}p_{1r}$ as

$$q_{1r}\mathbb{I} + \mathbb{I}p_{1r} = (q_{1r} + q_{2r})\mathbb{I} + \mathbb{I}(p_{1r} + p_{2r}) = \beta r \mathbb{I} + \mathbb{I}\gamma s \tag{5.76}$$

where $\beta r := \operatorname{gcld}(q_{1r}, q_{2r})$ and $\gamma s := \operatorname{gcrd}(p_{1r}, p_{2r})$, with r and s primitive. Note that $\beta = \gcd(\alpha_{q_1}, \alpha_{q_2})$ and $\gamma = \gcd(\alpha_{p_1}, \alpha_{p_2})$ are relatively prime, since α_{q_1} and α_{p_1} are relatively prime. By definition, $|r|^2$ divides $\frac{|p_1q_1|}{\beta}$ and $|s|^2$ divides $\frac{|p_1q_1|}{\gamma}$. Since β and γ are relatively prime, $\gcd(|r|^2, |s|^2)$ divides $\gcd(\frac{|p_1q_1|}{\beta}, \frac{|p_1q_1|}{\gamma}) = \frac{|p_1q_1|}{\beta\gamma}$. Applying Lemma 5.4.12 and noting that β_s and γ_r divide β and γ, respectively, we infer that $[\mathbb{I} : (\beta r\mathbb{I} + \mathbb{I}\gamma s)]$ must divide $\operatorname{Nr}(\beta_s\gamma_r|p_1q_1|)$. From $[\mathbb{I} : (\beta r\mathbb{I} + \mathbb{I}\gamma s)] = [\mathbb{I} : (q_{1\alpha}\mathbb{I} + \mathbb{I}p_{1\alpha})] = \operatorname{Nr}(\alpha_{q_1}\alpha_{p_1}|p_1q_1|)$ we infer that $\operatorname{Nr}(\alpha_{q_1}\alpha_{p_1})$ divides $\operatorname{Nr}(\beta_s\gamma_r)$ and hence $\beta_s = \beta = \alpha_{q_1} = \alpha_{q_2}$ and $\gamma_r = \gamma = \alpha_{p_1} = \alpha_{p_2}$. Using this new information we can apply Lemma 5.4.12 again and we infer that $\frac{|p_1q_1|}{\alpha_{q_1}\alpha_{p_1}} = \gcd(|q_1|^2, |p_1|^2)$ must divide $\gcd(\frac{|r|^2}{\alpha_{p_1}}, \frac{|s|^2}{\alpha_{q_1}})$. But since $|r|^2$ divides $\frac{|p_1q_1|}{\beta} = \frac{|p_1q_1|}{\alpha_{q_1}}$ as stated above, we must have $|r|^2 = \frac{|p_1q_1|}{\alpha_{q_1}} = |\operatorname{gcld}(q_1, |p_1q_1|)|^2$ and hence $r = \operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$. Analogously $s = \operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$, which finishes the proof. □

Remark 5.4.1. As in the case of the centred hypercubic lattice we may reformulate the conditions for equivalence, compare 4.1.3. In particular, (q_1, p_1) and (q_2, p_2) generate the same CSM, if and only if $|q_1|^2 = |q_2|^2$, $|p_1|^2 = |p_2|^2$, $\operatorname{gcld}(q_1, |p_1q_1|) = \operatorname{gcld}(q_2, |p_2q_2|)$ and $\operatorname{gcrd}(p_1, |p_1q_1|) = \operatorname{gcrd}(p_2, |p_2q_2|)$ (up to units) are satisfied.

It is now a purely combinatorial task to calculate $c_{\mathbb{I}}(m)$ and the corresponding Dirichlet series. Again, we can restrict our calculations to the cases that m is a prime power. As an example, we consider the case $p \equiv \pm 2 \pmod 5$. Here, we have to evaluate the sum

$$c_{\mathbb{I}}(\pi^{2r}) = f(\pi^r)^2 + 2\sum_{s=1}^{[r/2]} f(\pi^{r-s}) f(\pi^{r-2s}). \tag{5.77}$$

Note that the only difference between this sum and Eq. (5.58) is that a factor $f(\pi^r)$ has been replaced by a factor $f(\pi^{r-s})$, which reflects the condition $\operatorname{gcld}(q_1, |p_1 q_1|) = \operatorname{gcld}(q_2, |p_2 q_2|)$ or $\operatorname{gcrd}(p_1, |p_1 q_1|) = \operatorname{gcrd}(p_2, |p_2 q_2|)$, respectively.

For prime powers $m = p^r$, the multiplicative function $c_{\mathbb{I}}(m)$ can be expressed in terms of the function

$$h(x,r) = \begin{cases} 1 & \text{if } r = 0, \\ \frac{(x+1)^2}{x^3-1}\left(x^{2r+1} + x^{2r-2} - 2x^{(r-1)/2}\right), & \text{if } r \geq 1 \text{ is odd}, \\ \frac{(x+1)^2}{x^3-1}(x^{2r+1} + x^{2r-2} - 2x^{r/2-1}\frac{1+x^2}{1+x}), & \text{if } r \geq 2 \text{ is even}. \end{cases} \tag{5.78}$$

$c_{\mathbb{I}}(p^r)$ for $r \geq 1$ reads explicitly

$$c_{\mathbb{I}}(p^r) = \begin{cases} h(5,r) & \text{if } p = 5, \\ \sum\limits_{s=0}^{r} h(p, r-s) h(p,s) & \text{if } p \equiv \pm 1 \pmod 5. \\ h(p^2, \frac{r}{2}) & \text{if } p \equiv \pm 2 \pmod 5 \text{ and } r \text{ even}, \\ 0 & \text{if } p \equiv \pm 2 \pmod 5 \text{ and } r \text{ odd}, \end{cases} \tag{5.79}$$

Finally, by constructing the corresponding Euler factors we get the generating function for $c_{\mathbb{I}}(m)$.

THEOREM 5.4.14. *Let $c_{\mathbb{I}}(m)$ be the number of CSMs of the icosian ring $\mathbb{I}$. Then the Dirichlet series generating function for $c_{\mathbb{I}}(m)$ reads as follows*

$$\begin{aligned} \Psi_{\mathbb{I}}(s) &= \sum_{n \in \mathbb{N}} \frac{c_{\mathbb{I}}(n)}{n^s} \\ &= \frac{1 + 11 \cdot 5^{-s} + 7 \cdot 5^{-2s} + 5^{1-3s}}{(1 - 5^{2-s})(1 - 5^{1-2s})} \\ &\quad \times \prod_{p \equiv \pm 1(5)} \left(\frac{1 + p^{-s} + 2p^{1-s} + 2p^{-2s} + p^{1-2s} + p^{1-3s}}{(1-p^{2-s})(1-p^{1-2s})} \right)^2 \\ &\quad \times \prod_{p \equiv \pm 2(5)} \frac{1 + p^{-2s} + 2p^{2-2s} + 2p^{-4s} + p^{2-4s} + p^{2-6s}}{(1-p^{4-2s})(1-p^{2-4s})} \\ &= 1 + \frac{25}{4^s} + \frac{36}{5^s} + \frac{100}{9^s} + \frac{288}{11^s} + \frac{410}{16^s} + \frac{400}{19^s} + \frac{900}{20^s} + \frac{912}{25^s} + \frac{1800}{29^s} + \frac{2048}{31^s} + \cdots . \end{aligned}$$

We are not aware of a representation of $\Psi_{\mathbb{I}}(s)$ in terms of ζ-functions. Nevertheless, we can specify its analytic properties. We note that the Euler product

$$\begin{aligned}
\psi_{\mathbb{I}}(s) := \frac{\Psi_{\mathbb{I}}(s)}{\Psi_{\mathbb{I}}^{\mathsf{rot}}(s)} &= \left(1 - \frac{48 \cdot 5^{-2s}}{(1+5^{-s})(1+5^{1-s})(1-5^{1-2s})}\right) \\
&\times \prod_{p \equiv \pm 1 (5)} \left(1 - \frac{2(p^2-1)p^{-2s}}{(1+p^{-s})(1+p^{1-s})(1-p^{1-2s})}\right)^2 \\
&\times \prod_{p \equiv \pm 2 (5)} \left(1 - \frac{2(p^4-1)p^{-4s}}{(1+p^{-2s})(1+p^{2-2s})(1-p^{2-4s})}\right)
\end{aligned} \tag{5.80}$$

converges for $\mathrm{Re}(s) > \frac{3}{2}$, which implies that $\Psi_{\mathbb{I}}(s)$ is meromorphic in the half plane $\{\mathrm{Re}(s) > \frac{3}{2}\}$. Moreover, the rightmost pole of $\Psi_{\mathbb{I}}(s)$ is a simple pole located at $s = 3$ with residue

$$\rho_{\mathbb{I}} := \mathrm{Res}_{s=3}\, \Psi_{\mathbb{I}}(s) = \psi_{\mathbb{I}}(3)\rho_{\mathbb{I}}^{\mathsf{rot}} \approx 0.587063, \tag{5.81}$$

Here, $\psi_{\mathbb{I}}(3) \approx 0.9896918 < 1$ had to be calculated numerically. Finally, we apply Delange's theorem 7.A.1 to obtain the asymptotic behaviour of $c_{\mathbb{I}}(n)$.

COROLLARY 5.4.15. *The asymptotic behaviour of the summatory functions of $c_{\mathbb{I}}(n)$ reads as follows*

$$\sum_{m \leq x} c_{\mathbb{I}}(m) \sim \rho_{\mathbb{I}} \frac{x^3}{3} \approx 0.195688\, x^3, \text{ as } x \to \infty, \tag{5.82}$$

with $\rho_{\mathbb{I}}$ as given above.

Note that $\rho_{\mathbb{I}}$ and $\rho_{\mathbb{I}}^{\mathsf{rot}}$ differ by just about 1%. Thus, in most cases, two coincidence rotations that are not symmetry related generate different CSMs.

5.5. Equal CSLs for L

It remains to discuss when two CSLs of L are equal. We first reformulate Lemma 3.4.2 for L, which reads as follows, since $\mathrm{den}_{A_4}(R) = \mathrm{den}_{A_4}(R^{-1})$.

LEMMA 5.5.1. *Let L be the A_4-lattice. Then $L(R_1) = L(R_2)$ implies $\Sigma(R_1) = \Sigma(R_2)$ and* $\mathrm{den}(R_1) = \mathrm{den}(R_2)$.

For the following, it is convenient to introduce the $\mathbb{Q}$-linear maps $\phi_\pm : \mathbb{H}(K) \to \mathbb{H}(K), \phi_\pm(q) = q \pm \tilde{q}$, compare [**9**]. They map $\mathbb{H}(K)$ onto two disjoint 4-dimensional $\mathbb{Q}$-subspaces $V_\pm = \phi_\pm(\mathbb{H}(K))$. In particular, we have $\mathbb{H}(K) = V_+ \oplus V_-$, if we view $\mathbb{H}(K)$ as an 8-dimensional vector space over $\mathbb{Q}$.

In this setting, L and L_{q_α} can be viewed as images of ideals of $\mathbb{I}$. In particular, we have $L = \phi_+(\mathbb{I})$ and

$$L(R(q)) = L_{q_\alpha} = \phi_+(q_\alpha \mathbb{I}) = \phi_+(q_\alpha \mathbb{I} + \mathbb{I}\tilde{q_\alpha}) = (q_\alpha \mathbb{I} + \mathbb{I}\tilde{q_\alpha}) \cap L, \tag{5.83}$$

compare Theorem 5.2.6. Thus two CSLs are certainly equal, if the corresponding CSMs of $\mathbb{I}$ are equal. Applying Theorem 5.4.13 to our situation and observing $\operatorname{gcrd}(\tilde{q}_1, |q_1\tilde{q}_1|) = \operatorname{gcld}\widetilde{(q_1, |}q_1\tilde{q}_1|)$ gives the following result.

Lemma 5.5.2. *Assume that q_1 and q_2 are admissible. Assume that $|q_1|^2 = |q_2|^2$ and $\operatorname{gcld}(q_1, |q_1\tilde{q}_1|) = \operatorname{gcld}(q_2, |q_2\tilde{q}_2|)$. Then $L(R(q_1)) = L(R(q_2))$.*

It turns out that the converse is not true. However, we have the following statement:

Theorem 5.5.3. *Assume that q_1 and q_2 are admissible. Assume that one of $|q_1|^2$ and $|q_2|^2$ is not divisible by 5. Then $L(R(q_1)) = L(R(q_2))$ if and only if $|q_1|^2 = |q_2|^2$ and $\operatorname{gcld}(q_1, |q_1\tilde{q}_1|) = \operatorname{gcld}(q_2, |q_2\tilde{q}_2|)$.*

Proof. We need to prove only the “only if”-statement. Assume $L(R(q_1)) = L(R(q_2))$, i.e.,

$$\phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) = \phi_+(q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha}) = \phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha} + q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha}) = \phi_+(g\mathbb{I} + \mathbb{I}\tilde{g}), \tag{5.84}$$

where we have used the $\mathbb{Q}$-linearity of ϕ_+ and applied the definition $g = \operatorname{gcld}(q_{1\alpha}, q_{2\alpha})$. If g is the extension of an admissible primitive quaternion, we can apply Lemma 5.5.1 and $g\mathbb{I} = q_{1\alpha}\mathbb{I} = q_{2\alpha}\mathbb{I}$ and $q_1\mathbb{I} = q_2\mathbb{I}$ follows. However, in general, g is not the extension of a primitive admissible quaternion. So we have to argue differently. First, we observe that we can apply Lemma 5.5.1 to show $|q_{1\alpha}|^2 = |q_{2\alpha}|^2$, i.e. none of them is divisible by 5. Next, we consider the following chain of inclusions

$$\begin{aligned}
&\phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) + \tau\phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) = \\
&\qquad = \phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) \cap \phi_+(q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha}) + \tau\Big(\phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) \cap \phi_+(q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha})\Big) \\
&\qquad \subseteq (q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) \cap (q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha}) \subseteq (q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) \subseteq \mathbb{I}.
\end{aligned}$$

We know $[\mathbb{I} : (\phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) + \tau\phi_+(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}))] = 5\operatorname{lcm}(|q_1|^2, |\tilde{q}_1|^2)$ by Lemma 5.3.6 and $[\mathbb{I} : (q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha})] = \operatorname{lcm}(|q_1|^2, |\tilde{q}_1|^2) = [\mathbb{I} : (q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha})]$. Since the latter indices are not divisible by 5 by assumption, this implies

$$[\mathbb{I} : (q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) \cap (q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha})] = [\mathbb{I} : (q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha})]. \tag{5.85}$$

As a consequence, we have

$$(q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha}) \cap (q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha})] = q_{1\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{1\alpha} = q_{2\alpha}\mathbb{I} + \mathbb{I}\tilde{q}_{2\alpha} \tag{5.86}$$

and an application of Theorem 5.4.13 yields $|q_1\tilde{q}_1| = |q_2\tilde{q}_2|$, $\operatorname{lcm}(|q_1|^2, |\tilde{q}_1|^2) = \operatorname{lcm}(|q_2|^2, |\tilde{q}_2|^2)$, and $\operatorname{gcld}(q_1, |q_1\tilde{q}_1|) = \operatorname{gcld}(q_2, |q_2\tilde{q}_2|)$. Recalling $\frac{|q_i\tilde{q}_i|}{\alpha_{\tilde{q}_i}} = |\operatorname{gcld}(q_i, |q_i\tilde{q}_i|)|^2$ we see that $\alpha_{\tilde{q}_1} = \alpha_{\tilde{q}_2}$ and, hence, $\alpha_{q_1} = \alpha_{q_2}$, which gives $|q_1|^2 = |q_2|^2$ via $|q_i|^2 = \frac{\operatorname{lcm}(|q_i|^2, |\tilde{q}_i|^2)}{\alpha_{q_i}^2}$. □

Next, we consider the case where Σ is a power of 5. The general case will follow from a combination of these two special cases.

LEMMA 5.5.4. *Assume that q_1 and q_2 are admissible. Assume that one of $|q_1|^2$ and $|q_2|^2$ is a power of* 5*. Then $L(R(q_1)) = L(R(q_2))$ if and only if $|q_1|^2 = |q_2|^2$ and* $\mathrm{gcld}(q_1, |q_1\tilde{q}_1|/\sqrt{5}) = \mathrm{gcld}(q_2, |q_2\tilde{q}_2|/\sqrt{5})$.

PROOF. First, let us assume $L(R(q_1)) = L(R(q_2))$. If $|q_1|^2$ is a power of 5, then $|q_1|^2 = |\tilde{q}_1|^2 = \Sigma_{A_4}(R(q_1))$ and $q_1 = q_{1\alpha}$, i.e., we may drop the subscript α everywhere. Hence, $|q_2|^2$ is a power of 5 as well and $|q_1|^2 = |q_2|^2$, since the coincidence indices must be the same. We proceed now as above and find that either

$$[\mathbb{I} : (q_1\mathbb{I} + \mathbb{I}\tilde{q}_1) \cap (q_2\mathbb{I} + \mathbb{I}\tilde{q}_2)] = [\mathbb{I} : (q_1\mathbb{I} + \mathbb{I}\tilde{q}_1)] \tag{5.87}$$

– in this case we argue as above and conclude that $\mathrm{gcld}(q_1, |q_1\tilde{q}_1|) = \mathrm{gcld}(q_2, |q_2\tilde{q}_2|)$ and, a fortiori, $\mathrm{gcld}(q_1, |q_1\tilde{q}_1|/\sqrt{5}) = \mathrm{gcld}(q_2, |q_2\tilde{q}_2|/\sqrt{5})$ – or

$$[\mathbb{I} : (q_1\mathbb{I} + \mathbb{I}\tilde{q}_1) \cap (q_2\mathbb{I} + \mathbb{I}\tilde{q}_2)] = 5[\mathbb{I} : (q_1\mathbb{I} + \mathbb{I}\tilde{q}_1)]. \tag{5.88}$$

In this case, $(q_1\mathbb{I} + \mathbb{I}\tilde{q}_1)$ has index 5 in

$$(q_1\mathbb{I} + \mathbb{I}\tilde{q}_1) + (q_2\mathbb{I} + \mathbb{I}\tilde{q}_2) = g\mathbb{I} + \mathbb{I}\tilde{g}, \tag{5.89}$$

where $g = \mathrm{gcld}(q_1, q_2)$ need not be an admissible quaternion, since $|g|^2$ may be an odd power of $\sqrt{5}$ (up to units, of course). However, $|g|^2$ and hence $|g\tilde{g}|$ are still in $\mathbb{Z}[\tau]$, thus $(g, \tilde{g})$ is an admissible pair for $\mathbb{I}$. Since $g = g_\alpha$ we see that $g\mathbb{I} + \mathbb{I}\tilde{g}$ is the CSM generated by the pair $(g, \tilde{g})$ and, hence, its coincidence index $\Sigma_{\mathbb{I}}$ is given by $\mathrm{Nr}(|g|^2)$, i.e., $\mathrm{Nr}(|q_1|^2) = 5\,\mathrm{Nr}(|g|^2)$. This is equivalent to $|q_1|^2 = \sqrt{5}|g|^2$. As g is a left divisor of q_1 and $|g|^2$ we infer $g = \mathrm{gcld}(q_1, |g|^2) = \mathrm{gcld}(q_1, |q_1|^2/\sqrt{5})$ and, by symmetry, $g = \mathrm{gcld}(q_2, |q_2|^2/\sqrt{5})$ as well.

Conversely, let us assume $|q_1|^2 = |q_2|^2$ and $\mathrm{gcld}(q_1, |q_1\tilde{q}_1|/\sqrt{5}) = \mathrm{gcld}(q_2, |q_2\tilde{q}_2|/\sqrt{5})$. Then either $q_1 = q_2$ (up to units) and we are done, or $g = \mathrm{gcld}(q_1, q_2) = \mathrm{gcld}(q_1, |q_1\tilde{q}_1|/\sqrt{5})$. In this case g is not admissible for L since $|g|^2 = |q_1|^2/\sqrt{5}$ is no integer. We define $g_1 = \mathrm{gcld}(q_1, |q_1\tilde{q}_1|/5)$, which is the greatest admissible divisor of g. We have $|g_1|^2 = |q_1|^2/5$ and

$$\phi_+(q_1\mathbb{I}) \subseteq \phi_+(q_1\mathbb{I}) + \phi_+(q_2\mathbb{I}) = \phi_+(g\mathbb{I}) \subseteq \phi_+(g_1\mathbb{I}) \tag{5.90}$$

with $[\phi_+(g_1\mathbb{I}) : \phi_+(q_1\mathbb{I})] = 5$. Hence, either $\phi_+(q_1\mathbb{I}) = \phi_+(q_1\mathbb{I}) + \phi_+(q_2\mathbb{I})$ – in this case we are done – or $\phi_+(g\mathbb{I}) = \phi_+(g_1\mathbb{I})$. We want to rule out the latter by contradiction. So assume the latter. Then $\phi_+(q_1\mathbb{I})$ has index 5 in $\phi_+(g\mathbb{I})$. Moreover, $\phi_+(g\mathbb{I}) + \tau\phi_+(g\mathbb{I})$ has index $|g_1|^4 = |q_1|^4/25$ in $L[\tau]$ and index $5|g_1|^4 = |q_1|^4/5$ in $\mathbb{I}$. Furthermore,

$$\phi_+(g\mathbb{I}) + \tau\phi_+(g\mathbb{I}) \subseteq g\mathbb{I} + \mathbb{I}\tilde{g}, \tag{5.91}$$

where the latter has index $|g|^4 = |q_1|^4/5$ in $\mathbb{I}$. Hence,

$$g\mathbb{I} + \mathbb{I}\tilde{g} = \phi_+(g\mathbb{I}) + \tau\phi_+(g\mathbb{I}) \subset L[\tau]. \tag{5.92}$$

Now, Corollary 5.3.4 tells us $\sqrt{5}\mathbb{I} \subset L[\tau]$, i.e., with $m = \mathrm{gcld}(g, \sqrt{5})$, we have $m\mathbb{I} + \mathbb{I}\tilde{m} \subseteq L[\tau]$. Since the left hand side has index $\mathrm{Nr}(|m|^2) = 5$ in $\mathbb{I}$, this would imply $m\mathbb{I} + \mathbb{I}\tilde{m} = L[\tau]$. But this is impassible: as m is a prime quaternion of norm $|m|^2 = \sqrt{5}$, this would imply $m\mathbb{I} = m\mathbb{I} + \mathbb{I}\tilde{m} = \mathbb{I}\tilde{m}$. But $m\mathbb{I}$ cannot be a two-sided ideal, as m is not central (compare the proof of Lemma 5.3.6). This gives a contradiction and finishes the proof. □

Next, we combine Theorem 5.5.3 and Lemma 5.5.4 to obtain the corresponding statement for general indices that are divisible by 5.

THEOREM 5.5.5. *Assume that q_1 and q_2 are admissible. Assume that one of $|q_1|^2$ and $|q_2|^2$ is divisible by* 5. *Then $L(R(q_1)) = L(R(q_2))$ if and only if $|q_1|^2 = |q_2|^2$ and* $\operatorname{gcld}(q_1, |q_1\tilde{q}_1|/\sqrt{5}) = \operatorname{gcld}(q_2, |q_2\tilde{q}_2|/\sqrt{5})$.

PROOF. Using the same arguments as in the preceding proof, we can show that the conditions $|q_1|^2 = |q_2|^2$ and $\operatorname{gcld}(q_1, |q_1\tilde{q}_1|/\sqrt{5}) = \operatorname{gcld}(q_2, |q_2\tilde{q}_2|/\sqrt{5})$ are sufficient.

To show the converse, we note that the unique prime factorisation in $\mathbb{I}$ guarantees that every coincidence rotation R can be written as $R = R_1R_2$, where $\varSigma_{A_4}(R_1)$ is not divisible by 5 and $\varSigma_{A_4}(R_2)$ is a power of 5. Thus, with $m := \varSigma_{A_4}(R_1)$ and $n := \varSigma_{A_4}(R_2)$ all conditions of Lemma 3.4.7 are met. Now, $(nL) \cap L(R_1R_2) = nL(R_1)$ and $(mRL) \cap L(R_1R_2) = nR_1L(R_2)$. This allows us to determine $L(R_1)$ and $L(R_2)$ from the knowledge of $L(R_1R_2)$ alone. Thus, two coincidence rotations R and R' can generate the same CSL only if $L(R_1) = L(R'_1)$ as well as $L(R_2) = L(R'_2)$. We can now apply Theorem 5.5.3 and Lemma 5.5.4 to obtain the result. □

We can calculate $c_{A_4}(m)$ now. As $c_{A_4}(m)$ is multiplicative, we only need to determine it for prime powers. Actually, we do not need Theorem 5.5.5, but Lemma 5.5.4 and Theorem 5.5.3 are sufficient. If $|q|^2 = \sqrt{5}^{\,r}\varepsilon$, then the lemma tells us that the last prime quaternion in the prime factorisation does not matter, which gives $c_{A_4}(5^r) = \frac{1}{5}c^{\mathsf{rot}}_{A_4}(5^r)$. If $p \equiv \pm 2 \pmod 5$, the conditions of the theorem reduce to $q_1\mathbb{I} = q_2\mathbb{I}$, and, hence, $c_{A_4}(p^r) = c^{\mathsf{rot}}_{A_4}(p^r)$ in this case.

The case $p \equiv \pm 1 \pmod 5$ is again more complicated. But similar arguments as in the previous sections finally yield the following explicit formula

(5.93)
$$c_{A_4}(p^r) = \begin{cases} 6 \cdot 5^{2r-2}, & \text{if } p = 5, \\ \frac{(p+1)^2}{p^3-1}\left(p^{2r+1} + p^{2r-2} - 2p^{(r-1)/2}\right), & \text{if } p \equiv \pm 1 \pmod 5 \text{ and } r \text{ is odd}, \\ \frac{(p+1)^2}{p^3-1}(p^{2r+1} + p^{2r-2} - 2p^{r/2-1}\frac{1+p^2}{1+p}), & \text{if } p \equiv \pm 1 \pmod 5 \text{ and } r \text{ is even}, \\ p^{2r} + p^{2r-2}, & \text{if } p \equiv \pm 2 \pmod 5). \end{cases}$$

This enables us to write down the generating function.

THEOREM 5.5.6. *Let $c_{A_4}(m)$ be the number of CSLs of the lattice A_4. Then the Dirichlet series generating function for $c_{A_4}(m)$ reads a follows*

$$\begin{aligned}\Psi_{A_4}(s) &= \sum_{n\in\mathbb{N}} \frac{c_{A_4}(n)}{n^s} \\ &= \left(1 + 6\frac{5^{-s}}{1-5^{2-s}}\right) \prod_{p\equiv\pm2(5)} \frac{1+p^{-s}}{1-p^{2-s}} \prod_{p\equiv\pm1(5)} \frac{1 + p^{-s} + 2p^{1-s} + 2p^{-2s} + p^{1-2s} + p^{1-3s}}{(1-p^{2-s})(1-p^{1-2s})} \\ &= 1 + \frac{5}{2^s} + \frac{10}{3^s} + \frac{20}{4^s} + \frac{6}{5^s} + \frac{50}{6^s} + \frac{50}{7^s} + \frac{80}{8^s} + \frac{90}{9^s} + \frac{30}{10^s} + \frac{144}{11^s} + \frac{200}{12^s} + \frac{170}{13^s} + \cdots .\end{aligned}$$

In order to compare $\Psi_{A_4}(s)$ and $\Psi^{\mathsf{rot}}_{A_4}(s)$ we consider the function

$$\begin{aligned}\psi_{A_4}(s) &:= \frac{\Psi_{A_4}(s)}{\Psi^{\mathsf{rot}}_{A_4}(s)} \\ &= \left(1 - \frac{24 \cdot 5^{-s}}{1+5^{1-s}}\right) \prod_{p \equiv \pm 1(5)} \left(1 - \frac{2(p^2-1)p^{-2s}}{(1+p^{-s})(1+p^{1-s})(1-p^{1-2s})}\right).\end{aligned} \tag{5.94}$$

It is analytic in the open half plane $\{\mathrm{Re}(s) > \frac{3}{2}\}$, as the Euler product converges there. This proves that $\Psi_{A_4}(s)$ is a meromorphic function in the open half plane $\{\mathrm{Re}(s) > \frac{3}{2}\}$. Its rightmost pole is a simple pole at $s = 3$ with residue

$$\rho_{A_4} = \mathrm{Res}_{s=3}\, \Psi_{A_4}(s) = \psi_{A_4}(3)\rho^{\mathsf{rot}}_{A_4} \approx 1.025695, \tag{5.95}$$

where $\psi_{A_4}(3) \approx 0.8152576 < 1$ has been calculated numerically. Finally, we apply Delange's theorem 7.A.1, which gives us the asymptotic growth rate of $c_{A_4}(m)$.

Corollary 5.5.7. *With the residue ρ_{A_4} from above, the asymptotic behaviour of $c_{A_4}(m)$ is given by*

$$\sum_{m \le x} c_{A_4}(m) \sim \rho_{A_4} \frac{x^3}{3} \approx 0.341898\, x^3, \quad \textit{as } x \to \infty. \tag{5.96}$$

Comparing the growth rates of the number of CSLs and coincidence rotations, we see that the former is approximately 20% lower than the latter. This difference is much bigger than in the case of the icosian ring. Nevertheless, it is still more an exception than a rule that two coincidence rotations that are not symmetry related generate the same CSL.

CHAPTER 6

Multiple CSLs of the cubic lattices

So far, we have considered ordinary CSLs and CSMs. The problem of finding all multiple CSLs (MCSLs) is, in general, more difficult than determining all CSLs. There are only few cases, where the problem of multiple coincidences has been solved so far. These include some 2-dimensional lattices and modules of n-fold symmetry [**6**] and the 3-dimensional cubic lattices, which we want to discuss in this chapter. Some of the present results can be found in [**75**].

6.1. Basic results

Let us recall from Section 3.5 that any coincidence rotation R of the cubic lattices can be parametrised by primitive quaternions. Moreover, there is a bijection between the CSLs of the body-centred cubic lattice and the ideals $q\mathbb{J}$ generated by odd primitive quaternions. In particular, we have $\varGamma_{bcc} = \mathrm{Im}(\mathbb{J})$ and $\varGamma_{bcc}(R(q)) = \mathrm{Im}(q\mathbb{J})$ with $\varSigma(R(q)) = |q|^2$ if q is a primitive odd quaternion. If q is an even primitive quaternion, then $\varSigma(R(q)) = \frac{|q|^2}{2}$. In this case, q can be written as a product $r(1,1,0,0)$ of an odd primitive quaternion with an even one, and the corresponding CSL can be written as $\varGamma_{bcc}(R(q)) = \mathrm{Im}(r\mathbb{J})$.

Thus, it is sufficient to consider CSLs generated by primitive odd quaternions. Just as in the case of ordinary CSLs, we start with the analysis of the body-centred cubic lattice and derive from it the MCSLs of the other cubic lattices.

Let us discuss the spectrum of possible coincidence indices first. We know that the possible indices for ordinary CSLs for all three types of cubic lattices are the positive odd integers, and, indeed, all of them occur as indices. Moreover, we have seen in Section 3.3 that $\varSigma(R_1, \ldots, R_m)$ divides $\varSigma(R_1) \cdot \ldots \cdot \varSigma(R_m)$. Thus, the spectrum of indices of MCSLs is again the set of positive odd integers.

Proposition 6.1.1. *Let $\varGamma$ be any cubic lattice. The possible values for the coincidence indices $\varSigma(R_1, \ldots, R_m)$ are exactly the positive odd integers, and all of those values do occur.*

Hence, no new indices occur. Nevertheless, additional lattices emerge and the multiplicity of a given index will increase. We have seen that $c_{\varGamma}(m)$ is a multiplicative function, and by Theorem 3.4.9 this implies that any ordinary CSL can be written as the intersection $\varGamma(R) = \varGamma(R_1) \cap \ldots \cap \varGamma(R_n)$, where the indices $\varSigma_{\varGamma}(R_i)$ are powers of distinct primes. In this case, the MCSL $\varGamma(R_1) \cap \ldots \cap \varGamma(R_n)$ is equal to an ordinary CSL. However, if the indices of the $\varGamma(R_i)$ are not relatively prime, the corresponding MCSL $\varGamma(R_1) \cap \ldots \cap \varGamma(R_n)$ is, in general, not equal to an ordinary CSL.

More generally, the multiplicativity of $c_{\Gamma}(m)$ guarantees by Theorem 3.4.9 that any MCSL $\Gamma(R_1, \ldots, R_n)$ can be written as the intersection of MCSLs Γ_k of prime power index. Furthermore, the Γ_k can be chosen in such a way that they are intersections of at most n ordinary CSLs. Thus, we may restrict our analysis of MCSLs to those MCSLs, whose index is a prime power.

To become more concrete, we mention that the decomposition of CSLs into CSLs of prime power index corresponds to the prime factorisation in $\mathbb{J}$. In particular, if $|q|^2 = \pi_1^{\alpha_1} \cdot \ldots \cdot \pi_k^{\alpha_k}$ is the prime factorisation of $|q|^2$ in $\mathbb{N}$ and $p_i := \operatorname{gcld}(q, \pi_i^{\alpha_i})$, then the aforementioned decomposition is given by $\Gamma(R(q)) = \Gamma(R(p_1)) \cap \ldots \cap \Gamma(R(p_k))$. Note that q is a common right multiple of all p_i. Conversely, if p_i are primitive odd quaternions such that all $|p_i|^2$ are relatively prime, then any least common right multiple q is primitive and odd, and we have $\Gamma(R(q)) = \Gamma(R(p_1)) \cap \ldots \cap \Gamma(R(p_k))$. Likewise, if we define $p_{ij} = \operatorname{gcld}(q_i, \pi_j^{\alpha_{ij}})$, where the α_{ij} are the exponents in the prime factorisation $|q_i|^2 = \pi_1^{\alpha_{i1}} \cdot \ldots \cdot \pi_k^{\alpha_{jk}}$, then the corresponding decomposition of the MCSL reads $\Gamma(R(q_1), \ldots, R(q_n)) = \Gamma_1 \cap \ldots \cap \Gamma_k$ with $\Gamma_\ell = \Gamma(R(p_{1\ell})) \cap \ldots \cap \Gamma(R(p_{n\ell}))$.

Moreover, this guarantees the multiplicativity of the corresponding counting functions $c^{(\infty)}(m)$ and $c^{(k)}(m)$, where $c^{(\infty)}(m)$ is the number of all MCSLs of a given index m and $c^{(k)}(m)$ the corresponding number of all MCSLs that can be written as the intersection of at most k ordinary CSLs.

As we want to count all different MCSLs, an essential question is under which condition two MCSLs are equal. A preliminary result is the following one, which generalises Lemma 3.4.2 for the present situation.

LEMMA 6.1.2. *Let Γ be any cubic lattice and assume $\Gamma(R(q_1), \ldots, R(q_n)) = \Gamma(R(q_1'), \ldots, R(q_m'))$, where q_i and q_j' are primitive odd quaternions. Then*

$$\Sigma_{\Gamma}\left(R(q_1), \ldots, R(q_n)\right) = \Sigma_{\Gamma}\left(R(q_1'), \ldots, R(q_m')\right)$$

and

$$\operatorname{lcm}\left(|q_1|^2, \ldots, |q_n|^2\right) = \operatorname{lcm}\left(|q_1'|^2, \ldots, |q_n'|^2\right).$$

PROOF. The proof is similar to the proof of Lemma 3.4.2. Note that $\operatorname{lcm}(|q_1|^2, \ldots, |q_n|^2)$ is the least common multiple of all denominators $\operatorname{den}_{\Gamma}(R(q_i)) = \operatorname{den}_{\Gamma}(R(q_i)^{-1}) = |q_i|^2$. Let β be the smallest positive integer such that $\beta\Gamma \subseteq \Gamma(R(q_1), \ldots, R(q_n))$. Since $\beta\Gamma \subseteq \Gamma(R(q_i)) \subseteq R(q_i)\Gamma$ for all i, β must be a multiple of $\operatorname{den}_{\Gamma}(R(q_i)^{-1}) = |q_i|^2$ for all i. Hence, by definition, $\beta = \operatorname{lcm}(|q_1|^2, \ldots, |q_n|^2)$, and from $\Gamma(R(q_1), \ldots, R(q_n)) = \Gamma(R(q_1'), \ldots, R(q_m'))$ we infer $\operatorname{lcm}\left(|q_1|^2, \ldots, |q_n|^2\right) = \operatorname{lcm}\left(|q_1'|^2, \ldots, |q_n'|^2\right)$. □

The conditions of the lemma are necessary, but by no means sufficient. For ordinary CSLs we have the much stronger condition $q\mathbb{J} = q'\mathbb{J}$, and we expect additional conditions for MCSLs. Let us start with the case $n = 2$ first.

6.2. Intersection of two CSLs of the body-centred cubic lattice

As the body-centred cubic lattice $\varGamma = \varGamma_{bcc} = \mathrm{Im}(\mathbb{J})$ has the most convenient representation in terms of quaternions, we start with this lattice. The first step to determine all possible MCSLs $\varGamma(R_1, R_2)$ that can be written as the intersection of at most two ordinary CSLs is the calculation of their indices. We note that $\varGamma_+(R_1, R_2) := \varGamma(R_1) + \varGamma(R_2) = \mathrm{Im}(q_1\mathbb{J} + q_2\mathbb{J}) = \mathrm{Im}(q\mathbb{J})$, where q is the greatest common left divisor of q_1 and q_2. Hence, we have – recall that we may assume that $|q_i|^2$ is odd –

$$\varSigma(R_1, R_2) = \frac{|q_1|^2|q_2|^2}{|q|^2} \quad \text{with } q = \mathrm{gcld}(q_1, q_2). \tag{6.1}$$

In case that $|q_1|^2$ and $|q_2|^2$ are relatively prime, this reduces to $\varSigma(R_1, R_2) = |q_1|^2|q_2|^2$. This is the aforementioned case when the MCSL is equal to an ordinary CSL. Another special case is the case that q_1 is a left divisor of q_2. Here, we have $\varGamma(R_2) \subseteq \varGamma(R_1)$ and the MCSL $\varGamma(R_1, R_2) = \varGamma(R_2)$ is again an ordinary CSL. In order to understand the general situation, we start with the case that both $|q_i|^2$ are powers of the same prime $p \in \mathbb{N}$.

6.2.1. Intersection of two CSLs of prime power index.

Actually, confining our consideration to MCSLs of prime power index is no real restriction, as we can recover the general case from this one, as we have mentioned before. We are mainly interested in the case of two different CSLs, where none of them is a sublattice of the other one, i.e. neither q_1 nor q_2 is a right multiple of the other one. But we do not need to exclude the latter case explicitly, as all formulas include the case of ordinary CSLs implicitly.

Our first aim is to find an explicit expression for the MCSLs. We note that there is always a quaternion $r \in \mathbb{J}$ such that $q_1 r \bar{q}_2$ is a primitive quaternion, if q_1 and $\bar{q}_2$ are primitive odd quaternions. This follows from the unique prime factorisation in $\mathbb{J}$. In fact, we can even choose r to be a unit quaternion u – we just have to choose r such that q_1 and $q_2\bar{r}$ have no common right divisor.

Lemma 6.2.1. *Let q_i, $i = 1, 2$, be primitive quaternions such that $|q_i|^2 = p^{\alpha_i}$, where p is an odd prime. Choose r such that $q_1 r \bar{q}_2$ is a primitive quaternion and let q be a least common right multiple of q_1 and q_2. Then $\varGamma(R_1, R_2) = \varGamma(R(q_1)) \cap \varGamma(R(q_2)) = \mathrm{Im}(q\mathbb{J} + q_1 r \bar{q}_2 \mathbb{Z})$.*

Proof. Without loss of generality, we may assume $\alpha_1 \geq \alpha_2$. Let d denote a greatest common left divisor of q_1 and q_2. If $|d|^2 =: p^{\beta} = p^{\alpha_2}$, we can choose $d = q_2$ and $q = q_1$. Then, $\varGamma(R(q_1)) \subseteq \varGamma(R(q_2))$ and hence, $\varGamma(R_1, R_2) = \varGamma(R(q_1)) = \mathrm{Im}(q_1\mathbb{J}) = \mathrm{Im}(q\mathbb{J} + q_1 r \bar{q}_2 \mathbb{Z})$. Assume $|d|^2 = p^{\beta} < p^{\alpha_2}$ now, i.e. $d \neq q_i$. Thus, $\varSigma(R_1, R_2) = p^{\alpha_1+\alpha_2-\beta} > p^{\alpha_1}$. Clearly, d divides q, moreover, q can be chosen such that $q = p^{\alpha_2-\beta} d q'$ where $|q'|^2 = p^{\alpha_1-\alpha_2}$ and dq' is a primitive quaternion. Now $q\mathbb{J} \subseteq q_i\mathbb{J}$ implies $\mathrm{Im}(q\mathbb{J}) \subseteq \mathrm{Im}(q_1\mathbb{J}) \cap \mathrm{Im}(q_2\mathbb{J}) = \varGamma(R_1, R_2)$, where $\mathrm{Im}(q\mathbb{J})$ has index $p^{\alpha_1+2\alpha_2-2\beta}$ in $\varGamma$ and index $p^{\alpha_2-\beta}$ in $\varGamma(R_1, R_2)$. We choose r such that $q_1 r \bar{q}_2$ is a primitive quaternion. Then, $\mathrm{Im}(q_1 r \bar{q}_2) = -\mathrm{Im}(q_2 \bar{r} \bar{q}_1) \in \varGamma(R_1, R_2)$ is not divisible by p – otherwise $\mathrm{Re}(q_1 r \bar{q}_2)$ would be divisible by p as well and $q_1 r \bar{q}_2$ would not be primitive. Hence, the $p^{\alpha_2-\beta}$ cosets $k\,\mathrm{Im}(q_1 r \bar{q}_2) + \mathrm{Im}(q\mathbb{J})$, $k = 0, \ldots, p^{\alpha_2-\beta} - 1$ are all disjoint. Thus,

$\operatorname{Im}(q\mathbb{J} + q_1 r\bar{q}_2\mathbb{Z}) \subseteq \Gamma(R_1, R_2)$, and since both lattices have the same index in Γ, they must be equal. □

The r in the previous lemma is by no means unique. This means that we can represent $\Gamma(R_1, R_2)$ in different ways. Alternatively, we may write $\Gamma(R_1, R_2)$ as follows:

LEMMA 6.2.2. *Let q_i, $i = 1, 2$, be primitive quaternions such that $|q_i|^2 = p^{\alpha_i}$, where p is an odd prime, and let q be a least common right multiple of q_1 and q_2. Then we have $\Gamma(R_1, R_2) = \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2) = \operatorname{Im}(q\mathbb{J} + q_2\mathbb{J}\bar{q}_1)$.*

PROOF. From the previous lemma we conclude $\Gamma(R_1, R_2) = \operatorname{Im}(q\mathbb{J} + q_1 r\bar{q}_2\mathbb{Z}) \subseteq \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$. The converse inclusion $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2) \subseteq \Gamma(R_1, R_2)$ follows from $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2) \subseteq \operatorname{Im}(q_i\mathbb{J}) = \Gamma(R_i)$, $i = 1, 2$. □

Alternatively, we can prove this result without reference to Lemma 6.2.1 as follows.

PROOF NO. 2. We prove $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2) \subseteq \Gamma(R_1, R_2)$ as above. Hence, it remains to prove that every vector of $\Gamma(R_1, R_2)$ indeed can be written as $\operatorname{Im}(qm + q_1 n\bar{q}_2)$ for appropriate integer quaternions m and n. If $x \in \Gamma(R_1, R_2)$ there exist integer quaternions a, b such that $x = \operatorname{Im}(q_1 a) = \operatorname{Im}(q_2 b)$, i.e. there exist integers c, d such that $q_1 a = q_2 b + c\mathbf{e} = -\bar{b}\bar{q}_2 + d\mathbf{e}$, where $\mathbf{e} = (1, 0, 0, 0)$. Since q_2 is primitive, there exists an integer quaternion r such that $1 = \langle r, q_2\rangle = \frac{1}{2}(r\bar{q}_2 + q_2\bar{r})$. Thus, we have $2q_1 a = q_1 a r\bar{q}_2 + q_1 a q_2\bar{r}$. But the second term

$$q_1 a q_2 \bar{r} = (-\bar{b}\bar{q}_2 + d\mathbf{e})q_2\bar{r} = -|\bar{q}_2|^2\bar{b} + dq_2\bar{r}$$

is a right multiple of q_1 and q_2, and, hence, a multiple of q, i.e. $q_1 a q_2\bar{r} = qm$ for a suitable integer quaternion m. With $n := ar$ this proves the representation $2x = \operatorname{Im}(qm + q_1 n\bar{q}_2)$, i.e. $2x \in \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$. In addition, $|q|^2 x \in \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$, and since $|q|^2$ is odd we have $x \in \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$ for all $x \in \Gamma(R_1, R_2)$ and our claim follows. □

Note that $q\mathbb{J} + q_1\mathbb{J}\bar{q}_2$ is, in general, no ideal and, hence, $\Gamma(R_1, R_2)$ is neither an ordinary CSL nor a multiple of an ordinary CSL. Further, note that $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)/\operatorname{Im}(q\mathbb{J})$ is a cyclic group of order $\frac{|q|^2}{\max(|q_1|^2, |q_2|^2)}$ and that $\operatorname{Im}(q\mathbb{J})$ is a multiple of an ordinary CSL (q is not primitive here). The next lemma tells us under which conditions different pairs of CSLs give rise to different MCSLs:

THEOREM 6.2.3. *Let q_i be primitive quaternions with $|q_i|^2 = p^{\alpha_i}$, where p is a prime and $\alpha_1 \geq \alpha_2 \geq \alpha_4, \alpha_3 \geq \alpha_4$. Let q_{ij} with $|q_{ij}|^2 = p^{\alpha_{ij}}$ be the greatest common left divisor of q_i and q_j. If $\alpha_1 = \alpha_2$ let $\alpha_{13} \geq \alpha_{23}$. If $\alpha_3 = \alpha_4$ let $\alpha_{13} \geq \alpha_{14}$. Then $\Gamma(R_1) \cap \Gamma(R_2) = \Gamma(R_3) \cap \Gamma(R_4)$ if and only if $\alpha_1 = \alpha_3, \alpha_2 - \alpha_{12} = \alpha_4 - \alpha_{34}, \alpha_1 - \alpha_{13} \leq \min(\alpha_4 - \alpha_{34}, \alpha_{34})$ and $\alpha_4 - \alpha_{24} \leq \min(\alpha_4 - \alpha_{34}, \alpha_{34})$ are satisfied.*

Note that the ordering conditions on the α's do not put any restrictions on the validity of the theorem, since we can always interchange the role of the q_i such that these conditions are met.

REMARK 6.2.1. The two conditions $\alpha_1 = \alpha_3$ and $\alpha_2 - \alpha_{12} = \alpha_4 - \alpha_{34}$ correspond to the two conditions in Lemma 6.1.2. The first one means that the least common multiples of the denominators must be the same, and the second follows from the equality of the indices, which gives $\alpha_1 + \alpha_2 - \alpha_{12} = \alpha_3 + \alpha_4 - \alpha_{34}$. Furthermore, the condition $\alpha_1 - \alpha_{13} \leq \alpha_4 - \alpha_{34}$ can be easily understood by considering

$$\Gamma(R_1) \cap \Gamma(R_3) \supseteq \Gamma(R_1) \cap \Gamma(R_2) \cap \Gamma(R_3) \cap \Gamma(R_4) = \Gamma(R_3) \cap \Gamma(R_4).$$

Comparing the indices of the two sublattices gives $\alpha_1 + \alpha_3 - \alpha_{13} \leq \alpha_3 + \alpha_4 - \alpha_{34}$. Similarly, we get the condition $\alpha_4 - \alpha_{24} \leq \alpha_4 - \alpha_{34}$, where we have to apply $\alpha_2 \leq \alpha_1 = \alpha_3$ in addition.

PROOF. We have already proven part of the necessary conditions in the remark above. Nevertheless, we will prove them in a different way here, as they follow from a set of inequalities that we need anyway.

Recall that the content $\operatorname{cont}(q)$ of a quaternion $q \in \mathbb{J}$ is defined as the largest integer c such that $\frac{1}{c}q \in \mathbb{J}$. Now, let q be a greatest common right multiple of q_1 and q_2. We may choose $q = q_1 \operatorname{gcld}\left(\bar{q}_1, \frac{|q_2|^2}{|q_{12}|^2}\right)$ by our assumption $\alpha_1 \geq \alpha_2$. From this, we conclude $\operatorname{cont}(q) = p^{\alpha_2 - \alpha_{12}}$. Likewise, if q' is a greatest common right multiple of q_1 and q_2, then $\operatorname{cont}(q') = p^{\alpha_3 - \alpha_{34}}$.

A vector $\operatorname{Im}(x)$ is in $\Gamma(R_i) \cap \Gamma(R_j)$ if and only if $\operatorname{Im}(x) \in \Gamma(R_k)$ for $k = i, j$. This is equivalent to

$$R_k^{-1} \operatorname{Im}(x) = \operatorname{Im}\left(\frac{\bar{q}_k x q_k}{|q_k|^2}\right) \in \Gamma$$

for all $k = i, j$. Now, $R_k^{-1} \operatorname{Im}(x) \in \Gamma$ if and only if $|q_k|^2$ divides $\operatorname{cont}(\bar{q}_k x q_k)$. Next, by applying $\Gamma(R_1) \cap \Gamma(R_2) = \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$, we see that $\Gamma(R_1) \cap \Gamma(R_2) \subseteq \Gamma(R_3) \cap \Gamma(R_4)$ if and only if $|q_i|^2$ divides $\operatorname{cont}(\bar{q}_i q)$ and $\operatorname{cont}(\bar{q}_i q_1) \operatorname{cont}(\bar{q}_i q_2)$ for $i = 3, 4$. Analogous results hold for$\Gamma(R_3) \cap \Gamma(R_4) \subseteq \Gamma(R_1) \cap \Gamma(R_2)$. If we calculate the contents and take logarithms, we see that $\Gamma(R_1) \cap \Gamma(R_2) = \Gamma(R_3) \cap \Gamma(R_4)$ is equivalent to the following set of inequalities

$$\alpha_{13} + \alpha_{23} \geq \alpha_3 \leq \alpha_2 - \alpha_{12} + \min(\alpha_{13}, \alpha_1 - \alpha_2 + \alpha_{12}) \tag{6.2}$$

$$\alpha_{14} + \alpha_{24} \geq \alpha_4 \leq \alpha_2 - \alpha_{12} + \min(\alpha_{14}, \alpha_1 - \alpha_2 + \alpha_{12}) \tag{6.3}$$

$$\alpha_{13} + \alpha_{14} \geq \alpha_1 \leq \alpha_4 - \alpha_{34} + \min(\alpha_{13}, \alpha_3 - \alpha_4 + \alpha_{34}) \tag{6.4}$$

$$\alpha_{23} + \alpha_{24} \geq \alpha_2 \leq \alpha_4 - \alpha_{34} + \min(\alpha_{23}, \alpha_3 - \alpha_4 + \alpha_{34}). \tag{6.5}$$

As the α_{ij} correspond to the greatest common left divisors q_{ij}, they are not independent. In particular, $\alpha_{ij} > \alpha_{ik}$ implies $\alpha_{ik} = \alpha_{jk}$, whereas $\alpha_{ij} = \alpha_{ik}$ implies $\alpha_{jk} \geq \alpha_{ij} = \alpha_{ik}$. Under these restrictions and our assumptions on the α_i, the inequalities from above can be shown to be equivalent to the following set

$$\alpha_1 = \alpha_3 \tag{6.6}$$

$$\alpha_2 - \alpha_{12} = \alpha_4 - \alpha_{34} \tag{6.7}$$

$$\alpha_1 - \alpha_{13} \leq \min(\alpha_4 - \alpha_{34}, \alpha_{34}) \tag{6.8}$$

$$\alpha_4 - \alpha_{24} \leq \min(\alpha_4 - \alpha_{34}, \alpha_{34}), \tag{6.9}$$

which finishes the proof. □

We know now, in principle, under which conditions two MCSLs are equal. However, the theorem is not very intuitive and we should try to find a more accessible approach to understand it. It first tells us that q_1 and q_3 must have the same norm if $\Gamma(R_1, R_2) = \Gamma(R_3, R_4)$, but q_2 and q_4 may have different norm. However, write $q_2 = q_{12}q_2'$, i.e. decompose q_2 into a "common part" and a "different part", and do the analogous thing for $q_4 = q_{34}q_4'$. Then we see that the different parts q_2' and q_4', respectively, must have the same norm. At last the theorem tells us something about the difference of q_1 and q_3 and the difference between q_2 and q_4 (or q_2' and q_4'). In fact, they must not differ too much, i.e. the prime decompositions of q_1 and q_3 may differ only in the last $\min(\alpha_4 - \alpha_{34}, \alpha_{34})$ prime factors (read from the left). This guarantees that the least common right multiples $\operatorname{lcrm}(q_1, q_2)$ and $\operatorname{lcrm}(q_3, q_4)$ are the same.

For q_2 and q_4, the situation is a bit more involved, due to the fact that they do not need to have the same norm. To understand their situation better, we need some information on the greatest common divisors q_{ij}. We first observe $\alpha_{34} \leq \alpha_{24}$ due to $\alpha_4 - \alpha_{24} \leq \min(\alpha_4 - \alpha_{34}, \alpha_{34}) \leq \alpha_4 - \alpha_{34}$. Similarly we see $\alpha_{34} \leq \alpha_{13}$, where the equality sign holds if and only if $\alpha_1 = \alpha_2 = \alpha_4$. That means that q_{34} is a left divisor of both q_1 and q_2 and thus of q_{12}, resulting in $\alpha_{34} \leq \alpha_{12}$. Here, the equality sign holds if and only if $\alpha_2 = \alpha_4$. Thus, q_{34} is a left divisor of all q_i and, hence, it is the greatest common left divisor of the q_i, which implies $\alpha_{34} = \min(\alpha_{12}, \alpha_{13}, \alpha_{24})$. But this is only possible, if $\alpha_{24} = \alpha_{34}$ or $\alpha_2 = \alpha_4$.

Now, we have everything at hand to understand the relationship of q_2 and q_4 in more detail. Let us consider the case $\alpha_4 - \alpha_{34} > \alpha_{34}$ first. Then $\alpha_4 - \alpha_{24} \leq \alpha_{34} < \alpha_4 - \alpha_{34}$ gives $\alpha_{34} < \alpha_{24}$, which means that $\alpha_2 = \alpha_4$, i.e. q_2 and q_4 have the same norm and differ only in the last α_{34} prime factors (viewed from the left). If $\alpha_4 - \alpha_{34} \leq \alpha_{34}$ we have two possibilities: Either $\alpha_2 = \alpha_4$, i.e. q_2 and q_4 have again the same norm and differ only in the last $\alpha_4 - \alpha_{34}$ prime factors, or $\alpha_2 > \alpha_4$ and hence $\alpha_{24} = \alpha_{34}$, $\alpha_{12} > \alpha_{34}$ and $\alpha_{13} > \alpha_{34}$.

The latter case is of particular interest. Let (q_1, q_2) be any pair with $\alpha_1 \geq \alpha_2$. We construct a pair (q_3, q_4) as follows: we set $q_3 = q_1$ and choose q_4 such that its norm is equal to $p^{2(\alpha_2 - \alpha_{12})}$ and that the greatest common divisor of q_4 and $q_3 = q_1$ has norm $p^{\alpha_2 - \alpha_{12}}$ (such a choice is always possible). Then (q_3, q_4) generates the same MCSL as (q_1, q_2). Moreover, $\alpha_4 = 2\alpha_{34} = 2(\alpha_2 - \alpha_{12})$, which implies that q_4 has a certain minimality property: there is no pair (q_3, q_4) with $\alpha_4 < 2(\alpha_2 - \alpha_{12})$ that generates the same MCSL as (q_1, q_2).

Now, we can proceed to the calculation of the number $c^{(2)}(\Sigma)$ of different MCSLs with coincidence index Σ which are intersections of at most two ordinary CSLs. This task is equivalent to counting all pairs (q_1, q_2) that generate different MCSLs. From the previous paragraph, it is evident that we need to consider only pairs such that $\alpha_2 - \alpha_{12} \geq \alpha_{12}$. Now, we take into account that the MCSLs do not depend on the last α_{12} prime factors of q_i and that the first α_{12} prime factors of q_2 are the same as those of q_1. If we use the notation $\alpha := \alpha_1$, $\beta := \alpha_2$, $\gamma := \alpha_{12}$ and define $c^{(2)}(p, \alpha, \beta, \gamma)$ as the number of different MCSLs for given α, β, γ we obtain (recall that we assume $\alpha \geq \beta$)

$$c^{(2)}(p, \alpha, \beta, \gamma) = \begin{cases} (p+1)p^{\alpha-\gamma-1} & \text{if } \beta - \gamma = \gamma > 0 \\ (p^2-1)p^{\alpha+\beta-3\gamma-2} & \text{if } \alpha > \beta, \beta - \gamma > \gamma \geq 1 \\ \frac{1}{2}(p^2-1)p^{\alpha+\beta-3\gamma-2} & \text{if } \alpha = \beta, \beta - \gamma > \gamma \geq 1 \\ (p+1)p^{\alpha+\beta-1} & \text{if } \alpha > \beta > \gamma = 0 \\ \frac{1}{2}(p+1)p^{\alpha+\beta-1} & \text{if } \alpha = \beta > \gamma = 0 \\ (p+1)p^{\alpha-1} = f(p^\alpha) & \text{if } \alpha > \beta = \gamma = 0. \end{cases} \tag{6.10}$$

Note that the factor $\frac{1}{2}$ for $\alpha = \beta$ is due to the fact that interchanging the role of q_1 and q_2 does not give new MCSLs. The last equation just tells us that the MCSL reduces to an ordinary CSL in case of $\beta = 0$. If we sum all these values for fixed $\alpha + \beta - \gamma$ we get

Theorem 6.2.4. *Let p be an odd prime number. Then the number $c^{(2)}(p^r)$ of different MCSLs of index p^r that are an intersection of at most two ordinary CSLs is given by*

$$\begin{aligned} c^{(2)}(p^r) =& \frac{r+1}{2}(p+1)p^{r-1} + \left(\frac{r}{2} - 1\right)p^{r-2} - \left(\frac{r}{2} - \left[\frac{r}{2}\right]\right)p^{r-4} \\ &+ \frac{p^{r-1} - p^{r-2[r/3]-1}}{p^2-1} + \frac{p^{4[r/3]-r+2} - p^{4[r/2]-r-2}}{2(p^2-1)}, \end{aligned} \tag{6.11}$$

where $[x]$ is Gauss' symbol denoting the largest integer n such that $n \leq x$. □

Using the sums

$$\sum_{r=1}^{\infty}(r+1)p^r p^{-rs} = \frac{1}{(1-p^{1-s})^2} - 1 \tag{6.12}$$

$$\sum_{r=1}^{\infty}\left(\frac{r}{2} - \left[\frac{r}{2}\right]\right)p^r p^{-rs} = \frac{p^{1-s}}{2(1-p^{2-2s})} \tag{6.13}$$

$$\sum_{r=1}^{\infty} p^{r-2[r/3]}p^{-rs} = \frac{p^{1-s} + p^{2-2s} + p^{1-3s}}{1-p^{1-3s}} \tag{6.14}$$

$$\sum_{r=1}^{\infty} p^{4[r/3]-r}p^{-rs} = \frac{p^{-1-s} + p^{-2-2s} + p^{1-3s}}{1-p^{1-3s}} \tag{6.15}$$

$$\sum_{r=1}^{\infty} p^{4[r/2]-r}p^{-rs} = \frac{p^{-1-s} + p^{2-2s}}{1-p^{2-2s}} \tag{6.16}$$

we get the corresponding Euler factor for our generating function

$$\begin{aligned} \psi_2(p,s) :=& \sum_{r=1}^{\infty} \frac{c^{(2)}(p^r)}{p^{rs}} \\ =& 1 + \frac{(p+1)}{2p}\left(\frac{1}{(1-p^{1-s})^2} - 1\right) + \frac{(p+1)p^{-3s}}{2(1-p^{1-3s})}\left(\frac{1-p^{1-2s}}{(1-p^{1-s})^2} + 1\right) \end{aligned} \tag{6.17}$$

$$= \frac{(1+p^{-s})(1+p^{-3s})}{(1-p^{1-s})(1-p^{1-3s})} \times \left(1 + \frac{p^{-2s}(p^2+p)}{2(1+p^{-s})(1-p^{1-s})} - \frac{p^{-4s}(p+1)}{(1+p^{-s})(1-p^{1-s})(1+p^{-3s})}\right).$$

6.2.2. Intersection of two general CSLs. As we have seen in the beginning, $c^{(2)}$ is a multiplicative function. Thus, our results from above can be combined to give us the generating function for all MCSLs of the type $\Gamma(R_1) \cap \Gamma(R_2)$.

THEOREM 6.2.5. *Let $c^{(2)}(m)$ be the number of different MCSLs of index m that are an intersection of at most two ordinary CSLs. Then $c^{(2)}(\Sigma)$ is a multiplicative arithmetic function whose Dirichlet series is given by*

$$\begin{aligned}\Psi^{(2)}(s) := \sum_{n=1}^{\infty} \frac{c^{(2)}(n)}{n^s} &= \prod_{p\in\mathbb{P}\setminus\{2\}} \psi_2(p,s) = \frac{1-2^{1-3s}}{1+2^{-3s}} \frac{\zeta(3s-1)\zeta(3s)}{\zeta(6s)} \varphi^{(2)}(s)\Psi_{cub}(s)\\ &= \frac{(1-2^{1-s})(1-2^{1-3s})}{(1+2^{-s})(1+2^{-3s})} \frac{\zeta(s-1)\zeta(s)\zeta(3s-1)\zeta(3s)}{\zeta(2s)\zeta(6s)} \varphi^{(2)}(s)\\ &= 1 + \frac{4}{3^s} + \frac{6}{5^s} + \frac{8}{7^s} + \frac{18}{9^s} + \frac{12}{11^s} + \frac{14}{13^s} + \frac{24}{15^s} + \frac{18}{17^s} + \frac{20}{19^s} + \frac{32}{21^s} + \frac{24}{23^s} + \frac{45}{25^s} + \cdots,\end{aligned}$$

where $\psi_2(p,s)$ is given by Eq. (6.17) *and*

$$\varphi^{(2)}(s) = \prod_{p\in\mathbb{P}\setminus\{2\}} \left(1 + \frac{p^{-2s}(p^2+p)}{2(1+p^{-s})(1-p^{1-s})} - \frac{p^{-4s}(p+1)}{(1+p^{-s})(1-p^{1-s})(1+p^{-3s})}\right). \tag{6.18}$$

The explicit knowledge of $\Psi^{(2)}(s)$ allows us to find its analytic properties. We know from Section 3.5 that $\Psi_{cub}(s)$ is meromorphic function of s, whose right-most pole is located at $s = 2$. Furthermore, $\varphi^{(2)}(s)$ converges absolutely in the half plane $\{\mathrm{Re}(s) > \frac{3}{2}\}$, which guarantees its analyticity there.

Thus, $\Psi^{(2)}(s)$ is a meromorphic function in the half plane $\{\mathrm{Re}(s) > \frac{3}{2}\}$. Its rightmost pole is a simple located at $s = 2$ with residue

$$\rho^{(2)} := \mathrm{Res}_{s=2}\, \Psi^{(2)}(s) = \frac{124}{325} \frac{\zeta(2)\zeta(6)\zeta(5)}{\zeta(4)\zeta(12)} \varphi^{(2)}(2) = \frac{3866940}{691\pi^8} \zeta(5)\varphi^{(2)}(2) \approx 0.712983, \tag{6.19}$$

where we have used the explicit expressions

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945}, \qquad \zeta(12) = \frac{691\pi^{12}}{638512875}, \tag{6.20}$$

and the numerical values

$$\zeta(5) \approx 1.036928 \qquad \text{and} \qquad \varphi^{(2)}(2) \approx 1.165843. \tag{6.21}$$

This gives us to the following asymptotic behaviour of $c^{(2)}(m)$.

COROLLARY 6.2.6. *The asymptotic behaviour of the summatory function of $c^{(2)}(m)$ reads as follows*

$$\sum_{m\leq x} c^{(2)}(m) \sim \frac{\rho^{(2)}}{2} x^2 \approx 0.356491\, x^2 \quad \text{as } x \to \infty. \tag{6.22}$$

If we compare the asymptotic growth rates for ordinary CSLs and MCSLs, we see that the latter is not much bigger than the former. This shows that most MCSLs are ordinary CSLs. This behaviour is not surprising, since $c^{(2)}(m) = c(m)$ for square free indices m. Thus, all terms n^{-s} with n square free are missing in the expansion of $\Psi^{(2)}(s) - \Psi(s)$, whose first terms are given by

(6.23)
$$\Psi^{(2)}(s) - \Psi(s) = \frac{6}{9^s} + \frac{15}{25^s} + \frac{40}{27^s} + \frac{36}{45^s} + \frac{28}{49^s} + \frac{48}{63^s} + \frac{60}{75^s} + \frac{174}{81^s} + \frac{72}{99^s} + \frac{84}{117^s} + \cdots$$

For the determination of the counting function it was sufficient to have an explicit expression for $\Gamma(R_1, R_2)$ for prime power indices. Nevertheless, we can give an explicit expression for MCSLs with general index as well, which generalises Lemma 6.2.2

THEOREM 6.2.7. *Let q_i, $i = 1, 2$ be primitive odd quaternions and let q be their least common right multiple. Then $\Gamma(R(q_1), R(q_2)) = \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2) = \operatorname{Im}(q\mathbb{J} + q_2\mathbb{J}\bar{q}_1)$.*

PROOF. We can show the inclusion $\Gamma(R(q_1), R(q_2)) \supseteq \operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$ with the same arguments as in the proof of Lemma 6.2.2. The equality will follow if we show that both lattices have the same index in Γ. If d denotes the greatest common right divisor of q_1 and q_2, then $\Gamma(R(q_1), R(q_2))$ has index $\frac{|q_1|^2|q_2|^2}{|d|^2}$ in Γ by Eq. (6.1). Since $\operatorname{Im}(q\mathbb{J})$ has index $\operatorname{lcm}(|q_1|^2, |q_2|^2)(\frac{\gcd(|q_1|^2,|q_2|^2)}{|d|^2})^2$ it suffices to show that the order of $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)/\operatorname{Im}(q\mathbb{J})$ is a multiple of $\frac{\gcd(|q_1|^2,|q_2|^2)}{|d|^2}$. Note that q is a multiple of $\frac{\gcd(|q_1|^2,|q_2|^2)}{|d|^2}$, too, where the latter shall have the prime decomposition $\frac{\gcd(|q_1|^2,|q_2|^2)}{|d|^2} = p_1^{\delta_1} \cdots p_\ell^{\delta_\ell}$. Now, for each prime p_i there is a quaternion r_i such that $q_1 r_i \bar{q}_2$ and hence $\operatorname{Im}(q_1 r_i \bar{q}_2)$ is not divisible by p_i. But that implies that the cosets $n_i \operatorname{Im}(q_1 r_i \bar{q}_2) + \operatorname{Im}(q_1\mathbb{J})$ are all distinct for $0 \leq n_i < p_i^{\delta_i}$ i.e. the order of $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)/\operatorname{Im}(q\mathbb{J})$ is a multiple of $p_i^{\delta_i}$ for all i, from which the claim follows. □

6.3. Intersection of three CSLs of the body-centred cubic lattice

6.3.1. Intersection of three CSLs of prime power index. Our next step is to analyse MCSLs which are the intersection of three ordinary CSLs. It will turn out that any MCSL can be obtained by the intersection of at most three ordinary MCSLs. Again, it is sufficient to consider only MCSLs of prime power index.

First, we note that any MCSL $\Gamma(R_1, R_2, R_3)$ can be written as $\Gamma(R_1, R_2) \cap \Gamma(R_1, R_3)$, where we may assume, without loss of generality, $\Sigma(R_1) \geq \Sigma(R_i), i = 2, 3$. If we denote the least common right multiple of q_i, q_j by m_{ij}, then $\Gamma(R_1, R_2, R_3) = \operatorname{Im}(m_{12}\mathbb{J} + q_1\mathbb{J}\bar{q}_2) \cap \operatorname{Im}(m_{13}\mathbb{J} + q_1\mathbb{J}\bar{q}_3)$. In fact, we can show that taking the imaginary part Im commutes with the intersection, whence the analysis of the MCSLs can be reduced to the analysis of the corresponding quaternion modules.

Lemma 6.3.1. *Let q_i be odd primitive quaternions with prime power norm $|q_i|^2 = p^{\alpha_i}$, such that $|q_1|^2 \geq |q_i|^2$. Let m_{ij} be the least common right multiple of q_i, q_j. Then*

$$\varGamma(R(q_1), R(q_2), R(q_3)) = \operatorname{Im}\left((m_{12}\mathbb{J} + q_1\mathbb{J}\bar{q}_2) \cap (m_{13}\mathbb{J} + q_1\mathbb{J}\bar{q}_3)\right). \tag{6.24}$$

Proof. The inclusion

$$\varGamma(R(q_1), R(q_2), R(q_3)) \supseteq \operatorname{Im}\left((m_{12}\mathbb{J} + q_1\mathbb{J}\bar{q}_2) \cap (m_{13}\mathbb{J} + q_1\mathbb{J}\bar{q}_3)\right)$$

is immediate, so it remains to check the converse inclusion. Let $x \in \varGamma(R(q_1), R(q_2), R(q_3))$. Then there exist quaternions $y \in m_{12}\mathbb{J} + q_1\mathbb{J}\bar{q}_2$ and $z \in m_{13}\mathbb{J} + q_1\mathbb{J}\bar{q}_3$ such that $x = \operatorname{Im}(x) = \operatorname{Im}(y)$ and hence $x - y = n\mathbf{e}$ for some integer n. Now, q_1 divides both x and y and thus n must be a multiple of $|q_1|^2$. Since $|q_1|^2$ is a multiple of m_{13}, it is contained in $m_{13}\mathbb{J} + q_1\mathbb{J}\bar{q}_3$, hence, so is $x = y + n\mathbf{e}$, and the claim follows. □

Note that $m_{1i}\mathbb{J} + q_1\mathbb{J}\bar{q}_i$ can be written as $q_1(r_i\mathbb{J} + \mathbb{J}\bar{q}_i)$, where $\bar{r}_i$ is a right divisor of q_1 and satisfies $m_{1i} = q_1 r_i$. Thus the task of determining the MCSLs is reduced to analysing intersections of $\mathbb{Z}$–modules which are the sums of left and right ideals in $\mathbb{J}$. Hence, it is worthwhile to study these objects in more detail. We first consider their index in $\mathbb{J}$:

Lemma 6.3.2. *If a, b are primitive quaternions whose norm is a power of the same odd prime p, then the index of $a\mathbb{J} + \mathbb{J}b$ in $\mathbb{J}$ is given by $[\mathbb{J} : (a\mathbb{J} + \mathbb{J}b)] = \gcd(|a|^2, |b|^2) = \min(|a|^2, |b|^2)$.*

Proof. Without loss of generality, we may assume that $|a|^2$ divides $|b|^2$. Let c be a greatest common right divisor of $|a|^2$ and b. Then $|c|^2 = |a|^2$. Then $a\mathbb{J}+\mathbb{J}b = a\mathbb{J}+\mathbb{J}b+\mathbb{J}|a|^2 = a\mathbb{J}+\mathbb{J}c$ Thus, (a, c) is a primitive admissible pair in the sense of Chapter 4, and, hence, $a\mathbb{J}+\mathbb{J}c$ is a CSL of $\mathbb{J}$. This means that its index is given by $|a|^2 = \gcd(|a|^2, |b|^2)$ by Theorem 4.1.6 □

Actually, the proof shows even more. It gives us a sufficient condition for modules of the form $a\mathbb{J} + \mathbb{J}b$ to be equal, which we will need later on.

Corollary 6.3.3. *Let a, b, b' be primitive quaternions whose norm is a power of the same odd prime p and assume that the greatest common right divisor c of b and b' satisfies $|c|^2 \geq |a|^2$. Then $a\mathbb{J} + \mathbb{J}b = a\mathbb{J} + \mathbb{J}b' = a\mathbb{J} + \mathbb{J}c$. In particular, this holds true if $|b|^2 \geq |a|^2$ and b' is the greatest common right divisor of b and $|a|^2$.*

We will also need the following generalisation:

Lemma 6.3.4. *If a, b are primitive quaternions whose norm is a power of the same odd prime p with $|a|^2 \leq p^{\alpha}|b|^2$, $\alpha \in \mathbb{N}_0$, then the index of $a\mathbb{J} + p^{\alpha}\mathbb{J}b$ in $\mathbb{J}$ is given by $[\mathbb{J} : (a\mathbb{J} + \mathbb{J}b)] = |a|^2 \min(|a|^2, p^{\alpha})$.*

It follows immediately from the following more general version:

Lemma 6.3.5. *Let a and b be primitive quaternions whose norm is a power of the same odd prime p and let c be an arbitrary integer quaternion. Then $a\mathbb{J} + c\mathbb{J}b = a\mathbb{J} + d\mathbb{J}b$ and its index in $\mathbb{J}$ is given by $[\mathbb{J} : (a\mathbb{J} + c\mathbb{J}b)] = |d|^4 \min(\frac{|a|^2}{|d|^2}, |b|^2)$, where d is the greatest common left divisor of a and c.*

Proof. Let us write $a = da'$ and $c = dc'$. Then,

$$a\mathbb{J} + c\mathbb{J}b = d(a'\mathbb{J} + c'\mathbb{J}b) = d(a'\mathbb{J} + a'\mathbb{J}b + c'\mathbb{J}b) = d(a'\mathbb{J} + \mathbb{J}b) = a\mathbb{J} + d\mathbb{J}b, \tag{6.25}$$

since a' and c' have no common divisor. The statement about the index follows by applying Lemma 6.3.2 to the last expression but one in Eq. (6.25). □

Our next task is to determine intersections of modules $a\mathbb{J} + \mathbb{J}b$. For our purposes it is sufficient to consider the following special case:

Lemma 6.3.6. *Let a_i, b_i be primitive quaternions whose norm is a power of the same odd prime p such that $|a_i|^2 \leq |b_i|^2$ and assume that a_2 is a left divisor of a_1. Let c be the greatest common right divisor of b_1 and b_2. Then*

$$(a_1\mathbb{J} + \mathbb{J}b_1) \cap (a_2\mathbb{J} + \mathbb{J}b_2) = a_1\mathbb{J} + \frac{|a_2|^2}{|c|^2}\mathbb{J}b_1 \tag{6.26}$$

if $|c|^2 < |a_2|^2$ and

$$(a_1\mathbb{J} + \mathbb{J}b_1) \cap (a_2\mathbb{J} + \mathbb{J}b_2) = a_1\mathbb{J} + \mathbb{J}b_1 \tag{6.27}$$

if $|c|^2 \geq |a_2|^2$.

Proof. If $|c|^2 \geq |a_2|^2$, then applying Corollary 6.3.3 gives

$$a_2\mathbb{J} + \mathbb{J}b_2 = a_2\mathbb{J} + \mathbb{J}b_1 \supseteq a_1\mathbb{J} + \mathbb{J}b_1 \tag{6.28}$$

and the claim follows.

Let us assume $|c|^2 < |a_2|^2$ now. Clearly, $a_1\mathbb{J} + \mathbb{J}b_1 \supseteq a_1\mathbb{J} + \frac{|a_2|^2}{|c|^2}\mathbb{J}b_1$. If we denote the greatest common right divisor of b_2 and $|a_2|^2$ by d, then, by Corollary 6.3.3,

$$a_2\mathbb{J} + \mathbb{J}b_2 = a_2\mathbb{J} + \mathbb{J}d \supseteq a_2\mathbb{J} + \frac{|a_2|^2}{|c|^2}\mathbb{J}b_1 \supseteq a_1\mathbb{J} + \frac{|a_2|^2}{|c|^2}\mathbb{J}b_1, \tag{6.29}$$

since d is a right divisor of $\frac{|a_2|^2}{|c|^2}b_1$. Thus, $(a_1\mathbb{J} + \mathbb{J}b_1) \cap (a_2\mathbb{J} + \mathbb{J}b_2) \supseteq a_1\mathbb{J} + \frac{|a_2|^2}{|c|^2}\mathbb{J}b_1$ and we are done, if we can show that both expressions have the same index in $\mathbb{J}$. By Lemma 6.3.4, the index of the right hand side in $\mathbb{J}$ is given by $\frac{|a_1|^2|a_2|^2}{|c|^2}$. The index of the left hand side can be calculated by means of the second isomorphism theorem. Since $(a_1\mathbb{J} + \mathbb{J}b_1) + (a_2\mathbb{J} + \mathbb{J}b_2) = a_2\mathbb{J} + \mathbb{J}c$ has index $|c|^2$ in $\mathbb{J}$, the left hand side has index $\frac{|a_1|^2|a_2|^2}{|c|^2}$, too. □

We are now ready to formulate the solution of the coincidence problem:

THEOREM 6.3.7. *Let q_i be odd primitive quaternions with prime power norm $|q_i|^2 = p^{\alpha_i}$, such that $|q_1|^2 \geq |q_i|^2$. Let m_{ij} be the least common right multiple of q_i, q_j and let g_{ij} be their greatest common left divisor. Let $|m_{12}|^2 \geq |m_{13}|^2$. Then*

$$\Gamma(R(q_1), R(q_2), R(q_3)) = \operatorname{Im}\left(m_{12}\mathbb{J} + nq_1\mathbb{J}\bar{q}_2\right), \tag{6.30}$$

where $n = \max\left(\frac{|q_3|^2}{|g_{13}|^2|g_{23}|^2}, 1\right)$.

PROOF. Lemma 6.3.1 allows us to write

$$\Gamma(R(q_1), R(q_2), R(q_3)) = \operatorname{Im}\left(q_1\left[(r_2\mathbb{J} + \mathbb{J}\bar{q}_2) \cap (r_3\mathbb{J} + \mathbb{J}\bar{q}_3)\right]\right), \tag{6.31}$$

where the primitive quaternions r_i are defined by $m_{1i} = q_1 r_i$. Now, $|m_{12}|^2 \geq |m_{13}|^2$ implies that r_3 is a left divisor of r_2 (note that r_2 and r_3 both are left divisors of $\bar{q}_1$). Moreover, $|r_i|^2 \leq |q_i|^2$, so we can apply Lemma 6.3.6:

$$\begin{aligned}\Gamma(R(q_1), R(q_2), R(q_3)) &= \operatorname{Im}\left(q_1\left[(r_2\mathbb{J} + \mathbb{J}\bar{q}_2) \cap (r_3\mathbb{J} + \mathbb{J}\bar{q}_3)\right]\right)\\ &= \operatorname{Im}\left(q_1(r_2\mathbb{J} + n\mathbb{J}\bar{q}_2)\right) = \operatorname{Im}\left(m_{12}\mathbb{J} + nq_1\mathbb{J}\bar{q}_2\right),\end{aligned} \tag{6.32}$$

where $n = \max\left(\frac{|r_3|^2}{|g_{23}|^2}, 1\right) = \max\left(\frac{|q_3|^2}{|g_{13}|^2|g_{23}|^2}, 1\right)$. □

Note that the expression for the triple CSL is very similar to the expression for the double CSL. In fact, the only difference is that an additional factor n occurs. If $n = 1$ the triple CSL is just the intersection of two ordinary CSLs, since $\Gamma(R(q_1), R(q_2)) \subseteq \Gamma(R(q_1), R(q_3))$ in this case. But even if $n > 1$, the triple CSL is just a multiple of a double CSL, as we have the following result.

THEOREM 6.3.8. *Let Γ' be a sublattice of Γ of prime power index p^α in Γ. Then Γ' can be represented as the intersection of three ordinary CSLs $\Gamma' = \Gamma(R_1) \cap \Gamma(R_2) \cap \Gamma(R_3)$ if and only if there exists a $\beta \in \mathbb{N}_0$ and two coincidence rotations R_1' and R_2' such that $\Gamma' = p^\beta(\Gamma(R_1') \cap \Gamma(R_2'))$. The integer β is determined uniquely by Γ'.*

PROOF. Without loss of generality, we may assume that $R_i = R(q_i)$, where q_i, $i = 1, 2, 3$ are odd primitive quaternions with prime power norm $|q_i|^2 = p^{\alpha_i}$. Furthermore, we may assume $|q_1|^2 \geq |q_i|^2$ and, using the notation of the previous theorem, $|m_{12}|^2 \geq |m_{13}|^2$. If $n := \max\left(\frac{|q_3|^2}{|g_{13}|^2|g_{23}|^2}, 1\right) = 1$ then $\Gamma(R(q_1), R(q_2), R(q_3)) = \Gamma(R(q_1), R(q_2))$. Assume $n = p^\beta > 1$ now. Then p^β divides $|r_3|^2$, which, in turn, is a divisor of $|r_2|^2$. As r_2 is a left divisor of $\bar{q}_1$, this means that m_{12} is divisible by p^β and, hence, $m_{12}' := p^{-\beta}m_{12}$ is in $\mathbb{J}$. Define q_i' as the greatest common left divisor of q_i and m_{12}'. Then m_{12}' is the least common right multiple of q_1' and q_2'. Using Corollary 6.3.3 and Lemma 6.3.5, we infer

$$m_{12}\mathbb{J} + p^\beta q_1\mathbb{J}\bar{q}_2 = p^\beta\left(m_{12}'\mathbb{J} + q_1\mathbb{J}\bar{q}_2\right) = p^\beta\left(m_{12}'\mathbb{J} + q_1'\mathbb{J}\bar{q}_2'\right). \tag{6.33}$$

This shows

$$\Gamma(R(q_1), R(q_2), R(q_3)) = p^\beta \operatorname{Im}\left(m_{12}'\mathbb{J} + q_1'\mathbb{J}\bar{q}_2'\right) = p^\beta\Gamma(R(q_1'), R(q_2')),$$

which proves the first part of the theorem.

Conversely, we assume that $\mathit{\Gamma}' = p^{\beta}(\mathit{\Gamma}(R(q_1')) \cap \mathit{\Gamma}(R(q_2'))$ is given. We choose q_i $i = 1, 2, 3$ such that $|q_i|^2 = p^{\beta}|q_i'|^2$ and $\operatorname{gcld}(q_i, q_j') = \operatorname{gcld}(q_i', q_j')$, where $q_3' = 1$ (we note that such a choice is always possible, since we have $p + 1 > 2$ non-associate prime quaternions with norm p). Then $\mathit{\Gamma}' = \mathit{\Gamma}(R(q_1)) \cap \mathit{\Gamma}(R(q_2)) \cap \mathit{\Gamma}(R(q_3))$ as claimed. At last, the uniqueness of β is a consequence of the fact that no intersection of two ordinary CSLs is a sublattice of $p\mathit{\Gamma}$, i.e., β is the largest integer α such that $p^{-\alpha}\mathit{\Gamma}' \subseteq \mathit{\Gamma}$. □

Thus, we have established a one-to-one correspondence between intersections of three ordinary CSLs and multiples of intersections of two ordinary CSLs. We can now easily express $c^{(3)}(p^r)$ in terms of $c^{(2)}(p^r)$. We note that the index of $p^{\alpha}\mathit{\Gamma}(R_1, R_2)$ in $\mathit{\Gamma}$ is just $p^{3\alpha}$ times the index of $\mathit{\Gamma}(R_1, R_2)$ in $\mathit{\Gamma}$.

Corollary 6.3.9. *Let p be an odd prime number. Then*

$$c^{(3)}(p^r) = \sum_{0 \le n \le r/3} c^{(2)}(p^{r-3n}), \tag{6.34}$$

where $c^{(3)}(m)$ and $c^{(2)}(m)$ denote the number of MCSLs of index m that can be written as intersection of (up to) three and two ordinary CSLs, respectively.

6.3.2. General intersections of three CSLs. Since we know from our initial considerations that the multiplicity function $c^{(3)}$ is multiplicative, we can easily infer its generating function from Eq. (6.34).

Theorem 6.3.10. *Let $c^{(3)}(m)$ be the number of different MCSLs of index m that are an intersection of at most three ordinary CSLs. Then $c^{(3)}(m)$ is a multiplicative arithmetic function whose Dirichlet series is given by*

$$\begin{aligned}\Psi^{(3)}(s) := \sum_{n=1}^{\infty} \frac{c^{(3)}(n)}{n^s} &= (1 - 2^{-3s})\zeta(3s)\Psi^{(2)}(s)\\ &= 1 + \frac{4}{3^s} + \frac{6}{5^s} + \frac{8}{7^s} + \frac{18}{9^s} + \frac{12}{11^s} + \frac{14}{13^s} + \frac{24}{15^s} + \frac{18}{17^s} + \frac{20}{19^s} + \frac{32}{21^s} + \frac{24}{23^s} + \frac{45}{25^s} + \cdots,\end{aligned}$$

where $\Psi^{(2)}(s)$ is given by Theorem. (6.2.5).

Proof. This follows from Eq. (6.34) and multiplicativity by a standard calculation. We note that $c^{(3)}(m)$ is the Dirichlet convolution of $c^{(3)}(m)$ with the arithmetic function

$$\chi(m) = \begin{cases} 0 & \text{if } m \text{ is even} \\ 1 & \text{if } m \text{ is odd,} \end{cases}$$

whose Dirichlet series is given by $(1 - 2^{-3s})\zeta(3s)$. □

It follows immediately from the analytic properties of $\Psi^{(2)}(s)$ that $\Psi^{(3)}(s)$ is a meromorphic function in the half plane $\{\operatorname{Re}(s) > \frac{3}{2}\}$. Its rightmost pole is a simple located at $s = 2$

with residue

$$\begin{aligned}\rho^{(3)} := \operatorname{Res}_{s=2} \Psi^{(3)}(s) &= \frac{63}{64}\zeta(6)\rho^{(2)} = \frac{1953}{5200}\frac{\zeta(2)\zeta(6)^2\zeta(5)}{\zeta(4)\zeta(12)}\varphi^{(2)}(2) \\ &= \frac{64449}{11056\pi^2}\zeta(5)\varphi^{(2)}(2) \approx 0.714014,\end{aligned} \tag{6.35}$$

where we have used the values given in Eqs. (6.20) and (6.21).

A familiar argument involving Delange's theorem 7.A.1 gives us the following asymptotic behaviour.

Corollary 6.3.11. *The asymptotic behaviour of the summatory function of $c^{(3)}(m)$ reads as follows*

$$\sum_{m\leq x} c^{(3)}(m) = \frac{\rho^{(3)}}{2}x^2 \approx 0.357007\, x^2 \quad \textit{as } x \to \infty. \tag{6.36}$$

Comparing these results with Corollary 6.2.6, we see that the difference in the growth rate is much less than 1%. This small difference is not surprising as triple CSLs that are not double CSLs can occur only for indices that are divisible by p^3 for some odd p. In particular, the first such lattice occurs for the index $\varSigma = 27$. The fact that new MCSLs are rather rare is also illustrated by the first terms of the expansion

$$\begin{aligned}\Psi^{(3)}(s) - \Psi^{(2)}(s) &= \Psi^{(2)}(s)\Big((1-2^{-3s})\zeta(3s) - 1\Big) \\ &= \frac{1}{27^s} + \frac{4}{81^s} + \frac{1}{125^s} + \frac{6}{135^s} + \frac{8}{189^s} + \frac{18}{243^s} + \frac{12}{297^s} + \frac{1}{343^s} + \cdots .\end{aligned} \tag{6.37}$$

Here, all terms n^{-s} with n third power free are missing, which is just a reformulation of the fact that $c^{(3)}(n) = c^{(2)}(n)$ for these n.

Finally, let us mention that any triple CSL is just a multiple of a double CSL for general index m, as we have the following generalisation of Theorem 6.3.8.

Theorem 6.3.12. *Let R_i, $i = 1,2,3$ be coincidence rotations. Then there exist rotations R_i', $i = 1,2$ and an integer $n \in \mathbb{N}$ such that $\varGamma(R_1,R_2,R_3) = n\varGamma(R_1',R_2')$. Conversely, for any sublattice of the form $n\varGamma(R_1',R_2')$ there exist coincidence rotations R_i, $i = 1,2,3$ such that $\varGamma(R_1,R_2,R_3) = n\varGamma(R_1',R_2')$.*

Proof. Theorem 3.4.9 guarantees that we can decompose $\varGamma(R_1,R_2,R_3)$ into triple CSLs of prime power index. Now, we can apply Theorem 6.3.8 to these prime power CSLs to obtain multiples of double CSLs. Finally, we recombine the prime power CSLs by means of Theorem 3.4.9. Note that we have applied the fact that $n_1\varGamma_1 \cap n_2\varGamma_2 = n_1n_2(\varGamma_1 \cap \varGamma_2)$ if n_i and $[\varGamma : \varGamma_j]$ are coprime for $i \neq j$. Similarly, we can prove the converse statement. □

6.4. General MCSLs of the body-centred cubic lattices

So far, we have mainly discussed intersections of two and three ordinary CSLs. But in fact, this is no real restriction, since any MCSL can be represented as the intersection of three ordinary CSLs. From the considerations above this is not surprising since the intersections of three CSLs can be viewed, apart from a factor, as intersections of two CSLs.

In order to prove this statement we need two lemmas:

Lemma 6.4.1. *Let q be an odd primitive quaternion with prime power norm $|q|^2 = p^\alpha$ and assume that $2\operatorname{Im}(qr)$ is divisible by p^β. Then qr is divisible by $p^{\min(\alpha,\beta)}$.*

Proof. We write $2qr =: s = (s_0, s_1, s_2, s_3)$. We want to show that $p^\alpha | s_i$, for $i = 1, \dots, 3$ implies $p^{\min(\alpha,\beta)} | s_0$. Let p^γ be the maximal power that divides s_0 and let $\delta := \min(\beta, \gamma)$. Then q and p^δ divide s, and so does their least common right multiple m. Now, $|m|^2$ is divisible by $p^{\max(\alpha+\delta, 2\delta)}$ and hence so is $|s|^2$. Thus, $s_0^2 = |s|^2 - |2\operatorname{Im}(qr)|^2$ is divisible by $\min(p^{\max(\alpha+\delta,2\delta)}, p^{2\beta})$, which must divide $p^{2\gamma}$, since γ was chosen maximal. But this is only possible if either $\beta \leq \gamma$ or $\gamma = \delta \geq \alpha$ and the claim follows. □

Lemma 6.4.2. *Let $\Gamma(R)$ be a CSL with coincidence index p^β. Then there exists a coincidence rotation R' such that $p^\alpha \Gamma \cap \Gamma(R) = p^\alpha \Gamma(R')$.*

Proof. Without loss of generality, we may assume that $R = R(q)$ where q is an odd primitive quaternion. Then

$$p^\alpha \Gamma \cap \Gamma(R) = \operatorname{Im}(p^\alpha \mathbb{J}) \cap \operatorname{Im}(q\mathbb{J}) = \operatorname{Im}(p^\alpha \mathbb{J} \cap q\mathbb{J}), \tag{6.38}$$

where the last equation is a consequence of Lemma 6.4.1. Let $m = p^\alpha r$ be the least common right multiple of p^α and q. Then

$$p^\alpha \Gamma \cap \Gamma(R) = \operatorname{Im}(p^\alpha \mathbb{J} \cap q\mathbb{J}) = \operatorname{Im}(m\mathbb{J}) = p^\alpha \operatorname{Im}(r\mathbb{J}) = p^\alpha \Gamma(R(r)), \tag{6.39}$$

which finishes the proof. □

Theorem 6.4.3. *Let $R_1, \dots, R_n$ be a finite number of coincidence rotations. Then there exist coincidence rotations R_1', R_2', R_3' such that $\Gamma(R_1, \dots, R_n) = \Gamma(R_1', R_2', R_3')$.*

Proof. Obviously, it is sufficient to prove the claim for the case $n = 4$. Moreover, due to Theorem 3.4.9, we only need to consider MCSLs of prime power index. Now, we apply Theorem 6.3.8 and Lemma 6.4.2. They guarantee that there exist exponents α, β and and coincidence rotations R_i, R_i' such that

$$\begin{aligned} \Gamma(R_1, R_2, R_3, R_4) &\overset{6.3.8}{=} p^\alpha \Gamma(R_5, R_6) \cap \Gamma(R_4) = p^\alpha \Gamma(R_5, R_6) \cap (p^\alpha \Gamma \cap \Gamma(R_4)) \\ &\overset{6.4.2}{=} p^\alpha \Gamma(R_5, R_6) \cap p^\alpha \Gamma(R_7) \overset{6.3.8}{=} p^\alpha p^\beta \Gamma(R_8, R_9) \overset{6.3.8}{=} \Gamma(R_1', R_2', R_3'), \end{aligned} \tag{6.40}$$

which yields the claim. □

Thus, no new MCSLs emerge, if we consider intersections of more than three ordinary CSLs. Hence, the total number of MCSLs of given index m is given by $c^{(3)}(m)$ already, i.e. for all $n \geq 3$ we have $c^{(\infty)}(m) = c^{(n)}(m) = c^{(3)}(m)$. A similar phenomenon has been observed in two dimensions [**6**], where the set of MCSL stabilises already for $n = 2$.

6.5. Other cubic lattices

So far, we have only discussed the body centred cubic lattice. However, we know from the ordinary CSLs that all three types of cubic lattices have the same group of coincidence rotations, the same spectrum of indices and the same multiplicity function. In fact, this remains valid in the case of MCSLs, too. To see this, we need some general results about commensurate lattices, which generalise the corresponding results for ordinary CSLs of Chapter 3.

LEMMA 6.5.1. *Let $\varGamma_1 \subseteq \varGamma_2$ have index m in $\varGamma_2$. Then the indices $\varSigma_i$ of the MCSLs $\varGamma_i(R_1, \ldots, R_n)$ in $\varGamma_i$ satisfy $\varSigma_2 | m\varSigma_1$.*

PROOF. $\varGamma_1(R_1, \ldots, R_n) \subseteq \varGamma_2(R_1, \ldots, R_n) \subseteq \varGamma_2$ and $\varGamma_1(R_1, \ldots, R_n)$ has index $m\varSigma_1$ in $\varGamma_2$. □

In the following let $\varGamma_i$, $i = \{pc, bcc, fcc\}$ denote the primitive, body centred and face centred cubic lattices, respectively. Analogously $\varSigma_i(R_1, \ldots, R_n)$ denotes the indices of the MCSLs $\varGamma_i(R_1, \ldots, R_n)$ in their corresponding lattices $\varGamma_i$. Then we have at once:

THEOREM 6.5.2. *Let $R_1, \ldots, R_n$ be coincidence rotations. Then $\varSigma_{pc}(R_1, \ldots, R_n) = \varSigma_{bcc}(R_1, \ldots, R_n) = \varSigma_{fcc}(R_1, \ldots, R_n)$.*

PROOF. Clearly, $4\varGamma_{bcc} \overset{16}{\subset} 2\varGamma_{fcc} \overset{2}{\subset} \varGamma_{pc} \overset{2}{\subset} \varGamma_{bcc}$, where the superscripts indicate the relative indices. Hence, $\varSigma_i(R_1, \ldots, R_n)$ may only differ by a power of 2. But all indices must be odd by Proposition 6.1.1, so all three indices must be equal. □

Thus, we may drop the subscripts for the indices $\varSigma$. Moreover, this immediately implies the following result.

THEOREM 6.5.3. *All three cubic lattices share the same multiplicity functions $c(m)$, $c^{(2)}(m)$, and $c^{(\infty)}(m) = c^{(3)}(m)$.*

PROOF. Two MCSLs $\varGamma_i(R_1, \ldots, R_n)$ and $\varGamma_i(R'_1, \ldots, R'_m)$ are equal, if and only if the three indices $\varSigma(R_1, \ldots, R_n)$, $\varSigma(R'_1, \ldots, R'_m)$ and $\varSigma(R_1, \ldots, R_n, R'_1, \ldots, R'_m)$ are equal. But this implies that $\varGamma_i(R_1, \ldots, R_n) = \varGamma_i(R'_1, \ldots, R'_m)$ for all three types of cubic lattices or for none. Hence, the multiplicity function must be the same for all three types of cubic lattices. □

We have seen that there is an explicit expression for the MCSLs of the body centred cubic lattice in terms of submodules of the ring of Hurwitz quaternions. A similar expression is available for the primitive lattice. Recall that $\mathbb{L}$, the ring of Lipschitz quaternions, is a subring of index 2 in $\mathbb{J}$, and the same is valid for its projection onto the imaginary part, i.e. $\varGamma_{pc} = \mathbb{Z}^3 = \mathrm{Im}(\mathbb{L})$ is a sublattice of $\varGamma_{bcc} = \mathrm{Im}(\mathbb{J})$ with index 2. Similarly, if q_1 and q_2 are odd quaternions, then $q_1\mathbb{L}q_2$ has index 2 in $q_1\mathbb{J}q_2$ and the same holds for their projections $\mathrm{Im}(q_1\mathbb{L}q_2)$ and $\mathrm{Im}(q_1\mathbb{J}q_2)$. Thus, we expect the following result, where primitive means $\mathbb{J}$-primitive as usual.

THEOREM 6.5.4. *Let $q_i \in \mathbb{L}$, $i = 1, 2$ be primitive odd quaternions and let q be their least common right multiple. Then*

$$\Gamma_{pc}(R(q_1)) = \Gamma_{bcc}(R(q_1)) \cap \Gamma_{pc} = \operatorname{Im}(q_1\mathbb{L}) \tag{6.41}$$

$$\Gamma_{pc}(R(q_1), R(q_2)) = \Gamma_{bcc}(R(q_1), R(q_2)) \cap \Gamma_{pc} = \operatorname{Im}(q\mathbb{L} + q_1\mathbb{L}\bar{q}_2) = \operatorname{Im}(q\mathbb{L} + q_2\mathbb{L}\bar{q}_1). \tag{6.42}$$

Moreover,

$$\Gamma_{pc}(R_1, \ldots, R_n) = \Gamma_{bcc}(R_1, \ldots, R_n) \cap \Gamma_{pc}. \tag{6.43}$$

PROOF. First, observe $\Gamma_{pc}(R) \subset \Gamma_{bcc}(R)$ with index 2. Moreover, $\Gamma_{bcc}(R) \cap \Gamma_{pc} \subset \Gamma_{bcc}(R)$ has index 2 as well. This gives $\Gamma_{pc}(R) = \Gamma_{bcc}(R) \cap \Gamma_{pc}$. By induction, we see $\Gamma_{pc}(R_1, \ldots, R_n) = \Gamma_{bcc}(R_1, \ldots, R_n) \cap \Gamma_{pc}$ for arbitrary n. Now, $\operatorname{Im}(q_1\mathbb{L})$ has index 2 in $\operatorname{Im}(q_1\mathbb{J})$, as mentioned above. The same is true for all the sublattices $\operatorname{Im}(q_1\mathbb{L}) \subseteq \operatorname{Im}(q_1\mathbb{J}) \cap \operatorname{Im}(\mathbb{L}) = \Gamma_{bcc}(R(q_1)) \cap \Gamma_{pc}$, hence $\Gamma_{pc}(R(q_1)) = \operatorname{Im}(q_1\mathbb{J})$ as well.

Analogously, the second statement follows, once we have checked that $\operatorname{Im}(q\mathbb{L} + q_1\mathbb{L}\bar{q}_2)$ has index 2 in $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$. In fact, it is sufficient to check that the index of $\operatorname{Im}(q\mathbb{L} + q_1\mathbb{L}\bar{q}_2)$ in $\operatorname{Im}(q\mathbb{J} + q_1\mathbb{J}\bar{q}_2)$ is at most 2, and the latter follows immediately, if we have shown that $q\mathbb{L} + q_1\mathbb{L}\bar{q}_2$ has index 2 in $q\mathbb{J} + q_1\mathbb{J}\bar{q}_2$. Clearly, we have $\mathbb{J} = \mathbb{L} \cup (r + \mathbb{L})$, where $r \in \mathbb{J} \setminus \mathbb{L}$. In particular, r may be chosen as $r_1 = \frac{1}{2}(1,1,1,1)\bar{q}_2$ or $r_2 = \frac{1}{2}q_3(1,1,1,1)$, where q_3 is uniquely defined by $q = q_1 q_3$. Now, $qr_1 \pm q_1 r_2 \bar{q}_2 = (\frac{1}{2} \pm \frac{1}{2})q(1,1,1,1)\bar{q}_2 \in q\mathbb{L}$ implies

$$q\mathbb{J} + q_1\mathbb{J}\bar{q}_2 = \bigcup_{n_1,n_2=0}^{1} \left[q(n_1 r_1 + \mathbb{L}) + q_1(n_2 r_2 + \mathbb{L})\bar{q}_2\right] = \bigcup_{n_1=0}^{1} \left[n_1 q r_1 + q\mathbb{L} + q_1\mathbb{L}\bar{q}_2\right], \tag{6.44}$$

which, indeed, proves that $q\mathbb{L} + q_1\mathbb{L}\bar{q}_2 \subset q\mathbb{J} + q_1\mathbb{J}\bar{q}_2$ has index 2. □

Although we do not have similar expressions for Γ_{fcc}, we still have the following theorem,

THEOREM 6.5.5. *The CSLs of Γ_{fcc} satisfy the following equations*

$$\Gamma_{fcc}(R) = \Gamma_{bcc}(R) \cap \Gamma_{fcc} \tag{6.45}$$

$$\Gamma_{fcc}(R_1, \ldots, R_n) = \Gamma_{bcc}(R_1, \ldots, R_n) \cap \Gamma_{fcc}. \tag{6.46}$$

PROOF. First, we note that $\Gamma_{fcc} \subset \Gamma_{pc}$ has index 2 in Γ_{pc} and contains exactly those vectors of Γ_{pc} whose square of the (3-dimensional) norm is even. Now, $\Gamma_{pc}(R) \cap \Gamma_{fcc} = R\Gamma_{pc} \cap \Gamma_{fcc} = R\Gamma_{fcc} \cap \Gamma_{fcc} = \Gamma_{fcc}(R)$, since R preserves the norm. Using the previous theorem, we see immediately $\Gamma_{fcc}(R) = \Gamma_{bcc}(R) \cap \Gamma_{fcc}$. The second statement follows by induction. □

6.6. Triple Junctions

Finally, let us mention an application to crystallography. One object crystallographers are interested in are so-called triple junctions [**29, 30, 31**]. Roughly speaking, triple junctions are three crystal grains meeting in a straight line. This means that there are three pairs of grains sharing a common plane (grain boundary) and, thus, giving rise to three simple CSLs, and a double CSL, which is the intersection of the former. In our terms, the latter is an MCSL

$\mathit{\Gamma}\cap R_1\mathit{\Gamma}\cap R_2\mathit{\Gamma}$, whereas the former are the simple CSLs $\mathit{\Gamma}\cap R_1\mathit{\Gamma}$, $\mathit{\Gamma}\cap R_2\mathit{\Gamma}$ and $R_1\mathit{\Gamma}\cap R_2\mathit{\Gamma}$, respectively. An important question is the relation of the indices of these lattices.

Let us denote the indices of the simple CSLs by $\mathit{\Sigma}_1 := \mathit{\Sigma}(R_1)$, $\mathit{\Sigma}_2 := \mathit{\Sigma}(R_2)$ and $\mathit{\Sigma}_3 := \mathit{\Sigma}(R_3)$, where $R_3 := R_1^{-1}R_2$. Let q_1 and q_2 be the quaternions generating R_1 and R_2, respectively. Then R_3 is generated by $\bar{q}_1q_2$, which is in general not a primitive quaternion. The corresponding primitive quaternion reads $q_3 := \frac{\bar{q}_1q_2}{|q_{12}|^2}$, where we have used the definition $q_{12} = \mathrm{gcld}(q_1,q_2)$. Hence, we can immediately reproduce Gertsman's result [**30**] for the index $\mathit{\Sigma}_3 = \frac{\mathit{\Sigma}_1\mathit{\Sigma}_2}{\mathit{\Sigma}_{12}^2}$, where $\mathit{\Sigma}_{12} := \mathit{\Sigma}(R(q_{12}))$ is the index corresponding to the rotation $R(q_{12})$. On the other hand, we know from Eqs. (3.20) and (6.1) that

$$\mathit{\Sigma}(R_1,R_2) = \frac{\mathit{\Sigma}_1\mathit{\Sigma}_2}{\mathit{\Sigma}_{12}} = \mathit{\Sigma}_{12}\mathit{\Sigma}_3. \tag{6.47}$$

Now, we define $q_1' := q_{12}^{-1}q_1$ and $q_2' := q_{12}^{-1}q_2$. Then we may write

$$q_1 = q_{12}q_1' \qquad\qquad q_2 = q_{12}q_2' \qquad\qquad q_3 = \bar{q}_1'q_2' \tag{6.48}$$

and correspondingly, we may decompose the rotations R_1, R_2, R_3 into the "basic" constituents $R_{12} := R(q_{12})$, $R_1' := R(q_1')$ and $R_2' := R(q_2')$. We note that the corresponding indices are multiplicative

$$\mathit{\Sigma}(R_1) = \mathit{\Sigma}(R_{12})\mathit{\Sigma}(R_1'), \qquad \mathit{\Sigma}(R_2) = \mathit{\Sigma}(R_{12})\mathit{\Sigma}(R_2'), \qquad \mathit{\Sigma}(R_3) = \mathit{\Sigma}(R_1')\mathit{\Sigma}(R_2'). \tag{6.49}$$

Furthermore, we see $\bar{q}_1' = \mathrm{gcld}(\bar{q}_1,q_3) =: q_{13}$ and $\bar{q}_2' = \mathrm{gcld}(\bar{q}_2,\bar{q}_3) =: q_{23}$ and thus Eq. (6.48) may be written in a more symmetrical way

$$q_1 = q_{12}\bar{q}_{13} = \frac{q_2\bar{q}_3}{|q_{23}|^2} \qquad q_2 = q_{12}\bar{q}_{23} = \frac{q_1q_3}{|q_{13}|^2} \qquad q_3 = \bar{q}_{13}\bar{q}_{23} = \frac{\bar{q}_1q_2}{|q_{12}|^2}. \tag{6.50}$$

If we define the corresponding indices in the intuitive way, we see that $\mathit{\Sigma}(R_1,R_2)$ can be written as

$$\mathit{\Sigma}(R_1,R_2) = \frac{\mathit{\Sigma}_1\mathit{\Sigma}_2}{\mathit{\Sigma}_{12}} = \frac{\mathit{\Sigma}_1\mathit{\Sigma}_3}{\mathit{\Sigma}_{13}} = \frac{\mathit{\Sigma}_2\mathit{\Sigma}_3}{\mathit{\Sigma}_{23}} = \mathit{\Sigma}_{12}\mathit{\Sigma}_3 = \mathit{\Sigma}_{13}\mathit{\Sigma}_2 = \mathit{\Sigma}_{23}\mathit{\Sigma}_1 \tag{6.51}$$

$$= \mathit{\Sigma}_{12}\mathit{\Sigma}_{13}\mathit{\Sigma}_{23} = \mathit{\Sigma}_{12}\mathit{\Sigma}_1'\mathit{\Sigma}_2' = (\mathit{\Sigma}_1\mathit{\Sigma}_2\mathit{\Sigma}_3)^{1/2}. \tag{6.52}$$

The last expression has been proved by different methods in [**30**]. Note that we can express $\mathit{\Sigma}(R_1,R_2)$ either in terms of the simple indices $\mathit{\Sigma}_1, \mathit{\Sigma}_2, \mathit{\Sigma}_3$ or in terms of the "reduced" indices $\mathit{\Sigma}_{12}, \mathit{\Sigma}_{13}, \mathit{\Sigma}_{23}$, which describe somehow the "common" part of R_1, R_2 and R_3. Note that R_{12}, R_{13}, R_{23} contain the complete information of the triple junction. In particular, we can write $\mathit{\Gamma}(R_1,R_2)$ as $\mathit{\Gamma}(R_1,R_2) = R_{12}(R_{12}^{-1}\mathit{\Gamma}\cap R_{13}^{-1}\mathit{\Gamma}\cap R_{23}^{-1}\mathit{\Gamma})$.

Bibliography

1. E. Akhtarkavan and M.F.M. Salleh, *Multiple description lattice vector quantization using Coinciding Similar Lattices of A_4*, Proc. IEEE Symposium on Industrial Electronics and Applications, 2010, pp. 716–721.
2. E. Akhtarkavan and M.F.M. Salleh, *Multiple description lattice vector quantization using multiple A_4 quantizers*, IEICE Electron. Express **7** (2010), 1233–1239.
3. ______, *Multiple descriptions coinciding lattice vector quantizer for wavelet image coding*, IEEE Transactions on Image Processing **21** (2012), 653–661.
4. M. Baake, *Solution of the coincidence problem in dimensions $d \leq 4$*, The Mathematics of Long-Range Aperiodic Order (Dordrecht) (R. V. Moody, ed.), Kluwer, 1997, Rev. version: `arXiv:math.MG/0605222`, pp. 9–44.
5. M. Baake and U. Grimm, *Bravais colourings of planar modules with N–fold symmetry*, Z. Kristallogr. **219** (2004), 72–80, `math.CO/0301021`.
6. ______, *Multiple planar coincidences with N–fold symmetry*, Z. Kristallogr. **221** (2006), 571–581, `arXiv:math.MG/0511306`.
7. ______, *Aperiodic Order. vol. 1: A Mathematical Invitation*, Cambridge University Press, Cambridge, 2013.
8. M. Baake, M. Heuer, U. Grimm, and P. Zeiner, *Coincidence rotations of the root lattice A_4*, Europ. J. Combinatorics **29** (2008), 1808–1819, `arXiv:0709.1341`.
9. M. Baake, M. Heuer, and R.V. Moody, *Similar sublattices of the root lattice A_4*, J. Algebra **320** (2008), 1391–1408, `arXiv:math/0702448`.
10. M. Baake and R.V. Moody, *Similarity submodules and root systems in four dimensions*, Canad. J. Math. **51** (1999), 1258–1276, `arXiv:math/9904028`.
11. M. Baake, P.A.B. Pleasants, and U. Rehmann, *Coincidence site modules in 3–space*, Discr. Comput. Geom. **38** (2007), 111–138, `arXiv:math/0609793`.
12. M. Baake, R. Scharlau, and P. Zeiner, *Similar sublattices of planar lattices*, Canad. J. Math. **63** (2011), 1220–1237, arXiv:0908.2558v1 [math.MG].
13. ______, *Well-rounded sublattices of planar lattices*, Acta Arithmetica **166.4** (2014), 301–334, `arXiv:1311.6306 [math.NT]`.
14. M. Baake and P. Zeiner, *Geometric enumeration problems for lattices and embedded $\mathbb{Z}$-modules*, to appear in *Aperiodic Order. Vol. 2: Crystallography and Almost Periodicity* (M. Baake and U. Grimm, ed.).
15. ______, *Multiple coincidences in dimensions $d \leq 3$*, Phil. Mag. **87** (2007), 2869–2876.
16. ______, *Coincidences in 4 dimensions*, Phil. Mag. **88** (2008), 2025–2032, `arXiv:0712.0363v1[math.MG]`.
17. G. L. Bleris and P. Delavignette, *A new formulation for the generation of coincidence site lattices (CSL's) in the cubic system*, Acta Cryst. **A37** (1981), 779–786.
18. W. Bollmann, *Crystal defects and crystalline interfaces*, Springer, Berlin, 1970.
19. ______, *Crystal lattices, interfaces, matrices*, published by the author, Geneva, 1982.
20. L. Chen, R.V. Moody, and J. Patera, *Non-crystallographic root systems*, Quasicrystals and Discrete Geometry (Providence, RI) (J. Patera, ed.), AMS, 1998, pp. 135–178.
21. H. Cohen, *A course in computational algebraic number theory*, 4. print. ed., Springer, Berlin, 2000.

22. J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices, and groups*, 3rd ed., Fundamental Principles of Mathematical Sciences, vol. 290, Springer, New York, 1999.
23. J.H. Conway and D.A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A.K. Peters, Ltd., Wellesley, Massachusetts, 2003.
24. S.N. Diggavi, N.J.A. Sloane, and Vinay A. Vaishampayan, *Asymmetric multiple description lattice vector quantizers*, IEEE Transactions Information Theory **48** (2002), 174–191.
25. P. du Val, *Homographies, quaternions and rotations*, Clarendon Press, Oxford, 1964.
26. H.F. Fischmeister, *Structure and properties of high angle grain boundaries*, J. Phys. Colloques **46** (1985), C4–3–C4–23.
27. J. Freiberger, *Koinzidenzgitter von Rechteckgittern*, Diploma thesis (in German), 2008.
28. G. Friedel, *Leçons de Cristallographie*, Blanchard, Paris, 1911.
29. V.Y. Gertsman, *Coincidence site lattice theory of multicrystalline ensembles*, Acta Cryst. **A57** (2001), 649–655.
30. ______, *Geometrical theory of triple junctions of CSL boundaries*, Acta Cryst. **A57** (2001), 369–377.
31. ______, *On the auxiliary lattices and dislocation reactions at triple junctions*, Acta Cryst. **A58** (2002), 155–161.
32. H. Gleiter and B. Chalmers, *High-angle grain boundaries*, Progress in Materials Science vol. 16 (Oxford), Pergamon Press, 1972, pp. 1–12.
33. S. Glied, *Similarity and coincidence isometries for modules*, Can. Math. Bull. **55** (2011), 98–107.
34. S. Glied and M. Baake, *Similarity versus coincidence rotations of lattices*, Z. Krist. **223** (2008), 770–772, `arXiv:0808.0109`.
35. H. Grimmer, *Coincidence rotations for cubic lattices*, Scripta Met. **7** (1973), 1295–1300.
36. ______, *Disorientations and coincidence rotations for cubic lattices*, Acta Cryst. **A 30** (1974), 685–688.
37. ______, *The generating function for coincidence site lattices in the cubic system*, Acta Cryst. **A 40** (1984), 108–112.
38. ______, *Systematic Determination of Coincidence Orientations for all Hexagonal Lattices with Axial Ratio c/a in a Given Interval*, Acta Cryst. **A 45** (1989), 320–325.
39. H. Grimmer, W. Bollmann, and D. H. Warrington, *Coincidence-site lattices and complete pattern-shift lattices in cubic crystals*, Acta Cryst. **A 30** (1974), 197–207.
40. H. Grimmer and D. H. Warrington, *Fundamentals for the Description of Hexagonal Lattices in General and in Coincidence Orientation*, Acta Cryst. A **43** (1987), 232–243.
41. G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University, Oxford, 2008.
42. M. Heuer, *Combinatorial Aspects of Root Lattices and Words*, Ph.D. thesis, The Open University, Milton Keynes, UK, 2010.
43. M. Heuer and P. Zeiner, *CSLs of the root lattice A_4*, J. Phys.: Conf. Ser. **226** (2010), 012024.
44. C. Huck, *A note on coincidence isometries of modules in Euclidean space*, Z. Kristallogr. **224** (2009), 341–344.
45. A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Springer, Berlin, 1919.
46. E.M. Rains J.H. Conway and N.J.A. Sloane, *On the existence of similar sublattices*, Can. J. Math. **51** (1999), 1300–1306.
47. M. Koecher and R. Remmert, *Hamilton's quaternions*, Numbers (Berlin) (H.-D. Ebbinghaus et al., eds.), Springer, 1991, pp. 189–220.
48. M.L. Kronberg and F.H. Wilson, *Secondary recrystallization in copper*, Trans. A.I.M.E. **185** (1949), 501–14.
49. M. J. Loquias and P. Zeiner, *Coincidence isometries of a shifted square lattice*, J. Phys.: Conf. Ser. **226** (2010), 012026, `arXiv:1002.0519v1 [math.MG]`.

50. M.J. Loquias, *Coincidences and Colorings of Lattices and $\mathbb{Z}$–modules*, Ph.D. thesis, University of Bielefeld, Bielefeld, Germany, 2010.
51. M.J. Loquias and P. Zeiner, *Colourings of lattices and coincidence site lattices*, Phil. Mag. **91** (2011), 2680–2689, `arXiv:1011.1001v1 [math.MG]`.
52. ______, *The coincidence problem for shifted lattices and crystallographic point packings*, Acta Cryst. A **70** (2014), 656–669, `arXiv:1301.3689 [math.MG]`.
53. ______, *Coincidence indices of sublattices and coincidences of colorings*, 2015, `arXiv:1506.00028 [math.MG]`.
54. R. V. Moody and J. Patera, *Quasicrystals and icosians*, J. Phys. A **26** (1993), 2829–2853.
55. P.A.B. Pleasants, M. Baake, and J. Roth, *Planar coincidences for N–fold symmetry*, J. Math. Phys. **37** (1996), 1029–1058, rev. version: `arXiv:math/0511147`.
56. O. Radulescu, *An elementary approach to the crystallography of twins in icosahedral quasicrystals*, J. Phys. I (France) **5** (1995), 719–728.
57. O. Radulescu and D.H. Warrington, *Arithmetic properties of module directions in quasicrystals, coincidence modules and coincidence quasilattices*, Acta Cryst. A **51** (1995), 335–343.
58. S. Ranganathan, *On the Geometry of Coincidence–Site Lattices*, Acta Cryst. **21** (1966), 197–199.
59. ______, *Coincidence-site lattices, superlattices and quasicrystals*, Trans. Indian Inst. Met. **43** (1990), 1–7.
60. I. Reiner, *Maximal orders*, Clarendon Press, Oxford, 2006.
61. M.A. Rodríguez, J.L. Aragón, and L. Verde-Star, *Clifford algebra approach to the coincidence problem for planar lattices*, Acta Cryst. A **61** (2005), 173–184.
62. M.A. Rodríguez-Andrade, G. Aragón-González, J.L. Aragón, and A. Gómez-Rodríguez, *Coincidence lattices in the hyperbolic plane*, Acta Cryst. A **67** (2011), 35–44.
63. R. Scharlau, *Unimodular lattices over real quadratic fields*, Math. Z. **216** (1994), 437–452.
64. D. Shechtman, I. Blech, D. Gratias, and J. W. Cahn, *Metallic phase with long–range orientational order and no translational symmetry*, Phys. Rev. Lett. **53** (1984), 1951–1953.
65. N.J.A. Sloane and B. Beferull-Lozano, *Quantizing using lattice intersections*, Discrete and Computational Geometry (Berlin) (B. Aronov, S. Basu, J. Pach, and M. Sharir, eds.), Springer, 2003, math.CO/0207147, pp. 799–824.
66. M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Mathematics, Springer, Berlin, 1980.
67. D.H. Warrington, *Coincidence site lattices in quasicrystal tilings*, Mat. Science Forum **126-128** (1993), 57–60.
68. D.H. Warrington and R. Lück, *The use of the Wieringa roof to examine coincidence site quasilattices in quasicrystals*, Proc. Intl. Conf. on Aperiodic Crystals (Les Diablerets) (Singapore) (G. Chapuis and W. Paciorek, eds.), World Scientific, 1994, pp. 30–34.
69. ______, *Healing of slip planes and interfaces in quasiperiodic patterns*, Ferroelectrics **250** (2001), 357–360.
70. L.C. Washington, *Introduction to cyclotomic fields*, 2 ed., Springer, New York, 1997.
71. P. Zeiner, *Supplement to "well-rounded sublattices of planar lattices"*, `arXiv:1311.6306 [math.NT]`.
72. P. Zeiner, *Remarks on CSLs for cubic and hypercubic lattices*, Group Theoretical Methods in Physics (IoP Conf. Series 185) (Bristol), 2005, pp. 569–573.
73. ______, *Symmetries of coincidence site lattices of cubic lattices*, Z. Kristallogr. **220** (2005), 915–925, `arXiv:math/0605525`.
74. ______, *Coincidences of hypercubic lattices in 4 dimensions*, Z. Kristallogr. **221** (2006), 105–114, `arXiv:math/0605526`.
75. ______, *Multiple CSLs for the body centered cubic lattice*, J. Phys.: Conf. Ser. **30** (2006), 163–167, `arXiv:math/0605521`.
76. ______, *Multiplicativity in the theory of coincidence site lattices*, J. Phys.: Conf. Ser. **226** (2010), 012025.

77. ______, *Well-rounded sublattices and coincidence site lattices*, Aperiodic Crystals (Dordrecht), Springer, 2013, `arXiv:1210.0571 [math.MG]`, pp. 43–48.

78. ______, *Similar submodules and coincidence site modules*, Acta Physica Polonica **126** (2014), 641–645, `arXiv:1402.5013`.

79. Y.M. Zou, *Indices of coincidence isometries of the hypercubic lattice $\mathbb{Z}^n$*, Acta Cryst. **A 62** (2006), 454–458.

80. ______, *Structures of coincidence symmetry groups*, Acta Cryst. **A 62** (2006), 109–114.

CHAPTER 7

Well-rounded sublattices of planar lattices

ABSTRACT. A lattice in Euclidean d-space is called well-rounded if it contains d linearly independent vectors of minimal length. This class of lattices is important for various questions, including sphere packing or homology computations. The task of enumerating well-rounded sublattices of a given lattice is of interest already in dimension 2, and has recently been treated by several authors. In this paper, we analyse the question more closely in the spirit of earlier work on similar sublattices and coincidence site sublattices. Combining explicit geometric considerations with known techniques from the theory of Dirichlet series, we arrive, after a considerable amount of computation, at asymptotic results on the number of well-rounded sublattices up to a given index in any planar lattice. For the two most symmetric lattices, the square and the hexagonal lattice, we present detailed results.

7.1. Introduction

A lattice in Euclidean space $\mathbb{R}^d$ is *well-rounded* if the non-zero lattice vectors of minimal length span $\mathbb{R}^d$. Well-rounded lattices are interesting for several reasons. First of all, the concept is put into a broader context by the notion of the *successive minima* of a lattice (more precisely, of a norm function on a lattice). By definition, a lattice is well-rounded if and only if all its d successive minima (norms of successively shortest linearly independent vectors) are equal to each other.

A first observation is that many important 'named' lattices in higher-dimensional space are well-rounded, such as the Leech lattice, the Barnes-Wall lattice(s), the Coxeter-Todd lattice, all irreducible root lattices, and many more [**10**]. There are essentially two reasons for this (which often apply both). First of all, distinct successive minima give rise to proper subspaces of $\mathbb{R}^d$ that are invariant under the orthogonal group (automorphism group) of the lattice. If this finite group acts irreducibly on $\mathbb{R}^d$, the lattice must be well-rounded. Secondly, a lattice which gives rise to a locally densest sphere packing (a so-called extreme lattice), is well-rounded. It is actually perfect by Voronoi's famous theorem (this part goes back to Korkine and Zolotareff), and it is easily seen that perfection implies well-roundedness; compare [**21**].

However, these two observations are not at the core of the notion. They might give the impression that well-rounded lattices are very rare or special, which is not the case. In terms of Gram matrices or quadratic forms, the well-rounded ones lie in a subspace of codimension $d-1$ in the space of all symmetric matrices, similarly for the cone of positive definite Minkowski-reduced forms. Despite its codimension, this subspace is large enough so that certain questions about general forms can be reduced to well-rounded ones. A good illustration for this is Minkowski's proof of the fact that the geometric mean of all d successive minima of a lattice is bounded by the same quantity $\gamma_d \cdot \bigl(\mathrm{disc}(\Lambda)\bigr)^{\frac{1}{d}}$ as the first minimum (see Section 7.2). Here, γ_d is the Hermite constant in dimension d, and for well-rounded lattices this estimate reduces to the definition of this constant. The proof is obtained by a certain deformation of the quadratic form; see [**29**]. A sharpened version of this technique asks for a diagonal matrix which transforms a given lattice into a well-rounded one. In general, its existence is unknown, but C. McMullen [**22**] recently proved a weaker version which suffices for applications to Minkowski's conjecture on the minimum of a (multiplicative) norm function on lattices. The method of proof is related to applications of well-rounded lattices to cohomology questions as described in the introduction of [**18**]; compare the references given there.

Having this kind of 'richness' of well-rounded lattices in mind, it is tempting to ask how frequent they are in terms of counting sublattices. So, the principal object of study in this paper is the function

$$a_{\Gamma}(n) \;:=\; \mathrm{card}\{\Lambda \mid \Lambda \subseteq \Gamma \text{ is a well-rounded sublattice with } [\Gamma : \Lambda] = n\}, \tag{7.1}$$

where Γ is an in principle arbitrary lattice, and $[\Gamma : \Lambda]$ denotes the index of Λ in Γ. This question is of interest already in dimension 2 (where some of the general features described above reduce to rather obvious facts). Moreover, since the well-rounded sublattices are the objects of interest, and not so much the enveloping 'lattice of reference' Γ, it seems natural to focus mainly on the two most symmetric lattices, the hexagonal lattice and the square lattice. In this paper, we shall obtain complete and explicit results on the asymptotic number of well-rounded sublattices, as a function of the index, of the hexagonal lattice and of the square lattice. We also have results for general Γ which are somewhat weaker, which seems to be unavoidable.

In special situations, lattice enumeration problems have a long history. The coefficients of the Dedekind zeta functions of an algebraic number field K of degree d over the rationals count the number of ideals of given index in the ring of integers $\mathbb{Z}_K$, which is considered as a lattice in a well-known way [**7**]. The perhaps most basic result on lattice enumeration, which is also one of the most frequently rediscovered ones, is the determination of the number $g(n)$ of all distinct sublattices of index n in a given lattice $\Gamma \subset \mathbb{R}^d$. The result follows easily from the Hermite normal form for integral matrices and reads

$$g_d(n) \;=\; g(n) \;=\; \sum_{m_1 \cdot \ldots \cdot m_d = n} m_1^0 \cdot m_2^1 \cdots m_d^{d-1} \tag{7.2}$$

with Dirichlet series generating function

$$D_g(s) \;=\; \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \;=\; \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1) \tag{7.3}$$

(compare [**26**, p. 64], [**27**, p. 307], [**20, 2**]; for several different proofs, see [**20**, Theorem 15.1]). This result of Eq. (7.2) is insensitive to any geometric property of the lattice Γ, in the sense that it is actually a result for the free Abelian group of rank d and its subgroups. In [**11, 15**], extensions to more general classes of finitely generated groups are treated.

As for lattices, it is natural to refine the question by looking at classes of sublattices with particular properties (number-theoretic or geometric), possibly defined by an additional structure on the enveloping vector space. In addition to the classical case of the Dedekind zeta function mentioned above, we are aware of only few, scattered results. Quite a while ago, in [**27, 9**], modules in an order in a semisimple algebra over a number field were considered. Well-rounded lattices in dimension 2 have recently been analysed in [**12, 13, 14, 18**]; see also the references in [**14**]. Together with our earlier work on similar sublattices [**4, 6**] and on coincidence site sublattices (CSLs) [**2, 31, 5, 33**], these papers were our starting point.

One benefit of Dirichlet series is the access to asymptotic results on the growth of a (non-negative) arithmetical function $f(n)$. Since f in general need not behave regularly, in particular need not be monotone, one usually considers the average growth of $f(n)$, that is, one studies the summatory function $F(x) = \sum_{n\leq x} f(n)$. For the above counting function $g_d(n)$ for sublattices, the summatory function $G_d(x)$ satisfies

$$G_d(x) \; = \; cx^d + \Delta_d(x), \tag{7.4}$$

with $c = 1$ for $d = 1$ and $c = \frac{1}{d}\prod_{\ell=2}^{d} \zeta(\ell)$ otherwise, which follows from Eq. (7.3) by applying Delange's theorem; compare Theorem 7.A.1 in Appendix 7.A. Clearly, $G_1(x) = [x]$, where $[\cdot]$ denotes the Gauss bracket, and thus $\Delta_1(x) = \mathcal{O}(1)$. In dimension 2, $G_2 = \sigma_1(n) := \sum_{\ell | n} \ell$, so we have the well-known asymptotic growth behaviour of the divisor function, whose error term can be estimated as $\Delta_2(x) = \mathcal{O}\bigl(x \log(x)\bigr)$; see [**1**, Thm 3.4].

One can ask for a more refined description of the asymptotic growth of an arithmetic function, consisting of a main term for the summatory function, a term of second order (a 'first order error term'), and an error term of a strictly smaller order of magnitude than the term of second order. For instance, for the number of divisors of n, it is known that

$$\sum_{n\leq x} \sigma_0(n) \; = \; x\log(x) + (2\gamma - 1)x + \mathcal{O}\bigl(\sqrt{x}\bigr), \tag{7.5}$$

where γ is the Euler–Mascheroni constant; compare [**1, 28**]. So we have a term of second order which is linear in this case and thus of 'almost the same' growth as the main term, whereas the error term is much smaller.

The content of this paper can now be summarised as follows. In the short preparatory Section 7.2, we recall a few facts about reduced bases and Bravais classes of lattices in the plane, and state some auxiliary remarks about well-rounded (sub-)lattices.

In Section 7.3, we begin with an explicit description of all well-rounded sublattices of the square lattice, the latter viewed as the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers. After these preparations, the main result then is Theorem 7.3.2, which gives a refined asymptotic description of the function $A_{\square}$, of the kind that we have explained above for the divisor function in Eq. (7.5); the constants for the main term and the term of second order are determined explicitly. The proof relies on classic methods from analytic number theory, including Delange's theorem and some elementary tools around Euler's summation formula and Dirichlet's hyperbola method. We describe the strategy and the main steps of the proof; some of the details, which are long and technical, have been transferred to a supplement to this paper. A weaker result, namely the explicit asymptotics without the second-order term, is stated in Theorem 7.3.1, which is fully proved here.

Section 7.4 provides the analogous analysis for the hexagonal lattice, realised as the ring of Eisenstein integers $\mathbb{Z}[\rho]$ with $\rho = e^{2\pi \mathrm{i}/3}$; Theorems 7.4.1 and 7.4.2 are completely analogous to Theorems 7.3.1 and 7.3.2.

The general case of well-rounded sublattices of two-dimensional case is treated in Section 7.5, which is subdivided into two parts. The first one starts with a criterion for the existence of well-rounded sublattices. The lattices that have a well-rounded sublattice include all 'rational' lattices, that is, lattices whose Gram matrix consists of rational numbers (or even rational integers), up to a common multiple. So these are exactly the lattices that correspond to integral quadratic forms in the classical sense. There is an interesting connection between well-rounded sublattices and CSLs, which is established in Lemma 7.5.1. In the rest of this part, it is shown in Theorem 7.5.8 that all non-rational lattices that contain well-rounded sublattices have essentially the same power-law growth (linear) of their average number $A_\Gamma(x)$. The second part of Section 7.5 deals with the behaviour of $A_\Gamma(x)$ in the general rational case. The discussion is more complicated, but nevertheless we can show that the growth rate is proportional to $x \log(x)$, as in the square and hexagonal case. Summarising, we see that three regimes exist as follows: A planar lattice can have many, some or no well-rounded sublattices, the first case is exactly the rational case, while the second case is explained by the existence of an essentially unique coincidence reflection.

Our paper is complemented by four appendices. In Appendix 7.A, some classic results about Dirichlet series are collected in a way that suits our needs. In Appendix 7.B, we explicitly record the asymptotic behaviour of the number of similar sublattices of the square and the hexagonal lattice, which are a useful by-product of Sections 7.3 and 7.4. Appendix 7.C summarises key properties of a special type of sublattices that we need, while Appendix 7.D recalls some facts about Epstein's zeta functions.

7.2. Tools from the geometry of planar lattices

Let us collect some simple, but useful facts from the geometric theory of lattices. We assume throughout this paper that we are in dimension $d = 2$, so we consider an arbitrary lattice $\varLambda$ in the Euclidean plane. Let $v \in \varLambda$ be a shortest non-zero vector, and $w \in \varLambda$ shortest among the lattice vectors linearly independent from v. Then v, w form a basis of $\varLambda$. (The reader may consult [**7**, Chapter 2, §7.7] for this and for related statements below.) Changing the sign of w if necessary, we may assume that the inner product satisfies $(v, w) \geq 0$. A basis of this kind is called a *reduced basis* of $\varLambda$. By definition, we have the following chain of inequalities,

$$|v| \leq |w| \leq |v-w| \leq |v+w| \,. \tag{7.6}$$

In terms of the quantities $a := |v|^2, c := |w|^2$, and $b := (v,w)$, which are the entries of the Gram matrix $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with respect to v, w, these conditions read

$$0 \leq 2b \leq a \leq c. \tag{7.7}$$

Conversely, if we start with any two linearly independent vectors v, w satisfying Eqs. (7.6) or (7.7), then v, w form a reduced basis of the lattice that they generate. Concerning the reduction conditions (7.6), there are six cases possible for the pair v, w as follows,

(a)	$\lvert v\rvert < \lvert w\rvert < \lvert v-w\rvert < \lvert v+w\rvert \,,$	$(v,w) > 0$	general type
(b)	$\lvert v\rvert < \lvert w\rvert < \lvert v-w\rvert = \lvert v+w\rvert \,,$	$(v,w) = 0$	rectangular type
(c)	$\lvert v\rvert < \lvert w\rvert = \lvert v-w\rvert < \lvert v+w\rvert \,,$	$(v,w) > 0$	centred rectangular type
(d)	$\lvert v\rvert = \lvert w\rvert < \lvert v-w\rvert < \lvert v+w\rvert \,,$	$(v,w) > 0$	rhombic type
(e)	$\lvert v\rvert = \lvert w\rvert < \lvert v-w\rvert = \lvert v+w\rvert \,,$	$(v,w) = 0$	square type
(f)	$\lvert v\rvert = \lvert w\rvert = \lvert v-w\rvert < \lvert v+w\rvert \,,$	$(v,w) > 0$	hexagonal type

It is well-known and easily shown that the entries a, b, c of the Gram matrix with respect to a reduced basis v, w, only depend on the lattice, but not on the choice of the reduced basis v, w. Therefore, it is well-defined to talk about the *geometric type* of the lattice, which is one of the types (a) to (f) above. As a further consequence of this uniqueness property, the orthogonal group $\mathrm{O}(\varLambda)$ acts transitively (and thus sharply transitively) on the set of all (ordered) reduced bases of $\varLambda$. (By definition, $\mathrm{O}(\varLambda)$ is the set of orthogonal transformations of the enveloping vector space which maps the lattice into, and thus onto itself.) $\mathrm{O}(\varLambda)$ is cyclic of order 2 for lattices of general type, a dihedral group of order 4 (generated by two perpendicular reflections) for the types (b), (c) and (d), a dihedral group of order 8 for the square lattice, and of order 12 for the hexagonal lattice.

Typically, one wants to classify lattices only up to similarity, which means that the Gram matrix may be multiplied with a positive constant. Clearly, a square or hexagonal lattice is unique up to similarity. Similarity classes of rhombic type depend on one parameter, the angle α formed by v and w, where $\pi/3 < \alpha < \pi/2$. The limiting cases $\alpha = \pi/3$ and $\alpha = \pi/2$ lead to the hexagonal, respectively square lattice.

A lattice $\varLambda$ (in any dimension) is called *rational* if its similarity class contains a lattice with rational Gram matrix. The *discriminant* $\mathrm{disc}(\varLambda)$ of a lattice $\varLambda$ is the determinant of any of its Gram matrices. (This is the square of the volume of a fundamental domain for the action of $\varLambda$ by translations.)

Two lattices $\varGamma, \varLambda$ (on the same space) are called *commensurate* (or commensurable) if their intersection $\varGamma \cap \varLambda$ has finite index in both. Equivalently, there exists a non-zero integer a such that $a\varGamma \subseteq \varLambda \subseteq a^{-1}\varGamma$. This in turn is equivalent to the condition that $\varGamma$ and $\varLambda$

generate the same space over the rationals, $\mathbb{Q}\varGamma = \mathbb{Q}\varLambda$. If $\varGamma$ and $\varLambda$ are commensurate, the ratio of their discriminants is a rational square.

A *coincidence isometry* for $\varLambda$ is an isometry (an orthogonal transformation R of the underlying real space) such that $\varLambda$ and $R\varLambda$ are commensurate. In earlier work [**2**], we have introduced the notation $\mathrm{OC}(\varLambda)$ for the set of all coincidence isometries for $\varLambda$. If $R \in \mathrm{OC}(\varLambda)$, it follows that $R\mathbb{Q}\varLambda = \mathbb{Q}R\varLambda = \mathbb{Q}\varLambda$ (see above), i.e. R induces an orthogonal transformation of the rational space $\mathbb{Q}\varLambda$. Conversely, any such orthogonal transformation maps $\varLambda$ onto a lattice of full rank in the same rational space, which, by the above remarks, is commensurate with $\varLambda$. Altogether, $\mathrm{OC}(\varLambda)$ is equal to the rational orthogonal group $\mathrm{O}(\mathbb{Q}\varLambda)$ (in particular, it is a group). If $\varGamma$ and $\varLambda$ are commensurate, their groups of coincidence isometries coincide,

$$\mathrm{OC}(\varGamma) = \mathrm{O}(\mathbb{Q}\varGamma) = \mathrm{O}(\mathbb{Q}\varLambda) = \mathrm{OC}(\varLambda).$$

A *coincidence site lattice* (CSL) for $\varLambda$ is a sublattice of the form $\varLambda \cap R\varLambda$ with $R \in \mathrm{OC}(\varLambda)$; see [**2**] for further motivation concerning this notion.

Geometric types as introduced above are closely related, but not identical, with the so-called *Bravais types* of lattices, which are defined in any dimension. Two lattices $\varGamma$ and $\varLambda$ are Bravais equivalent if and only if there exists a linear transformation which maps $\varGamma$ onto $\varLambda$ and also conjugates $\mathrm{O}(\varGamma)$ into $\mathrm{O}(\varLambda)$. The Bravais type (or Bravais class) of a lattice depends only on its geometric type; the centred rectangular and the rhombic lattices belong to the same Bravais type (thus we call them rhombic-cr lattices). Otherwise, geometric types and Bravais types (or rather the respective equivalence classes of lattices) coincide.

Let us return to well-rounded lattices. Clearly, a planar lattice is well-rounded if and only if it is of rhombic, square or hexagonal type. Any rhombic-cr lattice contains a rectangular sublattice of index 2. In fact, if v and w form a reduced basis, then $v - w$ and $v + w$ are orthogonal, and form a reduced basis of the desired sublattice. Conversely, if v, w is a reduced basis of a rectangular lattice, and if we further assume that $|w^2| = c < 3a = 3|v|^2$, then $v + w$ and $-v + w$ form a reduced basis of a rhombic sublattice of index 2. (If $c = 3a$, this sublattice is hexagonal, whereas for $c > 3a$, we have $|2v| < | \pm v + w|$, and thus the vectors are not shortest any more; in this case, the sublattice is centred rectangular.)

Similarly, a hexagonal lattice contains a rectangular sublattice of index 2, or more precisely, it contains exactly three rectangular sublattices of index 2 for symmetry reasons. Analogously, the square lattice contains precisely one square sublattice of index 2.

7.3. Well-rounded sublattices of $\mathbb{Z}[\mathrm{i}]$

We use the Gaussian integers as a representation of the square lattice. Note that there is no hexagonal sublattice of $\mathbb{Z}[\mathrm{i}]$ (consider the discriminant). Hence, all well-rounded sublattices are either rhombic or square lattices, which we treat separately, in line with the geometric classification explained above.

A fundamental quantity that will appear frequently below is the Dirichlet series generating function for the number of similar sublattices of $\mathbb{Z}[\mathrm{i}]$, compare [**4, 6**], which is equal to the

Dedekind zeta function of the quadratic field $\mathbb{Q}(\mathrm{i})$,

$$\Phi_{\square}(s) \;=\; \zeta_{\mathbb{Q}(\mathrm{i})}(s) \;=\; \zeta(s)L(s,\chi_{-4})\,. \tag{7.8}$$

Here, $\zeta(s)$ is Riemann's zeta function, and $L(s,\chi_{-4})$ is the L-series corresponding to the Dirichlet character χ_{-4} defined by

$$\chi_{-4}(n) \;=\; \begin{cases} 0, & \text{if } n \text{ is even,} \\ 1, & \text{if } n \equiv 1 \bmod 4, \\ -1, & \text{if } n \equiv 3 \bmod 4; \end{cases}$$

see [**2, 6, 30**] and Appendix 7.A.

Before dealing with the well-rounded sublattices, let us consider all rhombic-cr and square sublattices of $\mathbb{Z}[\mathrm{i}]$ (recall that the term 'rhombic-cr' means rhombic or centred rectangular). Let $z_1, z_2 \in \mathbb{Z}[\mathrm{i}]$ be any two elements of equal norm. The sublattice $\varGamma = \langle z_1, z_2\rangle_{\mathbb{Z}}$ is of rhombic or centred rectangular or square type, and every rhombic-cr or square sublattice is obtained in this way (see Section 2). We can write $z_1 + z_2$ and $z_1 - z_2$ as $z_1 + z_2 = pz$ and $z_1 - z_2 = \mathrm{i}qz$ where p, q are integers and z is primitive, which means that $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ are relatively prime. W.l.o.g., we may assume that p and q are positive (interchange z_1 and z_2 if necessary). Thus $\varGamma = \langle z_1, z_2\rangle_{\mathbb{Z}} = \langle \frac{p+\mathrm{i}q}{2}z, \frac{p-\mathrm{i}q}{2}z\rangle_{\mathbb{Z}}$ is a sublattice of $\mathbb{Z}[\mathrm{i}]$ of index $\frac{1}{2}pq|z|^2$. The lattice $\varGamma$ is a square lattice if and only if $p = q$. Determining the number of rhombic-cr and square sublattices is thus equivalent to finding all rectangular and square sublattices of $\mathbb{Z}[\mathrm{i}]$ with the additional constraint that $(p + q\mathrm{i})z$ is divisible by 2.

We distinguish two cases (note that z is primitive, hence, in particular, not divisible by 2, and thus p and q must have the same parity), which we call 'rectangular' and 'rhombic case' for reasons that will become clear later.

(1) 'rectangular' case: z is not divisible by $1 + \mathrm{i}$, hence p and q must be even. We write $p = 2p', q = 2q'$. The index is even since it is given by $2p'q'|z|^2$. Note that p', q' may take any positive integral value, even or odd.

(2) 'rhombic' case: z is divisible by $1 + \mathrm{i}$. We write $z = (1 + \mathrm{i})w$.
   (a) If p and q are both even, we again write $p = 2p', q = 2q'$. The index is divisible by 4 since it is given by $4p'q'|w|^2$. Note that p', q' may take any positive integral value, even or odd.
   (b) If p and q are both odd, the index is odd and given by $pq|w|^2$.

For fixed z, interchanging $p \neq q$ gives a rhombic-cr (and rectangular) lattice which is rotated through an angle $\frac{\pi}{2}$, hence we count no lattice twice if we let p, q run over all positive integers.

Let $\Phi_{\text{even}}(s)$ be the Dirichlet series for the number of rhombic-cr and square sublattices of even index. This comprises the cases (1) and (2a). As p', q' run over all positive integers, they each contribute a factor of $\zeta(s)$, and since z is primitive, this gives the factor $\Phi^{\mathsf{pr}}_{\square}(s)$, where $\Phi^{\mathsf{pr}}_{\square}(s)$ is the Dirichlet series generating function of primitive similar sublattices of $\mathbb{Z}[\mathrm{i}]$. The additional factor of 2 in the index formula gives a contribution of 2^{-s}, and combining all these factors finally yields

$$\Phi_{\text{even}}(s) \;=\; \frac{1}{2^s}\,\zeta(s)^2\,\Phi^{\mathsf{pr}}_{\square}(s). \tag{7.9}$$

It remains to calculate the number of rhombic-cr and square sublattices of odd index, with generating function $\Phi_{\text{odd}}(s)$. Here, p and q run over all odd positive integers and hence each contribute a factor of $(1-2^{-s})\zeta(s)$, whereas w runs over all primitive w with $|w|^2$ odd, and hence gives the contribution $\frac{1}{1+2^{-s}}\Phi^{\mathsf{pr}}_{\square}(s)$, so that we have

$$\Phi_{\text{odd}}(s) \;=\; \frac{(1-2^{-s})^2}{1+2^{-s}}\,\zeta(s)^2\,\Phi^{\mathsf{pr}}_{\square}(s). \tag{7.10}$$

In total, the generating function $\Phi_{\Diamond+\square}(s)$ for the number of all rhombic-cr and square sublattices is given by

$$\Phi_{\Diamond+\square}(s) \;=\; \Phi_{\text{even}}(s) + \Phi_{\text{odd}}(s) \;=\; \frac{1-2^{-s}+2^{-2s+1}}{1+2^{-s}}\,\zeta(s)^2\,\Phi^{\mathsf{pr}}_{\square}(s). \tag{7.11}$$

Via standard arguments involving Moebius inversion (see [**6**] and references therein), the number of *primitive* rhombic-cr and square sublattices together is given by

$$\Phi^{\mathsf{pr}}_{\Diamond+\square}(s) \;=\; \frac{1}{\zeta(2s)}\,\Phi_{\Diamond+\square}(s) \;=\; \frac{1-2^{-s}+2^{-2s+1}}{1+2^{-s}}\,\frac{\zeta(s)^2}{\zeta(2s)}\,\Phi^{\mathsf{pr}}_{\square}(s). \tag{7.12}$$

Putting all this together, we obtain the generating functions $\Phi^{\mathsf{pr}}_{\square}$, $\Phi^{\mathsf{pr}}_{\Diamond}$ and $\Phi^{\mathsf{pr}}_{\sqsubset\!\sqsupset}$ for the number of primitive square, rhombic-cr and rectangular sublattices, respectively, as

$$\Phi^{\mathsf{pr}}_{\square}(s) \;=\; (1+2^{-s})\prod_{p\equiv 1(4)}\frac{1+p^{-s}}{1-p^{-s}} \;=\; \frac{\zeta(s)L(s,\chi_{-4})}{\zeta(2s)}, \tag{7.13}$$

$$\Phi^{\mathsf{pr}}_{\Diamond}(s) \;=\; \left(\frac{1-2^{-s}+2^{-2s+1}}{1+2^{-s}}\,\frac{\zeta(s)^2}{\zeta(2s)} - 1\right)\Phi^{\mathsf{pr}}_{\square}(s), \tag{7.14}$$

$$\Phi^{\mathsf{pr}}_{\sqsubset\!\sqsupset}(s) \;=\; \left(\frac{\zeta(s)^2}{\zeta(2s)} - 1\right)\Phi^{\mathsf{pr}}_{\square}(s), \tag{7.15}$$

with the L-series and the character χ_{-4} from above (see Appendix 7.A for details and notation). Note that the last equation follows from the fact that the generating function for all rectangular lattices including the square lattices is given by $\zeta(s)^2\Phi^{\mathsf{pr}}_{\square}(s)$.

Let us return to the well-rounded sublattices. Since z_1 and z_2 are shortest (non-zero) vectors, we have $|z_1 \pm z_2|^2 \geq |z_1|^2 = |z_2|^2$, which is equivalent to $\min(p^2,q^2) \geq \frac{p^2+q^2}{4}$, which in turn is equivalent to $3p^2 \geq q^2 \geq \frac{1}{3}p^2$. Note that this condition is also sufficient. Hence, we have to apply this extra condition to our considerations from above. We distinguish two cases:

(1) p and q are both even, $\sqrt{3}p \geq q \geq \frac{1}{\sqrt{3}}p$, and z may or may not be divisible by $1+\mathrm{i}$. We write $p=2p', q=2q'$, for which we likewise have $\sqrt{3}p' \geq q' \geq \frac{1}{\sqrt{3}}p'$. The index is even since it is given by $2p'q'|z|^2$. Here, p' and q' may take any positive integral

values, even or odd, which satisfy $\sqrt{3}p' \geq q' \geq \frac{1}{\sqrt{3}}p'$. This corresponds to $\mathcal{E}, \mathcal{E}'$ in Eqs. (29) and (31) of [**12**].

(2) p and q are both odd, $\sqrt{3}p \geq q \geq \frac{1}{\sqrt{3}}p$, and z is divisible by $1+\mathrm{i}$. We write $z = (1+\mathrm{i})w$. The index is odd and given by $pq|w|^2$. This corresponds to $\mathcal{O}, \mathcal{O}'$ in Eqs. (30) and (32) of [**12**].

The set of all possible indices of well-rounded sublattices is thus given by (we may interchange p and q if necessary)

$$\big\{2pq|z|^2 \,\big|\, q \leq p \leq \sqrt{3}q, z \in \mathbb{Z}[\mathrm{i}]\big\} \cup \big\{pq|z|^2 \,\big|\, q \leq p \leq \sqrt{3}q, z \in \mathbb{Z}[\mathrm{i}], 2 \nmid pq|z|^2\big\} \tag{7.16}$$

Note that this set is a proper subset of Fukshansky's [**12**, Thm 1.2, Thm 3.6] index set

$$\mathcal{D} := \big\{pq|z|^2 \,\big|\, q \leq p \leq \sqrt{3}q, z \in \mathbb{Z}[\mathrm{i}]\big\} \tag{7.17}$$

since $6 = 2 \cdot 3 \cdot |1|^2 \in \mathcal{D}$, but 6 is not contained in the set (7.16).

The Dirichlet series generating function for the well-rounded sublattices may now be calculated as above by taking the condition $\sqrt{3}p \geq q \geq \frac{1}{\sqrt{3}}p$ into account, so that the generating Dirichlet series for the well-rounded sublattices of even index is given by

$$\frac{1}{2^s} \sum_{p\in\mathbb{N}} \sum_{\frac{1}{\sqrt{3}}p<q<\sqrt{3}p} \frac{1}{p^s q^s}\, \Phi_{\Box}^{\mathsf{pr}}(s). \tag{7.18}$$

Clearly, this sum is symmetric in p and q, and comprises the similar sublattices. In fact, if we exclude the square sublattices (those lattices with $p = q$) from Eq. (7.18) and note that $\sum_{p\in\mathbb{N}} \sum_{\frac{1}{\sqrt{3}}p<q<p} = \sum_{q\in\mathbb{N}} \sum_{q<p<\sqrt{3}q}$, we obtain the generating function for the rhombic lattices with even index as

$$\Phi_{\mathsf{wr},\mathrm{even}}(s) = \frac{2}{2^s} \sum_{p\in\mathbb{N}} \sum_{p<q<\sqrt{3}p} \frac{1}{p^s q^s}\, \Phi_{\Box}^{\mathsf{pr}}(s). \tag{7.19}$$

The case of odd indices is slightly more cumbersome. Here, we have to replace the factor $(1-2^{-s})^2\zeta(s)^2$ by the corresponding sum over all odd integers with $p < q < \sqrt{3}p$. Writing $p = 2k+1$ and $q = 2\ell+1$, our condition reads $k < \ell < \sqrt{3}k + \frac{\sqrt{3}-1}{2}$. Since this inequality has no integral solution for $k = 0$, we may start our sum with $k = 1$, and finally arrive at

$$\Phi_{\mathsf{wr},\mathrm{odd}}(s) = \frac{2}{1+2^{-s}}\, \Phi_{\Box}^{\mathsf{pr}}(s) \sum_{k\in\mathbb{N}} \sum_{k<\ell<\sqrt{3}k+\frac{\sqrt{3}-1}{2}} \frac{1}{(2k+1)^s(2\ell+1)^s}. \tag{7.20}$$

Now, $\Phi_{\mathsf{wr},\mathrm{even}}(s)+\Phi_{\mathsf{wr},\mathrm{odd}}(s)+\Phi_{\Box}(s)$ gives the Dirichlet series generating function $\Phi_{\Box,\mathsf{wr}}(s)$ for the arithmetic function $a_{\Box}(n)$ of well-rounded sublattices of $\mathbb{Z}[\mathrm{i}]$ of index n. To get a better understanding of it, we 'sandwich' it, on the half-axis $s > 1$, between two explicitly known meromorphic functions. All these Dirichlet series satisfy the conditions of Theorem 7.A.1 (see Appendix 7.A). This gives a result on the asymptotic growth and its error as follows.

THEOREM 7.3.1. *Let $a_{\Box}(n)$ be the number of well-rounded sublattices of index n in the square lattice, and $\Phi_{\Box,\mathsf{wr}}(s) = \sum_{n=1}^{\infty} a_{\Box}(n) n^{-s}$ the corresponding Dirichlet series generating* *function. The latter is given by*

$$\Phi_{\square,\mathsf{wr}}(s) \;=\; \Phi_{\square}(s) + \Phi_{\mathsf{wr,even}}(s) + \Phi_{\mathsf{wr,odd}}(s)$$

via Eqs. (7.8), (7.19) *and* (7.20). *The generating function* $\Phi_{\square,\mathsf{wr}}$ *is meromorphic in the half plane* $\{\mathrm{Re}(s) > \frac{1}{2}\}$, *with a pole of order* 2 *at* $s = 1$, *and no other pole in the half plane* $\{\mathrm{Re}(s) \geq 1\}$.

If $s > 1$, *we have the inequality*

$$D_{\square}(s) - \Phi_{\square}(s) \;<\; \Phi_{\square,\mathsf{wr}}(s) \;<\; D_{\square}(s) + \Phi_{\square}(s),$$

with $\Phi_{\square}(s)$ *from Eq.* (7.8) *and the function*

$$D_{\square}(s) \;=\; \frac{2+2^s}{1+2^s}\,\frac{1-\sqrt{3}^{\,1-s}}{s-1}\,\frac{L(s,\chi_{-4})}{\zeta(2s)}\,\zeta(s)\zeta(2s-1).$$

As a consequence, the summatory function $A_{\square}(x) = \sum_{n\leq x} a_{\square}(n)$ *possesses the asymptotic growth behaviour*

$$A_{\square}(x) \;=\; \frac{\log(3)}{2\pi}\,x\log(x) + \mathcal{O}\bigl(x\log(x)\bigr), \quad \textit{as } x \to \infty.$$

Proof. Clearly, $\Phi_{\square,\mathsf{wr}}(s)$ is the sum of $\Phi_{\square}(s)$ and the two contributions from Eqs. (7.19) and (7.20). For real $s > 1$, the latter can be both bounded from below and above by an application of Lemma 7.A.2 from Appendix 7.A with $\alpha = \sqrt{3}$, the former with parameters $\beta = \gamma = 0$ and the latter (after pulling out a factor of 2^s in the denominator) with $\beta = (\sqrt{3}-1)/2$ and $\gamma = \frac{1}{2}$. A straight-forward calculation leads to the explicit expression for the function $D_{\square}(s)$, as well as to the inequality stated.

It follows from the explicit expression for $D_{\square}(s)$ that it is a meromorphic function in the whole plane. Using the Euler summation formula, we see that the difference $\bigl(\Phi_{\square,\mathsf{wr}}(s) - D_{\square}(s)\bigr)/\Phi^{\mathsf{pr}}_{\square}(s)$ is an analytic function for $\mathrm{Re}(s) > \frac{1}{2}$, guaranteeing that $\Phi_{\square,\mathsf{wr}}(s)$ is meromorphic in the half plane $\{\mathrm{Re}(s) > \frac{1}{2}\}$.

The right-most singularity of $\zeta(s)\zeta(2s-1)$ is $s = 1$, with a pole of the form $\frac{1}{2(s-1)^2}$, while the entire factor of $D_{\square}(s)$ in front of it is analytic near $s = 1$ (as well as on the line $\{\mathrm{Re}(s) = 1\}$). An application of Theorem 7.A.1 from Appendix A now leads to the claimed growth rate. □

The difference of the bounds in Theorem 7.3.1 is $2\Phi_{\square}(s)$, which is a Dirichlet series that itself allows an application of Theorem 7.A.1. The corresponding summatory function has an asymptotic growth of the form $cx + \mathcal{O}(x)$, which suggests that the error term of $A_{\square}(x)$ might be improved in this direction. However, it seems difficult to extract good error terms from Delange's theorem; compare the example in [**8**, Sec 1.8]. Since numerical calculations support the above suggestion, we employed direct methods such as Dirichlet's hyperbola method; compare [**1**, Sec 3.5] or [**28**, Sec. I.3]. A lengthy calculation (see [**32**] for the details) finally leads to the following result.

Theorem 7.3.2. *Let $a_{\square}(n)$ be the number of well-rounded sublattices of index n in the square lattice. Then, the summatory function $A_{\square}(x) = \sum_{n\le x} a_{\square}(n)$ possesses the asymptotic growth behaviour*

$$\begin{aligned}A_{\square}(x) \;&=\; \frac{\log(3)}{3}\frac{L(1,\chi_{-4})}{\zeta(2)}x(\log(x)-1)+c_{\square}x+\mathcal{O}\big(x^{3/4}\log(x)\big)\\ &=\; \frac{\log(3)}{2\pi}x\log(x)+\left(c_{\square}-\frac{\log(3)}{2\pi}\right)x+\mathcal{O}\big(x^{3/4}\log(x)\big)\end{aligned}$$

where, with γ denoting the Euler–Mascheroni constant,

$$\begin{aligned}c_{\square} := \frac{L(1,\chi_{-4})}{\zeta(2)}\Bigg(&\zeta(2)+\frac{\log(3)}{3}\left(\frac{L'(1,\chi_{-4})}{L(1,\chi_{-4})}+\gamma-2\frac{\zeta'(2)}{\zeta(2)}\right)+\frac{\log(3)}{3}\left(2\gamma-\frac{\log(3)}{4}-\frac{\log(2)}{6}\right)\\ &-\sum_{p=1}^{\infty}\frac{1}{p}\Bigg(\frac{\log(3)}{2}-\sum_{p<q<p\sqrt{3}}\frac{1}{q}\Bigg)-\frac{4}{3}\sum_{k=0}^{\infty}\frac{1}{2k+1}\Bigg(\frac{1}{4}\log(3)-\sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2}\frac{1}{2\ell+1}\Bigg)\Bigg)\\ \approx\, &0.6272237\end{aligned}$$

is the coefficient of $(s-1)^{-1}$ in the Laurent series of $\sum_{n\ge1} a_{\square}(n)n^{-s}$ around $s=1$.

Note that $L'(1,\chi_{-4})$ can be computed efficiently via

$$\frac{L'(1,\chi_{-4})}{L(1,\chi_{-4})} \;=\; \log\left(M(1,\sqrt{2})^2\,\frac{e^{\gamma}}{2}\right) \;=\; \log\!\left(\Gamma\!\left(\frac{3}{4}\right)^4\frac{e^{\gamma}}{\pi}\right) \;\approx\; 0.2456096, \tag{7.21}$$

where $M(x,y)$ is the arithmetic-geometric mean of x and y, and Γ denotes the gamma function; see [**23**] and references therein.

Sketch of proof. $\Phi_{\square,\mathsf{wr}}(s) = \sum_{n=1}^{\infty} a_{\square}(n)n^{-s}$ is a sum of three Dirichlet series, each of which is itself a product of several Dirichlet series. Hence, each contribution to $a_{\square}(n)$ is a Dirichlet convolution of arithmetic functions. The asymptotic behaviour can thus be calculated by elementary methods as described in [**1**, Sec. 3.5], making use of Euler's summation formula (7.42) wherever appropriate. To be more specific, let

$$\Phi_{\mathsf{wr,even}}(s) \;=\sum_{n\in\mathbb{N}}\frac{a_{\mathrm{even}}(n)}{n^s}, \tag{7.22}$$

which is a product of the Dirichlet series

$$\begin{aligned}\frac{2}{2^s}\frac{1}{\zeta(2s)} \;&=\sum_{n\in\mathbb{N}}\frac{c(n)}{n^s},\\ \sum_{p\in\mathbb{N}}\;\sum_{p<q<\sqrt{3}p}\frac{1}{p^sq^s} \;&=\sum_{n\in\mathbb{N}}\frac{w(n)}{n^s},\\ \Phi_{\square}(s) \;&=\sum_{n\in\mathbb{N}}\frac{b(n)}{n^s}.\end{aligned}$$

Hence $a_{\text{even}} = c * w * b$ is the Dirichlet convolution of c, w, b. The summatory function of a Dirichlet convolution $f * g$ can now be calculated via the classic formulas (compare [**1**] and [**28**, Sec. I.3.2])

$$\sum_{n \le x} (f * g)(n) = \sum_{m \le x} \sum_{d \le x/m} f(m) g(d) \tag{7.23}$$

$$= \sum_{m \le \sqrt{x}} \sum_{m < d \le x/m} \big(f(m) g(d) + f(d) g(m) \big) + \sum_{m \le \sqrt{x}} f(m) g(m), \tag{7.24}$$

where the latter formula is used for the convolutions $w * b$ and $b = \chi_{-4} * 1$. □

7.4. Well-rounded sublattices of $\mathbb{Z}[\rho]$

Next, we consider the hexagonal lattice $\mathbb{Z}[\rho]$, with $\rho = \frac{1+\mathrm{i}\sqrt{3}}{2}$. As an arithmetic object, it is the ring of Eisenstein integers, the maximal order of the quadratic field $\mathbb{Q}(\mathrm{i}\sqrt{3}\,)$. The Dirichlet series generating function for the number of similar sublattices of $\mathbb{Z}[\rho]$ is

$$\Phi_{\triangle}(s) = \zeta_{\mathbb{Q}(\rho)}(s) = L(s, \chi_{-3}) \zeta(s), \tag{7.25}$$

with the character

$$\chi_{-3}(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod 3, \\ 1, & \text{if } n \equiv 1 \bmod 3, \\ -1, & \text{if } n \equiv 2 \bmod 3, \end{cases}$$

see [**6, 30**] and Appendix 7.A.

Let $\{z_1, z_2\}$ be a reduced basis of a well-rounded sublattice of $\mathbb{Z}[\rho]$. The orthogonality of $z_1 + z_2$ and $z_1 - z_2$ implies that $\frac{z_1+z_2}{z_1-z_2} = \mathrm{i}\sqrt{3}\, r$ with $r \in \mathbb{Q}$. This shows that square lattices cannot occur here since this would require $|z_1 + z_2|^2 = |z_1 - z_2|^2$, which is impossible. Thus, the well-rounded sublattices of $\mathbb{Z}[\rho]$ are rhombic-cr or hexagonal lattices. However, at least one of $z_1 + z_2$ and $z_1 - z_2$ is divisible by $\mathrm{i}\sqrt{3} = \rho - \bar{\rho}$, and w.l.o.g. we may assume that $\mathrm{i}\sqrt{3}$ divides $z_1 - z_2$. Hence, there exist p and $q \in \mathbb{Z}$ together with a primitive $z \in \mathbb{Z}[\rho]$ such that $z_1 + z_2 = pz$ and $z_1 - z_2 = \mathrm{i}\sqrt{3} qz$. Here, primitive means that $n = 1$ is the only integer $n \in \mathbb{N}$ that divides z. We may again choose p and q positive and

$$\varGamma = \langle z_1, z_2 \rangle_{\mathbb{Z}} = \left\langle \tfrac{p+\mathrm{i}\sqrt{3}q}{2} z, \tfrac{p-\mathrm{i}\sqrt{3}q}{2} z \right\rangle_{\mathbb{Z}} = \left\langle \left(\tfrac{p-q}{2} + \rho q\right) z, \left(\tfrac{p+q}{2} - \rho q\right) z \right\rangle_{\mathbb{Z}} \tag{7.26}$$

is thus a sublattice of index $pq|z|^2$. In particular, $\varGamma$ is a hexagonal lattice if and only if $p = q$ or $p = 3q$. Note that Eq. (7.26) shows that p and q have the same parity.

Well-rounded sublattices must satisfy the additional constraints $|z_1 \pm z_2|^2 \ge |z_1|^2 = |z_2|^2$, which, in this case, are equivalent to $q \le p \le 3q$. The set of possible indices of well-rounded sublattices is thus given by

$$\big\{ 4pq|z|^2 \,\big|\, q \le p \le 3q, z \in \mathbb{Z}[\rho] \big\} \cup \big\{ pq|z|^2 \,\big|\, q \le p \le 3q, z \in \mathbb{Z}[\rho], 2 \nmid pq \big\}. \tag{7.27}$$

An alternative parametrisation of this set can be found in [**13**, Cor. 4.9]. The equivalence of these formulations can easily be checked by recalling that the (rational) primes represented by the norm form $m^2 - mn + n^2$ of $\mathbb{Z}[\rho]$ are precisely 3 and all primes $p \equiv 1 \pmod 3$.

Counting the number of distinct well-rounded sublattices of a given index works essentially as in the square lattice case. However, we have to avoid counting the same lattice twice. Let z be divisible by $\mathrm{i}\sqrt{3}$, so that $z = \mathrm{i}\sqrt{3}w$. Then,

$$z_1 = \frac{p + \mathrm{i}\sqrt{3}q}{2} z = -\frac{3q - \mathrm{i}\sqrt{3}p}{2} w, \tag{7.28}$$

$$z_2 = \frac{p - \mathrm{i}\sqrt{3}q}{2} z = \frac{3q + \mathrm{i}\sqrt{3}p}{2} w \tag{7.29}$$

shows that the tuples (p, q, z) and $(3q, p, w)$ correspond to the same sublattice. Thus, we only sum over primitive z that are not divisible by $\mathrm{i}\sqrt{3}$.

Since we know the generating function (7.25) for the similar sublattices already from [**4**], we concentrate on the rhombic sublattices here (excluding hexagonal sublattices, as before). The summation over all primitive $z \in \mathbb{Z}[\rho]$ not divisible by $\mathrm{i}\sqrt{3}$ gives the contribution $\frac{1}{1+3^{-s}} \Phi^{\mathsf{pr}}_{\triangle}(s)$. The generating function of all rhombic sublattices of even index then reads

$$\Phi_{\triangle,\mathsf{wr},\mathsf{even}}(s) = \frac{3}{4^s(1+3^{-s})} \sum_{p\in\mathbb{N}} \sum_{p<q<3p} \frac{1}{p^s q^s} \Phi^{\mathsf{pr}}_{\triangle}(s), \tag{7.30}$$

where the factor of 3 reflects that each sublattice occurs in three different orientations.

In the case of odd indices, we substitute again $p = 2k + 1$ and $q = 2\ell + 1$, wherefore our constraints read $k < \ell < 3k + 1$. This leads to the following expression for the generating function of all rhombic sublattices of odd index:

$$\Phi_{\triangle,\mathsf{wr},\mathsf{odd}}(s) = \frac{3}{1+3^{-s}} \sum_{k\in\mathbb{N}} \sum_{k<\ell<3k+1} \frac{1}{(2k+1)^s(2\ell+1)^s} \Phi^{\mathsf{pr}}_{\triangle}(s). \tag{7.31}$$

Now, we can apply the same strategy as in the square lattice case.

Theorem 7.4.1. *Let $a_{\triangle}(n)$ be the number of well-rounded sublattices of index n in the hexagonal lattice, and $\Phi_{\triangle,\mathsf{wr}}(s) = \sum_{n=1}^{\infty} a_{\triangle}(n) n^{-s}$ the corresponding Dirichlet series generating function. It is given by*

$$\Phi_{\triangle,\mathsf{wr}}(s) = \Phi_{\triangle}(s) + \Phi_{\triangle,\mathsf{wr},\mathsf{even}}(s) + \Phi_{\triangle,\mathsf{wr},\mathsf{odd}}(s),$$

with the series from Eqs. (7.25)*,* (7.30) *and* (7.31)*.*

If $s > 1$, we have the inequality

$$D_{\triangle}(s) - E_{\triangle}(s) < \Phi_{\triangle,\mathsf{wr}}(s) < D_{\triangle}(s),$$

with the functions

$$D_{\triangle}(s) = \frac{1}{2} \frac{3}{1+3^{-s}} \frac{1-3^{1-s}}{s-1} \frac{L(s,\chi_{-3})}{\zeta(2s)} \zeta(s)\zeta(2s-1),$$

$$E_{\triangle}(s) = \frac{3}{1+3^{-s}} L(s,\chi_{-3})\zeta(s).$$

The function $\Phi_{\triangle,\mathsf{wr}}(s)$ is meromorphic in the half plane $\{\mathrm{Re}(s) > \frac{1}{2}\}$, with a pole of order 2 *at $s = 1$, and no other pole in the half plane $\{\mathrm{Re}(s) \geq 1\}$. As a consequence, the summatory* *function $A_\triangle(x) = \sum_{n\le x} a_\triangle(n)$, as $x\to\infty$, possesses the asymptotic growth behaviour*

$$A_\triangle(x) \;=\; \frac{3\sqrt{3}\log(3)}{8\pi}\, x\log(x) + o\bigl(x\log(x)\bigr).$$

Sketch of proof. In analogy to before, $\Phi_{\triangle,\mathsf{wr}}(s)$ is the sum of the contributions from Eqs. (7.30) and (7.31). The calculation of the upper and lower bounds can be done as in Theorem 7.3.1 via Lemma 7.A.2, this time with $\alpha = 3$ and appropriate choices for β and γ. The conclusion on the growth rate of $A_\triangle(x)$ follows as before from Theorem 7.A.1. □

As for the square lattice, we can improve the error term considerably by lengthy but elementary calculations (see [**32**] for the details). Eventually, we obtain the following result.

Theorem 7.4.2. *Let $a_\triangle(n)$ be the number of well-rounded sublattices of index n in the hexagonal lattice. Then, the summatory function $A_\triangle(x) = \sum_{n\le x} a_\triangle(n)$ possesses the asymptotic growth behaviour*

$$\begin{aligned} A_\triangle(x) \;&=\; \frac{9\log(3)}{16}\,\frac{L(1,\chi_{-3})}{\zeta(2)}\, x(\log(x)-1) + c_\triangle x + \mathcal{O}\bigl(x^{3/4}\log(x)\bigr)\\ &=\; \frac{3\sqrt{3}\,\log(3)}{8\pi} x(\log(x)-1) + c_\triangle x + \mathcal{O}\bigl(x^{3/4}\log(x)\bigr), \end{aligned}$$

where

$$\begin{aligned} c_\triangle \;=\; L(1,\chi_{-3}) + \frac{9\log(3)L(1,\chi_{-3})}{16\zeta(2)}\Biggl(\biggl(\gamma + \frac{L'(1,\chi_{-3})}{L(1,\chi_{-3})} - 2\frac{\zeta'(2)}{\zeta(2)}\biggr) + 2\gamma - \frac{\log(3)}{4}\\ -\sum_{p=1}^{\infty}\frac{1}{p}\biggl(\log(3) - \sum_{p<q\le 3p-1}\frac{1}{q}\biggr) - \sum_{k=0}^{\infty}\frac{4}{2k+1}\biggl(\frac{1}{2}\log(3) - \sum_{k<\ell\le 3k}\frac{1}{2\ell+1}\biggr)\Biggr)\\ \approx\; 0.4915036 \end{aligned}$$

is the coefficient of $(s-1)^{-1}$ in the Laurent series of $\sum_n \frac{a_\triangle(n)}{n^s}$ around $s=1$. □

The number $L'(1,\chi_{-3})$ can be computed efficiently as well, via a formula involving the arithmetic-geometric mean (see [**23**]), and reads

$$\frac{L'(1,\chi_{-3})}{L(1,\chi_{-3})} \;=\; \log\left(\frac{2^{\frac{3}{4}}M\bigl(1,\cos(\frac{\pi}{12})\bigr)^2\, e^{\gamma}}{3}\right) \;=\; \log\left(\frac{2^4\pi^4 e^{\gamma}}{3^{\frac{3}{2}}\,\Gamma\bigl(\frac{1}{3}\bigr)^6}\right) \;\approx\; 0.3682816. \tag{7.32}$$

Above and in the previous section, we have seen that the asymptotic growth rate for the hexagonal and square lattice is of the form $c_1 x\log(x) + c_2 x + \mathcal{O}\bigl(x^{3/4}\log(x)\bigr)$. Actually, numerical calculations suggest that the error term is $\mathcal{O}(x^{1/2})$ or maybe even slightly better.

Let us now see what we can say about the other planar lattices.

7.5. The general case

7.5.1. Existence of well-rounded sublattices. Recall from Section 7.2 that a lattice allows a well-rounded sublattice if and only if it contains a rectangular or square sublattice. The following lemma contains several reformulations of this property.

LEMMA 7.5.1. *Let $\varGamma$ be any planar lattice. There are natural bijections between the following objects:*

(1) Rational orthogonal frames *for $\varGamma$, that is, unordered pairs $\mathbb{Q}w, \mathbb{Q}z$ of perpendicular ($w \perp z$), one-dimensional subspaces of the rational space $\mathbb{Q}\varGamma$ generated by $\varGamma$ (so we may assume $w, z \in \varGamma$).*

(2) *Unordered pairs $\{\pm R\}$ of coincidence reflections of $\varGamma$; from now on, we shall simply write $\pm R$ for such a pair.*

(3) Basic *rectangular or square sublattices $\varLambda \subseteq \varGamma$, where 'basic' means that $\varLambda = \langle w, z\rangle_{\mathbb{Z}}$ with w, z primitive in $\varGamma$ (so $\mathbb{Q}w \cap \varGamma = \mathbb{Z}w$ and $\mathbb{Q}z \cap \varGamma = \mathbb{Z}z$). We shall call them* BRS sublattices *for short.*

(4) *Four-element subsets $\{\pm w, \pm z\} \subset \varGamma$ of non-zero primitive lattice vectors with $w \perp z$.*

Given $\varGamma$, we use the notation $\mathcal{R} = \mathcal{R}_{\varGamma}$ for the set of all pairs $\pm R$ of coincidence reflections of $\varGamma$. So $\mathcal{R}_{\varGamma}$ is in natural bijection with any of the four sets described in Lemma 7.5.1. For the rest of the paper, we introduce the following notation, based on Lemma 7.5.1. For $\pm R \in \mathcal{R}_{\varGamma}$, we denote by $\varGamma_R$ (rather than $\varGamma_{\pm R}$) the corresponding BRS sublattice. Explicitly, this is

$$\begin{aligned} \varGamma_R &= \varGamma \cap \mathrm{Fix}(R) \oplus \varGamma \cap \mathrm{Fix}(-R) \\ &= \mathbb{Z}w \oplus \mathbb{Z}z, \quad \text{where } Rw = w,\ Rz = -z \end{aligned}$$

(thus w, z are primitive in $\varGamma$). In accordance with part (2) of Lemma 7.5.1, we have $\varGamma_R = \varGamma_{-R}$, with the roles of w and z interchanged. If we start with an arbitrary primitive vector $w \in \varGamma$, we similarly write

$$\varGamma_w := \mathbb{Z}w \oplus \mathbb{Z}z, \quad \text{where } z \perp w,\ z \text{ primitive in } \varGamma.$$

The four element set $\{\pm w, \pm z\}$ is uniquely determined by any of its members, and $\varGamma_w$ is the unique BRS-sublattice belonging to this set, according to part (4) of the remark.

In addition to $\varGamma_R$, there is a second sublattice of $\varGamma$ which is invariant under R and contains w, z as primitive vectors. This is

$$\widetilde{\varGamma}_R := \Big\langle \frac{w+z}{2}, \frac{w-z}{2} \Big\rangle_{\mathbb{Z}}, \tag{7.33}$$

the unique superlattice of $\varGamma_R$ containing $\varGamma_R$ with index 2 in such a way that w, z are still primitive in $\widetilde{\varGamma}_R$. By the way, it is a purely algebraic fact that, if R is a non-trivial automorphism of order 2 of an abstract lattice $\varLambda$ (free $\mathbb{Z}$-module) of rank 2, i.e. $R^2 = \mathrm{id} \neq \pm R$, then either $\varLambda$ has a $\mathbb{Z}$-basis w, z of eigenvectors of R (so $Rz = z$, $Rw = -w$), or $\varLambda$ possesses a $\mathbb{Z}$-basis u, v with $Ru = v$. Thus, already on the level of abstract reflections, one can distinguish between 'rectangular type' and 'rhombic type' of a reflection acting on a lattice. In the situation considered above, the reflection R on $\varGamma_R$ is of rectangular type, and the lattice $\varGamma_R$ itself thus of rectangular or square Bravais type, whereas the reflection R on $\widetilde{\varGamma}_R$ is of rhombic type, which implies that $\widetilde{\varGamma}_R$ is of rhombic-cr, square or hexagonal Bravais type. The significance of $\widetilde{\varGamma}_R$ is explained by the following lemma.

LEMMA 7.5.2. *Given $\mathit{\Gamma}$ and $\pm R \in \mathcal{R}_{\mathit{\Gamma}}$ as above, let $\mathit{\Lambda} \supseteq \mathit{\Gamma}_R = \langle w, z\rangle$ be an R-invariant superlattice containing w, z as primitive vectors. Then, either $\mathit{\Lambda} = \mathit{\Gamma}_R$ or $\mathit{\Lambda} = \widetilde{\mathit{\Gamma}}_R$.*

PROOF. Since z is primitive, $\mathit{\Lambda}$ has a $\mathbb{Z}$-basis u, z, where u is of the form $u = \frac{1}{m}w + \frac{k}{m}z$ with $m = [\mathit{\Lambda} : \mathit{\Gamma}_R]$ and $0 \leq k < m$. The condition $Ru \in \mathit{\Lambda}$ immediately leads to $m \in \{1, 2\}$ and $k \in \{0, 1\}$, respectively. □

LEMMA 7.5.3. *Given $\mathit{\Gamma}$ and $\pm R \in \mathcal{R}_{\mathit{\Gamma}}$ as above, $\widetilde{\mathit{\Gamma}}_R$ is contained in $\mathit{\Gamma}$ if and only if the index $[\mathit{\Gamma} : \mathit{\Gamma}_R]$ is even.*

PROOF. If $[\mathit{\Gamma} : \mathit{\Gamma}_R] = [\mathit{\Gamma} : \langle w, z\rangle]$ is even and $\frac{1}{2}(aw + bz)$ with $a, b \in \{0, 1\}$ represents an element of order 2 in the factor group $\mathit{\Gamma}/\mathit{\Gamma}_R$, then, since $w/2, z/2 \notin \mathit{\Gamma}$, we must have $a = b = 1$, leading to the sublattice $\widetilde{\mathit{\Gamma}}_R$. The converse is clear. □

COROLLARY 1. *For any pair of coincidence reflections $\pm R \in \mathcal{R}_{\mathit{\Gamma}}$, the coincidence site lattice $\mathit{\Gamma}(R) = \mathit{\Gamma} \cap R\mathit{\Gamma}$ is equal to $\mathit{\Gamma}_R$ or to $\widetilde{\mathit{\Gamma}}_R$. The latter occurs if and only if the index $[\mathit{\Gamma} : \mathit{\Gamma}_R]$ is even.* □

The following basic result partitions the set of all planar lattices admitting a well-rounded (or rectangular) sublattice into two disjoint classes, as announced at the end of the introduction. Clearly, a rational lattice possesses infinitely many BRS sublattices, since for any non-zero lattice vector v, the orthogonal subspace of v also contains a non-zero lattice vector (simply by solving a linear equation with rational coefficients). In contrast, the non-rational case can be analysed as follows.

PROPOSITION 7.5.4. *Let $\mathit{\Gamma}$ be non-rational planar lattice which possesses a rectangular sublattice, so that $\mathcal{R}_{\mathit{\Gamma}} \neq \varnothing$ by Lemma 7.5.1. Then, $|\mathcal{R}_{\mathit{\Gamma}}| = 1$, whence $\mathit{\Gamma}$ possesses exactly one BRS sublattice, and one pair of coincidence reflections.*

PROOF. $\mathit{\Gamma}$ has a sublattice $\mathit{\Lambda}$ with an orthogonal basis v, w, where we may assume $|v| = 1$ and $|w|^2 = c > 0$. Now assume that there is a further vector $u = rv + sw$ with $rs \neq 0$ admitting an orthogonal, non-zero vector $u' = r'v + s'w$. Then, $rr' + css' = 0$ and necessarily $s' \neq 0$, thus $c = -rr'/ss' \in \mathbb{Q}$. Therefore $\mathit{\Lambda}$, and thus also $\mathit{\Gamma}$, is rational. □

The previous result (with a slightly more complicated proof) is also found in [**18**], Lemma 2.5 and Remark 2.6. Our approach suggests the following distinction of cases.

PROPOSITION 7.5.5. *Let $\mathit{\Gamma} = \langle 1, \tau\rangle_{\mathbb{Z}}$ be a lattice in $\mathbb{R}^2 \simeq \mathcal{C}$, and write $n = |\tau|^2$ and $t = \tau + \bar{\tau}$. Then, $\mathit{\Gamma}$ has a well-rounded sublattice if and only if one of the following conditions is satisfied:*

(1) *$\mathit{\Gamma}$ is rational, i.e. both t and n are rational;*
(2) *t is rational, but n is not;*
(3) *t is irrational, and there exist $q, r \in \mathbb{Q}$ with $\sqrt{q + r^2} \in \mathbb{Q}$ and $n = q + rt$.*

Note that case (3) includes both rational and irrational n. In the case that n is rational, this means that n has to be a rational square.

Proof. Recall that Γ has a well-rounded sublattice if and only if it has a rectangular or a square sublattice. This happens if and only if there exist integers a, b, c, d such that the non-zero vectors $a + b\tau$ and $c + d\tau$ are orthogonal. The latter condition holds if and only if

$$ac + bdn + (ad + bc)\frac{t}{2} \,=\, 0 \tag{7.34}$$

has a non-trivial integral solution, where $n = |\tau|^2$ and $t = \tau + \bar{\tau}$ are the norm and the trace of τ, respectively. In fact, there exists an integral solution if and only if there exists a rational one. This leads to the following three cases:

(1) Clearly, Eq. (7.34) has a solution if both t and n are rational.

(2) Let $t \in \mathbb{Q}, n \notin \mathbb{Q}$: Condition (7.34) is equivalent to $bd = 0 = ac + (ad + bc)\frac{t}{2}$. With $\frac{t}{2} = \frac{p}{q}$, $p, q \in \mathbb{Z}$, an integer solution is given by $a = 1, b = 0, c = p, d = -q$.

(3) Let $t \notin \mathbb{Q}$, with $n = q + rt$. As $n > 0$, at least one of q and r is non-zero. Here, condition (7.34) is equivalent to $ac + bdq = 0$ and $2bdr + (ad + bc) = 0$. As $a = c = 0$ would imply $a + b\tau = 0$ or $c + d\tau = 0$, we may assume w.l.o.g. that $a \neq 0$. This gives $c = -\frac{bdq}{a}$ and $1 + 2\frac{b}{a}r - \left(\frac{b}{a}\right)^2 q = 0$, where we have assumed $d \neq 0$ in the latter equation, since otherwise $c + d\tau = 0$. The latter has a rational solution if and only if $r^2 + q$ is a square.

Finally, we have to check that the remaining case does not allow for integral solutions. Let t and n be irrational and assume that they are independent over $\mathbb{Q}$. This clearly requires $ac = bd = ad + bc = 0$, which implies $a + b\tau = 0$ or $c + d\tau = 0$. □

Remark 7.5.1. After we had arrived at Proposition 7.5.5, we became aware of an essentially equivalent result by Kühnlein [**18**, Lemma 2.5], where the invariant $\delta(\Gamma) = \dim\langle 1, t, n\rangle_{\mathbb{Q}}$ is introduced. Clearly, condition (1) of Proposition 7.5.5 is equivalent with $\delta(\Gamma) = 1$, and our conditions (2) and (3) are equivalent with $\delta(\Gamma) = 2$ together with the condition that Kühnlein's 'strange invariant' $\sigma(\Gamma)$ is the class of all squares in $\mathbb{Q}^{\times}$. Here, $\sigma(\Gamma)$ is the square class of $-\det(X)$, where $X = \left(\begin{smallmatrix} x & y \\ y & z \end{smallmatrix}\right)$ is a non-trivial integral matrix satisfying $\mathrm{tr}(XG) = 0$, with $G = \left(\begin{smallmatrix} 1 & t/2 \\ t/2 & n \end{smallmatrix}\right)$ being the Gram matrix of Γ. Altogether, this shows that our criterion is equivalent to Kühnlein's.

In the situation of Proposition 7.5.4, let R be the unique (up to a sign) coincidence reflection and $\Gamma_R = \langle w, z\rangle$ the unique BRS sublattice. We get all well-rounded sublattices by considering the rectangular sublattices generated by kw, ℓz with the constraint

$$k\frac{1}{\sqrt{3}}\frac{|w|}{|z|} \,\leq\, \ell \,\leq\, k\sqrt{3}\,\frac{|w|}{|z|}, \tag{7.35}$$

whose superlattice $\left\langle \frac{1}{2}kw \pm \frac{1}{2}\ell z\right\rangle_{\mathbb{Z}}$ is a sublattice of Γ. The latter requires that k and ℓ have the same parity. By Lemma 7.5.3, odd values k, ℓ occur if and only if the index $\sigma = \sigma_{\Gamma} := [\Gamma : \Gamma_R]$ is even. This gives the following result.

Proposition 7.5.6. *Let Γ be a lattice that has a well-rounded sublattice and assume that Γ is not rational (cf. Proposition* 7.5.4*). Let σ be the index of its unique BRS sublattice Γ_R*

and κ be the ratio of the lengths of its orthogonal basis vectors. The generating function for the number of well-rounded sublattices then reads as follows.

(1) *If σ is odd, one has*

$$\Phi_{\Gamma,\mathsf{wr}}(s) \;=\; \frac{1}{\sigma^s}\,\phi_{\mathsf{wr},\mathrm{even}}(\kappa;s),$$

with

$$\phi_{\mathsf{wr},\mathrm{even}}(\kappa;s) \;=\; \frac{1}{2^s}\sum_{k\in\mathbb{N}}\;\sum_{\frac{\kappa}{\sqrt{3}}k\le\ell\le\sqrt{3}\,\kappa\,k}\frac{1}{k^s\ell^s}\,.$$

(2) *If σ is even, one has*

$$\Phi_{\Gamma,\mathsf{wr}}(s) \;=\; \frac{1}{\sigma^s}\,\phi_{\mathsf{wr},\mathrm{even}}(\kappa;s)+\frac{2^s}{\sigma^s}\,\phi_{\mathsf{wr},\mathrm{odd}}(\kappa;s),$$

with $\phi_{\mathsf{wr},\mathrm{even}}(\kappa;s)$ as above and

$$\phi_{\mathsf{wr},\mathrm{odd}}(\kappa;s) \;=\sum_{k\in\mathbb{N}}\;\sum_{\frac{\kappa}{\sqrt{3}}(k+\frac12)-\frac12\le\ell\le\sqrt{3}\,\kappa\,(k+\frac12)-\frac12}\frac{1}{(2k+1)^s(2\ell+1)^s}\,.$$

Remark 7.5.2. The quantity $\kappa = |w|/|z|$ is unique up to taking its inverse. Note that $\phi_{\mathsf{wr},\mathrm{even}}(\kappa;s) = \phi_{\mathsf{wr},\mathrm{even}}(\frac{1}{\kappa};s)$ and $\phi_{\mathsf{wr},\mathrm{odd}}(\kappa;s) = \phi_{\mathsf{wr},\mathrm{odd}}(\frac{1}{\kappa};s)$. Hence, there is no ambiguity in the definition of the generating functions.

In the cases of the square and hexagonal lattices we have been able to give lower and upper bounds for the generating functions Φ_{wr}. In a similar way we obtain the following result.

Remark 7.5.3. We have the following inequalities for real $s > 1$:

$$\begin{aligned}D_{\mathrm{even}}(\kappa;s)-E_{\mathrm{even}}(\kappa;s) \;<\; \phi_{\mathsf{wr},\mathrm{even}}(\kappa;s) \;<\; D_{\mathrm{even}}(\kappa;s)+E_{\mathrm{even}}(\kappa;s),\\ D_{\mathrm{odd}}(\kappa;s)-E_{\mathrm{odd}}(\kappa;s) \;<\; \phi_{\mathsf{wr},\mathrm{odd}}(\kappa;s) \;<\; D_{\mathrm{odd}}(\kappa;s)+E_{\mathrm{odd}}(\kappa;s),\end{aligned}$$

with the generating functions

$$\begin{aligned}D_{\mathrm{even}}(\kappa;s) \;&=\; \frac{1}{2^s}\left(\frac{\sqrt{3}}{\kappa}\right)^{s-1}\frac{1-3^{1-s}}{s-1}\zeta(2s-1),\\ E_{\mathrm{even}}(\kappa;s) \;&=\; \frac{1}{2^s}\left(\frac{\sqrt{3}}{\kappa}\right)^{s}\zeta(2s),\\ D_{\mathrm{odd}}(\kappa;s) \;&=\; \frac{1}{2}\left(\frac{\sqrt{3}}{\kappa}\right)^{s-1}\frac{1-3^{1-s}}{s-1}\left(1-\frac{1}{2^{2s-1}}\right)\zeta(2s-1),\\ E_{\mathrm{odd}}(\kappa;s) \;&=\; \left(\frac{\sqrt{3}}{\kappa}\right)^{s}\left(1-\frac{1}{2^{2s}}\right)\zeta(2s).\end{aligned}$$

Let us now have a closer look at the analytic properties of $\Phi_{\Gamma,\mathsf{wr}}$. Before formulating the theorem, we observe that the two cases of Proposition 7.5.6 can be unified by considering the index $\Sigma := [\Gamma : \Gamma(R)]$ of the unique non-trivial CSL in Γ. By Corollary 1, $\sigma = \Sigma$ if σ is odd and $\sigma = 2\Sigma$ if σ is even. We can now formulate a refinement of Lemma 3.3 and Corollary 3.4 in [**18**] as follows.

PROPOSITION 7.5.7. *Let Γ be a lattice with a well-rounded sublattice and assume that Γ is not rational, so that Γ has exactly one non-trivial CSL. Let Σ be its index in Γ. Then, the generating function $\Phi_{\Gamma,\mathsf{wr}}$ for the number of well-rounded sublattices has an analytic continuation to the open half plane $\{\mathrm{Re}(s) > \frac{1}{2}\}$ except for a simple pole at $s = 1$, with residue $\frac{\log(3)}{4\Sigma}$.*

PROOF. We proceed in a similar way as in the proof of Theorem 7.3.1 by applying Euler's summation formula to the inner sum. This shows that both $\phi_{\mathsf{wr,even}}(\kappa; s) - D_{\mathrm{even}}(\kappa; s)$ and $\phi_{\mathsf{wr,odd}}(\kappa; s) - D_{\mathrm{odd}}(\kappa; s)$ are analytic in the open half plane $\{\mathrm{Re}(s) > \frac{1}{2}\}$. Moreover, the explicit formulas from above show that both $D_{\mathrm{even}}(\kappa; s)$ and $D_{\mathrm{odd}}(\kappa; s)$ are analytic in the whole complex plane except at $s = 1$, where they have a simple pole with residue $\frac{\log(3)}{4}$ and $\frac{\log(3)}{8}$, respectively. Inserting this result into the expressions for $\Phi_{\Gamma,\mathsf{wr}}(s)$, we compute the residue at $s = 1$ to $\frac{\log(3)}{4\Sigma}$, where we have used that $\sigma = \Sigma$ if σ is odd and $\sigma = 2\Sigma$ if σ is even. □

Using similar arguments as in the proofs of Theorems 7.3.1 and 7.3.2, one can derive from Proposition 7.5.7 the asymptotic behaviour of the number of well-rounded sublattices as follows.

THEOREM 7.5.8. *Under the assumptions of Proposition 7.5.7, the summatory function $A_\Gamma(x) = \sum_{n \le x} a_\Gamma(n)$ possesses the asymptotic growth behaviour*

$$A_\Gamma(x) = \frac{\log(3)}{4\Sigma} x + \mathcal{O}\bigl(\sqrt{x}\bigr)$$

as $x \to \infty$. □

7.5.2. The rational case. A rational lattice Γ contains infinitely many BRS sublattices Γ_R. Using the same considerations as in the previous subsection, for any given pair $\pm R$ we can count the number of well-rounded sublattices invariant under $\pm R$ (that is, contained in $\widetilde{\Gamma}_R$). Counting all possible well-rounded sublattices then amounts to sum over all possible pairs $\pm R$. However, some care is needed in case of square and hexagonal lattices.

For convenience, we use the notation $\mathcal{R}_1 := \{\pm R \mid \widetilde{\Gamma}_R \nsubseteq \Gamma\}$ and $\mathcal{R}_2 := \{\pm R \mid \widetilde{\Gamma}_R \subseteq \Gamma\}$, which, by Lemma 7.5.3, is a partition of $\mathcal{R}$ into sets of odd and even index of Γ_R, which is reflected by the indices 1 and 2.

PROPOSITION 7.5.9. *Let Γ be a rational lattice and let $\Phi_\Gamma^{\triangle}(s)$ be the generating function of all hexagonal sublattices of Γ. Now, for any pair of coincidence reflections $\pm R \in \mathcal{R}_\Gamma$, let*

$\sigma(R) = [\varGamma : \varGamma_R]$ and let $\kappa(R)$ be the length ratio of orthogonal basis vectors of $\varGamma_R$. Then, the generating function for the number of well-rounded sublattices reads

$$\begin{aligned}\Phi_{\varGamma,\mathsf{wr}}(s) &= \sum_{\pm R\in\mathcal{R}_1} \frac{1}{\sigma(R)^s}\, \phi_{\mathsf{wr},\text{even}}(\kappa(R); s) \\ &+ \sum_{\pm R\in\mathcal{R}_2} \frac{1}{\sigma(R)^s} \big(\phi_{\mathsf{wr},\text{even}}(\kappa(R); s) + 2^s \phi_{\mathsf{wr},\text{odd}}(\kappa(R); s)\big) \\ &- 2\Phi^{\triangle}_{\varGamma}(s),\end{aligned} \tag{7.36}$$

where $\phi_{\mathsf{wr},\text{even}}(\kappa; s)$ and $\phi_{\mathsf{wr},\text{odd}}(\kappa; s)$ are as in Proposition 7.5.6.

Keep in mind that we sum over pairs of coincidence reflections $\pm R$ here. According to Lemma 7.5.1, we could alternatively sum over BRS sublattices or rational orthogonal frames. Furthermore, note that $\Phi^{\triangle}_{\varGamma}(s) = 0$ unless $\varGamma$ is commensurate to a hexagonal lattice.

Before proving Proposition 7.5.9, let us have a closer look at some special cases.

Remark 7.5.4. If $\varGamma$ is not commensurate to a square or a hexagonal lattice, all well-rounded sublattices are rhombic. Likewise, all CSLs $\varGamma(R)$ generated by a reflection are either rectangular or rhombic-cr. In fact, there exists a bijection between BRS sublattices $\varGamma_R$ and the corresponding CSLs $\varGamma(R)$, which implies that the summation in Eq. (7.36) could be carried out over CSLs as well. In particular, $\mathcal{R}_1 = \mathcal{R}_{\text{rec}} := \{\pm R \mid \varGamma(R) \text{ rectangular}\}$ and $\mathcal{R}_2 = \mathcal{R}_{\text{rh-cr}} := \{\pm R \mid \varGamma(R) \text{ rhombic-cr}\}$ by Lemma 7.5.3.

The case that $\varGamma$ is commensurate to a hexagonal lattice is the only one where the additional term $-2\Phi^{\triangle}_{\varGamma}(s)$ is non-trivial, which compensates for the fact that the sum over $\pm R \in \mathcal{R}_2$ counts every hexagonal sublattice thrice. Here, we do not have the bijection between the BRS sublattices $\varGamma_R$ and CSLs $\varGamma(R)$ any more, and the sums cannot be replaced by sums over CSLs. Still, we have a characterisation of the sets $\mathcal{R}_1$ and $\mathcal{R}_2$ via CSLs, namely $\mathcal{R}_1 = \mathcal{R}_{\text{rec}} := \{\pm R \mid \varGamma(R) \text{ rectangular}\}$ and $\mathcal{R}_2 = \mathcal{R}_{\text{rh-cr-hex}} := \{\pm R \mid \varGamma(R) \text{ rhombic-cr or hexagonal}\}$.

If $\varGamma$ is commensurate to a square lattice, no simple characterisation of $\mathcal{R}_1$ and $\mathcal{R}_2$ via CSLs is possible. This is due to the fact that square CSLs may appear both in $\mathcal{R}_1$ and in $\mathcal{R}_2$.

Proof of Proposition 7.5.9. As indicated above, counting all well-rounded sublattices that are invariant under a given pair $\pm R$ (that is, contained in $\widetilde{\varGamma}_R$) gives a contribution

$$\frac{1}{\sigma(R)^s}\, \phi_{\mathsf{wr},\text{even}}\big(\kappa(R); s\big)$$

if $\widetilde{\varGamma}_R \not\subseteq \varGamma$, and

$$\frac{1}{\sigma(R)^s}\Big(\phi_{\mathsf{wr},\text{even}}\big(\kappa(R); s\big) + 2^s \phi_{\mathsf{wr},\text{odd}}\big(\kappa(R); s\big)\Big)$$

if $\widetilde{\varGamma}_R \subseteq \varGamma$. If $\varGamma$ is not commensurate to a hexagonal or a square lattice, every well-rounded sublattice is of rhombic type and belongs to a unique pair $\pm R$ of coincidence reflections. Thus, summing over all pairs $\pm R$ immediately gives the result in this case.

The situation is more complex for lattices that are commensurate to a hexagonal or a square lattice, since some well-rounded sublattices may be of hexagonal or square type, respectively, and hence there may be more than one pair $\pm R$ of coincidence reflections associated with it. The rhombic well-rounded sublattices may still be treated in the same way as above, but the hexagonal and square sublattices need extra care.

A hexagonal sublattice corresponds to exactly three pairs of coincidence reflections. Thus we count the hexagonal lattices thrice if we sum over all pairs of coincidence reflections, which we compensate by subtracting the term $2\Phi^{\triangle}_{\varGamma}(s)$.

Similarly, a square sublattice $\varLambda$ is invariant under two pairs $\pm R, \pm S$ of coincidence reflections. However, these two pairs play different roles, as exactly one of these pairs, say $\pm S$, has eigenvectors which form a reduced basis of $\varLambda$. This implies that $\varLambda$ is only counted in the set of rhombic and square lattices which emerge from $\varGamma_R$. Hence, we have a unique pair $\pm R$ in this case as well, and no correction term is needed here. □

THEOREM 7.5.10. *For any rational lattice $\varGamma$, the generating function $\Phi_{\varGamma,\mathsf{wr}}(s)$ has an analytic continuation to the half plane $\{\mathrm{Re}(s) > \frac{1}{2}\}$ except for a pole of order 2 at $s = 1$. Hence there exists a constant $c > 0$ such that the asymptotic growth rate, as $x \to \infty$, is*

$$A_{\varGamma}(x) = \sum_{n \le x} a_{\varGamma}(n) \sim cx \log(x).$$

PROOF. We have already shown that $\phi_{\mathsf{wr,even}}(\kappa; s)$ and $\phi_{\mathsf{wr,odd}}(\kappa; s)$ are analytic in the half plane $\{\mathrm{Re}(s) > \frac{1}{2}\}$ except for $s = 1$, where both functions have a simple pole. The same holds true for $\Phi^{\triangle}_{\varGamma}(s)$. It thus remains to analyse the sums over the pairs of coincidence reflections in Proposition 7.5.9. By Lemma 7.5.1, summing over all pairs of coincidence reflections is equivalent to summing over all four-element subsets $\{\pm w, \pm z\}$ of primitive orthogonal lattice vectors. Since these sets are disjoint, we can as well sum over all primitive vectors in $\varGamma$, obtaining each summand exactly four times. As earlier, we denote by $\varGamma_w$ the BRS-sublattice corresponding to $\{\pm w, \pm z\}$, and we define $\sigma(w) := [\varGamma : \varGamma_w]$, the index of $\varGamma_w$ in $\varGamma$. Finally, we use the notation $\kappa(w) = \frac{|w|}{|z|}$ for the quantity κ introduced in Remark 7.5.2. We thus obtain

$$\begin{aligned}\Phi_{\varGamma,\mathsf{wr}}(s) - 2\Phi^{\triangle}_{\varGamma}(s) \;=\;& \frac{1}{4} \sum_{\substack{w \text{ primitive} \\ \sigma(w) \text{ odd}}} \frac{1}{\sigma(w)^s}\, \phi_{\mathsf{wr,even}}(\kappa(w); s) \\ &+ \frac{1}{4} \sum_{\substack{w \text{ primitive} \\ \sigma(w) \text{ even}}} \frac{1}{\sigma(w)^s} \left(\phi_{\mathsf{wr,even}}(\kappa(w); s) + 2^s \phi_{\mathsf{wr,odd}}(\kappa(w); s)\right),\end{aligned}$$

where the factor $\frac{1}{4}$ reflects the four elements of $\{\pm w, \pm z\}$, as observed above.

From now on, we assume w.l.o.g. that $\varGamma$ is integral and primitive. Then, by Proposition 7.C.1 of Appendix 7.C, we have $\sigma(w) = \frac{(w,w)}{g^*(w)}$, and $\kappa(w) = \frac{g^*(w)}{\sqrt{d}}$, where d is the discriminant of $\varGamma$ and $g^*(w)$ is the coefficient of w in $\varGamma^*$. By Proposition 7.C.1, $g^*(w)$ is a divisor of d, and can therefore take only a finite number of distinct values. As a consequence, also $\kappa(w)$ takes only finitely many values. Moreover, $g^*(w)$ and $\kappa(w)$ are constant on the cosets of an appropriate sublattice of $\varGamma$. Accordingly, we can subdivide the above summation into finitely many sums of simpler type.

To work this out explicitly, we choose a basis $\{v_1, v_2\}$ of $\varGamma^*$ such that $\{v_1, dv_2\}$ is a basis of $\varGamma$, as in Appendix 7.C. Using the quadratic form $Q(m,n) := |mv_1 + ndv_2|^2$, and similarly the notation $g^*(m,n) := g^*(mv_1{+}ndv_2)$, $\sigma(m,n) := \sigma(mv_1{+}ndv_2)$ and $\kappa(m,n) := \kappa(mv_1{+}ndv_2)$, for $(m,n) \in \mathbb{Z}^2$, we have $g^*(m,n) = \gcd(m,d)$ and $\sigma(m,n) = \frac{Q(m,n)}{g^*(m,n)}$, by formula (7.48), assuming $\gcd(m,n) = 1$. It follows from Proposition 7.C.2 that the parity of $\sigma(m,n)$ only depends on $\gcd(m,D)$ and $\gcd(n,2)$, where $D = \operatorname{lcm}(2,d)$, and if the residues $m \bmod D$ and $n \bmod 2$ are fixed, the index $\sigma(m,n)$ only depends on $Q(m,n)$. Hence,

$$\begin{aligned}
\Phi_{\varGamma,\mathsf{wr}}(s) - 2\Phi_{\varGamma}^{\triangle}(s) &= \frac{1}{4} \sum_{\gcd(m,n)=1} \frac{\gcd(m,d)^s}{Q(m,n)^s} \\
&\qquad \times \bigl(\phi_{\mathsf{wr,even}}(\kappa(m,n);s) + \delta_\sigma(m,n)\, 2^s \phi_{\mathsf{wr,odd}}(\kappa(m,n);s)\bigr) \\
&= \frac{1}{4} \sum_{k|D} \sum_{\ell|2} \bigl(\phi_{\mathsf{wr,even}}(\kappa(k,\ell);s) + \delta_\sigma(k,\ell)\, 2^s \phi_{\mathsf{wr,odd}}(\kappa(k,\ell);s)\bigr) \\
&\qquad \times \sum_{\substack{\gcd(m,n)=1 \\ \gcd(m,D)=k \\ \gcd(n,2)=\ell}} \frac{\gcd(k,d)^s}{Q(m,n)^s} \, ,
\end{aligned}$$

where δ_σ is defined by

$$\delta_\sigma(m,n) := \begin{cases} 1 & \text{if } \sigma(m,n) \text{ is even} \\ 0 & \text{if } \sigma(m,n) \text{ is odd} \end{cases}$$

and depends on $\gcd(m,D)$ and $\gcd(n,2)$, only. By Remark 7.5.3, both $\phi_{\mathsf{wr,even}}(\kappa(k,\ell);s)$ and $\phi_{\mathsf{wr,odd}}(\kappa(k,\ell);s)$ are analytic in the open half plane $\{\operatorname{Re}(s) > \frac{1}{2}\}$ except for $s = 1$, where both have a simple pole. Invoking Appendix 7.D, this is true of

$$\sum_{\substack{\gcd(m,n)=1 \\ \gcd(m,D)=k \\ \gcd(n,2)=\ell}} \frac{1}{Q(m,n)^s}$$

as well, which shows that $\Phi_{\varGamma,\mathsf{wr}}(s) - 2\Phi_{\varGamma}^{\triangle}(s)$, and thus $\Phi_{\varGamma,\mathsf{wr}}(s)$, has a pole of order 2 at $s = 1$ and is analytic elsewhere in $\{\operatorname{Re}(s) > \frac{1}{2}\}$, as claimed. The asymptotic behaviour now follows from an application of Delange's theorem; compare Theorem 7.A.1. □

At this stage, it remains an open question whether, in the general rational case, the growth rate behaves as $c_1 x \log(x) + c_2 x + \mathcal{O}(x)$, like for the square and hexagonal lattices.

Appendix 7.A. Some useful results from analytic number theory

In what follows, we summarise some results from analytic number theory that we need to determine certain asymptotic properties of the coefficients of Dirichlet series generating functions. For the general background, we refer to [**1**] and [**30**].

Consider a Dirichlet series of the form $F(s) = \sum_{m=1}^{\infty} a(m) m^{-s}$. We are interested in the summatory function $A(x) = \sum_{m \leq x} a(m)$ and its behaviour for large x. Let us give one classic result for the case that $a(m)$ is real and non-negative.

Theorem 7.A.1. *Let $F(s)$ be a Dirichlet series with non-negative coefficients which converges for $\mathrm{Re}(s) > \alpha > 0$. Suppose that $F(s)$ is holomorphic at all points of the line $\{\mathrm{Re}(s) = \alpha\}$ except at $s = \alpha$. Here, when approaching α from the half-plane to the right of it, we assume $F(s)$ to have a singularity of the form $F(s) = g(s) + h(s)/(s-\alpha)^{n+1}$ where n is a non-negative integer, and both $g(s)$ and $h(s)$ are holomorphic at $s = \alpha$. Then, as $x \to \infty$, we have*

$$A(x) \;:=\; \sum_{m \leq x} a(m) \;\sim\; \frac{h(\alpha)}{\alpha \cdot n!}\, x^{\alpha} \left(\log(x)\right)^{n}. \tag{7.37}$$

The proof follows easily from Delange's theorem, for instance by taking $q = 0$ and $\omega = n$ in Tenenbaum's formulation of it; see [**28**, ch. II.7, Thm. 15] and references given there.

The critical assumption in Theorem 7.A.1 is the behaviour of $F(s)$ along the line $\{\mathrm{Re}(s) = \alpha\}$. In all cases where we apply it, this can be checked explicitly. To do so, we have to recall a few properties of the Riemann zeta function $\zeta(s)$, and of the Dedekind zeta functions of imaginary quadratic fields.

It is well-known that $\zeta(s)$ is a meromorphic function in the complex plane, and that it has a sole simple pole at $s = 1$ with residue 1; see [**1**, Thm. 12.5(a)]. It has no zeros in the half-plane $\{\mathrm{Re}(s) \geq 1\}$; compare [**28**, ch. II.3, Thm. 9]. The values of $\zeta(s)$ at positive even integers are known [**1**, Thm. 12.17] and we have

$$\zeta(2) \;=\; \frac{\pi^2}{6}. \tag{7.38}$$

This is all we need to know for this case.

Let us now consider an imaginary quadratic field K, written as $K = \mathbb{Q}(\sqrt{d}\,)$ with $d < 0$ squarefree. The corresponding discriminant is

$$D \;=\; \begin{cases} 4d, & \text{if } d \equiv 2, 3 \bmod 4, \\ d, & \text{if } d \equiv 1 \bmod 4, \end{cases}$$

see [**30**, §10] for more. We need the Dedekind zeta function of K (with fundamental discriminant $D < 0$). It follows from [**30**, §11, Eq. (10)] that it can be written as

$$\zeta_K(s) \;=\; \zeta(s) \cdot L(s, \chi_D) \tag{7.39}$$

where $L(s, \chi_D) = \sum_{m=1}^{\infty} \chi_D(m)\, m^{-s}$ is the L-series [**1**, Ch. 6.8] of the primitive Dirichlet character χ_D. The latter is a totally multiplicative arithmetic function, and thus completely specified by

$$\chi_D(p) \;=\; \bigl(\frac{D}{p}\bigr), \tag{7.40}$$

for odd primes, where $\bigl(\frac{D}{p}\bigr)$ is the usual Legendre symbol, together with

$$\Bigl(\frac{D}{2}\Bigr) \;=\; \begin{cases} 0, & \text{if } D \equiv 0 \bmod 4, \\ 1, & \text{if } D \equiv 1 \bmod 8, \\ -1, & \text{if } D \equiv 5 \bmod 8. \end{cases}$$

$L(s,\chi_D)$ is an entire function [**1**, Thm. 12.5]. Consequently, $\zeta_K(s)$ is meromorphic, and its only pole is simple and located at $s=1$. The residue is $L(1,\chi_D)$, and from [**30**, §9, Thm. 2] we get the simple formula

$$L(1,\chi_D) \;=\; -\frac{\pi}{|D|^{3/2}} \sum_{n=1}^{|D|-1} n\,\chi_D(n). \tag{7.41}$$

In particular, for the two fields $\mathbb{Q}(\mathrm{i})$ and $\mathbb{Q}(\rho)$, one has the values $\pi/4$ and $\pi/3\sqrt{3}$, respectively.

Our next goal is an estimate on sums of the form $\sum_{\ell<n<\alpha\ell} n^{-s}$ for $\ell \in \mathbb{N}$, $\alpha > 1$ and $s > 0$. Invoking Euler's summation formula from [**1**, Thm. 3.1], one has

$$\sum_{\ell<n\le\alpha\ell} \frac{1}{n^s} \;=\; \int_\ell^{\alpha\ell} \frac{\mathrm{d}x}{x^s} - \int_\ell^{\alpha\ell} \bigl(x-[x]\bigr)\,\frac{s\,\mathrm{d}x}{x^{s+1}} \;+\; \frac{[\alpha\ell]-\alpha\ell}{(\alpha\ell)^s} \;-\; \frac{[\ell]-\ell}{\ell^s}. \tag{7.42}$$

The last term vanishes (since $\ell \in \mathbb{N}$), while the second last does whenever $\alpha\ell \in \mathbb{N}$ (otherwise, it is negative). Since the second integral on the right hand side is strictly positive (due to $\alpha > 1$), we see that

$$\sum_{\ell<n<\alpha\ell} \frac{1}{n^s} \;\le\; \sum_{\ell<n\le\alpha\ell} \frac{1}{n^s} \;<\; I_s \;:=\; \int_\ell^{\alpha\ell} \frac{\mathrm{d}x}{x^s} \;=\; \frac{1-\alpha^{1-s}}{s-1}\,\ell^{1-s}. \tag{7.43}$$

Observing next (once again due to $\alpha > 1$) that

$$\int_\ell^{\alpha\ell} \bigl(x-[x]\bigr)\,\frac{s\,\mathrm{d}x}{x^{s+1}} \;<\; \frac{1}{\ell^s} \;-\; \frac{1}{(\alpha\ell)^s},$$

one can separately consider the two cases $\alpha\ell \notin \mathbb{N}$ and $\alpha\ell \in \mathbb{N}$ to verify that we always get

$$\sum_{\ell<n<\alpha\ell} \frac{1}{n^s} > I_s - \frac{1}{\ell^s}.$$

This can immediately be generalised to sums of the form $\sum_{\ell<n<\alpha\ell+\beta} (n+\gamma)^{-s}$ with $\beta,\gamma \ge 0$, which we summarise as follows.

LEMMA 7.A.2. *Let $\ell \in \mathbb{N}$, $\alpha > 1$, $\beta \ge 0$ and $0 \le \gamma < 1$. If $s \ge 0$, one has the estimate*

$$I_s - \frac{1}{(\ell+\gamma)^s} \;<\; \sum_{\ell<n<\alpha\ell+\beta} \frac{1}{(n+\gamma)^s} \;<\; I_s,$$

with the integral $I_s = \int_\ell^{\alpha\ell+\beta} \frac{\mathrm{d}x}{(x+\gamma)^s}$ as the generalisation of that in Eq. (7.43). □

Let us finally mention that

$$\frac{1-\alpha^{1-s}}{s-1} \;=\; \log(\alpha) \sum_{m\geq 0} \frac{\bigl(\log(\alpha)(1-s)\bigr)^m}{(m+1)!},$$

so that this function is analytic in the entire complex plane. In particular, one has the asymptotic expression $\frac{1-\alpha^{1-s}}{s-1} = \log(\alpha) + \mathcal{O}\bigl(|1-s|\bigr)$ for $s \to 1$.

Appendix 7.B. Asymptotics of similar sublattices

We have sketched how to determine the asymptotics of the number of well-rounded sublattices of the square and hexagonal lattices. As a by-product of these calculations, and as a refinement of the results from [**4**], we obtain the asymptotics of the number of similar and primitive similar sublattices as follows.

THEOREM 7.B.1. *The asymptotics of the number of similar and of primitive similar sublattices of the square lattice is given by*

$$\sum_{n\leq x} b_{\square}(n) \;=\; L(1,\chi_{-4})\, x + \mathcal{O}\bigl(\sqrt{x}\,\bigr) \;=\; \frac{\pi}{4}\, x + \mathcal{O}\bigl(\sqrt{x}\,\bigr) \tag{7.44}$$

and

$$\sum_{n\leq x} b_{\square}^{\mathsf{pr}}(n) \;=\; \frac{L(1,\chi_{-4})}{\zeta(2)}\, x + \mathcal{O}\bigl(\sqrt{x}\log(x)\bigr) \;=\; \frac{3}{2\pi}\, x + \mathcal{O}\bigl(\sqrt{x}\log(x)\bigr). \tag{7.45}$$

SKETCH OF PROOF. Note that $b_{\square}(n) = (\chi_{-4} * 1)(n)$. We now get the asymptotics of its summatory function by an application of Eq. (7.24). Observe $b_{\square}^{\mathsf{pr}} = \nu * b_{\square}$, where $\nu(n) := \mu(\sqrt{n})$ is defined to be 0 if n is not a square and μ is the Moebius function. An application of Eq. (7.23) then yields the result. □

Similarly, one proves the following result.

THEOREM 7.B.2. *The asymptotics of the number of similar and of primitive similar sublattices of the hexagonal lattice is given by*

$$\sum_{n\leq x} b_{\triangle}(n) \;=\; L(1,\chi_{-3})\, x + \mathcal{O}\bigl(\sqrt{x}\,\bigr) \;=\; \frac{\pi}{3\sqrt{3}}\, x + \mathcal{O}\bigl(\sqrt{x}\,\bigr) \tag{7.46}$$

and

$$\sum_{n\leq x} b_{\triangle}^{\mathsf{pr}}(n) = \frac{L(1,\chi_{-3})}{\zeta(2)}\, x + \mathcal{O}\bigl(\sqrt{x}\log(x)\bigr) = \frac{2}{\pi\sqrt{3}}\, x + \mathcal{O}\bigl(\sqrt{x}\log(x))), \tag{7.47}$$

as $x \to \infty$. □

Appendix 7.C. The index of BRS sublattices

Let us complement the discussion of rational orthogonal frames and BRS sublattices as introduced in Lemma 7.5.1. We start with an arbitrary rational, primitive, planar lattice Γ and denote by $(v,w) \in \mathbb{Z}$ with $v, w \in \Gamma$ the given positive definite integer-valued primitive symmetric bilinear form on Γ, extended to the rational space $\mathbb{Q}\Gamma$. Primitivity means that the form is not a proper integral multiple of another form; it is equivalent to the condition that $\gcd(a,b,c) = 1$, where $G = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ is the Gram matrix with respect to an arbitrary basis v_1, v_2 of Γ.

In the following, we need the notion of the *coefficient* $g_\Gamma(v)$ of an arbitrary vector $v \in \mathbb{Q}\Gamma$ with respect to Γ. This is the unique positive rational number g such that $v = gv_0$, where $v_0 \in \Gamma$ is primitive in Γ. Equivalently, $g_\Gamma(v)$ is the unique positive generator of the rank one $\mathbb{Z}$-submodule of $\mathbb{Q}$ consisting of all $q \in \mathbb{Q}$ such that $q^{-1}v \in \Gamma$. So, a vector v is primitive in Γ if and only if $g_\Gamma(v) = 1$, in accordance with the first definition. Still another description of $g_\Gamma(v)$ is the gcd (taken in $\mathbb{Q}$) of the coefficients of v with respect to an arbitrary $\mathbb{Z}$-basis of Γ. Below, we shall use the coefficient $g^* := g_{\Gamma^*}$ in particular with respect to the dual lattice $\Gamma^* := \{w \in \mathbb{Q}\Gamma \mid \forall v \in \Gamma : (v,w) \in \mathbb{Z}\}$.

For an arbitrary primitive vector $w \in \Gamma$, we recall the notation Γ_w for the BRS sublattice spanned by w and its orthogonal sublattice $w^\perp \cap \Gamma$, i.e. by w and z, where z is the primitive lattice vector orthogonal to w (unique up to sign). The main result of this appendix is to compute the index of $\Gamma_w \in \Gamma$ as follows.

Proposition 7.C.1. *Let w be a primitive vector in a planar lattice Γ with primitive symmetric bilinear form, let $g^*(w)$ denote its coefficient in the dual lattice $\Gamma^* \subseteq \Gamma$. Then, $g^*(w)$ is a divisor of the discriminant d of the lattice, and*

$$[\Gamma : \Gamma_w] \;=\; \frac{(w,w)}{g^*(w)}\,.$$

Proof. The first claim follows easily from the fact that d is equal to the order of the factor group Γ^*/Γ, but it is also a consequence of the following computation leading to a proof of the second claim. Since w is primitive, we can complement it to a basis $v_1 = w, v_2$ of Γ. Consider the dual basis v_1^*, v_2^* with respect to the given scalar product; it is a $\mathbb{Z}$-basis of Γ^*. Writing the above vector z as $z = sv_1^* + tv_2^*$ with $s, t \in \mathbb{Z}$ clearly leads to $s = 0$, and t is the smallest integer such that $tv_2^* \in \Gamma$. If G is the Gram matrix with respect to v_1, v_2 as above, then G is also the transformation matrix which expresses the original basis vectors v_1, v_2 in terms of their dual vectors, in particular $v_1 = av_1^* + bv_2^*$, which shows that the coefficient of $w = v_1$ in Γ^* is

$$g^*(w) \;=\; \gcd(a,b).$$

On the other hand, with $d := ac - b^2$,

$$G^{-1} \;=\; \frac{1}{d}\begin{pmatrix} c & -b \\ -b & a \end{pmatrix}$$

is the transformation matrix expressing the dual basis in terms of the original basis. In particular

$$v_2^* = \frac{1}{d}(-bv_1 + av_2),$$

which implies that

$$t = \frac{d}{\gcd(a,b)}.$$

To compute the index of Γ_w in Γ, we use the bases v_1, v_2 of Γ and v_1, tv_2^* of Γ_w. The corresponding transformation matrix is $\begin{pmatrix} 1 & -\frac{b}{d}t \\ 0 & \frac{a}{d}t \end{pmatrix}$, which has determinant

$$\frac{a}{d}t = \frac{a}{d}\frac{d}{\gcd(a,b)} = \frac{a}{g^*(w)},$$

as claimed. □

Since the vector w was assumed primitive in Γ, it is even true that $g^*(w)$ is a divisor of the exponent of the factor group Γ^*/Γ. But from the primitivity of the bilinear form it follows that this factor group is actually cyclic of order d, so its exponent is equal to d, and we do not get an improvement: all divisors of the discriminant d can occur as a value $g^*(w)$.

It is easy to see that the quantity $g^*(w)$ only depends on an appropriate coset of w; in fact, under the assumptions of the last proposition, the coset modulo $d\Gamma^*$ suffices. For purposes of reference, we state this as an explicit remark.

Remark 7.C.1. Under the assumptions of Proposition 7.C.1, let w, w' be primitive such that $w \equiv w' \pmod{d\Gamma^*}$. Then, $g^*(w) = g^*(w')$.

For explicit computations involving g^*, it is convenient to use a basis corresponding to the elementary divisors of Γ in Γ^*, that is, a basis $\{v_1, v_2\}$ of Γ^* such that $\{v_1, dv_2\}$ is a basis of Γ. The primitive vectors in Γ read $w = mv_1 + ndv_2$ with $\gcd(m,n) = 1$. Using $g := \gcd(m,d)$, we can rewrite this as $w = g((m/g)v_1 + n(d/g)v_2)$, where the coefficients m/g and $n(d/g)$ are coprime, in other words, $(m/g)v_1 + n(d/g)v_2$ is primitive in Γ^*. This proves

$$g^*(mv_1 + ndv_2) = \gcd(m,d), \quad \text{if } \gcd(m,n) = 1. \tag{7.48}$$

Notice that this formula again proves Remark 7.C.1.

For our application to well-rounded sublattices, we also have to consider the parity of the index $[\Gamma : \Gamma_w]$. For this, we need the following refinement of Remark 7.C.1.

Proposition 7.C.2. *Under the assumptions of Proposition 7.C.1, let w, w' be primitive such that $w \equiv w' \pmod{d\Gamma^*}$ and $w \equiv w' \pmod{2\Gamma}$. Then, $[\Gamma : \Gamma_w] \equiv [\Gamma : \Gamma_{w'}] \pmod 2$.*

Proof. The proof is of course based on Proposition 7.C.1, taking into account that, under our assumptions, $g := g^*(w) = g^*(w')$, by Remark 7.C.1. First of all, recall that g divides d. Now, we write $w' = w + u = w + du'$ with $u' \in \Gamma^*$ and $u \in 2\Gamma$, and we compute explicitly

$$\frac{(w',w')}{g} = \frac{(w,w)}{g} + 2\frac{d}{g}(w,u') + \frac{d}{g}(u,u') \equiv \frac{(w,w)}{g} \pmod 2.$$

Notice that the last inner product (u,u') is indeed in $2\mathbb{Z}$, since $u \in 2\Gamma$ and $u' \in \Gamma^*$. □

Appendix 7.D. Epstein's ζ-function

For a quadratic form $Q(m,n) = am^2 + 2bmn + cn^2$, the Epstein ζ-function is defined as

$$\zeta_Q(s) := \sum_{(m,n)\neq(0,0)} \frac{1}{Q(m,n)^s}, \tag{7.49}$$

where the sum runs over all non-zero vectors $(m,n) \in \mathbb{Z}^2$. The series converges in the half plane $\{\mathrm{Re}(s) > 1\}$. It has an analytic continuation which is a meromorphic function in the whole complex plane with a single simple pole at $s = 1$ with residue $\frac{\pi}{\sqrt{d}}$, where $d = ac - b^2$ as before; see [**17, 25**]. It is closely connected to

$$\zeta_Q^{\mathsf{pr}}(s) := \sum_{(m,n)=1} \frac{1}{Q(m,n)^s} = \frac{1}{\zeta(2s)}\,\zeta_Q(s), \tag{7.50}$$

where the sum runs over all pairs of integers that are relatively prime. In the explicit summations, we now use (m,n) instead of $\gcd(m,n)$.

In Section 7.5.2, we need the sum

$$\sum_{\substack{(m,n)=1\\(m,D)=k\\(n,C)=\ell}} \frac{1}{Q(m,n)^s}, \tag{7.51}$$

where C, D, k, ℓ are some fixed positive integers with k, ℓ relatively prime. Using the Moebius μ-function, we can express

$$\sum_{\substack{(m,n)=1\\(m,D)=k\\(n,C)=\ell}} \frac{1}{Q(m,n)^s} = \sum_{\substack{(m,n)=1\\(m,\ell D/k)=1\\(n,kC/\ell)=1}} \frac{1}{Q(km,\ell n)^s} = \sum_{c\,|\,\frac{\ell D}{k}} \mu(c)\,\varphi_Q\left(c\frac{kC}{\ell}; ck, \ell; s\right) \tag{7.52}$$

in terms of

$$\varphi_Q(a;k,\ell;s) := \sum_{\substack{(m,n)=1\\(n,a)=1}} \frac{1}{Q(km,\ell n)^s}. \tag{7.53}$$

As $Q(m,n)$ is homogeneous of degree 2, we have

$$\varphi_Q(a;kb,\ell b;s) = \frac{1}{b^{2s}}\,\varphi_Q(a;k,\ell;s). \tag{7.54}$$

Furthermore, observe that $\varphi_Q(a;k,\ell;s) = \varphi_Q(b;k,\ell;s)$, whenever a and b have the same prime factors. In particular, we may assume that a is squarefree in the following. Using the same methods as above, we can derive the following recursion

$$\varphi_Q(a;k,\ell;s) = \sum_{b|a} \sum_{c\,|\,\frac{a}{b}} \mu(c) \frac{1}{b^{2s}}\,\varphi_Q(b;k,c\ell;s), \tag{7.55}$$

where we have made use of the assumption that a is squarefree and employed the multiplicativity of μ. This recursion has the solution

$$\varphi_Q(a;k,\ell;s) \;=\; \left(\prod_{p|a}\frac{1}{1-p^{-2s}}\right)\left(\sum_{b|a}\mu(b)\,\varphi_Q(1;k,b\ell;s)\right), \tag{7.56}$$

where the product is taken over all primes p dividing a. As $\varphi_Q(1;k,b\ell;s)$ is the primitive Epstein ζ-function $\zeta^{\mathsf{pr}}_{\tilde{Q}}(s)$ corresponding to the quadratic form $\tilde{Q}(m,n) = Q(km,b\ell n)$, this shows that $\varphi_Q(a;k,\ell;s)$ and thus

$$\sum_{\substack{(m,n)=1\\(m,D)=k\\(n,C)=\ell}}\frac{1}{Q(m,n)^s}$$

are sums of Epstein zeta functions, and thus are meromorphic functions with a simple pole at $s=1$ and analytic elsewhere in $\{\mathrm{Re}(s)>\frac{1}{2}\}$.

Alternatively, we can obtain this result by an application of Theorem 3 in [**25**]; see also [**19**]. Applied to our situation, it states that

$$\psi_Q(D,C,i,j;s) \;:=\; \sum_{\substack{m\equiv i(D)\\n\equiv j(C)}}\frac{1}{Q(m,n)^s} \tag{7.57}$$

has an analytic continuation, which is analytic in the entire complex plane except for a simple pole at $s=1$ with residue $\frac{\pi}{\sqrt{\det(Q')}}$, where $Q'(m,n) := Q(Dm,Cn)$. Using methods similar to those in [**3, 24**], we first observe for k,ℓ coprime

$$\begin{aligned}\sum_{\substack{(m,n)=1\\(m,D)=k\\(n,C)=\ell}}\frac{1}{Q(m,n)^s} &= \sum_{\substack{(m,D)=k\\(n,C)=\ell}}\frac{1}{Q(m,n)^s}\sum_{r|(m,n)}\mu(r)\\ &= \sum_{r\in\mathbb{N}}\mu(r)\frac{1}{r^{2s}}\sum_{\substack{(rm,D)=k\\(rn,C)=\ell}}\frac{1}{Q(m,n)^s}\\ &= \sum_{u|k}\sum_{v|\ell}\sum_{\substack{r\in\mathbb{N}\\(r,CD)=1}}\frac{\mu(uvr)}{(uvr)^{2s}}\sum_{\substack{(uvrm,D)=k\\(uvrn,C)=\ell}}\frac{1}{Q(m,n)^s}\,.\end{aligned}$$

As r is coprime with C and D we see that

$$\sum_{\substack{(uvrm,D)=k\\(uvrn,C)=\ell}}\frac{1}{Q(m,n)^s} \;=\; \sum_{\substack{(vm,D/u)=k/u\\(un,C/v)=\ell/v}}\frac{1}{Q(m,n)^s} \tag{7.58}$$

is independent of r. Moreover, the latter sum can be written as a (finite) sum of suitable functions of the form $\psi_Q(D,C,i,j;s)$ and therefore it is analytic in the entire complex plane except for a simple pole at $s = 1$. As u, v, r are coprime, $\mu(uvr) = \mu(u)\mu(v)\mu(r)$, and hence the only remaining infinite sum

$$\sum_{\substack{r \in \mathbb{N} \\ (r,CD)=1}} \frac{\mu(r)}{r^{2s}} = \frac{1}{\zeta(2s)} \prod_{p|CD} \frac{1}{1-p^{2s}} \tag{7.59}$$

is analytic in $\{\mathrm{Re}(s) > \frac{1}{2}\}$, which again shows that

$$\sum_{\substack{(m,n)=1 \\ (m,D)=k \\ (n,C)=\ell}} \frac{1}{Q(m,n)^s}$$

is a meromorphic function with a simple pole at $s = 1$ and analytic elsewhere in $\{\mathrm{Re}(s) > \frac{1}{2}\}$.

Acknowledgements

The authors thank S. Akiyama, J. Brüdern and L. Fukshansky for discussions, R. Schulze-Pillot for bringing Siegel's work on Epstein's zeta function to our attention, and S. Kühnlein for making [**18**] available to us prior to publication. This work was supported by the German Research Foundation (DFG), within the CRC 701.

Bibliography

1. T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York (1976).
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, Kluwer, Dordrecht (1997), 9–44; rev. version: `arXiv:math.MG/0605222`.
3. M. Baake, R.V. Moody and P.A.B. Pleasants, Diffraction from visible lattice points and kth power free integers, *Discr. Math.* **221** (200), 3–42; `arXiv:math/9906132`.
4. M. Baake and U. Grimm, Bravais colourings of planar modules with N-fold symmetry, *Z. Kristallogr.* **219** (2004), 72–80; `arXiv:math.CO/0301021`.
5. M. Baake, U. Grimm, M. Heuer and P. Zeiner, Coincidence rotations of the root lattice A_4, *Europ. J. Combin.* **29** (2008), 1808–1819; `arXiv:0709.1341`.
6. M. Baake, R. Scharlau and P. Zeiner, Similar sublattices of planar lattices, *Canad. J. Math.* **63** (2011), 1220–1237; `arXiv:0908.2558`.
7. I. Borevich and I. Shafarevich, *Number Theory*, translated by N. Greenleaf, Academic Press, New York (1966).
8. J. Brüdern, *Einführung in die analytische Zahlentheorie*, Springer, Berlin (1995).
9. C.J. Bushnell and I. Reiner, Zeta functions of arithmetic orders and Solomon's conjectures, *Math. Z.* **173** (1980), 135–161.
10. J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, 3^{rd} ed. Springer, New York (2010).
11. M. du Sautoy and F. Grunewald, Analytic properties of zeta functions and subgroup growth, *Ann. Math.* **152** (2000), 793–833.
12. L. Fukshansky, On distribution of well-rounded sublattices of $\mathbb{Z}^2$, *J. Number Th.* **128** (2008), 2359–2393.
13. L. Fukshansky, On well-rounded sublattices of the hexagonal lattice, *Discr. Math.* **310** (2010), 3287–3302.
14. L. Fukshansky, Well-rounded zeta-function of planar arithmetic lattices, *Proc. AMS* **142** (2014), 369–380.
15. F. Grunewald, D. Segal and G.C. Smith, Subgroups of finite index in nilpotent groups, *Invent. Math.* **93** (1988), 185–223.
16. M. Klemm, *Symmetrien von Ornamenten und Kristallen*, Springer, Berlin (1982).
17. M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen*, Springer, Berlin (2007).
18. S. Kühnlein, Well-rounded sublattices, *Int. J. Number Th.* **8** (2012), 1133–1144.
19. S. Kühnlein and R. Schwerdt, Well-rounded sublattices and twisted Epstein zeta functions, Preprint (2014).
20. A. Lubotzky and D. Segal, *Subgroup Growth*, Birkhäuser, Basel (2003).
21. J. Martinet, *Perfect Lattices in Euclidean Spaces*, Springer, Berlin (2010).
22. C. McMullen, Minkowski's conjecture, well-rounded lattices and topological dimension, *J. Amer. Math. Soc.* **18** (2005), 711–734.
23. P. Moree, Chebyshev's bias for composite numbers with restricted prime divisors, *Math. Comp.* **73** (2004), 425–449.
24. P.A.B. Pleasants and C. Huck, Entropy and diffraction of the k-free points in n-dimensional lattices, *Discr. Comput. Geom.* **50** (2013), 39–68; `arXiv:1112.1629`.
25. C.L. Siegel, *Advanced Analytic Number Theory*, Tata, Bombay (1980).
26. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten, Tokyo, and Princeton University Press, Princeton, NJ (1971).

27. L. Solomon, Zeta functions and integral representation theory, *Adv. Math.* **26** (1977), 306–326.

28. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, Cambridge (1995).

29. B.L. van der Waerden, Die Reduktionstheorie der positiven quadratischen Formen, *Acta Math.* **96** (1956), 265–309.

30. D.B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin (1981).

31. P. Zeiner, Coincidences of hypercubic lattices in 4 dimensions, *Z. Kristallogr.* **221** (2006), 105–114; `arXiv:math/0605526`.

32. P. Zeiner, Supplement to “Well-rounded sublattices of planar lattices”, available from the author, or as supplement to the `arXiv`-version.

33. Y.M. Zou, Structures of coincidence symmetry groups, *Acta Cryst. A* **62** (2006), 109–114.

CHAPTER 8

Supplement to “Well-rounded sublattices of planar lattices”

Abstract. Additional material to the article “Well-rounded sublattices of planar lattices”, including some calculations on the asymptotic behaviour of various arithmetic functions and some remarks on BRS lattices.

In this supplement we present the details of our calculations for the asymptotic growth rates of the number of well-rounded sublattices, which we have mentioned only briefly in our main article. In addition, we add some details on BRS lattices.

This supplement was initially intended for private use only, but it has been adapted for a wider audience now. Nevertheless, some parts are rather sketchy, and the explicit calculations vary in style, ranging from very detailed textbook-like calculations to rather short ones.

8.1. Explicit expressions for BRS lattices

In Section 7.5.1 we have discussed the existence of well-rounded lattices. In particular, Prop. 7.5.5 mentions all lattices that have well-rounded sublattices and distinguishes three cases. Here, we want to give explicit formulas for BRS lattices in all three cases.

Recall that BRS lattices correspond to basic solutions of the equation

$$ac + bdn + (ad + bc)\frac{t}{2} = 0, \tag{8.1}$$

where ‘*basic*’ means that $\gcd(a, b) = \gcd(c, d) = 1$. By symmetry, the number of basic solutions is a multiple of eight.

Using the same methods as in the proof of Prop. 7.5.5, we obtain the following results.

Remark 8.1.1. (1) n, t rational: we write $\tau = \frac{p}{q} + \mathrm{i}\beta$ with $\beta = \sqrt{\frac{r}{s}}$. Then $z_1 = a + b\tau$ and $z_2 = q^2 s\mathrm{i}\beta z_1$ yield an integral solution with $c = -(spqa + sp^2b + rq^2b), d = s(q^2a + pqb)$, albeit not necessarily a basic one. If z_1 is primitive, we get a basic solution by dividing z_2 by $g := \gcd\big(spqa + sp^2b + rq^2b, s(q^2a + pqb)\big)$.

(2) t rational, but n irrational: There are only eight basic solutions. If we write $t = 2\frac{p}{q}$ with $p, q \in \mathbb{Z}$ coprime, a basic one is $a = 1, b = 0, c = p, d = -q$.

(3) t irrational, with $n = \frac{p}{q} + \frac{r}{s}t$, where $q, r, s \in \mathbb{Z}\backslash\{0\}$ and $\sqrt{\frac{r^2}{s^2} + \frac{p}{q}} \in \mathbb{Q}$. There are eight basic solutions. If we define $\frac{u}{v} := \sqrt{\frac{r^2}{s^2} + \frac{p}{q}}$ a solution is given by $a = -b(\frac{r}{s} + \frac{u}{v}), b = \frac{sv}{\gcd(sv, rv+su)}, c = -d(\frac{r}{s} - \frac{u}{v}), d = \frac{sv}{\gcd(sv, rv-su)}$.

Clearly, eight basic solutions correspond to each BRS sublattice.

We have seen that two quantities play an important role for calculating the generating functions in the case of a unique BRS sublattice, namely the index $\sigma := [\Gamma : \Gamma_R]$ of this BRS sublattice and the ratio κ of the lengths of its orthogonal basis vectors. By means of the expressions for the BRS sublattices given above we can easily compute the values of σ and κ explicitly for these cases. We obtain the following result.

REMARK 8.1.2. The explicit values for σ and κ read as follows:

(1) n irrational, t rational with $\frac{t}{2} = \frac{p}{q}$: we have $\sigma = q, \kappa = q\sqrt{n - t^2/4}$.

(2) t irrational, with $n = \frac{p}{q} + \frac{r}{s}t$, where $q, r, s \in \mathbb{Z} \setminus \{0\}$ and $\frac{u}{v} := \sqrt{\frac{r^2}{s^2} + \frac{p}{q}} \in \mathbb{Q}$: we have

$$\sigma = \frac{2s^2uv}{\gcd(sv, rv + su)\gcd(sv, rv - su)}, \quad \kappa = \frac{\gcd(sv, rv - su)}{\gcd(sv, rv + su)} \frac{\sqrt{2rv + 2su - svt}}{\sqrt{-2rv + 2su + svt}}.$$

In the special case that n is rational, i.e. $n = \frac{p^2}{q^2}$ for some $p, q \in \mathbb{Z}$ coprime, the equations above simplify considerably: $\sigma = 2pq$, $\kappa = \sqrt{\frac{2\sqrt{n}-t}{2\sqrt{n}+t}}$.

8.2. Asymptotic behaviour — Introduction

Here, we calculate the asymptotic behaviour of certain arithmetic functions, in particular the functions counting well-rounded sublattices. We are interested in functions such as

$$A(x) = \sum_{n \le x} a(n). \tag{8.2}$$

The functions we are interested in are typically Dirichlet convolutions of simpler functions. If $f * g$ denotes the Dirichlet convolution, then

$$\sum_{n \le x} (f * g)(n) = \sum_{n \le x} \sum_{d|n} f(d) g(\tfrac{n}{d}) = \sum_{m \le x} \sum_{d \le x/m} f(m) g(d) \tag{8.3}$$

$$= \sum_{m \le \sqrt{x}} \sum_{m < d \le x/m} (f(m)g(d) + f(d)g(m)) + \sum_{m \le \sqrt{x}} f(m)g(m), \tag{8.4}$$

where the latter may allow for better error terms. [**Su-1**]

We often approximate sums by integrals using the Euler-Maclaurin formula

$$\sum_{y < n \le x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t - [t]) f'(t)\,dt + f(x)([x] - x) - f(y)([y] - y). \tag{8.5}$$

8.3. Similar Sublattices

8.3.1. Hexagonal lattice. The Dirichlet series generating function for the number of similar and primitive similar sublattices of $\mathbb{Z}[\rho]$ are

$$\Phi_{\triangle}(s) \;=\; \zeta_{\mathbb{Q}(\rho)}(s) \;=\; L(s,\chi_{-3})\zeta(s) \;=\; \sum_{n\in\mathbb{N}} \frac{b_{\triangle}(n)}{n^s} \tag{8.6}$$

$$\Phi^{\mathsf{pr}}_{\triangle}(s) \;=\; \frac{\zeta_{\mathbb{Q}(\rho)}(s)}{\zeta(2s)} \;=\; \frac{L(s,\chi_{-3})\zeta(s)}{\zeta(2s)} \;=\; \sum_{n\in\mathbb{N}} \frac{b^{\mathsf{pr}}_{\triangle}(n)}{n^s}, \tag{8.7}$$

respectively. We can immediately read off that

$$b_{\triangle} = 1 * \chi_{-3} \qquad\text{and}\qquad b^{\mathsf{pr}}_{\triangle} = 1 * \chi_{-3} * \nu = b_{\triangle} * \nu, \tag{8.8}$$

with the character

$$\chi_{-3}(n) \;=\; \begin{cases} 0, & \text{if } n \equiv 0 \bmod 3, \\ 1, & \text{if } n \equiv 1 \bmod 3, \\ -1, & \text{if } n \equiv 2 \bmod 3. \end{cases}$$

and

$$\nu(n) \;=\; \begin{cases} \mu(\sqrt{n}), & \text{if } n \text{ is a square}, \\ 0, & \text{otherwise}, \end{cases} \tag{8.9}$$

where μ is the Moebius function.

8.3.1.1. *Asymptotics of similar sublattices.* We apply Eq. (8.4) to $b_{\triangle} = 1 * \chi_{-3}$, which gives

$$\begin{aligned} \sum_{n\le x} b_{\triangle}(n) &= \sum_{m\le\sqrt{x}} \; \sum_{m<d\le x/m} \big(\chi_{-3}(d) + \chi_{-3}(m)\big) + \sum_{m\le\sqrt{x}} \chi_{-3}(m) \\ &= \sum_{m\le\sqrt{x}} \Big(O(1) + \chi_{-3}(m)\left(\left[\frac{x}{m}\right] - m\right)\Big) + O(1) \\ &= \sum_{m\le\sqrt{x}} \Big(O(1) + \chi_{-3}(m)\left(\frac{x}{m} - m\right)\Big) + O(1) \\ &= L(1,\chi_{-3})\, x + O(\sqrt{x}) = \frac{\pi}{3\sqrt{3}}\, x + O(\sqrt{x}). \end{aligned} \tag{8.10}$$

8.3.1.2. *Asymptotics of primitive similar sublattices.* As $b^{\mathsf{pr}}_{\triangle} = b_{\triangle} * \nu$, we can make use of Eq. (8.4) again.

$$\sum_{n\le x} b^{\mathsf{pr}}_{\triangle}(n) = \sum_{m\le\sqrt{x}} \; \sum_{m<d\le x/m} \big(\nu(m)\, b_{\triangle}(d) + \nu(d)\, b_{\triangle}(m)\big) + \sum_{m\le\sqrt{x}} \nu(m)\, b_{\triangle}(m) \tag{8.11}$$

The last term only contributes to the error term since

$$\left| \sum_{m\le\sqrt{x}} \nu(m)\, b_{\triangle}(m) \right| \le \sum_{m\le\sqrt{x}} b_{\triangle}(m) = O(\sqrt{x}) \tag{8.12}$$

by Eq. (8.10). The first term gives

(8.13)

$$\begin{aligned}\sum_{m\leq\sqrt{x}}\ \sum_{m<d\leq x/m}\nu(m)\,b_{\triangle}(d) &= \sum_{m\leq\sqrt{x}}\nu(m)\left(L(1,\chi_{-3})\left(\frac{x}{m}-m\right)+O\left(\sqrt{\frac{x}{m}}\right)+O(\sqrt{m})\right)\\ &= \frac{L(1,\chi_{-3})}{\zeta(2)}\,x+O(x^{3/4}) = \frac{2}{\pi\sqrt{3}}\,x+O(x^{3/4}),\end{aligned}$$

where we have made use of Eqs. (8.51)–(8.53). The second term yields

$$\begin{aligned}\sum_{m\leq\sqrt{x}}\ \sum_{m<d\leq x/m}\nu(d)\,b_{\triangle}(m) &= \sum_{m\leq\sqrt{x}} b_{\triangle}(m)\sum_{\sqrt{m}<\ell\leq\sqrt{x/m}}\mu(\ell)\\ &= \sum_{m\leq\sqrt{x}} b_{\triangle}(m)\left(O(\sqrt{m})+O\left(\sqrt{\frac{x}{m}}\right)\right)\\ &= O(x^{3/4}),\end{aligned} \tag{8.14}$$

where we have used Theorem 8.A.2. Thus

Lemma 8.3.1.

$$\sum_{n\leq x} b^{\mathsf{pr}}_{\triangle}(n) = \frac{2}{\pi\sqrt{3}}\,x+O(x^{3/4}). \tag{8.15}$$

Recall that ν is the arithmetic function corresponding to $\frac{1}{\zeta(2s)}$, which is analytic at $s=1$. So one might hope that this term should not influence the asymptotics too much, in particular as $\frac{1}{\zeta(2s)}$ has an abscissa of convergence of $\sigma=\frac{1}{2}$. The fact that only the first term in Eq. (8.11) contributes to the asymptotics supports this idea. In fact, using the simpler formula

$$\begin{aligned}\sum_{n\leq x} b^{\mathsf{pr}}_{\triangle}(n) &= \sum_{m\leq x}\ \sum_{d\leq x/m}\nu(m)\,b_{\triangle}(d)\\ &= \sum_{m\leq x}\nu(m)\left(L(1,\chi_{-3})\frac{x}{m}+O\left(\sqrt{\frac{x}{m}}\right)\right)\\ &= L(1,\chi_{-3})\,x\sum_{m\leq x}\nu(m)\frac{1}{m}+\sqrt{x}\sum_{\ell\leq\sqrt{x}}\mu(\ell)O\left(\frac{1}{\ell}\right)\\ &= \frac{L(1,\chi_{-3})}{\zeta(2)}\,x+L(1,\chi_{-3})\,xO(x^{-1/2})+\sqrt{x}\sum_{\ell\leq\sqrt{x}}O\left(\frac{1}{\ell}\right)\\ &= \frac{L(1,\chi_{-3})}{\zeta(2)}\,x+O(\sqrt{x}\log(x)) = \frac{2}{\pi\sqrt{3}}\,x+O(\sqrt{x}\log(x))\end{aligned}$$

gives a better result. Note that we have made use of Eq. (8.53) here. Thus

THEOREM 8.3.2. *The asymptotics of the number of similar and of primitive similar sublattices of the hexagonal lattice is given by*

$$\sum_{n\le x} b_{\triangle}(n) = L(1,\chi_{-3})\,x + O(\sqrt{x}) = \frac{\pi}{3\sqrt{3}}\,x + O(\sqrt{x}) \tag{8.16}$$

and

$$\sum_{n\le x} b^{\mathsf{pr}}_{\triangle}(n) = \frac{L(1,\chi_{-3})}{\zeta(2)}\,x + O(\sqrt{x}\log(x)) = \frac{2}{\pi\sqrt{3}}\,x + O(\sqrt{x}\log(x)). \tag{8.17}$$

8.3.2. Square lattice. The Dirichlet series generating function for the number of similar and primitive similar sublattices of $\mathbb{Z}[\rho]$ are

$$\Phi_{\square}(s) \;=\; \zeta_{\mathbb{Q}(i)}(s) \;=\; L(s,\chi_{-4})\zeta(s) \;=\; \sum_{n\in\mathbb{N}} \frac{b_{\square}(n)}{n^s} \tag{8.18}$$

$$\Phi^{\mathsf{pr}}_{\square}(s) \;=\; \frac{\zeta_{\mathbb{Q}(i)}(s)}{\zeta(2s)} \;=\; \frac{L(s,\chi_{-4})\zeta(s)}{\zeta(2s)} \;=\; \sum_{n\in\mathbb{N}} \frac{b^{\mathsf{pr}}_{\square}(n)}{n^s}, \tag{8.19}$$

respectively. We can immediately read off that

$$b_{\square} = 1 * \chi_{-4} \qquad\qquad \text{and} \qquad\qquad b^{\mathsf{pr}}_{\square} = 1 * \chi_{-4} * \nu = b_{\square} * \nu, \tag{8.20}$$

with the character

$$\chi_{-4}(n) \;=\; \begin{cases} 0, & \text{if } n \text{ even,} \\ 1, & \text{if } n \equiv 1 \bmod 4, \\ -1, & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

8.3.2.1. *Asymptotics of similar sublattices.* We apply Eq. (8.4) to $b_{\square} = 1 * \chi_{-4}$, which gives

$$\begin{aligned} \sum_{n\le x} b_{\square}(n) &= \sum_{m\le\sqrt{x}} \; \sum_{m<d\le x/m} \big(\chi_{-4}(d) + \chi_{-4}(m)\big) + \sum_{m\le\sqrt{x}} \chi_{-4}(m) \\ &= \sum_{m\le\sqrt{x}} \Big(O(1) + \chi_{-4}(m)\left(\left[\frac{x}{m}\right] - m\right)\Big) + O(1) \\ &= \sum_{m\le\sqrt{x}} \Big(O(1) + \chi_{-4}(m)\left(\frac{x}{m} - m\right)\Big) + O(1) \\ &= L(1,\chi_{-4})\,x + O(\sqrt{x}) = \frac{\pi}{4}\,x + O(\sqrt{x}). \end{aligned} \tag{8.21}$$

8.3.2.2. *Asymptotics of primitive similar sublattices.* A calculation similar to the hexagonal lattice gives

$$\begin{aligned}
\sum_{n\leq x} b^{\mathsf{pr}}_{\Box}(n) &= \sum_{m\leq x}\ \sum_{d\leq x/m} \nu(m)\, b_{\Box}(d)\\
&= \sum_{m\leq x} \nu(m) \left(L(1,\chi_{-4}) \frac{x}{m} + O\left(\sqrt{\frac{x}{m}}\right)\right)\\
&= L(1,\chi_{4})\, x \sum_{m\leq x} \nu(m) \frac{1}{m} + \sqrt{x} \sum_{\ell\leq\sqrt{x}} \mu(\ell) O\left(\frac{1}{\ell}\right)\\
&= \frac{L(1,\chi_{-4})}{\zeta(2)}\, x + L(1,\chi_{-4})\, x O(x^{-1/2}) + \sqrt{x} \sum_{\ell\leq\sqrt{x}} O\left(\frac{1}{\ell}\right)\\
&= \frac{L(1,\chi_{-4})}{\zeta(2)}\, x + O(\sqrt{x}\log(x)) = \frac{3}{2\pi}\, x + O(\sqrt{x}\log(x)),
\end{aligned}$$

where we have made use of Eq. (8.53). Thus we have proved

THEOREM 8.3.3. *The asymptotics of the number of similar and of primitive similar sublattices of the square lattice is given by*

$$\sum_{n\leq x} b_{\Box}(n) = L(1,\chi_{-4})\, x + O(\sqrt{x}) = \frac{\pi}{4}\, x + O(\sqrt{x}) \tag{8.22}$$

and

$$\sum_{n\leq x} b^{\mathsf{pr}}_{\Box}(n) = \frac{L(1,\chi_{-4})}{\zeta(2)}\, x + O(\sqrt{x}\log(x)) = \frac{3}{2\pi}\, x + O(\sqrt{x}\log(x)). \tag{8.23}$$

8.4. Well-rounded sublattices

8.4.1. Hexagonal lattice. In order to compute the number of well-rounded lattices we need the following functions

$$\sum_{n\in\mathbb{N}} \frac{w_{\triangle,even}(n)}{n^s} = \frac{1}{4^s} \sum_{p\in\mathbb{N}}\ \sum_{p<q<3p} \frac{1}{p^s q^s} \tag{8.24}$$

$$\sum_{n\in\mathbb{N}} \frac{w_{\triangle,odd}(n)}{n^s} = \sum_{k\in\mathbb{N}}\ \sum_{k<\ell<3k+1} \frac{1}{(2k+1)^s(2\ell+1)^s} \tag{8.25}$$

For $w_{\triangle,even}$ observe that $4pq \leq x$ together with $p < q$ means $p < \frac{\sqrt{x}}{2}$. Thus

$$
\begin{aligned}
\sum_{n\leq x} w_{\triangle,even}(n) &= \sum_{p<\sqrt{x}/2} \; \sum_{p<q\leq \min(3p-1,[x/(4p)])} 1 \\
&= \sum_{p<\sqrt{x}/2} \left(\min\left(3p-1, \left[\frac{x}{4p}\right]\right) - p \right) \\
&= \sum_{p\leq (1+\sqrt{1+3x})/6} (2p-1) + \sum_{(1+\sqrt{1+3x})/6<p<\sqrt{x}/2} \left(\left[\frac{x}{4p}\right] - p \right) \\
&= \left[\frac{1+\sqrt{1+3x}}{6}\right]^2 + \sum_{(1+\sqrt{1+3x})/6<p\leq\sqrt{x}/2} \left(\frac{x}{4p} - p + O(1) \right) \\
&= \frac{x}{12} + \frac{x}{4}\left(\log\left(\frac{\sqrt{x}}{2}\right) - \log\left(\frac{1+\sqrt{1+3x}}{6}\right)\right) - \frac{1}{2}\left(\frac{x}{4} - \frac{(1+\sqrt{1+3x})^2}{36}\right) + O(\sqrt{x}) \\
&= \frac{x}{8}\log(3) + O(\sqrt{x}).
\end{aligned}
\tag{8.26}
$$

Similarly we get for the odd indices — observe that $(2k+1)(2\ell+1) \leq x$ together with $k < \ell$ implies $k < \frac{\sqrt{x}-1}{2}$ —

$$
\begin{aligned}
\sum_{n\leq x} w_{\triangle,odd}(n) &= \sum_{k<(\sqrt{x}-1)/2} \; \sum_{k<\ell\leq \min(3k,[x/(4k+2)-1/2])} 1 \\
&= \sum_{k<(\sqrt{x}-1)/2} \left(\min\left(3k, \left[\frac{x}{4k+2} - \frac{1}{2}\right]\right) - k \right) \\
&= \sum_{k\leq(-1+\sqrt{4+3x})/6} 2k + \sum_{(-1+\sqrt{4+3x})/6<k<(\sqrt{x}-1)/2} \left(\left[\frac{x}{4k+2} - \frac{1}{2}\right] - k \right) \\
&= \frac{x}{12} + \frac{x}{4}\left(\log\left(\frac{\sqrt{x}}{2}\right) - \log\left(\frac{-1+\sqrt{4+3x}}{6}\right)\right) \\
&\qquad - \frac{1}{2}\left(\frac{(\sqrt{x}-1)^2}{4} - \frac{(-1+\sqrt{4+3x})^2}{36}\right) + O(\sqrt{x}) \\
&= \frac{x}{8}\log(3) + O(\sqrt{x}).
\end{aligned}
\tag{8.27}
$$

In total, this gives for $w_{\triangle} := w_{\triangle,even} + w_{\triangle,odd}$

$$
\sum_{n\leq x} w_{\triangle}(n) = \frac{x}{4}\log(3) + O(\sqrt{x}). \tag{8.28}
$$

The next step is to calculate

$$
\sum_{n\leq x} w_{\triangle} * b_{\triangle}(n) = \sum_{m\leq\sqrt{x}} \; \sum_{m<d\leq x/m} \big(w_{\triangle}(m)\, b_{\triangle}(d) + w_{\triangle}(d)\, b_{\triangle}(m) \big) + \sum_{m\leq\sqrt{x}} w_{\triangle}(m)\, b_{\triangle}(m)
$$

Note that both $w_\triangle$ and $b_\triangle$ are non-negative, so we can apply the asymptotic formulas for $w_\triangle$ and $b_\triangle$ also to the error terms. The first term gives

$$\begin{aligned}
&\sum_{m\le\sqrt{x}}\ \sum_{m<d\le x/m} w_\triangle(m)\, b_\triangle(d)\\
&\quad= \sum_{m\le\sqrt{x}} w_\triangle(m)\left(L(1,\chi_{-3})\frac{x}{m} + O\left(\sqrt{\frac{x}{m}}\right) - L(1,\chi_{-3})\, m + O(\sqrt{m})\right)\\
&\quad= L(1,\chi_{-3})x\left(\frac{\log(3)}{8}\log(x) + c_3\right) - L(1,\chi_{-3})\frac{\log(3)}{8}x + O(x^{3/4}\log(x)),\\
&\quad= L(1,\chi_{-3})x\left(\frac{\log(3)}{8}\log(x) + c_3 - \frac{\log(3)}{8}\right) + O(x^{3/4}\log(x)),
\end{aligned}$$

where we have used Eq. (8.16) and Theorem 8.A.3. The second term yields

$$\begin{aligned}
&\sum_{m\le\sqrt{x}}\ \sum_{m<d\le x/m} w_\triangle(d)\, b_\triangle(m)\\
&\quad= \sum_{m\le\sqrt{x}} b_\triangle(m)\left(\frac{x}{4m}\log(3) + O\left(\sqrt{\frac{x}{m}}\right) - \frac{m}{4}\log(3) + O(\sqrt{m})\right)\\
&\quad= \frac{\log(3)}{4}x\left(\frac{1}{2}L(1,\chi_{-3})\log(x) + C_\triangle(1) + O(x^{-1/4}\log(x))\right)\\
&\qquad - \frac{\log(3)}{4}\left(\frac{L(1,\chi_{-3})}{2}x + O(x^{3/4})\right)\\
&\quad= \frac{\log(3)}{8}x\left(L(1,\chi_{-3})\log(x) - L(1,\chi_{-3}) + 2C_\triangle(1)\right) + O(x^{3/4}\log(x)),
\end{aligned}$$

where we have used Eq. (8.28) and Theorem 8.A.2. The third term only contributes to the error term. Note that $w_\triangle(m) \le d(m)$, where $d(m)$ is the divisor function. As $d(m) = o(m^\varepsilon)$ for all $\varepsilon > 0$ (see [**Su-1**, p.296]) we see

$$\sum_{m\le\sqrt{x}} w_\triangle(m)\, b_\triangle(m) = \sum_{m\le\sqrt{x}} b_\triangle(m) o(m^\varepsilon) = O(x^{(1+\varepsilon)/2}). \tag{8.29}$$

Hence we get in total

$$\begin{aligned}
\sum_{n\le x} w_\triangle * b_\triangle(n) &= \frac{\log(3)}{4}L(1,\chi_{-3})x(\log(x)-1)\\
&\qquad + x\left(\frac{\log(3)}{4}C_\triangle(1) + L(1,\chi_{-3})c_3\right) + O(x^{3/4}\log(x)).
\end{aligned}$$

Taking the convolution with ν gives

$$\begin{aligned}
\sum_{n\leq x} w_{\triangle} * b^{\mathsf{pr}}_{\triangle}(n) &= \sum_{n\leq x} \nu * w_{\triangle} * b_{\triangle}(n) \\
&= \sum_{m\leq x} \sum_{d\leq x/m} \nu(m)(w_{\triangle} * b_{\triangle})(d) \\
&= \sum_{m\leq x} \nu(m)\Bigg(\frac{\log(3)}{4} L(1,\chi_{-3}) \frac{x}{m}(\log(x)-\log(m)-1) \\
&\qquad + \frac{x}{m}\left(\frac{\log(3)}{4} C_{\triangle}(1) + L(1,\chi_{-3})c_3\right) + O\left(\frac{x^{3/4}}{m^{3/4}}\log(x/m)\right)\Bigg) \\
&= \frac{\log(3)}{4}\frac{L(1,\chi_{-3})}{\zeta(2)} x(\log(x)-1) \\
&\qquad + x\left(-\frac{\log(3)}{2}\frac{L(1,\chi_{-3})\zeta'(2)}{\zeta(2)^2} + \frac{\log(3)}{4\zeta(2)} C_{\triangle}(1) + \frac{L(1,\chi_{-3})}{\zeta(2)} c_3\right) \\
&\qquad + O(x^{3/4}\log(x)),
\end{aligned}$$

where we have made use of Eqs. (8.53) and (8.54). Note that this has added an overall factor of $\frac{1}{\zeta(2)}$ and an additional linear term.

Now it remains to take the factor $\frac{3}{1+3^{-s}}$ into account and add the similar sublattices. Using Lemma 8.A.1, we get

Theorem 8.4.1. *Let $a_{\triangle}(n)$ be the number of well-rounded sublattices of the hexagonal lattice with index n. Then, the summatory function $A_{\triangle}(x) = \sum_{n\leq x} a_{\triangle}(n)$ possesses the asymptotic growth behaviour*

$$\begin{aligned}
A_{\triangle}(x) &= \frac{9\log(3)}{16}\frac{L(1,\chi_{-3})}{\zeta(2)} x(\log(x)-1) + c_{\triangle}x + O(x^{3/4}\log(x)) \\
&= \frac{3\sqrt{3}\log(3)}{8\pi} x(\log(x)-1) + c_{\triangle}x + O(x^{3/4}\log(x))
\end{aligned}\tag{8.30}$$

where

$$\begin{aligned}
c_{\triangle} &:= \frac{9\log(3)}{16\zeta(2)} C_{\triangle}(1) + \frac{9L(1,\chi_{-3})}{4\zeta(2)} c_3 - \frac{9\log(3)}{8}\frac{L(1,\chi_{-3})\zeta'(2)}{\zeta(2)^2} \\
&\qquad + \frac{9\log(3)^2}{64}\frac{L(1,\chi_{-3})}{\zeta(2)} + L(1,\chi_{-3}) \\
&= L(1,\chi_{-3}) + \frac{9\log(3)L(1,\chi_{-3})}{16\zeta(2)}\Bigg(\left(\gamma + \frac{L'(1,\chi_{-3})}{L(1,\chi_{-3})} - 2\frac{\zeta'(2)}{\zeta(2)}\right) + 2\gamma - \frac{\log(3)}{4} \\
&\qquad + \sum_{p=1}^{\infty}\frac{1}{p}\Bigg(\sum_{p<q\leq 3p-1}\frac{1}{q} - \log(3)\Bigg) + \sum_{k=0}^{\infty}\frac{4}{2k+1}\Bigg(\sum_{k<\ell\leq 3k}\frac{1}{2\ell+1} - \frac{1}{2}\log(3)\Bigg)\Bigg) \\
&\approx 0.4915036
\end{aligned}\tag{8.31}$$

is the coefficient of $(s-1)^{-1}$ *in the Laurent series of* $\sum_n \frac{a_\triangle(n)}{n^s}$ *around* $s=1$ *with* $C_\triangle(1)$ *and* c_3 *from Eqs.* (8.62) *and* (8.68)*, respectively.*

8.4.2. Square lattice. In order to compute the number of well-rounded lattices of the square lattice we need the following functions

$$\sum_{n\in\mathbb{N}} \frac{w_{\square,even}(n)}{n^s} = \frac{1}{2^s}\sum_{p\in\mathbb{N}}\ \sum_{p<q<\sqrt{3}p} \frac{1}{p^s q^s} \tag{8.32}$$

$$\sum_{n\in\mathbb{N}} \frac{w_{\square,odd}(n)}{n^s} = \sum_{k\in\mathbb{N}}\ \sum_{k<\ell<\sqrt{3}k+(\sqrt{3}-1)/2} \frac{1}{(2k+1)^s(2\ell+1)^s} \tag{8.33}$$

$$\sum_{n\in\mathbb{N}} \frac{w_{\square,odd,2}(n)}{n^s} = \frac{1}{1+2^{-s}}\sum_{k\in\mathbb{N}}\ \sum_{k<\ell<\sqrt{3}k+(\sqrt{3}-1)/2} \frac{1}{(2k+1)^s(2\ell+1)^s} \tag{8.34}$$

Obviously $w_{\square,odd,2} = g_2 * w_{\square,odd}$, where

$$g_2(n) = \begin{cases} (-1)^r & \text{if } n = 2^r \\ 0 & \text{otherwise.} \end{cases}$$

For $w_{\square,even}$ observe that $2pq \le x$ together with $p < q$ means $p < \sqrt{x/2}$. Thus

$$\begin{aligned}
\sum_{n\le x} w_{\square,even}(n) &= \sum_{p<\sqrt{x/2}}\ \sum_{p<q\le\min([p\sqrt{3}],[x/(2p)])} 1 \\
&= \sum_{p<\sqrt{x/2}} \left(\min\left([p\sqrt{3}], \left[\frac{x}{2p}\right]\right) - p\right) \\
&= \sum_{p\le\sqrt{x/(2\sqrt{3})}} ([p\sqrt{3}]-p) + \sum_{\sqrt{x/(2\sqrt{3})}<p<\sqrt{x/2}} \left(\left[\frac{x}{2p}\right]-p\right) \\
&= \sum_{p\le\sqrt{x/(2\sqrt{3})}} (p(\sqrt{3}-1)+O(1)) + \sum_{\sqrt{x/(2\sqrt{3})}<p<\sqrt{x/2}} \left(\frac{x}{2p}-p+O(1)\right) \\
&= \frac{\sqrt{3}-1}{4\sqrt{3}}x + \frac{x}{2}\left(\log\left(\sqrt{\frac{x}{2}}\right) - \log\left(\sqrt{\frac{x}{2\sqrt{3}}}\right)\right) - \frac{1}{2}\left(\frac{x}{2}-\frac{x}{2\sqrt{3}}\right) + O(\sqrt{x}) \\
&= \frac{x}{8}\log(3) + O(\sqrt{x}).
\end{aligned} \tag{8.35}$$

Similarly, we get for the odd indices — observe that $(2k+1)(2\ell+1) \le x$ together with $k<\ell$ implies $k < \frac{\sqrt{x}-1}{2}$ —

$$\sum_{n\le x} w_{\square,odd}(n) = \sum_{k<(\sqrt{x}-1)/2}\ \sum_{k<\ell\le\min([\sqrt{3}k+(\sqrt{3}-1)/2],[x/(4k+2)-1/2])} 1 \tag{8.36}$$

$$
\begin{aligned}
&= \sum_{k<(\sqrt{x}-1)/2} \left(\min\left(\left[\sqrt{3}k + \frac{\sqrt{3}-1}{2} \right], \left[\frac{x}{4k+2} - \frac{1}{2} \right] \right) - k \right) \\
&= \sum_{k\leq\sqrt{x}/(2\sqrt[4]{3})-1/2} \left[\sqrt{3}k + \frac{\sqrt{3}-1}{2} \right] \\
&\qquad + \sum_{(\sqrt{x}/(2\sqrt[4]{3})-1/2<k<(\sqrt{x}-1)/2} \left[\frac{x}{4k+2} - \frac{1}{2} \right] - \sum_{k<(\sqrt{x}-1)/2} k \\
&= \frac{x}{8} + \frac{x}{4}\left(\log\left(\frac{\sqrt{x}}{2} \right) - \log\left(\frac{\sqrt{x}}{2\sqrt[4]{3}} \right) \right) - \frac{x}{8} + O(\sqrt{x}) \\
&= \frac{x}{16}\log(3) + O(\sqrt{x}).
\end{aligned}
$$

The next step is to calculate

$$
\sum_{n\leq x} w_{\square,i} * b_{\square}(n) = \sum_{m\leq\sqrt{x}} \sum_{m<d\leq x/m} \big(w_{\square,i}(m)\, b_{\square}(d) + w_{\square,i}(d)\, b_{\square}(m) \big) + \sum_{m\leq\sqrt{x}} w_{\square,i}(m)\, b_{\square}(m)
$$

for $i \in \{even, odd\}$. Note that both $w_{\square,i}$ and $b_{\square}$ are non-negative, so we can apply the asymptotic formulas for $w_{\square,i}$ and $b_{\square}$ also to the error terms. The first term gives

$$
\begin{aligned}
&\sum_{m\leq\sqrt{x}} \sum_{m<d\leq x/m} w_{\square,even}(m)\, b_{\square}(d) \\
&\qquad = \sum_{m\leq\sqrt{x}} w_{\square,even}(m) \left(L(1,\chi_{-4})\frac{x}{m} + O\left(\sqrt{\frac{x}{m}} \right) - L(1,\chi_{-4})\, m + O(\sqrt{m}) \right) \\
&\qquad = L(1,\chi_{-4})x \left(\frac{\log(3)}{16}\log(x) + c_{even} \right) - L(1,\chi_{-4})\frac{\log(3)}{16}x + O(x^{3/4}\log(x)), \\
&\qquad = L(1,\chi_{-4})x \left(\frac{\log(3)}{16}\log(x) + c_{even} - \frac{\log(3)}{16} \right) + O(x^{3/4}\log(x)),
\end{aligned}
$$

where we have used Eq. (8.22) and Theorem 8.A.5. The second term yields

$$
\begin{aligned}
&\sum_{m\leq\sqrt{x}} \sum_{m<d\leq x/m} w_{\square,even}(d)\, b_{\square}(m) \\
&\qquad = \sum_{m\leq\sqrt{x}} b_{\square}(m) \left(\frac{x}{8m}\log(3) + O\left(\sqrt{\frac{x}{m}} \right) - \frac{m}{8}\log(3) + O(\sqrt{m}) \right) \\
&\qquad = \frac{\log(3)}{8}x \left(\frac{1}{2}L(1,\chi_{-4})\log(x) + C_{\square}(1) + O(x^{-1/4}\log(x)) \right) \\
&\qquad\qquad - \frac{\log(3)}{8}\left(\frac{L(1,\chi_{-4})}{2}x + O(x^{3/4}) \right) \\
&\qquad = \frac{\log(3)}{16}x \big(L(1,\chi_{-3})\log(x) - L(1,\chi_{-3}) + 2C_{\square}(1) \big) + O(x^{3/4}\log(x)),
\end{aligned}
$$

where we have used Eq. (8.35) and Theorem 8.A.4. The third term only contributes to the error term

$$\sum_{m\leq\sqrt{x}} w_{\square,even}(m)\, b_{\square}(m) = \sum_{m\leq\sqrt{x}} b_{\square}(m) o(m^{\varepsilon}) = O(x^{(1+\varepsilon)/2}), \tag{8.37}$$

which is shown by the same argument as in the hexagonal case. Hence we get in total

$$\begin{aligned}\sum_{n\leq x} w_{\square,even} * b_{\square}(n) &= \frac{\log(3)}{8} L(1,\chi_{-4}) x(\log(x)-1)\\ &\quad + x\left(\frac{\log(3)}{8} C_{\square}(1) + L(1,\chi_{-4}) c_{even}\right) + O(x^{3/4}\log(x)).\end{aligned}$$

Along the same lines we get

$$\begin{aligned}\sum_{n\leq x} w_{\square,odd} * b_{\square}(n) &= \frac{\log(3)}{16} L(1,\chi_{-4}) x(\log(x)-1)\\ &\quad + x\left(\frac{\log(3)}{16} C_{\square}(1) + L(1,\chi_{-4}) c_{odd}\right) + O(x^{3/4}\log(x)).\end{aligned}$$

Applying Lemma 8.A.1 we get

$$\begin{aligned}\sum_{n\leq x} w_{\square,odd,2} * b_{\square}(n) &= \frac{\log(3)}{24} L(1,\chi_{-4}) x(\log(x)-1)\\ &\quad + x\left(\frac{\log(3)}{24} C_{\square}(1) + \frac{2}{3} L(1,\chi_{-4}) c_{odd} + \frac{\log(2)\log(3)}{72} L(1,\chi_{-4})\right) + O(x^{3/4}\log(x)).\end{aligned}$$

Hence we get for $w_{\square} := w_{\square,even} + w_{\square,odd,2}$ the asymptotic behaviour

$$\begin{aligned}\sum_{n\leq x} w_{\square} * b_{\square}(n) &= \frac{\log(3)}{6} L(1,\chi_{-4}) x(\log(x)-1)\\ &\quad + x\left(\frac{\log(3)}{6} C_{\square}(1) + L(1,\chi_{-4}) c\right) + O(x^{3/4}\log(x)),\end{aligned}$$

where

$$\begin{aligned} c &= c_{even} + \frac{2}{3} c_{odd} + \frac{\log(2)\log(3)}{72}\\ &= \frac{\log(3)}{3}\left(\gamma - \frac{\log(3)}{8} - \frac{\log(2)}{12}\right) + \sum_{p=1}^{\infty} \frac{1}{2p}\left(\sum_{p<q<p\sqrt{3}} \frac{1}{q} - \frac{\log(3)}{2}\right)\\ &\quad + \frac{2}{3}\sum_{k=0}^{\infty} \frac{1}{2k+1}\left(\sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2} \frac{1}{2\ell+1} - \frac{1}{4}\log(3)\right)\\ &\approx -0.5250229. \end{aligned} \tag{8.38}$$

Taking the convolution with ν gives

$$\begin{aligned}\sum_{n\le x} w_\square * b_\square^{\mathsf{pr}}(n) &= \sum_{n\le x} \nu * w_\square * b_\square(n)\\ &= \sum_{m\le x}\ \sum_{d\le x/m} \nu(m)(w_\square * b_\square)(d)\\ &= \sum_{m\le x} \nu(m)\Bigg(\frac{\log(3)}{6}L(1,\chi_{-4})\frac{x}{m}(\log(x)-\log(m)-1)\\ &\qquad + \frac{x}{m}\left(\frac{\log(3)}{6}C_\square(1) + L(1,\chi_{-4})c\right) + O\left(\frac{x^{3/4}}{m^{3/4}}\log(x/m)\right)\Bigg)\\ &= \frac{\log(3)}{6}\frac{L(1,\chi_{-4})}{\zeta(2)}x(\log(x)-1)\\ &\qquad + x\left(-\frac{\log(3)}{3}\frac{L(1,\chi_{-3})\zeta'(2)}{\zeta(2)^2} + \frac{\log(3)}{6\zeta(2)}C_\square(1) + \frac{L(1,\chi_{-4})}{\zeta(2)}c\right)\\ &\qquad + O(x^{3/4}\log(x)),\end{aligned}$$

Finally, multiplying by a factor 2 and adding the similar sublattices yields

Theorem 8.4.2. *Let $a_\square(n)$ be the number of well-rounded sublattices of the square lattice with index n. Then, the summatory function $A_\square(x) = \sum_{n\le x} a_\square(n)$ possesses the asymptotic growth behaviour*

$$\begin{aligned}A_\square(x) &= \frac{\log(3)}{3}\frac{L(1,\chi_{-4})}{\zeta(2)}x(\log(x)-1) + c_\square x + O(x^{3/4}\log(x))\\ &= \frac{\log(3)}{2\pi}x(\log(x)-1) + c_\square x + O(x^{3/4}\log(x))\end{aligned} \tag{8.39}$$

where

$$\begin{aligned}c_\square &:= \frac{\log(3)}{3\zeta(2)}C_\square(1) + \frac{2L(1,\chi_{-4})}{\zeta(2)}c - \frac{2\log(3)}{3}\frac{L(1,\chi_{-4})\zeta'(2)}{\zeta(2)^2} + L(1,\chi_{-4})\\ &= \frac{L(1,\chi_{-4})}{\zeta(2)}\Bigg(\zeta(2) + \frac{\log(3)}{3}\left(\frac{L'(1,\chi_{-4})}{L(1,\chi_{-4})} + \gamma - 2\frac{\zeta'(2)}{\zeta(2)}\right) + \frac{\log(3)}{3}\left(2\gamma - \frac{\log(3)}{4} - \frac{\log(2)}{6}\right)\\ &\qquad + \sum_{p=1}^{\infty}\frac{1}{p}\left(\sum_{p<q<p\sqrt{3}}\frac{1}{q} - \frac{\log(3)}{2}\right)\\ &\qquad + \frac{4}{3}\sum_{k=0}^{\infty}\frac{1}{2k+1}\left(\sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2}\frac{1}{2\ell+1} - \frac{1}{4}\log(3)\right)\Bigg)\\ &\approx 0.6272237\end{aligned} \tag{8.40}$$

is the coefficient of $(s-1)^{-1}$ *in the Laurent series of* $\sum_n \frac{a_\square(n)}{n^s}$ *around* $s=1$ *with* $C_\square(1)$ *and* c *from Eqs.* (8.75) *and* (8.38)*, respectively.*

8.4.3. Lattices with exactly one BRS lattice (i.e., lattices with exactly one non-trivial CSL). In this case we need

$$\phi_{\mathsf{wr},even}(\kappa;s) = \sum_{n\in\mathbb{N}} \frac{w_{even}(\kappa,n)}{n^s} = \frac{1}{2^s}\sum_{p\in\mathbb{N}} \sum_{\frac{\kappa}{\sqrt{3}}p<q<\sqrt{3}\,\kappa\, p} \frac{1}{p^s q^s} \tag{8.41}$$

$$\phi_{\mathsf{wr},odd}(\kappa;s) = \sum_{n\in\mathbb{N}} \frac{w_{odd}(\kappa,n)}{n^s} = \sum_{k\in\mathbb{N}} \sum_{\frac{\kappa}{\sqrt{3}}(k+\frac12)-\frac12<\ell<\sqrt{3}\,\kappa\,(k+\frac12)-\frac12} \frac{1}{(2k+1)^s(2\ell+1)^s} \tag{8.42}$$

Here $\kappa\sqrt{3}\notin\mathbb{Q}$ and we may assume w.l.o.g. $\kappa\geq 1$. For w_{even} observe that $2pq\leq x$ together with $p<\frac{q\sqrt{3}}{\kappa}$ means $p<\sqrt{\frac{x\sqrt{3}}{2\kappa}}$ and thus

$$\begin{aligned}
\sum_{n\leq x} w_{even}(\kappa,n) &= \sum_{p<\sqrt{x\sqrt{3}/(2\kappa)}}\ \sum_{p\kappa/\sqrt{3}<q\leq\min([p\sqrt{3}\,\kappa],[x/(2p)])} 1\\
&= \sum_{p<\sqrt{x/(2\kappa\sqrt{3})}} \left(\frac{2p\kappa}{\sqrt{3}}+O(1)\right) + \sum_{\sqrt{x/(2\kappa\sqrt{3})}\leq p<\sqrt{x\sqrt{3}/(2\kappa)}} \left(\frac{x}{2p}-\frac{p\kappa}{\sqrt{3}}+O(1)\right)\\
&= \frac{x}{6}+\frac{x}{2}\log\left(\frac{\sqrt{x\sqrt{3}/(2\kappa)}}{\sqrt{x/(2\kappa\sqrt{3})}}\right) - \frac{\kappa}{2\sqrt{3}}\left(\frac{x\sqrt{3}}{2\kappa}-\frac{x}{2\kappa\sqrt{3}}\right)+O(\sqrt{x})\\
&= \frac{x}{4}\log 3+O(\sqrt{x}).
\end{aligned}$$

Note that the leading term is independent of κ.

Similarly, we get for the odd indices — observe that $(2k+1)(2\ell+1)\leq x$ together with $\frac{\kappa}{\sqrt{3}}(2k+1)<2\ell+1$ implies $k<\sqrt{\frac{x\sqrt{3}}{4\kappa}}-\frac12$ —

$$\begin{aligned}
\sum_{n\leq x} w_{odd}(\kappa,n) &= \sum_{k<\sqrt{x\sqrt{3}/(4\kappa)}-1/2}\ \sum_{\frac{\kappa}{\sqrt{3}}(k+\frac12)-\frac12<\ell\leq\min([\sqrt{3}\,\kappa\,(k+\frac12)-\frac12],[\frac{x}{4k+2}-\frac12])} 1\\
&= \sum_{k<\sqrt{x/(4\kappa\sqrt{3})}-1/2} \left(\frac{\kappa(2k+1)}{\sqrt{3}}+O(1)\right)\\
&\quad + \sum_{\sqrt{x/(4\kappa\sqrt{3})}-1/2\leq k<\sqrt{x\sqrt{3}/(4\kappa)}-1/2} \left(\frac{x}{4k+2}-\frac{\kappa}{\sqrt{3}}\left(k+\frac12\right)+O(1)\right)\\
&= \frac{x}{12}+\frac{x}{4}\log\left(\frac{\sqrt{x\sqrt{3}/(4\kappa)}}{\sqrt{x/(4\kappa\sqrt{3})}}\right) - \frac{\kappa}{2\sqrt{3}}\left(\frac{x\sqrt{3}}{4\kappa}-\frac{x}{4\kappa\sqrt{3}}\right)+O(\sqrt{x})\\
&= \frac{x}{8}\log 3+O(\sqrt{x}).
\end{aligned}$$

Taking the index of the (unique) BRS sublattice into account we finally get

PROPOSITION 8.4.3. *Let Γ be a lattice that has a well-rounded sublattice and assume that at least one of n and t is irrational. Let σ be the index of the BRS sublattice and κ be the ratio of the lengths of its orthogonal basis vectors. Let $a_\Gamma(n)$ denote the number of well-rounded sublattices of Γ with index n. Then, the summatory function $A_\Gamma(x) = \sum_{n\le x} a_\Gamma(n)$ possesses the asymptotic growth behaviour*

$$A_\Gamma(x) = \begin{cases} \frac{\log 3}{4\sigma} x + O(\sqrt{x}) & \text{if } \sigma \text{ is odd} \\ \frac{\log 3}{2\sigma} x + O(\sqrt{x}) & \text{if } \sigma \text{ is even.} \end{cases} \tag{8.43}$$

In particular, the leading term is independent of κ and depends on σ only.

Recall that the BRS sublattice is a CSL if and only if it has odd index (we do not have square sublattices in the present case). Hence, if Σ is the index of the unique non-trivial CSL, then $\sigma = \Sigma$ if σ is odd and $\sigma = 2\Sigma$ if σ is even. Thus we can reformulate our results as follows:

THEOREM 8.4.4. *Let Γ be a lattice that has a well-rounded sublattice and assume that at least one of n and t is irrational, i.e. Γ has exactly one non-trivial CSL. Let Σ be its index in Γ. Let $a_\Gamma(n)$ denote the number of well-rounded sublattices of Γ with index n. Then, the summatory function $A_\Gamma(x) = \sum_{n\le x} a_\Gamma(n)$ possesses the asymptotic growth behaviour*

$$A_\Gamma(x) = \frac{\log 3}{4\Sigma} x + O(\sqrt{x}). \tag{8.44}$$

Appendix 8.A. Some formulas

8.A.1. General formulas. We first cite some well-known formulas, see [**Su-1**, Theorem 3.2]. It is always to be understood that summation starts with $n = 1$.

$$\sum_{n\le y} n^s = \frac{1}{s+1}\, y^{s+1} + O(y^s) \qquad \text{for } s > 0 \tag{8.45}$$

$$\sum_{n\le y} \frac{1}{n^s} = \frac{1}{1-s} y^{1-s} + \zeta(s) + O(y^{-s}) \qquad \text{for } s > 0, s \neq 1 \tag{8.46}$$

$$\sum_{n\le y} \frac{1}{n} = \log(y) + \gamma + O\left(\frac{1}{y}\right), \tag{8.47}$$

where $\gamma \approx 0.57721566$ is the Euler-Mascheroni constant. We also need the following variant for sums over odd integers $n \geq 3$

$$\begin{aligned} \sum_{k\le y} \frac{1}{2k+1} &= \frac{1}{2}\log(2y+1) + \frac{1}{2}\gamma + \frac{1}{2}\log(2) - 1 + O\left(\frac{1}{y}\right) \\ &= \frac{1}{2}\log(y) + \frac{1}{2}\gamma + \log(2) - 1 + O\left(\frac{1}{y}\right). \end{aligned} \tag{8.48}$$

Furthermore, we need a formula involving the logarithm

$$\sum_{n\le y} \frac{\log(n)}{n} = \frac{1}{2}\log(y)^2 + \gamma_1 + O\left(\frac{\log(y)}{y}\right), \tag{8.49}$$

where

$$\gamma_1 = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{\log(k)}{k} - \frac{1}{2}\log(n)^2 \approx -0.07281585 \tag{8.50}$$

is the first Stieltjes constant.

Next we state some formulas involving the Moebius function. For $s > -\frac{1}{2}$,

$$\sum_{n\le y} \nu(n)\, n^s = \sum_{m\le\sqrt{y}} \mu(m)\, m^{2s} = O(y^{s+\frac{1}{2}}) \tag{8.51}$$

is a rough estimate, which is good enough for our purposes. This equation even holds for $s = -\frac{1}{2}$ as

$$\left|\sum_{n\le y} \nu(n)\, n^{-1/2}\right| = \left|\sum_{m\le\sqrt{y}} \mu(m)\, \frac{1}{m}\right| \le 1, \tag{8.52}$$

see [**Su-1**, Theorem 3.13] for a proof. For $s < -\frac{1}{2}$

$$\sum_{n\le y} \nu(n)\, n^s = \sum_{m\in\mathbb{N}} \mu(m)\, m^{2s} - \sum_{m>\sqrt{y}} \mu(m)\, m^{2s} = \frac{1}{\zeta(-2s)} + O(y^{s+\frac{1}{2}}). \tag{8.53}$$

In addition, we mention

$$\sum_{n\le y} \nu(n)\, \frac{\log(n)}{n^s} = 2\sum_{m\in\mathbb{N}} \mu(m)\, \frac{\log(m)}{m^{2s}} - 2\sum_{m>\sqrt{y}} \mu(m)\, \frac{\log(m)}{m^{2s}} = 2\frac{\zeta'(2s)}{\zeta(2s)^2} + O(y^{\frac{1}{2}-s}\log(y)), \tag{8.54}$$

which holds for $s > \frac{1}{2}$.

Finally we state

LEMMA 8.A.1. *Let f be an arithmetic function such that $\sum_{n\le x} f(n) = ax\log(x) + bx + O(x^\alpha \log(x))$ with $0 < \alpha < 1$ and*

$$g(n) = \begin{cases} (-1)^r & \textit{if } n = q^r \\ 0 & \textit{otherwise,} \end{cases}$$

where q is some fixed positive integer. Then

$$\sum_{n\le x} f * g(n) = \frac{q}{q+1}\,(ax\log(x) + bx) + \frac{q\log(q)}{(q+1)^2} ax + O(x^\alpha \log(x)). \tag{8.55}$$

8.A.2. Hexagonal lattice. In the following, k is always a positive integer.

8.A.2.1. *Formulas for χ_{-3}.* For $s>0$ we have

$$\sum_{n\le y}\chi_{-3}(n)=\left[\frac{y-1}{3}\right]-\left[\frac{y-2}{3}\right]=O(1) \tag{8.56}$$

$$\sum_{n\le y}\chi_{-3}(n)n^s=O(y^s) \tag{8.57}$$

$$\sum_{n\le y}\frac{\chi_{-3}(n)}{n^s}=\sum_{n\in\mathbb{N}}\frac{\chi_{-3}(n)}{n^s}-\sum_{y<n}\frac{\chi_{-3}(n)}{n^s}=L(s,\chi_{-3})+O\left(\frac{1}{y^s}\right) \tag{8.58}$$

$$\sum_{k<n\le y}\frac{\chi_{-3}(n)}{n^s}=\sum_{k<n}\frac{\chi_{-3}(n)}{n^s}+O\left(\frac{1}{y^s}\right)=O\left(\frac{1}{k^s}\right)+O\left(\frac{1}{y^s}\right) \tag{8.59}$$

8.A.2.2. *Formulas involving $b_\triangle$.* For $s>0$

$$\begin{aligned}\sum_{n\le y}b_\triangle(n)n^s&=\sum_{m\le\sqrt{y}}\sum_{m<d\le y/m}\big(\chi_{-3}(m)+\chi_{-3}(d)\big)(md)^s+\sum_{m\le\sqrt{y}}\chi_{-3}(m)m^{2s}\\&=\sum_{m\le\sqrt{y}}m^s\chi_{-3}(m)\frac{1}{s+1}\left(\frac{y^{s+1}}{m^{s+1}}-m^{s+1}\right)\\&\quad+\sum_{m\le\sqrt{y}}m^s\left(O\left(\frac{y^s}{m^s}\right)+O(m^s)\right)+O(y^s)\\&=\frac{1}{s+1}L(1,\chi_{-3})\,y^{s+1}+O(y^{s+\frac12})\end{aligned}$$

for $0<s<\frac12$

$$\begin{aligned}\sum_{n\le y}\frac{b_\triangle(n)}{n^s}&=\sum_{m\le\sqrt{y}}\sum_{m<d\le y/m}\frac{\chi_{-3}(m)+\chi_{-3}(d)}{(md)^s}+\sum_{m\le\sqrt{y}}\frac{\chi_{-3}(m)}{m^{2s}}\\&=\sum_{m\le\sqrt{y}}\frac{\chi_{-3}(m)}{m^s}\frac{1}{1-s}\left(\frac{y^{1-s}}{m^{1-s}}-m^{1-s}\right)\\&\quad+\sum_{m\le\sqrt{y}}\frac{1}{m^s}\left(O\left(\frac{y^{-s}}{m^{-s}}\right)+O(m^{-s})\right)+L(2s,\chi_{-3})+O\left(\frac{1}{y^s}\right)\\&=\frac{L(1,\chi_{-3})}{1-s}\,y^{1-s}+O(y^{1/2-s})\end{aligned}$$

for $\frac12<s<1$

$$\begin{aligned}\sum_{n\le y}\frac{b_\triangle(n)}{n^s}&=\sum_{m\le\sqrt{y}}\sum_{m<d\le y/m}\frac{\chi_{-3}(m)+\chi_{-3}(d)}{(md)^s}+\sum_{m\le\sqrt{y}}\frac{\chi_{-3}(m)}{m^{2s}}\\&=\sum_{m\le\sqrt{y}}\frac{\chi_{-3}(m)}{m^s}\left(\frac{1}{1-s}\frac{y^{1-s}}{m^{1-s}}+\zeta(s)+O\left(\frac{y^{-s}}{m^{-s}}\right)-\sum_{d=1}^{m}\frac{1}{d^s}\right)\end{aligned}$$

$$
\begin{aligned}
&+\sum_{m\le\sqrt{y}}\frac{1}{m^s}\left(\sum_{d=m+1}^{\infty}\frac{\chi_{-3}(d)}{d^s}+O\left(\frac{m^s}{y^s}\right)\right)+L(2s,\chi_{-3})+O\left(\frac{1}{y^s}\right)\\
&=\frac{L(1,\chi_{-3})}{1-s}\,y^{1-s}+C(s)+O(y^{1/2-s}),
\end{aligned}
$$

with

$$
C(s)=L(s,\chi_{-3})\zeta(s)-\sum_{m=1}^{\infty}\frac{\chi_{-3}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s}+\sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{d=m+1}^{\infty}\frac{\chi_{-3}(d)}{d^s}+L(2s,\chi_{-3}).
$$

The sums in $C(s)$ are Dirichlet series that converge for $\mathrm{Re}(s)>\frac{1}{2}$, and are thus analytic for $\mathrm{Re}(s)>\frac{1}{2}$. They converge absolutely for $\mathrm{Re}(s)>1$, and a reordering of terms shows that the last three terms add up to zero for $\mathrm{Re}(s)>1$, and hence due to the analyticity also for $\mathrm{Re}(s)>\frac{1}{2}$. Hence $C(s)=L(s,\chi_{-3})\zeta(s)$ and thus

$$
\sum_{n\le y}\frac{b_\triangle(n)}{n^s}=\frac{L(1,\chi_{-3})}{1-s}\,y^{1-s}+L(s,\chi_{-3})\zeta(s)+O(y^{1/2-s})
$$

for $\frac{1}{2}<s<1$. For $s=\frac{1}{2}$ the situation is a bit more tricky and we want to avoid logarithmic error terms. The only two difficult terms are

$$
\sum_{m\le\sqrt{y}}\frac{\chi_{-3}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s}\qquad\text{and}\qquad\sum_{m\le\sqrt{y}}\frac{1}{m^s}\sum_{d=m+1}^{\infty}\frac{\chi_{-3}(d)}{d^s}
$$

The first term

$$
\begin{aligned}
\sum_{m\le\sqrt{y}}\frac{\chi_{-3}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s}&=\sum_{k\le(\sqrt{y}-1)/3}\left(\left(\frac{1}{(3k+1)^s}-\frac{1}{(3k+2)^s}\right)\sum_{d=1}^{3k+1}\frac{1}{d^s}-\frac{1}{(3k+2)^{2s}}\right)\\
&\quad+O\left(\frac{1}{\sqrt{y}^s}\right)\sum_{d\le\sqrt{y}}\frac{1}{d^s}\\
&=\sum_{k\le(\sqrt{y}-1)/3}\left(\frac{1}{(3k+1)^s}\left(\frac{s}{3k+1}+O\left(\frac{1}{(3k+1)^2}\right)\right)\left(\frac{(3k+1)^{1-s}}{1-s}+O(1)\right)\right.\\
&\quad\left.-\frac{1}{(3k+2)^{2s}}\right)+O(y^{1/2-s})\\
&=\left(\frac{s}{1-s}-1\right)\sum_{k\le(\sqrt{y}-1)/3}\frac{1}{(3k+1)^{2s}}\\
&\quad+\sum_{k\le(\sqrt{y}-1)/3}O\left(\frac{1}{(3k+1)^{s+1}}\right)+O(y^{1/2-s})
\end{aligned}
$$

is seen to be bounded for $1 > s \geq \frac{1}{2}$ and so is the second term

$$\begin{aligned}\sum_{m\leq\sqrt{y}} \frac{1}{m^s} \sum_{d=m+1}^{\infty} \frac{\chi_{-3}(d)}{d^s} &= \sum_{0\leq k\leq(\sqrt{y}-1)/3} \sum_{j=1}^{3} \frac{1}{(3k+j)^s} \sum_{d=3k+j+1}^{\infty} \frac{\chi_{-3}(d)}{d^s} + O(y^{-s}) \\ &= \sum_{0\leq k\leq(\sqrt{y}-1)/3} \left(\frac{1}{(3k+1)^s} \frac{-2}{3(3k+2)^s} + \frac{1}{(3k+2)^s} \frac{1}{3(3k+4)^s} \right. \\ &\qquad \left. + \frac{1}{(3k+3)^s} \frac{1}{3(3k+4)^s} + O\left(\frac{1}{k^{1+2s}}\right)\right) + O(y^{-s}) \\ &= \sum_{0\leq k\leq(\sqrt{y}-1)/3} O\left(\frac{1}{k^{1+2s}}\right) + O(y^{-s})\end{aligned}$$

where we have made use of

$$\begin{aligned}\sum_{d=3k}^{\infty} \frac{\chi_{-3}(d)}{d^s} &= \sum_{d=3k+1}^{\infty} \frac{\chi_{-3}(d)}{d^s} \\ &= \sum_{\ell=k}^{\infty} \left(\frac{1}{(3\ell+1)^s} - \frac{1}{(3\ell+2)^s} \right) \\ &= \sum_{\ell=k}^{\infty} \frac{1}{(3\ell+1)^s} \left(\frac{s}{3\ell+1} + O\left(\frac{1}{(3\ell+1)^2}\right)\right) \\ &= \frac{1}{3(3k+1)^s} + O\left(\frac{1}{k^{1+s}}\right)\end{aligned}$$

and

$$\begin{aligned}\sum_{d=3k+2}^{\infty} \frac{\chi_{-3}(d)}{d^s} &= -\sum_{\ell=k}^{\infty} \left(\frac{1}{(3\ell+2)^s} - \frac{1}{(3\ell+4)^s} \right) \\ &= -\frac{2}{3(3k+2)^s} + O\left(\frac{1}{k^{1+s}}\right).\end{aligned}$$

Hence

$$\sum_{n\leq y} \frac{b_\triangle(n)}{n^{1/2}} = 2L(1,\chi_{-3})\, y^{1/2} + O(1).$$

For $s = 1$ we get

$$\begin{aligned}\sum_{n\leq y} \frac{b_\triangle(n)}{n} &= \sum_{m\leq\sqrt{y}} \sum_{m<d\leq y/m} \frac{\chi_{-3}(m) + \chi_{-3}(d)}{md} + \sum_{m\leq\sqrt{y}} \frac{\chi_{-3}(m)}{m^2} \\ &= \sum_{m\leq\sqrt{y}} \frac{\chi_{-3}(m)}{m} \left(\log\left(\frac{y}{m}\right) + \gamma + O\left(\frac{m}{y}\right) - \sum_{d=1}^{m} \frac{1}{d} \right) \\ &\quad + \sum_{m\leq\sqrt{y}} \frac{1}{m} \left(\sum_{d=m+1}^{\infty} \frac{\chi_{-3}(d)}{d} + O\left(\frac{m}{y}\right)\right) + L(2,\chi_{-3}) + O\left(\frac{1}{y}\right)\end{aligned}$$

$$= L(1, \chi_{-3}) \log(y) + C(1) + O(y^{-1/2} \log(y)),$$

with

$$\begin{aligned} C(1) &= L(1, \chi_{-3})\gamma - \sum_{m=1}^{\infty} \frac{\chi_{-3}(m)}{m} \left(\log(m) + \sum_{d=1}^{m} \frac{1}{d} \right) \\ &\quad + \sum_{m=1}^{\infty} \frac{1}{m} \sum_{d=m+1}^{\infty} \frac{\chi_{-3}(d)}{d} + L(2, \chi_{-3}) \\ &= L(1, \chi_{-3})\gamma - \sum_{m=1}^{\infty} \frac{\chi_{-3}(m)}{m} \log(m) = L(1, \chi_{-3})\gamma + L'(1, \chi_{-3}). \end{aligned}$$

by a similar argument as above.

For $s > 1$ we get

$$\begin{aligned} \sum_{n \le y} \frac{b_\triangle(n)}{n^s} &= \sum_{m \le \sqrt{y}} \sum_{m < d \le y/m} \frac{\chi_{-3}(m) + \chi_{-3}(d)}{(md)^s} + \sum_{m \le \sqrt{y}} \frac{\chi_{-3}(m)}{m^{2s}} \\ &= \sum_{m \le \sqrt{y}} \frac{\chi_{-3}(m)}{m^s} \left(\zeta(s) + \frac{1}{1-s} \frac{m^{s-1}}{y^{s-1}} + O\left(\frac{m^s}{y^s}\right) - \sum_{d=1}^{m} \frac{1}{d^s} \right) \\ &\quad + \sum_{m \le \sqrt{y}} \frac{1}{m^s} \left(\sum_{d=m+1}^{\infty} \frac{\chi_{-3}(d)}{d^s} + O\left(\frac{m^s}{y^s}\right) \right) + L(2s, \chi_{-3}) + O\left(\frac{1}{y^s}\right) \\ &= L(s, \chi_{-3})\zeta(s) + \frac{L(1, \chi_{-3})}{1-s} y^{1-s} + O(y^{-s/2}), \end{aligned}$$

where we again have used the identity

$$(8.60) \qquad -\sum_{m=1}^{\infty} \frac{\chi_{-3}(m)}{m^s} \sum_{d=1}^{m} \frac{1}{d^s} + \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{d=m+1}^{\infty} \frac{\chi_{-3}(d)}{d^s} + L(2s, \chi_{-3}) = 0.$$

Summarising we have

THEOREM 8.A.2.

$$(8.61) \qquad \sum_{n \le y} b_\triangle(n) n^{-s} = \begin{cases} \frac{L(1,\chi_{-3})}{1-s} y^{1-s} + O(y^{1/2-s}) & \textit{for } s < \frac{1}{2} \\ 2L(1, \chi_{-3})\, y^{1/2} + O(1) & \textit{for } s = \frac{1}{2} \\ \frac{L(1,\chi_{-3})}{1-s} y^{1-s} + L(s, \chi_{-3})\zeta(s) + O(y^{1/2-s}) & \textit{for } \frac{1}{2} < s < 1 \\ L(1, \chi_{-3}) \log(y) + C_\triangle(1) + O(y^{-1/2} \log(y)) & \textit{for } s = 1 \\ L(s, \chi_{-3})\zeta(s) + \frac{L(1,\chi_{-3})}{1-s} y^{1-s} + O(y^{-s/2}) & \textit{for } s > 1 \end{cases}$$

where

$$(8.62) \qquad C_\triangle(1) = L(1, \chi_{-3})\gamma + L'(1, \chi_{-3}) \approx 0.5716475.$$

Note that $L'(1,\chi_{-3})$ can be computed efficiently (see [**Su-2**] and references therein), in particular

$$\frac{L'(1,\chi_{-3})}{L(1,\chi_{-3})}=\log\left(\frac{2^{\frac{3}{4}}M\left(1,\cos(\frac{\pi}{12})\right)^2e^{\gamma}}{3}\right)=\log\left(\frac{2^4\pi^4e^{\gamma}}{3^{\frac{3}{2}}\Gamma\left(\frac{1}{3}\right)^6}\right), \tag{8.63}$$

where $M(x,y)$ is the arithmetic-geometric mean of x and y.

8.A.2.3. *Formulas for $w_{\triangle}$.* For $s>-1$ we have

$$\begin{aligned}
\sum_{n\le y}w_{\triangle,even}(n)n^s &= \sum_{p<\sqrt{y}/2}\ \sum_{p<q\le\min(3p-1,[y/(4p)])}(4pq)^s\\
&= \sum_{p\le(1+\sqrt{1+3y})/6}(4p)^s\sum_{p<q\le 3p-1}q^s+\sum_{(1+\sqrt{1+3y})/6<p<\sqrt{y}/2}(4p)^s\sum_{p<q\le[y/(4p)]}q^s\\
&= \sum_{p\le(1+\sqrt{1+3y})/6}(4p)^s\left(\frac{1}{s+1}p^{1+s}(3^{s+1}-1)+O(p^s)\right)\\
&\quad+\sum_{(1+\sqrt{1+3y})/6<p<\sqrt{y}/2}(4p)^s\left(\frac{1}{s+1}\left(\frac{y^{s+1}}{(4p)^{s+1}}-p^{s+1}\right)+O(p^s)+O\left(\frac{y^s}{p^s}\right)\right)\\
&= \frac{4^s(3^{s+1}-1)}{2(s+1)^2}\frac{(3y)^{s+1}}{6^{2s+2}}+O(y^{s+\frac{1}{2}})+O(1)\\
&\quad+\frac{y^{s+1}}{4(s+1)}\log\left(\frac{3\sqrt{y}}{1+\sqrt{1+3y}}\right)-\frac{4^s}{2(s+1)^2}\left(\frac{y^{s+1}}{2^{2s+2}}-\frac{(3y)^{s+1}}{6^{2s+2}}\right)\\
&= \frac{\log(3)}{8(s+1)}y^{s+1}+O(y^{s+\frac{1}{2}})+O(1).
\end{aligned}$$

Similarly (again for $s>-1$)

$$\begin{aligned}
\sum_{n\le y}w_{\triangle,odd}(n)n^s &= \sum_{k<(\sqrt{y}-1)/2}\ \sum_{k<\ell\le\min(3k,[y/(4k+2)-1/2])}(2k+1)^s(2\ell+1)^s\\
&= \sum_{k\le(-1+\sqrt{4+3y})/6}(2k+1)^s\sum_{k<\ell\le 3k}(2\ell+1)^s\\
&\quad+\sum_{(-1+\sqrt{4+3y})/6<k<(\sqrt{y}-1)/2}(2k+1)^s\sum_{k<\ell\le[y/(4k+2)-1/2]}(2\ell+1)^s\\
&= \sum_{k\le(-1+\sqrt{4+3y})/6}(2k+1)^s\frac{1}{2(s+1)}\underbrace{\left((6k+1)^{s+1}-(2k+1)^{s+1}\right)}_{(3^{s+1}-1)(2k+1)^{s+1}+O(k^s)}\\
&\quad+\sum_{(-1+\sqrt{4+3y})/6<k<(\sqrt{y}-1)/2}(2k+1)^s\times\\
&\quad\times\left(\frac{1}{2(s+1)}\left(\frac{y^{s+1}}{(2k+1)^{s+1}}-(2k+1)^{s+1}\right)+O(k^s)+O\left(\frac{y^s}{(2k+1)^s}\right)\right)\\
&= \frac{3^{s+1}-1}{8(s+1)^2}\frac{2^{2s+2}(3y)^{s+1}}{6^{2s+2}}+O(y^{s+\frac{1}{2}})+O(1)
\end{aligned}$$

$$\begin{aligned}
&+\frac{y^{s+1}}{4(s+1)}\log\left(\frac{3(\sqrt{y}-1)}{-1+\sqrt{4+3y}}\right)\\
&-\frac{1}{8(s+1)^2}\left(\frac{(\sqrt{y}-1)^{2s+2}}{2^{2s+2}}-\frac{(-1+\sqrt{4+3y})^{2s+2}}{6^{2s+2}}\right)\\
=&\ \frac{\log(3)}{8(s+1)}y^{s+1}+O(y^{s+\frac{1}{2}})+O(1),
\end{aligned}$$

and hence in total for $s>-1$

$$\sum_{n\leq y} w_{\triangle}(n)n^s=\sum_{n\leq y}\left(w_{\triangle,even}(n)+w_{\triangle,odd}(n)\right)n^s=\frac{\log(3)}{4(s+1)}y^{s+1}+O(y^{s+\frac{1}{2}})+O(1).$$

For $s=-1$ we get

$$\begin{aligned}
\sum_{n\leq y}\frac{w_{\triangle,even}(n)}{n}
&=\sum_{p<\sqrt{y}/2}\ \sum_{p<q\leq\min(3p-1,[y/(4p)])}\frac{1}{4pq}\\
&=\sum_{p\leq(1+\sqrt{1+3y})/6}\frac{1}{4p}\sum_{p<q\leq 3p-1}\frac{1}{q}+\sum_{(1+\sqrt{1+3y})/6<p<\sqrt{y}/2}\frac{1}{4p}\sum_{p<q\leq[y/(4p)]}\frac{1}{q}\\
&=\sum_{p\leq(1+\sqrt{1+3y})/6}\frac{1}{4p}\Bigg(\log(3)+\underbrace{\sum_{p<q\leq 3p-1}\frac{1}{q}-\log(3)}_{O\left(\frac{1}{p}\right)}\Bigg)\\
&\quad+\sum_{(1+\sqrt{1+3y})/6<p<\sqrt{y}/2}\frac{1}{4p}\left(\log\left(\frac{y}{4p^2}\right)+O\left(\frac{1}{p}\right)+O\left(\frac{p}{y}\right)\right)\\
&=\frac{\log(3)}{4}\left(\log\left(\frac{1+\sqrt{1+3y}}{6}\right)+\gamma+O(y^{-1/2})\right)\\
&\quad+\underbrace{\sum_{p=1}^{\infty}\frac{1}{4p}\left(\sum_{p<q\leq 3p-1}\frac{1}{q}-\log(3)\right)}_{=:\,c_1}+O(y^{-1/2})\\
&\quad+\frac{\log(y)-2\log(2)}{4}\log\left(\frac{3\sqrt{y}}{1+\sqrt{1+3y}}\right)\\
&\quad-\frac{1}{4}\left(\left(\log\left(\frac{\sqrt{y}}{2}\right)\right)^2-\left(\log\left(\frac{1+\sqrt{1+3y}}{6}\right)\right)^2\right)+O(y^{-1/2}\log(y))\\
&=\frac{\log(3)}{8}\log(y)+\frac{\log(3)}{4}\left(\gamma-\frac{1}{4}\log(3)-\log(2)\right)+c_1+O(y^{-1/2}\log(y)).
\end{aligned}$$

where we have made use of

$$\left(\log\left(\frac{\sqrt{y}}{2}\right)\right)^2-\left(\log\left(\frac{1+\sqrt{1+3y}}{6}\right)\right)^2=\log\left(\frac{3\sqrt{y}}{1+\sqrt{1+3y}}\right)\log\left(\frac{\sqrt{y}(1+\sqrt{1+3y})}{12}\right)$$

$$= \frac{\log(3)}{2}\left(\log(y) - \frac{1}{2}\log(3) - 2\log(2)\right) + O(y^{-1/2}\log(y))$$

Similarly

$$\begin{aligned}
\sum_{n\le y}\frac{w_{\triangle,odd}(n)}{n} &= \sum_{k<(\sqrt{y}-1)/2}\ \sum_{k<\ell\le\min(3k,[y/(4k+2)-1/2])}\frac{1}{(2k+1)(2\ell+1)}\\
&= \sum_{k\le(-1+\sqrt{4+3y})/6}\frac{1}{2k+1}\sum_{k<\ell\le 3k}\frac{1}{2\ell+1}\\
&\quad+\sum_{(-1+\sqrt{4+3y})/6<k<(\sqrt{y}-1)/2}\frac{1}{2k+1}\sum_{k<\ell\le[y/(4k+2)-1/2]}\frac{1}{2\ell+1}\\
&= \sum_{k\le(-1+\sqrt{4+3y})/6}\frac{1}{2k+1}\left(\frac{1}{2}\log(3)+\underbrace{\sum_{k<\ell\le 3k}\frac{1}{2\ell+1}-\frac{1}{2}\log(3)}_{O\left(\frac{1}{k}\right)}\right)\\
&\quad+\sum_{(-1+\sqrt{4+3y})/6<k<(\sqrt{y}-1)/2}\frac{1}{2k+1}\left(\frac{1}{2}\log\left(\frac{y}{(2k+1)^2}\right)+O\left(\frac{1}{k}\right)+O\left(\frac{k}{y}\right)\right)\\
&= \frac{1}{2}\log(3)\left(\frac{1}{2}\log\left(\frac{-1+\sqrt{4+3y}}{6}\right)+\frac{1}{2}\gamma+\log(2)-1+O(y^{-1/2})\right)\\
&\quad+\underbrace{\sum_{k=1}^{\infty}\frac{1}{2k+1}\left(\sum_{k<\ell\le 3k}\frac{1}{2\ell+1}-\frac{1}{2}\log(3)\right)}_{=:\,c_2+\frac{1}{2}\log(3)}+O(y^{-1/2})\\
&\quad+\frac{\log(y)}{4}\log\left(\frac{3\sqrt{y}}{2+\sqrt{4+3y}}\right)\\
&\quad-\frac{1}{4}\left((\log(\sqrt{y}))^2-\left(\log\left(\frac{2+\sqrt{4+3y}}{3}\right)\right)^2\right)+O(y^{-1/2}\log(y))\\
&= \frac{\log(3)}{8}\log(y)+\frac{\log(3)}{4}\left(\gamma-\frac{1}{4}\log(3)+\log(2)\right)+c_2+O(y^{-1/2}\log(y))
\end{aligned}$$

where we have made use of

$$\begin{aligned}
(\log(\sqrt{y}))^2-\left(\log\left(\frac{2+\sqrt{4+3y}}{3}\right)\right)^2 &= \log\left(\frac{3\sqrt{y}}{2+\sqrt{4+3y}}\right)\log\left(\frac{\sqrt{y}(2+\sqrt{4+3y})}{3}\right)\\
&= \frac{\log(3)}{2}\left(\log(y)-\frac{1}{2}\log(3)\right)+O(y^{-1/2}\log(y)).
\end{aligned}$$

In total, this gives

$$\begin{aligned}\sum_{n\le y}\frac{w_{\triangle}(n)}{n} &= \sum_{n\le y}\frac{w_{\triangle,even}(n)+w_{\triangle,odd}(n)}{n}\\ &= \frac{\log(3)}{4}\log(y)+\frac{\log(3)}{2}\left(\gamma-\frac{1}{4}\log(3)\right)+c_1+c_2+O(y^{-1/2}\log(y)),\end{aligned}$$

where

$$c_1=\sum_{p=1}^{\infty}\frac{1}{4p}\left(\sum_{p<q\le 3p-1}\frac{1}{q}-\log(3)\right)\approx -0.2534695 \tag{8.64}$$

$$c_2=\sum_{k=0}^{\infty}\frac{1}{2k+1}\left(\sum_{k<\ell\le 3k}\frac{1}{2\ell+1}-\frac{1}{2}\log(3)\right)\approx -0.6976870 \tag{8.65}$$

Summarising we have

Theorem 8.A.3.

$$\sum_{n\le y} w_{\triangle}(n)n^s=\frac{\log(3)}{4(s+1)}y^{s+1}+O(y^{s+\frac{1}{2}})+O(1). \quad \textit{for } s>-1 \tag{8.66}$$

$$\sum_{n\le y}\frac{w_{\triangle}(n)}{n}=\frac{\log(3)}{4}\log(y)+c_3+O(y^{-1/2}\log(y)), \tag{8.67}$$

where

$$c_3:=\frac{\log(3)}{2}\left(\gamma-\frac{1}{4}\log(3)\right)+c_1+c_2\approx -0.7849570 \tag{8.68}$$

and c_1 and c_2 are given by Eqs. (8.64) *and* (8.65)*, respectively.*

8.A.3. Square lattice. In the following, k is always a positive integer.

8.A.3.1. *Formulas for χ_{-4}.* For $s>0$ we have

$$\sum_{n\le y}\chi_{-4}(n)=\left[\frac{y-1}{4}\right]-\left[\frac{y-3}{4}\right]=O(1) \tag{8.69}$$

$$\sum_{n\le y}\chi_{-4}(n)n^s=O(y^s) \tag{8.70}$$

$$\sum_{n\le y}\frac{\chi_{-4}(n)}{n^s}=\sum_{n\in\mathbb{N}}\frac{\chi_{-4}(n)}{n^s}-\sum_{y<n}\frac{\chi_{-4}(n)}{n^s}=L(s,\chi_{-4})+O\left(\frac{1}{y^s}\right) \tag{8.71}$$

$$\sum_{k<n\le y}\frac{\chi_{-4}(n)}{n^s}=\sum_{k<n}\frac{\chi_{-4}(n)}{n^s}+O\left(\frac{1}{y^s}\right)=O\left(\frac{1}{k^s}\right)+O\left(\frac{1}{y^s}\right) \tag{8.72}$$

8.A.3.2. *Formulas involving* $b_\square$. Calculations completely analogous to those for the hexagonal lattice yield

$$\sum_{n\leq y} b_\square(n)n^{-s} = \frac{1}{1-s}L(1,\chi_{-4})\, y^{1-s} + O(y^{\frac{1}{2}-s})$$

for $s<0$, whereas for $0<s<\frac{1}{2}$ we get

$$\sum_{n\leq y} b_\square(n)n^{-s} = \frac{L(1,\chi_{-4})}{1-s}\, y^{1-s} + O(y^{1/2-s}).$$

For $\frac{1}{2}<s<1$ we get

$$\sum_{n\leq y} b_\square(n)n^{-s} = \frac{L(1,\chi_{-4})}{1-s}\, y^{1-s} + C(s) + O(y^{1/2-s}),$$

with

$$C(s) = L(s,\chi_{-4})\zeta(s) - \sum_{m=1}^{\infty}\frac{\chi_{-4}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s} + \sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{d=m+1}^{\infty}\frac{\chi_{-4}(d)}{d^s} + L(2s,\chi_{-4}).$$

The sums in $C(s)$ are Dirichlet series that converge for $\mathrm{Re}(s)>\frac{1}{2}$, and are thus analytic for $\mathrm{Re}(s)>\frac{1}{2}$. They converge absolutely for $\mathrm{Re}(s)>1$, and a reordering of terms shows that the last three terms add up to zero for $\mathrm{Re}(s)>1$, and hence due to the analyticity also for $\mathrm{Re}(s)>\frac{1}{2}$. Hence $C(s)=L(s,\chi_{-4})\zeta(s)$ and thus

$$\sum_{n\leq y}\frac{b_\square(n)}{n^s} = \frac{L(1,\chi_{-4})}{1-s}\, y^{1-s} + L(s,\chi_{-4})\zeta(s) + O(y^{1/2-s}).$$

For $s=\frac{1}{2}$ the situation is again a bit more tricky and we want to avoid logarithmic error terms. The only two difficult terms are

$$\sum_{m\leq\sqrt{y}}\frac{\chi_{-4}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s} \qquad\text{and}\qquad \sum_{m\leq\sqrt{y}}\frac{1}{m^s}\sum_{d=m+1}^{\infty}\frac{\chi_{-4}(d)}{d^s}$$

The first term

$$\begin{aligned}\sum_{m\leq\sqrt{y}}\frac{\chi_{-4}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s} &= \sum_{k\leq(\sqrt{y}-1)/4}\left(\left(\frac{1}{(4k+1)^s}-\frac{1}{(4k+3)^s}\right)\sum_{d=1}^{4k+1}\frac{1}{d^s}-\frac{1}{(4k+3)^{2s}}\right)\\ &\qquad + O\left(\frac{1}{\sqrt{y}^s}\right)\sum_{d\leq\sqrt{y}}\frac{1}{d^s}\\ &= \sum_{k\leq(\sqrt{y}-1)/4}\left(\frac{1}{(4k+1)^s}\left(\frac{2s}{4k+1}+O\left(\frac{1}{(4k+1)^2}\right)\right)\left(\frac{(4k+1)^{1-s}}{1-s}+O(1)\right)\right.\\ &\qquad \left.-\frac{1}{(4k+3)^{2s}}\right)+O(y^{1/2-s})\end{aligned}$$

$$= \left(\frac{s}{1-s} - 1\right) \sum_{k \le (\sqrt{y}-1)/4} \frac{1}{(4k+1)^{2s}} + \sum_{k \le (\sqrt{y}-1)/4} O\left(\frac{1}{(4k+1)^{s+1}}\right) + O(y^{1/2-s})$$

is seen to be bounded for $1 > s \geq \frac{1}{2}$ and so is the second

$$\begin{aligned}\sum_{m \le \sqrt{y}} \frac{1}{m^s} \sum_{d=m+1}^{\infty} \frac{\chi_{-4}(d)}{d^s} &= \sum_{0 \le k \le (\sqrt{y}-1)/4} \sum_{j=1}^{4} \frac{1}{(4k+j)^s} \sum_{d=4k+j+1}^{\infty} \frac{\chi_{-4}(d)}{d^s} + O(y^{-s}) \\ &= \sum_{0 \le k \le (\sqrt{y}-1)/4} \left(\left(\frac{1}{(4k+1)^s} + \frac{1}{(4k+2)^s}\right) \frac{-1}{2(4k+3)^s} \right. \\ &\quad \left. + \left(\frac{1}{(4k+3)^s} + \frac{1}{(4k+4)^s}\right) \frac{1}{2(4k+5)^s} + O\left(\frac{1}{k^{1+2s}}\right)\right) + O(y^{-s}) \\ &= \sum_{0 \le k \le (\sqrt{y}-1)/4} O\left(\frac{1}{k^{1+2s}}\right) + O(y^{-s})\end{aligned}$$

where we have made use of

$$\begin{aligned}\sum_{d=4k}^{\infty} \frac{\chi_{-4}(d)}{d^s} = \sum_{d=4k+1}^{\infty} \frac{\chi_{-4}(d)}{d^s} &= \sum_{\ell=k}^{\infty} \left(\frac{1}{(4\ell+1)^s} - \frac{1}{(4\ell+3)^s}\right) \\ &= \sum_{\ell=k}^{\infty} \frac{1}{(4\ell+1)^s} \left(\frac{2s}{4\ell+1} + O\left(\frac{1}{(4\ell+1)^2}\right)\right) \\ &= \frac{1}{2(4k+1)^s} + O\left(\frac{1}{k^{1+s}}\right)\end{aligned}$$

and

$$\begin{aligned}\sum_{d=4k+2}^{\infty} \frac{\chi_{-4}(d)}{d^s} = \sum_{d=4k+3}^{\infty} \frac{\chi_{-4}(d)}{d^s} &= -\sum_{\ell=k}^{\infty} \left(\frac{1}{(4\ell+3)^s} - \frac{1}{(4\ell+5)^s}\right) \\ &= -\frac{1}{2(4k+3)^s} + O\left(\frac{1}{k^{1+s}}\right).\end{aligned}$$

Hence

$$\sum_{n \le y} \frac{b_\square(n)}{n^{1/2}} = 2L(1, \chi_{-4})\, y^{1/2} + O(1).$$

For $s = 1$ we get

$$\sum_{n \le y} \frac{b_\square(n)}{n} = L(1, \chi_{-4}) \log(y) + C(1) + O(y^{-1/2} \log(y)),$$

with

$$\begin{aligned}C(1) &= L(1,\chi_{-4})\gamma - \sum_{m=1}^{\infty} \frac{\chi_{-4}(m)}{m}\left(\log(m) + \sum_{d=1}^{m}\frac{1}{d}\right)\\ &\quad + \sum_{m=1}^{\infty}\frac{1}{m}\sum_{d=m+1}^{\infty}\frac{\chi_{-4}(d)}{d} + L(2,\chi_{-4})\\ &= L(1,\chi_{-4})\gamma - \sum_{m=1}^{\infty}\frac{\chi_{-4}(m)}{m}\log(m) = L(1,\chi_{-4})\gamma + L'(1,\chi_{-4}).\end{aligned}$$

by a similar reordering and analyticity argument as above.

For $s > 1$ we get

$$\sum_{n\le y}\frac{b_\square(n)}{n^s} = L(s,\chi_{-4})\zeta(s) + \frac{L(1,\chi_{-4})}{1-s}\,y^{1-s} + O(y^{-s/2}),$$

where we again have used the identity

$$-\sum_{m=1}^{\infty}\frac{\chi_{-4}(m)}{m^s}\sum_{d=1}^{m}\frac{1}{d^s} + \sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{d=m+1}^{\infty}\frac{\chi_{-4}(d)}{d^s} + L(2s,\chi_{-4}) = 0. \tag{8.73}$$

Summarising we have

Theorem 8.A.4.

$$\sum_{n\le y} b_\square(n)n^{-s} = \begin{cases} \frac{L(1,\chi_{-4})}{1-s}\,y^{1-s} + O(y^{1/2-s}) & \textit{for } s < \frac{1}{2}\\ 2L(1,\chi_{-4})\,y^{1/2} + O(1) & \textit{for } s = \frac{1}{2}\\ \frac{L(1,\chi_{-4})}{1-s}\,y^{1-s} + L(s,\chi_{-4})\zeta(s) + O(y^{1/2-s}) & \textit{for } \frac{1}{2} < s < 1\\ L(1,\chi_{-4})\log(y) + C_\square(1) + O(y^{-1/2}\log(y)) & \textit{for } s = 1\\ L(s,\chi_{-4})\zeta(s) + \frac{L(1,\chi_{-4})}{1-s}\,y^{1-s} + O(y^{-s/2}) & \textit{for } s > 1\end{cases} \tag{8.74}$$

where

$$C_\square(1) = L(1,\chi_{-4})\gamma + L'(1,\chi_{-4}) \approx 0.6462454. \tag{8.75}$$

Note that we have the following formula (see [**Su-2**])

$$\frac{L'(1,\chi_{-4})}{L(1,\chi_{-4})} = \log\left(M(1,\sqrt{2})^2\frac{e^\gamma}{2}\right) = \log\left(\Gamma\left(\frac{3}{4}\right)^4\frac{e^\gamma}{\pi}\right), \tag{8.76}$$

where $M(x,y)$ is the arithmetic-geometric mean of x and y.

8.A.3.3. *Formulas for $w_\square$.* For $s > -1$ we have

$$\begin{aligned}
\sum_{n\le y} w_{\square,even}(n)n^s &= \sum_{p<\sqrt{y/2}} \ \sum_{p<q\le\min([p\sqrt{3}],[y/(2p)])} (2pq)^s \\
&= \sum_{p\le\sqrt{y/(2\sqrt{3})}} (2p)^s \sum_{p<q<p\sqrt{3}} q^s + \sum_{\sqrt{y/(2\sqrt{3})}<p<\sqrt{y/2}} (2p)^s \sum_{p<q\le y/(2p)} q^s \\
&= \sum_{p\le\sqrt{y/(2\sqrt{3})}} (2p)^s \left(\frac{1}{s+1}\, p^{1+s}(3^{(s+1)/2}-1) + O(p^s)\right) \\
&\quad + \sum_{\sqrt{y/(2\sqrt{3})}<p<\sqrt{y/2}} (2p)^s \left(\frac{1}{s+1}\left(\frac{y^{s+1}}{(2p)^{s+1}} - p^{s+1}\right) + O(p^s) + O\left(\frac{y^s}{p^s}\right)\right) \\
&= \frac{2^s(3^{(s+1)/2}-1)}{2(s+1)^2}\,\frac{y^{s+1}}{2^{s+1}3^{(s+1)/2}} + O(y^{s+\frac{1}{2}}) + O(1) \\
&\quad + \frac{y^{s+1}}{2(s+1)}\log\left(\frac{\sqrt{y/2}}{\sqrt{y/(2\sqrt{3})}}\right) - \frac{2^s}{2(s+1)^2}\left(\frac{y^{s+1}}{2^{s+1}} - \frac{y^{s+1}}{2^{s+1}3^{(s+1)/2}}\right) \\
&= \frac{\log(3)}{8(s+1)}y^{s+1} + O(y^{s+\frac{1}{2}}) + O(1).
\end{aligned}$$

Similarly (again for $s > -1$)

$$\begin{aligned}
\sum_{n\le y} w_{\square,odd}(n)n^s &= \sum_{k<(\sqrt{y}-1)/2} \ \sum_{k<\ell\le\min([\sqrt{3}k+(\sqrt{3}-1)/2],[y/(4k+2)-1/2])} (2k+1)^s(2\ell+1)^s \\
&= \sum_{k\le\sqrt{y}/(2\sqrt[4]{3})-1/2} (2k+1)^s \sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2} (2\ell+1)^s \\
&\quad + \sum_{\sqrt{y}/(2\sqrt[4]{3})-1/2<k<(\sqrt{y}-1)/2} (2k+1)^s \sum_{k<\ell\le y/(4k+2)-1/2} (2\ell+1)^s \\
&= \sum_{k\le\sqrt{y}/(2\sqrt[4]{3})-1/2} (2k+1)^s \frac{1}{2(s+1)} \underbrace{\left(\left(2k\sqrt{3}+\sqrt{3}\right)^{s+1} - (2k+1)^{s+1}\right)}_{(3^{(s+1)/2}-1)(2k+1)^{s+1}+O(k^s)} \\
&\quad + \sum_{\sqrt{y}/(2\sqrt[4]{3})-1/2<k<(\sqrt{y}-1)/2} (2k+1)^s \times \\
&\quad \times \left(\frac{1}{2(s+1)}\left(\frac{y^{s+1}}{(2k+1)^{s+1}} - (2k+1)^{s+1}\right) + O(k^s) + O\left(\frac{y^s}{(2k+1)^s}\right)\right) \\
&= \frac{3^{(s+1)/2}-1}{8(s+1)^2}\,\frac{y^{s+1}}{3^{(s+1)/2}} + O(y^{s+\frac{1}{2}}) + O(1) \\
&\quad + \frac{y^{s+1}}{4(s+1)}\log\left(\frac{\sqrt{y}}{\sqrt{y}/\sqrt[4]{3}}\right) - \frac{1}{8(s+1)^2}\left(y^{s+1} - \frac{y^{s+1}}{3^{(s+1)/2}}\right)
\end{aligned}$$

$$= \frac{\log(3)}{16(s+1)} y^{s+1} + O(y^{s+\frac{1}{2}}) + O(1),$$

For $s=-1$ we get

$$\begin{aligned}
\sum_{n\le y} \frac{w_{\square,even}(n)}{n} &= \sum_{p<\sqrt{y/2}} \; \sum_{p<q\le \min([p\sqrt{3}],[y/(2p)])} \frac{1}{2pq} \\
&= \sum_{p\le\sqrt{y/(2\sqrt{3})}} \frac{1}{2p} \sum_{p<q<p\sqrt{3}} \frac{1}{q} + \sum_{\sqrt{y/(2\sqrt{3})}<p<\sqrt{y/2}} \frac{1}{2p} \sum_{p<q\le y/(2p)} \frac{1}{q} \\
&= \sum_{p\le\sqrt{y/(2\sqrt{3})}} \frac{1}{2p} \Bigg(\frac{\log(3)}{2} + \underbrace{\sum_{p<q<p\sqrt{3}} \frac{1}{q} - \frac{\log(3)}{2}}_{O\left(\frac{1}{p}\right)} \Bigg) \\
&\quad + \sum_{\sqrt{y/(2\sqrt{3})}<p<\sqrt{y/2}} \frac{1}{2p} \left(\log\left(\frac{y}{2p^2}\right) + O\left(\frac{1}{p}\right) + O\left(\frac{p}{y}\right) \right) \\
&= \frac{\log(3)}{4} \left(\log\left(\sqrt{\frac{y}{2\sqrt{3}}} \right) + \gamma + O(y^{-1/2}) \right) \\
&\quad + \underbrace{\sum_{p=1}^{\infty} \frac{1}{2p} \left(\sum_{p<q<p\sqrt{3}} \frac{1}{q} - \frac{\log(3)}{2} \right)}_{=:\, c_4} + O(y^{-1/2}) \\
&\quad + \frac{\log(y)-\log(2)}{2} \log\left(\sqrt[4]{3}\right) \\
&\quad - \frac{1}{2} \left(\left(\log\left(\sqrt{\frac{y}{2}} \right) \right)^2 - \left(\log\left(\sqrt{\frac{y}{2\sqrt{3}}} \right) \right)^2 \right) + O(y^{-1/2}\log(y)) \\
&= \frac{\log(3)}{8}\log(y) + \frac{\log(3)}{4} \left(\gamma - \frac{1}{8}\log(3) - \frac{1}{2}\log(2) \right) + c_4 + O(y^{-1/2}\log(y)).
\end{aligned}$$

where we have made use of

$$\begin{aligned}
\left(\log\left(\sqrt{\frac{y}{2}} \right) \right)^2 - \left(\log\left(\sqrt{\frac{y}{2\sqrt{3}}} \right) \right)^2 &= \log\left(\sqrt[4]{3}\right) \log\left(\frac{y}{2\sqrt[4]{3}} \right) \\
&= \frac{\log(3)}{4} \left(\log(y) - \frac{1}{4}\log(3) - \log(2) \right)
\end{aligned}$$

Similarly

$$\begin{aligned}
\sum_{n\le y} \frac{w_{\square,odd}(n)}{n} &= \sum_{k<(\sqrt{y}-1)/2} \; \sum_{k<\ell\le\min([\sqrt{3}k+(\sqrt{3}-1)/2],[y/(4k+2)-1/2])} \frac{1}{(2k+1)(2\ell+1)} \\
&= \sum_{k\le\sqrt{y}/(2\sqrt[4]{3})-1/2} \frac{1}{2k+1} \sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2} \frac{1}{2\ell+1}
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\sqrt{y}/(2\sqrt[4]{3})-1/2<k<(\sqrt{y}-1)/2} \frac{1}{2k+1} \sum_{k<\ell\leq y/(4k+2)-1/2} \frac{1}{2\ell+1} \\
&= \sum_{k\leq\sqrt{y}/(2\sqrt[4]{3})-1/2} \frac{1}{2k+1}\left(\frac{1}{4}\log(3) + \underbrace{\sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2}\frac{1}{2\ell+1}-\frac{1}{4}\log(3)}_{O\left(\frac{1}{k}\right)}\right) \\
&\quad+ \sum_{\sqrt{y}/(2\sqrt[4]{3})-1/2<k<(\sqrt{y}-1)/2} \frac{1}{2k+1}\left(\frac{1}{2}\log\left(\frac{y}{(2k+1)^2}\right)+O\left(\frac{1}{k}\right)+O\left(\frac{k}{y}\right)\right) \\
&= \frac{1}{4}\log(3)\left(\frac{1}{2}\log\left(\frac{\sqrt{y}}{\sqrt[4]{3}}\right)+\frac{1}{2}\gamma+\frac{1}{2}\log(2)-1+O(y^{-1/2})\right) \\
&\quad+ \underbrace{\sum_{k=1}^{\infty}\frac{1}{2k+1}\left(\sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2}\frac{1}{2\ell+1}-\frac{1}{4}\log(3)\right)}_{=:\, c_5+\frac{1}{4}\log(3)} + O(y^{-1/2}) \\
&\quad+ \frac{\log(y)}{4}\log\left(\sqrt[4]{3}\right)-\frac{1}{4}\left((\log(\sqrt{y}))^2-\left(\log\left(\frac{\sqrt{y}}{\sqrt[4]{3}}\right)\right)^2\right)+O(y^{-1/2}\log(y)) \\
&= \frac{\log(3)}{16}\log(y)+\frac{\log(3)}{8}\left(\gamma-\frac{1}{8}\log(3)+\log(2)\right)+c_5+O(y^{-1/2}\log(y))
\end{aligned}
$$

where we have made use of

$$
\begin{aligned}
(\log(\sqrt{y}))^2-\left(\log\left(\frac{\sqrt{y}}{\sqrt[4]{3}}\right)\right)^2 &= \log\left(\sqrt[4]{3}\right)\log\left(\frac{y}{\sqrt[4]{3}}\right) \\
&= \frac{\log(3)}{4}\left(\log(y)-\frac{1}{4}\log(3)\right).
\end{aligned}
$$

Summarising we have

Theorem 8.A.5. *The asymptotic formulas for $w_{\Box,even}$ and $w_{\Box,odd}$ read*

$$\sum_{n\leq y} w_{\Box,even}(n)n^s = \frac{\log(3)}{8(s+1)}y^{s+1}+O(y^{s+\frac{1}{2}})+O(1), \tag{8.77}$$

$$\sum_{n\leq y} w_{\Box,odd}(n)n^s = \frac{\log(3)}{16(s+1)}y^{s+1}+O(y^{s+\frac{1}{2}})+O(1) \tag{8.78}$$

for $s>-1$. Furthermore

$$\sum_{n\leq y} \frac{w_{\Box,even}(n)}{n} = \frac{\log(3)}{8}\log(y)+c_{even}+O(y^{-1/2}\log(y)), \tag{8.79}$$

$$\sum_{n\leq y} \frac{w_{\Box,odd}(n)}{n} = \frac{\log(3)}{16}\log(y)+c_{odd}+O(y^{-1/2}\log(y)), \tag{8.80}$$

where

(8.81)

$$c_{even} = \frac{\log(3)}{4}\left(\gamma - \frac{\log(3)}{8} - \frac{\log(2)}{2}\right) + \sum_{p=1}^{\infty} \frac{1}{2p}\left(\sum_{p<q<p\sqrt{3}} \frac{1}{q} - \frac{\log(3)}{2}\right)$$

$$\approx -0.3966993$$

(8.82)

$$c_{odd} = \frac{\log(3)}{8}\left(\gamma - \frac{\log(3)}{8} + \log(2)\right) + \sum_{k=0}^{\infty} \frac{1}{2k+1}\left(\sum_{k<\ell<k\sqrt{3}+(\sqrt{3}-1)/2} \frac{1}{2\ell+1} - \frac{1}{4}\log(3)\right)$$

$$\approx -0.2083500$$

Bibliography

Su-1. T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York (1976).

Su-2. P. Moree, Chebyshev's bias for composite numbers with restricted prime divisors, *Math. Comp.*, **73** (2004), 425–449.