Decompositions in algebra

Gent, D.M.H. van

Decompositions in algebra

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof. dr. ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op dinsdag 5 maart 2024
klokke 15.00 uur

door

Daniël Martinus Herman van Gent
geboren te Leiden, Nederland
in 1995

Promotor:

Prof. dr. R. M. van Luijk

Copromotor:

Prof. dr. H. W. Lenstra

Promotiecommissie:

Prof. dr. ir. G. L. A. Derks

Prof. dr. D. S. T. Holmes

Prof. dr. P. Stevenhagen

Prof. dr. A. Bartel (University of Glasgow)

Prof. dr. T. Chinburg (University of Pennsylvania)

Samenvatting

In dit proefschrift getiteld "*Decompositions in algebra*" bestuderen we ontbindingen van Abelse groepen uitgerust met verscheidene algebraïsche structuren, en relevante algoritmen.

In Hoofdstuk 1 beschouwen we stromen in ongerichte grafen waarvan de waarden, in contrast met de klassieke theorie, leven in niet noodzakelijk Abelse groepen. Voor Abelse stromen is het zo, dat als in alle knopen van de graaf met ten hoogste één uitzondering voldaan is aan de *behoudswet van Kirchhoff*, die stelt dat de inkomende stroom gelijk is aan de uitgaande stroom, dan ook deze uitgezonderde knoop aan de behoudswet voldoet. We bewijzen het verbazende resultaat dat de grafen waarvoor deze implicatie ook geldt voor iedere niet-Abelse stroom, precies de *vlakke grafen* zijn. Ook construeren we van een gegeven groep een ontbinding in zijn maximale Abelse ondergroepen, aan de hand waarvan algoritmisch te beslissen is of deze groep voor alle grafen aan de behoudswet voldoet.

In Hoofdstuk 2 generaliseren we de theorie van roosters naar oneindige dimensie, waar het volgende hoofdstuk op rust. Waar klassiek een rooster een discrete ondergroep vormt van een Euclidische vectorruimte, beschouwen wij discrete ondergroepen van Hilbertruimten, die wij *Hilbertroosters* noemen. We bewijzen dat ieder Hilbertrooster een unieke maximale orthogonale ontbinding in deelroosters heeft, en bestuderen daartoe de *onontbindbare vectoren*. De onontbindbare vectoren ontlenen hun bestaan aan het *Voronoi-polyeder*, waarvan we laten zien dat het een fundamenteel domein is. Aftelbare Hilbertroosters blijken vrije Abelse groepen te zijn. Het is een open probleem of dit algemeen geldt.

In Hoofdstuk 3 beschouwen we de gehele afsluiting van de gehele getallen in een algebraïsche afsluiting van het lichaam van rationale getallen, de *ring van algebraïsch gehelen* genaamd, uitgerust met de natuurlijke Hilbertroosterstructuur zoals bekend uit de theorie van de meetkunde van getallen. We

pogen voor dit rooster invarianten uit te rekenen. In het bijzonder geven we onder- en bovengrenzen op de *overdekkingsstraal*. Hieruit leiden we een partiële oplossing af van de algoritmische tegenhanger van dit probleem, namelijk het *dichtstbijzijnde-vectorprobleem*. Als proeve voor zulke algoritmen dragen wij het berekenen van de onontbindbare vectoren van gegeven graad aan. Het blijkt lastig om alle onontbindbare vectoren van graad drie te bepalen, hoewel het aantal kandidaten beperkt is, omdat de termen van een ontbinding een arbitrair hoge graad kunnen hebben. Om dezelfde reden is het niet eens duidelijk of onontbindbaarheid beslisbaar is. Het is ook onbekend of het rooster isometrieën heeft naast de isometrieën die komen van de ringstructuur.

In Hoofdstuk 4 ontbinden we ringen in *graderingen*, een constructie die de graad van een monoom in een polynoomring generaliseert. We bewijzen dat de roosterstructuur op de ring van algebraïsch gehelen en diens deelringen aanleiding geeft tot het bestaan van een *universele gradering* voor deze ringen, en we bepalen de structuur hiervan in enkele speciale gevallen. In het bijzonder is de maximale orthogonale ontbinding, en dus ook de universele gradering, van het rooster van algebraïsch gehelen triviaal. Los van een roosterstructuur bestaat een universele gradering onder zekere p-adische voorwaarden, en in het verlengde hiervan bewijzen we dat *eenheidswortels* en *idempotenten* 'monomen' zijn. Verder geven we een algoritme om snel de universele gradering van ringen te bepalen die additief worden voortgebracht door hun eenheidswortels en idempotenten.

In Hoofdstuk 5 passen we de theorie van het voorgaande hoofdstuk toe op het speciale geval van *groepenringen*. Voor groepenringen over gereduceerde ordes blijkt ook aan een zekere universaliteit voldaan: op isomorfie na is er een unieke maximale manier om een dergelijke ring als groepenring te ontbinden. In termen hiervan beschrijven we diens automorfismengroep. Zeer verrassend blijkt dat in het samenhangende geval, de deelringen en ondergroepen die gebruikt kunnen worden om een maximale ontbinding te vormen compleet onafhankelijk gekozen kunnen worden. Dit bewijzen we door de theorie van modulen, in het bijzonder ontbindingen van modulen van eindige lengte, toe te passen op een morfisme van eindige abelse groepen, namelijk de *graadafbeelding* beperkt tot de groep van eenheidswortels.

In Hoofdstuk 6 geven we een efficiënte algoritme om *wortels van gebroken idealen* van ordes in getallenlichamen te trekken. We zijn zorgvuldig om deze algoritme zo te formuleren dat de uitvoer voldoende functorieel is. Het is hierbij een obstructie dat een wortel niet hoeft te bestaan of uniek hoeft te zijn. We vinden een toepassing van het worteltrekken in een generalisatie van de *coprieme-basisalgoritme*. Deze algoritme vindt voor een verzameling

positieve gehele getallen een verzameling paarsgewijs coprieme gehelen, een *coprieme basis*, waarbij ieder getal uit de eerste verzameling een (uniek) machtsproduct is van getallen uit de tweede. Dit machtsproduct kan gezien worden als de beste polynomiale-tijd benadering van de priemontbinding. Echter, het is nog mogelijk de coprieme basis te verbeteren door wortels te trekken uit diens elementen. Wanneer we de copriemebasisalgoritme generaliseren naar idealen in ordes, zijn we ook daar in staat om deze laatste verbetering te maken.

Summary

In this thesis entitled "*Decompositions in algebra*" we study decompositions of abelian groups equipped with several algebraic structures, and relevant algorithms.

In Chapter 1 we consider flows in undirected graphs of which the values, in contrast to the classical theory, live in not necessarily abelian groups. For abelian flows it is the case, that if for all vertices of the graph with at most one exception *Kirchhoff's law of conservation* holds, which states that the incoming flow equals the outgoing flow, then the exceptional vertex also satisfies this law. We prove the surprising result that graphs for which this implication also holds for each non-abelian flow are precisely the *planar graphs*. We also construct from a given group a decomposition into its maximal abelian subgroups, in terms of which we can decide algorithmically whether this group satisfies the conservation law for all graphs.

In Chapter 2 we generalize the theory of lattices to infinite dimension, on which the next chapter relies. Where classically a lattice forms a discrete subgroup of a Euclidean vector space, we consider discrete subgroups of Hilbert spaces, which we call *Hilbert lattices*. We prove that every Hilbert lattice has a maximal orthogonal decomposition into sublattices, and to that end study the *indecomposable vectors*. The indecomposables derive their existence from the *Voronoi polyhedron*, for which we show that it is a fundamental domain. Countable Hilbert lattices turn out to be free abelian groups. It is an open problem whether this holds generally.

In Chapter 3 we consider the integral closure of the integers in an algebraic closure of the field of rational numbers, called the *ring of algebraic integers*, equipped with the natural Hilbert lattice structure known from the theory of the geometry of numbers. We attempt to compute invariants of this lattice. In particular, we give lower and upper bounds on the *covering radius*. From this we derive a partial solution to the algorithmic counter-

part of this problem, namely the *closest vector problem*. As a test for such algorithms we propose the computation of indecomposable vectors of given degree. It turns out to be hard to compute all indecomposables of degree three, even though the number of candidates is limited, because the terms of a decomposition can have an arbitrarily large degree. For the same reason it is not even clear whether indecomposability is decidable. It is also unknown whether the lattice has isometries other than the isometries that come from the ring structure.

In Chapter 4 we decompose rings into *gradings*, a construction that generalizes the degree of a monomial in a polynomial ring. We prove that the lattice structure of the ring of algebraic integers and its subrings gives rise to the existence of a *universal grading* of such rings, and we determine their structure in several special cases. In particular, the maximal orthogonal decomposition, and hence also the universal grading, of the lattice of algebraic integers is trivial. Separate from a lattice structure, a universal grading exists under certain p-adic assumptions, and in extension to this we show that *roots of unity* and *idempotents* are 'monomials'. Furthermore, we give an algorithm to quickly compute the universal grading of rings that are additively generated by their roots of unity and idempotents.

In Chapter 5 we apply the theory of the previous chapter to the special case of *group rings*. It turns out that also for group rings over reduced orders a certain universality is satisfied: up to isomorphism there is a unique maximal way to decompose such a ring as a group ring. In terms of this we describe its automorphism group. Very surprisingly it turns out that in the connected case the subrings and subgroups that can be used to form a maximal decomposition can be chosen entirely independently. We prove this by applying the theory of modules, in particular decompositions of finite length modules, to a morphism of finite abelian groups, namely the *degree map* restricted to the group of roots of unity.

In Chapter 6 we give an efficient algorithm to take *roots of fractional ideals* in orders in number fields. We are careful in formulating this algorithm so that the output is sufficiently functorial. Here it is an obstruction that roots need not exist or be unique. We find an application of taking roots in a generalization of the coprime basis algorithm. This algorithm finds for a set of positive integers a set of pairwise coprime integers, called a *coprime basis*, where every number from the first set is a (unique) power product of numbers from the second. This power product can be seen as the best polynomial-time approximation of the prime factorization. However, it is possible to improve the coprime basis by taking roots of its elements. When we generalize the coprime basis algorithm to ideals in orders, we are able to also there make this final improvement.

Publications and preprints

Parts of this thesis are based on the following publications and preprints.

D. M. H. van Gent. Nonabelian flows in networks. *Journal of Graph Theory*, 104(1):245–256, 2023. https://doi.org/10.1002/jgt.22958

D. M. H. van Gent. Indecomposable algebraic integers, 2021. https://arxiv.org/abs/2111.00499

H. W. Lenstra Jr., A. Silverberg, and D. M. H. van Gent. Realizing orders as group rings. *Journal of Algebra*, 2023. https://doi.org/10.1016/j.jalgebra.2023.11.017

The following paper is not part of this thesis.

M. J. H. van den Bergh, S. T. Castelein, and D. M. H. van Gent. Order versus chaos. In *2020 IEEE Conference on Games (CoG)*, pages 391–398, 2020. https://doi.org/10.1109/CoG47356.2020.9231895

Contents

Preliminaries

Definitions

In this section we will list some definitions and notations that we assume a reader of the coming chapters be familiar with.

Rings We write $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ for the rings of integers, rationals, reals and complex numbers respectively. We will avoid the use of the term 'natural numbers' and instead write $\mathbb{Z}_{\geq 0} = \{n \in \mathbb{Z} \mid n \geq 0\}$ for the set of non-negative integers and $\mathbb{Z}_{>0} = \{n \in \mathbb{Z} \mid n > 0\}$ for the set of positive integers. Like in any modern mathematical text, our rings include a multiplicative identity element.

Let R be a ring and let $x \in R$. We say x is *regular* if the maps $R \to R$ given by $y \mapsto xy$ and $y \mapsto yx$ are injective, while x is a *zero-divisor* if it is not regular. We say x is a *unit* if both maps are bijective, and we write R^* for the group of units of R. For a positive integer n, we say x is an *n-th root of unity* if $x^n = 1$, and write $\mu_n(R)$ for the subgroup of R^* of n-th roots of unity when R is commutative. We say x is a *root of unity* if it is an n-th root of unity for some n, and analogously write $\mu(R)$ for the group of roots of unity when R is commutative. We say x is *idempotent* if $x^2 = x$ and write $\mathrm{Id}(R)$ for the set of idempotents of R. We say x is *nilpotent* if $x^n = 0$ for some positive integer n. We write $\mathrm{nil}(R)$ for the set of nilpotents of R, which we call the *nilradical* when R is commutative. We write $\mathrm{Jac}(R) = \{x \in R \mid 1 + RxR \subseteq R^*\}$ for the *Jacobson radical* of R.

Suppose now that R is a commutative ring. We say R is *connected* if it has exactly two idempotents, i.e. the only idempotents are 0 and 1 and $R \neq 0$. We say R is *reduced* if 0 is the only nilpotent of R.

A *number field* is a field of characteristic 0 which has finite dimension as a $\mathbb{Q}$-module. An *order* is a commutative ring whose additive group is

isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. Note that we do not require, as some authors do, that an order be contained in a number field, i.e. that it is an integral domain. Instead, we say R is an order of a number field K if $R \subseteq K$ is an order such that R generates K as $\mathbb{Q}$-module.

Modules Let R be a ring and M and N be (left) R-modules. For a morphism $f\colon M \to N$ of R-modules we write $\ker(f) = \{m \in M \mid f(m) = 0\}$ for the *kernel* of f, write $\operatorname{im}(f) = \{f(m) \mid m \in M\}$ for the *image* of f and write $\operatorname{coker}(f) = N/\operatorname{im}(f)$ for the *cokernel* of f. For a set I, an *I-indexed decomposition* of M is a family $\{M_i\}_{i\in I}$ of R-submodules of M such that the natural map $\bigoplus_{i\in I} M_i \to M$ is an isomorphism, a condition we abbreviate by $\bigoplus_{i\in I} M_i = M$. A *decomposition* of M is an I-indexed decomposition for any set I. We say M is *indecomposable* if $M \neq 0$ and for all $M_1, M_2 \subseteq M$ such that $M_1 \oplus M_2 = M$ we have $M_1 = 0$ or $M_2 = 0$. We make the class of decompositions of M into a (locally small) category, where the morphisms from $\{M_i\}_{i\in I}$ to $\{N_j\}_{j\in J}$ are the maps $f\colon I \to J$ such that $N_j = \bigoplus_{i\in f^{-1}\{j\}} M_i$ for all $j \in J$. For commutative R and $r \in R$ we write $M[r] = \{m \in M : rm = 0\}$ for the *r-torsion submodule* and $M[r^\infty] = \bigcup_{n\geq 0} M[r^n]$. For a set S we write $M^S = \prod_{s\in S} M$ and $M^{(S)} = \bigoplus_{s\in S} M$.

Graphs A *simple graph* is a pair (V, E) where V is a (potentially infinite) set and E is a set of size-2 subsets of V. Let $G = (V, E)$ be a graph. We call the elements of V the *vertices* of G and those of E its *edges*. A *subgraph* of G is a simple graph (W, F) with $W \subseteq V$ and $F \subseteq E$. For $W \subseteq V$ we call $(W, \{\{u, v\} \in E \,|\, u, v \in W\})$ the subgraph of G *induced by* W. For $u \in V$ we call $v \in V$ a *neighbor* of u if $\{u, v\} \in E$. A *connected component* of G is a non-empty set $S \subseteq V$ such that for all $e \in E$ we have $e \subseteq S$ or $e \subseteq V \setminus S$ and which is minimal with respect to inclusion given these properties. We say a simple graph is *connected* if it has precisely one connected component; in particular V is non-empty.

Algorithms

In this thesis we will encounter several algorithms, ranging from theoretical to computational in nature. The computational algorithms [19, 21] are programmed in either Sage [41] or GAP [15]. For our theoretical algorithms it would be important to specify our model of computation and the encoding of our mathematical objects, were it not that in our complexity analyses we will at best prove that the algorithm in question terminates in polynomial time. Assuming we remain sensible, polynomial runtime is invariant

under choice of model and encodings. Thus we allow ourselves in the coming chapters the luxury to reason about these algorithms in an informal and conceptual manner, rather than worry about implementation details. Nonetheless, in this section we will state some basic encodings and results that we will later implicitly use.

We let k be either $\mathbb{Z}$ or $\mathbb{Q}$ and assume there to be some sensible encoding of its elements.

Modules We encode a *linear map* $\alpha\colon k^m \to k^n$ as a matrix, i.e. a k-valued $(n \times m)$-tuple, in the obvious way. We encode a *finitely generated k-module* by a linear map $\alpha\colon k^m \to k^n$, where the corresponding module is $\operatorname{coker}(\alpha)$. The elements of $\operatorname{coker}(\alpha)$ are encoded by representatives in k^n. For $\alpha\colon k^m \to k^n$ and $\beta\colon k^r \to k^s$, a *morphism of finitely generated k-modules* $f\colon \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta)$ is encoded as a linear map $\varphi\colon k^n \to k^s$ on the underlying representations of the elements of $\operatorname{coker}(\alpha)$ and $\operatorname{coker}(\beta)$. Note that every linear map $\alpha\colon k^m \to k^n$ encodes a valid k-module. However, with α and β as above, not every $\varphi\colon k^n \to k^s$ encodes a valid morphism $\operatorname{coker}(\alpha) \to \operatorname{coker}(\beta)$, as it does so if and only if $\operatorname{im}(\varphi\alpha) \subseteq \operatorname{im}(\beta)$. This is generally not a problem however, since our algorithms are only required to work for legal input. Regardless, we can test whether φ encodes a morphism. A submodule of A is encoded as a module A' together with an injective morphism $A' \to A$.

If $k = \mathbb{Q}$, then using linear algebra one can answer most questions about finitely generated k-modules in polynomial time. This also includes computing kernels and images of linear maps, computing hom-sets and splitting exact sequences. For $k = \mathbb{Z}$ one can find an exposition on algorithms for basic questions and constructions involving finitely generated k-modules in Chapter 2 of [5].

Rings A *k-algebra* structure on a finitely generated k-module represented by some map $k^m \to k^n$ is encoded as a k-valued $(n \times n \times n)$-tuple $(e_{hij})_{h,i,j}$, where the multiplication is given by

$$(a_h)_h \cdot (b_i)_i = \Big(\sum_{h,i} a_h b_i e_{hij} \Big)_j .$$

In particular, we can encode finite rings, orders and number fields. We may also compute quotient rings. For some commutative ring R with a given encoding we encode the elements of the *polynomial ring* $R[X]$ as a sequence $(n, f_0, \ldots, f_n)$ with $n \in \mathbb{Z}_{\geq 0}$ and $f_0, \ldots, f_n \in R$, where the corresponding polynomial is given by $\sum_{i=0}^{n} f_i X^i$.

Number fields Suppose for some set S we have an encoding of its elements. We say a map $\varphi\colon S \to \mathbb{C}$ is *computable* if there exists an algorithm A that takes as input an $s \in S$ and $n \in \mathbb{Z}_{\geq 0}$ and computes some $a \in \mathbb{Q}(\mathrm{i})$ such that $|\varphi(s) - a| \leq 2^{-n}$. We represent computable maps by such an algorithm. We say a complex number is computable if the map $\{0\} \to \mathbb{C}$ given by $0 \mapsto z$ is computable. It is undecidable whether two computable complex numbers are equal.

For any k-algebra A which is finitely generated and free as a module one can find for each element of A its minimal polynomial using linear algebra. For a number field K it is possible to factor polynomials over K into irreducibles in polynomial time [31]. Repeated application allows us to compute the splitting field of such a polynomial, although not generally in polynomial time. The roots (with multiplicity) of $f \in \mathbb{Q}[X]$ in $\mathbb{C}$ are computable [25]. Using this, each ring homomorphism $K \to \mathbb{C}$ is computable and we may compute the set of ring homomorphisms $K \to \mathbb{C}$.

CHAPTER 1

Nonabelian flows in graphs

1.1 Introduction

This chapter is based on [20]. In this chapter, *graph* will mean a simple graph with a finite number of vertices. We consider groups which are not required to be abelian and therefore write our group operations multiplicatively.

With Γ a group and $G = (V, E)$ a graph, we call a map $f\colon V^2 \to \Gamma$ a Γ-*flow in* G if for all $u, v \in V$ we have $f(u, v) = f(v, u)^{-1}$, and $f(u, v) = 1$ if $\{u, v\} \notin E$. This definition agrees with the classical definition of a graph flow when $\Gamma = \mathbb{R}$.

Non-abelian graph flows, i.e. flows where Γ need not be abelian, were first considered by M.J. DeVos in his PhD thesis [9] and later by A.J. Goodall et al. [22] and B. Litjens [36]. They consider graphs embedded on surfaces and ask whether flows exist which are nowhere trivial, i.e. $f(u, v) \neq 1$ if and only if $\{u, v\} \in E$. Although likewise our main result involves planar embeddings of graphs, we instead ask to which extent Kirchhoff's law of conservation holds.

Let $G = (V, E)$ be a graph, Γ a group and f a Γ-flow in G. We call f *tractable* if for each $v \in V$ the subgroup $\langle f(u, v) \mid u \in V \rangle$ of Γ is abelian. For tractable f we define the *excess* $e_f\colon V \to \Gamma$ to be the map given by $v \mapsto \prod_{u \in V} f(u, v)$ and we say f is *conserving* in v if $e_f(v) = 1$. In the classical case, we have the following lemma.

Lemma 1.1.1. *Let Γ be an* abelian *group, let f be a Γ-flow in a graph $G = (V, E)$ and let $w \in V$. If f is conserving in all vertices of $V \setminus \{w\}$, then f is conserving in w.*

Proof. We have

$$e_f(w) = \prod_{v \in V} e_f(v) = \prod_{(u,v) \in V^2} f(u, v) = \prod_{\{u,v\} \in E} f(u, v) f(v, u) = 1,$$

so f is conserving in w. □

We will show that Lemma 1.1.1 can fail for non-abelian Γ. We say a flow f *leaks* if it is tractable and conserving in all but precisely one vertex and we call a graph G *leak-proof* if there exist no flows in G that leak for any group Γ. Our main result, proven in Section 1.4, is as follows.

Theorem 1.4.3. *A graph is leak-proof if and only if it is planar.*

We say a flow f of G has a *binary leak* at distinct vertices $u, v \in V$ if it is tractable and conserving in all vertices of $V \setminus \{u, v\}$ while $e(u)e(v) \neq 1$. Here u and v can be thought of as a source and sink of the flow. We call

G binary leak-proof if no binary leaking flows exist for G. Analogously to Lemma 1.1.1 one can show that a flow cannot have a binary leak when the group is abelian. We also prove the following analogue to Theorem 1.4.3 in Section 1.5.

Definition 1.1.2. We call a graph $G = (V, E)$ *extra-planar* if for all pairs of distinct $u, v \in V$ the graph $(V, E \cup \{u, v\})$ is planar.

Theorem 1.5.2. *A graph is binary leak-proof if and only if it is extra-planar.*

Instead of studying leak-proof graphs, one could also study leak-proof groups, where we call a group Γ *leak-proof* if for all graphs $G = (V, E)$ no tractable flows $f\colon V^2 \to \Gamma$ of G leak. Theorem 1.4.3 shows that the decision problem 'Is this graph leak-proof?' can be decided in time $O(|V|)$, as Hopcroft and Tarjan gave an algorithm to test graph planarity in [24] of this complexity. For leak-proof groups, we prove the following in Section 1.6.

Theorem 1.6.4. *The decision problem 'Is this finite group leak-proof?' is decidable.*

The present work, in particular Theorem 1.5.2, was inspired by a problem the author encountered in his Master's thesis [17] on graded rings. Here a flow with a binary leak gives rise to an example (Example 2.17 of [17]) of an efficient ring grading with a non-abelian group that cannot be replaced by an abelian group.

1.2 Definitions and basic properties

We briefly go through some basic definitions. Let $G = (V, E)$ be a graph. With $H = (W, F)$ a graph we call a map $f\colon V \to W$ a *morphism* from G to H if $f[E] \subseteq F$. We call this f an *embedding* if it is injective and an *isomorphism* if f and its induced map $E \to F$ are bijections. A *path from $u \in V$ to $v \in V$* in G is a finite sequence of vertices $(x_0, \ldots, x_n)$ for some $n \in \mathbb{Z}_{\geq 0}$ such that $x_0 = u$, $x_n = v$ and $\{x_i, x_{i+1}\} \in E$ for all $0 \leq i < n$. We call this path *non-trivial* if $n > 0$ and *closed* if $x_0 = x_n$. We say $u \in V$ is *connected* to $v \in V$ in G if there exists a path from u to v in G. The 'is connected to' relation is an equivalence relation on V and we call its equivalence classes the *connected components* of G. For $u \in V$ we call $v \in V$ a *neighbor* of u if $\{u, v\} \in E$ and we write $N_G(u) \subseteq V$ for the set of neighbors of u. An edge $\{u, v\} \in E$ is called a *bridge* if all paths in G from

u to v contain the edge $\{u, v\}$. A *forest* is a graph in which every edge is a bridge.

We now give some facts about (non-)planar graphs.

Definition 1.2.1. For $A, B \in \mathbb{R}^2$ write $\ell(A, B)$ for the line $\{tA + (1 - t)B \mid t \in (0, 1)\}$. Let $G = (V, E)$ be a graph. A *planar embedding* of G is an injective map $\varepsilon\colon V \to \mathbb{R}^2$ such that for all distinct $\{a, b\}, \{c, d\} \in E$ we have $\ell(\varepsilon(a), \varepsilon(b)) \cap \ell(\varepsilon(c), \varepsilon(d)) = \varnothing$, and for all $\{a, b\} \in E$ we have $\ell(\varepsilon(a), \varepsilon(b)) \cap \varepsilon[V] = \varnothing$. We call G *planar* if it has a planar embedding.

The above definition of a planar embedding has been simplified for our purposes, which is justified by Fáry's Theorem [13].

Definition 1.2.2. Let $G = (V, E)$ be a graph with a planar embedding ε. The *orientation* of (G, ε) at $v \in V$ is the clockwise permutation $\rho_\varepsilon(v)$ of $N_G(v)$. A *boundary walk* of (G, ε) is a non-trivial closed path $(x_0, x_2, \ldots, x_n)$ in G such that for all $i, j \in \mathbb{Z}/n\mathbb{Z}$ we have $x_{i+2} = \rho_\varepsilon(x_{i+1})(x_i)$ and if $(x_i, x_{i+1}) = (x_j, x_{j+1})$, then $i = j$.

Lemma 1.2.3. *Let ε be a planar embedding of a graph $G = (V, E)$ and let $p = (u_1, u_2, \ldots, u_n)$ be a boundary walk. If $(u_i, u_{i+1}) = (u_{j+1}, u_j)$ for some $i, j \in \mathbb{Z}/n\mathbb{Z}$, then $\{u_i, u_j\}$ is a bridge.*

Proof. To show that $e = \{u_i, u_j\}$ is a bridge, it suffices to show that u_i and u_j are disconnected in the graph $G' = (V, E')$ with $E' = E \setminus \{e\}$. Note that $a, b \in V$ are connected in G' if and only if $\varepsilon(a)$ and $\varepsilon(b)$ are connected in the topological space $X = \varepsilon[V] \cup \bigcup_{\{x,y\} \in E'} \ell(\varepsilon(x), \varepsilon(y))$. Hence it suffices by the Jordan curve theorem to show that there exists a loop C in $\mathbb{R}^2 \setminus X$ separating u_i and u_j, as any path from u_i to u_j must intersect this loop.

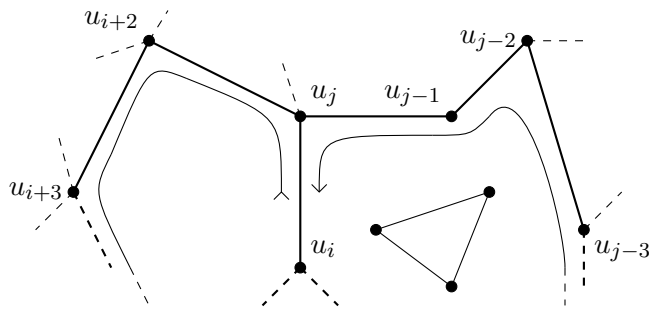


Figure 1.1: Boundary walk

We informally construct this loop as follows (see Figure 1.1). Place yourself at the midway point between u_i and u_j. Walk along the path p in G in

the direction of u_j and while doing so draw a continuous curve C on your left hand side, being careful not to let C intersect itself or the graph. That this is possible follows from the definition of a boundary walk. Stop once you have reached your starting point for the first time again, and note that this time you are facing u_i by the assumption that $(u_i, u_{i+1}) = (u_{j+1}, u_j)$. Thus on your right hand side is the start of your curve C, and connect the endpoints, crossing $\ell(\varepsilon(u_i), \varepsilon(u_j))$ once. Then C satisfies the requirements, so e is a bridge. □

Definition 1.2.4. Let $G = (V, E)$ be a graph. We call a subgraph $H = (W, F)$ of G a *spanning forest* if it is a forest and $W = V$. For a spanning forest $H = (W, F)$ of G we define $G_H = (C, D)$ to be the *contraction of H in G*, where C is the set of connected components of H and $D = \{\{X, Y\} \in \binom{C}{2} \mid (\exists\, u \in X,\, v \in Y)\ \{u, v\} \in E\}$. A graph M is a *minor* of G if it can be embedded in some contraction of G.

Note that the 'is a minor of' relation is a partial order (up to graph isomorphism). In particular, if I is a minor of H and H is a minor of G, then I is a minor of G. Write K_5 for the complete graph on 5 vertices and $K_{3,3}$ for the complete bipartite graph on 3 and 3 vertices.

Proposition 1.2.5 (Kuratowski, Theorem 4.4.6 in [10])**.** *A graph G is planar if and only if G does not have K_5 or $K_{3,3}$ as a minor.*

1.3 Non-planar graphs

First we show that all non-planar graphs can leak.

Lemma 1.3.1. *A graph is leak-proof if and only if all its subgraphs are leak-proof.*

Proof. Since each graph is its own subgraph, the implication ($\Leftarrow$) is trivial. Let $G = (V, E)$ be a graph with a subgraph $H = (W, F)$ and assume that there exists some group Γ with a leaking Γ-flow $g\colon W^2 \to \Gamma$ of H. Then we consider $f\colon V^2 \to \Gamma$ by taking $f(u, v) = g(u, v)$ when $\{u, v\} \in F$ and $f(u, v) = 1$ otherwise. Then f is a leaking flow for G, proving ($\Rightarrow$). □

Proposition 1.3.2. *A graph is leak-proof if and only if all its minors are leak-proof.*

Proof. Let $G = (V, E)$ be a graph. By Lemma 1.3.1 it suffices to show that if a contraction of a spanning tree H in G admits a leaking flow, then so does G. By induction we may even assume H has only a single edge

$e = \{a, b\}$. Then $(W, F) \cong G_H$ with $W = (V \setminus e) \cup \{e\}$ under the natural isomorphism $e \mapsto e$ and $w \mapsto \{w\}$ for $w \in V \setminus e$. Assume (W, F) admits a flow $f\colon W^2 \to \Gamma$ leaking at $w \in W$ for some group Γ. Let $X = N_G(a) \setminus e$ and $Y = N_G(b) \setminus (e \cup X)$. We define a flow $g\colon V^2 \to \Gamma$ such that for $u, v \in W$ it is given by

$$\begin{aligned} g(u,v) &= f(u,v) && u, v \notin e, \\ g(a,u)^{-1} = g(u,a) &= f(u,e) && u \in X, \\ g(v,b)^{-1} = g(b,v) &= f(e,v) && v \in Y, \\ g(b,a)^{-1} = g(a,b) &= \prod_{u \in X \setminus \{b\}} f(u,a), \end{aligned}$$

and $g(u, v) = 1$ otherwise. Note that g agrees with f outside of e and that the flows going to e have been divided among a and b. Thus g is tractable and $e_g(u) = e_f(u)$ for $u \notin e$. By definition of $g(a, b)$ we have that $e_g(a) = 1$ and $e_g(b) = e_f(e)$. Hence g is a leaking flow for G. □

To show that non-planar graphs are not leak-proof, it now suffices by Proposition 1.2.5 to show that K_5 and $K_{3,3}$ admit a leaking flow.

Definition 1.3.3. Let C_2 be the cyclic group with two elements. Let $n \in \mathbb{Z}_{>0}$ and consider the groups $N = C_2^{n+1} = \langle z, x_1, \ldots, x_n \rangle$ and $G = C_2^n = \langle x_{n+1}, \ldots, x_{2n} \rangle$. Consider the action $\varphi\colon G \to \mathrm{Aut}(N)$ defined on the generators as

$$x_{n+i} \mapsto \left(x_j \mapsto x_j z^{\delta_{ij}}, \quad z \mapsto z\right) \quad \text{for all } 1 \le i, j \le n,$$

where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. Then define the group $\mathrm{ES}_n = N \rtimes_\varphi G$.

Although we will not use the fact, the ES_n are all *extraspecial 2-groups*.

Example 1.3.4. Consider the utility graph $K_{3,3} = (V, E)$ with $V = \{1, 2, 3, 4, 5, 6\}$ and $E = \{\{u, v\} \mid u \in \{1, 2, 3\},\ v \in \{4, 5, 6\}\}$. We define a flow $f\colon V^2 \to \mathrm{ES}_2$ which we specify by an ES_2-valued (symmetric) matrix where the omitted entries are trivial:

$$f = \left(\begin{array}{ccc|ccc} & & & x_1 & x_2 & x_1x_2 \\ & & & x_4 & x_3 & x_4x_3 \\ & & & x_1x_4 & x_2x_3 & x_1x_4x_2x_3 \\ \hline x_1 & x_4 & x_1x_4 & & & \\ x_2 & x_3 & x_2x_3 & & & \\ x_1x_2 & x_4x_3 & x_1x_4x_2x_3 & & & \end{array}\right).$$

For the first 5 columns it is easy to see that multiplying the first two non-trivial entries yields the third. Thus for the first five vertices v we have $\langle f(u,v) \,|\, u \in V\rangle \cong C_2^2$, which is abelian, and $e_f(v) = 1$. For $v = 6$ we observe that $(x_1x_2)(x_4x_3)(x_1x_4x_2x_3) = z$ and thus $\langle f(u,6) \,|\, u \in V\rangle = \langle x_1x_2, x_4x_3, z\rangle \cong C_2^3$ is abelian, and $e_f(6) = z \neq 1$. Hence f is a tractable flow that leaks at 6 and $K_{3,3}$ is not leak-proof.

Example 1.3.5. Consider the complete graph $K_5 = (V, E)$ with $V = \{1, 2, 3, 4, 5\}$. Now we consider $f\colon V^2 \to \mathrm{ES}_3$ given by

$$f = \begin{pmatrix} & x_1 & x_2 & x_3 & x_1x_2x_3 \\ x_1 & & x_6 & x_5 & x_1x_6x_5 \\ x_2 & x_6 & & x_4 & x_2x_6x_4 \\ x_3 & x_5 & x_4 & & x_3x_5x_4 \\ x_1x_2x_3 & x_1x_6x_5 & x_2x_6x_4 & x_3x_5x_4 & \end{pmatrix}.$$

For each of the first four columns one notes that its first three non-trivial elements commute pairwise, while multiplying them yields the fourth. Thus for the first four vertices v the group $\langle f(u,v) \,|\, u \in V\rangle \cong C_2^3$ is abelian and $e_f(v) = 1$. For the last column, note that each pair (a, b) of entries is of the form $a = x_ix_jx_k$ and $b = x_ix_{j+3}x_{k+3}$ with $i, j, k, j+3, k+3 \in \mathbb{Z}/6\mathbb{Z}$ distinct. Hence

$$ab = x_i^2(x_jx_k)(x_{j+3}x_{k+3}) = x_i^2(x_{j+3}x_{k+3})(x_jx_k) = ba,$$

so each pair commutes. Finally, one computes

$$e_f(5) = (x_1x_2x_3)(x_1x_6x_5)(x_2x_6x_4)(x_3x_5x_4) = z \neq 1.$$

Thus f is a tractable leaking flow and thus K_5 is not leak-proof.

Both examples were found by starting with the free group F with symbols V^2 and dividing out the relations $N \trianglelefteq F$ required to make the obvious map $f\colon V^2 \to F/N$ a tractable flow that is conserving in $\#V - 1$ vertices. Adding the restriction that the generators have order 2 gives us the groups ES_2 and ES_3.

It now follows that all non-planar graphs leak, so we are half-way done proving Theorem 1.4.3.

1.4 Planar graphs

Now we will prove that all planar graphs are leak-proof by induction. For this we require a definition of the excess for non-tractable flows.

Definition 1.4.1. Let $G = (V, E)$ be a graph with planar embedding ε and let $f\colon V^2 \to \Gamma$ be a flow of G. Write $C(\Gamma)$ for the set of conjugacy classes of Γ and $\equiv$ for equality up to conjugation. Then we define for (G, ε, f) the *round flow* $r\colon V \to C(\Gamma)$ as $r(v) \equiv 1$ if $N_G(V) = \varnothing$, and otherwise

$$r(v) \equiv f(\rho_\varepsilon(v)^0(u), v) \cdot f(\rho_\varepsilon(v)^1(u), v) \cdots f(\rho_\varepsilon(v)^{n-1}(u), v),$$

where $u \in N_G(v)$, $n = \#N_G(v)$ and ρ_ε is as in Definition 1.2.2.

Note that choosing a different $u \in N_G(v)$ in the above definition results in a cyclic permutation of the factors, hence the products are conjugate in Γ. Thus the round flow is well-defined. Since $1 \in \Gamma$ is only conjugate to itself, we have that $r(v) \equiv 1$ if and only if $e(v) = 1$ when the latter is defined.

Proposition 1.4.2. *Let $G = (V, E)$ be a graph with planar embedding ε and let $f\colon V^2 \to \Gamma$ be a flow of G. Let $u \in V$ and assume $r(v) \equiv 1$ for all $v \in V \setminus \{u\}$. Then $r(u) \equiv 1$.*

Proof. Firstly, if G is the singleton graph, then $r(u) \equiv 1$ is the empty product, so we are done. We now apply induction and thus assume that the statement holds for all strict subgraphs (W, F) of G with planar embedding $\varepsilon|_W$. We may now assume $\#V > 1$.

Secondly, we consider the case where G is not connected. Here we may apply the induction hypothesis to the induced subgraph of G with as vertex set the connected component of u to conclude that $r(u) \equiv 1$. We may now assume G is connected.

Thirdly, we consider the case where G is a forest. Then G has at least two vertices of degree 1, of which one, say v, is not u. Let $e = \{v, w\} \in E$ be the unique edge incident to v, and note that $1 \equiv r_f(v) \equiv f(w, v)$ implies $f(w, v) = 1$. Hence f is a flow of the subgraph H of G obtained by removing e. Note that ε is a planar embedding of H with the same round flow in each vertex, hence by the induction hypothesis we have $r_f(u) \equiv 1$.

Lastly we consider the case where G not a forest. Then G has an edge $\{v, w\} \in E$ that is not a bridge. Then by Lemma 1.2.3 the boundary walk $p = (x_0, \ldots, x_n)$ of (G, ε) with $x_0 = v$ and $x_1 = w$ satisfies $(w, v) \neq (x_i, x_{i+1})$ for all $i \in \mathbb{Z}/n\mathbb{Z}$. Let $b\colon V^2 \to \{0, 1\}$ be the map such that for all $s, t \in V$ we have $b(s, t) = 1$ if and only if there exists some $i \in \mathbb{Z}/n\mathbb{Z}$ such that $(s, t) = (x_i, x_{i+1})$. Now consider $\gamma = f(v, w)$ and $g\colon V^2 \to \Gamma$ given by

$$(s, t) \mapsto \gamma^{b(t,s)} \cdot f(s, t) \cdot \gamma^{-b(s,t)}.$$

Firstly note that g is a flow of G: For all $s, t \in V$ we have

$$g(s, t)^{-1} = \gamma^{b(s,t)} \cdot f(s, t)^{-1} \cdot \gamma^{-b(t,s)} = g(t, s)$$

since f is a flow, and if $\{s,t\} \notin E$ we have $g(s,t) = f(s,t) = 1$ as $b(s,t) = b(t,s) = 0$. Secondly, we have that $g(v,w) = \gamma^0 \cdot \gamma \cdot \gamma^{-1} = 1$ by choice of $\{v,w\}$, so g is even a flow of the subgraph H of G obtained by removing $\{v,w\}$. We now show that the round flows r_f and r_g of f respectively g in (G,ε) are conjugates in Γ at each vertex. Then by the induction hypothesis applied to H it follows that $r(u) \equiv 1$. Note that for all $s,t \in V$ we have by definition of b that $b(t,s) = b(s,\rho_\varepsilon(s)(t))$. Using this, we now simply verify for $\{s,t\} \in E$, $n = \#N_G(s)$ and $\rho = \rho_\varepsilon(s)$ that

$$\begin{aligned} r_g(s) &\equiv \prod_{k=0}^{n-1} g(\rho^k(t),s) \equiv \prod_{k=0}^{n-1} \gamma^{b(s,\rho^k(t))} \cdot f(\rho^k(t),s) \cdot \gamma^{-b(\rho^k(t),s)} \\ &\equiv \gamma^{b(s,t)} \left(\prod_{k=0}^{n-1} f(\rho^k(t),s) \gamma^{-b(\rho^k(t),s)} \gamma^{b(s,\rho^{k+1}(t))} \right) \gamma^{-b(s,\rho^n(t))} \\ &\equiv \gamma^{b(s,t)} \left(\prod_{k=0}^{n-1} f(\rho^k(t),s) \right) \gamma^{-b(s,t)} \equiv \prod_{k=0}^{n-1} f(\rho^k(t),s) \equiv r_f(s), \end{aligned}$$

as was to be shown. We conclude that the statement holds for all planar graphs by induction. □

An earlier proof of Proposition 1.4.2 was due to H.W. Lenstra. In his version he does not remove edges in the inductive step but contracts them in the sense of Definition 1.2.4. This proof turned out to be more difficult to formalize.

Theorem 1.4.3. *A graph is leak-proof if and only if it is planar.*

Proof. A non-planar graph has either K_5 or $K_{3,3}$ as minor by Proposition 1.2.5. Both K_5 and $K_{3,3}$ are not leak-proof by Example 1.3.5 respectively Example 1.3.4, so by Proposition 1.3.2 neither are the non-planar graphs. Let $G = (V,E)$ be a planar graph with $u \in V$ and let f be a tractable flow of G such that $e(v) = 1$ for all $v \in V \setminus \{u\}$. After choosing a planar embedding for G we have $r(u) \equiv 1$ by Proposition 1.4.2 and thus $e(u) = 1$. Hence f does not leak and G is leak-proof. □

1.5 Extra-planar graphs

In this section we will prove Theorem 1.5.2, classifying the binary leak-proof graphs. To do this we first prove a 'Kuratowski's Theorem' for extra-planar graphs. Write K_5^- and $K_{3,3}^-$ for the graphs obtained from K_5 respectively $K_{3,3}$ by removing a single edge, which by symmetry we do not have to specify.

Proposition 1.5.1. *A graph G is extra-planar if and only if G does not have K_5^- or $K_{3,3}^-$ as a minor.*

Proof. ($\Rightarrow$) This follows directly from Kuratowski's Theorem: If K_5^- or $K_{3,3}^-$ is a minor of G, then we may add a single edge to G such that K_5 respectively $K_{3,3}$ becomes a minor of this new graph, which is then non-planar.

($\Leftarrow$) We proceed by contraposition, so assume that G is not extra-planar. Let $u, v \in V$ be such that $G^+ = (V, E \cup \{\{u, v\}\})$ is non-planar and let $H^+ = (V, F)$ be a spanning forest of G^+ such that K_5 or $K_{3,3}$ embeds into G_H^+. Consider the spanning forest $H = (V, F \setminus \{\{u, v\}\})$ of G. Then H has the same connected components as H^+ with the exception that if H^+ has a connected component containing both u and v, it might have been split into two. Let T_u and T_v be the connected components of u respectively v in H.

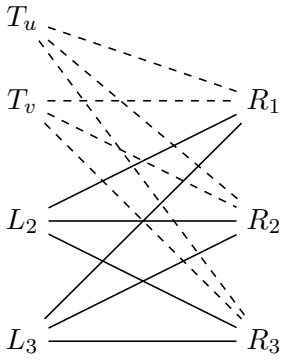


Figure 1.2: Case $K_{3,3}$

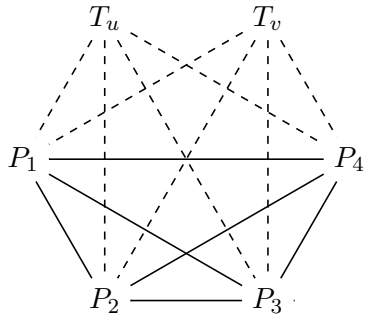


Figure 1.3: Case K_5

Case $K_{3,3}$: First consider the case where $K_{3,3}$ embeds into $G_{H^+}^+$, meaning there is a subset $C = \{L_1, L_2, L_3, R_1, R_2, R_3\}$ of size 6 of the set of connected components of H^+ such that $S^+ = (C, \{\{L_i, R_j\} \mid i, j \in \{1, 2, 3\}\})$ is a subgraph of $G_{H^+}^+$. If all elements of C are also connected components of H, then G_H has the graph S^+ minus possibly a single edge induced by $\{u, v\}$ as subgraph, hence G has $K_{3,3}^-$ as a minor. Otherwise, for some $X \in C$ we have $X = T_u \sqcup T_v$ and without loss of generality $X = L_1$. Then the subgraph S of G_H induced by $\{T_u, T_v, L_2, L_3, R_1, R_2, R_3\}$ is as in Figure 2, where the dashed lines indicate edges which are possibly present. Merging T_u and T_v in S yields $S^+ \cong K_{3,3}$, hence for each $i \in \{1, 2, 3\}$ the edge $\{T_u, R_i\}$ or $\{T_v, R_i\}$ is present. Thus T_u or T_v has degree at least 2, which without loss of generality is T_v. It follows that $K_{3,3}^-$ embeds into the subgraph of G_H induced by $\{T_v, L_2, L_3, R_1, R_2, R_3\}$, so $K_{3,3}^-$ is a minor of G.

Case K_5: Now consider the case K_5 embeds into $G^+_{H^+}$, meaning there is a subset $C = \{P_1, \dots, P_5\}$ of the set of connected components of H^+ such that the subgraph of $G^+_{H^+}$ induced by C is isomorphic to K_5. As before, the only interesting case is where $P_5 = T_u \sqcup T_v$. Then the subgraph S of G_H induced by $\{T_u, T_v, P_1, P_2, P_3, P_4\}$ is as in Figure 3. Since merging T_u and T_v in S yields K_5, for each $i \in \{1, \dots, 4\}$ the edge $\{T_u, P_i\}$ or $\{T_v, P_i\}$ is present. If both T_u and T_v have degree 2, then without loss of generality S contains the edges $\{T_u, P_3\}$, $\{T_u, P_4\}$, $\{T_v, P_1\}$ and $\{T_v, P_2\}$. Now note that S contains a $K^-_{3,3}$ which partitions its vertices as $\{\{T_u, P_1, P_2\}, \{T_v, P_3, P_4\}\}$. Hence G contains $K^-_{3,3}$ as a minor. Otherwise, without loss of generality T_u has degree at least 3 in S and the subgraph of G_H induced by $\{T_u, P_1, \dots, P_4\}$ is either K_5 or K^-_5. Hence G has K^-_5 as a minor.

As G has $K^-_{3,3}$ or K^-_5 as a minor, the claim follows. □

We are now able to prove Theorem 1.5.2.

Theorem 1.5.2. *A graph is binary leak-proof if and only if it is extra-planar.*

Proof. ($\Leftarrow$) Let $G = (V, E)$ be an extra-planar graph and let $f \colon V^2 \to \Gamma$ be a tractable flow of G such that there are distinct $u, v \in V$ with $e_f(w) = 1$ for all $w \in V \setminus \{u, v\}$. Consider the graph $H = (V, E \cup \{\{u, v\}\})$ and let ε be a planar embedding of H. Now let $g \colon V^2 \to \Gamma$ be the map such that $g(s, t) = f(s, t)$ if $\{s, t\} \neq \{u, v\}$ and $g(u, v) = g(v, u)^{-1} = f(u, v) r_f(v)^{-1}$, where $r_f(v)$ is computed by starting from the vertex right after u in the ordering of $N_H(v)$. Then g is a (not necessarily tractable) flow in H such that $r_g(w) = 1$ for $w \in V \setminus \{u\}$. From $g(v, u) = r_f(v) f(v, u)$ it follows that $r_g(u)$ differs from $r_f(u)$ by a factor $r_f(v)$ when starting the multiplication at v. By Proposition 1.4.2 we have $1 \equiv r_g(u) \equiv r_f(u) r_f(v)$ and thus $e_f(u) e_f(v) = 1$. Hence G is binary leak-proof.

($\Rightarrow$) If $G = (V, E)$ is not extra-planar, then it has K^-_5 or $K^-_{3,3}$ as minor by Proposition 1.5.1. It is straightforward to generalize Proposition 1.3.2 to show that a graph is binary leak-proof if and only if all its minors are too. It therefore suffices to show that K^-_5 and $K^-_{3,3}$ have a binary leaking flow. Simply take the flow f as defined in Example 1.3.4 which leaks at vertex 6 of $K_{3,3}$ and consider $K^-_{3,3}$ as the $K_{3,3}$ with the edge $\{3, 6\}$ removed. Then the flow f^- of $K^-_{3,3}$ which equals f except for $f^-(3, 6) = f^-(6, 3) = 1$ has a binary leak at 3 and 6. Using Example 1.3.5 for K^-_5 can be done analogously. □

1.6 Leak-proof groups

In this section we prove Theorem 1.6.4 and give some computational results.

Definition 1.6.1. Let Γ be a (not necessarily finite) group. Write $V(\Gamma)$ for the set of maximal abelian subgroups of Γ. We define the group

$$F(\Gamma) = \Big\{ (f_{u,v})_{(u,v)} \in \bigoplus_{(u,v)\in V(\Gamma)^2} (u \cap v) \;\Big|\; (\forall\, u, v)\ f_{u,v} = f_{v,u}^{-1},\ (\forall\, v)\ f_{v,v} = 1 \Big\}$$

and the homomorphism

$$e_\Gamma \colon F(\Gamma) \to \bigoplus_{v\in V(\Gamma)} v, \quad (f_{u,v})_{(u,v)} \mapsto \Big(\prod_{u\in V(\Gamma)} f_{u,v} \Big)_{v\in V(\Gamma)}.$$

One can think of $V(\Gamma)$ as the vertex set of a complete graph, $F(\Gamma)$ the set of tractable flows in this graph, and $e_\Gamma(f)$ to be the excess for such flow $f \in F(\Gamma)$. However, $V(\Gamma)$ need not be finite. For example $\Gamma = \mathrm{GL}_2(\mathbb{R})$ has a maximal abelian subgroup $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{R},\ a \neq 0\}$ with infinitely many conjugates.

Lemma 1.6.2. *Let Γ be a group. For $u \in V(\Gamma)$ and $\gamma \in u$ let $[\gamma]_u \in \bigoplus_{v\in V(\Gamma)} v$ be the vector consisting of all-ones except for a γ at coordinate u. We write $\Gamma^\bullet = (\bigoplus_{v\in V(\Gamma)} v)/\operatorname{im}(e)$. Then the map $d\colon \Gamma \to \Gamma^\bullet$ given by $\gamma \mapsto [\gamma]_v$ for any choice of v containing γ, does not depend on the choice of v.*

Proof. Let $\gamma \in \Gamma$ and suppose $u, v \in V(\Gamma)$ are such that $\gamma \in u$ and $\gamma \in v$. Then $\gamma \in u \cap v$, and $f = (f_{s,t})_{(s,t)\in V(\Gamma)^2}$, with $f_{u,v} = f_{v,u}^{-1} = \gamma$ and $f_{s,t} = 1$ for $\{s,t\} \neq \{u,v\}$, is an element of $F(\Gamma)$. We have $e(f) = [\gamma]_v \cdot [\gamma]_u^{-1}$, so $[\gamma]_u$ is equivalent to $[\gamma]_v$ in the quotient $\Gamma^\bullet$. □

An example one can consider is where Γ is abelian. Then $V(\Gamma) = \{\Gamma\}$ and $\Gamma^\bullet = \Gamma$ and d is the identity. Note that d is (in general) not a group homomorphism.

Proposition 1.6.3. *A group Γ is leak-proof if and only if $d(\gamma) = 1$ implies $\gamma = 1$.*

Proof. Suppose Γ is leak-proof and $d(\gamma) = 1$ for some $\gamma \in \Gamma$. Then there is some $u \in V(\Gamma)$ and $f \in F(\Gamma)$ such that $[\gamma]_u = e(f)$. Note that $E = \{\{u,v\} \in V(\Gamma) \mid f_{u,v} \neq 1\}$ and $V = \{u \mid \{u,v\} \in E\}$ are finite. Now f is a Γ-flow in (V,E) which is preserving in all vertices except possibly u. Since Γ is leak-proof, f is also preserving in u and $1 = e(f) = [\gamma]_u$, so $\gamma = 1$.

Conversely, suppose f is a tractable Γ-flow in some graph (V, E). Pick some map $c\colon V \to V(\Gamma)$ such that for all $v \in V$ we have $\langle f(u, v) \mid u \in V\rangle \subseteq c(v)$. Then f induces a tractable Γ-flow f' in the complete graph with vertex set $\{c(v) \mid v \in V\}$ where

$$f'(s, t) = \prod_{u\colon c(u)=s} \prod_{v\colon c(v)=t} f(u, v) \in s \cap t.$$

Hence $f' \in F(\Gamma)$. Moreover, if f leaks, then so does f'. Assume f' is preserving in all vertices except potentially $v \in V$. Then $e(f') = [\gamma]_v$ for some $\gamma \in v$ and $d(\gamma) = 1$. If $d(\gamma) = 1$ implies $\gamma = 1$, we obtain that f' and hence f does not leak, so Γ is leak-proof. □

Similarly, one can consider binary leak-proof groups. With a proof analogous to that of Proposition 1.6.3 one obtains that Γ is binary leak proof if and only if d is injective.

Theorem 1.6.4. *The decision problem 'Is this finite group leak-proof?' is decidable.*

Proof. Simply note that for finite Γ the corresponding group $\Gamma^\bullet$ is finite abelian and can thus be computed explicitly. In particular, we can decide for each $\gamma \in \Gamma$ whether $d(\gamma) = 1$. The theorem thus follows from Proposition 1.6.3. □

From Lemma 1.1.1 it follows that abelian groups are leak-proof, but they are hardly the only ones. By computer search we found the two extraspecial groups of order 32 to be the only smallest leaking groups, one of which we encountered in Example 1.3.4. The smallest leaking groups of order greater than 32 occur at order 64. That there are groups of order 64 that leak was to be expected, because a group leaks when it has a leaking subgroup. The smallest leaking symmetric group is the S_6 and the smallest leaking alternating group is the A_7. That for sufficiently large n the group S_n leaks is to be expected by Cayley's theorem, but interestingly no strict subgroup of S_6 leaks. It would be interesting to have a classification of leak-proof groups or to know whether there is some equivalent, better understood property of groups which is equivalent to being leak-proof like planarity is for graphs.

Our code is available online [21] and is written in GAP [15].

CHAPTER 2

Hilbert lattices

2.1 Introduction

This chapter is based on [18]. A set of $\mathbb{R}$-linearly independent vectors $\{b_1, \ldots, b_k\}$ of some Euclidean vector space such as $\mathbb{R}^n$ gives rise to a discrete subgroup

$$\Big\{ \sum_{i=1}^{k} x_i b_i \,\Big|\, x_1, \ldots, x_k \in \mathbb{Z} \Big\},$$

which we call a lattice. In particular, a lattice is a free abelian group of finite rank. In preparation of Chapter 3 we study a generalization of lattices that includes 'infinite rank lattices'. These will be the discrete subgroups of Hilbert spaces, which we call *Hilbert lattices*, and they include the 'Euclidean lattices' as a special case. We will primarily generalize existing theory from the finite dimensional case, and highlight the things that fail to generalize.

Theorem 2.3.13. *Every countable subgroup of a Hilbert lattice is free.*

Whether or not all Hilbert lattices are free themselves is still an open problem. Let Λ be a Hilbert lattice. An *orthogonal decomposition* of Λ is a decomposition $\{\Lambda_i\}_{i\in I}$ of Λ as abelian group, as defined in the Preliminaries, such that $\langle \Lambda_i, \Lambda_j \rangle = \{0\}$ for all distinct $i, j \in I$. The collection of orthogonal decompositions of Λ inherit the structure of a category. We say an orthogonal decomposition is *universal* if it is an initial object in this category.

Theorem 2.5.4. *Every Hilbert lattice has a universal orthogonal decomposition.*

Let Λ be a Hilbert lattice in a Hilbert space $\mathcal{H}$. The *Voronoi cell* of Λ is the set

$$\mathrm{Vor}(\Lambda) = \{ z \in \mathcal{H} \mid (\forall\, x \in \Lambda \setminus \{0\})\ \|z\| < \|z - x\| \},$$

i.e. the set of all points which have the origin as their unique closest lattice point. It is almost a 'fundamental domain' for Λ.

Theorem 2.6.9. *Let Λ be a Hilbert lattice in a Hilbert space $\mathcal{H}$ and consider the natural map $\mathcal{H} \to \mathcal{H}/\Lambda$. Its restriction to $\mathrm{Vor}(\Lambda)$ is injective and for all $\varepsilon > 0$ its restriction to $(1+\varepsilon)\,\mathrm{Vor}(\Lambda)$ is surjective.*

A *decomposition* of $z \in \Lambda$ is a pair $(x, y) \in \Lambda^2$ such that $x + y = z$ and $\langle x, y \rangle \geq 0$. We say $x \in \Lambda$ is *indecomposable* or *Voronoi relevant* if it has precisely 2 decompositions, i.e. $(0, x)$ and $(x, 0)$ are the only decompositions and $x \neq 0$. One can interpret the Voronoi cell as the intersection of half

spaces $H_x = \{z \in \mathcal{H} \mid \|z\| < \|z - x\|\}$, but we do not need all $x \in \Lambda \setminus \{0\}$ to carve out $\mathrm{Vor}(\Lambda)$. For example, $H_x \cap H_{2x} = H_x$.

Theorem 2.6.11. *Let Λ be a Hilbert lattice in a Hilbert space $\mathcal{H}$. Then there exists a unique set $S \subseteq \Lambda \setminus \{0\}$ which is minimal with respect to inclusion such that $\mathrm{Vor}(\Lambda) = \{z \in \mathcal{H} \mid (\forall\, x \in S)\ \|z\| < \|z - x\|\}$, and S equals the set of indecomposable vectors.*

2.2 Inner products and Hilbert spaces

Definition 2.2.1. Let $R \subseteq \mathbb{C}$ be a subring. An *R-norm* on an R-module M is a map $\|\cdot\| \colon M \to \mathbb{R}_{\geq 0}$ that satisfies:

(*Absolute homogeneity*) For all $x \in M$ and $a \in R$ we have $\|ax\| = |a| \cdot \|x\|$;

(*Triangle inequality*) For all $x, y \in M$ we have $\|x + y\| \leq \|x\| + \|y\|$;

(*Positive-definiteness*) For all non-zero $x \in M$ we have $\|x\| \in \mathbb{R}_{>0}$.

A *normed R-module* is an R-module M together with an R-norm on M. For normed R-modules M and N an R-module homomorphism $f \colon M \to N$ is called an *isometric map* if $\|x\| = \|f(x)\|$ for all $x \in M$. The isometric maps are the morphisms in the category of normed R-modules.

Note that an isometric map is injective, but not necessarily surjective.

Definition 2.2.2. Let $R \subseteq \mathbb{C}$ be a subring and M be an R-module. An *R-inner product* on M is a map $\langle \cdot, \cdot \rangle \colon M^2 \to \mathbb{C}$ that satisfies:

(*Conjugate symmetry*) For all $x, y \in M$ we have $\langle x, y \rangle = \overline{\langle y, x \rangle}$;

(*Left linearity*) For all $x, y, z \in M$ and $a \in R$ we have

$$\langle x + ay, z \rangle = \langle x, z \rangle + a\langle y, z \rangle;$$

(*Positive-definiteness*) For all non-zero $x \in M$ we have $\langle x, x \rangle \in \mathbb{R}_{>0}$.

We say it is a *real* inner product if $\langle M, M \rangle \subseteq \mathbb{R}$, which implies $R \subseteq \mathbb{R}$ when $M \neq 0$. An *R-inner product space* is an R-module together with an R-inner product. For R-inner product spaces M and N a morphism is an R-module homomorphism $f \colon M \to N$ for which there exists an R-module homomorphism $f^* \colon N \to M$ such that $\langle f(x), y \rangle = \langle x, f^*(y) \rangle$ for all $x \in M$ and $y \in N$. This f^* is unique if it exists, and we call it the *adjoint* of f.

Remark 2.2.3. An R-inner product space M comes with an R-norm given by $\|x\| = \sqrt{\langle x, x \rangle}$, which in turn induces a metric $d(x, y) = \|x - y\|$ and a topology. One can then speak about the completeness of M with respect to this metric.

Lemma 2.2.4. *Suppose $R \subseteq \mathbb{C}$ is a subring and M is a real R-inner product space. Then the induced norm satisfies the* parallelogram law*: For all $x, y \in M$ we have*

$$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2. \quad \square$$

The following is an exercise in many standard texts.

Theorem 2.2.5 (Jordan–von Neumann [26])**.** *Let $R \subseteq \mathbb{Q}$ be a subring, M an R-module and suppose a map $\|\cdot\| \colon M \to \mathbb{R}_{\geq 0}$ satisfies positive-definiteness and the parallelogram law. Then $\|\cdot\|$ is an R-norm on M induced by a real R-inner product $\langle \cdot\,, \cdot \rangle \colon M^2 \to \mathbb{R}$ given by*

$$\langle x, y \rangle = \tfrac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2).$$

Proof. Note that taking $x = y = 0$ in the parallelogram law shows $2\|0\|^2 = 4\|0\|^2$, hence $\|0\| = 0$. For all $x \in M$ we have $\|x+x\|^2 = 2\|x\|^2 + 2\|x\|^2 - \|x-x\|^2 = 4\|x\|^2$, hence $\langle x, x \rangle = \frac{1}{2}(\|2x\|^2 - 2\|x\|^2) = \|x\|^2$. It now suffices to show that $\langle \cdot\,, \cdot \rangle$ is an inner product, as $\|\cdot\|$ is then the associated norm as in Remark 2.2.3. Clearly $\langle \cdot\,, \cdot \rangle$ satisfies conjugate symmetry and positive definiteness, so it remains to prove left linearity. It suffices to show for all $x \in M$ that $x \mapsto \langle x, z \rangle$ is $\mathbb{Z}$-linear: Since R is in the field of fractions of $\mathbb{Z}$, any $\mathbb{Z}$-linear map to $\mathbb{R}$ is also R-linear. Let $x, y, z \in M$ and note that $\langle x, y \rangle = \frac{1}{4}(\|x+y\|^2 - \|x-y\|^2)$. By the parallelogram law we have

$$\begin{aligned} 2\|y+z\|^2 + 2\|x\|^2 - \|-x+y+z\|^2 &= \|x+y+z\|^2 \\ &= 2\|x+z\|^2 + 2\|y\|^2 - \|x-y+z\|^2. \end{aligned}$$

so

$$\begin{aligned} 2\|x+y+z\|^2 + \|-x+y+z\|^2 + \|x-y+z\|^2 \\ = 2\|x+z\|^2 + 2\|y+z\|^2 + 2\|x\|^2 + 2\|y\|^2. \end{aligned}$$

Applying this equation also with z replaced by $-z$, we obtain

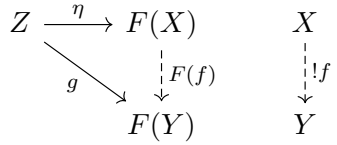
$$\begin{aligned} 8\langle x+y, z \rangle &= 2\|x+y+z\|^2 - 2\|x+y-z\|^2 \\ &= 2\|x+z\|^2 + 2\|y+z\|^2 - 2\|x-z\|^2 - 2\|y-z\|^2 \\ &= 8\langle x, z \rangle + 8\langle y, z \rangle, \end{aligned}$$

as was to be shown. We conclude that $\langle \cdot\,, \cdot \rangle$ is an R-inner product. $\square$

Inner product spaces over $\mathbb{Z}$ or $\mathbb{Q}$ can be extended to $\mathbb{R}$ in a 'canonical' way. This can best be expressed in a categorical sense in terms of universal morphisms. We proceed as in Chapter III of [37].

Definition 2.2.6. Let $\mathcal{C}$ be a category. An object U of $\mathcal{C}$ is called *universal* if for each object X of $\mathcal{C}$ there exists a unique morphism $U \to X$ in $\mathcal{C}$.

Definition 2.2.7. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. Let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor and Z an object of $\mathcal{D}$. A *universal morphism* from Z to F is a pair (X, η) with X an object of $\mathcal{C}$ and $\eta \in \mathrm{Hom}_{\mathcal{D}}(Z, F(X))$ such that for all objects Y of $\mathcal{C}$ and every $g \in \mathrm{Hom}_{\mathcal{D}}(Z, F(Y))$ there exists a unique $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ for which $F(f) \circ \eta = g$. Equivalently, for all objects Y of $\mathcal{C}$ and morphisms $g\colon Z \to F(Y)$ we have the following diagram:



For a reader familiar with category theory we remark that, if for a functor $F\colon \mathcal{C} \to \mathcal{D}$ every object Z of $\mathcal{D}$ has a universal morphism to F, then F is a *right adjoint* functor.

Example 2.2.8. We will give a concrete example of a universal morphism.

1. Let k be a field. Consider the forgetful functor F from the category of k-vector spaces to the category of abelian groups, i.e. the functor that sends a k-vector space to its underlying abelian group. Now let Z be an abelian group. We take $X = k \otimes_{\mathbb{Z}} Z$, which is a k-vector space, and $\eta\colon Z \to F(X)$ the map $z \mapsto 1 \otimes z$. Because F is a forgetful functor, as will always be the case in our applications, we may omit it in the notation for simplicity and state that η is a morphism $Z \to X$ of abelian groups.

Now let $g\colon Z \to Y$ be a morphism of abelian groups, and take $f\colon X \to Y$ to be the morphism $a \otimes z \mapsto a \cdot g(z)$ of k-vector spaces. Then $(f \circ \eta)(z) = f(1 \otimes z) = g(z)$ for all $z \in Z$, so $f \circ \eta = g$. Suppose f' also satisfies $f' \circ \eta = g$. Then $(f - f') \circ \eta = 0$. Since $\eta(Z)$ generates X as a k-vector space we obtain $f - f' = 0$, so f is unique and (X, η) is a universal morphism.

Since (X, η) is universal the vector space X corresponding to Z is 'uniquely unique', meaning that any other universal morphism (X', η') induces a unique isomorphism $\varphi\colon X \to X'$ such that $\varphi \circ \eta = \eta'$.

Note that η need not be injective. For $k = \mathbb{Q}$ it is only injective when A is torsion-free. Then η can be thought of as a canonical embedding.

2. Similarly, we can consider a forgetful functor F from the category of $\mathbb{Q}$-inner product spaces to the category of $\mathbb{Z}$-inner product spaces. The underlying universal morphism (X, η) is the same as before, and we equip X with the inner product we extend $\mathbb{Q}$-bilinearly from Z. To show that

this inner product is positive definite we use that A is torsion-free, being a $\mathbb{Z}$-inner product space.

Definition 2.2.9. A *Hilbert space* is an $\mathbb{R}$-module $\mathcal{H}$ equipped with a real $\mathbb{R}$-inner product such that $\mathcal{H}$ is complete with respect to the induced metric. The morphisms of Hilbert spaces are the isometric maps.

Theorem 2.2.10 (Theorem 3.2-3 in [29])**.** *Let F be the forgetful functor from the category of Hilbert spaces to the category of $\mathbb{Q}$-inner product spaces. Then every $\mathbb{Q}$-inner product space V has an injective universal morphism to F, and a morphism $f\colon V \to \mathcal{H}$ for some Hilbert space $\mathcal{H}$ is universal precisely when f is injective and the image of f is dense in $\mathcal{H}$.* □

The Hilbert space constructed for V in Theorem 2.2.10 can be obtained as the topological completion of V with respect to the metric induced by the inner product, and the inner product is extended continuously.

Definition 2.2.11. For a set B and $p \in \mathbb{R}_{>0}$ we define the $\mathbb{R}$-vector space

$$\ell^p(B) = \left\{ (x_b)_b \in \mathbb{R}^B \;\middle|\; \begin{array}{l} x_b = 0 \text{ for all but countably many } b \in B \\ \text{and } \sum_{b\in B} |x_b|^p < \infty \end{array} \right\}$$

and $\|x\|_p = (\sum_{b\in B} |x_b|^p)^{1/p}$ for all $x = (x_b)_b \in \ell^p(B)$.

Theorem 2.2.12 (Minkowski's inequality, Theorem 1.2-3 in [29])**.** *For any set B and $p \in \mathbb{R}_{\geq 1}$ the map $\|\cdot\|_p$ is an $\mathbb{R}$-norm on $\ell^p(B)$.* □

Lemma 2.2.13 (Example 3.1-6 in [29])**.** *For any set B the space $\ell^2(B)$ is a Hilbert space with inner product given by $\langle x, y\rangle = \sum_{b\in B} x_b \cdot y_b$ for $x = (x_b)_b, y = (y_b)_b \in \ell^2(B)$, such that $\langle x, x\rangle = \|x\|_2^2$.* □

Lemma 2.2.14. *Let $n \in \mathbb{Z}_{\geq 1}$, $x \in \mathbb{R}^n$ and let $0 < p \leq q$ be real. Then we have*

$$\|x\|_q \leq \|x\|_p \quad \textit{and} \quad n^{-1/p} \cdot \|x\|_p \leq n^{-1/q} \cdot \|x\|_q.$$

Proof. Clearly we may assume $x \neq 0$. For the first inequality, consider $y = x/\|x\|_p$. Then $|y_i| \leq 1$ for all i, from which $|y_i|^q \leq |y_i|^p$ follows. Now

$$\|y\|_q^q = \sum_{i=1}^n |y_i|^q \leq \sum_{i=1}^n |y_i|^p = \|y\|_p^p = 1.$$

Hence $\|x\|_q/\|x\|_p = \|y\|_q \leq 1$, as was to be shown. For the second inequality, note that $x \mapsto x^{q/p}$ is a convex function on $\mathbb{R}_{\geq 0}$. We have by Jensen's inequality (Theorem 7.3 in [7]) that

$$\|x\|_q^q = \sum_{i=1}^n |x_i|^q = \sum_{i=1}^n |x_i^p|^{q/p} \geq n \left(\frac{1}{n} \sum_{i=1}^n |x_i|^p \right)^{q/p} = n^{1-q/p} \|x\|_p^q,$$

so $n^{-1/p} \cdot \|x\|_p \leq n^{-1/q} \cdot \|x\|_q$. □

Definition 2.2.15. Let $\mathcal{H}$ be a Hilbert space. A subset $S \subseteq \mathcal{H}$ is called *orthogonal* if $0 \notin S$ and $\langle x, y\rangle = 0$ for all distinct $x, y \in S$. The *orthogonal dimension* of $\mathcal{H}$, written $\operatorname{orth\,dim} \mathcal{H}$, is the cardinality of a maximal orthogonal subset of $\mathcal{H}$.

That the orthogonal dimension is well-defined, i.e. that maximal orthogonal subsets of a given Hilbert space have the same cardinality follows from Proposition 4.14 in [6].

Theorem 2.2.16 (Theorem 5.4 in [6])**.** *Let $\mathcal{H}$ be a Hilbert space and B a set. Then the Hilbert spaces $\mathcal{H}$ and $\ell^2(B)$ are isomorphic if and only if the cardinality of B equals* $\operatorname{orth\,dim} \mathcal{H}$. □

In particular, up to isomorphism every Hilbert space is of the form $\ell^2(B)$ for some set B.

2.3 Hilbert lattices

Definition 2.3.1. A *Hilbert lattice* is an abelian group Λ together with a map $q\colon \Lambda \to \mathbb{R}$, which we then call the *square-norm* of Λ, that satisfies:

(*Parallelogram law*) For all $x, y \in \Lambda$ we have

$$q(x + y) + q(x - y) = 2q(x) + 2q(y);$$

(*Positive packing radius*) There exists an $r \in \mathbb{R}_{>0}$ such that $q(x) \geq r$ for all non-zero $x \in \Lambda$.

We write $\mathrm{P}(\Lambda) = \inf\{q(x) \mid x \in \Lambda \setminus \{0\}\}$.

The following lemma gives an equivalent definition of a Hilbert lattice.

Lemma 2.3.2. *A Hilbert lattice Λ with square-norm q is a discrete $\mathbb{Z}$-inner product space with inner product given by*

$$(x, y) \mapsto \frac{1}{2}(q(x + y) - q(x) - q(y)).$$

Conversely, every discrete $\mathbb{Z}$-inner product space M is a Hilbert lattice with square norm given by $x \mapsto \langle x, x\rangle$.

Proof. The first statement is Theorem 2.2.5 with the observation that the positive packing radius implies non-degeneracy and discreteness. The second statement is Lemma 2.2.4 with the observation that discreteness implies a positive packing radius. □

Example 2.3.3. Consider for some $n \in \mathbb{Z}_{\geq 0}$ the vector space $\mathbb{R}^n$ with the standard inner product. If $\Lambda \subseteq \mathbb{R}^n$ is a discrete subgroup, then Λ is a Hilbert lattice when q is given by $x \mapsto \|x\|^2$.

Example 2.3.4. Let B be a set. Then

$$\mathbb{Z}^{(B)} = \{(x_b)_b \in \mathbb{Z}^B \mid x_b = 0 \text{ for all but finitely many } b\}$$

is a Hilbert lattice in $\ell^2(B)$ when q is given by $x \mapsto \|x\|^2$. In fact, any discrete subgroup of $\ell^2(B)$ is a Hilbert lattice.

Example 2.3.5. The infimum defining $\mathrm{P}(\Lambda)$ of a Hilbert lattice Λ need not be attained. Certainly if $\Lambda = 0$ we have that $\mathrm{P}(\Lambda) = \infty$ is not attained. For an example of a non-degenerate Λ consider the following. For a set I and a map $f\colon I \to \mathbb{R}_{\geq 0}$ we write Λ^f for the group $\mathbb{Z}^{(I)}$ together with the map $q((x_i)_i) = \sum_{i \in I} f(i)^2 x_i^2$. Note that $\inf\{q(x) \mid x \in \Lambda^f \setminus \{0\}\} = \inf\{f(i)^2 \mid i \in I\}$, so Λ^f is a Hilbert lattice if and only if $\inf\{f(i) \mid i \in I\} > 0$. We now simply take $f\colon \mathbb{Z}_{>0} \to \mathbb{R}_{\geq 0}$ given by $n \mapsto 1 + 1/n$.

Lemma 2.3.6. *Let Λ be a Hilbert lattice with square-norm q. Then any subgroup $\Lambda' \subseteq \Lambda$ is a Hilbert lattice when equipped with the square-norm $q|_{\Lambda'}$.* □

Theorem 2.3.7. *Let F be the forgetful functor from the category of Hilbert spaces to the category of $\mathbb{Z}$-inner product spaces. Then every $\mathbb{Z}$-inner product space L has an injective universal morphism η to F. For every $\mathbb{Z}$-inner product space L, Hilbert space $\mathcal{H}$ and injective morphism $f\colon L \to \mathcal{H}$ we have that f is universal if and only if $\mathbb{Q} \cdot f(L)$ is dense in $\mathcal{H}$, and L is a Hilbert lattice if and only if $f(L)$ is discrete in $\mathcal{H}$.*

It follows from this theorem that the Hilbert lattices are, up to isomorphism, precisely the discrete subgroups of Hilbert spaces. Hence Theorem 2.3.7 allows us to assume without loss of generality that a Hilbert lattice is a discrete subgroup of a Hilbert space.

Proof. The first and second statement are just a combination of Example 2.2.8.2 and Theorem 2.2.10, while the third is trivial when taking the equivalent definition of Lemma 2.3.2. □

Remark 2.3.8. Let Λ be a Hilbert lattice in a Hilbert space $\mathcal{H}$ and suppose that Λ is finitely generated. Then $\mathbb{R}\Lambda$ is a finite dimensional $\mathbb{R}$-inner product space and thus complete. It follows that $\Lambda \to \mathbb{R}\Lambda$ is a universal morphism because $\mathbb{Q}\Lambda$ is dense in $\mathbb{R}\Lambda$. Since $\mathbb{R}\Lambda$ is finite dimensional, Λ is a lattice in the classical sense: a discrete subgroup of a Euclidean vector space.

Lemma 2.3.9. *Let Λ be a Hilbert lattice in a Hilbert space $\mathcal{H}$. Then the natural map $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \to \mathcal{H}$ is injective.*

Proof. To show $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \to \mathcal{H}$ is injective we may assume by Lemma 2.3.6 without loss of generality that Λ is finitely generated, as any element in the kernel is also in $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda'$ for some finitely generated sublattice $\Lambda' \subseteq \Lambda$. Write $V = \mathbb{R}\Lambda \subseteq \mathcal{H}$. We may choose an $\mathbb{R}$-basis for V in Λ, and let Λ' be the group generated by this basis. Then $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda' \to V$ is an isomorphism. As Λ is discrete in V, also Λ/Λ' is discrete in V/Λ'. Now V/Λ' is compact, so the quotient Λ/Λ' is finite. Then $\Lambda \subseteq \frac{1}{n}\Lambda'$, where $n = \#(\Lambda/\Lambda')$. Now the natural map $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \to \mathcal{H}$ is injective because it is the composition of the map $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \to \mathbb{R} \otimes_{\mathbb{Z}} (\frac{1}{n}\Lambda') = \mathbb{R} \otimes_{\mathbb{Z}} \Lambda'$, which is injective since $\mathbb{R}$ is flat over $\mathbb{Z}$, and the map $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda' \to V$, which is injective by construction. □

Proposition 2.3.10. *Let Λ be a Hilbert lattice in a Hilbert space $\mathcal{H}$ and suppose Λ is finitely generated as $\mathbb{Z}$-module. Then Λ has a $\mathbb{Z}$-basis and any $\mathbb{Z}$-basis is $\mathbb{R}$-linearly independent.*

Proof. Since Λ is finitely generated and torsion free, it is clear that Λ is free. By Lemma 2.3.9, any $\mathbb{Z}$-linearly independent subset of Λ is $\mathbb{R}$-linearly independent. □

Proposition 2.3.11. *Suppose Λ is a Hilbert lattice in a Hilbert space $\mathcal{H}$ and let $\Lambda' \subseteq \Lambda$ be a finitely generated subgroup. Let $\pi\colon \mathcal{H} \to \mathcal{H}$ be the orthogonal projection onto the orthogonal complement of Λ'. Then for each $0 \leq t < \frac{1}{4}\mathrm{P}(\Lambda)$ there are only finitely many $z \in \pi\Lambda$ such that $q(z) \leq t$, and $\pi\Lambda$ is a Hilbert lattice.*

Proof. Suppose that $\pi\Lambda$ contains infinitely many points z with $q(z) \leq t$, or equivalently there exists some infinite set $S \subseteq \Lambda$ such that $\pi|_S$ is injective and $q(\pi(x)) \leq t$ for all $x \in S$. Consider the map $\tau\colon \mathcal{H} \to \mathbb{R}\Lambda'$, the complementary projection to π. As $(\mathbb{R}\Lambda')/\Lambda'$ is compact, there must exist distinct $x, y \in S$ such that $q(\tau(x) - \tau(y) + w) < \mathrm{P}(\Lambda) - 4t$ for some $w \in \Lambda'$. Then

$$\begin{aligned} 0 < q(x - y + w) &= q(\pi(x - y)) + q(\tau(x - y) + w) \\ &< 2\big(q(\pi(x)) + q(\pi(y))\big) + \mathrm{P}(\Lambda) - 4t \leq \mathrm{P}(\Lambda), \end{aligned}$$

a contradiction. Hence there are only finitely many $z \in \pi\Lambda$ such that $q(z) \leq t$. To verify that $\pi\Lambda$ is a Hilbert lattice it suffices to show that it is discrete in $\mathcal{H}$, which follows from the previous by taking any non-zero value for t. □

Lemma 2.3.12. *Let Λ be a Hilbert lattice which is finitely generated as $\mathbb{Z}$-module and let $S \subseteq \Lambda$ be a set of vectors that forms a basis for $\Lambda \cap (\mathbb{R}S)$. Then there exists a basis $B \supseteq S$ of Λ.*

Proof. Let π be the projection onto the orthogonal complement of S. Then $\pi\Lambda$ is a Hilbert lattice by Proposition 2.3.11 with a basis B_π by Proposition 2.3.10. Now choose for every $b_\pi \in B_\pi$ a lift $b \in \Lambda$ and let T be the set of those elements. It is easy to show that $B = S \cup T$ is a basis of Λ. □

Theorem 2.3.13. *Every countable subgroup of a Hilbert lattice is free.*

We call an abelian group for which all its countable subgroups are free an *almost free* abelian group.

Proof. Let Λ be a Hilbert lattice. By Lemma 2.3.6 suffices to show that if Λ is countable then Λ is free. We may write $\Lambda = \{x_1, x_2, \dots\}$ and let $V_i = \sum_{j=1}^{i} \mathbb{R}x_j$ and $\Lambda_i = V_i \cap \Lambda$. We claim that there exist bases B_i for Λ_i such that $B_i \subseteq B_j$ for all $i \leq j$. Indeed, take $B_0 = \varnothing$ and inductively for Λ_{i+1} note that B_i is a basis for $\Lambda_i = \Lambda_{i+1} \cap V_i$, so that by Lemma 2.3.12 there exists some basis B_{i+1} for Λ_{i+1} containing B_i. Then $B = \bigcup_{i=0}^{\infty} B_i$ is a basis for Λ, so Λ is free. □

Question 2.3.14. We have by Example 2.3.4 and Theorem 2.3.13 two inclusions

$$\begin{aligned}\{\text{free abelian groups}\} &\subseteq \{\text{underlying groups of Hilbert lattices}\}\\ &\subseteq \{\text{almost free abelian groups}\}.\end{aligned}$$

Is one of these inclusions an equality, and if so, which?

Example 2.3.15. There are abelian groups which are almost free but not free. Let X be a countably infinite set and consider the Baer–Specker group $B = \mathbb{Z}^X$. Then by Theorem 21 in [27], we have that B is not free. Since B is a torsion-free $\mathbb{Z}$-module, so is any countable subgroup, which is then free by Theorem 16 in [27], i.e. B is almost free.

Definition 2.3.16. For a Hilbert lattice Λ we define its *rank* as $\operatorname{rk}\Lambda = \dim_{\mathbb{Q}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})$. We will say a Hilbert lattice Λ is of *full rank* in an ambient Hilbert space $\mathcal{H}$ if $\mathbb{Q}\Lambda$ is dense in $\mathcal{H}$.

For free Hilbert lattices Λ we have $\Lambda \cong \mathbb{Z}^{(\operatorname{rk}\Lambda)}$ as abelian group. By Theorem 2.3.7 every Hilbert lattice has a uniquely unique Hilbert space in which it is contained and of full rank.

Lemma 2.3.17. *Let $\mathcal{H}$ be a Hilbert space and let $S, T \subseteq \mathcal{H}$ be subsets such that S is infinite, the $\mathbb{Q}$-vector space generated by S is dense in $\mathcal{H}$ and $\inf\{\|x - y\| \mid x, y \in T,\ x \neq y\} > 0$. Then $\#S \geq \#T$.*

Proof. Because S is infinite, the set S and the $\mathbb{Q}$-vector space V generated by S have the same cardinality. Let $\rho = \inf\{\|x-y\| \,|\, x, y \in T,\, x \neq y\}$. Since V is dense in $\mathcal{H}$ we may for each $x \in T$ choose $f(x) \in V$ such that $\|x - f(x)\| < \rho/2$. If $f(x) = f(y)$, then $\|x-y\| = \|(x-f(x))-(y-f(y))\| \leq \|x - f(x)\| + \|y - f(y)\| < \rho$, so $x = y$. Hence f is injective and we have $\#S = \#V \geq \#T$. □

The following proposition is generalized from proofs by O. Berrevoets and B. Kadets.

Proposition 2.3.18. *If Λ is a Hilbert lattice in a Hilbert space $\mathcal{H}$, then* $\operatorname{rk}\Lambda \leq \operatorname{orth}\dim\mathcal{H}$ *with equality if Λ is of full rank in $\mathcal{H}$.*

Proof. First suppose $\operatorname{rk}\Lambda$ is finite. It follows from Lemma 2.3.9 that $\operatorname{rk}\Lambda = \dim_{\mathbb{R}}(\mathbb{R}\otimes_{\mathbb{Z}}\Lambda) = \dim_{\mathbb{R}}(\mathbb{R}\Lambda) \leq \dim_{\mathbb{R}}\mathcal{H}$. If Λ is of full rank, then $\mathbb{R}\Lambda$ is dense in $\mathcal{H}$, but $\mathbb{R}\Lambda$ is complete as it is finite-dimensional, so $\mathbb{R}\Lambda = \mathcal{H}$ and $\operatorname{rk}\Lambda = \dim_{\mathbb{R}}\mathcal{H}$. Lastly, it follows from Theorem 2.2.16 that $\dim_{\mathbb{R}}\mathcal{H} = \operatorname{orth}\dim\mathcal{H}$ when $\dim_{\mathbb{R}}\mathcal{H}$ is finite.

Now suppose $\operatorname{rk}\Lambda$ is infinite and thus $\#\Lambda = \operatorname{rk}\Lambda$. By Theorem 2.2.16 we may assume without loss of generality that $\mathcal{H} = \ell^2(B)$ for some set B of cardinality $\operatorname{orth}\dim\mathcal{H}$, which must be infinite. Observe that the $\mathbb{Q}$-vector space generated by B is dense in $\mathcal{H}$. We may apply Lemma 2.3.17 by discreteness of Λ to obtain $\operatorname{orth}\dim\mathcal{H} = \#B \geq \#\Lambda = \operatorname{rk}\Lambda$, as was to be shown. If $\mathbb{Q}\Lambda$ is dense in $\mathcal{H}$, then we may apply Lemma 2.3.17 since $\|b-c\|^2 = \|b\|^2 + \|c\|^2 = 2$ for all distinct $b, c \in B$ to conclude that $\operatorname{rk}\Lambda = \#\Lambda \geq \#B = \operatorname{orth}\dim\mathcal{H}$, and thus we have equality. □

2.4 Decompositions

Definition 2.4.1. Let Λ be a Hilbert lattice. A *decomposition* of an element $z \in \Lambda$ is a pair $(x, y) \in \Lambda^2$ such that $z = x + y$ and $\langle x, y\rangle \geq 0$. A decomposition (x, y) of $z \in \Lambda$ is *trivial* if $x = 0$ or $y = 0$. We say $z \in \Lambda$ is *indecomposable* if it has exactly two decompositions, i.e. $z \neq 0$ and the only decompositions of z are trivial. Write $\operatorname{dec}(z)$ for the set of decompositions of $z \in \Lambda$ and $\operatorname{indec}(\Lambda)$ for the set of indecomposable elements of Λ.

Indecomposable elements are in the computer science literature often called Voronoi-relevant vectors, for example in [23]. This name is clearly inspired by Theorem 2.6.11.

Example 2.4.2. Let $f\colon I \to \mathbb{R}_{\geq 0}$ be such that Λ^f as in Example 2.3.5 is a Hilbert lattice. We will compute the indecomposables of Λ^f. Let $x = (x_i)_i \in \operatorname{indec}(\Lambda^f)$ and write e_i for the i-th standard basis vector. Note that

x must be *primitive*, i.e. not be of the form ny for any $y \in \Lambda^f$ and $n \in \mathbb{Z}_{>1}$, because otherwise $\langle y, (n-1)y\rangle = (n-1)\langle y, y\rangle > 0$ shows $(y, (n-1)y)$ is a non-trivial decomposition. If x_i and x_j are non-zero for distinct $i, j \in I$, then $q(x - e_i x_i) + q(e_i x_i) = q(x)$ and we have a non-trivial decomposition of x. Hence $x = \pm e_i$ for some $i \in I$. Note that e_i is indeed indecomposable for all $i \in I$: Any decomposition $(x, y) \in \operatorname{dec}(e_i)$ must have $|x_i| + |y_i| = 1$ and $x_j = y_j = 0$ for $i \neq j$, so $x = 0$ or $y = 0$. As $z \mapsto -z$ is an isometry of Λ^f, we have that $-e_i$ is indecomposable as well. Hence $\operatorname{indec}(\Lambda^f) = \{\pm e_i \mid i \in I\}$.

Lemma 2.4.3. *Let Λ be a Hilbert lattice and let $x, y, z \in \Lambda$. Then the following are equivalent:*

(i) *The pair (x, y) is a decomposition of z.*
(ii) *We have $x + y = z$ and $q(x) + q(y) \leq q(z)$.*
(iii) *We have $x + y = z$ and $q(x - z/2) \leq q(z/2)$.*
(iv) *We have $x + y = z$ and $q(z - 2y) \leq q(z)$.*

For a visual aid to this lemma see Figure 2.1.

Proof. (i $\Leftrightarrow$ ii) By bilinearity we have

$$q(z) = \langle x + y, x + y\rangle = q(x) + q(y) + 2\langle x, y\rangle.$$

(ii $\Leftrightarrow$ iii) By the parallelogram law we have

$$q(x) + q(y) = 2q\Big(\frac{x+y}{2}\Big) + 2q\Big(\frac{x-y}{2}\Big) = 2q\Big(\frac{z}{2}\Big) + 2q\Big(x - \frac{z}{2}\Big),$$

so $q(x) + q(y) - q(z) = 2 \cdot [q(x - z/2) - q(z/2)]$. The claim then follows trivially.

(iii $\Leftrightarrow$ iv) Note that $z - 2y = x - y = 2(x/2 - y/2) = 2(x - z/2)$. By the parallelogram law we have $q(2w) = 4q(w)$ for all $w \in \mathbb{Q}\Lambda$, from which this equivalence trivially follows. □

By Lemma 2.4.3, finding decompositions of $z \in \Lambda$ amounts to finding $x \in \Lambda$ sufficiently close to $z/2$.

Lemma 2.4.4. *Let $z \in \Lambda$ such that $0 < q(z) \leq 2\mathrm{P}(\Lambda)$. Suppose that the latter inequality is strict or $\mathrm{P}(\Lambda)$ is not attained by any vector in Λ. Then $z \in \operatorname{indec}(\Lambda)$.*

Proof. If $(x, y) \in \operatorname{dec}(z)$ is non-trivial, then by Lemma 2.4.3 we have $2\mathrm{P}(\Lambda) \geq q(z) \geq q(x) + q(y) \geq \mathrm{P}(\Lambda) + \mathrm{P}(\Lambda)$ with either the first or last inequality strict, which is a contradiction. Since $z \neq 0$ it follows that z is indecomposable. □

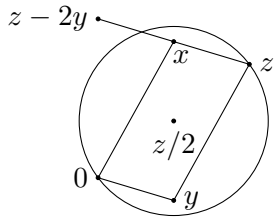


Figure 2.1: A decomposition $z = x + y$

Proposition 2.4.5. *If Λ is a non-zero Hilbert lattice, then every $z \in \Lambda$ can be written as a sum of at most $q(z)/\mathrm{P}(\Lambda)$ indecomposables $z_1, \ldots, z_n \in \Lambda$ such that $\sum_i q(z_i) \leq q(z)$.*

Proof. By scaling q we may assume without loss of generality that $\mathrm{P}(\Lambda) = 1$. We apply induction to $\lfloor q(z) \rfloor$. When this equals 0 we have $q(z) < \mathrm{P}(\Lambda)$, so $z = 0$, which we can write as a sum of zero indecomposables. Now suppose $\lfloor q(z) \rfloor \geq 1$ and thus $z \neq 0$. If z is indecomposable then indeed it is the sum of $1 \leq \lfloor q(z) \rfloor$ indecomposable, so suppose there is a non-trivial $(x, y) \in \mathrm{dec}(z)$. Then $q(x) + q(y) \leq q(z)$ by Lemma 2.4.3 and since $y \neq 0$ also $q(y) \geq \mathrm{P}(\Lambda) = 1$. Hence $\lfloor q(x) \rfloor \leq \lfloor q(z) - q(y) \rfloor < \lfloor q(z) \rfloor$, so by the induction hypothesis we may write $x = \sum_i x_i$ with $x_1, \ldots, x_a \in \mathrm{indec}(\Lambda)$ and $a \leq q(x)$ such that $\sum_i q(x_i) \leq q(x)$. By symmetry we may similarly write y as a sum of at most $q(y)$ indecomposables $y_1, \ldots, y_b$. Hence we can write $z = \sum_i x_i + \sum_i y_i$ as a sum of $a + b \leq q(x) + q(y) \leq q(z)$ indecomposables such that $\sum_i q(x_i) + \sum_i q(y_i) \leq q(x) + q(y) \leq q(z)$. The proposition follows by induction. □

Lemma 2.4.6. *Suppose Λ is a Hilbert lattice and $z \in \Lambda$ is the sum of some non-zero $z_1, \ldots, z_n \in \Lambda$ and $n \in \mathbb{Z}_{\geq 2}$. If $\sum_i q(z_i) \leq q(z)$, then z has a non-trivial decomposition.*

Proof. We have

$$\sum_{i=1}^{n} \langle z_i, z - z_i \rangle = \sum_{i=1}^{n} \langle z_i, z \rangle - \sum_{i=1}^{n} \langle z_i, z_i \rangle = q(z) - \sum_{i=1}^{n} q(z_i) \geq 0,$$

so $\langle z_i, z - z_i \rangle \geq 0$ for some i. As neither z_i nor $z - z_i$ are 0, we conclude that $(z_i, z - z_i)$ is a non-trivial decomposition of z. □

Proposition 2.4.7. *Let Λ be a Hilbert lattice. The group $\{\pm 1\}$ acts on* $\mathrm{indec}(\Lambda)$ *by multiplication, and the natural map* $\mathrm{indec}(\Lambda)/\{\pm 1\} \to \Lambda/2\Lambda$ *is injective.*

Proof. Note that $\{\pm 1\}$ acts on Λ and thus also on $\operatorname{indec}(\Lambda)$. By (i $\Leftrightarrow$ iv) of Lemma 2.4.3 we have

$$\operatorname{dec}(z) = \left\{ \left(\frac{z-a}{2}, \frac{z+a}{2} \right) \,\middle|\, a \in z + 2\Lambda,\ q(a) \leq q(z) \right\}.$$

Let $z \in \operatorname{indec}(\Lambda)$. Then $\{(0,z),(z,0)\} = \operatorname{dec}(z)$, so the only $a \in z+2\Lambda$ such that $q(a) \leq q(z)$ are $a = z$ and $a = -z$. Thus z is a q-minimal element of its coset in $\Lambda/2\Lambda$ and this minimal element is unique up to sign. Consequently, the map $\operatorname{indec}(\Lambda)/\{\pm 1\} \to \Lambda/2\Lambda$ is injective. □

Corollary 2.4.8. *Let Λ be a Hilbert lattice. Then* $\operatorname{indec}(\Lambda)$ *is finite if and only if* $\operatorname{rk}\Lambda < \infty$.

Proof. Recall that $\operatorname{indec}(\Lambda)$ generates Λ by Proposition 2.4.5. Hence if $\operatorname{indec}(\Lambda)$ is finite, then $\operatorname{rk}\Lambda < \infty$. If $\operatorname{rk}\Lambda < \infty$, then Proposition 2.4.7 implies $\#\operatorname{indec}(\Lambda) \leq 2 \cdot \#(\Lambda/2\Lambda) = 2^{1+\operatorname{rk}\Lambda} < \infty$. □

The zero coset of $\Lambda/2\Lambda$ is never in the image of the map of Proposition 2.4.7, as any non-zero element of the form $2x$ with $x \in \Lambda$ has a non-trivial decomposition (x,x). A non-zero coset C of $\Lambda/2\Lambda$ can fail to be in the image for two reasons: Either C has no minimal element or a minimal element exists but is not unique up to sign. In the latter case, with $z \in C$ minimal, there exists a $(x,y) \in \operatorname{dec}(z)$ with $x, y \neq 0$ and $q(x) + q(y) = q(z)$ and thus $\langle x, y\rangle = 0$, i.e. z has an orthogonal decomposition. This is exhibited, for example, by the lattice $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ with the standard inner product and $z = (1,1)$, where $(-1,1) \in z + 2\mathbb{Z}^2$ gives rise to the orthogonal decomposition $(1,0) + (0,1) = z$. In the former case, $\operatorname{rk}\Lambda$ has to be infinite: If $\operatorname{rk}\Lambda$ is finite, then for any $x \in \Lambda$ there are only finitely many $y \in \Lambda$ with $q(y) \leq q(x)$, so q assumes a minimum on any non-empty subset of Λ, in particular C. An example is the following.

Example 2.4.9. We will exhibit a Hilbert lattice Λ and a coset of 2Λ on which q does not attain a minimum. Let $f\colon I \to \mathbb{R}_{\geq 0}$ be such that Λ^f as in Example 2.3.5 is a Hilbert lattice. We define the Λ_2^f to be the sublattice

$$\Lambda_2^f = \ker(\Lambda^f \xrightarrow{\Sigma} (\mathbb{Z}/2\mathbb{Z})) = \left\{ (x_i)_i \in \mathbb{Z}^{(I)} \,\middle|\, \sum_{i\in I} x_i \equiv 0 \bmod 2 \right\}.$$

Consider $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ strictly decreasing, write $f(\infty)$ for its limit, assume $f(\infty) > 0$, and let $\Lambda = \Lambda_2^f$. Let $z = 2e_k \in \Lambda$ for any $k \in \mathbb{Z}_{\geq 0}$. Then for all $y = (y_i)_i \in \Lambda$ we have

$$q(z-2y) = 4\Big((1-y_k)^2 f(k)^2 + \sum_{i\neq k} y_i^2 f(i)^2 \Big) > 4f(\infty)^2,$$

since either $y_i^2 \geq 1$ for some $i \neq k$ or y_k is even. However, we also have for $y = e_k + e_i$ that $q(z - 2y) = q(2e_i) = 4f(i)^2 \to 4f(\infty)^2$ as $i \to \infty$. Hence $\{q(z - 2y) \,|\, y \in \Lambda\}$ does not contain a minimum.

If we eliminate the zero coset in the proof of Corollary 2.4.8 the upper bound on the number of indecomposables becomes $2(2^{\mathrm{rk}(\Lambda)} - 1)$ and this bound is tight. If one took the effort to define a sensible probability measure on the space of all Hilbert lattices of given finite rank, then this upper bound will in fact be an equality with probability 1.

2.5 Orthogonal decompositions

The main motivation for considering indecomposable elements is found in the study of decompositions of lattices. In this section we generalize a result of Eichler [11] on the existence of a universal decomposition in lattices to Hilbert lattices.

Recall the definition of a graph and of a decomposition of a module from the Preliminaries. We say a decomposition $\mathcal{M}$ of a module M is *universal* if it is an initial object in this category, i.e. for all decompositions $\mathcal{N}$ of M there exists a unique morphism $\mathcal{M} \to \mathcal{N}$.

Definition 2.5.1. Let Λ be a Hilbert lattice. For a set I, an *I-indexed orthogonal decomposition* of Λ is an I-indexed decomposition $\{\Lambda_i\}_{i \in I}$ of Λ as $\mathbb{Z}$-module such that $\langle \Lambda_i, \Lambda_j \rangle = 0$ for all $i \neq j$, which we write as $\bigoplus_{i \in I} \Lambda_i = \Lambda$. An *orthogonal decomposition* of Λ is an I-indexed orthogonal decomposition for any set I. We say Λ is *orthogonally indecomposable* if $\Lambda \neq 0$ and for all $\Lambda_1, \Lambda_2 \subseteq \Lambda$ such that $\Lambda_1 \oplus \Lambda_2 = \Lambda$ we have $\Lambda_1 = 0$ or $\Lambda_2 = 0$. We interpret the class of orthogonal decompositions of Λ as a full subcategory of the category of decompositions of Λ.

Lemma 2.5.2. *Let $G = (V, E)$ be a graph. Then the connected components of G are pairwise disjoint, and if for $S \subseteq V$ there exist no $\{u, v\} \in E$ such that $u \in S$ and $v \notin S$, then S is a union of connected components.*

Proof. Let $\mathcal{C}$ be the set of $S \subseteq V$ such that there are no $\{u, v\} \in E$ such that $u \in S$ and $v \notin S$, so that the connected components of G become the minimal non-empty elements of $\mathcal{C}$ with respect to inclusion. Note that $\mathcal{C}$ is closed under taking complements, arbitrary unions and arbitrary intersections, i.e. $\mathcal{C}$ is a clopen topology on V. Suppose $S, T \in \mathcal{C}$ are connected components that intersection non-trivially, then $S \cap T \in \mathcal{C}$ is non-empty, so by minimality $S = T$. Hence the connected components are pairwise disjoint.

Now let $S \in \mathcal{C}$ and for all $s \in S$ let $A_s = \{T \in \mathcal{C} \mid s \in T\}$ and $C_s = \bigcap_{T \in A_s} T$, which is an element of A_s. For all $T \in \mathcal{C}$ we either have $T \in A_s$ or $V \setminus T \in A_s$, and thus either $C_s \subseteq T$ or $C_s \cap T = \varnothing$. It follows that no non-empty $T \in \mathcal{C}$ is strictly contained in C_s, i.e. C_s is a connected component of G. As $S \in A_s$ we have $s \in C_s \subseteq S$ and thus $S = \bigcup_{s \in S} C_s$ is a union of connected components. □

The following is a generalization of a theorem due to Eichler [11], although the proof more closely resembles that of Theorem 6.4 in [39].

Theorem 2.5.3. *Let Λ be a Hilbert lattice and $V \subseteq \operatorname{indec}(\Lambda)$ such that V generates Λ as a group. Let G be the graph with vertex set V and with an edge between x and y if and only if $\langle x, y\rangle \neq 0$. Let U be the set of connected components of G and for $u \in U$ let $\mathrm{Y}_u \subseteq \Lambda$ be the subgroup generated by the elements in u. Then $\{\mathrm{Y}_u\}_{u \in U}$ is a universal orthogonal decomposition of Λ.*

As corollary to this theorem we have that Λ is orthogonally indecomposable if and only if G is connected.

Proof. We have $V \subseteq \bigcup_{u \in U} \mathrm{Y}_u$ by Lemma 2.5.2, so $\sum_{u \in U} \mathrm{Y}_u = \Lambda$ by assumption on V. For $u, v \in U$ distinct we have $\langle u, v\rangle = \{0\}$ by definition of G, so $\langle \mathrm{Y}_u, \mathrm{Y}_v\rangle = \{0\}$. We conclude that $\Lambda = \bigoplus_{u \in U} \mathrm{Y}_u$ is an orthogonal decomposition.

To show it is universal, let $\{\Lambda_i\}_{i \in I}$ be a family of sublattices of Λ such that $\bigoplus_{i \in I} \Lambda_i = \Lambda$. Let $x \in \operatorname{indec}(\Lambda)$ and write $x = \sum_{i \in I} \lambda_i$ with $\lambda_i \in \Lambda_i$ for all $i \in I$. If $j \in I$ is such that $\lambda_j \neq 0$, then $\langle \lambda_j, \sum_{i \neq j} \lambda_i\rangle = 0$ and thus $\lambda_j = x$, because otherwise we obtain a non-trivial decomposition of x. Therefore every indecomposable of Λ is in precisely one of the Λ_i. We conclude that the $S_i = \Lambda_i \cap V$ for $i \in I$ are pairwise disjoint and have V as their union. Then by Lemma 2.5.2 every connected component $u \in U$ is contained in precisely one of the S_i, say in $S_{f(u)}$. By definition of the map $f \colon U \to I$ and the Y_u we have $\bigoplus_{u \in f^{-1}\{i\}} \mathrm{Y}_u \subseteq \Lambda_i$ for all i, and since both the Y_u and the Λ_i sum to Λ we must have equality for all i. It follows trivially from the construction that f is the unique map $\{\mathrm{Y}_u\}_{u \in U} \to \{\Lambda_i\}_{i \in I}$, and we conclude that $\{\mathrm{Y}_u\}_{u \in U}$ is a universal orthogonal decomposition of Λ. □

We will use this theorem in Section 4.3 to generalize some theorems from [34].

Theorem 2.5.4. *Every Hilbert lattice has a universal orthogonal decomposition.*

Proof. Take $V = \mathrm{indec}(\Lambda)$ in Theorem 2.5.3 and note that it satisfies the conditions to this theorem by Proposition 2.4.5. □

2.6 Voronoi cells

We will generalize the Voronoi cell as defined for classical lattices to Hilbert lattices and extend some known definitions and properties. Some of these definitions relate to the ambient Hilbert space of the Hilbert lattice, which exists and is uniquely unique by Theorem 2.3.7 when we require the $\mathbb{Q}$-vector space generated by the lattice to lie dense in the Hilbert space. In this section we will write $\mathcal{H}_\Lambda$ for this ambient Hilbert space of a Hilbert lattice Λ.

Definition 2.6.1. Let Λ be a Hilbert lattice. The *packing radius* of Λ is

$$\rho(\Lambda) = \inf\{\tfrac{1}{2}\|x - y\| \mid x, y \in \Lambda,\, x \neq y\} = \tfrac{1}{2}\sqrt{\mathrm{P}(\Lambda)},$$

the *covering radius* of Λ is

$$r(\Lambda) = \inf\{b \in \mathbb{R}_{>0} \mid (\forall z \in \mathcal{H}_\Lambda)\,(\exists\, x \in \Lambda)\, \|z - x\| \leq b\}$$

and the *Voronoi cell* of Λ in $\mathcal{H}$ is the set

$$\mathrm{Vor}(\Lambda) = \{z \in \mathcal{H}_\Lambda \mid (\forall x \in \Lambda \setminus \{0\})\ \|z\| < \|z - x\|\}.$$

We call $\rho(\Lambda)$ the packing radius because it is the radius of the largest open sphere $B \subseteq \mathcal{H}_\Lambda$ such that the spheres $x + B$ for $x \in \Lambda$ are pairwise disjoint. Similarly $r(\Lambda)$ is the radius of the smallest closed sphere $B \subseteq \mathcal{H}_\Lambda$ for which $\bigcup_{x\in\Lambda}(x + B) = \mathcal{H}_\Lambda$. Note that $r(\Lambda) = 0$ only for $\Lambda = 0$ by discreteness.

Example 2.6.2. The covering radius of a Hilbert lattice need not be finite. Take Λ^f as in Example 2.3.5 but with $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ diverging to infinity. The lattice point closest to $\frac{1}{3}e_i$ is 0 for all $i \in \mathbb{Z}_{\geq 0}$, so it has distance $\frac{1}{3}f(i)$ to the lattice. Hence $r(\Lambda^f) \geq \sup\{\frac{1}{3}f(i) \mid i \in \mathbb{Z}_{\geq 0}\} = \infty$.

Example 2.6.3. The Voronoi cell does not need to be an open set. Consider the lattice $\Lambda = \Lambda_2^f$ as in Example 2.4.9 with $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{>0}$ strictly decreasing. Let $i \in \mathbb{Z}_{\geq 0}$ and $\mathrm{A} = (1 + f(\infty)^2 f(i)^{-2})/2$ and write e_i for the i-th standard basis vector. We claim that $\alpha e_i \in \mathrm{Vor}(\Lambda)$ for $\alpha \in \mathbb{R}$ precisely when $|\alpha| \leq \mathrm{A}$, which proves the Voronoi cell is not open.

Let $x = \sum_j x_j e_j \in \Lambda$ such that $x_i \neq 0$. Then $|x_i| = 1$ or $q(x)/|x_i| \geq |x_i| f(i)^2 > f(i)^2 + f(i+1)^2$. It follows that

$$\inf\left\{\frac{q(x)}{2|x_i|f(i)^2} \,\middle|\, x \in \Lambda,\, x_i \neq 0\right\} = \frac{f(i)^2 + f(\infty)^2}{2f(i)^2} = \mathrm{A}$$

and that the infimum is not attained. By definition $\alpha e_i \in \mathrm{Vor}(\Lambda)$ if and only if $g(x) := q(\alpha e_i - x) - q(\alpha e_i) > 0$ for all $x \in \Lambda \setminus \{0\}$. Note that $g(x) = q(x) - 2\alpha x_i f(i)^2$.

Suppose $|\alpha| \leq \mathrm{A}$ and let $x \in \Lambda \setminus \{0\}$. If $\alpha x_i \leq 0$, then $g(x) \geq q(x) > 0$, so suppose $\alpha x_i > 0$. Then

$$\frac{g(x)}{2|x_i|f(i)^2} = \frac{q(x)}{2|x_i|f(i)^2} - |\alpha| > \mathrm{A} - |\alpha| \geq 0,$$

so $g(x) > 0$. We conclude that $\alpha e_i \in \mathrm{Vor}(\Lambda)$. Conversely, if $|\alpha| > \mathrm{A}$, then

$$\inf\left\{\frac{g(x)}{2|x_i|f(i)^2} \,\middle|\, x \in \Lambda,\, x_i \neq 0\right\} = \mathrm{A} - |\alpha| < 0,$$

hence there exists some $x \in \Lambda$ such that $g(x) < 0$ and thus $\alpha e_i \notin \mathrm{Vor}(\Lambda)$.

Definition 2.6.4. Let $\mathcal{H}$ be a Hilbert space and let $S \subseteq \mathcal{H}$ be a subset. We say S is *symmetric* if for all $x \in S$ also $-x \in S$. We say S is *convex* if for all $x, y \in S$ and $t \in [0,1]$ also $(1-t)x + ty \in S$.

Lemma 2.6.5. *Let $\mathcal{H}$ be a Hilbert space. For $X \subseteq \mathcal{H}$ write $\overline{X}$ for the topological closure of X. Then*

1. *The intersection $\bigcap_i S_i$ of convex sets $(S_i)_{i\in I}$ in $\mathcal{H}$ is convex;*
2. *The topological closure $\overline{S}$ of a convex set S in $\mathcal{H}$ is convex;*
3. *For all S in $\mathcal{H}$ open convex, $x \in S$, $y \in \overline{S}$ and $t \in [0,1)$ we have $(1-t)x + ty \in S$;*
4. *For convex open sets $(S_i)_{i\in I}$ in $\mathcal{H}$ with non-empty intersection we have $\overline{\bigcap_i S_i} = \bigcap_i \overline{S_i}$.*

Proof. 1. Trivial.

2. Let $x, y \in \overline{S}$ and let $(x_n)_n$ and $(y_n)_n$ be sequences in S with limit x respectively y. For all $t \in [0,1]$ we have $(1-t)x_n + ty_n \in S$, and since addition and scalar multiplication are continuous also have $(1-t)x + ty = \lim_{n\to\infty}[(1-t)x_n + ty_n] \in \overline{S}$.

3. By translating S we may assume without loss of generality that $(1-t)x + ty = 0$. Since $x \in S$ and S is open there exists some $r_x > 0$ such that the open ball B_x of radius r_x around x is contained in S. For $r_y > 0$ sufficiently small (in fact $r_y = r_x \cdot (1-t)/t$ suffices, see Figure 2.2) it holds that for any z in the open ball B_y of radius r_y around y the line through 0 and z intersects B_x. Taking $z \in B_y \cap S$, which exists because y is in the closure of S, there exists some $w \in B_x \subseteq S$ such that 0 lies on the line segment between w and z. By convexity $0 \in S$ follows, as was to be shown.

4. Since $\bigcap_i \overline{S_i}$ is closed and contains $\bigcap_i S_i$, clearly $\overline{\bigcap_i S_i} \subseteq \bigcap_i \overline{S_i}$. By 1 the set $\bigcap_i S_i$ is convex and by assumption it contains some x. For $t \in [0,1)$

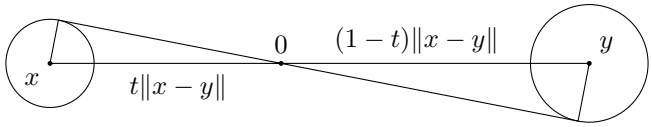


Figure 2.2: Computation of r_y from r_x via similar triangles.

and $y \in \bigcap_i \overline{S_i}$ we have $z_t = (1-t)x + ty \in S_i$ by 3. Thus $z_t \in \bigcap_i S_i$ for all $t \in [0,1)$, so $y = \lim_{t\to 1} z_t \in \overline{\bigcap_i S_i}$, proving the reverse inclusion. □

Lemma 2.6.6. *Let $\mathcal{H}$ be a Hilbert space. Then for $x, y \in \mathcal{H}$ we have $\|y\| \leq \|y - x\|$ if and only if $2\langle x, y\rangle \leq \langle x, x\rangle$, and similarly with $\leq$ replaced by $<$.*

Proof. We have $\|y - x\|^2 - \|y\|^2 = \langle x, x\rangle - 2\langle x, y\rangle$, from which the lemma trivially follows. □

Proposition 2.6.7. *For all Hilbert lattices Λ the set $\mathrm{Vor}(\Lambda)$ is symmetric, convex and has topological closure*

$$\overline{\mathrm{Vor}}(\Lambda) := \{z \in \mathcal{H}_\Lambda \mid (\forall x \in \Lambda)\ \|z\| \leq \|z - x\|\}.$$

Proof. It follows readily from the definition that $\mathrm{Vor}(\Lambda)$ is symmetric. Now for $x \in \Lambda$ consider $H_x = \{z \in \mathcal{H}_\Lambda \mid 2\langle x, z\rangle < \langle x, x\rangle\}$. It is easy to show for all $x \in \Lambda$ that H_x is convex: For $a, b \in H_x$ and $t \in [0,1]$ we have

$$2\langle (1-t)a + tb, x\rangle = (1-t)2\langle a, x\rangle + t2\langle b, x\rangle < (1-t)\langle x, x\rangle + t\langle x, x\rangle = \langle x, x\rangle,$$

so $(1-t)a + tb \in H_x$. As $\mathrm{Vor}(\Lambda)$ is the intersection of all H_x with $x \in \Lambda$ non-zero by Lemma 2.6.6, it follows from Lemma 2.6.5.1 that $\mathrm{Vor}(\Lambda)$ is convex. The H_x are all open, and for x non-zero we have $0 \in H_x$. Hence the topological closure of $\mathrm{Vor}(\Lambda)$ equals $\{z \in \mathcal{H}_\Lambda \mid (\forall x \in \Lambda \setminus \{0\})\ \|z\| \leq \|z - x\|\}$ by Lemma 2.6.5.4, from which the proposition follows. □

Example 2.6.8. We do not have in general that $\mathcal{H}_\Lambda = \Lambda + \overline{\mathrm{Vor}}(\Lambda)$ for all Hilbert lattices Λ, as in the finite-dimensional case. Note that $z \in \mathcal{H}_\Lambda$ is in $\Lambda + \overline{\mathrm{Vor}}(\Lambda)$ if and only if the infimum $\inf\{\|z - x\| \mid x \in \Lambda\}$ is attained for some $x \in \Lambda$. Consider Example 2.4.9, where we exhibit a lattice Λ and a coset $z + 2\Lambda$ of $\Lambda/2\Lambda$ where $\inf\{q(z + 2x) \mid x \in \Lambda\}$ is not attained. Equivalently, $\inf\{\|\frac{1}{2}z - x\| \mid x \in \Lambda\}$ is not attained, so $\frac{1}{2}z \notin \Lambda + \overline{\mathrm{Vor}}(\Lambda)$.

Theorem 2.6.9. *Let Λ be a Hilbert lattice and consider the natural map $\mathcal{H}_\Lambda \to \mathcal{H}_\Lambda/\Lambda$. Its restriction to $\mathrm{Vor}(\Lambda)$ is injective and for all $\varepsilon > 0$ its restriction to $(1+\varepsilon)\,\mathrm{Vor}(\Lambda)$ is surjective.*

Proof. Suppose $x, y \in \mathrm{Vor}(\Lambda)$ are distinct such that $x - y \in \Lambda$. Then

$$\|x\| < \|x - (x-y)\| = \|y\| < \|y - (y-x)\| = \|x\|,$$

which is a contradiction. Hence the map $\mathrm{Vor}(\Lambda) \to \mathcal{H}_\Lambda/\Lambda$ is injective.

Assume without loss of generality that $\mathrm{P}(\Lambda) = 2$. Let $\varepsilon > 0$ and $z \in \mathcal{H}_\Lambda$. Choose $y \in \Lambda$ such that $q(z-y) \leq \varepsilon + \inf\{q(z-w) \,|\, w \in \Lambda\}$. Suppose $x \in \Lambda \setminus \{0\}$. Then

$$\begin{aligned}(1+\varepsilon)\langle x, x\rangle - 2\langle x, z-y\rangle &= \varepsilon q(x) + (q(z-y-x) - q(z-y)) \\ &\geq \varepsilon q(x) - \varepsilon \geq \varepsilon(\mathrm{P}(\Lambda) - 1) = \varepsilon > 0.\end{aligned}$$

It follows that $2\langle x, (z-y)/(1+\varepsilon)\rangle < \langle x, x\rangle$ for all $x \in \Lambda \setminus \{0\}$, so $(z-y)/(1+\varepsilon) \in \mathrm{Vor}(\Lambda)$ by Lemma 2.6.6. Thus $z \in \Lambda + (1+\varepsilon)\,\mathrm{Vor}(\Lambda)$, and the map $(1+\varepsilon)\,\mathrm{Vor}(\Lambda) \to \mathcal{H}_\Lambda/\Lambda$ is surjective. □

Proposition 2.6.10. *For all Hilbert lattices Λ the set $\mathrm{Vor}(\Lambda)$ contains the open sphere of radius $\rho(\Lambda)$ around $0 \in \Lambda$ and $\overline{\mathrm{Vor}}(\Lambda)$ is contained in the closed sphere of radius $r(\Lambda)$ around 0.*

Proof. Let $z \in \mathcal{H}_\Lambda$ be such that $\|z\| < \rho(\Lambda)$ and let $x \in \Lambda \setminus \{0\}$. By Cauchy–Schwarz we have $\langle x, z\rangle \leq \|x\| \cdot \|z\| < \|x\| \cdot \frac{1}{2}\|x\| = \frac{1}{2}\langle x, x\rangle$, so $z \in \mathrm{Vor}(\Lambda)$ by Lemma 2.6.6.

Let $z \in \overline{\mathrm{Vor}}(\Lambda)$. For each $r > r(\Lambda)$ there exists $x \in \Lambda$ such that $\|z - x\| \leq r$ by definition of $r(\Lambda)$. Then by Proposition 2.6.7 we have $\|z\| \leq \|z - x\| \leq r$. Taking the limit of r down to $r(\Lambda)$ proves the second inclusion. □

Theorem 2.6.11. *Let Λ be a Hilbert lattice. Then there is a unique subset $S \subseteq \Lambda \setminus \{0\}$ that is minimal with respect to inclusion such that $\mathrm{Vor}(\Lambda) = \{z \in \mathcal{H}_\Lambda \,|\, (\forall\, x \in S)\ \|z\| < \|z - x\|\}$. This subset is equal to $\mathrm{indec}(\Lambda)$.*

Proof. For $S \subseteq \Lambda$ write $V(S) = \{z \in \mathcal{H}_\Lambda \,|\, (\forall\, x \in S)\ \|z\| < \|z - x\|\}$.

First suppose $V(S) = \mathrm{Vor}(\Lambda)$ for some $S \subseteq \Lambda \setminus \{0\}$. Let $z \in \mathrm{indec}(\Lambda)$ and note that $\frac{1}{2}z \notin \mathrm{Vor}(\Lambda)$ since $\|\frac{1}{2}z\| \geq \|\frac{1}{2}z - z\|$. As $V(S) = \mathrm{Vor}(\Lambda)$ there must be some $x \in S$ such that $\|\frac{1}{2}z\| \geq \|\frac{1}{2}z - x\|$. Hence $(x, z-x)$ is a decomposition of z by Lemma 2.4.3, so $z = x$ since z is indecomposable and $x \neq 0$. We conclude that $z \in S$ and $\mathrm{indec}(\Lambda) \subseteq S$.

It remains to show that $V(\mathrm{indec}(\Lambda)) = \mathrm{Vor}(\Lambda)$. We clearly have that $\mathrm{Vor}(\Lambda) \subseteq V(\mathrm{indec}(\Lambda))$. Suppose $z \in V(\mathrm{indec}(\Lambda))$ and let $x \in \Lambda \setminus \{0\}$. By Proposition 2.4.5 we may write $x = \sum_{i=1}^n x_i$ for some $n \in \mathbb{Z}_{\geq 1}$ and $x_i \in \mathrm{indec}(\Lambda)$ such that $\sum_{i=1}^n \langle x_i, x_i\rangle \leq \langle x, x\rangle$. Then by Lemma 2.6.6 we have

$$2\langle x, z\rangle = \sum_{i=1}^n 2\langle x_i, z\rangle < \sum_{i=1}^n \langle x_i, x_i\rangle \leq \langle x, x\rangle$$

and thus $z \in \mathrm{Vor}(\Lambda)$. We conclude that $\mathrm{Vor}(\Lambda) = V(\mathrm{indec}(\Lambda))$. □

Corollary 2.6.12. *Let Λ be a Hilbert lattice. Then*

$$\overline{\mathrm{Vor}}(\Lambda) = \{z \in \mathcal{H}_\Lambda \mid (\forall x \in \mathrm{indec}(\Lambda))\ \|z\| \leq \|z - x\|\}.$$

Proof. By Lemma 2.6.5.4 we have for $S \subseteq \Lambda$ not containing 0 that $\overline{V}(S) = \{z \in \mathcal{H}_\Lambda \mid (\forall x \in S)\ \|z\| \leq \|z - x\|\}$ is the topological closure of $V(S)$ as defined in the proof of Theorem 2.6.11. The corollary then follows from Proposition 2.6.7 and Theorem 2.6.11. □

Example 2.6.13. For a Hilbert lattice Λ the set $\mathrm{indec}(\Lambda)$ can fail to be the minimum among all sets $S \subseteq \Lambda$ such that $\overline{V}(S) = \{z \in \mathcal{H}_\Lambda \mid (\forall x \in S)\ \|z\| \leq \|z - x\|\}$ equals $\overline{\mathrm{Vor}}(\Lambda)$. We will give a counterexample.

Let $I = \mathbb{Z}_{\geq 0} \cup \{\infty\}$ and let $f\colon I \to \mathbb{R}_{\geq 0}$ such that $f|_{\mathbb{Z}_{\geq 0}}$ is strictly decreasing with limit $f(\infty) > 0$. Consider the lattice $\Lambda = \Lambda_2^f$ as in Example 2.4.9. Note that $\mathrm{P}(\Lambda) = 2f(\infty)^2$ and that $\mathrm{P}(\Lambda)$ is not attained by any vector. Hence $2e_\infty \in \Lambda$ is indecomposable by Lemma 2.4.4. Now let $S = \mathrm{indec}(\Lambda) \setminus \{\pm 2e_\infty\}$. We claim that $\overline{V}(S) = \overline{V}(\mathrm{indec}(\Lambda))$, the latter being equal to $\overline{\mathrm{Vor}}(\Lambda)$ by Corollary 2.6.12. It remains to show for all $z = (z_i)_i \in \overline{V}(S)$ that $\|z\| \leq \|z - 2e_\infty\|$ by symmetry.

For all i let $s_i \in \{\pm 1\}$ such that $s_i z_i = |z_i|$. Since f is strictly decreasing there exists some $N \in \mathbb{Z}_{\geq 0}$ such that $f(n) < \sqrt{3} f(\infty)$ for all integers $n \geq N$. For all integers $n \geq N$ we have $s_n e_n + e_\infty \in S$ by Lemma 2.4.4 as $q(s_n e_n + e_\infty) = f(n)^2 + f(\infty)^2 < 4f(\infty)^2 = 2\mathrm{P}(\Lambda)$. Then

$$0 \leq \|z - (s_n e_n + e_\infty)\|^2 - \|z\|^2 = (1 - 2|z_n|) f(n)^2 + (1 - 2z_\infty) f(\infty)^2.$$

As $z \in \mathcal{H}_\Lambda$ we must have $\lim_{n \to \infty} |z_n| = 0$, so taking the limit over the above inequality we get $0 \leq 2(1 - z_\infty) f(\infty)^2$ and thus $z_\infty \leq 1$. But then $\|z - 2e_\infty\|^2 - \|z\|^2 = 4f(\infty)^2(1 - z_\infty) \geq 0$ and we are done.

CHAPTER 3

Indecomposable algebraic integers

3.1 Introduction

This chapter is based on [18]. In number theory, in particular the theory of the geometry of numbers, one equips a number field K with an inner product, turning any order R in K into a lattice in $\mathbb{R}\otimes_{\mathbb{Q}}K$. After normalizing this inner product, we may define it on an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ as

$$\langle \alpha, \beta \rangle = \frac{1}{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]} \sum_{\sigma\colon \mathbb{Q}(\alpha,\beta)\to\mathbb{C}} \sigma(\alpha)\cdot\overline{\sigma(\beta)},$$

where the sum ranges over all ring homomorphisms from $\mathbb{Q}(\alpha,\beta)$ to $\mathbb{C}$. We write $\overline{\mathbb{Z}}$ for the ring of integers of $\overline{\mathbb{Q}}$, i.e. the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$, and we call its elements the algebraic integers. Although $\overline{\mathbb{Z}}$ is not of finite rank, we may still meaningfully call it a lattice in the sense of Chapter 2.

Theorem 3.2.10. *The abelian group $\overline{\mathbb{Z}}$ equipped with the inner product from Definition 3.2.5 is a Hilbert lattice. Its shortest non-zero vectors are precisely the roots of unity, which all have length 1, and its packing radius, see Definition 2.6.1, is $1/2$.*

We will treat this lattice structure on $\overline{\mathbb{Z}}$ as intrinsically interesting. The theory in this chapter is motivated by the closest vector problem for $\overline{\mathbb{Z}}$. Since $\overline{\mathbb{Z}}$ has infinite rank, it may be that a closest vector does not exist. Formally we ask the question: 'Does there exist an algorithm that, given $n \in \mathbb{Z}_{>0}$, some $r \in \mathbb{R}_{>0}\cap\overline{\mathbb{Q}}$ and $\alpha \in \overline{\mathbb{Q}}$, decides whether there exist n distinct elements $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha-\beta\| < r$ and if so computes n such β?' Since $\overline{\mathbb{Z}}$ is enumerable, once we know such β exist we can find them. However, it is certainly of interest to compute β efficiently. The following result derived from classical capacity theory by T. Chinburg, for which we give a direct proof in Section 3.6, answers the question affirmatively for $r > 1$.

Corollary 3.6.7. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r > 1$, then there exist infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha-\beta\| < r$.*

The proof is sufficiently constructive that we are able to derive an algorithm to compute arbitrarily many such β, see Proposition 3.6.10. This result also gives an upper bound on the covering radius.

Theorem 3.6.9. *The covering radius of $\overline{\mathbb{Z}}$, see Definition 2.6.1, is between $\sqrt[4]{1/2}$ and 1.*

Our main result is the following theorem, which is complementary to Corollary 3.6.7.

Theorem 3.11.2. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r < \sqrt[4]{\mathrm{e}/4}$, then there exist only finitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$.*

Again, one can algorithmically enumerate all such β, solving the problem for $r < \sqrt[4]{\mathrm{e}/4}$. This leaves a gap for r between $\sqrt[4]{\mathrm{e}/4}$ and 1 for which we do not know an answer to the decision problem.

Next we consider the related problem of computing the indecomposable vectors of $\overline{\mathbb{Z}}$, see Definition 2.4.1. A consequence of Corollary 3.6.7 is that for every $d \in \mathbb{Z}_{>0}$ there exist only finitely many indecomposable algebraic integers of degree up to d. We will prove the following effective upper and lower bounds.

Theorem 3.7.7. *There are least* $\exp(\frac{1}{4}(\log 2)d^2 + O(d \log d))$ *and at most* $\exp(\frac{1}{2}(1 + \log 2)d^2 + O(d \log d))$ *indecomposable algebraic integers of degree up to d.*

A decomposition of $\alpha \in \overline{\mathbb{Z}}$ corresponds to a lattice point with distance at most $\|\alpha/2\|$ to $\alpha/2$, and non-trivial decompositions exist if and only if there are at least 3 such lattice points. Hence deciding whether a lattice point is indecomposable is easier than the closest vector problem. It is also a good challenge problem for our algorithms. To this end, we derive the following numerical results.

Theorem 3.14.1. *There are exactly* 2 *indecomposable algebraic integers of degree* 1*, there are exactly* 14 *of degree* 2*, and there are at least* 354 *and at most* 588 *of degree* 3*.*

It would be interesting to study other lattice invariants of $\overline{\mathbb{Z}}$, but most constructions seem to fail to generalize to infinite rank, like the determinant and the dual lattice. One that does survive is the isometry group. For $\overline{\mathbb{Z}}$ it certainly contains $\mu(\overline{\mathbb{Z}}) \rtimes \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, see Lemma 3.2.13, but we do not know whether that is all.

3.2 The lattice of algebraic integers

We will write $\overline{\mathbb{Q}}$ for an algebraic closure of $\mathbb{Q}$. An *algebraic integer* is an element $\alpha \in \overline{\mathbb{Q}}$ for which there exists a monic $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. The algebraic integers form a subring of $\overline{\mathbb{Q}}$, which we denote $\overline{\mathbb{Z}}$. In this section we will prove that $\overline{\mathbb{Z}}$ together with a natural choice of square-norm is a Hilbert lattice.

Definition 3.2.1. For a ring K we define the *fundamental set* to be the set $\mathrm{X}(K)$ of ring homomorphisms from K to $\mathbb{C}$. For a ring L with subring K and $\sigma \in \mathrm{X}(K)$ we define $\mathrm{X}_\sigma(L) = \{\rho \in \mathrm{X}(L) \mid \rho|_K = \sigma\}$.

Lemma 3.2.2. *Let $\alpha \in \overline{\mathbb{Q}}$ and $\mathbb{Q}(\alpha) \subseteq L \subseteq \overline{\mathbb{Q}}$ subfields with $[L:\mathbb{Q}] < \infty$. Then the quantities*

$$\prod_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha)|^{1/[L:\mathbb{Q}]} \quad \text{and} \quad \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha)|^2$$

are in $\mathbb{R}_{\geq 0}$, equal to zero if and only if $\alpha = 0$, and do not depend on the choice of L. □

Definition 3.2.3. We define the maps $N, q \colon \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ by

$$N(\alpha) = \prod_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} \quad \text{and}$$
$$q(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^2.$$

Lemma 3.2.4. *For $\alpha, \beta \in \overline{\mathbb{Q}}$ we have $q(\alpha+\beta) + q(\alpha-\beta) = 2q(\alpha) + 2q(\beta)$.*

Proof. By Lemma 3.2.2 the restriction of q to $L = \mathbb{Q}(\alpha, \beta)$ is given by $q(\gamma) = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\gamma)|^2$. The norm $|\cdot|$ on $\mathbb{C}$ satisfies the parallelogram law and we may apply this term-wise to the sum defining q to obtain the lemma. □

Definition 3.2.5. For $\alpha, \beta \in \overline{\mathbb{Q}}$ we write $\langle \alpha, \beta \rangle$ for the inner product on $\overline{\mathbb{Q}}$ induced by q as given by Theorem 2.2.5 and Lemma 3.2.4. Explicitly, it is given by

$$\langle \alpha, \beta \rangle = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} \sigma(\alpha)\overline{\sigma(\beta)}$$

for any field $\mathbb{Q}(\alpha, \beta) \subseteq L \subseteq \overline{\mathbb{Q}}$ with $[L:\mathbb{Q}] < \infty$.

Lemma 3.2.6 (AM-GM inequality, Theorem 5.1 in [7])**.** *Let $n \in \mathbb{Z}_{\geq 1}$ and $x_1, \ldots, x_n \in \mathbb{R}_{\geq 0}$. Then*

$$\sqrt[n]{x_1 \cdots x_n} \leq \frac{x_1 + \cdots + x_n}{n},$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$. □

Definition 3.2.7. An element $\delta \in \overline{\mathbb{Q}}$ is called *uniform* if $|\sigma(\delta)| = |\tau(\delta)|$ for all $\sigma, \tau \in \mathrm{X}(\overline{\mathbb{Q}})$.

Lemma 3.2.8. *For all $\alpha \in \overline{\mathbb{Q}}$ we have $N(\alpha)^2 \leq q(\alpha)$ with equality if and only if α is uniform.*

Proof. This follows from a straightforward application of Lemma 3.2.6:

$$\begin{aligned} q(\alpha) &= \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^2 \\ &\geq \Big(\prod_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^2 \Big)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} = N(\alpha)^2, \end{aligned}$$

with equality if and only if $|\sigma(\alpha)|^2 = |\rho(\alpha)|^2$ for all $\sigma, \rho \in \mathrm{X}(\mathbb{Q}(\alpha))$. □

Proposition 3.2.9. *If $\alpha \in \overline{\mathbb{Z}}$, then $q(\alpha) \leq 1$ if and only if $\alpha = 0$ or α is a root of unity. If α is a root of unity, then $q(\alpha) = 1$.*

Proof. Let $\alpha \in \overline{\mathbb{Z}}$. The 'if' part of the implication follows directly from the definition. For the 'only if' part, suppose α is non-zero. If $q(\alpha) \leq 1$, then $N(\alpha)^2 \leq 1$ by Lemma 3.2.8. Then $N(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]} = |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| \in \mathbb{Z}_{\geq 1}$, so $N(\alpha)^2 = q(\alpha) = 1$. By Lemma 3.2.8 we have $|\sigma(\alpha)| = 1$ for all $\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))$, so α is a root of unity by Kronecker's theorem (Corollary 5.6 in [38]). □

Theorem 3.2.10. *The abelian group $\overline{\mathbb{Z}}$ equipped with the inner product from Definition 3.2.5 is a Hilbert lattice. Its shortest non-zero vectors are precisely the roots of unity, which all have length* 1*, and its packing radius, see Definition 2.6.1, is* $1/2$.

Proof. By Lemma 3.2.4 and Proposition 3.2.9 respectively the group $\overline{\mathbb{Z}}$ together with q satisfies the parallelogram law and is discrete, so indeed it is a Hilbert lattice. The remaining statements follow also from Proposition 3.2.9. □

We may write $\|x\|$ for $\sqrt{q(x)}$, the *2-norm* of $x \in \overline{\mathbb{Q}}$. Similarly, we may think of $N(x)$ as the *0-norm* of x, in the sense that $\lim_{p \to 0} \|x\|_p = N(x)$.

Lemma 3.2.11. *Suppose $\alpha, \delta \in \overline{\mathbb{Q}}$ and δ is uniform. Then $q(\alpha\delta) = q(\alpha)q(\delta)$. If also $\alpha, \delta \in \overline{\mathbb{Z}}$ and $\alpha\delta$ is indecomposable, then α is indecomposable.*

Proof. Let $L \supseteq \mathbb{Q}(\alpha, \delta)$. Then for all $\sigma \in \mathrm{X}(L)$ we have $q(\delta) = |\sigma(\delta)|^2$. Moreover,

$$q(\alpha\delta) = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha\delta)|^2 = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha)|^2 \cdot q(\delta) = q(\alpha)q(\delta).$$

Now suppose $\alpha, \delta \in \overline{\mathbb{Z}}$ and let $(\beta, \gamma) \in \mathrm{dec}(\alpha)$. Then $\alpha\delta = \beta\delta + \gamma\delta$ and

$$q(\alpha\delta) = q(\alpha)q(\delta) \geq (q(\beta) + q(\gamma))q(\delta) = q(\beta\delta) + q(\gamma\delta),$$

so $(\beta\delta, \gamma\delta) \in \operatorname{dec}(\alpha\delta)$. If $\alpha\delta$ is indecomposable, then $\delta \neq 0$ and $0 \in \{\beta\delta, \gamma\delta\}$, so $0 \in \{\beta, \gamma\}$ and (β, γ) must be a trivial decomposition. Hence α is indecomposable. □

Definition 3.2.12. Write μ_∞ for the group of roots of unity in $\overline{\mathbb{Z}}$ and $\mathrm{Gal}(\overline{\mathbb{Q}})$ for the group of ring automorphisms of $\overline{\mathbb{Q}}$. Note that $\mathrm{Gal}(\overline{\mathbb{Q}})$ naturally acts on μ_∞, and write $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ for their semi-direct product with respect to this action.

Lemma 3.2.13. *The group $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ acts faithfully on the Hilbert lattice $\overline{\mathbb{Z}}$, where μ_∞ acts by multiplication and $\mathrm{Gal}(\overline{\mathbb{Q}})$ by application.*

Proof. Let $\alpha \in \overline{\mathbb{Z}}$, $\zeta \in \mu_\infty$ and $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}})$. Let K be the normal closure of $\mathbb{Q}(\zeta, \alpha)$ and $n = [K : \mathbb{Q}]$.

First we show that the individual group actions on $\overline{\mathbb{Z}}$ are well-defined. Clearly $\zeta\alpha \in \overline{\mathbb{Z}}$ and note that ζ is uniform with $q(\zeta) = 1$. Hence multiplication by ζ is an isometry, i.e. preserves length, by Lemma 3.2.11. Recall that automorphisms preserve integrality and thus $\rho(\alpha) \in \overline{\mathbb{Z}}$. Since K is normal over $\mathbb{Q}$ we have $\rho K = K$ and thus $\mathrm{X}(K) \circ \rho = \mathrm{X}(K)$. Hence applying ρ to α simply results in a reordering of the terms in the sum defining q with respect to K, and thus ρ is an isometry.

Note that for $(\chi, \sigma), (\xi, \tau) \in \mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ we have

$$(\chi, \sigma)\big((\xi, \tau)\,\alpha\big) = \chi \cdot \sigma(\xi \cdot \tau(\alpha)) = (\chi\sigma(\xi))((\sigma\tau)(\alpha)) = \big((\chi, \sigma) \cdot (\xi, \tau)\big)\,\alpha,$$

so the semi-direct product acts on $\overline{\mathbb{Z}}$ as well. Finally, suppose (ζ, ρ) acts as the identity. Note that $\mathrm{Gal}(\overline{\mathbb{Q}})$ fixes 1, so letting (ζ, ρ) act on 1 shows that $\zeta = 1$, and thus $\rho = \mathrm{id}$. Hence the action is faithful. □

Question 3.2.14. Is $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ the entire isometry group of $\overline{\mathbb{Z}}$?

Proposition 3.2.15. *Let $\alpha \in \overline{\mathbb{Z}}$, $r \in \mathbb{Z}_{\geq 0}$ and $s \in \mathbb{Z}_{>0}$ such that $r/s \leq 1$. Then any root β of $X^s - \alpha^r$ satisfies $q(\beta) \leq q(\alpha)^{r/s}$.*

Proof. Let β be a root of $X^s - \alpha^r$, let $K = \mathbb{Q}(\alpha, \beta)$ and $n = [K : \mathbb{Q}]$. The case $r = 0$ follows from Proposition 3.2.9, so suppose $r > 0$. Then

$$\begin{aligned} q(\beta) &= \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\beta)|^2 = \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\beta^s)|^{2/s} = \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\alpha^r)|^{2/s} \\ &= \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} \big(|\sigma(\alpha)|^2\big)^{r/s} \leq \Big(\frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\alpha)|^2\Big)^{r/s} = q(\alpha)^{r/s}, \end{aligned}$$

where the inequality is $n^{-1/r}\|x\|_r \leq n^{-1/s}\|x\|_s$ from Lemma 2.2.14 applied to the vector $x = (|\sigma(\alpha)|^{2/s})_{\sigma \in \mathrm{X}(K)}$, using that $0 < r \leq s$. □

3.3 Indecomposable algebraic integers

We will now focus on the indecomposables of the lattice $\overline{\mathbb{Z}}$.

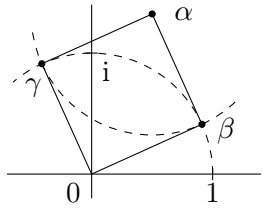


Figure 3.1: Integral $\alpha = \frac{1}{2}(1 + \mathrm{i}\sqrt{7})$ with $q(\alpha) = 2$.

Proposition 3.3.1. *Let $\alpha \in \overline{\mathbb{Z}}$. If $0 < q(\alpha) < 2$, then α is indecomposable. If $q(\alpha) = 2$, then α is decomposable if and only if it is the sum of two roots of unity. Such roots of unity are necessarily orthogonal, unique up to reordering, and of degree at most 2 over $\mathbb{Q}(\alpha)$.*

Proof. If $0 < q(\alpha) < 2$, then α is indecomposable by combining Theorem 3.2.10 and Lemma 2.4.4. Suppose $q(\alpha) = 2$. If $\alpha = \zeta + \xi$ for roots of unity $\zeta, \xi \in \overline{\mathbb{Q}}$, then $q(\alpha) = 2 = q(\zeta) + q(\xi)$, so $(\zeta, \xi) \in \mathrm{dec}(\alpha)$ is non-trivial. Conversely, suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ is non-trivial. By Theorem 3.2.10 we have $q(\beta), q(\gamma) \geq 1$. Then $0 \leq q(\alpha) - q(\beta) - q(\gamma) = 2 - q(\beta) - q(\gamma) \leq 0$, so we must have $q(\beta) = q(\gamma) = 1$. It follows that β and γ are orthogonal, and by Proposition 3.2.9 they are roots of unity.

Suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ is non-trivial. For any $\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))$ and $\rho \in \mathrm{X}_\sigma(\mathbb{Q}(\alpha, \beta))$ the points 0, $\rho(\alpha)$, $\rho(\beta)$ and $\rho(\gamma)$ form the vertices of a rhombus with unit length sides, as can be seen in Figure 3.1. It follows that $\{\rho(\beta), \rho(\gamma)\}$ is uniquely determined by $\rho(\alpha) = \sigma(\alpha)$. As ρ is uniquely determined by $\rho(\beta)$ there are at most two elements in $\mathrm{X}_\sigma(\mathbb{Q}(\alpha, \beta))$, in other words $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq 2$. □

Remark 3.3.2. Proposition 3.3.1 gives us a way to decide whether an $\alpha \in \overline{\mathbb{Z}}$ with $q(\alpha) = 2$ is indecomposable, as it puts an upper bound on the degree of the roots of unity, leaving only finitely many to check. Knowledge of $\mathbb{Q}(\alpha)$ can further reduce this number.

Example 3.3.3. There exist $\alpha \in \overline{\mathbb{Z}}$ with $q(\alpha) = 2$ which are indecomposable. Consider $f = X^2 - X + 2$ with root $\alpha \in \overline{\mathbb{Z}}$, as in Figure 3.1. Note that the roots of f in $\mathbb{C}$ are $\frac{1}{2}(1 \pm \mathrm{i}\sqrt{7})$ with absolute value $\frac{1}{2}\sqrt{1^2 + 7} = \sqrt{2}$, so $q(\alpha) = 2$. Suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ is a non-trivial decomposition. Proposition 3.3.1 shows that β and γ are roots of unity. Note that $|\alpha^2| = 2$ under

all embeddings of α in $\mathbb{C}$, and $\alpha^2 = |\alpha|^2 \cdot \beta\gamma$. Hence $\alpha^2/2 = \frac{1}{2}\alpha - 1$ is a root of unity. Either one notes that $\alpha^2/2$ is not even integral, or that $\alpha^2/2 = \pm 1$, as those are the only roots of unity in $\mathbb{Q}(\alpha)$, which is clearly absurd. Hence we have a contradiction and α is indecomposable.

Lemma 3.3.4. *Let $\mathbb{Q} \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}}$ be fields with $[L : \mathbb{Q}] < \infty$. Then for all $\alpha \in K$ and $\beta \in L$ we have*

$$[L : K] \cdot \langle \alpha, \beta \rangle = \langle \alpha, \mathrm{Tr}_{L/K}(\beta) \rangle.$$

Proof. Recall for $\sigma \in \mathrm{X}(K)$ the definition $\mathrm{X}_\sigma(L) = \{\rho \in \mathrm{X}(L) \mid \rho|_K = \sigma\}$ from Definition 3.2.1. For all $\sigma \in \mathrm{X}(K)$ and $\beta \in L$ we have $\sigma(\mathrm{Tr}_{L/K}(\beta)) = \sum_{\rho \in \mathrm{X}_\sigma(L)} \rho(\beta)$. Then with $\alpha \in K$ and $\beta \in L$ we have

$$\begin{aligned}
[L : K] \cdot \langle \alpha, \beta \rangle &= \frac{[L : K]}{[L : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} \sum_{\rho \in \mathrm{X}_\sigma(L)} \rho(\alpha)\overline{\rho(\beta)} \\
&= \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} \sigma(\alpha) \overline{\sum_{\rho \in \mathrm{X}_\sigma(L)} \rho(\beta)} \\
&= \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} \sigma(\alpha)\overline{\sigma(\mathrm{Tr}_{L/K}(\beta))} \\
&= \langle \alpha, \mathrm{Tr}_{L/K}(\beta) \rangle,
\end{aligned}$$

as was to be shown. □

One could phrase Lemma 3.3.4 in terms of adjoint linear maps. For number fields $K \subseteq L$, the linear map $t_{L/K} = [L : K]^{-1} \cdot \mathrm{Tr}_{L/K} : L \to K$, the *trace*, is adjoint to the inclusion $K \to L$ with respect to the induced inner products.

Proposition 3.3.5. *Roots of unity $\zeta, \xi \in \overline{\mathbb{Z}}$ are orthogonal, i.e. $\langle \zeta, \xi \rangle = 0$, if and only if $\zeta^{-1}\xi$ does not have square-free order.*

Proof. Let $K = \mathbb{Q}(\zeta^{-1}\xi)$. We have $[K : \mathbb{Q}] \cdot \langle \zeta, \xi \rangle = [K : \mathbb{Q}] \cdot \langle 1, \zeta^{-1}\xi \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\zeta^{-1}\xi)$ by Lemma 3.2.13 and Lemma 3.3.4. Recall that the trace of an n-th root of unity equals $\mu(n)$, the Möbius function, which is zero precisely when n has a square divisor in $\mathbb{Z}_{>1}$. □

For $\alpha, \beta \in \overline{\mathbb{Z}}$ we say β *divides* α, and write $\beta \mid \alpha$, if there exists some $\gamma \in \overline{\mathbb{Z}}$ such that $\alpha = \beta\gamma$. We write $\beta \nmid \alpha$ if β does not divide α. Recall from Definition 3.2.7 that for $\delta \in \overline{\mathbb{Z}}$ we say δ is uniform if $|\sigma(\delta)| = |\tau(\delta)|$ for all $\sigma, \tau \in \mathrm{X}(\overline{\mathbb{Q}})$.

Proposition 3.3.6. *If $\alpha \in \overline{\mathbb{Z}}$ is such that $\sqrt{2} \mid \alpha$ or $\sqrt{3} \mid \alpha$, then $\alpha \notin \mathrm{indec}(\overline{\mathbb{Z}})$.*

Proof. Let $\zeta \in \overline{\mathbb{Q}}$ be a primitive 8-th root of unity, which we may choose such that $\zeta + \zeta^{-1} = \sqrt{2}$. Thus $(\zeta, \zeta^{-1}) \in \mathrm{dec}(\sqrt{2})$, because $\langle \zeta, \zeta^{-1} \rangle = 0$ by Proposition 3.3.5. Moreover, $\sqrt{2}$, ζ and ζ^{-1} are all uniform. For any $\beta \in \overline{\mathbb{Z}}$ we get from Lemma 3.2.11 that

$$q(\zeta\beta) + q(\zeta^{-1}\beta) = (q(\zeta) + q(\zeta^{-1})) \cdot q(\beta) = q(\sqrt{2}) \cdot q(\beta) = q(\sqrt{2}\beta),$$

so $\sqrt{2}\beta$ has a non-trivial decomposition.

With ξ a primitive twelfth root of unity we have $\xi + \xi^{-1} = \sqrt{3}$ with ξ, ξ^{-1} and $\sqrt{3}$ uniform. We have a decomposition because $\langle \xi, \xi^{-1} \rangle = \langle 1, \xi^{-2} \rangle = \frac{1}{2} \geq 0$, so the argument from before applies. □

Lemma 3.3.7. *If $\alpha \in \overline{\mathbb{Z}}$ is such that $\sqrt{2} \nmid \alpha \mid 2$ and α is uniform, then $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$.*

Proof. By assumption we may write $2 = \alpha\gamma$ for some non-zero $\gamma \in \overline{\mathbb{Z}}$. Note that γ is not a unit, since otherwise $\sqrt{2} \mid 2 \mid \alpha$. Now let $(\beta, \alpha - \beta) \in \mathrm{dec}(\alpha)$. Then by Lemma 2.4.3 and Lemma 3.2.11 we have $q(\alpha) \geq q(\alpha - 2\beta) = q(\alpha - \alpha\beta\gamma) = q(\alpha) \cdot q(1 - \beta\gamma)$, so $q(1 - \beta\gamma) \leq 1$. As γ is not a unit we have $\beta\gamma \neq 1$, so $\beta\gamma = 1 - \zeta$ for some root of unity ζ of order say n by Proposition 3.2.9. Suppose n is not a power of 2. Then $1 - \zeta$ and 2 are coprime. As $2 \mid 2\beta = \alpha(1 - \zeta)$ we have that $2 \mid \alpha$, which contradicts $\sqrt{2} \nmid \alpha$. Hence n is a power of 2. If $n > 2$, then $1 - \zeta \mid \sqrt{2}$ so $\sqrt{2} \mid \alpha$, which is again a contradiction. Therefore $n = 1$ or $n = 2$, which correspond to the trivial decompositions with $\beta = 0$ and $\beta = \alpha$ respectively. We conclude that α is indecomposable. □

Proposition 3.3.8. *It holds that*

$$2\sqrt{2} \leq \sup\{q(\alpha) \mid \alpha \in \overline{\mathbb{Z}} \text{ is indecomposable}\}.$$

Proof. We will prove that for each $r \in \mathbb{Q} \cap [1, 3/2)$ there exists $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ such that $q(\alpha) = 2^r$.

Consider $\beta = \frac{1+\sqrt{-7}}{2}$ as in Example 3.3.3 and write $\overline{\beta} = 1 - \beta$ for its conjugate. Write $r = \frac{a}{b}$ with integers $a \geq b > 0$ and let $\gamma \in \overline{\mathbb{Z}}$ be a zero of $X^b - \beta$. Now take $\alpha = \overline{\beta} \cdot \gamma^{a-b}$. We will show α satisfies the conditions to Lemma 3.3.7. Because $|\sigma(\alpha)| = |\sigma(\beta)|^r = 2^{r/2}$ for all $\sigma \in \mathrm{X}(\overline{\mathbb{Q}})$, and hence α is uniform, we then have that α is indecomposable and $q(\alpha) = 2^r$.

Note that $\alpha \cdot \gamma^{2b-a} = \overline{\beta} \cdot \beta = 2$, so $\alpha \mid 2$. Let $v \colon K \to \mathbb{R} \cup \{\infty\}$ be a valuation over 2 for some number field K which is Galois over $\mathbb{Q}$ containing

the relevant elements. Because $0 = v(1) = v(\overline{\beta} + \beta) \geq \min\{v(\overline{\beta}), v(\beta)\}$, we have $v(\beta) = 0$ or $v(\overline{\beta}) = 0$. By potentially composing v with an automorphism swapping β and $\overline{\beta}$ we obtain a valuation v' such that $v'(\overline{\beta}) = 0$. We have $1 = v'(2) = v'(\beta \cdot \overline{\beta}) = v'(\beta)$ and thus $v'(\gamma) = 1/b$. Then $v'(\alpha) = r - 1 < 1/2 = v'(\sqrt{2})$, from which we conclude that $\sqrt{2} \nmid \alpha$. Thus α satisfies the conditions to Lemma 3.3.7, as was to be shown. □

3.4 Enumeration of degree-2 indecomposables

The indecomposables of $\overline{\mathbb{Z}}$ of degree 1 are 1 and -1. In this section we compute the indecomposables of degree 2. The fields of degree 2 over $\mathbb{Q}$ are $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z} \setminus \{1\}$ square-free. The following lemma is easily verified by separating the cases d negative and positive.

Lemma 3.4.1. *Let $d \in \mathbb{Z} \setminus \{1\}$ be square-free and let $a, b \in \mathbb{Q}$. Then $q(a + b\sqrt{d}) = a^2 + |d| \cdot b^2$.* □

Lemma 3.4.2. *Let $\alpha \in \overline{\mathbb{Z}}$ and suppose one of the following holds:*

1. *the real part of α^2 is at least 2 under every embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$;*
2. *the real part of α^2 is at most -2 under every embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$;*
3. *$\alpha = (1 + \sqrt{d})/2$ with $d \in \mathbb{Z}$ square-free such that $9 \leq d \leq 25$.*

Then α has a non-trivial decomposition in a degree 2 extension of $\mathbb{Q}(\alpha)$.

Proof. Let $K = \mathbb{Q}(\alpha)$ and $\gamma = \alpha^2/4$. Let $f = X^2 - \alpha X + 1 \in K[X]$, let $\beta \in \overline{\mathbb{Z}}$ be a root of f and write $L = K(\beta)$. Then $(\beta - \alpha/2)^2 = \beta^2 - \alpha\beta + \alpha^2/4 = \alpha^2/4 - 1 = \gamma - 1$. For 1 and 3 we will show $q(\beta - \alpha/2) \leq q(\alpha/2)$. Then $(\beta, \alpha - \beta)$ is a decomposition of α by Lemma 2.4.3, and since neither 0 nor α is a root of f we conclude that this decomposition is non-trivial.

1. Let $\sigma \in \mathrm{X}(L)$. For $\delta \in L$ write $\mathrm{Re}_\sigma(\delta)$ and $\mathrm{Im}_\sigma(\delta)$ for the real respectively imaginary part of $\sigma(\delta)$. By assumption $\mathrm{Re}_\sigma(\gamma) \geq 1/2$. Thus $\mathrm{Re}_\sigma(\gamma - 1)^2 = (\mathrm{Re}_\sigma(\gamma) - 1)^2 \leq \mathrm{Re}_\sigma(\gamma)^2$. As $\mathrm{Im}_\sigma(\gamma - 1)^2 = \mathrm{Im}_\sigma(\gamma)^2$ we may conclude that $|\sigma(\gamma - 1)| \leq |\sigma(\gamma)|$. Then

$$q(\beta - \alpha/2) = \frac{1}{[L : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\gamma - 1)| \leq \frac{1}{[L : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\gamma)| = q(\alpha/2),$$

as was to be shown.

2. Let $\mathrm{i} \in \overline{\mathbb{Q}}$ be a primitive fourth root of unity. Then $\mathrm{i}\alpha$ satisfies the conditions to 1, hence it has a non-trivial decomposition $(\beta, \mathrm{i}\alpha - \beta)$, where β is a root of $X^2 - \mathrm{i}\alpha X + 1$. In turn, $(-\mathrm{i}\beta, \alpha + \mathrm{i}\beta)$ is a non-trivial decomposition of α, where $-\mathrm{i}\beta$ is a root of $X^2 - \alpha X - 1$. In particular $-\mathrm{i}\beta$ is of degree at most 2 over $\mathbb{Q}(\alpha)$.

3. Since $d > 0$ the field K is totally real. Let $\gamma_1, \gamma_2 \in \mathbb{R}$ be the images of γ under $\mathrm{X}(K)$ such that $\gamma_1 < \gamma_2$. Because $9 \leq d \leq 25$ we have $\gamma_1 = (\sqrt{d}-1)^2/16 \leq 1$ and $\gamma_2 = (\sqrt{d}+1)^2/16 \geq 1$. Hence

$$\begin{aligned} q(\beta - \alpha/2) &= \frac{1}{2}\big(|\gamma_1 - 1| + |\gamma_2 - 1|\big) = \frac{1}{2}\big((1-\gamma_1) + (\gamma_2 - 1)\big) \\ &= \frac{2\sqrt{d}}{16} \leq \frac{1+d}{16} = q(\alpha/2), \end{aligned}$$

as was to be shown. □

Theorem 3.4.3. *The indecomposable elements of $\overline{\mathbb{Z}}$ of degree 2 up to conjugacy and sign are $\sqrt{-1}$, $\frac{1+\sqrt{-7}}{2}$, $\frac{1+\sqrt{-3}}{2}$ and $\frac{1+\sqrt{5}}{2}$, for a total of 14 indecomposables.*

Proof. First note that the 4 listed elements indeed are indecomposable: We treated $(1+\sqrt{-7})/2$ in Example 3.3.3, and the remaining 3 have square-norm less than 2, so Proposition 3.3.1 applies. Since conjugation and multiplication by -1 are isometries by Lemma 3.2.13, all 14 are indecomposable.

Let $\alpha \in \overline{\mathbb{Z}}$ be of degree 2 over $\mathbb{Q}$. It remains to show that α, up to conjugation and sign, admits a non-trivial decomposition or is one of the 4 listed indecomposables. Since α is of degree 2 over $\mathbb{Q}$ it is an element of $\mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}\setminus\{1\}$. Then we may write $\alpha = (a+b\sqrt{d})/2$ for some $a, b \in \mathbb{Z}$ with $a+b \in 2\mathbb{Z}$ and by conjugating and changing sign we may assume $a, b \geq 0$. If $a \geq 2$ we have

$$q(\alpha/2-1) = \Big(\frac{a}{4}-1\Big)^2 + |d|\Big(\frac{b}{4}\Big)^2 = \Big(\Big(\frac{a}{4}\Big)^2 + |d|\Big(\frac{b}{4}\Big)^2\Big) + \Big(1-\frac{a}{2}\Big) \leq q(\alpha/2),$$

so $(1, \alpha - 1)$ is a decomposition of α. Since $\alpha \neq 1$, this decomposition is non-trivial. Similarly we get a decomposition $(\sqrt{d}, \alpha - \sqrt{d})$ if $b \geq 2$, so either this decomposition is non-trivial or $\alpha = \sqrt{d}$.

First suppose $\alpha = \sqrt{d}$. If $|d| < 2$ then $d = -1$, and $\sqrt{-1}$ is listed. Otherwise $\alpha^2 = d$ satisfies the hypotheses of Lemma 3.4.2.1 or Lemma 3.4.2.2, so $\sqrt{d}$ is not indecomposable.

For $\alpha \neq \sqrt{d}$ the remaining cases are $\alpha = (1+\sqrt{d})/2$, which is integral only if $d \equiv 1 \bmod 4$. If $d \leq -9$ the real part of α^2 is $(1+d)/4 \leq -2$ under either embedding, so α satisfies the conditions to Lemma 3.4.2.2. If $-9 < d < 9$ we have $d \in \{-7, -3, 5\}$ and thus $\alpha = (1+\sqrt{d})/2$ is listed. For $9 \leq d \leq 25$ we may apply Lemma 3.4.2.3. The remaining case is $25 < d$, where we have that $\sigma(\alpha^2) = [(1 \pm \sqrt{d})/2]^2 \geq (\sqrt{d}-1)^2/4 \geq 2$ for all $\sigma \in \mathrm{X}(\mathbb{Q}(\sqrt{d}))$, so Lemma 3.4.2.1 applies. Hence α is either listed or not indecomposable. □

It is interesting to note that all non-trivial decompositions of $\alpha \in \overline{\mathbb{Z}}$ of degree 2 over $\mathbb{Q}$ that are produced in Theorem 3.4.3 live in a field extension of degree at most 2 over $\mathbb{Q}(\alpha)$.

3.5 Geometry of numbers

In this section we gather some known results about the geometry of numbers.

Definition 3.5.1. Let K be a number field. We write $K_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Q}} K$ and $K_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Q}} K$.

Recall for a number field K the definition of $\mathrm{X}(K)$, the set of ring homomorphisms from K to $\mathbb{C}$.

Lemma 3.5.2. *We have an isomorphism of $\mathbb{C}$-algebras $\Phi_K \colon K_{\mathbb{C}} \to \mathbb{C}^{\mathrm{X}(K)}$ given by*

$$\Phi_K(z \otimes \alpha) = (z \cdot \sigma(\alpha))_{\sigma \in \mathrm{X}(K)}.$$

We have a natural inclusion $K_{\mathbb{R}} \to K_{\mathbb{C}} \to \mathbb{C}^{\mathrm{X}(K)}$, and its image is given by the subspace of elements invariant under the involution $(x_\sigma)_\sigma \mapsto (\overline{x_{\overline{\sigma}}})_\sigma$. This inclusion induces an isomorphism of $\mathbb{R}$-algebras $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$ for integers $r, s \geq 0$ such that $r = \#\{\sigma \in \mathrm{X}(K) \mid \sigma[K] \subseteq \mathbb{R}\}$ and $r + 2s = [K : \mathbb{Q}]$. □

Definition 3.5.3. We equip $K_{\mathbb{C}}$ with the inner product induced by the standard Hermitian inner product on $\mathbb{C}^{\mathrm{X}(K)}$ and $K_{\mathbb{R}}$ with its restriction, turning $K_{\mathbb{R}}$ into a real inner product space. Since $K_{\mathbb{R}}$ is an inner product space we have an induced measure on $K_{\mathbb{R}}$ we denote vol.

Remark 3.5.4. For a number field K and $\alpha \in K$ we have

$$\|\alpha\|^2 = \frac{1}{[K : \mathbb{Q}]} \|\Phi_K(\alpha)\|^2.$$

In fact, $K_{\mathbb{R}}$ is the universal Hilbert space of the lattice $\overline{\mathbb{Z}} \cap K$. Note that the norm on $K_{\mathbb{R}}$ is not the 'standard' norm on $\mathbb{R}^r \times \mathbb{C}^s$. In terms of the latter vector space it is given by

$$(x_1, \ldots, x_r, z_1, \ldots, z_s) \mapsto \sqrt{|x_1|^2 + \cdots + |x_r|^2 + 2|z_1|^2 + \cdots + 2|z_s|^2}.$$

Theorem 3.5.5 (Proposition 4.26 in [38])**.** *Let R be an order in a number field K. Then $\Phi_K[R]$ is a full rank lattice in $K_{\mathbb{R}}$ with determinant $|\Delta(R)|^{1/2}$, where $\Delta(R)$ is the discriminant of R.* □

Definition 3.5.6. For a commutative ring R and $d \in \mathbb{Z}_{\geq 0}$ we write $R[X]_d = \{f \in R[X] \mid \deg(f) < d\}$.

Lemma 3.5.7. *The functor $-[X]_d$ commutes with finite products.* □

Lemma 3.5.8. *For a number field K we have an isomorphism of real vector spaces $K_{\mathbb{R}}[X]_d \cong (\mathbb{R}[X]_d)^r \times (\mathbb{C}[X]_d)^s$ for all $d \in \mathbb{Z}_{\geq 0}$ induced by the isomorphism $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$ of Lemma 3.5.2.* □

Theorem 3.5.9 (Minkowski, Theorem 4.19 in [38])**.** *Let $n \in \mathbb{Z}_{\geq 0}$, let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and let $S \subseteq \mathbb{R}^n$ be a symmetric convex body. If $\mathrm{vol}(S) > 2^n \det(\Lambda)$, then there exists a non-zero element in $\Lambda \cap S$.* □

Definition 3.5.10. For all $\alpha \in \overline{\mathbb{Q}}$ the set $\mathrm{X}(\overline{\mathbb{Q}}) \cdot \alpha$ is finite. Hence we may equip $\overline{\mathbb{Q}}$ with the *max-norm*

$$|x|_\infty = \max_{\sigma \in \mathrm{X}(\overline{\mathbb{Q}})} |\sigma(x)|.$$

We extend this definition to the universal Hilbert space containing $\overline{\mathbb{Q}}$, and in turn restrict it to $K_{\mathbb{C}}$ and $K_{\mathbb{R}}$ for any number field K.

Lemma 3.5.11. *For $\alpha \in \overline{\mathbb{Q}}$ we have $\|\alpha\| \leq |\alpha|_\infty$ and for $n \geq 0$ we have $|\alpha^n|_\infty = |\alpha|_\infty^n$.* □

3.6 Szegő capacity theory

In this section we will give a proof of a specialization of a theorem on capacity theory due to Szegő. As a corollary (Corollary 3.6.7) to this theorem T. Chinburg derives a solution to the closest vector problem for large radii as discussed in the introduction of this chapter. We will present the proof in a manner to be explicit enough to derive an algorithm.

Definition 3.6.1. Let X be a metric space with metric d and let $S \subseteq X$ be a subset. A *rounding function from X to S* is a map $\lfloor \cdot \rceil \colon X \to S$ for which there exists some constant $\varepsilon \in \mathbb{R}_{\geq 0}$ such that for all $x \in X$ we have $d(x, \lfloor x \rceil) \leq \varepsilon$. We call such an ε an *error constant* for $\lfloor \cdot \rceil$.

Example 3.6.2. For $\mathbb{Z}$ in $\mathbb{Q}$ with the metric induced by the usual absolute value we may round to a nearest integer, giving a rounding function with error constant $1/2$. For a naive rounding map for an arbitrary order R with basis $(\alpha_i)_i$ of a number field K with metric induced by q we may simply send $\sum_i x_i \alpha_i \in K$ with $x_i \in \mathbb{Q}$ to $\sum_i \lfloor x_i \rceil \alpha_i \in R$. An error constant for this rounding function is for example $\frac{1}{2} \sum_{i=1}^n |\alpha_i|_\infty$. The same method works for R in $K_{\mathbb{R}}$.

Definition 3.6.3. Let A be a commutative ring, let $c \in A$, and let $|\cdot|$ be a norm on A. We define the *induced c-norm on* $A[X]$ to be the norm

$$f = \sum_{k=0}^{\infty} f_k \cdot (X-c)^k = \sum_{k=0}^{\infty} f_k Y^k \mapsto \max_k |f_k|$$

for $Y = X - c$. Let $R \subseteq A$ be a subring and $[\cdot] : A \to R$ a rounding function. We say this rounding function is *translation invariant* if $[a+r] = [a] + r$ for all $a \in A$ and $r \in R$. We recursively define the *induced rounding function with respect to c* to be the rounding function $\lfloor \cdot \rceil : A[X] \to R[X]$ with respect to the c-norm on $A[X]$ given by $\lfloor 0 \rceil = 0$ and

$$\lfloor aX^n + f \rceil \mapsto [a]X^n + \left\lfloor (a - [a])(X^n - Y^n) + f \right\rceil$$

for all $a \in A$ and $f \in A[X]_n$.

We will verify that this is indeed a rounding function.

Proposition 3.6.4. *Using the same notation as in Definition 3.6.3, the map* $\lfloor \cdot \rceil : A[X] \to R[X]$ *is a rounding function with the same error constant as the rounding function* $[\cdot] : A \to R$*. If the latter is translation invariant, then so is the former.*

Proof. Let ε be the error constant for $[\cdot]$ and $Y = X - c$. We with induction on n that $\lfloor \cdot \rceil$ restricts to a rounding function $A[X]_{n+1} \to R[X]_{n+1}$ with error constant ε. Clearly $\|0 - \lfloor 0 \rceil\| = 0 \leq \varepsilon$. Suppose $n \in \mathbb{Z}_{\geq 0}$ and consider $aX^n + f$ for $a \in A$ and $f \in A[X]_n$. Write

$$g = (a - [a])(X^n - Y^n) + f \in A[X]_n.$$

Then by the induction hypothesis

$$\|f - \lfloor f \rceil\| = \|(a - [a])Y^n + (g - \lfloor g \rceil)\| = \max\{|a - [a]|, \|g - \lfloor g \rceil\|\} \leq \varepsilon,$$

as was to be shown. Hence $\lfloor \cdot \rceil : A[X] \to R[X]$ is a rounding function with error constant ε.

Suppose $[\cdot]$ is translation invariant. To show $\lfloor \cdot \rceil$ is translation invariant, it suffices to show with induction to n that for all $a \in A$, $b \in R$, $f \in A[X]_n$ and $g \in R[X]_n$ we have $\lfloor (aX^n + f) + (bX^n + g) \rceil = \lfloor aX^n + f \rceil + (bX^n + g)$. The base case reduces to translation invariance of $[\cdot]$. For $n \geq 0$ we have

$$\begin{aligned}
&\lfloor (aX^n + f) + (bX^n + g) \rceil \\
&\quad = [a+b]X^n + \lfloor ((a+b) - [a+b])(X^n - Y^n) + f + g \rceil \\
&\quad = ([a] + b)X^n + \lfloor (a - [a])(X^n - Y^n) + f \rfloor + g \\
&\quad = \lfloor aX^n + g \rceil + (bX^n + g),
\end{aligned}$$

as was to be shown. □

Recall the the max-norm from Definition 3.5.10.

Theorem 3.6.5 (Szegő)**.** *Let R be an order of a number field K and let $r > 1$. Then for each $c \in K$ there exists a monic non-constant $g \in R[X]$ such that for all $z \in K_{\mathbb{C}}$ satisfying $|g(z)|_\infty < r$ we have $|z - c|_\infty < r$.*

This theorem is a special case of a theorem of Szegő, adapted from [40]. For simplicity we take $c \in K$ instead of $c \in K_{\mathbb{R}}$. The proof of this theorem will be sufficiently constructive that one can easily distill an algorithm from it.

Proof. Let $[\cdot] : K \to R$ be some translation invariant rounding function, for example as in Example 3.6.2, and let ε be its error constant. Let $\lfloor \cdot \rceil$ be the induced rounding function with respect to c. Let $d \in \mathbb{Z}_{>0}$ such that $dc \in R$, which exists since $c \in \mathbb{Q}R$. Successively choose $b, n \in \mathbb{Z}_{>0}$ such that

$$(1)\ 2\varepsilon r^{-b} \leq r - 1, \quad (2)\ b! \cdot d^b \mid n \quad \text{and} \quad (3)\ r^{n-1} \geq 2.$$

We claim $g = \lfloor (X - c)^n \rceil$ satisfies the conclusion to the theorem.

Write $f = (X - c)^n = \sum_k f_k X^k$. It follows from (2) that for all $k \leq b$ we have $d^k \mid \frac{b! d^b}{k!} \mid \binom{n}{n-k}$. Hence for all $k \geq n - b$ we have $f_k = \binom{n}{n-k} c^{n-k} \in R$. Thus by translation invariance we have $e \colon = f - g \in K[X]_{n-b}$. Let $\mathrm{X}(K)$ act on $K[X]$ coefficient-wise and fix $\sigma \in \mathrm{X}(K)$. Let $z \in \mathbb{C}$ such that $s := |z - \sigma(c)| \geq r$. Then

$$\left| \frac{\sigma(e)(z)}{\sigma(f)(z)} \right| \leq s^{-n} \sum_{i=0}^{n-b-1} \varepsilon \cdot s^i \leq \frac{\varepsilon s^{-b}}{s - 1} \leq \frac{c r^{-b}}{r - 1} \overset{(1)}{\leq} \frac{1}{2}.$$

It follows that

$$\left| \frac{\sigma(g)(z)}{\sigma(f)(z)} \right| = \left| 1 - \frac{\sigma(e)(z)}{\sigma(f)(z)} \right| \geq \frac{1}{2} \quad \text{and}$$
$$|\sigma(g)(z)| \geq \frac{|\sigma(f)(z)|}{2} \geq \frac{r^n}{2} \overset{(3)}{\geq} r.$$

Thus, if $|\sigma(g)(z)| < r$, then $|z - \sigma(c)| < r$. Taking the maximum over all $\sigma \in \mathrm{X}(K)$ proves the theorem for $c \in K$. □

Theorem 3.6.6 (Szegő)**.** *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r > 1$, then there exist infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $|\alpha - \beta|_\infty < r$.*

Proof. Consider $K = \mathbb{Q}(\alpha)$ and let $R \subseteq K$ be some order of K. By Theorem 3.6.5 there exists some monic non-constant $g \in R[X]$ such that for all

$z \in K_{\mathbb{C}}$ satisfying $|g(z)|_\infty < r$ we have $|z - \alpha|_\infty < r$. Now $g^n - 1 \in R[X]$ is monic and non-constant for all $n \in \mathbb{Z}_{\geq 1}$, so

$$S = \{\beta \in \overline{\mathbb{Z}} \mid (\exists\, n \in \mathbb{Z}_{\geq 1})\ g^n(\beta) = 1\}$$

is infinite. Let $\beta \in S$ and $L = K(\beta)$. It suffices to show that $|\alpha - \beta|_\infty < r$. We have that

$$|g(\beta)|_\infty^n = |g(\beta)^n|_\infty = |1|_\infty = 1,$$

so $|g(\beta)|_\infty < r$. Thus by definition of g we have $|\alpha - \beta|_\infty < r$. □

Combined with Lemma 3.5.11 we obtain the following.

Corollary 3.6.7. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r > 1$, then there exist infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$.* □

Proposition 3.6.8. *If $\alpha \in \overline{\mathbb{Z}}$ satisfies $\|\alpha\| > 2$, then α has infinitely many decompositions in $\overline{\mathbb{Z}}$.*

Proof. Let $\gamma = \alpha/2$. By Corollary 3.6.7 there are infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\gamma - \beta\| < \|\gamma\|$ as $\|\gamma\| = \|\alpha\|/2 > 1$. By Lemma 2.4.3 each such β gives a decomposition $(\beta, \alpha - \beta)$ of α. □

It follows from this proposition, as we will show later in the form of Proposition 3.7.4, that there are only finitely many indecomposables in $\overline{\mathbb{Z}}$ of a given degree.

Theorem 3.6.9. *The covering radius of $\overline{\mathbb{Z}}$, see Definition 2.6.1, is between $\sqrt[4]{1/2}$ and 1.*

Proof. By Proposition 3.3.8 we have $2^{3/4} \leq \sup\{\|\alpha\| \mid \alpha \in \mathrm{indec}(\overline{\mathbb{Z}})\}$ and consequently we get the lower bound $2^{-1/4} \leq \sup\{\|\alpha/2\| \mid \alpha \in \mathrm{indec}(\overline{\mathbb{Z}})\}$. For any $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ we have by Lemma 2.4.3 for all $x \in \overline{\mathbb{Z}}$ that $\|\alpha/2\| \leq \|\alpha/2 - x\|$, and thus $\alpha/2 \in \overline{\mathrm{Vor}}(\overline{\mathbb{Z}})$ by Corollary 2.6.12. Therefore $2^{-1/4} \leq r(\overline{\mathbb{Z}})$ by Proposition 2.6.10. For all $r > 1$ and $\alpha \in \overline{\mathbb{Q}}$ there exist $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$ by Corollary 3.6.7. Taking the limit of r down to 1 and noting that $\overline{\mathbb{Q}} = \mathbb{Q} \cdot \overline{\mathbb{Z}}$ is dense in the Hilbert space of $\overline{\mathbb{Z}}$ proves the theorem. □

Proposition 3.6.10. *There exists an algorithm that, given $n \in \mathbb{Z}_{>0}$, some $r \in \mathbb{R} \cap \overline{\mathbb{Q}}$ and $\alpha \in \overline{\mathbb{Q}}$, decides whether $r > 1$ and if so computes n distinct $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$, each represented by their minimal polynomial over $\mathbb{Q}(\alpha)$.*

Proof. Since $r \in \overline{\mathbb{Q}}$ we may decide whether $r = 1$, and if it is not we may approximate r to arbitrary precision so that we may decide whether $r > 1$. We may compute an error constant $\varepsilon \in \mathbb{Q}_{>1}$ for the rounding function and then the polynomial g as in Theorem 3.6.5. For sufficiently many m we then compute the irreducible factors of $g^m - 1$ over $\mathbb{Q}(\alpha)$ as in [31], following the proof of Theorem 3.6.6. □

Corollary 3.6.11. *There is an algorithm that takes as input an $n \in \mathbb{Z}_{\geq 0}$ and an element $\alpha \in \overline{\mathbb{Z}}$ given by its minimal polynomial, and decides whether $\|\alpha\| > 2$ and if so computes n non-trivial decompositions $(\beta, \gamma) \in \mathrm{dec}(\alpha)$, each represented by the minimal polynomial of β over $\mathbb{Z}[\alpha]$.*

Proof. We apply Proposition 3.6.10 with $\alpha/2$ in the place of α and $\|\alpha/2\|$ in the place of r. Note that $r \in \mathbb{R} \cap \overline{\mathbb{Q}}$. □

3.7 Bounds on indecomposable algebraic integers

In this section we will prove an effective upper bound on the total number of indecomposable algebraic integers of a given degree. In particular, we will show that this number is finite. We do this by constructing a complete list of candidates for indecomposability among all algebraic integers of given degree. We also give a lower bound on the number of indecomposables.

Proposition 3.7.1. *Suppose $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ has minimal polynomial $f = \sum_{k=0}^{n} f_{n-k} X^k \in \mathbb{Z}[X]$. Then $|f_k| \leq \binom{n}{k} 2^k$ for all $0 \leq k \leq n$.*

Proof. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^\times$ be the roots of f. We have Maclaurin's inequalities (Theorem 11.2 in [7])

$$s_1 \geq s_2^{1/2} \geq s_3^{1/3} \geq \cdots \geq s_n^{1/n}, \quad \text{where } s_k = \binom{n}{k}^{-1} \cdot \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=k}} \prod_{i \in I} |\alpha_i|.$$

By Proposition 3.6.8 we have that $\|\alpha\| \leq 2$. Then by Lemma 2.2.14 we have

$$s_1 = \frac{1}{n} \sum_i |\alpha_i| \leq \Big(\frac{1}{n} \sum_i |\alpha_i|^2 \Big)^{1/2} = \|\alpha\| \leq 2.$$

Then $|f_k| \leq \binom{n}{k} s_k \leq \binom{n}{k} s_1^k \leq \binom{n}{k} 2^k$ for all k, as was to be shown. □

Corollary 3.7.2. *Suppose $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ has degree at most m. Then there exists a monic polynomial $g = \sum_{k=0}^{m} g_{m-k} X^k \in \mathbb{Z}[X]$ of degree m such that $g(\alpha) = 0$ and $|g_k| \leq \binom{m}{k} 2^k$ for all $0 \leq k \leq m$.*

Proof. Let f as in Proposition 3.7.1 and $g = X^{m-n} \cdot f$. Then $|g_k| = |f_k| \leq \binom{n}{k} 2^k \leq \binom{m}{k} 2^k$. □

Proposition 3.7.3. *Considered as functions of $n \in \mathbb{Z}_{\geq 1}$, the following hold:*

1. $$\log(n!) = n \log n - n + O(\log n);$$
2. $$\log\Big(\prod_{k=1}^{n} k^k\Big) = \tfrac{1}{2} n^2 \log n - \tfrac{1}{4} n^2 + O(n \log n);$$
3. $$\log\Big(\prod_{k=0}^{n} (k!)\Big) = \tfrac{1}{2} n^2 \log n - \tfrac{3}{4} n^2 + O(n \log n);$$
4. $$\log\Big(\prod_{k=0}^{n} \binom{n}{k}\Big) = \tfrac{1}{2} n^2 + O(n \log n).$$

Proof. 1. This is Stirling's approximation, which is classical.

2. Note that $f(x) = x \log x$ is an increasing function on $\mathbb{R}_{\geq 1}$. Hence

$$\begin{aligned} \log\Big(\prod_{k=1}^{n} k^k\Big) = \sum_{k=1}^{n} f(k) &\leq \int_1^{n+1} f(x)\,\mathrm{d}x = \Big[\tfrac{1}{2} x^2 \log(x) - \tfrac{1}{4} x^2\Big]_{x=1}^{n+1} \\ &= \tfrac{1}{2} n^2 \log(n) - \tfrac{1}{4} n^2 + O(n \log(n)). \end{aligned}$$

We analogously get the same estimate for a lower bound by considering $\int_1^n f(x)\,\mathrm{d}x$.

3. From 1 and 2 we get

$$\begin{aligned} \log\Big(\prod_{k=0}^{n} (k!)\Big) &= \sum_{k=1}^{n} \Big(k \log(k) - k + O(\log(k))\Big) \\ &= \big(\tfrac{1}{2} n^2 \log(n) - \tfrac{1}{4} n^2\big) - \tfrac{1}{2} n^2 + O(n \log(n)). \end{aligned}$$

4. We first rewrite the binomials in terms of factorials and then apply 1 and 3, so that

$$\begin{aligned} \log\Big(\prod_{k=0}^{n} \binom{n}{k}\Big) = \log\left(\frac{(n!)^n}{\big(\prod_{k=0}^{n} (k!)\big)^2}\right) &= n \log(n!) - 2 \log\Big(\prod_{k=0}^{n} (k!)\Big) \\ &= (n^2 \log(n) - n^2) - 2(\tfrac{1}{2} n^2 \log n - \tfrac{3}{4} n^2) + O(n \log n) \\ &= \tfrac{1}{2} n^2 + O(n \log n), \end{aligned}$$

as was to be shown. □

Proposition 3.7.4. *Let $n \in \mathbb{Z}_{\geq 1}$. There are at most*

$$n \prod_{k=1}^{n} \left(2\binom{n}{k}2^k + 1\right) = \exp\left(\tfrac{\log(2)+1}{2}\, n^2 + O(n\log(n))\right)$$

indecomposable elements in $\overline{\mathbb{Z}}$ of degree up to n.

Proof. By Corollary 3.7.2 every indecomposable of degree at most n is the root of a monic polynomial $f = \sum_{k=0}^{n} f_{n-k}X^k$ such that $|f_k| \leq \binom{n}{k}2^k$ for all $0 \leq k \leq n$. Hence every such polynomial corresponds to at most n indecomposables. For every $0 < k \leq n$ there are $2\binom{n}{k}2^k + 1$ choices for f_k, and $f_0 = 1$, proving the first upper bound. We may bound $2\binom{n}{k}2^k + 1 \leq 3\binom{n}{k}2^k$, so that by Proposition 3.7.3.4 we get

$$\begin{aligned} n \prod_{k=1}^{n} \left(2\binom{n}{k}2^k + 1\right) &\leq n \cdot 3^n \cdot 2^{\binom{n+1}{2}} \cdot \prod_{k=0}^{n} \binom{n}{k} \\ &= \exp\left(\tfrac{\log(2)+1}{2}\, n^2 + O(n\log(n))\right), \end{aligned}$$

as was to be shown. □

For $f \in \mathbb{Q}[X]$ monic write $q(f)$ for the average of the square length of the roots of f in $\mathbb{C}$, such that for all $\alpha \in \overline{\mathbb{Z}}$ with minimal polynomial $f_\alpha \in \mathbb{Q}[X]$ we get $q(\alpha) = q(f_\alpha)$. Note that $f = (X+2)^n$, although it is not irreducible, has $q(f) = 4$ and attains the bounds of Proposition 3.7.1. However, that does not imply that Proposition 3.7.4 cannot be improved, as it is not clear that all combinations of coefficients occur for polynomials f with $q(f) \leq 4$. Some small degree numerical results might suggest improvements can be made.

degree	1	2	3	4
# monic $f \in \mathbb{Z}[X]$ s.t. $(\forall k)\ \lvert f_k\rvert \leq \binom{n}{k}2^k$	5	81	5525	1786785
# monic $f \in \mathbb{Z}[X]$ s.t. $q(f) \leq 4$	5	49	989	48422
# $\alpha \in \overline{\mathbb{Z}}$ s.t. $q(\alpha) \leq 4$	5	39	739	40354

We also have the following lower bound.

Proposition 3.7.5. *Let $n \in \mathbb{Z}_{\geq 1}$. There are at least*

$$\exp\left(\frac{\log 2}{4}n^2 + O(n\log n)\right)$$

indecomposable algebraic integers of degree n.

Proof. Let $n \in \mathbb{Z}_{\geq 1}$ and recall the definition of $\mathbb{Z}[X]_n$ from Definition 3.5.6. Consider the set

$$S_n = \left\{ f = \sum_{k=0}^{n-1} f_k X^k \in 2X\mathbb{Z}[X]_{n-1} + 2 \;\middle|\; (\forall k)\ |f_k|(\sqrt{2})^k n \leq (\sqrt{2})^{n-1} \right\}.$$

For $f \in S_n$ consider $g = X^n - f$ and note that g is irreducible by Eisenstein's criterion. Consider the ball $D \subseteq \mathbb{C}$ of radius $r = (\sqrt{2})^{1-1/n} < \sqrt{2}$ around 0. For all z on the boundary of D we have

$$|f(z)| \leq \sum_{k=0}^{n-1} |f_k||z|^k \leq \sum_{k=0}^{n-1} |f_k|(\sqrt{2})^k \overset{\text{(i)}}{\leq} \sum_{k=0}^{n-1} \frac{(\sqrt{2})^{n-1}}{n} = (\sqrt{2})^{n-1} = |z|^n,$$

where (i) is strict for n sufficiently large due to $|f_0|n = 2n < (\sqrt{2})^{n-1}$. Hence by Rouché's theorem (Theorem 4.18 in [1]) the polynomials X^n and g have the same number of roots in D. It follows that all roots of g in $\mathbb{C}$ have length less than $\sqrt{2}$. Thus $q(\alpha) < 2$ for all roots $\alpha \in \overline{\mathbb{Z}}$ of g, so α is indecomposable by Proposition 3.3.1.

We conclude that for n sufficiently large there are at least $n \cdot \#S_n$ indecomposable algebraic integers of degree n, so it remains to prove a lower bound on $\#S_n$. Note that the coefficients of $f \in S_n$ satisfy independent inequalities, so we may simply give a lower bound per coefficient. Let $B = n - 3\log_2(n) - 2$, which is positive for n sufficiently large. For $k > B$ we consider only $f_k = 0$ and get a lower bound of 1 for this coefficient. For $0 < k \leq B$ we have

$$2\left\lfloor \frac{(\sqrt{2})^{n-k-1}}{2n} \right\rfloor + 1 \geq 2\Big(\frac{(\sqrt{2})^{n-k-1}}{2n} - 1\Big) + 1 = \frac{(\sqrt{2})^{n-k-1}}{n} - 1 = \text{(ii)}$$

choices for f_k. Then for n sufficiently large we have

$$\frac{n}{(\sqrt{2})^{n-k-2}} \leq \frac{n}{n^{3/2}} \leq \sqrt{2} - 1, \quad \text{so that} \quad \text{(ii)} \geq \frac{(\sqrt{2})^{n-k-2}}{n}.$$

Hence S_n contains, for n sufficiently large, at least

$$\begin{aligned} \prod_{k=1}^{B} \frac{(\sqrt{2})^{n-k-2}}{n} &= \exp\Big(\frac{\log 2}{2} \sum_{k=1}^{B} (n-k-2) - B\log n\Big) \\ &= \exp\Big(\frac{\log 2}{4} n^2 + O(n\log n)\Big) \end{aligned}$$

elements, from which the proposition follows. □

Corollary 3.7.6. *Let $n \in \mathbb{Z}_{\geq 1}$. There are at least*

$$\exp\Big(\frac{\log 2}{4}n^2 + O(n \log n)\Big)$$

indecomposable algebraic integers of degree up to n. □

From the upper and lower bound we may now conclude the following.

Theorem 3.7.7. *There are least* $\exp(\frac{1}{4}(\log 2)d^2 + O(d \log d))$ *and at most* $\exp(\frac{1}{2}(1 + \log 2)d^2 + O(d \log d))$ *indecomposable algebraic integers of degree up to d.* □

3.8 Fekete capacity theory

In this section we present a proof of a special case of Fekete's theorem using Minkowski's convex body theorem. Fekete's theorem can be thought of as a partial converse to Theorem 3.6.6 of Szegő. Although this does not give us a converse to Corollary 3.6.7, using similar techniques as in this section we will later prove Theorem 3.11.2 mentioned in the introduction. The goal of this section is to showcase the proof technique we will use to prove Theorem 3.11.2 so that we may later improve clarity by brevity. Recall the definition of the norm $|\cdot|_\infty$ from Definition 3.5.10.

Theorem 3.8.1 (Fekete)**.** *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r < 1$, then there exist only finitely many $\beta \in \overline{\mathbb{Z}}$ such that $|\beta - \alpha|_\infty \leq r$.*

Just like for Szegő's theorem, it is possible to derive an algorithmic counterpart to Fekete's theorem. Combining Theorem 3.8.1 and Theorem 3.6.6, the point $r = 1$ is still a singularity. For $\alpha \in \overline{\mathbb{Z}}$ and $r = 1$ clearly all $\beta \in \alpha + \mu_\infty$ satisfy $|\beta - \alpha|_\infty \leq r$. However, when $\alpha \notin \overline{\mathbb{Z}}$ we do not know what happens in general. We start with a volume computation.

Definition 3.8.2. Let A be an $\mathbb{R}$-algebra equipped with a real inner product. We equip $A[Y]$ with an inner product

$$\Big\langle \sum_{k=0}^{\infty} f_k Y^k, \sum_{k=0}^{\infty} g_k Y^k \Big\rangle = \sum_{k=0}^{\infty} \langle f_k, g_k \rangle,$$

which is the 'standard' inner product when we naturally identify $A[Y]$ with $A^{(\mathbb{Z}_{\geq 0})}$. For $n \in \mathbb{Z}_{\geq 0}$ we equip $A[Y]_n$, as defined in Definition 3.5.6, with the restriction of this inner product.

Remark 3.8.3. Obviously $\mathbb{R}$ is an $\mathbb{R}$-algebra with a real inner product. We identify $\mathbb{C}$ with $\mathbb{R}^2$ by choosing $\mathbb{R}$-basis $\{1, \mathrm{i}\}$, and equip $\mathbb{C}$ with the inner product induced by the natural inner product on $\mathbb{R}^2$. For a number field K we remark that $K_{\mathbb{R}}$ has a real inner product as in Definition 3.5.3.

Lemma 3.8.4. *Let A be an $\mathbb{R}$-algebra of dimension $d < \infty$. For all $a, b \in \mathbb{R}$, $c \in A$ and $n \in \mathbb{Z}_{\geq 0}$ we have an $\mathbb{R}$-linear transformation ϕ on $A[X]_n$ given by $f \mapsto bf(a(X - c))$ with $\det \phi = (a^{n(n-1)/2} \cdot b^n)^d$.*

Proof. Note that ϕ is trivially an $\mathbb{R}$-linear transformation. Choose an $\mathbb{R}$-basis $\{e_1, \ldots, e_d\}$ for A. Writing ϕ as a matrix with respect to the basis $\{e_i X^j \mid 1 \leq i \leq d, 0 \leq j < n\}$ for $A[X]_n$ we note that ϕ is a lower triangular matrix with diagonal entries $b, ba, ba^2, \ldots, ba^{n-1}$, each occurring with multiplicity d. The determinant of ϕ is then simply the product of the diagonal. □

Lemma 3.8.5. *Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{C}$ and let $r \in \mathbb{R}_{>0}$. For $n \in \mathbb{Z}_{\geq 0}$ consider*

$$S_n(r) = \{f \in \mathbb{F}[Y]_n \mid (\forall\, z \in \mathbb{C})\ |z| \leq r \Rightarrow |f(z)| \leq r\}.$$

Then as function of n we have

$$\log \mathrm{vol}(S_n(r)) \geq -\tfrac{1}{2} n^2 \cdot [\mathbb{F} : \mathbb{R}] \cdot \log r + O(n \log n).$$

Proof. Write $S_n = S_n(1)$. By applying the transformation $f \mapsto rf(r^{-1}Y)$ to $\mathbb{F}[Y]_n$ we bijectively map S_n to $S_n(r)$. From Lemma 3.8.4 it follows that $\log \mathrm{vol}(S_n(r)) = -\frac{1}{2} n^2 \cdot [\mathbb{F} : \mathbb{R}] \cdot \log r + \log \mathrm{vol}(S_n) + O(n \log n)$. It remains to prove $\log \mathrm{vol}\, S_n \geq O(n \log n)$.

First suppose $\mathbb{F} = \mathbb{R}$. Consider the set

$$T_n = \Big\{ \sum_{k=0}^{n-1} f_k Y^k \in \mathbb{R}[Y]_n \;\Big|\; \sum_{k=0}^{n-1} |f_k| \leq 1 \Big\}.$$

Note that for all $f \in T_n$ and $z \in \mathbb{C}$ such that $|z| \leq 1$ we have $|f(z)| \leq \sum_{k=0}^{n-1} |f_k| \leq 1$, so $f \in S_n$. Hence $T_n \subseteq S_n$ and $\mathrm{vol}(T_n) \leq \mathrm{vol}(S_n)$. With Proposition 3.7.3.1 we compute $\log \mathrm{vol}(T_n) = \log(2^n/n!) = O(n \log n)$, from which the lemma follows for $\mathbb{F} = \mathbb{R}$.

For $\mathbb{F} = \mathbb{C}$, note that we have an isometry $\mathbb{R}[X]_n^2 \to \mathbb{C}[X]_n$ given by $(f, g) \mapsto f + \mathrm{i} \cdot g$. For $f, g \in \frac{1}{2} T_n$ and $z \in \mathbb{C}$ such that $|z| \leq 1$ we have $|f(z) + \mathrm{i} \cdot g(z)| \leq |f(z)| + |g(z)| \leq \frac{1}{2} + \frac{1}{2} = 1$, so $f + \mathrm{i} \cdot g \in S_n$. Hence $\log \mathrm{vol}(S_n) \geq \log(\mathrm{vol}(\frac{1}{2} T_n)^2) = 2 \log \mathrm{vol}(T_n) - 2n \log 2 = O(n \log n)$, from which the lemma follows for $\mathbb{F} = \mathbb{C}$. □

Theorem 3.8.6. *Let R be an order of a number field K and let $0 < r < 1$. For all $c \in K_{\mathbb{R}}$ there exists a non-zero $g \in R[X]$ such that for all $z \in K_{\mathbb{R}}$, if $|z - c|_\infty \leq r$ then $|g(z)|_\infty \leq r$.*

Proof. Write $d = [K : \mathbb{Q}]$. Let $n \in \mathbb{Z}_{\geq 0}$ and consider the lattice $\Lambda_n = R[X]_n$ in the inner product space $K_{\mathbb{R}}[Y]_n$, where $Y = X - c$. Note that $\dim_{\mathbb{R}} K_{\mathbb{R}}[Y]_n = dn$ and that Λ_n is a full-rank lattice in $K_{\mathbb{R}}[Y]_n$ with $\det(\Lambda_n) = |\Delta(R)|^{n/2}$ by Lemma 3.8.4 and Theorem 3.5.5. Consider

$$S_n = \left\{ f \in K_{\mathbb{R}}[Y]_n \;\middle|\; (\forall\, \sigma \in \mathrm{X}(K))\,(\forall\, z \in \mathbb{C})\ |z| \leq r \Rightarrow |\sigma(f)(z)| \leq r \right\}$$

and note that it is both symmetric and convex. Moreover, it follows from Lemma 3.8.5 that $\log \mathrm{vol}(S_n) \geq -\frac{1}{2} n^2 d \log r + O(n \log n)$. Hence

$$\log\left(\frac{\mathrm{vol}(S_n)}{2^{dn} \cdot \det(\Lambda_n)}\right) \geq -\tfrac{1}{2} n^2 d \log r + O(n \log n).$$

Because $-\frac{1}{2} d \log r > 0$ there exists some n sufficiently large such that $\mathrm{vol}(S_n) > 2^{dn} \det(\Lambda_n)$. By Theorem 3.5.9 there then exists some non-zero $g \in \Lambda_n \cap S_n$ which as polynomial in X satisfies the requirements. □

Proof of Theorem 3.8.1. Let $K = \mathbb{Q}(\alpha)$ and let $R \subseteq K$ be some order of K. Then by Theorem 3.8.6 there exists some non-zero $g \in R[X]$ such that for all $z \in K_{\mathbb{R}}$, if $|z - \alpha|_\infty \leq r$ then $|g(z)|_\infty \leq r$. Suppose $\beta \in \overline{\mathbb{Z}}$ satisfies $|\beta - \alpha|_\infty \leq r$. Then $|g(\beta)|_\infty \leq r$, or equivalently $|\rho(g(\beta))| \leq r$ for all $\rho \in \mathrm{X}(L)$. Hence

$$|N_{L/\mathbb{Q}}(g(\beta))| = \prod_{\rho \in \mathrm{X}(L)} |\rho(g(\beta))| \leq r^{[L:\mathbb{Q}]} < 1.$$

As $g(\beta) \in \overline{\mathbb{Z}}$, we must then have $g(\beta) = 0$. As β must be a root of g and g is non-zero, there can only be finitely many β. □

3.9 Reduction to exponentially bounded polynomials

We now prepare to prove the main theorem. If there are only finitely many decompositions of an algebraic integer α, then certainly there exists a non-zero polynomial $f \in \mathbb{Z}[X]$ such that $f(\beta) = 0$ for all decompositions $(\beta, \alpha - \beta)$ of α. The goal is to exhibit such a polynomial when α is short using a lattice argument, similarly to the proof of Theorem 3.8.1. In this section we derive an analytic sufficient condition for a polynomial f to have this property.

Definition 3.9.1. Let K be a number field. We define $\mathcal{S}(K) = \mathrm{X}(K) \times \mathbb{C}$, the coproduct (i.e. disjoint union) of measurable spaces of $\#\,\mathrm{X}(K)$ copies of $\mathbb{C}$, where $\mathbb{C}$ has the standard Lebesgue measurable space structure. We write $\mathcal{M}(K)$ for the set of probability measures μ on $\mathcal{S}(K)$, i.e. all measures μ such that $\mu(\mathcal{S}(K)) = 1$.

Definition 3.9.2. Let K be a number field and $r \in \mathbb{R}_{>0}$. For $f \in K_{\mathbb{R}}[Y]$ we say f is *exponentially bounded at radius* r if for all $\mu \in \mathcal{M}(K)$ satisfying $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < r^2$ it holds that $\int \log|\sigma(f)(z)| \,\mathrm{d}\mu(\sigma, z) < 0$.

Proposition 3.9.3. *Let $\alpha \in \overline{\mathbb{Z}}$, $K = \mathbb{Q}(\alpha)$ and $r > \|\alpha/2\|$. If $f \in \mathcal{O}_K[X]$ is exponentially bounded at radius $r \in \mathbb{R}_{>0}$ as polynomial in the variable $Y = X - \alpha/2$, then for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ we have $f(\beta) = 0$.*

Proof. Suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$. Then $\|\beta - \alpha/2\| \leq \|\alpha/2\| < r$ by Lemma 2.4.3. Let $L = K(\beta)$ and

$$B = \{(\rho|_K, \rho(\beta - \alpha/2)) \,|\, \rho \in \mathrm{X}(L)\} \subseteq \mathcal{S}(K),$$

which has $\#B = [L : \mathbb{Q}]$ and $\#(B \cap (\{\sigma\} \times \mathbb{C})) = [L : K]$ for all $\sigma \in \mathrm{X}(K)$. Let $\mu \in \mathcal{M}(K)$ be the uniform probability measure on B and write f_Y for f as a polynomial in the variable Y. Because $\int |x|^2 \,\mathrm{d}\mu(\sigma, x) = \|\beta - \alpha/2\|^2 < r^2$ and f_Y is exponentially bounded at radius r we get

$$\begin{aligned}\log\left(N(f(\beta))^{[L:\mathbb{Q}]}\right) &= \log \prod_{\rho \in \mathrm{X}(L)} |\rho(f(\beta))| = \sum_{\rho \in \mathrm{X}(L)} \log|\rho(f_Y(\beta - \alpha/2))| \\ &= [L : \mathbb{Q}] \cdot \int \log|\sigma(f_Y)(x)| \,\mathrm{d}\mu(\sigma, x) < 0.\end{aligned}$$

We conclude that $N(f(\beta)) < 1$. Since $f(\beta)$ is integral we have $f(\beta) = 0$, as was to be shown. □

Example 3.9.4. The set of polynomials of $K_{\mathbb{R}}$ exponentially bounded at radius r is closed under multiplication and is symmetric. However, we will show that it is not convex.

Let $r = 1$ and $K = \mathbb{Q}$. For all $c \in (-1, 1)$ the constant polynomial c is trivially exponentially bounded at any positive radius, in particular at radius 1. Also the polynomial Y^2 is exponentially bounded: For any $\mu \in \mathcal{M}(K)$ such that $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < 1$ we have

$$\int \log|z^2| \,\mathrm{d}\mu(\sigma, z) \leq \log \int |z|^2 \,\mathrm{d}\mu(\sigma, z) < \log 1 = 0.$$

Here the first inequality is Jensen's inequality for integrals. When μ has finite support, this comes down to Lemma 3.2.6. For $c \in (-1, 1)$ and

$k \in \mathbb{Z}_{\geq 0}$ the product cY^{2k} of exponentially bounded polynomials at radius 1 is exponentially bounded at radius 1. We claim that $\frac{1}{4}(1 + Y^{2k})$ for k sufficiently large, which is a convex combination of $\frac{1}{2}$ and $\frac{1}{2}Y^{2k}$, is not exponentially bounded at radius 1. Taking $\mu \in \mathcal{M}(\mathbb{Q})$ with weight $\frac{1}{5}$ at 2 and remaining weight at 0 we have $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) = \frac{4}{5} < 1$, yet $\int \log|\frac{1}{4}(1 + Y^{2k})| \,\mathrm{d}\mu(\sigma, z) = \frac{1}{5}\log(1 + 2^{2k}) - \log 4 \to \infty$ as $k \to \infty$. We conclude that the set of exponentially bounded polynomials at radius 1 is not convex. A similar argument works for all radii and number fields.

Lemma 3.9.5. *Let $D \subseteq \mathbb{C}$ be a convex subset and let $f\colon D \to \mathbb{C}$ be analytic. Then for distinct $x, y \in D$ we have*

$$\left|\frac{f(x) - f(y)}{x - y}\right| \leq \sup_{z \in D} |f'(z)|.$$

Proof. Let $\gamma\colon [0,1] \to D$ be the parametrization of the straight line connecting x and y, which is well-defined since D is convex. First note that

$$\begin{aligned}\int_0^1 f'(\gamma(t)) \,\mathrm{d}t &= \int_0^1 f'(tx + (1-t)y) \,\mathrm{d}t \\ &= \frac{1}{x - y}\Big[f(tx + (1-t)y)\Big]_{t=0}^{1} \\ &= \frac{f(x) - f(y)}{x - y}.\end{aligned}$$

Then

$$\begin{aligned}\left|\frac{f(x) - f(y)}{x - y}\right| = \left|\int_0^1 f'(\gamma(t)) \,\mathrm{d}t\right| &\leq \int_0^1 \big|f'(\gamma(t))\big| \,\mathrm{d}t \\ &\leq \int_0^1 \big(\sup_{z \in D} |f'(z)|\big) \,\mathrm{d}t = \sup_{z \in D} |f'(z)|,\end{aligned}$$

as was to be shown. □

We will now translate the measure theoretic property of Definition 3.9.2 to an analytic one. Our results in the coming sections only depend on the 'if' part of the following equivalence.

Theorem 3.9.6. *Let K be a number field, $0 < r < 1$ and $f \in K_{\mathbb{R}}[Y]$. Then f is exponentially bounded at radius r if and only if there exists an $a \in \mathbb{R}_{>0}$ such that for all $\sigma \in \mathrm{X}(K)$ and $z \in \mathbb{C}$ we have*

$$|\sigma(f)(z)| \leq \exp(a(|z|^2 - r^2)).$$

Proof. ($\Leftarrow$) Suppose such a exists. Let $\mu \in \mathcal{M}(K)$ such that

$$\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < r^2.$$

Then

$$\int \log|\sigma(f)(z)| \,\mathrm{d}\mu(\sigma, z) \leq \int a(|z|^2 - r^2) \,\mathrm{d}\mu(\sigma, z) < ar^2 - ar^2 = 0,$$

so f is exponentially bounded at radius r.

($\Rightarrow$) Let $D_0 = \{z \in \mathbb{C} \,|\, |z| < r\}$ and $D_\infty = \{z \in \mathbb{C} \,|\, |z| > r\}$. For $c \in \{0, \infty\}$ let

$$A_c = \big\{a \in \mathbb{R} \,\big|\, (\forall\, \rho \in \mathrm{X}(K))\, (\forall\, z \in D_c)\ |\rho(f)(z)| \leq \exp(a(|z|^2 - r^2))\big\}.$$

Firstly, we show that A_0 is non-empty. Let $\rho \in \mathrm{X}(K)$ and $z_0 \in D_0$, and let $\mu \in \mathcal{M}(K)$ be the measure with weight 1 at (ρ, z_0). Then $\int |x|^2 \,\mathrm{d}\mu(\sigma, x) = |z_0|^2 < r^2$, so by exponential boundedness

$$|\rho(f)(z_0)| = \exp\Big(\int \log|\sigma(f)(x)| \,\mathrm{d}\mu(\sigma, x)\Big) < 1.$$

It follows that $0 \in A_0$, and even $(-\infty, 0] \subseteq A_0$. This argument also shows that $\rho(f)$ is bounded by 1 on the boundary of D_0, the circle of radius r.

Secondly, we show that A_∞ is non-empty. Since $\exp(|z|^2 - r^2)$ grows faster than any polynomial, there exists some $b > r$ such that $|\rho(f)(z)| \leq \exp(|z|^2 - r^2)$ for all $|z| \geq b$. Write $B = \{z \in \mathbb{C} \,|\, |z| \leq b\}$. Let $\rho \in \mathrm{X}(K)$ and $z \in B \cap D_\infty$, and write $g = \rho(f)$ and $\theta = z/|z|$. As remarked at the end of the previous paragraph we have $|g(r\theta)| \leq 1$, so that

$$\begin{aligned}
\log|g(z)| &\leq \log(1 + |g(z) - g(r\theta)|) \\
&\leq |g(z) - g(r\theta)| \\
&= \frac{|z|^2 - r^2}{|z| + r} \cdot \left|\frac{g(z) - g(r\theta)}{z - r\theta}\right| \\
&\overset{*}{\leq} (|z|^2 - r^2) \cdot \frac{\sup_{x \in B} |g'(x)|}{2r} \\
&\leq a(|z|^2 - r^2),
\end{aligned}$$

where $*$ follows from Lemma 3.9.5 and a is the maximum of 1 and all $(2r)^{-1} \sup_{x \in B} |\rho(f)'(x)|$ for $\rho \in \mathrm{X}(K)$. Thus $a \in A_\infty$.

Thirdly, we show that $A_0 \cap A_\infty$ is non-empty. Suppose for the sake of contradiction that $A_0 \cap A_\infty$ is empty. Clearly A_0 and A_∞ are closed.

Hence there exist reals that are neither in A_0 nor A_∞, and let a be such a real number. It follows that $a > 0$. In turn, there exist $z_0 \in D_0$ and $z_\infty \in D_\infty$ with $\rho_0, \rho_\infty \in \mathrm{X}(K)$ such that $|\rho_0(f)(z_0)| > \exp(a(|z_0|^2 - r^2))$ and $|\rho_\infty(f)(z_\infty)| > \exp(a(|z_\infty|^2 - r^2))$. Choose some $t \in (0,1)$ such that $(1-t)|z_0|^2 + t|z_\infty|^2 < r^2$ and let μ be the measure that assigns weight $1-t$ to (ρ_0, z_0) and weight t to (ρ_∞, z_∞). Then $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < r^2$ and thus

$$0 > \int \log|\sigma(f)(z)| \,\mathrm{d}\mu(\sigma, z) = (1-t)\log|\rho_0(f)(z_0)| + t\log|\rho_\infty(f)(z_\infty)|.$$

Taking the limit of t up to $s \in \mathbb{R}$ such that $(1-s)|z_0|^2 + s|z_\infty|^2 = r^2$ we get

$$\begin{aligned} 0 &\geq (1-s)\log|\rho_0(f)(z_0)| + s\log|\rho_\infty(f)(z_\infty)| \\ &> a((1-s)|z_0|^2 + s|z_\infty|^2 - r^2) = 0, \end{aligned}$$

a contradiction. Hence $A_0 \cap A_\infty$ is non-empty, as was to be shown.

Note that $D_0 \cup D_\infty$ is dense in $\mathbb{C}$, so any positive $a \in A_0 \cap A_\infty$ gives the inequality we set out to prove. Suppose $a \in A_0 \cap A_\infty$ is such that $a \leq 0$. Thus $|\rho(f)(z)| \leq \exp(a(|z|^2 - r^2)) \leq 1$ for all $z \in D_\infty$ and $\rho \in \mathrm{X}(K)$, so $\rho(f)$ is a constant function. However, as $|\rho(f)(z)| < 1$ for $z \in D_0$ as shown before, this constant is strictly less than 1. Let $c \in (0,1)$ be a constant that bounds $\rho(f)$ for all $\rho \in \mathrm{X}(K)$. Then $-r^{-2}\log c \in A_0 \cap A_\infty$ is positive. Hence $A_0 \cap A_\infty$ always contains a positive element. □

3.10 Volume computation

The next step is to compute the volume of a symmetric convex set of exponentially bounded polynomials. As in Lemma 3.8.5 it suffices for the sake of volume computation to consider the case where the radius is 1 and the base field is $\mathbb{R}$. In view of Theorem 3.9.6, we consider the unit-ball of the following norm.

Definition 3.10.1. Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{C}$. We equip $\mathbb{F}[Y]$ with the *exp-norm*

$$\|f\|_{\mathrm{e}} = \max_{z \in \mathbb{C}} \frac{|f(z)|}{\exp(|z|^2)},$$

not to be confused with $\|-\|_p$ for $p = \mathrm{e}$ from Definition 2.2.11.

Lemma 3.10.2. *Consider the map* $\phi\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ *given by*

$$\phi(n) = \begin{cases} \left(\frac{n}{2}\right)! & \text{if } n \text{ is even} \\ \left(\frac{n-1}{2}\right)! \cdot \sqrt{\frac{n+1}{2}} & \text{if } n \text{ is odd} \end{cases}.$$

Then we have

$$\log\Big(\prod_{k=0}^{n}\phi(k)\Big) = \tfrac{1}{4}n^2\log n - (\tfrac{3}{8}+\tfrac{1}{4}\log 2)n^2 + O(n\log n)$$

and for all $x \in \mathbb{R}_{\geq 0}$ *and* $m \in \mathbb{Z}_{\geq 0}$ *we have*

$$\frac{x^{2m+1}}{\phi(2m+1)} \leq \frac{1}{2}\bigg(\frac{x^{2m}}{\phi(2m)} + \frac{x^{2m+2}}{\phi(2m+1)}\bigg).$$

Proof. Writing out the product we have

$$\begin{aligned}\prod_{k=0}^{n}\phi(k) &= \bigg(\prod_{m=0}^{\lfloor n/2\rfloor}\phi(2m)\bigg)\bigg(\prod_{m=0}^{\lfloor (n-1)/2\rfloor}\phi(2m+1)\bigg)\\ &= \bigg(\prod_{m=0}^{\lfloor n/2\rfloor} m!\bigg)\bigg(\prod_{m=0}^{\lfloor (n-1)/2\rfloor} m!\bigg)\bigg(\prod_{m=0}^{\lfloor (n-1)/2\rfloor}\sqrt{m+1}\bigg).\end{aligned}$$

We then apply Proposition 3.7.3 to compute

$$\begin{aligned}\log\Big(\prod_{k=0}^{n}\phi(k)\Big) &= \lfloor\tfrac{n}{2}\rfloor^2\big(\tfrac{1}{2}\log\lfloor\tfrac{n}{2}\rfloor - \tfrac{3}{4}\big) + \lfloor\tfrac{n-1}{2}\rfloor^2\big(\tfrac{1}{2}\log\lfloor\tfrac{n-1}{2}\rfloor - \tfrac{3}{4}\big)\\ &\quad + \lfloor\tfrac{n-1}{2}\rfloor\big(\log\lfloor\tfrac{n-1}{2}\rfloor - 1\big) + O(n\log n)\\ &= \big(\tfrac{n}{2}\big)^2\big(\tfrac{1}{2}\log\tfrac{n}{2} - \tfrac{3}{4}\big) + \big(\tfrac{n}{2}\big)^2\big(\tfrac{1}{2}\log\tfrac{n}{2} - \tfrac{3}{4}\big) + O(n\log n)\\ &= \tfrac{1}{4}n^2\log n - (\tfrac{3}{8}+\tfrac{1}{4}\log 2)n^2 + O(n\log n),\end{aligned}$$

proving the first part. For the second, let $m \in \mathbb{Z}_{\geq 0}$ and $x \in \mathbb{R}_{\geq 0}$. Then

$$\begin{aligned}\frac{1}{\phi(2m)} + \frac{x^2}{\phi(2m+2)} &= \frac{1}{m!}\Big(\Big(1 - \frac{x}{\sqrt{m+1}}\Big)^2 + \frac{2x}{\sqrt{m+1}}\Big)\\ &\geq \frac{1}{m!}\frac{2x}{\sqrt{m+1}} = 2\cdot\frac{x}{\phi(2m+1)},\end{aligned}$$

from which the second part follows. □

Recall the notation $R[X]_n$ from Definition 3.5.6, the subset of $R[X]$ of polynomials of degree strictly less than n.

Proposition 3.10.3. *Write* $S = \{f \in \mathbb{R}[Y] \mid \|f\|_{\mathrm{e}} \leq 1\}$. *Then for* $n \in \mathbb{Z}_{\geq 0}$ *we have*

$$\log \operatorname{vol}(S \cap \mathbb{R}[Y]_n) \geq -\tfrac{1}{4}n^2\log n + (\tfrac{3}{8}+\tfrac{1}{4}\log 2)n^2 + O(n\log n).$$

Proof. Consider ϕ as in Lemma 3.10.2 and define

$$T = \Big\{ \sum_{i=0}^{\infty} f_i Y^i \in \mathbb{R}[Y] \;\Big|\; (\forall i)\ |f_i| \leq \frac{1}{2\phi(i)} \Big\}.$$

Then for all $f \in T$ and $z \in \mathbb{C}$ we have using Lemma 3.10.2 that

$$\begin{aligned} |f(z)| &\leq \sum_{i=0}^{\infty} |f_i| \cdot |z|^i \leq \sum_{i=0}^{\infty} \frac{|z|^i}{2\phi(i)} \\ &= \frac{1}{2}\left[\sum_{k=0}^{\infty} \frac{|z|^{2k}}{k!} + \sum_{k=0}^{\infty} \frac{|z|^{2k+1}}{\phi(2k+1)} \right] \\ &\leq \frac{1}{2}\left[\sum_{k=0}^{\infty} \frac{|z|^{2k}}{k!} + \sum_{k=0}^{\infty} \frac{1}{2}\left(\frac{|z|^{2k}}{k!} + \frac{|z|^{2k+2}}{(k+1)!} \right) \right] \\ &\leq \sum_{k=0}^{\infty} \frac{|z|^{2k}}{k!} = \exp|z^2|, \end{aligned}$$

so $f \in S$ and $T \subseteq S$. Then by Lemma 3.10.2 we have

$$\begin{aligned} \log \mathrm{vol}(T \cap \mathbb{R}[Y]_n) &= -n\log 2 - \log\Big(\prod_{k=0}^{n-1} \phi(k) \Big) \\ &= -\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2 + O(n \log n), \end{aligned}$$

from which the proposition follows. □

Proposition 3.10.3 is sufficient for our purposes. It may interest a reader that the lower bound of Proposition 3.10.3 is actually an equality, which we will show in the remainder of this section.

Theorem 3.10.4 (Brunn–Minkowski inequality, Theorem 4.1 in [16])**.** *Let $n \in \mathbb{Z}_{\geq 1}$ and let $A, B \subseteq \mathbb{R}^n$ be bounded non-empty measurable sets. Then for all $t \in [0,1]$ such that*

$$(1-t)A + tB = \{(1-t)a + tb \,|\, a \in A,\, b \in B\}$$

is measurable we have the inequality

$$\mathrm{vol}((1-t)A + tB)^{1/n} \geq (1-t)\mathrm{vol}(A)^{1/n} + t\mathrm{vol}(B)^{1/n}. \quad \square$$

We will only apply this theorem to compact subsets of $\mathbb{R}^n$, which are indeed measurable and bounded. Moreover, for $A, B \subseteq \mathbb{R}^n$ compact and $t \in (0,1)$ also the set $(1-t)A + tB$ is compact, hence measurable.

Corollary 3.10.5. *Let $n \in \mathbb{Z}_{\geq 0}$, let $V \subseteq \mathbb{R}^n$ be a subspace and let $S \subseteq \mathbb{R}^n$ be a symmetric convex body. Then the map that sends $x \in \mathbb{R}^n$ to $\mathrm{vol}_V(V \cap (S - x))$ takes a maximum at 0.*

Proof. Let $x \in \mathbb{R}^n$ and write $m = \dim V$ and $H_x = V \cap (S - x)$. If $m = 0$ the corollary holds trivially, so suppose $m > 0$. Note that $H_{-x} = -H_x$ since S and V are symmetric. Because S and V are convex we have $\frac{1}{2}H_x + \frac{1}{2}H_{-x} \subseteq H_0$. Hence by Theorem 3.10.4 we have

$$\begin{aligned}\mathrm{vol}(H_0)^{1/m} &\geq \mathrm{vol}(\tfrac{1}{2}H_x + \tfrac{1}{2}H_{-x})^{1/m} \\ &\geq \tfrac{1}{2}\mathrm{vol}(H_x)^{1/m} + \tfrac{1}{2}\mathrm{vol}(H_{-x})^{1/m} \\ &= \mathrm{vol}(H_x)^{1/m},\end{aligned}$$

from which the corollary follows. □

Recall the definition of $\oplus$ from Definition 2.5.1.

Corollary 3.10.6. *Let $n \in \mathbb{Z}_{\geq 0}$, let $U, V \subseteq \mathbb{R}^n$ be subspaces such that $U \oplus V = \mathbb{R}^n$ and write π for the projection $U \oplus V \to U$. If $S \subseteq \mathbb{R}^n$ is a symmetric convex body, then $\mathrm{vol}_{\mathbb{R}^n}(S) \leq \mathrm{vol}_U(\pi S) \cdot \mathrm{vol}_V(S \cap V)$.*

Proof. By Corollary 3.10.5 we have

$$\begin{aligned}\mathrm{vol}(S) &= \int_{\pi S} \mathrm{vol}_V(V \cap (S - x))\,\mathrm{d}x \\ &\leq \int_{\pi S} \mathrm{vol}_V(V \cap S)\,\mathrm{d}x \\ &= \mathrm{vol}_U(\pi S) \cdot \mathrm{vol}_V(V \cap S).\end{aligned}$$

□

Theorem 3.10.7. *Write $S = \{f \in \mathbb{R}[Y] \mid \|f\|_{\mathrm{e}} \leq 1\}$. Then for $n \in \mathbb{Z}_{\geq 0}$ we have*

$$\log \mathrm{vol}(S \cap \mathbb{R}[Y]_n) = -\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2 + O(n \log n).$$

Proof. We already proved a lower bound in Proposition 3.10.3, so it remains to prove an upper bound. We will inductively show that

$$\mathrm{vol}(S \cap \mathbb{R}[Y]_n) \leq 2^n \prod_{k=1}^{n-1} \Big(\frac{2\mathrm{e}}{k}\Big)^{k/2}.$$

It then follows from Proposition 3.7.3 that

$$\begin{aligned}\log \mathrm{vol}(S \cap \mathbb{R}[Y]_n) &\leq n \log 2 + \frac{1}{2}\sum_{k=1}^{n-1} k\big(\log(2\mathrm{e}) - \log k\big) \\ &= -\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2 + O(n \log n).\end{aligned}$$

For $n = 0$ and $n = 1$ the inequality certainly holds. Now suppose the inequality holds for $n \geq 1$. Write $\mathbb{R}[Y]_{n+1} = (\mathbb{R}Y^n) \oplus \mathbb{R}[Y]_n$ and let $\pi\colon \mathbb{R}[Y]_{n+1} \to \mathbb{R}Y^n$ be the projection map. By Corollary 3.10.6 it suffices to show for $n > 0$ that $\mathrm{vol}(\pi(S \cap \mathbb{R}[Y]_{n+1})) \leq 2(\frac{n}{2\mathrm{e}})^{-n/2}$. We do this by proving

$$\pi(S \cap \mathbb{R}[Y]_{n+1}) \overset{\text{(i)}}{\subseteq} S \cap (\mathbb{R}Y^n) \overset{\text{(ii)}}{\subseteq} [-1, +1]\Big(\frac{2\mathrm{e}}{n}\Big)^{n/2} Y^n.$$

(i) Suppose $f \in \mathbb{R}[Y]_{n+1}$ and $\|f\|_{\mathrm{e}} < \|\pi(f)\|_{\mathrm{e}}$. Since $\pi(f)$ is a monomial, the function $z \mapsto |\pi(f)(z)| \exp(-|z|^2)$ takes its maximum on a circle of radius say r. Then for all z on this circle we have

$$|f(z)| \leq \|f\|_{\mathrm{e}} \exp(r^2) < \|\pi(f)\|_{\mathrm{e}} \exp(r^2) = |\pi(f)(z)|.$$

Hence by Rouché's theorem (Theorem 4.18 in [1]), the polynomial $f - \pi(f)$ has as many roots as $\pi(f)$ in the disk $\{z \in \mathbb{C} \,|\, |z| \leq r\}$, counting multiplicities. However, since $f - \pi(f)$ has degree at most $n - 1$ and $\pi(f)$ has n such roots, this is a contradiction. Hence $\|\pi(f)\|_{\mathrm{e}} \leq \|f\|_{\mathrm{e}}$, from which (i) follows.

(ii) Consider the map $g\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by $x \mapsto x^n \exp(-x^2)$. Then

$$\frac{\mathrm{d}g}{\mathrm{d}x} = x^{n-1}(n - 2x^2)\exp(-x^2) = 0 \iff x = 0 \ \vee \ x = \sqrt{n/2}.$$

Hence g takes a maximum at $(n/2)^{1/2}$, so we conclude that $\|Y^n\|_{\mathrm{e}} = g((n/2)^{1/2}) = (\frac{n}{2\mathrm{e}})^{n/2}$. Thus $\max\{c \in \mathbb{R} \,|\, cY^n \in S\} = (\frac{2\mathrm{e}}{n})^{n/2}$, as was to be shown.

The theorem now follows by induction. □

3.11 Proof of the main theorem

We are now ready to give a proof of Theorem 3.11.2.

Proposition 3.11.1. *Let R be an order of a number field K, let $\alpha \in K$ and $0 < r^2 < \frac{1}{2}\exp(\frac{1}{2})$. Then there exists some non-zero $f \in R[X]$ such that $f(X - \alpha)$ is exponentially bounded at radius r.*

Proof. Let $n \in \mathbb{Z}_{\geq 1}$ and $d = [K : \mathbb{Q}]$. Write $Y = X - \alpha$ and consider the real vector space $K_{\mathbb{R}}[Y]_n$, which we equip with an inner product as in Definition 3.8.2 with respect to the variable Y. By Theorem 3.5.5 and Lemma 3.8.4 the lattice $R[X]_n$ in $K_{\mathbb{R}}[Y]_n$ is full rank and has determinant $\det(R[Y]_n) = |\det(R)|^n = |\Delta(R)|^{n/2}$. For $b \in \mathbb{R}_{\geq 0}$ consider

$$\begin{aligned} S_n &= \{f \in K_{\mathbb{R}}[Y]_n \,|\, (\forall\, \sigma \in \mathrm{X}(K),\, z \in \mathbb{C})\ |\sigma(f)(z)| \leq \exp(bn(|z|^2 - r^2))\} \\ &= \{f \in K_{\mathbb{R}}[Y]_n \,|\, (\forall\, \sigma \in \mathrm{X}(K))\ \|\exp(bnr^2)\sigma(f)((bn)^{-1/2}Y)\|_{\mathrm{e}} \leq 1\}. \end{aligned}$$

We have a natural orthogonal decomposition $K_{\mathbb{R}} \cong \mathbb{R}^u \times \mathbb{C}^v$ for some $u, v \in \mathbb{Z}_{\geq 0}$ which in turn gives an orthogonal decomposition $K_{\mathbb{R}}[Y]_n = (\mathbb{R}[Y]_n)^u \times (\mathbb{C}[Y]_n)^v$. Note that S_n is simply a product over $\sigma \in \mathrm{X}(K)$ of

$$S_n(\sigma) = \{f \in \mathbb{F}[Y]_n \mid \| \exp(bnr^2) \cdot \sigma(f)((bn)^{-1/2} \cdot Y)\|_{\mathrm{e}} \leq 1\}$$

where $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$ depending on whether $\sigma(K) \subseteq \mathbb{R}$. Then using Lemma 3.8.4 and Proposition 3.10.3 we compute

$$\begin{aligned}\log \mathrm{vol}(S_n) &\geq d\Big(\big(-\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2\big) + \big(\tfrac{1}{4}n^2 \log(bn) - bn^2r^2\big)\Big) \\ &\quad + O(n \log n) \\ &= dn^2 \cdot \varepsilon(b) + O(n \log n),\end{aligned}$$

with $\varepsilon(b) = \frac{1}{4}\log(2b) + \frac{3}{8} - r^2 b$. Choosing $b = (2r)^{-2}$ we get $\varepsilon(b) = \frac{1}{4}(\frac{1}{2} - \log(2r^2)) > 0$. Hence

$$\log\Big(\frac{\mathrm{vol}(S_n)}{2^{dn} \cdot |\Delta(R)|^{n/2}}\Big) \geq dn^2 \cdot \varepsilon(b) + O(n \log n) \to \infty \quad (\text{as } n \to \infty).$$

Thus by Minkowski's theorem there exists for n sufficiently large some non-zero $g \in S_n \cap R[X]$. Because $g \in S_n$, this polynomial is exponentially bounded at radius r by Theorem 3.9.6. □

Theorem 3.11.2. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r < \sqrt[4]{\mathrm{e}/4}$, then there exist only finitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$.*

Proof. Let $\gamma = \alpha/2$, let $K = \mathbb{Q}(\gamma)$ and let R be some order in K. Choose $r \in \mathbb{R}_{>0}$ such that $\|\gamma\| < r < \sqrt[4]{\mathrm{e}/4}$. Then by Proposition 3.11.1 there exists some non-zero polynomial $f \in R[X]$ which as polynomial in $Y = X - \gamma$ is exponentially bounded at radius r. Hence by Proposition 3.9.3 all $(\beta, \alpha - \beta) \in \mathrm{dec}(\alpha)$ satisfy $f(\beta) = 0$. As f has only finitely many roots, the theorem follows. □

From the proof of Theorem 3.11.2 one easily derives the following result.

Proposition 3.11.3. *There exists an algorithm that, given some $r \in \mathbb{R} \cap \overline{\mathbb{Q}}$ and $\alpha \in \overline{\mathbb{Q}}$, decides whether $r < \sqrt[4]{\mathrm{e}/4}$ and if so computes all $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| \leq r$, each represented by their minimal polynomial over $\mathbb{Q}(\alpha)$.*

Proof. Clearly $r \neq \sqrt[4]{\mathrm{e}/4}$ as the latter is not algebraic. However, both are computable, and after finitely many steps of approximation we can decide whether $r < \sqrt[4]{\mathrm{e}/4}$. We have an explicit formula for a lower bound on the volume of the set S as defined in the proof of Proposition 3.10.3. So moreover

we can compute a sufficiently large n such that Minkowski's theorem, as in the proof of Proposition 3.11.1, guarantees the existence of a non-zero lattice point in S. We may then simply enumerate all lattice points to eventually find a polynomial f as in Proposition 3.11.1. We determine using [31] the monic irreducible factors of f and decide which factors g have a root β satisfying $\|\alpha - \beta\| \leq r$. □

Corollary 3.11.4. *There is an algorithm that takes as input an element $\alpha \in \overline{\mathbb{Z}}$ given by its minimal polynomial, and decides whether $\|\alpha\| < \sqrt[4]{4\mathrm{e}}$ and if so, computes all non-trivial $(\beta, \gamma) \in \mathrm{dec}(\alpha)$, each represented by the minimal polynomial of β over $\mathbb{Q}(\alpha)$.*

Proof. We apply Proposition 3.11.3 with $\alpha/2$ in the place of α and $\|\alpha/2\|$ in the place of r. By Lemma 2.4.3 each β found gives a decomposition $(\beta, \alpha - \beta)$. Note that we can filter out the trivial decompositions. □

3.12 Remarks on the proof of the main theorem

In this section we briefly discuss the proof of Theorem 3.11.2 and make some practical remarks for explicit computation.

The proof of Theorem 3.11.2 proceeds in the following steps:

1. We determine a sufficient condition for a polynomial to have all lattice points close to α as roots.
2. We translate this condition into an analytic one.
3. We determine the volume of a symmetric convex set of polynomials satisfying this condition.
4. We apply Minkowski's convex body theorem to find integral polynomials in this set.

Theorem 3.9.6 suggests that step (2) can hardly be improved upon. By Theorem 3.10.7 we correctly computed the volume of our symmetric convex set in step (3). However, in order to make it convex we fixed the constant a that comes out of Theorem 3.9.6. It is easy to verify that we indeed made an optimal choice of a in Proposition 3.11.1, although that does not guarantee we chose the best convex subset. If the weakest link in the proof is step (4), we likely require a completely different approach. It should be noted however that Minkowski's convex body theorem is powerful enough to prove the classical Theorem 3.8.6.

One could also ask for stronger results in the case we are only interested in decompositions of lattice points, i.e. when $\alpha \in \frac{1}{2}\overline{\mathbb{Z}}$. A piece of information we can exploit is the following symmetry: For all $\alpha \in \overline{\mathbb{Z}}$ we have an involution $x \mapsto \alpha - x$ on $\overline{\mathbb{Z}}$ which induces action on $\mathrm{dec}(\alpha)$, given by $(\beta, \gamma) \mapsto (\gamma, \beta)$.

Lemma 3.12.1. *Let $\alpha \in \overline{\mathbb{Z}}$ and let $\mathbb{Z}[\alpha] \subseteq R$ be an order of $\mathbb{Q}(\alpha)$. For all $f \in R[X]$ such that $f(\beta) = 0$ for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$, also $g = f(\alpha - X) \in R[X]$ satisfies $g(\beta) = 0$ for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$.* □

Lemma 3.12.1 turns the involution on $\overline{\mathbb{Z}}$ into an R-algebra automorphism on $R[X]$. We can incorporate this automorphism in our proof of Theorem 3.11.2.

Proposition 3.12.2. *Let $\alpha \in \overline{\mathbb{Z}}$, let $\mathbb{Z}[\alpha] \subseteq R$ be an order of $K = \mathbb{Q}(\alpha)$ and let $r \in \mathbb{R}_{>0}$. For all $f \in R[X]$ such that f as a polynomial in $Y = X - \alpha/2$ is exponentially bounded at radius r, so is $f(X) \cdot f(\alpha - X) \in K[Y^2]$.*

Proof. Note that the involution $X \mapsto \alpha - X$ is with respect to Y given by $Y \mapsto -Y$. Hence if f as a polynomial in Y is exponentially bounded at radius r, then so is $f(\alpha - X)$. As noted in Example 3.9.4, the set of polynomials exponentially bounded at r is closed under multiplication. Hence $g = f(X) \cdot f(\alpha - X)$ is exponentially bounded at radius r. Now g is invariant under $Y \mapsto -Y$, meaning all coefficients at odd degree monomials in Y are zero, i.e. $g \in K[Y^2]$. □

An interesting question to ask is how dissimilar f and $f(\alpha - X)$ can be for exponentially bounded f. Certainly both should have β as root for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ by Lemma 3.12.1. In the context of finding 'small' f algorithmically it seems that often f and $f(\alpha - X)$ are the same (up to sign).

As a consequence of Proposition 3.12.2, when proving a specialization of Theorem 3.11.2 to $\alpha \in \frac{1}{2}\overline{\mathbb{Z}}$ we may look at the lattice $R[X(\alpha - X)]$ in $K_{\mathbb{R}}[Y^2]$ instead of $R[X]$ in $K_{\mathbb{R}}[Y]$. The effect is two-fold. Firstly, it simplifies the volume computation of Proposition 3.10.3, as we no longer require the ad-hoc function ϕ from Lemma 3.10.2. Secondly, any integral polynomial in our symmetric body can be found in a lower dimensional lattice in Proposition 3.11.1. This follows from the suggested changes to Proposition 3.10.3, but can heuristically be seen as follows. If f is a solution in the original lattice $R[X]$, then $f(X) \cdot f(\alpha - X)$ is a solution in our new lattice $R[X(\alpha - X)]$ at the same dimension. However, as discussed before, f is likely to be an element of $R[X(\alpha - X)]$ anyway, and if so we would have found f at half the dimension in $R[X(\alpha - X)]$. Neither of these changes have an effect on the quality of our theoretical results. However, when we want to compute decompositions in practice, the latter 'dimension reduction' is very useful.

3.13 Computational example

We will now work out an example proving an algebraic integer α is indecomposable.

Showing that α is indecomposable will be trivial when $\|\alpha\| \leq \sqrt{2}$ as we have seen in Proposition 3.3.1, so we will choose α such that $\|\alpha\| > \sqrt{2} \approx 1.414$. On the other hand, the algorithm from Proposition 3.11.3 terminates faster the smaller $\|\alpha\|$ is, so for this example we will consider $\alpha = \sqrt[3]{3}$ with $\|\alpha\| = 3^{1/3} \approx 1.442$.

Setup. Let $\alpha = \sqrt[3]{3}$ and let $r^2 = 6/11$, so that $\|\alpha/2\| < r < \sqrt[4]{\mathrm{e}/4}$. Write $K = \mathbb{Q}(\alpha)$ and $R = \mathbb{Z}[\alpha]$ and consider the ring $R[X]$. Writing $Y = X - \alpha/2$, we are looking for a polynomial $f \in R[X]$ such that f as polynomial in Y is exponentially bounded at radius r. However, writing $Z = X(\alpha - X)$ we may instead look for such a polynomial in $R[Z]$, as follows from Lemma 3.12.1.

Finding a polynomial. It is quite involved to systematically find short vectors in a lattice. Instead we will employ a more ad-hoc approach, more along the lines of Theorem 3.6.6. We guess that our polynomial f will be monic in Z of some degree n. We start with Z^n and then greedily subtract $\mathbb{Z}[\alpha]$-multiples of lower degree powers of Z such that the resulting polynomial in Y becomes 'small', i.e. has small coefficients under every embedding $K \to \mathbb{C}$ with lower degree terms weighing more heavily. Effectively, we are applying a rounding function in the sense of Definition 3.6.3. Note that $Z = -Y^2 + \alpha^2/4$. Similarly as in the proof of Theorem 3.6.6, taking $n = 4$ the Y^6 term becomes integral, which is useful. Thus we will try $n = 4$. We compute:

$$\begin{array}{rrrcllll}
Z^4 & & & = & Y^8 & -\alpha^2 Y^6 & +\frac{9}{8}\alpha Y^4 & -\frac{9}{16}Y^2 & +\frac{9}{256}\alpha^2 \\
 & \alpha^2 Z^3 & & = & & -\alpha^2 Y^6 & +\frac{9}{4}\alpha Y^4 & -\frac{27}{16}Y^2 & +\frac{9}{64}\alpha^2 \\
\hline
Z^4 & -\alpha^2 Z^3 & & = & Y^8 & & -\frac{9}{8}\alpha Y^4 & +\frac{9}{8}Y^2 & -\frac{27}{256}\alpha^2 \\
 & & -\alpha Z^2 & = & & & -\alpha Y^4 & +\frac{3}{2}Y^2 & -\frac{3}{16}\alpha^2 \\
\hline
Z^4 & -\alpha^2 Z^3 & +\alpha Z^2 & = & Y^8 & & -\frac{1}{8}\alpha Y^4 & -\frac{3}{8}Y^2 & +\frac{21}{256}\alpha^2
\end{array}$$

The remaining coefficients with respect to Y look pretty small in every embedding $K \to \mathbb{C}$, so we guess

$$f(Y) = Y^8 - \tfrac{1}{8}\alpha Y^4 - \tfrac{3}{8}Y^2 + \tfrac{21}{256}\alpha^2 = Z^4 - \alpha^2 Z^3 + \alpha Z^2 \in R[Z].$$

is going to be exponentially bounded at radius r as polynomial in Y.

Proving exponentially boundedness. If we take $b\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by

$$b(w) = w^4 + \tfrac{1}{8} \cdot 3^{1/3} \cdot w^2 + \tfrac{3}{8} \cdot w + \tfrac{21}{256} \cdot 3^{2/3},$$

then for all $\sigma \in \mathrm{X}(K)$ and $z \in \mathbb{C}$ we have $|\sigma(f)(z)| \leq b(|z|^2)$. To prove that f is exponentially bounded at radius r it suffices to find $a \in \mathbb{R}$ such that $b(w) \leq \exp(a(w - r^2))$ for all $w \in \mathbb{R}_{\geq 0}$. Because $b(0) = \frac{21}{256}3^{2/3}$, we must have $a \leq -\log(b(0))/r^2 \approx 3.4$. We will try $a = 3$ for simplicity. Consider the function $B(w) = b(w) \cdot \exp(-a(w - r^2))$, for which we want to show $B(w) \leq 1$ for all w. Then

$$0 = B'(w) = \exp(-a(w - r^2))(b'(w) - ab(w))$$

if and only if $ab(w) - b'(w) = 0$. Since the latter is simply a polynomial equation we will find using standard techniques that it has no positive real roots. We compute:

$$\begin{aligned} ab(w) - b'(w) &= 3w^4 - 4w^3 + \tfrac{3}{8}3^{1/3}w^2 + (\tfrac{9}{8} - \tfrac{1}{4}3^{1/3})w + (\tfrac{63}{256}3^{2/3} - \tfrac{3}{8}) \\ &> 3w^4 - 4w^3 + \tfrac{3}{5}w^2 + \tfrac{3}{4}w + \tfrac{1}{4}. \end{aligned}$$

For $1 \leq w$ we get $ab(w) - b'(w) > 3w^4 - 4w^3 + \frac{3}{2} = w^2(3^{1/2}w - 2 \cdot 3^{-1/2})^2 + (\frac{3}{2} - \frac{4}{3}w^2) \geq 0$ and for $0 < w \leq 1$ we get $ab(w) - b'(w) > 3w^4 - 4w^3 + \frac{3}{2}w^2 = 3w^2(w^2 - \frac{4}{3}w + \frac{1}{2}) \geq 3w^2(w - 2^{-1/2})^2 \geq 0$. Hence B has no local maxima besides possibly at 0, and because $B(w) \to 0$ as $w \to \infty$ we conclude that B takes a maximum at 0. Therefore b is bounded by $w \mapsto \exp(a(w - r^2))$ and thus f is exponentially bounded at radius r.

Finding decompositions. Writing f as a polynomial in X we get

$$\begin{aligned} f &= X^8 - 4\alpha X^7 + 7\alpha^2 X^6 - 21X^5 + 13\alpha X^4 - 5\alpha^2 X^3 + 3X^2 \\ &= X^2 \cdot (\alpha - X)^2 \cdot (X^4 - 2\alpha X^3 + 2\alpha^2 X^2 - 3X + \alpha). \end{aligned}$$

By Proposition 3.9.3 all decompositions of α can be found among the roots of f. The factors X and $\alpha - X$ correspond to the trivial decompositions $(0, \alpha)$ and $(\alpha, 0)$ of α. The polynomial $h = X^4 - 2\alpha X^3 + 2\alpha^2 X^2 - 3X + \alpha$ is irreducible as it is Eisenstein at the prime (α). Let $\beta \in \overline{\mathbb{Z}}$ be a root of h. By Lemma 3.2.8 we have $\|\beta\| \geq N(\beta) = N(h(0)) = 3^{1/3} = \|\alpha\|$. We can only have $\|\beta\|^2 + \|\alpha - \beta\|^2 \leq \|\alpha\|^2$ if $\|\alpha - \beta\| = 0$, i.e. $\alpha = \beta$, which is impossible. Hence α is indecomposable by Lemma 2.4.3.

3.14 Enumeration of degree-3 indecomposables

In this section we discuss our attempt to compute the indecomposable algebraic integers of degree 3 and derive Theorem 3.14.1. We will refer to tables of computational results, which can be found in the appendix, and are obtained by a computer program [19] written in Sage [41].

We will write $f_\alpha \in \mathbb{Z}[x]$ for the minimal polynomial of $\alpha \in \overline{\mathbb{Z}}$. We will consider α up to 'trivial isometries' of $\overline{\mathbb{Z}}$, namely those of $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ as in Lemma 3.2.13. Using Proposition 3.7.1 we compute a set of 5525 polynomials among which we can find all minimal polynomials of the indecomposable algebraic integers of degree 3. Among those 5525 polynomials f only 700 are in fact irreducible with $q(\alpha) \leq 4$ for all roots α of f. We already eliminated the Galois action by considering minimal polynomials instead of elements, and by choosing only one element of each μ_∞-orbit $\{f, -f(-x)\}$ we eliminate the action of μ_∞, and end up with 'only' 350 polynomials to check. Of those 350, there are 27 polynomials f_α such that $q(\alpha) < 2$, so that α is indecomposable by Proposition 3.3.1.

Small degree decompositions. For 95 polynomials f, the roots α of f have a non-trivial decomposition in the ring of integers of $\mathbb{Q}(\alpha)$. For 116 of the remaining polynomials f_α we can find a non-trivial decomposition $(\beta, \alpha - \beta)$ of α with β in the ring of integers of a degree 2 extension of $\mathbb{Q}(\alpha)$. Of those 116 there are 84 for which the minimal polynomial g_β of β over $\mathbb{Q}(\alpha)$ is of the form $x^2 - \alpha x \pm 1$, a polynomial we encountered in the proof of Lemma 3.4.2. The remaining 32 polynomials and corresponding decompositions can be found in Table 1. We are now left with 112 polynomials to check.

Large degree decompositions. To find decompositions in higher degree extensions we implemented a lattice algorithm. Since we are interested in finding only one decomposition instead of all of them, and since verifying whether something is a decomposition is computationally easy, we can get away with a lot of heuristics. For $(\beta, \alpha - \beta) \in \mathrm{dec}(\alpha)$ we have, on average of squares over all embeddings of $\mathbb{Q}(\alpha, \beta)$ in $\mathbb{C}$, that $|\beta - \alpha/2| \leq \sqrt{q(\alpha/2)} = r$ by Lemma 2.4.3. Hence if we write $g_\beta = \sum_i c_i (x - \alpha/2)^i$ we have that $\sum_i |c_i| r^i$ should be small. It is useful for our lattice algorithm to instead consider the 2-norm $(\sum_i r^i \sum_\sigma |\sigma(c_i)|^2)^{1/2}$ and hope this does not affect the quality of our results for the worse. We enumerate small polynomials $\varepsilon \in \mathbb{Q}(\alpha)[x]$ of degree less than $d \in \mathbb{Z}_{>0}$ such that $(x - \alpha/2)^d - x^d + \varepsilon$ is in the lattice of integral polynomials, and thus $(x - \alpha/2)^d + \varepsilon$ is monic, integral and small. We then verify for each of those whether they induce a decomposition of α. The 41 polynomials f_α for which this method has found a non-trivial decomposition $(\beta, \alpha - \beta)$ of α with g_β of degree greater than 2 are listed in Table 2 together with the polynomial g_β found. This leaves 71 polynomials to check and gives an upper bound of $6 \cdot 98 = 588$ on the number of indecomposable algebraic integers of degree 3.

Indecomposables. On the other hand, we want to prove that certain α are indecomposable. To this end, we implemented a lattice algorithm similar

to that of Proposition 3.11.3. To hopefully speed up the algorithm we also apply the dimension reducing symmetry trick discussed from Lemma 3.12.1. Writing R for the ring of integers of $\mathbb{Q}(\alpha)$ and $z = x(\alpha - x)$, we enumerate short $g \in R[z]$ for which we verify whether g as polynomial in $y = x - \alpha/2$ is exponentially bounded. The 32 polynomials f_α for which we found such a g proving indecomposability of α are listed in Table 3. We present g in factored form for compactness. This leaves 39 polynomials undetermined and gives a lower bound of $6 \cdot 59 = 354$ on the number of indecomposable algebraic integers of degree 3.

Theorem 3.14.1. *There are exactly* 2 *indecomposable algebraic integers of degree* 1*, there are exactly* 14 *of degree* 2*, and there are at least* 354 *and at most* 588 *of degree* 3*.*

Proof. The degree 1 case is obvious: 1 and -1 are the only indecomposable integers. The degree 2 case is Theorem 3.4.3. The bounds for degree 3 are the result of the computation in this section. □

CHAPTER 4

Graded rings

4.1 Introduction

This chapter contains parts of [18] and [35], the authors of which include H.W. Lenstra and A. Silverberg.

Let R be a ring. A *grading* of R is a decomposition $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ of R as a $\mathbb{Z}$-module such that Γ is an abelian group and for all $\gamma, \delta \in \Gamma$ we have $R_\gamma \cdot R_\delta \subseteq R_{\gamma\delta}$. We will refer to Γ as the group of $\mathcal{R}$. We equip the collection of gradings of R with a category structure as we do for module decompositions (see Preliminaries), where the morphisms $\{R_\gamma\}_{\gamma\in\Gamma} \to \{S_\delta\}_{\delta\in\Delta}$ are group homomorphisms $f\colon \Gamma \to \Delta$ so that $S_\delta = \sum_{\gamma\in f^{-1}\delta} R_\gamma$ for all $\delta \in \Delta$.

By a theorem of Lenstra and Silverberg, every reduced order has a *universal* grading [34], see Definition 4.2.1. It proceeds by showing every reduced order has a lattice structure and thus a universal orthogonal decomposition (Theorem 2.5.3), and that every grading is in fact an orthogonal decomposition of this lattice. We will generalize their results to subrings of $\overline{\mathbb{Z}}$.

Theorem 4.3.5. *Every subring of $\overline{\mathbb{Z}}$ has a universal grading with a countable abelian torsion group, and every countable abelian torsion group occurs.*

Theorem 4.3.5 neither implies the results of Lenstra and Silverberg nor vice versa. In Example 4.7.7 we exhibit an obstruction to a common generalization.

For integrally closed subrings of $\overline{\mathbb{Z}}$ we determine precisely which groups occur as the group of their universal grading. For $\overline{\mathbb{Z}}$ it turns out to be the trivial group.

Theorem 4.4.3. *The universal orthogonal decomposition and the universal grading of $\overline{\mathbb{Z}}$ are both trivial.*

Theorem 4.5.3. *Every integrally closed subring of $\overline{\mathbb{Z}}$ has a universal grading with a subgroup of $\mathbb{Q}/\mathbb{Z}$, and every subgroup occurs.*

In [17] we give an algebraic proof of the existence of a universal grading that applies to a broader class of rings than that of reduced orders. The following theorem is a similar generalization to Theorem 1.5 in [34]. We say an element $x \in R$ is *homogeneous* in a grading $\{R_\gamma\}_{\gamma\in\Gamma}$ of R if there exists a unique $\gamma \in \Gamma$ such that $x \in R_\gamma$.

Theorem 4.6.6. *Let R be a commutative ring with a grading $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ where Γ is a torsion group. Suppose for every prime p such that Γ has an element of order p, in the ring R both p and $1+px$ are regular for all $x \in R$. Then:*

1. *The ideal* $\mathrm{nil}(R)$ *is homogeneous, i.e.* $\mathrm{nil}(R) = \sum_{\gamma\in\Gamma}(\mathrm{nil}(R) \cap R_\gamma)$;

2. *The idempotents of R are in R_1;*
3. *If R is connected, then the elements of $\mu(R)$ are homogeneous.*

In [17] we give an algorithm to compute the universal grading of a reduced order. We will show that in a special case we can do this computation in polynomial time. We write $\alpha(R)$ for the set of $x \in R$ for which there exists some $n \geq 1$ such that $x^{n+1} = x$. This set includes the idempotents and roots of unity of R.

Theorem 4.7.13. *There exists a polynomial-time algorithm that, given an order R, decides whether $\alpha(R)$ generates R as a group and if so computes the universal grading of R.*

4.2 Definitions and basic properties

In this section k will be a commutative ring.

Definition 4.2.1. Let R be a k-algebra. A *grading* of R is a decomposition $\{R_\gamma\}_{\gamma\in\Gamma}$ of R as a k-module such that Γ is an abelian group and for all $\gamma, \delta \in \Gamma$ we have $R_\gamma \cdot R_\delta \subseteq R_{\gamma\delta}$. For gradings $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ and $\mathcal{S} = \{S_\delta\}_{\delta\in\Delta}$ of R, a morphism $\mathcal{R} \to \mathcal{S}$ of gradings is a morphism of decompositions for which the underlying map $\Gamma \to \Delta$ is a group homomorphism. A grading $\mathcal{R}$ of R is *universal* if for every grading $\mathcal{S}$ of R there exists a unique morphism $\mathcal{R} \to \mathcal{S}$. We say an element $x \in R$ is *homogeneous* in a grading $\{R_\gamma\}_{\gamma\in\Gamma}$ of R if there exists a unique $\gamma \in \Gamma$ such that $x \in R_\gamma$.

Lemma 4.2.2 (Lemma 2.1.1 in [34])**.** *If $\{R_\gamma\}_{\gamma\in\Gamma}$ is a grading of a k-algebra, then $1 \in R_1$.* □

Example 4.2.3. Let R be a k-algebra. Then R has a *trivial grading* $\{R\}$ with the trivial group. We may naturally grade $R[X]$ with $\{R_n\}_{n\in\mathbb{Z}}$, where $R_n = RX^n$ for $n \geq 0$ and $R_n = 0$ otherwise. The ring $\mathrm{Mat}_2(R)$ of 2×2-matrices with coefficients in R admits a grading with the summands $\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) : a, d \in R\right\}$ and $\left\{\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) : b, c \in R\right\}$. Similarly $\mathbb{Q}^2$ can be graded with a group of order 2 and summands $\mathbb{Q} \cdot (1, 1)$ and $\mathbb{Q} \cdot (1, -1)$.

Lemma 4.2.4. *Suppose $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ is a grading of a k-algebra R and let $\Gamma' = \langle \gamma \in \Gamma \mid R_\gamma \neq 0 \rangle$. Then:*

1. *We have that $\mathcal{R}' = \{R_\gamma\}_{\gamma\in\Gamma'}$ is a grading of R.*
2. *The inclusion $i\colon \Gamma' \to \Gamma$ is a morphism $\mathcal{R}' \to \mathcal{R}$ of gradings.*
3. *If $\mathcal{S}$ is a grading of R and there exists a morphism $f\colon \mathcal{R} \to \mathcal{S}$, then there exists a unique morphism $f'\colon \mathcal{R}' \to \mathcal{S}$. It equals $f \circ i$.*
4. *If there exists a morphism from $\mathcal{R}'$ to a universal grading, then $\mathcal{R}'$ is universal.*

5. *If $\mathcal{R}$ is universal, then $\Gamma = \Gamma'$.*

Proof. Both 1 and 2 are trivial. For 3, clearly $f \circ i$ is such a morphism. For uniqueness, it follows from the definitions that f' must equal f for all $\gamma \in \Gamma$ such that $R_\gamma \neq 0$, and such γ generate Γ'. For 4, we have a map from $\mathcal{R}'$ to any other grading by passing through the universal grading, and such a map is unique by 3. For 5, if $\mathcal{R}$ is universal, then so is $\mathcal{R}'$ by 2 and 4, and then i is a bijection because universal objects are uniquely unique. □

Lemma 4.2.5. *Let S and T be k-algebras and let $\pi\colon S \times T \to S$ be the natural projection.*

1. *Let $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ be a grading of $S \times T$ such that $(1,0)$ is homogeneous. Then $\pi\mathcal{R} := \{\pi(R_\gamma)\}_{\gamma\in\Gamma}$ is a grading of S.*
2. *If $\mathcal{S} = \{S_\delta\}_{\delta\in\Delta}$ and $\mathcal{T} = \{T_\varepsilon\}_{\varepsilon\in\mathrm{E}}$ are gradings of S and T respectively, then $\mathcal{S} \times \mathcal{T} := \{R_{(\delta,\varepsilon)}\}_{(\delta,\varepsilon)\in\Delta\times\mathrm{E}}$ with*

$$R_{(\delta,\varepsilon)} = \begin{cases} S_1 \times T_1 & \text{if } \delta = \varepsilon = 1 \\ S_\delta \times 0 & \text{if } \delta \neq 1 \text{ and } \varepsilon = 1 \\ 0 \times T_\varepsilon & \text{if } \delta = 1 \text{ and } \varepsilon \neq 1 \\ 0 \times 0 & \text{otherwise} \end{cases}$$

is a grading of $S \times T$.

Note that by Theorem 1.5.ii in [34] the condition that $(1,0)$ be homogeneous is automatically satisfied when S and T are orders. We will show in Theorem 4.6.6 that this is even true for a broader class of rings.

Proof. One easily verifies that if $\pi\mathcal{R}$ and $\mathcal{S} \times \mathcal{T}$ are decompositions, then they are also gradings. It is clear that $\mathcal{S} \times \mathcal{T}$ is a decomposition, so this remains to be shown for $\pi\mathcal{R}$.

Note that $S = \sum_{\gamma\in\Gamma} \pi(R_\gamma)$. We identify S with $S \times 0 \subseteq R$, so that $\pi(R_\gamma) = (1,0) \cdot R_\gamma$. As $(1,0) \in R_1$, we find $\pi(R_\gamma) \subseteq R_\gamma$. Hence the sum of the $\pi(R_\gamma)$ is a direct sum, and thus $\pi\mathcal{R}$ is a decomposition. □

Proposition 4.2.6. *Let S and T be k-algebras, write $R = S \times T$ and let $\pi\colon R \to S$ be the natural projection. Suppose that $(1,0)$ is homogeneous in every grading of R. Then:*

1. *If $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ is a universal grading of $S \times T$, then $\{\pi(R_\gamma)\}_{\gamma\in\Gamma'}$ with $\Gamma' = \langle \gamma \in \Gamma \mid \pi(R_\gamma) \neq 0\rangle$ is a universal grading of S.*
2. *If $\mathcal{S}$ and $\mathcal{T}$ are universal gradings of S and T respectively, then with the notation as in Lemma 4.2.5 the grading $\mathcal{S} \times \mathcal{T}$ is universal.*

Proof. 1. From Lemma 4.2.5.1 and Lemma 4.2.4.1 we conclude that $\mathcal{R}_S = \{\pi(R_\gamma)\}_{\gamma\in\Gamma'}$ is a grading of S. Let $\mathcal{S} = \{S_\delta\}_{\delta\in\Delta}$ be a grading of S and let $\mathcal{T}$ be the trivial grading of T. Then $\mathcal{S}\times\mathcal{T}$ is a grading of R, so by universality there exists a morphism $f\colon \Gamma \to \Delta \times 1$ that maps $\mathcal{R}$ to $\mathcal{S}\times\mathcal{T}$. It is easy to see the induced map $f'\colon \Gamma' \to \Delta$ sends $\mathcal{R}_S$ to $\mathcal{S}$. By Lemma 4.2.4.3 this map is unique, so $\mathcal{R}_S$ is universal.

2. Suppose $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ is a grading of R and let Δ and E be the groups of $\mathcal{S}$ and $\mathcal{T}$ respectively. Again $\pi\mathcal{R}$ is a grading of S by Lemma 4.2.5.1 and analogously $(1-\pi)\mathcal{R}$ is a grading of T. Universality gives morphisms $f\colon \Delta \to \Gamma$ and $g\colon \mathrm{E} \to \Gamma$ that respectively map $\mathcal{S}$ to $\pi\mathcal{R}$ and $\mathcal{T}$ to $(1-\pi)\mathcal{R}$. Let $\mathcal{R}' = \{R'_\gamma\}_{\gamma\in\Gamma}$ be the image of $\mathcal{S}\times\mathcal{T}$ under the induced map $\Delta\times\mathrm{E} \to \Gamma$. One easily verifies that $\pi\mathcal{R} = \pi\mathcal{R}'$. From Lemma 4.2.2 we obtain that $(0,1)$ is also homogeneous, so analogously $(1-\pi)\mathcal{R} = (1-\pi)\mathcal{R}'$. Then $R_\gamma = \pi(R_\gamma) + (1-\pi)(R_\gamma) = \pi(R'_\gamma) + (1-\pi)(R'_\gamma) = R'_\gamma$ for all $\gamma \in \Gamma$. Hence $\mathcal{R} = \mathcal{R}'$ and indeed there exists a map $\mathcal{S}\times\mathcal{T} \to \mathcal{R}$. That it is unique follows from Lemma 4.2.4.3 and Lemma 4.2.4.5 together with the observation that $\Delta \times \mathrm{E}$ is generated by the coordinates where $\mathcal{S}\times\mathcal{T}$ is non-zero. □

Example 4.2.7. The conclusion to Proposition 4.2.6 becomes false when we drop the assumption that $(1,0)$ be homogeneous in R.

As in Example 4.2.3 the decomposition $\{\mathbb{Q}\cdot(1,1), \mathbb{Q}\cdot(1,-1)\}$ of $\mathbb{Q}^2$ gives a grading $\mathcal{R}$ with a group of order 2. However, the projection of $\mathcal{R}$ to the first factor of $\mathbb{Q}^2$ is not a decomposition, let alone a grading, of S. Hence 1 becomes false. For 2, note that the trivial decompositions of $\mathbb{Q}$ are universal, while the product of two such trivial decompositions does not give a universal grading of $\mathbb{Q}^2$. Namely, the product of trivial decompositions is trivial, while a non-trivial grading $\mathcal{R}$ of $\mathbb{Q}^2$ exists.

Lemma 4.2.8. *Suppose R is an commutative k-algebra that is a domain and integral over the image of k in R. If $\{R_\gamma\}_{\gamma\in\Gamma}$ is a grading of R, then $\Gamma' = \{\gamma \in \Gamma \mid R_\gamma \neq 0\}$ is a torsion subgroup of Γ.*

Proof. Since 0 is the only zero-divisor in R, we have for $\gamma, \delta \in \Gamma'$ that $0 \subsetneq R_\gamma R_\delta \subseteq R_{\gamma\delta}$, so $\gamma\delta \in \Gamma'$. For $\gamma \in \Gamma'$ and $x \in R_\gamma$ non-zero we have $x^n = \sum_{i=0}^{n-1} a_i x^i$ for some $n \in \mathbb{Z}_{\geq 1}$ and $a_i \in k$, so $0 \neq x^n \in R_{\gamma^n} \cap \sum_{i=0}^{n-1} R_{\gamma^i}$. Hence $\gamma^n = \gamma^i$ for some $0 \leq i < n$, so the order of γ is finite and Γ' is a torsion group. □

4.3 Universal gradings

In this section we generalize the result of Lenstra and Silverberg [34] that reduced orders have universal gradings to subrings of $\overline{\mathbb{Z}}$. Recall that $\overline{\mathbb{Z}}$ is a

Hilbert lattice; see Theorem 3.2.10.

Lemma 4.3.1. *Suppose $R \subseteq \overline{\mathbb{Z}}$ is a subring and $\{R_\gamma\}_{\gamma\in\Gamma}$ is a grading of R. Then for all $\delta, \varepsilon \in \Gamma$ distinct we have $\langle R_\delta, R_\varepsilon\rangle = 0$.*

Proof. Let $x \in R_\delta$ and $y \in R_\varepsilon$. With $S_\gamma = R_\gamma \cap \mathbb{Z}[x, y]$ we have an order $S = \bigoplus_{\gamma\in\Gamma} S_\gamma$ with grading $\{S_\gamma\}_\gamma$. Note that our inner product on $\overline{\mathbb{Z}}$ restricted to S differs from the inner product defined on S in [34] by a factor equal to the rank of S. Then by Proposition 5.8 in [34] we have that $\langle x, y\rangle \in \langle S_\delta, S_\varepsilon\rangle = 0$. Hence $\langle R_\delta, R_\varepsilon\rangle = 0$. □

Proposition 4.3.2. *Every subring of $\overline{\mathbb{Z}}$ has a universal grading.*

Proof. Let R be a subring of $\overline{\mathbb{Z}}$, which is also a sublattice of $\overline{\mathbb{Z}}$. Let $\mathcal{U} = \{U_i\}_{i\in I}$ be a universal decomposition of the lattice R, which exists by Theorem 2.5.3. We obtain this decomposition by starting with the graph G on the vertex set $\operatorname{indec}(R)$ with an edge between $x, y \in \operatorname{indec}(R)$ if and only if $\langle x, y\rangle \neq 0$, then taking I to be the set of connected components of G and U_i the group generated by $i \in I$. For $u = \sum_i u_i \in R$ with $u_i \in U_i$ write $\operatorname{supp}(u) = \{i \in I \mid u_i \neq 0\}$. Now consider the free abelian group $\mathbb{Z}^{(I)}$ and let Γ be the group obtained from it by dividing out

$$N = \langle i + j - k \mid i, j \in I,\ k \in \operatorname{supp}(U_i \cdot U_j)\rangle.$$

We have an induced map $f\colon I \to \mathbb{Z}^{(I)} \to \Gamma$ which induces a decomposition $f(\mathcal{U}) = \{R_\gamma\}_{\gamma\in\Gamma}$ of R, which is also a grading. We claim that it is universal.

Let $\{S_\delta\}_{\delta\in\Delta}$ be a grading of R. Then by Lemma 4.3.1 this is also an orthogonal decomposition of the lattice R. By universality there exists a map $\alpha\colon I \to \Delta$ such that $\alpha(\mathcal{U}) = \{S_\delta\}_{\delta\in\Delta}$. This map factor through the group homomorphism $\mathbb{Z}^{(I)} \to \Delta$, and we see that N is in the kernel. The induced map $a\colon \Gamma \to \Delta$ sends $\{R_\gamma\}_{\gamma\in\Gamma}$ to $\{S_\delta\}_{\delta\in\Delta}$. Such a map is necessarily unique: For all $\gamma \in \Gamma$ we have $0 \neq R_\gamma \subseteq S_{a(\gamma)}$, so $b(\gamma) = a(\gamma)$ for any morphism $b\colon \Gamma \to \Delta$ of decompositions. □

Lemma 4.3.3. *Suppose $R \subseteq \overline{\mathbb{Z}}$ is a subring and $\{R_\gamma\}_{\gamma\in\Gamma}$ is a grading of R. If the universal grading of R_1 is trivial and $R_\gamma \neq 0$ for all $\gamma \in \Gamma$, then $\{R_\gamma\}_{\gamma\in\Gamma}$ is universal.*

Proof. Suppose $\{S_\delta\}_{\delta\in\Delta}$ is a universal grading of R, which exists by Proposition 4.3.2, and let $f\colon \Delta \to \Gamma$ be the map given by universality. Then $R_1 = \bigoplus_{\delta\in\ker(f)} S_\delta$, which is a grading of R_1. Since the universal grading of R_1 is trivial, it follows that $R_1 = S_1$. By Lemma 4.2.8 we have $S_\delta \neq 0$ for all $\delta \in \ker(f)$, so it follows that $\ker(f) = 1$ and that f is injective. From

the fact that $R_\gamma \neq 0$ for all $\gamma \in G$ it follows that f must be surjective. Thus f is an isomorphism of gradings and $\{R_\gamma\}_{\gamma\in\Gamma}$ is universal. □

Example 4.3.4. Every countable abelian torsion group occurs as the group of a universal grading of a subring of $\overline{\mathbb{Z}}$. Note that such a group is a subgroup of $\Omega = \bigoplus_{p\in\mathcal{P}}(\mathbb{Q}/\mathbb{Z})$, where $\mathcal{P}$ is some countably infinite set. We choose $\mathcal{P}$ to be the set of positive prime numbers. Fixing some embedding $\overline{\mathbb{Z}} \to \mathbb{C}$ we have a well-defined x-th power of p in $\overline{\mathbb{Q}} \cap \mathbb{R}_{>0}$ for all $x \in \mathbb{Q}$. Let $[\cdot] : \mathbb{Q}/\mathbb{Z} \to [0,1) \cap \mathbb{Q}$ be the (bijective) map that assigns to each class its smallest non-negative representative. It is then easy to verify that $R = \mathbb{Z}[p^x \mid p \in \mathcal{P},\, x \in \mathbb{Q}_{\geq 0}] \subseteq \overline{\mathbb{Z}}$ has a grading $\{R_{(x_p)_p}\}_{(x_p)_p\in\Omega}$ with

$$R_{(x_p)_p} = \Big(\prod_{p\in\mathcal{P}} p^{[x_p]}\Big)\cdot\mathbb{Z}.$$

In turn any subgroup $\Gamma \subseteq \Omega$ gives a grading $\{R_\gamma\}_{\gamma\in\Gamma}$ of the subring $\bigoplus_{\gamma\in\Gamma} R_\gamma \subseteq R$. This grading is universal by Lemma 4.3.3, as $R_1 = \mathbb{Z}$.

Theorem 4.3.5. *Every subring of $\overline{\mathbb{Z}}$ has a universal grading with a countable abelian torsion group, and every countable abelian torsion group occurs.*

Proof. By Proposition 4.3.2 a universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ exists. By Lemma 4.2.4.5 and Lemma 4.2.8 the group $\Gamma = \{\gamma \in \Gamma : R_\gamma \neq 0\}$ is a torsion group, which is countable by countability of $\overline{\mathbb{Z}}$. In Example 4.3.4 we show all such groups occur. □

4.4 Decompositions of the lattice of algebraic integers

In this section we will show that $\overline{\mathbb{Z}}$ is indecomposable as a Hilbert lattice. The following lemma is a standard result from linear algebra.

Lemma 4.4.1. *Let V be a vector space over an infinite field and let S be a finite set of subspaces of V. If $\bigcup_{U\in S} U = V$, then $V \in S$.* □

Proposition 4.4.2. *Let $S \subseteq \overline{\mathbb{Z}}$ with S finite and $0 \notin S$. Then there exist $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ such that $\langle\alpha,\beta\rangle \neq 0$ for all $\beta \in S$.*

Proof. Let K be the field generated by S and fix $1 < r < \sqrt{2}$.

We will construct an element $u \in \mathcal{O}_K$ such that $0 \notin \langle u, S\rangle$ and $|\sigma(u)| > r$ for all $\sigma \in \mathrm{X}(K)$. For $x \in K$ write $x^\perp = \{y \in K \mid \langle x,y\rangle = 0\}$, which is a proper $\mathbb{Q}$-vector subspace of K when $x \neq 0$ because $x \notin x^\perp$. Hence $\bigcup_{x\in S} x^\perp \neq K$ by Lemma 4.4.1, so there exists some non-zero $u \in K$ such

that $0 \notin \langle u, S\rangle$. By scaling u by some non-zero integer we may assume $u \in \overline{\mathbb{Z}}$ as well. By further scaling u with integers we may assume $|\sigma(u)| > r$ for all $\sigma \in \mathrm{X}(K)$, as was to be shown.

As $|\sigma(u)| > r$ for all $\sigma \in \mathrm{X}(K)$ we have $N(u) > r > 1$, where N is as in Definition 3.2.3, so u is not a unit. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime containing u and let $v \in \mathfrak{p} \setminus \mathfrak{p}^2$. Let $f_n = X^n - uX^{n-1} - v \in \mathcal{O}_K[X]$ for $n \geq 2$ and note that it is Eisenstein at $\mathfrak{p}$ and therefore irreducible. Let $\alpha_n \in \overline{\mathbb{Z}}$ be a root of f_n. It suffices to show that for n sufficiently large α_n is indecomposable and satisfies $0 \notin \langle \alpha_n, S\rangle$. By Lemma 3.3.4 and by construction of u it holds for any $n \geq 2$ that

$$\langle \alpha_n, S\rangle = \frac{\langle \mathrm{Tr}_{K(\alpha_n)/K}(\alpha_n), S\rangle}{[K(\alpha_n) : K]} = \frac{\langle u, S\rangle}{[K(\alpha_n) : K]} \not\ni 0,$$

so it remains to be shown that α_n is indecomposable for n sufficiently large.

Let $D \subseteq \mathbb{C}$ be the closed disk of radius r around 0. Let n be sufficiently large such that we have $|\sigma(v)| \cdot r^{1-n} < |\sigma(u)| - r$ for all $\sigma \in \mathrm{X}(K)$. Fix $\sigma \in \mathrm{X}(K)$. For all x on the boundary of D we have

$$\begin{aligned} |x^n - \sigma(v)| &\leq r^n + |\sigma(v)| = r^{n-1}(r + |\sigma(v)| \cdot r^{1-n}) \\ &< |\sigma(u)| \cdot r^{n-1} = |\sigma(u) \cdot x^{n-1}|. \end{aligned}$$

Hence by Rouché's Theorem (Theorem 4.18 in [1]) the analytic functions $\sigma(u)X^{n-1}$ and $\sigma(f_n) = (X^n - \sigma(v)) - \sigma(u)X^{n-1}$ have the same number of zeros in D, counting multiplicities, which for $\sigma(u)X^{n-1}$ clearly is $n-1$. For the remaining zero $x_{\sigma,n} \in \mathbb{C}$ of $\sigma(f_n)$ with $|x_{\sigma,n}| > r$ we have $x_{\sigma,n}^{n-1}(x_{\sigma,n} - \sigma(u)) = \sigma(v)$ and thus

$$|x_{\sigma,n} - \sigma(u)| = |\sigma(v)| \cdot |x_{\sigma,n}|^{1-n} < |\sigma(v)| \cdot r^{1-n} \to 0 \quad (\text{as } n \to \infty),$$

i.e. $\lim_{n\to\infty} x_{\sigma,n} = \sigma(u)$. Now summing over all $\sigma \in \mathrm{X}(K)$ we get

$$\begin{aligned} q(\alpha_n) &= \frac{1}{n \cdot [K : \mathbb{Q}]} \sum_{\sigma \in X(K)} \sum_{\rho \in \mathrm{X}_\sigma(K(\alpha_n))} |\rho(\alpha_n)|^2 \\ &\leq \frac{1}{n \cdot [K : \mathbb{Q}]} \sum_{\sigma \in X(K)} \left((n-1)r^2 + |x_{\sigma,n}|^2\right) \\ &\leq r^2 + \frac{1}{n \cdot [K : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} |x_{\sigma,n}|^2 \to r^2 \quad (\text{as } n \to \infty). \end{aligned}$$

Because $r^2 < 2$ we have for sufficiently large n that $q(\alpha_n) < 2$. From Proposition 3.3.1 we may then conclude that α_n is indecomposable, as was to be shown. □

Theorem 4.4.3. *The universal orthogonal decomposition and the universal grading of $\overline{\mathbb{Z}}$ are both trivial.*

Proof. Let $\beta, \gamma \in \operatorname{indec}(\overline{\mathbb{Z}})$. Then there exists some $\alpha \in \operatorname{indec}(\overline{\mathbb{Z}})$ such that $\langle \alpha, \beta \rangle \neq 0 \neq \langle \alpha, \gamma \rangle$ by Proposition 4.4.2. Hence α, β and γ must be in the same connected component of the graph of Theorem 2.5.3. As this holds for all β and γ the graph is connected and hence $\overline{\mathbb{Z}}$ is orthogonally indecomposable. Equivalently, the universal orthogonal decomposition is trivial. It follows then from Lemma 4.3.1 and Lemma 4.2.8 that the universal grading of $\overline{\mathbb{Z}}$ is also trivial. □

4.5 Integrally closed orders

In this section we study the universal gradings of integrally closed subrings of $\overline{\mathbb{Z}}$.

Example 4.5.1. We will show that every subgroup of $\mathbb{Q}/\mathbb{Z}$ occurs as the group of a universal grading of an integrally closed subring of $\overline{\mathbb{Z}}$. Let $\mu = \mu(\overline{\mathbb{Z}})$ and $\mu_p = \mu_p(\overline{\mathbb{Z}})$ be as in the Preliminaries. For a prime number p write

$$\mu_{p^\infty} = \{\zeta \in \mu \mid (\exists\, n \in \mathbb{Z}_{\geq 0})\ \zeta^{p^n} = 1\} \quad \text{and}$$
$$\mu_0 = \{\zeta \in \mu \mid (\exists\, n \text{ square-free})\ \zeta^n = 1\}.$$

The map $\zeta \mapsto \zeta^p$ gives an isomorphism $\mu_{p^\infty}/\mu_p \to \mu_{p^\infty}$. Taking the direct sum over all p we get an isomorphism $\mu/\mu_0 \to \mu$. Thus it suffices to show that for every $\mu_0 \subseteq \mathrm{M} \subseteq \mu$ the group $\Gamma = \mathrm{M}/\mu_0$ occurs as a universal grading group.

Consider $R = \mathbb{Z}[\mathrm{M}]$, the smallest subring of $\overline{\mathbb{Z}}$ containing M, which is integrally closed. Define $R_{\zeta \cdot \mu_0} = \zeta \cdot \mathbb{Z}[\mu_0]$ for all $\zeta \cdot \mu_0 \in \mathrm{M}/\mu_0$ and note that this gives a grading $\{R_\gamma\}_{\gamma \in \Gamma}$ of R. To prove this is a universal grading it suffices by Lemma 4.3.3 to show that the universal grading of $\mathbb{Z}[\mu_0]$ is trivial, or in turn, by Lemma 4.3.1, that $\mathbb{Z}[\mu_0]$ is indecomposable. The elements of μ_0 are indecomposable in $\mathbb{Z}[\mu_0]$ because they are so in $\overline{\mathbb{Z}}$ by Proposition 3.3.1, and they generate $\mathbb{Z}[\mu_0]$ as an additive group. From Proposition 3.3.5 we may conclude that no pair $\zeta, \xi \in \mu_0$ is orthogonal, so from Theorem 2.5.3 it follows that $\mathbb{Z}[\mu_0]$ is indecomposable. Hence the grading is universal.

Lemma 4.5.2. *Suppose $R \subseteq \overline{\mathbb{Z}}$ is a subring and $\{R_\gamma\}_{\gamma \in \Gamma}$ is a grading of R. If $K = \mathbb{Q}(A)$ for some subset $A \subseteq \bigcup_{\gamma \in \Gamma} R_\gamma$, then $\{R_\gamma \cap K\}_{\gamma \in \Gamma}$ is a grading of $R \cap K$.*

Proof. It is clear that $\{R_\gamma \cap K\}_{\gamma \in \Gamma}$ is a grading of $R \cap K$ once we show $\bigoplus_\gamma (R_\gamma \cap K) = R \cap K$. For this it remains to show that $R \cap K \subseteq \sum_\gamma (R_\gamma \cap K)$.

Let $x \in R \cap K$. As $x \in R$ we may uniquely write $x = \sum_\gamma x_\gamma$ for some $x_\gamma \in R_\gamma$. Without loss of generality A is closed under multiplication, so that A generates K as a $\mathbb{Q}$-vector space. Then we may write $x = \sum_{a \in A} r_a a$ for some $r_a \in \mathbb{Q}$ which are almost all equal to zero. Hence a positive integer multiple nx of x satisfies $\sum_\gamma nx_\gamma = nx = \sum_{a \in A} nr_a a$ with $nr_a \in \mathbb{Z}$ for all a and thus $nr_a a \in R_{\gamma_a}$ for some $\gamma_a \in G$. It follows from uniqueness of the decomposition that $nx_\gamma = \sum_{a \in A,\, \gamma_a = \gamma} nr_a a$ and thus $x_\gamma \in K$. We conclude that $x_\gamma \in R_\gamma \cap K$ and thus $x \in \sum_\gamma (R_\gamma \cap K)$, as was to be shown. □

Theorem 4.5.3. *Every integrally closed subring of $\overline{\mathbb{Z}}$ has a universal grading with a subgroup of $\mathbb{Q}/\mathbb{Z}$, and every subgroup occurs.*

Proof. That every subgroup of $\mathbb{Q}/\mathbb{Z}$ occurs follows from Example 4.5.1. Let R be an integrally closed subring of $\overline{\mathbb{Z}}$ and let $\{R_\gamma\}_{\gamma \in \Gamma}$ be a universal grading, which exists by Theorem 4.3.5. It suffices to show that every finitely generated subgroup Δ of Γ is cyclic.

Let $\Delta \subseteq \Gamma$ be finitely generated and thus finite by Lemma 4.2.8. Moreover, by Lemma 4.2.8 we have $R_\delta \neq 0$ for all $\delta \in \Delta$, so we may choose some non-zero $a_\delta \in R_\delta$. Let $A = \{a_\delta \mid \delta \in \Delta\}$ and $K = \mathbb{Q}(A)$. Then by Lemma 4.5.2 we get a grading $\{R_\delta \cap K\}_{\delta \in \Delta}$ of $S = R \cap K$. Since K is a field and R is integrally closed, the ring S is integrally closed. The field of fractions of S is contained in K and is thus of finite degree over $\mathbb{Q}$. Hence we may apply Theorem 1.4 from [34] to conclude that the universal grading of S has a finite cyclic grading group Y. By universality we get a morphism of gradings and thus a morphism of groups $\mathrm{Y} \to \Delta$. The latter is surjective since $0 \neq R_\delta \cap K \ni a_\delta$ for all $\delta \in \Delta$. Thus Δ is cyclic, as was to be shown. □

4.6 Algebraic methods

In this section we will generalize Theorem 1.5 of [34] on the homogeneity of roots of unity and idempotents in gradings, from orders to a broader class of rings. For a commutative ring R and an element $p \in R$ we will consider the property that $1 + px$ is a regular element for all $x \in R$. In particular, such a p is not a unit, and for R a domain this is in fact equivalent.

Lemma 4.6.1. *Let R be a commutative ring and let $p \in R$ be such that $1 + px$ is regular for all $x \in R$. If $I \subseteq R$ is a finitely generated ideal such that $pI = I$, then $I = 0$.*

Proof. This is an immediate consequence of Nakayama's lemma. □

We will use the following notation in this section.

Definition 4.6.2. Let Γ be a finite abelian group. We define the polynomial ring $P_\Gamma = \mathbb{Z}[X_\gamma : \gamma \in \Gamma]$, which comes with a natural Γ-grading $\{P_\gamma\}_\gamma$ where $X_\gamma \in P_\gamma$ for all γ. For $m \in \mathbb{Z}_{\geq 0}$ we define the polynomials $e_{m,\gamma} \in P_\gamma$ by

$$\Big(\sum_{\gamma\in\Gamma} X_\gamma\Big)^m = \sum_{\gamma\in\Gamma} e_{m,\gamma}.$$

Let $\vec{n} = (n_\gamma)_\gamma \in (\mathbb{Z}_{\geq 0})^\Gamma$. We define the *weight* $\mathrm{wt}(\vec{n}) \in \mathbb{Z}_{\geq 0}$ and *degree* $\deg(\vec{n}) \in \Gamma$ of $\vec{n}$ to be the degree of $X^{\vec{n}} = \prod_\gamma X_\gamma^{n_\gamma}$ as monomial and as element of the grading $\{P_\gamma\}_\gamma$ respectively. With $m = \mathrm{wt}(\vec{n})$, we write

$$\binom{m}{\vec{n}} = \frac{m!}{\prod_{\gamma\in\Gamma}(n_\gamma!)} \quad \text{so that} \quad \Big(\sum_{\gamma\in\Gamma} X_\gamma\Big)^k = \sum_{\mathrm{wt}(\vec{n})=k} \binom{k}{\vec{n}} X^{\vec{n}}.$$

Proposition 4.6.3. *Let p be a prime and let $q > 1$ be a power of p. Let R be a commutative ring such that $1+px$ is regular for all x, and let $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ be a grading with $\bigcap_{n\geq 0} \Gamma^{p^n} = 1$. Let $r \in R_1$ and $x \in R$. If $rx^q = x$, then $x \in R_1$.*

Proof. Write $x = \sum_\gamma x_\gamma$ with $x_\gamma \in R_\gamma$ and $\vec{x} = (x_\gamma)_{\gamma\in\Gamma}$. Suppose first that Γ is a finite group of exponent p. Note that

$$\sum_{\gamma\in\Gamma} x_\gamma = x = rx^q = \sum_{\gamma\in\Gamma} re_{q,\gamma}(\vec{x})$$

with $re_{q,\gamma}(\vec{x}) \in R_\gamma$. From the fact that $\mathcal{R}$ is a grading we obtain $x_\gamma = re_{q,\gamma}(\vec{x})$. From congruences modulo p it follows that $p \nmid \binom{q}{\vec{n}}$ if and only if $n_\varepsilon = q$ for some ε, and all such $\vec{n}$ have trivial degree because $\varepsilon^q = 1$. With $I = \sum_{\gamma\neq 1} x_\gamma R$ we obtain $x_\gamma \in pI$ for all $\gamma \neq 1$, so $pI = I$. Thus $I = 0$ by Lemma 4.6.1 and $x = x_1 \in R_1$.

Now consider the general case. By replacing Γ by a subgroup and R by a subring we may assume that Γ is finitely generated by $\{\gamma \in \Gamma \,|\, x_\gamma \neq 0\}$. The quotient map $\pi\colon \Gamma \to \Gamma/p\Gamma$ induces a grading $\pi\mathcal{R} = \{S_\gamma\}_{\gamma\in\Gamma/p\Gamma}$. By the special case above we have $x \in S_1$, so $\Gamma = \langle \gamma \mid x_\gamma \neq 0\rangle \subseteq p\Gamma$. Hence $\Gamma \subseteq \bigcap_{k\geq 0} p^k\Gamma = 1$ and $x = x_1 \in R_1$. □

Lemma 4.6.4. *Let p be a prime and consider the ring $P = P_{\mathbb{Z}/p\mathbb{Z}}$. Then the ideals $I = \sum_{i\neq j} X_iX_jP$ and $J = p^2I + \sum_{i\neq 0} e_{p,i}P$ satisfy $pe_{p,0}I \subseteq J$.*

Proof. Write $e_i = e_{p,i}$. Let the affine group $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})^*$ act naturally on the variables of P. Then $\mathbb{Z}/p\mathbb{Z}$ fixes each e_i, while $a \in$

$(\mathbb{Z}/p\mathbb{Z})^*$ maps e_i to e_{ai}. In particular, the ideals I and J are invariant. Because the action is 2-transitive, it suffices to show that $pX_0X_1e_0 \in J$.

Consider now the ring P/J, on which $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ also acts. We have $ie_i \in J$ for all $i \in \mathbb{Z}/p\mathbb{Z}$. Hence

$$0 \equiv (p+1)\sum_{i=0}^{p-1} iX_ie_{-i} = (p+1)\sum_{i=0}^{p-1} iX_i \sum_{\substack{\mathrm{wt}(\vec{m})=p \\ \deg(\vec{m})=-i}} \binom{p}{\vec{m}} X^{\vec{m}}$$

$$= \sum_{\substack{\mathrm{wt}(\vec{n})=p+1 \\ \deg(\vec{n})=0}} \binom{p+1}{\vec{n}} \Big(\sum_{i=0}^{p-1} n_i i\Big) X^{\vec{n}} \pmod{J},$$

where the first equality is the definition of e_{-i} and the second orders the terms by monomial. Then note for each term that $\sum_{i=0}^{p-1} n_i i \equiv \deg(\vec{n}) \equiv 0 \pmod{p}$, and that $p \mid \binom{p+1}{\vec{n}}$ unless $n_i \geq p$ for some i. Hence most terms are in $p^2I \subseteq J$. The remaining p terms equal

$$0 \equiv \binom{p+1}{p+1} 0X_0^{p+1} + \binom{p+1}{p} \sum_{i=1}^{p-1} piX_0X_i^p \equiv pX_0 \sum_{i=0}^{p-1} iX_i^p \pmod{J}.$$

We now apply the affine transformations $a \mapsto a$ and $a \mapsto 1-a$ to this equality, so that

$$0 \equiv X_1\Big(pX_0 \sum_{i=0}^{p-1} iX_i^p\Big) + X_0\Big(pX_1 \sum_{i=0}^{p-1} (1-i)X_i^p\Big)$$

$$= pX_0X_1 \sum_{i=0}^{p-1} X_i^p \equiv pX_0X_1e_0 \pmod{J}$$

by considering e_0 modulo p, as was to be shown. □

Proposition 4.6.5. *Let p be a prime and let R be a connected commutative ring such that p is regular in R and such that $1+px$ is regular for all $x \in R$. Let $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ be a grading with $\bigcap_{n\geq 0} \Gamma^{p^n} = 1$. Let $x \in R^*$. If x^p is homogeneous, then so is x.*

Proof. Write $x = \sum_{\gamma\in\Gamma} x_\gamma$ with $x_\gamma \in R_\gamma$ and $e_i = e_{p,i}$ for $i \in \mathbb{Z}/p\mathbb{Z}$.

First suppose $\Gamma = \mathbb{Z}/p^k\mathbb{Z}$ for some k. We will apply induction on k. For $k = 0$ the statement is trivial. Now suppose $k > 0$ and that the statement holds for groups of order less than p^k. Consider the natural map $\varphi\colon \Gamma \to \Gamma/p^{k-1}\Gamma$. We obtain from the induction hypothesis that x is homogeneous

in $\varphi\mathcal{R}$. Thus there exists some $c \in \mathbb{Z}$ such that $x = \sum_{i \equiv c\,(p^{k-1})} x_i$. With $\vec{y} = (x_c, x_{c+p^{k-1}}, \ldots, x_{c+(p-1)p^{k-1}})$ we have

$$x^p = \sum_{i=0}^{p-1} e_i(\vec{y}),$$

where $e_i(\vec{y}) \in R_{f(i)}$ with injective $f\colon \mathbb{Z}/p\mathbb{Z} \to \Gamma$ given by $i \mapsto pc + p^k i$.

Since $x^p \neq 0$ is homogeneous there exists a unique h such that $x^p \in R_{f(h)}$. If $h \neq 0$, then $p \mid e_h$ and thus $p \mid x^p$ is a unit. By Lemma 4.6.1 we have $pR = R = 0$, which contradicts the connectivity assumption. Thus we may assume $x^p = e_0(\vec{y})$ and $e_i(\vec{y}) = 0$ for $i \neq 0$.

It follows from Lemma 4.6.4 that $pI = p^2 I$ for $I = \sum_{i \neq j} x_i x_j R$. Since p is regular we get $I = pI$, so $I = 0$ by Lemma 4.6.1. Hence $x_i x_j = 0$ for all $i \neq j$. Let $z_i = x_i/x$. Then

$$z_i(1 - z_i) = x^{-2} x_i (x - x_i) = x^{-2} x_i \sum_{j \neq i} x_j = 0.$$

Thus z_i is idempotent. Since R is connected we have $z_i \in \{0, 1\}$. From $\sum_i z_i = 1$ it follows that $z_i = 1$ for some i. Hence $x = x_i$ is homogeneous, as was to be shown.

It remains to prove the proposition for arbitrary Γ. As per usual we may assume Γ is finitely generated. Suppose there are distinct $\gamma, \delta \in \Gamma$ such that $x_\gamma, x_\delta \neq 0$. Then by either Pontryagin duality or the fundamental theorem on finitely generated abelian groups one deduces that there exists some subgroup $\Delta \subseteq \Gamma$ such that $\gamma\Delta \neq \delta\Delta$ and such that Γ/Δ is cyclic of p-power order. By the specific case above, applied to $\varphi\mathcal{R}$ for $\varphi\colon \Gamma \to \Gamma/\Delta$, we have that $\delta\Delta = \gamma\Delta$, which is a contradiction. It follows that x is homogeneous. □

Theorem 4.6.6 (cf. Theorem 1.5 in [34]). *Let R be a commutative ring with a grading $\mathcal{R} = \{R_\gamma\}_{\gamma \in \Gamma}$ where Γ is a torsion group. Suppose for every prime p such that Γ has an element of order p, in the ring R both p and $1 + px$ are regular for all $x \in R$. Then:*

1. *The ideal* $\operatorname{nil}(R)$ *is homogeneous, i.e.* $\operatorname{nil}(R) = \sum_{\gamma \in \Gamma} (\operatorname{nil}(R) \cap R_\gamma)$*;*
2. *The idempotents of R are in R_1;*
3. *If R is connected, then the elements of $\mu(R)$ are homogeneous.*

Proof. 1. This statement is equivalent to the following: If $x = \sum_{\gamma \in \Gamma} x_\gamma \in R$ is nilpotent, then so is x_γ for all $\gamma \in \Gamma$. Given $x \in \operatorname{nil}(R)$, we may pass to the subgroup of Γ generated by $\{\gamma \in \Gamma \mid x_\gamma \neq 0\}$, which is finite. Then by Proposition 4.1.ii in [34] every x_γ is nilpotent.

It suffices for the following statements to prove them when Γ is a p-group for the relevant primes p. For general Γ one reduces to this special case by considering the projections to the Sylow subgroups.

2. Let $e \in R$ be idempotent. Then $e^p = e$, hence $e \in R_1$ by Proposition 4.6.3.

3. Let $\zeta \in \mu(R)$ be of order n. If $(n,p) = 1$, then there exists some $k \in \mathbb{Z}_{>0}$ such that $p^k \equiv 1 \,(\bmod\, n)$. Then $\zeta^{p^k} = \zeta$, hence $\zeta \in R_1$ by Proposition 4.6.3. For general n we write $n = p^k m$ for $m, k \in \mathbb{Z}_{\geq 0}$ with $(m,p) = 1$. Then $\zeta^{p^k} \in R_1$ by the special case. Inductively $\zeta^{p^{k-i}}$ is homogeneous for $0 \leq i \leq k$ by Proposition 4.6.5, so ζ is homogeneous. □

We now present an alternative proof for Proposition 4.6.5 and hence Theorem 4.6.6.2, with weaker assumptions on p, in the form of Proposition 4.6.11.

Lemma 4.6.7. *Let $B \subseteq C$ be commutative rings and G a group acting on C via ring automorphisms that fix B pointwise and for which the orbits under G are finite. Let p be a prime. Suppose p is not a unit in B and that*

$$\sqrt[p]{B} := \{x \in C \,|\, (\exists\, n \in \mathbb{Z}_{\geq 0})\ x^{p^n} \in B\}$$

generates C as a B-module and contains $C^G = \{c \in C \,|\, (\forall g \in G)\ gc = c\}$. If B is connected, then C is connected.

Proof. Let $\mathfrak{p}$ be a prime of B above p. As $\sqrt[p]{B}$ generates C as B-module the ring extension $B \subseteq C$ is integral. Hence there exists a prime $\mathfrak{q}$ of C such that $\mathfrak{q} \cap B = \mathfrak{p}$ by the going up theorem. Let $x \in C$ and write $x = \sum_{s \in S} s$ for some finite $S \subseteq \sqrt[p]{B}$. We claim that $x \in \mathfrak{q}$ if and only if there exists some $n \in \mathbb{Z}_{\geq 0}$ such that $\sum_{s \in S} s^{p^n} \in \mathfrak{p}$. Namely, we have

$$\sum_{s \in S} s \in \mathfrak{q} \Leftrightarrow \Big(\sum_{s \in S} s\Big)^{p^n} \in \mathfrak{q} \Leftrightarrow \sum_{s \in S} s^{p^n} \in \mathfrak{q} \Leftrightarrow \sum_{s \in S} s^{p^n} \in \mathfrak{p},$$

where for the forward implications we take n sufficiently large such that $s^{p^n} \in B$ for all $s \in S$. We conclude that membership to $\mathfrak{q}$ only depends on $\mathfrak{p}$, i.e. $\mathfrak{q}$ is unique.

Let O be an orbit of non-zero idempotents of C under G, which is finite by assumption on G. Let $M = \{\prod_{s \in S} s \,|\, S \subseteq O\}$ be the monoid that O generates, which has a partial order given by $e \leq f$ when $ef = e$. Let P be the set of minimal non-zero elements of M and let X be an orbit of P under G. Then $e = \sum_{x \in X} x \in C^G \subseteq \sqrt[p]{B}$ is idempotent, so $e = e^{p^n} \in B$ for some n. But B is connected and $e \neq 0$, so $e = 1$. Hence $C \cong \prod_{x \in X} C/(1-x)C$ and G acts transitively on the factors. In particular, the cardinality of every

orbit of spec C under G is divisible by $\#X$. However, $\{\mathfrak{q}\}$ is an orbit, so $\#X = 1$. It follows that $O = \{1\}$, so C is connected. □

Proposition 4.6.8. *Let p be a prime and R a connected commutative ring for which p is regular but not a unit. Then*

1. *for all $\zeta \in \mu_{p^\infty}(\overline{\mathbb{Z}})$, the ring R is connected if and only if $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ is connected;*
2. *for all gradings $\{R_\gamma\}_{\gamma\in\Gamma}$ of R with Γ a finite abelian p-group, the ring R is connected if and only if R_1 is connected.*

Proof. 1. Write $S = R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$. As $R \to S$ is injective, the backward implication holds trivially. It suffices to verify the conditions to Lemma 4.6.7 applied to $R \subseteq S$ with $G = (\mathbb{Z}/p^k\mathbb{Z})^*$ naturally acting: We have $S^G = R \subseteq \sqrt[p]{R}$ by Proposition 3.15 in [17], and $\langle\zeta\rangle \subseteq \sqrt[p]{R}$ generates S as R-module.

2. Write $\#\Gamma = p^k$ and let ζ be a primitive p^k-th root of unity. It suffices by 1 to prove 2 for the grading $\mathcal{S} = \{S_\gamma\}_{\gamma\in\Gamma}$ of $S = R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ with $S_\gamma = R_\gamma \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$. The forward implication is trivial. We apply Lemma 4.6.7 to $S_1 \subseteq S$ with $G = \mathrm{Hom}(\Gamma, \langle\zeta\rangle)$, where $\chi \in G$ acts on S by sending $x \in S_\gamma$ to $\chi(\gamma) \cdot x$: We have that $S^G = \bigoplus_{\gamma\in\Gamma} S_\gamma^G = S_1$, since for all $\eta \in \langle\zeta\rangle$ and $x \in S$ we have $\eta x = x$ if and only if $\eta = 1$ or $x = 0$, and clearly the $S_\gamma \subseteq \sqrt[p]{S_1}$ generate S. □

Lemma 4.6.9. *Let p be a prime and let R be a connected commutative $\mathbb{Z}[\zeta]$-algebra with ζ a primitive p-th root of unity. Write $\pi = 1 - \zeta$. Then $f = \pi^{-p}\big((1 + \pi X)^p - 1\big) \in \mathbb{Z}[\zeta][X]$ has at exactly p distinct roots in R, namely the images of $(\zeta^i - 1)/\pi \in \mathbb{Z}[\zeta]$ in R for $i \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. Recall that $p = u\pi^{p-1}$ for some $u \in \mathbb{Z}[\zeta]^*$. Hence $(1 + \pi X)^p - 1 \equiv 0 \pmod{\pi^p}$, so indeed $f \in \mathbb{Z}[\zeta][X]$. Moreover, f is monic. We compute $f' = u(1+\pi X)^{p-1}$. Then $u^{-1}(1+\pi X)f' - \pi^p f = 1$, so $fR[X] + f'R[X] = R[X]$. Then by Theorem 1.5 in [32] we have that f has at most p roots in R. Each $r_i = (\zeta^i - 1)/\pi \in \mathbb{Z}[\zeta]$ for $0 \le i < p$ is a roots of f. For $0 \le i < j < p$ we have $r_j - r_i = \zeta^i(1 - \zeta^{j-i})/\pi \in \mathbb{Z}[\zeta]^*$. The image of $r_j - r_i$ in R is also a unit, and since $R \neq 0$ the images of $r_0, \ldots, r_{p-1}$ are all distinct, as was to be shown. □

Lemma 4.6.10. *Let p be a prime and let R be a connected commutative $\mathbb{Z}[\zeta]$-algebra with ζ a primitive p-th root of unity. Suppose p is regular in R and let $\mathcal{R} = \{R_\xi\}_{\xi\in\langle\zeta\rangle}$ be a grading of R. Let $x \in R^*$. If $x^p \in R_1$, then x is homogeneous.*

Proof. Write $x = \sum_{\xi\in\langle\zeta\rangle} x_\xi$ with $x_\xi \in R_\xi$. Let σ be the $\mathbb{Z}[\zeta]$-algebra homomorphism of R that maps $y \in R_\xi$ to $\xi y \in R_\xi$. Since $x^p \in R_1$, the element

$\eta = \sigma(x)/x \in R$ satisfies $\eta^p = \sigma(x^p)/x^p = 1$. Write $\pi = 1 - \zeta$. Then $\sigma(x) \equiv x \pmod{\pi R}$, so $\eta = 1 + \pi y$ for some $y \in R$. As π, because it divides p, is regular we obtain $(\eta - 1)/\pi = y = (\zeta^i - 1)/\pi$ for some i by Lemma 4.6.9, and $\eta = \zeta^i \in R_1^*$. From $\sigma(x) = \eta x$ it follows that $\xi x_\xi = \eta x_\xi$ for all $\xi \in \langle\zeta\rangle$. Unless $\xi = \eta$, we have that $\xi - \eta$ is regular as it divides p, and thus $x_\xi = 0$. Hence $x = x_\eta$ is homogeneous. □

Proposition 4.6.11. *Let p be a prime, let R be a connected commutative ring such that $p \in R$ is regular but not a unit. Let $\mathcal{R} = \{R_\gamma\}_{\gamma\in\Gamma}$ be a grading of R with $\bigcap_{n\geq 0} \Gamma^{p^n} = 1$. Let $x \in R^*$. If x^p is homogeneous, then x is homogeneous.*

Proof. As in Proposition 4.6.5 we may assume that Γ is a finite p-group. We apply induction on $\#\Gamma$. If $\#\Gamma = 1$, then clearly all elements are homogeneous. Suppose $\#\Gamma > 1$. Then we may choose a subgroup $\Delta \subseteq \Gamma$ of order p. By induction x is homogeneous in $\varphi\mathcal{R}$ for the natural map $\varphi : \Gamma \to \Gamma/\Delta$, so $x = \sum_{\gamma\in\varepsilon\Delta} x_\gamma$ for some $\varepsilon \in \Gamma$ and $x_\gamma \in R_\gamma$. Then $x^p = y + pz$ where $y = \sum_{\gamma\in\varepsilon\Delta} x_\gamma^p \in R_{\varepsilon^p}$ and $z \in R$. As p is not a unit, x^p can only be a homogeneous unit if $x^p \in R_{\varepsilon^p}$. Let ζ be a primitive p-th root of unity and consider the ring $A = R[\zeta][\Gamma]$ with grading $\mathcal{A} = \{A_\gamma\}_{\gamma\in\Gamma}$ where $A_\gamma = \bigoplus_{\beta\in\Gamma} \beta R_{\beta^{-1}\gamma}[\zeta]$. By Proposition 4.6.8 the ring A is connected. Since A is a free R-module, we conclude that p is regular but not a unit in A. Note that $R_\gamma = A_\gamma \cap R$ and that x is homogeneous in $\mathcal{R}$ if and only if $w = \varepsilon^{-1}x$ is homogeneous in $\mathcal{A}$. Since $w^p \in A_1$ and $\langle\gamma \in \Gamma \mid w_\gamma \neq 0\rangle \subseteq \Delta \cong \langle\zeta\rangle$, we may apply Lemma 4.6.10 to w in the grading $\{A_\gamma\}_{\gamma\in\Delta}$ to conclude that w is homogeneous, as was to be shown. □

Example 4.6.12. Proposition 4.6.11 is an improvement to Proposition 4.6.5, with the difference being the relaxation of the assumption that $1 + px$ be regular for all $x \in R$ to simply p not being a unit. We will show that a similar relaxation is not possible for Proposition 4.6.3.

Let ℓ and p be primes with $\ell \mid p - 1$. Consider $R = \mathbb{Z}[X]/(X^\ell, \ell X)$ with grading $\{\mathbb{Z} \cdot X^k\}_{k\in\mathbb{Z}/p\mathbb{Z}}$. Note that p is regular but not a unit in R, and that R is even connected. The element $x = 1 + X$ is an ℓ-th root of unity, so $x^p = x$. However, $x \notin R_1$, as was to be shown.

The following proposition can be used, together with other results from this section, to show that results from Chapter 5 can be similarly generalized from orders to rings with properties studied here.

Lemma 4.6.13. *Let R be a commutative ring and $p \in R$. If $\bigcap_{n\geq 1} p^n R = 0$, then $1 + px$ is regular for all $x \in R$. If R is Noetherian, then the converse holds.*

Proof. This follows from Theorem 10.17 in [2]. □

Lemma 4.6.14. *Let p be a prime, let R be a commutative ring and let $I \subseteq \mathrm{nil}(R)$ be an ideal. Then:*

1. *$1 + I$ is a subgroup of R^*;*
2. *if $I \subseteq R[p^\infty]$, then $1 + I \subseteq R^*[p^\infty]$;*
3. *if $I[p^\infty] = 0$, then $(1 + I)[p^\infty] = 1$.*

Proof. 1. For $1 - x \in 1 + I$ we have $x^m = 0$ for some $m > 0$, hence $(1 - x)(1 + x + \cdots + x^{m-1}) = 1 - x^m = 1$ and $1 - x \in R^*$.

2. One shows inductively that $(1 + x)^{p^k} \in 1 + xJ^k$ for each $x \in R$ and $J = pR + xR$. Given $x \in I$ we may take k sufficiently large so that $xJ^k = 0$ to conclude that $1 + x \in R^*[p^k]$.

3. We may replace R by $R[1/p]$, since $I[p^\infty] = 0$ implies the restriction of $R \to R[1/p]$ to $1 + I$ is injective. Thus we replace the assumption that $I[p^\infty] = 0$ by $p \in R^*$. We may also assume without loss of generality that I is finitely generated. Hence there exists some m such that $I^{2^m} = 0$. We will prove the lemma with induction on m. For $m = 0$ the statement becomes trivial.

Suppose $I^{2^{m+1}} = 0$ and consider the ideal $K = I^{2^m}$. The image J of I in R/K satisfies $J^{2^m} = 0$ and thus $(1 + J)[p^\infty] = 1$ by the induction hypothesis. It remains to show that $(1 + K)[p^\infty] = 1$. Note that $K^2 = 0$, so we have a group isomorphism $1 + K \to K$ given by $1 + x \mapsto x$. Hence $(1 + K)[p^\infty] \cong K[p^\infty] = 0$. □

Proposition 4.6.15. *Let p be a prime and R a Noetherian commutative ring such that $1 + px$ is regular for all $x \in R$. Then $\mathrm{nil}(R)[p^\infty]$ is finite if and only if $\mu_{p^\infty}(R)$ is finite.*

Proof. ($\Leftarrow$) This follows from Lemma 4.6.14.2.

($\Rightarrow$) First suppose R is a domain. For $k \geq 0$ write

$$I_k = \sum_{\zeta \in \mu_{p^k}(R)} (1 - \zeta)R.$$

As R is Noetherian, the chain $I_0 \subseteq I_1 \subseteq \cdots$ stabilizes at index say n. Because R is a domain we may choose a generator ξ for $\mu_{p^{n+1}}(R)$, and let us suppose that it is primitive. As $1 - \xi^a = (\sum_{i=0}^{a-1} \xi^i)(1 - \xi)$ for all $a \in \mathbb{Z}_{\geq 1}$, we conclude that $(1 - \xi)R = I_{n+1} = I_n = (1 - \xi^p)R$. Since $(1 - \xi)R \neq 0$ we obtain $\pi = \sum_{i=0}^{p-1} \xi^i \in R^*$. But $\pi^{p^n} \equiv \Phi_p(\xi^{p^n}) = 0 \pmod p$. Hence $p \mid \pi^{p^n}$ is a unit, which contradicts $1 - pp^{-1}$ being regular. We conclude that $\mu_{p^\infty}(R) = \mu_{p^n}(R)$ is finite.

Consider the case where R is reduced. We have an injective map

$$R \to \prod_{\mathfrak{p} \text{ min. prime}} R/\mathfrak{p}.$$

Note that $1+px \notin \mathfrak{p}$ for all $x \in R$ and minimal primes $\mathfrak{p}$, as each $\mathfrak{p}$ consists of only zero divisors (Theorem 3.1 in [12]). As $R/\mathfrak{p}$ is a domain, it follows that $1+py$ is regular for all $y \in R/\mathfrak{p}$. From the previous case we obtain that $\mu_{p^\infty}(R/\mathfrak{p})$ is finite for all $\mathfrak{p}$. As R is Noetherian, it has only finitely many minimal prime ideals (Theorem 7.13 in [2]), and thus $\mu_{p^\infty}(R)$ is finite.

Consider the case where p acts regularly on $\mathrm{nil}(R)$. Consider the map $R \to R/\mathrm{nil}(R)$. The induced map $\mu_{p^\infty}(R) \to \mu_{p^\infty}(R/\mathrm{nil}(R))$ is injective, because its kernel $(1+\mathrm{nil}(R))[p^\infty]$ is trivial by Lemma 4.6.14.3. It suffices that $\mu_{p^\infty}(R/\mathrm{nil}(R))$ is finite, which is the reduced case.

Consider the general case where $T = \mathrm{nil}(R)[p^\infty]$ is finite. As before we consider the quotient map $R \to R/T$. We have that $(1+T)[p^\infty]$ is finite as T is finite, while R/T satisfies the conditions to the previous case. Hence $\mu_{p^\infty}(R)$ is finite. □

Example 4.6.16. It is still possible for a reduced Noetherian commutative ring R to have infinitely many roots of unity when $1+px$ is regular for all primes p and $x \in R$.

Consider $\mathbb{Z}[\mu_0]$ as in Example 4.5.1 and let R be a localization of $\mathbb{Z}[\mu_0]$ such that for each prime p there is precisely one prime $\mathfrak{p}_p \subset R$ above p. Clearly R has infinitely many roots of unity. Since each prime p is non-invertible and R is a domain, the element $1+px$ is regular for all $x \in R$. For a prime p and primitive $\zeta_p \in \mu_p$ one shows inductively that, for finite subgroups $\langle \zeta_p \rangle \subseteq G \subset \mu_0$, the unique prime of $S = R \cap \mathbb{Q}(G)$ over p equals $pS + (1-\zeta_p)S$. Hence $\mathfrak{p}_p = pR + (1-\zeta_p)R$ is finitely generated for all p, and thus R is Noetherian.

4.7 Algorithms

In this section we describe an algorithm to compute the universal grading of a special type of order in polynomial time. Recall that we have an encoding for finitely generated abelian groups. To encode a grading $\{R_\gamma\}_{\gamma \in \Gamma}$ of an order, where Γ is a finitely generated abelian group, we specify this group Γ as well as the group R_γ for all γ such that $R_\gamma \neq 0$. By Theorem 1.4 in [17] we may compute the universal grading of any reduced order, but in general this does not run in polynomial time. We will restrict to orders generated by autopotents.

Definition 4.7.1. Let R be a ring. We call $x \in R$ *autopotent* if $x^{n+1} = x$ for some $n \in \mathbb{Z}_{>0}$. Write $\alpha(R)$ for the set of autopotents of R.

Lemma 4.7.2. *Let S and R be rings. Then:*

1. *The roots of unity and idempotents of R are autopotent;*
2. *The product of any two commuting autopotents of R is autopotent;*
3. *We have $\mu(R \times S) = \mu(R) \times \mu(S)$ and $\alpha(R \times S) = \alpha(R) \times \alpha(S)$;*
4. *Let $x \in R$. Then $x \in \alpha(R)$ if and only if there exist an idempotent $e \in R$ and $\zeta \in \mu(R)$ such that $x = e\zeta = \zeta e$;*
5. *If R is commutative, then R is generated as a ring by $\alpha(R)$ if and only if its additive group is generated by $\alpha(R)$;*
6. *As groups, $R \times S$ is generated by autopotents if and only if each of R and S is generated by autopotents;*
7. *If R is connected, then $\alpha(R) = \mu(R) \cup \{0\}$.*

Proof. Statements 1, 2 and 3 are trivial.

4. The 'if'-part follows from 1 and 2. Conversely, suppose $x^{n+1} = x$. Then $e = x^n$ satisfies $e^2 = e$, so e is idempotent. Assume without loss of generality that $R = \mathbb{Z}[x]$, so R is commutative. Hence we may decompose $R = eR \times (1-e)R$. As $ex \in eR$ is an n-th root of unity, so is $\zeta = ex + (1-e) \in R$. Then $x = e\zeta = \zeta e$.

5. By 2 the set of autopotents is closed under multiplication.

6. Combine 3 with the fact that $0 \in \alpha(R)$ and $0 \in \alpha(S)$.

7. This follows trivially from 4. □

Lemma 4.7.3. *Let R be an order that is generated as a group by $\alpha(R)$. Then R is reduced.*

Proof. It suffices to prove that $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$ is reduced, because $R \to K$ is injective. Each $x \in \alpha(R)$ has a minimal polynomial in $K[X]$ dividing $X^{n+1} - X$ for some $n > 0$. In particular x is separable, and consequently so are all elements of K. As 0 is the only separable nilpotent element, the lemma follows. □

We now equip reduced orders with the (Hilbert) lattice structure as defined in [34], similar to the Hilbert lattice structure defined on $\overline{\mathbb{Z}}$.

Definition 4.7.4 (Example 3.4 in [34])**.** For an order R we define a bilinear map

$$\langle x, y \rangle_R = \sum_{\sigma \in \mathrm{X}(R)} \sigma(x) \cdot \overline{\sigma(y)},$$

where the sum ranges over all ring homomorphisms from R to $\mathbb{C}$, of which there are only finitely many.

Remark 4.7.5. Following Example 3.4 in [34], the order R is reduced if and only if the map from Definition 4.7.4 is non-degenerate, i.e. $\langle x, x\rangle = 0$ implies $x = 0$ for all $x \in R$. We have a bijective correspondence

$$\{\sigma\colon R \to \mathbb{C}\} \leftrightarrow \{(\mathfrak{p}, \sigma_\mathfrak{p}) \mid \mathfrak{p} \subseteq R \text{ a minimal prime ideal, } \sigma_\mathfrak{p}\colon R/\mathfrak{p} \to \mathbb{C}\}$$

that sends $\sigma\colon R \to \mathbb{C}$ to $(\ker(\sigma), \tilde{\sigma})$ where $\tilde{\sigma}\colon R/\ker(\sigma) \to \mathbb{C}$ is given by the homomorphism theorem, and conversely sends $(\mathfrak{p}, \sigma_\mathfrak{p})$ to $\sigma_\mathfrak{p}$ composed with the projection $\pi_\mathfrak{p}\colon R \to R/\mathfrak{p}$. Thus for all $x, y \in R$ we have

$$\langle x, y\rangle_R = \sum_{\mathfrak{p} \subseteq R} \langle \pi_\mathfrak{p}(x), \pi_\mathfrak{p}(y)\rangle_{R/\mathfrak{p}},$$

where the sum ranges over all minimal prime ideals.

Remark 4.7.6. For an order R which is a domain, i.e. $R \subseteq \overline{\mathbb{Z}}$, we have now two lattice structures, namely that of a sublattice of $\overline{\mathbb{Z}}$ and the one from Definition 4.7.4. However, they are equal up to a factor $\#\mathrm{X}(R)$. In particular, the property of orthogonality is the same under either inner product. One might try to construct a common generalization of both inner products to subrings of $\overline{\mathbb{Z}}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. The following example highlights an obstruction for this.

Example 4.7.7. For arbitrary reduced orders $R \subseteq S$ the restriction $\langle -, -\rangle_S$ to R is not a scalar multiple of $\langle -, -\rangle_R$, as is the case for the inner product on $\overline{\mathbb{Z}}$. Consequently, there is no natural definition of an inner product on any class of rings that includes both $\overline{\mathbb{Z}}$ and reduced orders.

For $R = \mathbb{Z} \times \mathbb{Z}[\sqrt{2}]$ and $S = \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}]$ the element $x = (0, \sqrt{2})$ satisfies $\langle x, x\rangle_R = 4 = \langle x, x\rangle_S$, while $y = (1, 1)$ satisfies $\langle y, y\rangle_R = 3$ and $\langle y, y\rangle_S = 4$.

Lemma 4.7.8. *For all orders R that are generated as a group by $\alpha(R)$ we have $\langle R, R\rangle_R \subseteq \mathbb{Z}$. There exists a polynomial-time algorithm that, given an order R that is generated as a group by $\alpha(R)$ and $x, y \in R$, computes $\langle x, y\rangle_R$.*

Proof. Note that R is reduced by Lemma 4.7.3. Let X be the set of minimal primes of R. Using Theorem 1.10 in [33] we may compute X and for each $\mathfrak{p} \in X$ the map $R \to R/\mathfrak{p}$ in polynomial time. Note that as a group, $R/\mathfrak{p}$ is generated by $\alpha(R/\mathfrak{p})$. Then by the formula of Remark 4.7.5 it suffices to prove the lemma for the ring $R/\mathfrak{p}$. Thus we suppose R is a domain and consequently $\alpha(R) = \mu(R) \cup \{0\}$ by Lemma 4.7.2.7. For $\zeta, \xi \in \mu(R)$ and a ring homomorphism $\sigma\colon R \to \mathbb{C}$ we have $\sigma(\zeta) \cdot \overline{\sigma(\xi)} = \sigma(\zeta\xi^{-1})$. Thus $\langle \zeta, \xi\rangle_R = \sum_{\sigma \in \mathrm{X}(R)} \sigma(\zeta\xi^{-1})$, which is the trace of $\zeta\xi^{-1}$ from R to $\mathbb{Z}$, and

hence is an integer. As R is generated as a group by $\mu(R)$, it follows that $\langle R, R\rangle_R \subseteq \mathbb{Z}$ as well. Moreover, this shows that computing $\langle x, y\rangle_R$ reduces to computing traces of roots of unity, which clearly can be done in polynomial time. □

Lemma 4.7.9. *There exists a polynomial-time algorithm that, given a finite-dimensional commutative $\mathbb{Q}$-algebra A and a finite set $X \subseteq A$, computes a $\mathbb{Q}$-basis Y of the subalgebra B of A generated by X, where each element in Y is a finite (possibly empty) product of elements of X.*

Proof. We will write $\mathbb{Q}Y$ for the vector space generated by Y. The algorithm proceeds as follows. Start with $Y = \{1\}$. Compute the set of products $Z = \{xy \mid x \in X, y \in Y\}$ and update Y to be a maximal $\mathbb{Q}$-linearly independent subset of $Z \cup Y$ containing Y. Repeat this until Y is stable.

Write m for the dimension of B. Suppose in some step $\mathbb{Q}Y = \mathbb{Q}\cdot(Z\cup Y)$. Then $Z \subseteq \mathbb{Q}Y$, so $\mathbb{Q}Y$ is closed under taking products with X. Since X generates B as a $\mathbb{Q}$-algebra and $1 \in \mathbb{Q}Y$ by the choice of initial Y, it follows that $\mathbb{Q}Y = B$. Note that $\#Y \leq m$ and thus there are at most m steps in the algorithm. Moreover, in each step $\#Z \leq \#(X \times Y)$ is polynomially bounded in the input length, so in total there are only polynomially many multiplications. Lastly, note that in step i of the algorithm each element of Y can be written as a product of i elements from X, and therefore the encoding of every element has length proportional to at most i times that of the longest element of X. Hence the multiplications can be carried out in polynomial time. □

Example 4.7.10. Although it is possible to compute $\alpha(R)$ for a reduced order R, we cannot in general do this in polynomial time, even if R is connected. Note that for the ring

$$R = \{(a_i)_i \in \mathbb{Z}^n \mid (\forall\, i, j)\ a_i \equiv a_j \bmod 2\},$$

the set $\{-1, 1\}^n = \mu(R) = \alpha(R)$ is exponentially large.

Proposition 4.7.11. *There exists a polynomial-time algorithm that, given an order R, computes a set $Y \subseteq \alpha(R)$ such that $\mathbb{Z}\cdot Y = \mathbb{Z}\cdot\alpha(R)$.*

Proof. We may factor R into a product of connected orders in polynomial time using Algorithm 6.1 in [32]. Combined with Lemma 4.7.2.7 we may assume R is connected and $\alpha(R) = \mu(R) \cup \{0\}$. Apply Theorem 1.2 in [32] to compute in polynomial time a set X of generators of the group $\mu(R)$. Using Lemma 4.7.9 we may compute a basis $Z \subseteq \mu(R)$ for the subalgebra $\mathbb{Q}\cdot\mu(R)$ of $R \otimes \mathbb{Q}$ as $\mathbb{Q}$-vector space. We claim that $|\Delta| \leq n^{3n/2}$, where

$\Delta = \det((\mathrm{Tr}_{\mathbb{Q}\cdot\mu(R)/\mathbb{Q}}(xy))_{x,y\in Z})$ is the discriminant of $\mathbb{Z}\cdot Z$ and $n = \#Z = \dim_{\mathbb{Q}}(\mathbb{Q}\cdot\mu(R))$. This follows from Hadamard's inequality and the fact that $|\mathrm{Tr}(\zeta)| \leq n$ for $\zeta \in \mu(R)$. In particular, $\#\log_2(\mathbb{Z}\cdot\mu(R)/\mathbb{Z}\cdot Z)$ is polynomially bounded.

First we set $Y = Z$. Then we iterate over $x \in X$ and $y \in Y$ and add xy to Y whenever $xy \notin \mathbb{Z}\cdot Y$. Once $\mathbb{Z}\cdot Y$ stabilizes we have $\mathbb{Z}\cdot Y = \mathbb{Z}\cdot\mu(R)$ and may return Y. Each new element added to Y decreases $\log_2 \#(\mathbb{Z}\cdot\mu(R)/\mathbb{Z}\cdot Y)$ by at least 1, so the cardinality of Y and the number of steps taken in the algorithm are polynomially bounded. Finally, we remark that there is a polynomial upper bound on the lengths of the encodings of the elements of Y, since each element is the product of at most $\#Y$ elements of X and an element of Z. Hence the algorithm runs in polynomial time. □

Example 4.7.12. If R is an order generated as $\mathbb{Z}$-module by $\mu(R)$, then not every set $Y \subseteq \mu(R)$ that generates $\mathbb{Q}R$ as $\mathbb{Q}$-module also generates R as a $\mathbb{Z}$-modules. In particular, Lemma 4.7.9 is not sufficient to prove Proposition 4.7.11. Consider the ring R generated by $\mu(\mathbb{Z}[\mathrm{i}]^2)$. Then $Y = \{(1,1),(1,-1),(\mathrm{i},\mathrm{i}),(-\mathrm{i},\mathrm{i})\}$ is a basis for $\mathbb{Q}R = \mathbb{Q}(\mathrm{i})^2$. However, $(1,\mathrm{i}) = \frac{1}{2}\sum_{y\in Y} y \notin \mathbb{Z}Y$.

Theorem 4.7.13. *There exists a polynomial-time algorithm that, given an order R, decides whether $\alpha(R)$ generates R as a group and if so computes the universal grading of R.*

Proof. Using Algorithm 6.1 in [32] we may factor R into a product of connected orders. By Lemma 4.7.2.3 and Proposition 4.2.6 we may reduce to the case where R be connected, which we will now assume.

We compute $V \subseteq \mu(R)$ as in Proposition 4.7.11. We may then simply decide whether $\mathbb{Z}\cdot V = R$. Next we note that the elements of V are indecomposable by Corollary 5.6 in [34], as multiplication by elements of V is an automorphism of the lattice. We simply construct the graph as in Theorem 2.5.3 for this V and compute its connected components explicitly using Lemma 4.7.8. Thus we obtain the universal orthogonal decomposition of R. The universal grading of R, as constructed in the proof of Theorem 1.3 of [34], can then also be explicitly computed. □

CHAPTER 5

Group rings

5.1 Introduction

This chapter is based on [35], the authors of which include H.W. Lenstra and A. Silverberg. Given a ring A and a (multiplicatively written) group G we may construct the *group ring* $A[G]$, a ring whose additive group is simply the free A-module with basis G, and multiplication is given by $ag \cdot bh = (ab)(gh)$ for $a, b \in A$ and $g, h \in G$. This construction describes a functor

$$\underline{\text{Ring}} \times \underline{\text{Group}} \to \underline{\text{Ring}}.$$

The *Isomorphism Problem for Group Rings* asks to describe the fibers of this map up to isomorphism, i.e. given a ring R, what can one say about the pairs (A, G) such that $A[G] \cong R$? We will refine this question by not just asking for the existence of an isomorphism, but asking for the isomorphism as well, meaning we study the triples (A, G, ϕ) such that $\phi\colon A[G] \to R$ is an isomorphism. We will specialize to the case where A and G, and hence R, are commutative. Equivalently, for non-zero rings R, we study the set

$$\mathcal{D}(R) = \{(A, G) \,|\, \text{subring } A \subseteq R, \text{ subgroup } G \subseteq R^*,\ A[G] = R\},$$

where $A[G] = R$ is to mean that the natural map $A[G] \to R$ is an isomorphism of rings. We say a ring R is *stark* if it is non-zero, commutative and can only be written as a group ring in the trivial way, i.e. $\#\mathcal{D}(R) = 1$. Our main result reads as follows.

Theorem 5.6.4. *Let R be a non-zero reduced order. Then there exist a stark ring A, unique up to ring isomorphism, and a finite abelian group G, unique up to group isomorphism, such that $R \cong A[G]$ as rings.*

Clearly, if A is a ring and I and H are groups, then $A[I \times H]$ and $(A[I])[H]$ are isomorphic as rings. The following result, which is more or less equivalent to Theorem 5.6.4, expresses that, among reduced orders, group rings can only be isomorphic if they are so for this obvious reason.

Theorem 5.6.3. *Suppose A and B are reduced orders and G and H are finite abelian groups. Then the following are equivalent:*

(i) *$A[G] \cong B[H]$ as rings,*
(ii) *there exist an order C and finite abelian groups I and J such that $A \cong C[I]$ and $B \cong C[J]$ as rings and $I \times G \cong J \times H$ as groups.*

If R, A and G are as in Theorem 5.6.4, then A is isomorphic to a subring of R, and G is isomorphic to a subgroup of $\mu(R)$, but as Example 5.5.20 shows, this subring and subgroup need not be uniquely determined. However, the following theorem shows that in an important special case there is

a sense in which the subrings and subgroups that can be used are entirely independent. To a connected reduced order R we associate a group $U^*(R)$ acting on R by ring automorphisms (Definition 5.5.16), and $\mathrm{Aut}(R)$ in turn clearly acts on $\mathcal{D}(R)$.

Theorem 5.5.19. *Let R be a connected reduced order and suppose (A, G), $(B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then $A \cong B$ as rings, $G \cong H$ as groups, and (A, G), (A, H), (B, G) and (B, H) are all in $\mathcal{D}(R)$ and in particular in the same $U^*(R)$-orbit.*

As can be seen in Example 5.5.21, we cannot drop the assumption that R be connected in Theorem 5.5.19.

We will prove Theorem 5.5.19 using the theory of gradings from Chapter 4. For a non-zero commutative ring R and $(A, G) \in \mathcal{D}(R)$ we have a natural grading $\mathcal{R} = \{R_\zeta\}_{\zeta \in \mu(R)}$ where $R_\zeta = A\zeta$ if $\zeta \in G$ and $R_\zeta = 0$ otherwise. If R has a universal grading, we write $\Gamma(R)$ for the group of this grading, and we obtain a homomorphism $f\colon \Gamma(R) \to \mu(R)$ corresponding to $\mathcal{R}$. For a connected reduced order R we also get a homomorphism $d_R\colon \mu(R) \to \Gamma(R)$, the *degree map*, from Proposition 4.6.5. It turns out that the morphisms $f\colon \Gamma(R) \to \mu(R)$ for which the induced grading comes from a group ring are precisely those for which $fd_Rf = f$. We proceed to study d_R by commutative algebra on the Mitchell embedding.

Throughout this chapter, for abelian groups M and N we write the group $\mathrm{Hom}(M, N)$ additively, regardless of the notation used for N. Let A be a connected reduced order and G a finite abelian group. We have a left action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(G, \mu(A))$ given via the restriction $\mathrm{Aut}(A) \to \mathrm{Aut}(\mu(A))$ and a right action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(\Gamma(A), G)$ via the natural map $\mathrm{Aut}(A) \to \mathrm{Aut}(\Gamma(A))$. This is used implicitly in the following theorem, where we describe the automorphism group of a group ring over a stark reduced connected order.

Theorem 5.7.8. *Let A be a stark connected reduced order with degree map $d_A\colon \mu \to \Gamma$ and let G be a finite abelian group. We equip the cartesian product*

$$M = \begin{pmatrix} \mathrm{Aut}(A) & \mathrm{Hom}(G, \mu) \\ \mathrm{Hom}(\Gamma, G) & \mathrm{Aut}(G) \end{pmatrix}$$

of $\mathrm{Aut}(A)$, $\mathrm{Hom}(G, \mu)$, $\mathrm{Hom}(\Gamma, G)$, and $\mathrm{Aut}(G)$ with the following multiplication:

$$\begin{pmatrix} \alpha_1 & s_1 \\ t_1 & \sigma_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & s_2 \\ t_2 & \sigma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 + s_1t_2 & \alpha_1 s_2 + s_1\sigma_2 \\ t_1\alpha_2 + \sigma_1 t_2 & t_1 d_A s_2 + \sigma_1\sigma_2 \end{pmatrix},$$

where the sum in $\mathrm{Aut}(A)$ *is as in Lemma 5.7.7 and the sum in* $\mathrm{Aut}(G)$ *is taken inside* $\mathrm{End}(G)$. *For* $x \in A$ *and* $g \in G$ *write* $\binom{x}{g}$ *for the element* $x \cdot g \in A[G]$. *Then:*

1. M *is a group;*
2. *there is a natural isomorphism* $M \xrightarrow{\sim} \mathrm{Aut}(A[G])$ *such that the evaluation map* $M \times A[G] \to A[G]$ *is given by*

$$\begin{pmatrix} \alpha & s \\ t & \sigma \end{pmatrix} \begin{pmatrix} x \\ g \end{pmatrix} = \begin{pmatrix} \alpha(x) \cdot s(g) \\ t(\gamma) \cdot \sigma(g) \end{pmatrix}$$

for all $g \in G$, $\gamma \in \Gamma$ *and* $x \in A_\gamma$.

We also have an algorithmic result. We call a ring element x *autopotent* if $x^{n+1} = x$ for some $n \geq 1$.

Theorem 5.8.4. *There is an algorithm that, given a non-zero reduced order* R, *computes a stark subring* $A \subseteq R$ *and a subgroup* $G \subseteq \mu(R)$ *such that* $A[G] = R$. *This algorithm runs* (a) *in polynomial time when the additive group of* R *is generated by autopotents, and generally* (b) *in time* $n^{O(m)}$ *where* n *is the length of the input and* m *is the number of minimal prime ideals of* R.

Note that the algorithm runs in polynomial time when m is bounded by a constant. The case $m = 1$ is precisely the case where R is a domain, in which case one necessarily has $A = R$ and $G = 1$. A notable special case for (a) is when R is the product of finitely many group rings over $\mathbb{Z}$. We do not know whether there exists a polynomial-time algorithm that decides whether a given reduced order is stark.

5.2 Modules and decompositions

In this section we gather some results on modules, by which we mean left modules.

Definition 5.2.1. Let R be a ring and M an R-module. We write $\mathrm{Dec}(M)$ for the set

$$\mathrm{Dec}(M) = \{(D, N) \mid D, N \text{ are submodules of } M \text{ with } D \oplus N = M\},$$

or equivalently the set of $\{1, 2\}$-indexed decompositions of M. We equip $\mathrm{Dec}(M)$ with a partial order given by $(D, N) \leq (D', N')$ if and only if there exists a submodule $C \subseteq M$ such that $D = D' \oplus C$ and $N \oplus C = N'$.

Theorem 5.2.2 (Krull–Remak–Schmidt; see Theorem X.7.5 of [30])**.** *Suppose R is a ring and M is an R-module of finite length. Then there exists a decomposition of M into finitely many indecomposable submodules, and such a decomposition is unique up to automorphisms of M and relabeling of the indices.* □

Definition 5.2.3. Let R be a ring, and let $\mathcal{M}$ be a non-empty set of R-modules of finite length. For an R-module M we call an R-module D a *divisor* of M if $M \cong D \oplus N$ for some R-module N. As a consequence of Theorem 5.2.2, there exists up to isomorphism exactly one R-module D that is a divisor of every $M \in \mathcal{M}$ with the property that every R-module that is a divisor of every $M \in \mathcal{M}$ is also a divisor of D; it is called a *greatest common divisor* of the set $\mathcal{M}$. Every such D is of finite length. We say R-modules M and N are *coprime* if the greatest common divisor of $\{M, N\}$ is 0. Likewise, if $\mathcal{M}$ is a finite set of R-modules of finite length, then there exists up to isomorphism exactly one R-module L of which each $M \in \mathcal{M}$ is a divisor with the property that L is a divisor of each R-module of finite length of which each $M \in \mathcal{M}$ is a divisor; it is called a *least common multiple* of $\mathcal{M}$. Every such L is of finite length.

Definition 5.2.4. Suppose R is a ring, M is an R-module, and $h \in \mathrm{End}(M)$. We define the R-modules

$$\lim \mathrm{im}(h) = \bigcap_{n=1}^{\infty} \mathrm{im}(h^n) \quad \text{and} \quad \lim \ker(h) = \bigcup_{n=1}^{\infty} \ker(h^n).$$

Lemma 5.2.5 (Fitting; see Theorem X.7.3 of [30])**.** *Suppose R is a ring, M is an R-module of finite length, and $h \in \mathrm{End}(M)$. Then $M = \lim \mathrm{im}(h) \oplus \lim \ker(h)$, the restriction of h to $\lim \mathrm{im}(h)$ is an automorphism, and the restriction of h to $\lim \ker(h)$ is nilpotent.* □

Lemma 5.2.6. *Suppose R is a ring, M and N are R-modules, and $f\colon M \to N$ and $g\colon N \to M$ are morphisms. Then f restricts to morphisms*

$$i\colon \lim \mathrm{im}(gf) \to \lim \mathrm{im}(fg) \quad \text{and} \quad k\colon \lim \ker(gf) \to \lim \ker(fg).$$

If M and N have finite length, then i is an isomorphism.

Proof. For all $n \geq 1$ we have

$$f(\mathrm{im}((gf)^n)) = \mathrm{im}((fg)^n f) \subseteq \mathrm{im}((fg)^n).$$

Hence $f(\lim \mathrm{im}(gf)) \subseteq \lim \mathrm{im}(fg)$, so i is well-defined. As

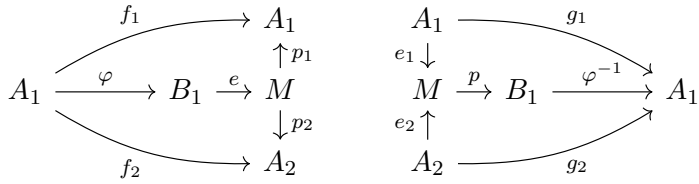
$$f(\ker((gf)^{n+1})) \subseteq \ker(g(fg)^n) \subseteq \ker((fg)^{n+1})$$

for all $n \geq 1$ we also get $f(\lim\ker(gf)) \subseteq \lim\ker(fg)$, so k is well-defined. By symmetry we obtain a restriction $j\colon \lim\operatorname{im}(fg) \to \lim\operatorname{im}(gf)$ of g. Under the finite length assumption both ji and ij are automorphisms by Lemma 5.2.5, hence i is an isomorphism. □

Proposition 5.2.7. *Suppose R is a ring, M is an R-module of finite length, and A_1, A_2, B_1, $B_2 \subseteq M$ are submodules such that A_1 and A_2 are coprime, $A_1 \oplus A_2 = B_1 \oplus B_2 = M$, and $A_1 \cong B_1$. Then $A_1 \oplus B_2 = B_1 \oplus A_2 = M$.*

Note that under the above assumptions it immediately follows that $A_1 \oplus B_2 \cong B_1 \oplus B_2 = M$. This is not equivalent to $A_1 \oplus B_2 = M$, as this concerns a specific isomorphism $A_1 \oplus B_2 \to M$. We need to show that the natural map $B_1 \to M \to A_1$ is an isomorphism.

Proof. From Theorem 5.2.2 it follows that $A_2 \cong B_2$ and thus B_1 and B_2 are coprime as well. By symmetry it therefore suffices to show $B_1 \oplus A_2 = M$. We consider the maps as in the following commutative diagram, where $\varphi\colon A_1 \to B_1$ is an isomorphism, the maps to and from M are the natural inclusions and projections, and the f_i and g_i are defined to make the diagram commute.



Note that $\mathrm{id}_{B_1} = pe$ and $\mathrm{id}_M = e_1p_1 + e_2p_2$, so

$$\begin{aligned}\mathrm{id}_{A_1} &= \varphi^{-1}pe\varphi = \varphi^{-1}p(e_1p_1 + e_2p_2)e\varphi \\ &= \varphi^{-1}pe_1 \cdot p_1e\varphi + \varphi^{-1}pe_2 \cdot p_2e\varphi = g_1f_1 + g_2f_2.\end{aligned}$$

Lemma 5.2.6 shows that $D = \lim\operatorname{im}(g_2f_2) \cong \lim\operatorname{im}(f_2g_2)$, so D is a divisor of both A_1 and A_2 by Lemma 5.2.5. Since A_1 and A_2 are coprime, we must have that $D = 0$ and thus g_2f_2 is nilpotent. We conclude that $g_1f_1 = \mathrm{id}_{A_1} - g_2f_2$ is an automorphism of A_1. Hence f_1 is injective, and since A_1 is of finite length it must be an automorphism. It follows that $p_1e = f_1\varphi^{-1}\colon B_1 \to A_1$ is an isomorphism, so $M = B_1 \oplus A_2$, as was to be shown. □

Definition 5.2.8. Let R be a ring. A class $\mathcal{S}$ of R-modules is *multiplicative* if $0 \in \mathcal{S}$ and for all R-modules M, N and D with $M \cong N \oplus D$ and N, $D \in \mathcal{S}$ one has $M \in \mathcal{S}$. We say a multiplicative class $\mathcal{S}$ of R-modules is *saturated* if

for all $M \in \mathcal{S}$ and all divisors D of M one has $D \in \mathcal{S}$. For a multiplicative class $\mathcal{S}$ of R-modules and an R-module M, write

$$\mathrm{Dec}_{\mathcal{S}}(M) = \{(M_1, M_2) \in \mathrm{Dec}(M) \mid M_2 \in \mathcal{S}\},$$

where $\mathrm{Dec}(M)$ is as in Definition 5.2.1. We equip $\mathrm{Dec}_{\mathcal{S}}(M)$ with the partial order inherited from $\mathrm{Dec}(M)$, and write $\max(\mathrm{Dec}_{\mathcal{S}}(M))$ for its set of maximal elements.

Proposition 5.2.9. *Let R be a ring, let $\mathcal{S}$ be a multiplicative class of R-modules, and let M and N be R-modules. Then:*

1. *if $M \cong N$ and $N \in \mathcal{S}$, then $M \in \mathcal{S}$;*
2. *the set $\mathrm{Dec}_{\mathcal{S}}(M)$ is non-empty.*

Suppose also that $\mathcal{S}$ is saturated and $(A_1, A_2) \in \mathrm{Dec}_{\mathcal{S}}(M)$. Then

3. *one has $(A_1, A_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$ if and only if 0 is the only divisor of A_1 that is in $\mathcal{S}$;*

Suppose also that M is of finite length and $(B_1, B_2) \in \mathrm{Dec}_{\mathcal{S}}(M)$. Then

4. *the set $\max(\mathrm{Dec}_{\mathcal{S}}(M))$ is non-empty and consists of one orbit of $\mathrm{Dec}_{\mathcal{S}}(M)$ under the action of $\mathrm{Aut}(M)$;*
5. *if (A_1, A_2), $(B_1, B_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$, then (A_1, B_2), $(B_1, A_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$.*

Proof. 1. Apply the definition of multiplicative with $D = 0$.

2. The trivial element $(M, 0)$ is in $\mathrm{Dec}_{\mathcal{S}}(M)$.

3. If (A_1, A_2) is maximal but $A_1 = D \oplus B_1$ for some $D \in \mathcal{S}$ and some B_1, then $(A_1, A_2) \leq (B_1, A_2 \oplus D) \in \mathrm{Dec}_{\mathcal{S}}(M)$ and thus $A_2 = A_2 \oplus D$ and $D = 0$. Conversely, suppose 0 is the only divisor of A_1 that is in $\mathcal{S}$ and $(A_1, A_2) \leq (B_1, B_2)$. Then there is some C such that $A_1 = B_1 \oplus C$ and $B_2 = A_2 \oplus C$. Since $\mathcal{S}$ is saturated we have $C \in \mathcal{S}$, and since C is a divisor of A_1 we must have that $C = 0$. Hence $(A_1, A_2) = (B_1, B_2)$ is maximal.

4. Let $M = \bigoplus_{i \in I} M_i$ with each M_i indecomposable. If A_2, respectively A_1, is the direct sum of those M_i that are, respectively are not, in $\mathcal{S}$, then (A_1, A_2) is in $\mathrm{Dec}_{\mathcal{S}}(M)$ and it is maximal by 3. If (B_1, B_2) is also maximal, then B_2, respectively B_1, is a direct sum of indecomposables that are, respectively are not, in $\mathcal{S}$; this follows from the definition of $\mathrm{Dec}_{\mathcal{S}}(M)$ and from 3. Since together these decompositions give a decomposition of M into indecomposables, Theorem 5.2.2 implies that $A_1 \cong B_1$ and $A_2 \cong B_2$, so (B_1, B_2) belongs to the $\mathrm{Aut}(M)$-orbit of (A_1, A_2). Because the action of $\mathrm{Aut}(M)$ preserves the partial order, this orbit is conversely contained in $\max(\mathrm{Dec}_{\mathcal{S}}(M))$.

5. By 3 we have that A_1 and A_2 are coprime and by 4 we have $A_1 \cong B_1$ and $A_2 \cong B_2$. We may conclude from Proposition 5.2.7 that $(A_1, B_2), (B_1, A_2) \in \mathrm{Dec}_{\mathcal{S}}(M)$. Applying 3 again we may conclude they are maximal. □

5.3 Morphisms as modules

In this section we will interpret a morphism of (finite) abelian groups as a (finite length) module, as expressed by Proposition 5.3.2. We will then study decompositions of this module and what this decomposition corresponds to in terms of the original morphism. This will enable us in the next section to apply the Krull–Remak–Schmidt theorem to morphisms of finite abelian groups.

We write $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$ for the ring of lower-triangular 2×2 matrices with integer coefficients, $\underline{\mathrm{Ab}}$ for the category of abelian groups, and $\underline{\mathrm{ab}}$ for the category of finite abelian groups.

Definition 5.3.1. Let $\mathcal{C}$ be a category. We define the *arrow category* of $\mathcal{C}$, written $\mathrm{Arr}(\mathcal{C})$, to be the category where the objects are the morphisms of $\mathcal{C}$ and for objects $f\colon A \to B$ and $g\colon C \to D$ the morphisms from f to g are the pairs $(\alpha, \beta) \in \mathrm{Hom}_{\mathcal{C}}(A, C) \times \mathrm{Hom}_{\mathcal{C}}(B, D)$ such that $\beta f = g\alpha$.

The following proposition can be thought of as an explicit instance of Mitchell's embedding theorem for abelian categories.

Proposition 5.3.2. *There is an equivalence of categories, specified in the proof, between the category* $\mathrm{Arr}(\underline{\mathrm{Ab}})$ *and the category of* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$*-modules. This equivalence restricts to an equivalence of categories between the subcategory* $\mathrm{Arr}(\underline{\mathrm{ab}})$ *and the subcategory of* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$*-modules of finite length.*

Proof. Write $\mathcal{M}$ for the category of $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules. We will define functors

$$F\colon \mathrm{Arr}(\underline{\mathrm{Ab}}) \to \mathcal{M} \quad \text{and} \quad G\colon \mathcal{M} \to \mathrm{Arr}(\underline{\mathrm{Ab}})$$

such that FG and GF are naturally isomorphic to the identity functors of their respective categories. For an object $f\colon A \to B$ we take $F(f)$ to be $A \oplus B$, where the $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure is given by

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa \\ yf(a) + zb \end{pmatrix},$$

for $x, y, z \in \mathbb{Z}$, $a \in A$ and $b \in B$. For a $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module M we take $G(M)$ to be the morphism $E_{11}M \to E_{22}M$ given by multiplication with E_{21}, where E_{ij} is the 2×2 matrix having a 1 at position (i, j) and zeros elsewhere. The remainder of this proposition is a straightforward verification. □

Definition 5.3.3. Write $\mathcal{I}$ for the class of $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules that correspond to isomorphisms under the equivalence of categories of Proposition 5.3.2.

One readily checks that the class $\mathcal{I}$ is multiplicative and saturated in the sense of Definition 5.2.8. We observe that a $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module M belongs to $\mathcal{I}$ if and only if its $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure can be extended to a $\left(\begin{smallmatrix}\mathbb{Z} & \mathbb{Z}\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure. This fact will not be needed, and we omit the proof.

Remark 5.3.4. Using the equivalence of categories of Proposition 5.3.2, one can translate terminology related to modules into terminology about morphisms of abelian groups. We briefly go through what is most relevant to us:

1. If $f\colon A \to B$ is a morphism of abelian groups, then a *submodule* of the $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module corresponding to f corresponds to a *restriction* of f, i.e. a morphism $f'\colon A' \to B'$ where $A' \subseteq A$ and $B' \subseteq B$ are subgroups and $f'(a') = f(a') \in B'$ for all $a' \in A'$.

2. For morphisms $f\colon A \to B$ and $g\colon C \to D$ of abelian groups and for $r = (\alpha, \beta) \in \mathrm{Hom}(f, g)$, the image $\mathrm{im}(r)$ equals the restriction $\mathrm{im}(\alpha) \to \mathrm{im}(\beta)$ of g, and the kernel $\ker(r)$ equals the restriction $\ker(\alpha) \to \ker(\beta)$ of f.

3. If $(f_i)_{i\in I}$ is a family of morphisms $f_i\colon A_i \to B_i$ of abelian groups, then we write $\bigoplus_{i\in I} f_i$ for the natural map $\bigoplus_{i\in I} A_i \to \bigoplus_{i\in I} B_i$ and we write f/f_i for the induced map $A/A_i \to B/B_i$. One verifies that $\bigoplus_{i\in I} f_i$ corresponds to the coproduct of the $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules that the f_i correspond to. If $f\colon A \to B$ is a morphism and $f_i\colon A_i \to B_i$ is a family of restrictions of f then, just as we do for modules, we will write $\bigoplus_{i\in I} f_i = f$ if the natural map $\bigoplus_{i\in I} f_i \to f$ is an isomorphism.

4. For a morphism $f\colon A \to B$, the set $\mathrm{Dec}(f)$ is the set of all pairs (f_0, f_1) of restrictions of f such that $f_0 \oplus f_1 = f$, which is a partially ordered set as in Definition 5.2.1. The set $\mathrm{Dec}_{\mathcal{I}}(f)$ is the set of $(f_0, f_1) \in \mathrm{Dec}(f)$ such that f_1 is an isomorphism.

Definition 5.3.5. Let $f\colon A \to B$ be a morphism of abelian groups. We say f is *nil* if for all morphisms $g\colon B \to A$ the element $fg \in \mathrm{End}(B)$ is nilpotent, or equivalently $gf \in \mathrm{End}(A)$ is nilpotent.

Lemma 5.3.6. *Suppose $f\colon A \to B$ is a morphism of abelian groups.*

1. *If f is a nil isomorphism, then $A = B = 0$.*
2. *If f is nil, then every divisor of f is nil.*

Proof. 1. If f is a nil isomorphism, then $ff^{-1} = \mathrm{id}_B$ is nilpotent, hence $A = B = 0$. 2. Suppose $f = f_0 \oplus f_1$ for morphisms $f_i\colon A_i \to B_i$. Let $g_1\colon B_1 \to A_1$ be a morphism. Then $g = g_1 \oplus 0 : B_1 \oplus B_2 \to A_1 \oplus A_2$ is a morphism such that fg is nilpotent if and only if $f_1 g_1$ is nilpotent. Hence f_1 is nil if f is nil. □

Lemma 5.3.7. *Let $f\colon A \to B$ be a morphisms of finite abelian groups.*

1. *Then f is nil if and only if all isomorphisms dividing f are trivial.*
2. *Suppose $f = f_0 \oplus f_1$. Then f is nil if and only if f_0 and f_1 are nil.*
3. *We may uniquely, up to automorphisms of f, write $f = f_0 \oplus f_1$ with f_0 nil and f_1 an isomorphism.*
4. *Suppose $(f_0, f_1) \in \mathrm{Dec}_{\mathcal{I}}(f)$. Then (f_0, f_1) is maximal if and only if f_0 is nil.*

Proof. 1. If f is nil, then every divisor is nil and the only nil isomorphism is trivial by Lemma 5.3.6. Suppose all isomorphisms dividing f are trivial. Let $g\colon B \to A$ be a morphism. Then $\lim \mathrm{im}\, fg = 0$ by Lemma 5.2.6, otherwise the restriction of f to $\lim \mathrm{im}\, fg \to \lim \mathrm{im}\, gf$ is an isomorphism and a non-trivial divisor of f. Hence fg is nilpotent by Lemma 5.2.5 and f is nil.

Both 2 and 3 follow from 1 combined with Theorem 5.2.2, while 4 follows from 1 and Proposition 5.2.9.3. □

5.4 The group U^*

In this section we fix a morphism $d\colon A \to B$ of abelian groups. We will define a group U^* that acts on d and study some of its properties.

Definition 5.4.1. For $f, g \in \mathrm{Hom}(B, A)$, we define $f \star g = fdg$ and extend $\star$ to a ring multiplication on the additive group $Q = Q(d) = \mathbb{Z} \oplus \mathrm{Hom}(B, A)$ by

$$(m, f) \star (n, g) = (mn, mg + nf + fdg)$$

for $m, n \in \mathbb{Z}$ and $f, g \in \mathrm{Hom}(B, A)$. We define the multiplicative monoid

$$U = U(d) = 1 + \mathrm{Hom}(B, A) \subseteq \mathbb{Z} \oplus \mathrm{Hom}(B, A) = Q$$

and write $U^* = U^*(d) = U \cap Q^*$.

It is easy to check that Q is indeed a ring with unit element $1 = (1, 0)$, and that the projection map $Q \to \mathbb{Z}$ is a ring homomorphism with kernel $\mathrm{Hom}(B, A)$. The inverse image of 1 equals U, and U^* is a group because it is the kernel of the induced group homomorphism $Q^* \to \mathbb{Z}^*$. The following lemma is easy to verify.

Lemma 5.4.2. *We have a ring homomorphism $q\colon Q \to \mathrm{End}(d)$ defined by sending 1 to the identity id_d and $f \in \mathrm{Hom}(B, A)$ to (fd, df). It restricts to a group homomorphism $U^* \to \mathrm{Aut}(d)$.* □

Remark 5.4.3. Note that A and B are $\mathrm{End}(d)$-modules. The map q makes A and B into Q-modules in such a way that d is Q-linear.

In the following results, we use the terminology from Remark 5.3.4. We let U^* act on $\mathrm{Dec}(d)$ via the map $U^* \to \mathrm{Aut}(d)$ from Lemma 5.4.2.

Lemma 5.4.4. *Let $d_i\colon A_i \to B_i$ with $i \in \{-1, 0, 1\}$ be restrictions of d such that (d_0, d_1) and (d_0, d_{-1}) belong to $\mathrm{Dec}(d)$, and suppose that d_0 or d_1 is an isomorphism. Then $(d_0, d_{-1}) \in U^* \cdot (d_0, d_1)$.*

Proof. We have $A_0 \oplus A_1 \cong A \cong A_0 \oplus A_{-1}$. Hence the map $A_1 \to A_{-1}$ given by $x \mapsto x_{-1}$ where $x = x_0 + x_{-1}$ with $x_i \in A_i$ is an isomorphism. Similarly, we have a natural isomorphism $g_1\colon d_1 \to d/d_0 \to d_{-1}$, and its extension $g = \mathrm{id}_{d_0} \oplus g_1 \in \mathrm{Aut}(d)$ maps (d_0, d_1) to (d_0, d_{-1}). Letting $r = \mathrm{id}_d - g \in \mathrm{End}(d)$, then $r(d_1) \subset d_0$ and $r(d_0) = 0$, so $r^2 = 0$. We first construct $f \in \mathrm{Hom}(B, A)$ that maps to r under $q\colon Q \to \mathrm{End}(d)$. Write $r = (r_A, r_B)$ with $r_A \in \mathrm{End}(A)$ and $r_B \in \mathrm{End}(B)$. Since d_0 or d_1 is invertible, there exists $f_1\colon B_1 \to A_0$ such that the diagram

$$\begin{array}{ccc} A_1 & \xrightarrow{d_1} & B_1 \\ {\scriptstyle r_A}\downarrow & \swarrow_{f_1} & \downarrow{\scriptstyle r_B} \\ A_0 & \xrightarrow[d_0]{} & B_0 \end{array}$$

commutes. Then $f = 0 \oplus f_1$ with $0\colon B_0 \to A_1$ satisfies $(fd, df) = r$, so f does map to r under $q\colon Q \to \mathrm{End}(d)$. From $f \star f \star f = fdfdf = r_A^2 f = 0$ we see that f is nilpotent, so the element $1 - f \in U$ belongs to U^*. Since $1 - f$ maps to $\mathrm{id}_d - r = g$ via q, it sends (d_0, d_1) to (d_0, d_{-1}). □

The proof of the following proposition, which can be considered a sharpening of Proposition 5.2.9.4 when $R = \left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix}\right)$, is the main reason for considering d as a module.

Proposition 5.4.5. *Assume A and B are finite. Then the set of maximal elements of $\mathrm{Dec}_{\mathcal{I}}(d)$ equals one orbit of $\mathrm{Dec}_{\mathcal{I}}(d)$ under the action of U^*.*

Proof. By Proposition 5.3.2 we may apply Proposition 5.2.9.4. Thus it suffices to show that any two maximal elements $(d_0, d_1), (e_0, e_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ are in the same U^*-orbit. Recall that $(d_0, e_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ by Proposition 5.2.9.5. Applying Lemma 5.4.4 we obtain $(d_0, e_1) \in U^* \cdot (d_0, d_1)$ since d_1 is an isomorphism, and $(e_0, e_1) \in U^* \cdot (d_0, e_1)$ since e_1 is an isomorphism. Thus $(e_0, e_1) \in U^* \cdot (d_0, e_1) = U^* \cdot (d_0, d_1)$. □

5.5 The degree map

In this section we will prove facts about group rings and interpret them as a special case of gradings. We will rely heavily on [34].

Definition 5.5.1. For a ring A and a group G the *group ring* $A[G]$ is an A-algebra with as underlying group the free A-module with basis G where multiplication is given by

$$\Big(\sum_{g\in G} a_g g\Big)\cdot\Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G}\Big(\sum_{h\in G} a_h b_{h^{-1}g}\Big)g.$$

We associate with $A[G]$ its natural grading $\{Ag\}_{g\in G}$.

First we observe that that the properties of being reduced and being connected are preserved under construction of group rings, as a consequence of Theorem 1.5 in [34] or Theorem 4.6.6.

Corollary 5.5.2. *Let A be an order and G a finite abelian group. Then:*

1. *We have* $\mathrm{nil}(A[G]) = \mathrm{nil}(A)[G]$*, and A is reduced if and only if $A[G]$ is reduced;*
2. *We have* $\mathrm{Id}(A[G]) = \mathrm{Id}(A)$*, and A is connected if and only if $A[G]$ is connected;*
3. *If A is connected, then $\mu(A[G]) = \mu(A)\times G$.* □

Definition 5.5.3. Let R be a reduced order. By Theorem 1.3 in [34] or Theorem 6.21 in [17] the ring R has a universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ (see Definition 4.2.1). We will write $\Gamma(R)$ for this group Γ.

Remark 5.5.4. If R and R' are commutative rings that have universal gradings, then any ring isomorphism $R\to R'$ induces a group isomorphism $\Gamma(R)\to\Gamma(R')$, so $\Gamma(R)$ behaves functorially under ring isomorphisms; in particular, the group $\mathrm{Aut}(R)$ of ring automorphisms of R acts in a natural way on $\Gamma(R)$.

Lemma 5.5.5. *Let R be a connected reduced order and let $\{R_\gamma\}_{\gamma\Gamma(R)}$ be its universal grading. Then there exists a morphism of finite abelian groups $d\colon \mu(R)\to\Gamma(R)$ that sends $\zeta\in\mu(R)$ to the unique $\gamma\in\Gamma(R)$ such that $\zeta\in R_\gamma$.*

Proof. The group $\Gamma(R)$ is finite by Theorem 1.3 of [34], and $\mu(R)$ is finite by Lemma 3.3.ii in [32]. By Theorem 1.5.iii of [34], if $\zeta\in\mu(R)$, then there exists a $\gamma\in\Gamma(R)$ such that $\zeta\in R_\gamma$. The element γ is unique, since $R_\gamma\cap R_\delta = 0$ for all $\gamma\neq\delta$. That d is a homomorphism follows from the definitions. □

Definition 5.5.6. For a connected reduced order R we call the map $d\colon \mu(R) \to \Gamma(R)$ from Lemma 5.5.5 the *degree map* of R.

The above definition depends on the choice of universal grading. However, the universal grading of R is uniquely unique. Moreover, the proof of Theorem 1.3 of [34], which states that a reduced order has a universal grading, exhibited an explicit canonical choice of universal grading. Thus we can confidently refer to *the* degree map of a connected reduced order. We now describe the degree map $d_{A[G]}$ of $A[G]$.

Proposition 5.5.7. *Let A be a connected reduced order and let G be a finite abelian group. Let $(\Gamma(A), (A_\gamma)_\gamma)$ and $(\Gamma(A[G]), (R_\gamma)_\gamma)$ be the universal grading of A and $A[G]$ respectively. Then*

1. *we have $\Gamma(A[G]) = \Gamma(A) \times G$, and $R_{(\gamma,g)} = A_\gamma \cdot g$ for all $\gamma \in \Gamma(A)$ and $g \in G$;*
2. *if we identify $\mu(A[G])$ with $\mu(A) \times G$ as in Proposition 5.5.2.iii, then the degree map $d_{A[G]}\colon \mu(A) \times G \to \Gamma(A) \times G$ equals $d_A \times \mathrm{id}_G$;*
3. *we have $\Gamma(A) = \langle \gamma \in \Gamma(A[G]) : R_\gamma \cap A \neq 0 \rangle$.*

Proof. Let $\mathcal{A} = (\Gamma(A), (A_\gamma)_\gamma)$ and $\mathcal{R} = (\Gamma(A[G]), (R_\gamma)_\gamma)$ be the universal gradings of A and $A[G]$ respectively and write $\mathcal{A}[G] = (\Gamma(A) \times G, (A_\gamma \cdot g)_{(\gamma,g)})$. By universality there exists a unique morphism of gradings $\varphi\colon \mathcal{R} \to \mathcal{A}[G]$, which by Definition 4.2.1 is a group homomorphism $\Gamma(A[G]) \to \Gamma(A) \times G$, and we will show that it is an isomorphism. Let $\pi\colon \Gamma(A) \times G \to G$ be the projection and $\Delta = \ker(\pi\varphi)$. For $g \in G$ we have $g \in R_{d_{A[G]}(g)}$ and $g \in A_1 \cdot g$, so $\pi\varphi d_{A[G]}$ is the identity on G. It follows that $\Gamma(A[G]) = \Delta \times G$. Then $\mathcal{R}_A = (\Delta, (R_\delta)_\delta)$ is a grading of A, and φ restricts to a morphism of gradings $\varphi'\colon \mathcal{R}_A \to \mathcal{A}$ with $\varphi = \varphi' \times \mathrm{id}_G$. With $\Delta' = \langle \delta \in \Delta : R_\delta \neq 0 \rangle$ we have

$$\bigoplus_{(\delta,g)\in\Delta'\times G} R_\delta \cdot g = A[G],$$

so by Lemma 4.2.4.5 we obtain $\Delta' \times G = \Gamma(A[G]) = \Delta \times G$. Hence $\Delta' = \Delta$, so $\mathcal{R}_A$ is universal by Lemma 4.2.4.4. It follows that φ' and hence φ is an isomorphism, proving 1. Now 2 and 3 follow by inspection. □

Proposition 5.5.7.2 expresses the degree map of $A[G]$ in terms of G and the degree map of A, but we will mainly use it in the opposite direction. Specifically, for a connected reduced order R, an element $(A, G) \in \mathcal{D}(R)$ corresponds to a certain decomposition $(d_A, \mathrm{id}_G) \in \mathrm{Dec}_{\mathcal{I}}(d)$ of the degree map d of R, as defined in Definition 5.2.1 and Definition 5.3.3.

Example 5.5.8. Note that the conclusion to Proposition 5.5.7 becomes false when we drop the assumption that A be connected.

Let $A = \mathbb{Z} \times \mathbb{Z}$, which has a trivial universal grading $\mathcal{A}$ by Proposition 4.2.6.2, and let G be a non-trivial finite abelian group. Because $A[G] \cong \mathbb{Z}[G] \times \mathbb{Z}[G]$ we get $\Gamma(A[G]) = G \times G$ by Proposition 4.2.6.2, while $\mathcal{A}[G]$ is G-indexed. Hence $\mathcal{A}[G]$ is not universal.

Definition 5.5.9. Suppose R is a commutative ring. We define the set

$$\mathcal{D}(R) = \left\{ (A, G) \;\middle|\; \begin{array}{l} A \subseteq R \text{ is a subring,} \\ G \subseteq R^* \text{ is a subgroup,} \\ A[G] = R \end{array} \right\}$$

which we equip with a partial order $\leq$ given by $(B, H) \leq (A, G)$ if and only if $H \subseteq G$ and $B \supseteq A$.

Lemma 5.5.10. *Suppose R is a non-zero order. Then for each $(A, G) \in \mathcal{D}(R)$ the order of G is at most the rank of R as $\mathbb{Z}$-module, and $\mathcal{D}(R)$ contains a maximal element.*

Proof. By definition of $\mathcal{D}(R)$ the elements of G are linearly independent, from which the first claim follows. We have $(R, 1) \in \mathcal{D}(R)$, so $\mathcal{D}(R)$ is not empty. Thus if $(A, G) \in \mathcal{D}(R)$ and $\#G$ is maximal, then (A, G) is a maximal element of $\mathcal{D}(R)$. □

Lemma 5.5.11. *Let R be a connected order and let $(A, G), (B, H) \in \mathcal{D}(R)$. Then $(B, H) \leq (A, G)$ if and only if there exists some subgroup $J \subseteq \mu(R)$ such that $B = A[J]$ and $G = J \times H$.*

Proof. The implication ($\Leftarrow$) is obvious, so it remains to prove ($\Rightarrow$). By Lemma 5.5.10 the group H is finite, and by Proposition 5.5.2.3 the multiplication map $\mu(B) \times H \to \mu(R)$ is an isomorphism. Since the inverse image of G is $J \times H$, we have $G = J \times H$. Thus $A[J][H] = A[J \times H] = A[G] = B[H]$ and therefore $A[J] = B$. □

Example 5.5.12. The conclusion to Lemma 5.5.11 does not hold in general for non-connected orders. Let p be prime and let $G = C_p \times C_p$ with C_p a group of order p. Then G is a 2-dimensional $\mathbb{F}_p$-vector space and thus there are precisely $p + 1$ subgroups $H_0, \ldots, H_p$ of G of order p. We have $H_i \cdot H_j = G$ if and only if $i \neq j$. Let $R = \mathbb{Z}[G] \times \mathbb{Z}[G]$ and let $\Delta \colon G \to \mu(R)$

be the map given by $g \mapsto (g, g)$. Now consider the elements $(\mathbb{Z}\times\mathbb{Z}, \Delta(G)) \geq (\mathbb{Z}[H_0] \times \mathbb{Z}[H_1], \Delta(H_p))$ of $\mathcal{D}(R)$. As Proposition 5.5.2 implies

$$\begin{aligned}\mu(\mathbb{Z}[H_0] \times \mathbb{Z}[H_1]) &= \mu(\mathbb{Z}[H_0]) \times \mu(\mathbb{Z}[H_1]) \\ &= \{(\pm h_0, \pm h_1) : h_0 \in H_0,\, h_1 \in H_1\},\end{aligned}$$

we get $J = \Delta(G) \cap \mu(\mathbb{Z}[H_0] \times \mathbb{Z}[H_1]) = 1$ and $(\mathbb{Z} \times \mathbb{Z})[J] \neq \mathbb{Z}[H_0] \times \mathbb{Z}[H_1]$.

Recall that we say a commutative ring R is *stark* if there do not exist a ring A and a non-trivial group G such that R is isomorphic to the group ring $A[G]$, or equivalently for R non-zero, if $\#\mathcal{D}(R) = 1$.

Lemma 5.5.13. *Let R be a non-zero commutative ring and let $(A, G) \in \mathcal{D}(R)$. If (A, G) is maximal, then A is stark. When R is a connected order, the converse also holds.*

Proof. If $A = B[J]$ for some $J \subseteq \mu(A)$, then $(A, G) \leq (B, J \times G) \in \mathcal{D}(R)$. Hence if (A, G) is maximal we have $(A, G) = (B, J\times G)$ and thus $J = 1$, so A is stark. For connected orders, the converse follows from Lemma 5.5.11. □

Note that from Theorem 5.6.3 it follows that maximality of $(A, G) \in \mathcal{D}(R)$ for a non-zero reduced order R is equivalent to A being stark even when R is not connected. However, we have not proved this yet.

Remark 5.5.14. Let R be a connected reduced order with universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ and degree map $d\colon \mu \to \Gamma$. Note that the group $\mathrm{Aut}(R)$ acts on the category of gradings of R. Under this action, $\sigma \in \mathrm{Aut}(R)$ sends $\{R_\gamma\}_{\gamma\in\Gamma}$ to $\{\sigma(R_\gamma)\}_{\gamma\in\Gamma}$, which is again a universal grading of R. Thus, by universality this induces a unique isomorphism $f\colon \Gamma \to \Gamma$ between them. It follows that $\mathrm{Aut}(R)$ acts on Γ. Clearly $\mathrm{Aut}(R)$ acts on $\mu(R)$, and it is then easy to see that the combination of these actions gives an action $\mathrm{Aut}(R) \to \mathrm{Aut}(d)$. Through this map the group $\mathrm{Aut}(R)$ acts on $\mathrm{Dec}_{\mathcal{I}}(d)$.

Theorem 5.5.15. *Let R be a connected reduced order. We have a natural isomorphism*

$$\mathcal{D}(R) \to \mathrm{Dec}_{\mathcal{I}}(d_R)$$

of partially ordered $\mathrm{Aut}(R)$-sets given by

$$\begin{aligned}(A, G) &\mapsto (d_A\colon \Gamma(A) \to \mu(A);\ \mathrm{id}_G\colon G \to G) \\ \Big(\bigoplus_{\gamma\in\Gamma_0} R_\gamma, \mu_1\Big) &\leftarrow\!\shortmid (d_0\colon \Gamma_0 \to \mu_0;\ d_1\colon \Gamma_1 \to \mu_1),\end{aligned}$$

where the first map is as induced by Proposition 5.5.7.2 and $\{R_\gamma\}_{\gamma\in\Gamma(R)}$ is the universal grading of R.

Proof. That the maps are well-defined and mutually inverse can be easily deduced from Proposition 5.5.7. Both maps are functorial, and thus commute with the action of $\mathrm{Aut}(R)$. That they respect the partial order follows from Lemma 5.5.11. □

Definition 5.5.16. For a connected reduced order R with degree map $d\colon \mu \to \Gamma$ we write $U^*(R)$ or $U^*(d)$ for the group as in Definition 5.4.1.

Lemma 5.5.17. *Let R be a connected reduced order with degree map d. Let $\varphi\colon U^*(d) \to \mathrm{Aut}(d)$ be as in Lemma 5.4.2 and $\chi\colon \mathrm{Aut}(R) \to \mathrm{Aut}(d)$ as in Remark 5.5.14. We then have a commutative diagram*

$$\begin{array}{ccc} & U^*(d) & \\ {\scriptstyle\psi}\swarrow & & \searrow{\scriptstyle\varphi} \\ \mathrm{Aut}(R) & \xrightarrow{\quad\chi\quad} & \mathrm{Aut}(d) \end{array}$$

where ψ is a morphism given in terms of the universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ of R by $1 + f \mapsto (x \in R_\gamma \mapsto f(\gamma) \cdot x)$.

Proof. Let $1 + f, 1 + g \in U^*$ and recall that their product equals $(1 + f) \star (1 + g) = 1 + f + g + fdg$ in U^*. It is easy to see that $\psi(1 + f)$ is an endomorphism of R. For $\gamma \in \Gamma$ we have

$$\begin{aligned} x \in R_\gamma &\xmapsto{\psi(1+g)} g(\gamma) \cdot x \in R_{dg(\gamma)} \cdot R_\gamma \subseteq R_{dg(\gamma)\cdot\gamma} \\ &\xmapsto{\psi(1+f)} f(dg(\gamma) \cdot \gamma) \cdot g(\gamma) \cdot x = f(\gamma)g(\gamma)fdg(\gamma) \cdot x, \end{aligned}$$

so indeed $\psi(1+f)\circ\psi(1+g) = \psi((1+f)\star(1+g))$. It follows that $\psi(1+f) \in \mathrm{Aut}(R)$ and that ψ is a morphism.

Let $1+f \in U^*$ and write $F = \psi(1+f)$. For $\zeta \in \mu$ we have $F(\zeta) = f(d\zeta)\zeta$, so $F|_{\mu(R)} = \mathrm{id}_\mu + fd$. For $\gamma \in \Gamma$ and $x \in R_\gamma$ non-zero we have $F(x) = f(\gamma) \cdot x$, so the induced action on Γ sends γ to $df(\gamma)\gamma$. Hence $1 + f$ gets sent to $\mathrm{id}_\Gamma + df$, since $\{\gamma \in \Gamma \mid R_\gamma \neq 0\}$ is a generating set of Γ by Lemma 4.2.4.5. We conclude that $\chi(\psi(1 + f)) = (\mathrm{id}_\mu + fd, \mathrm{id}_\Gamma + df) = \varphi(1 + f)$, as was to be shown. □

Example 5.5.18. The map $\psi\colon U^* \to \mathrm{Aut}(R)$ need not be injective, even when R is stark. Consider the subring $R = \mathbb{Z} \cdot (1, 1) + 2S$ of $S = \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}]$ where $\mathrm{i}^2 = -1$, which is clearly connected, reduced, and has $\mu(R) = \{\pm 1\} \times \{\pm 1\}$. Let $\Gamma = \mu(R)$ and write

$$R_{1,1} = R \cap (\mathbb{Q} \times \mathbb{Q}) = \mathbb{Z} \cdot (1, 1) + \mathbb{Z} \cdot (1, -1),$$

$$R_{1,-1} = 2\mathrm{i} \cdot (\mathbb{Z} \times \{0\}), \quad R_{-1,1} = 2\mathrm{i} \cdot (\{0\} \times \mathbb{Z}), \quad R_{-1,-1} = 0.$$

Then $(\Gamma, (R_\gamma)_\gamma)$ is the universal grading of R. Consider the identity $\mathrm{id}\colon \Gamma \to \mu$. Note that $2\,\mathrm{id} = 0$ and $d = 0$, hence $(1+\mathrm{id})^2 = 1$ in Q and so $1+\mathrm{id} \in U^*$. Moreover, $\psi(1+\mathrm{id})$ is the identity of R, so ψ is not injective. To see R is stark, we can apply Lemma 5.7.1 below since $d = 0$.

Note that $U^*(R)$ acts on $\mathcal{D}(R)$ through $\mathrm{Aut}(R)$.

Theorem 5.5.19. *Let R be a connected reduced order and suppose (A, G), $(B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then $A \cong B$ as rings, $G \cong H$ as groups, and (A, G), (A, H), (B, G) and (B, H) are all in $\mathcal{D}(R)$ and in particular in the same $U^*(R)$-orbit.*

Proof. Let d be the degree map of R and let $\Phi\colon \mathrm{Dec}_{\mathcal{I}}(d) \to \mathcal{D}(R)$ be the map from Theorem 5.5.15. Suppose $(A, G), (B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then (A, G) and (B, H) are maximal elements of $\mathcal{D}(R)$ by Lemma 5.5.13, and thus $\Phi(A, G) = (d_0, d_1)$ and $\Phi(B, H) = (e_0, e_1)$ are maximal in $\mathrm{Dec}_{\mathcal{I}}(d)$. Then by Proposition 5.2.9.5 and Proposition 5.4.5 all of (d_0, d_1), (d_0, e_1), (e_0, d_1), and (e_0, e_1) are maximal and in the same U^*-orbit. Note that the action of U^* on $\mathrm{Dec}_{\mathcal{I}}(d)$ factors through $\mathrm{Aut}(R)$ by Lemma 5.5.17, so Φ respects the action of U^*. Since $\Phi(d_0, e_1) = (A, H)$ and $\Phi(e_0, d_1) = (B, G)$, the last assertion of the theorem follows. As a consequence, (A, G) and (B, H) are in the same orbit of $\mathrm{Aut}(R)$, so $A \cong B$ as rings and $G \cong H$ as groups. □

Example 5.5.20. Let $C_2 = \langle\sigma\rangle$ be a group of order 2 and let $R = \mathbb{Z}[\mathrm{i}][C_2]$, where $\mathrm{i}^2 = -1$. We will compute $\mathcal{D}(R)$.

By Proposition 5.5.2 the ring R is both reduced and connected. With $\Gamma = (\mathbb{Z}/2\mathbb{Z})^2$, consider the grading $(\Gamma, (R_{a,b})_{(a,b)})$ of R with $R_{a,b} = \mathbb{Z}\mathrm{i}^a\sigma^b$, where although i^a is not well-defined, $\mathbb{Z}\mathrm{i}^a$ is. Since a universal grading exists, and all $R_{a,b}$ are of rank 1 over $\mathbb{Z}$, this must be the universal grading. Let $d\colon \mu \to \Gamma$ be the degree map. It follows from Proposition 5.5.2.3 that $\mu = \langle \mathrm{i}, \sigma\rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We will first compute $\mathrm{Dec}_{\mathcal{I}}(d)$. Suppose we have $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ with $d_i\colon \mu_i \to \Gamma_i$. If $\mu_1 = 1$, then $d_0 = d$, and (d_0, d_1) corresponds via Theorem 5.5.15 to the trivial element $(R, 1)$ of $\mathcal{D}(R)$. Now suppose $\mu_1 \neq 1$. Since d_1 is an isomorphism, the groups μ_1 and Γ_1 are isomorphic, so μ_1 is isomorphic to a direct summand of μ and of Γ. Since $\mathbb{Z}/2\mathbb{Z}$ is the greatest common divisor of μ and Γ as $\mathbb{Z}$-modules (in the sense of Definition 5.2.3), we have that μ_1 is a direct summand of μ isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It follows that $\mu_1 = \langle(-1)^b\sigma\rangle$ for some $b \in \mathbb{Z}/2\mathbb{Z}$, and the corresponding group Γ_1 equals $\langle(0, 1)\rangle$ in both cases. On the other hand $\mu_0 = \langle \mathrm{i}\sigma^a\rangle$ for some $a \in (\mathbb{Z}/2\mathbb{Z})$ since it must be a cyclic group of order 4,

and $\Gamma_0 = \langle (1, a) \rangle$. Upon inspection, all pairs (a, b) do indeed give a decomposition $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$. The rings corresponding to the possible d_0 are $\mathbb{Z}[\mathrm{i}\sigma^a]$, and the groups corresponding to d_1 are $\langle (-1)^b \sigma \rangle$. This gives

$$\mathcal{D}(R) = \{(R, 1)\} \cup \{(\mathbb{Z}[\mathrm{i}\sigma^a], \langle (-1)^b \sigma \rangle) \mid a, b \in \mathbb{Z}/2\mathbb{Z}\}.$$

Interesting to note is that, although $(\mathbb{Z}[\mathrm{i}\sigma], \langle \sigma \rangle)$ differs from $(\mathbb{Z}[\mathrm{i}\sigma], \langle -\sigma \rangle)$, the corresponding gradings are isomorphic, since $\mathbb{Z}[\mathrm{i}\sigma] \cdot \sigma = \mathbb{Z}[\mathrm{i}\sigma] \cdot (-\sigma)$.

Example 5.5.21. The conclusion to Theorem 5.5.19 does not hold in general for non-connected reduced orders. Let C be a non-trivial finite abelian group and consider $R = \mathbb{Z}[C \times C] \times \mathbb{Z}[C]$. Let

$$A = \mathbb{Z}[C \times 1] \times \mathbb{Z}, \qquad G = \{((1, \gamma), \gamma) \mid \gamma \in C\},$$
$$B = \mathbb{Z}[1 \times C] \times \mathbb{Z}, \qquad H = \{((\gamma, 1), \gamma) \mid \gamma \in C\}.$$

Then A and B are stark, and $A[G] = R = B[H]$. However, the natural map $A[H] \to R$ has image $\mathbb{Z}[C \times 1] \times \mathbb{Z}[C] \neq R$.

5.6 Proofs of main theorems

In this section we prove Theorems 5.6.3 and 5.6.4 by reducing to the connected case, where we can apply Theorem 5.5.19. Recall the definition of $\mathcal{D}$ from Definition 5.5.9.

Lemma 5.6.1. *Let S and T be orders with S non-zero, let $R = S \times T$ with projection map $\pi\colon R \to S$, and let $(A, G) \in \mathcal{D}(R)$. Then we have $(\pi(A), \pi(G)) \in \mathcal{D}(S)$ and the restriction $G \to \pi(G)$ of π is a group isomorphism.*

Proof. We have a natural map $\pi(A)[G] \twoheadrightarrow \pi(A)[\pi(G)] \to S$. Since S equals $\pi(A[G]) = \sum_{g \in G} \pi(A)\pi(g)$, this map is clearly surjective. Suppose $\sum_{g \in G} \pi(a_g)g$ is in its kernel. Writing $e = (1, 0) \in R$ and identifying S with $S \times \{0\}$, we have $\pi(x) = ex$ for all $x \in R$. By Proposition 5.5.2.2 we have $e \in A$ and therefore $\sum_{g \in G} ea_g g = 0$ in $A[G]$. We conclude that for all $g \in G$ we have $\pi(a_g) = ea_g = 0$, so the map $\pi(A)[G] \to S$ is an isomorphism. Then the maps $\pi(A)[G] \to \pi(A)[\pi(G)]$ and $\pi(A)[\pi(G)] \to S$ are isomorphisms as well. Since $S \neq 0$, this implies that the map $G \to \pi(G)$ is an isomorphism and that $(\pi(A), \pi(G)) \in \mathcal{D}(S)$. □

Given a group ring structure on a product of orders, Lemma 5.6.1 constructs on each of the factors a group ring structure, with the same group. The following proposition does the opposite. For the definition of greatest common divisors, see Definition 5.2.3.

Proposition 5.6.2. *Let X be a finite non-empty set. For all $x \in X$ let R_x be a connected order, let $(A_x, G_x) \in \mathcal{D}(R_x)$, and suppose we write $G_x = D_x \oplus E_x$ for some subgroups $D_x, E_x \subseteq G_x$ such that for all $y, z \in X$ we have $D_y \cong D_z$. Consider*

$$R = \prod_{x \in X} R_x \quad \text{and} \quad A = \prod_{x \in X} A_x[E_x], \quad \text{and let} \quad D \subseteq \prod_{x \in X} D_x$$

be a subgroup for which all the projection maps $\pi_x \colon D \to D_x$ are isomorphisms. Then $(A, D) \in \mathcal{D}(R)$. If in addition (A_x, G_x) is maximal in $\mathcal{D}(R_x)$ for all $x \in X$, and D is a greatest common divisor of $\{G_x \mid x \in X\}$, then (A, D) is maximal in $\mathcal{D}(R)$.

Proof. Clearly $A \subseteq R$ and $D \subseteq \mu(R)$. There is a sequence of ring isomorphisms

$$A[D] \cong \prod_{x \in X} (A_x[E_x][D]) \cong \prod_{x \in X} (A_x[E_x][D_x]) \cong \prod_{x \in X} A_x[G_x] = R,$$

where one obtains the first isomorphism by tensoring $A = \prod_{x \in X} A_x[E_x]$ with $\mathbb{Z}[D]$ over $\mathbb{Z}$ and the second isomorphism is induced by the group isomorphisms π_x. The resulting isomorphism $A[D] \to R$ restricts to the inclusion on both A and D, so $A[D] = R$ and indeed $(A, D) \in \mathcal{D}(R)$.

Now suppose that (A_x, G_x) is maximal in $\mathcal{D}(R_x)$ for all $x \in X$, and that D is a greatest common divisor of $\{G_x \mid x \in X\}$. Let $(B, H) \in \mathcal{D}(R)$ be such that $(A, D) \leq (B, H)$. For $x \in X$ let B_x and H_x be the projection of B and H to R_x respectively. By Lemma 5.6.1 we have $(B_x, H_x) \in \mathcal{D}(R_x)$ and $H \cong H_x$. Choose $(C_x, I_x) \in \mathcal{D}(R_x)$ to be maximal such that $(B_x, H_x) \leq (C_x, I_x)$. Since R_x is connected, Lemma 5.5.11 implies that there exists a finite abelian group F_x such that $I_x \cong H_x \oplus F_x$. Since both (A_x, G_x) and (C_x, I_x) are maximal in $\mathcal{D}(R_x)$, we have $G_x \cong I_x$ by Theorem 5.5.19. Hence $G_x \cong I_x \cong H_x \oplus F_x \cong H \oplus F_x$. Thus H is a common divisor of all G_x, and H contains D. Since D is a greatest common divisor, we obtain $H = D$. From $A[D] = B[H] = B[D]$ and $A \supseteq B$ we see $A = B$, so $(A, D) = (B, H)$ and (A, D) is maximal. □

Theorem 5.6.3. *Suppose A and B are reduced orders and G and H are finite abelian groups. Then the following are equivalent:*

(i) *$A[G] \cong B[H]$ as rings,*

(ii) *there exist an order C and finite abelian groups I and J such that $A \cong C[I]$ and $B \cong C[J]$ as rings and $I \times G \cong J \times H$ as groups.*

Proof. If $A = 0$ or $B = 0$, then Theorem 5.6.3 holds trivially. Hence assume A and B are non-zero. (ii $\Rightarrow$ i) Assuming (ii), we have ring isomorphisms

$$A[G] \cong C[I][G] \cong C[I \times G] \cong C[J \times H] \cong C[J][H] \cong B[H].$$

(i $\Rightarrow$ ii) First assume $A[G]$ is connected. Let $(C, V) \geq (A, G)$ and $(D, W) \geq (B, H)$ be a maximal element of $\mathcal{D}(A[G])$, respectively $\mathcal{D}(B[H])$. By Lemma 5.5.13 the orders C and D are stark, so by Theorem 5.5.19 there exists a ring isomorphism $\sigma\colon B[H] \to A[G]$ that sends (D, W) to (C, V). It follows that $(C, V) \geq (\sigma(B), \sigma(H))$, so applying Lemma 5.5.11 twice, we find subgroups I, $J \subseteq V$ such that $I \times G = V = J \times \sigma(H) \cong J \times H$ and $C[I] = A$ and $C[J] = \sigma(B) \cong B$. This concludes the proof of the connected case.

Next consider the general case, where $A[G] = \prod_{x \in X} R_x$ is a non-empty product of connected reduced orders R_x. Without loss of generality we may assume $A[G] = B[H]$. Let $x \in X$. Write A_x and B_x for the image of A, respectively B, of the projection onto R_x. Then $A_x[G] \cong R_x \cong B_x[H]$ by Lemma 5.6.1. Since R_x is connected and we proved (i $\Rightarrow$ ii) in the connected case, there exist a reduced order C_x and finite abelian groups I_x and J_x such that $C_x[I_x] \cong A_x$ and $C_x[J_x] \cong B_x$ and $I_x \times G \cong J_x \times H = P_x$. Replacing C_x by $C_x[D_x]$ for some greatest common divisor D_x of I_x and J_x, we may assume that I_x and J_x are coprime. It follows that P_x is a least common multiple of G and H, as defined in Definition 5.2.3. In particular, when x ranges over X, the finite abelian groups P_x are pairwise isomorphic, and as a consequence the same holds for the groups I_x. Hence there exists a subgroup $I \subseteq \prod_{x \in X} I_x$ such that all projections $I \to I_x$ are isomorphisms, so from Proposition 5.6.2.1 it follows that $C[I] \cong A$ with $C = \prod_{x \in X} C_x$. Similarly we find a finite abelian group J that is isomorphic to all J_x such that $C[J] \cong B$. Now I and J together satisfy $I \times G \cong J \times H$, as desired. □

Theorem 5.6.4. *Let R be a non-zero reduced order. Then there exist a stark ring A, unique up to ring isomorphism, and a finite abelian group G, unique up to group isomorphism, such that $R \cong A[G]$ as rings.*

Proof. Let $(A, G) \in \mathcal{D}(R)$ be a maximal element (Lemma 5.5.10). Then A is stark by Lemma 5.5.13. Suppose B is a stark ring and H is a finite abelian group such that $B[H] \cong R$. By Theorem 5.6.3 there exist an order C and finite abelian groups I and J such that $A \cong C[I]$ and $B \cong C[J]$ and $I \times G \cong J \times H$. Since both A and B are stark we conclude that $I = J = 1$, so $G \cong H$ and $A \cong C \cong B$. Hence A and G are unique up to ring and group isomorphism, respectively. □

5.7 Automorphisms of group rings

In this section we will describe $\mathrm{Aut}(A[G])$, for a stark connected reduced order A with degree map d and a finite abelian group G, in terms of $U^*(d)$, G, and $\mathrm{Aut}(A)$. In this section we write $Q(A)$ for $Q(d)$ and similarly for U and U^* as defined in Definition 5.4.1. In our context $U^*(A)$ is equal to $U(A)$ due to the following.

Lemma 5.7.1. *Let A be a connected reduced order with degree map $d\colon \Gamma \to \mu$. Then the following are equivalent:*

(i) *A is stark;*
(ii) *d is nil;*
(iii) $\mathrm{Hom}(\Gamma, \mu) = \mathrm{nil}(Q(A))$*;*
(iv) $\mathrm{Hom}(\Gamma, \mu) = \mathrm{Jac}(Q(A))$*;*
(v) $U^*(A) = U(A)$*;*

Proof. We will write $Q = Q(A)$ and similarly for U and U^*.

(i $\Leftrightarrow$ ii) This follows from Theorem 5.5.15 and Lemma 5.3.7.4.

(ii $\Leftrightarrow$ iii) This follows immediately from the definition of nil and the multiplication on Q, and the fact that in general $\mathrm{nil}(Q) \subseteq \mathrm{Hom}(\Gamma, \mu)$.

(iii $\Rightarrow$ iv) Since $\mathrm{nil}(Q)$ is a nil two-sided ideal we have $\mathrm{Hom}(\Gamma, \mu) \subseteq \mathrm{nil}(Q) \subseteq \mathrm{Jac}(Q)$. The surjection $Q \twoheadrightarrow \mathbb{Z}$ must map $\mathrm{Jac}(Q)$ to $\mathrm{Jac}(\mathbb{Z}) = 0$, so in general $\mathrm{Jac}(Q) \subseteq \mathrm{Hom}(\Gamma, \mu)$, hence we have equality.

(iv $\Rightarrow$ v) We have $U = 1 + \mathrm{Jac}(Q) \subseteq Q^*$, so $U = U^*$.

(v $\Rightarrow$ iii) The involution $x \mapsto 1 - x$ on Q maps U to $\mathrm{Hom}(\Gamma, \mu)$. Hence both sets have the same number of idempotents, which by assumption is only 1 for U. Since $\mathrm{Hom}(\Gamma, \mu)$ is finite, every element has some power which is idempotent and hence 0, so $\mathrm{Hom}(\Gamma, \mu) \subseteq \mathrm{nil}(Q)$. The reverse inclusion holds in general. □

A category $\mathcal{C}$ is *small* if the class of objects of $\mathcal{C}$ is a set, and for any two objects A and B of $\mathcal{C}$ the class $\mathrm{Hom}(A, B)$ is a set. A category $\mathcal{C}$ is *preadditive* (see Section 1.2 in [4]) if for any two objects A and B of $\mathcal{C}$ the class $\mathrm{Hom}(A, B)$ is an abelian group such that composition of morphisms is bilinear, i.e. for all objects A, B, and C and morphisms $f, f'\colon A \to B$ and $g, g'\colon B \to C$ we have $g \circ (f + f') = (g \circ f) + (g \circ f')$ and $(g + g') \circ f = (g \circ f) + (g' \circ f)$.

Lemma 5.7.2. *Let $\mathcal{C}$ be a preadditive small category with precisely two objects $\mathbf{0}$ and $\mathbf{1}$. Then:*

1. *With $M_{ij} = \mathrm{Hom}(j, i)$ for $i, j \in \{\mathbf{0}, \mathbf{1}\}$ both $M_{\mathbf{00}}$ and $M_{\mathbf{11}}$ are rings and $M_{\mathbf{01}}$ and $M_{\mathbf{10}}$ are a $M_{\mathbf{00}}$-$M_{\mathbf{11}}$-bimodule and $M_{\mathbf{11}}$-$M_{\mathbf{00}}$-bimodule respectively.*

2. *The product of groups*

$$\mathrm{M}(\mathcal{C}) = \prod_{i,j\in\{\mathbf{0},\mathbf{1}\}} M_{ij} = \begin{pmatrix} M_{\mathbf{00}} & M_{\mathbf{01}} \\ M_{\mathbf{10}} & M_{\mathbf{11}} \end{pmatrix}$$

is a ring with respect to the addition and multiplication implied by the matrix notation.

3. *If* $M_{\mathbf{01}} \cdot M_{\mathbf{10}} = \mathrm{im}(M_{\mathbf{01}} \otimes M_{\mathbf{10}} \to M_{\mathbf{00}}) \subseteq \mathrm{Jac}(M_{\mathbf{00}})$*, then*

$$M_{\mathbf{10}} \cdot M_{\mathbf{01}} \subseteq \mathrm{Jac}(M_{\mathbf{11}}),$$
$$\mathrm{Jac}(\mathrm{M}(\mathcal{C})) = \begin{pmatrix} \mathrm{Jac}(M_{\mathbf{00}}) & M_{\mathbf{01}} \\ M_{\mathbf{10}} & \mathrm{Jac}(M_{\mathbf{11}}) \end{pmatrix} \quad \textit{and}$$
$$\mathrm{M}(\mathcal{C})^* = \begin{pmatrix} M^*_{\mathbf{00}} & M_{\mathbf{01}} \\ M_{\mathbf{10}} & M^*_{\mathbf{11}} \end{pmatrix}.$$

Proof. That the M_{ij} are groups, and that the addition is compatible with the composition of morphisms, follows from the fact that $\mathcal{C}$ is preadditive. It is then easy to verify that the M_{ij} are rings and modules as claimed, and that $\mathrm{M}(\mathcal{C})$ is a ring, giving 1 and 2.

Now suppose $M_{\mathbf{01}} \cdot M_{\mathbf{10}} \subseteq \mathrm{Jac}(M_{\mathbf{00}})$. We will show that for all $m \in M_{\mathbf{01}}$ and $n \in M_{\mathbf{10}}$ we have $nm \in \mathrm{Jac}(M_{\mathbf{11}})$. Let $s \in M_{\mathbf{11}}$. Then $(ms)n \in M_{\mathbf{01}} \cdot M_{\mathbf{10}} \subseteq \mathrm{Jac}(M_{\mathbf{00}})$, so $1 + msn$ has an inverse $r \in M_{\mathbf{00}}$. Then

$$\begin{aligned}(1 - snrm)(1 + snm) &= 1 - sn(r(1 + msn) - 1)m \\ &= 1 - sn(1 - 1)m = 1.\end{aligned}$$

Hence $1 + snm$ has a left inverse $1 - snrm$, and similarly $1 - snrm$ is a right inverse of $1 + snm$. Thus $1 + snm \in M^*_{\mathbf{11}}$ and $nm \in \mathrm{Jac}(M_{\mathbf{11}})$. We conclude that $M_{\mathbf{10}} \cdot M_{\mathbf{01}} \subseteq \mathrm{Jac}(M_{\mathbf{11}})$. Consider

$$T = \begin{pmatrix} \mathrm{Jac}(M_{\mathbf{00}}) & M_{\mathbf{01}} \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 \\ M_{\mathbf{10}} & \mathrm{Jac}(M_{\mathbf{11}}) \end{pmatrix}$$

and write $J = T + B$. We will first show that $T \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. For $x = \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \in T$ it suffices to show for all $y = \left(\begin{smallmatrix} r & m \\ n & s \end{smallmatrix}\right) \in \mathrm{M}(\mathcal{C})$ that $1 + xy \in \mathrm{M}(\mathcal{C})^*$. As $1 + xy = \left(\begin{smallmatrix} 1+ar+bn & ma+bs \\ 0 & 1 \end{smallmatrix}\right)$ is upper triangular, it is invertible if its diagonal elements are. The element $1 + ar + bn$ is invertible because $ar + bn \in \mathrm{Jac}(M_{\mathbf{00}})$, so $T \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. Analogously $B \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. Thus we have a two-sided ideal $J \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. To see equality, note that the ring $\mathrm{M}(\mathcal{C})/J \cong (M_{\mathbf{00}}/\mathrm{Jac}(M_{\mathbf{00}})) \times (M_{\mathbf{11}}/\mathrm{Jac}(M_{\mathbf{11}}))$ has a trivial Jacobson

radical. An element of $\mathrm{M}(\mathcal{C})$ is a unit if and only if it maps to a unit in $\mathrm{M}(\mathcal{C})/\mathrm{Jac}(\mathrm{M}(\mathcal{C}))$, hence if and only if its diagonal elements are units, proving the final statement. □

Naturally, the construction $\mathrm{M}(\mathcal{C})$ can be generalized to categories $\mathcal{C}$ with any finite number of objects. We call $\mathrm{M}(\mathcal{C})$ the *matrix ring* of $\mathcal{C}$.

Remark 5.7.3. Given four abelian groups M_{ij} with $i, j \in \{0, 1\}$ together with compatible (i.e. associative) multiplications $M_{ij} \otimes M_{jk} \to M_{ik}$ for all $i, j, k \in \{0, 1\}$ with appropriate unit elements, we can construct the preadditive category $\mathcal{C}$ with two objects 0 and 1, with $\mathrm{Hom}(j, i) = M_{ij}$, and with composition being these multiplications. In particular, if M_{00} and M_{11} are rings, M_{01} is an M_{00}-M_{11}-bimodule, and M_{10} is an M_{11}-M_{00}-bimodule, then it remains only to specify the multiplications $M_{01} \otimes M_{10} \to M_{00}$ and $M_{10} \otimes M_{01} \to M_{11}$.

Let A be a connected reduced order and G a finite abelian group. Recall that $\mu(A)$ and $\Gamma(A)$ are $Q(A)$-modules by Remark 5.4.3, hence $\mathrm{Hom}(G, \mu(A))$ and $\mathrm{Hom}(\Gamma(A), G)$ are respectively left and right $Q(A)$-modules. We next describe $U^*(A[G])$ in terms of A and G.

Proposition 5.7.4. *Let A be a connected reduced order and G a finite abelian group. Then:*

1. *We have a matrix ring*

$$E = \begin{pmatrix} Q(A) & \mathrm{Hom}(G, \mu(A)) \\ \mathrm{Hom}(\Gamma(A), G) & \mathrm{End}(G) \end{pmatrix},$$

   where $\mathrm{Hom}(G, \mu(A)) \otimes \mathrm{Hom}(\Gamma(A), G) \to \mathrm{Hom}(\Gamma(A), \mu(A)) \subseteq Q(A)$ is the composition map and $\mathrm{Hom}(\Gamma(A), G) \otimes \mathrm{Hom}(G, \mu(A)) \to \mathrm{End}(G)$ is given by $g \otimes f \mapsto gdf$.
2. *There is a natural ring isomorphism $E \xrightarrow{\sim} Q(A[G])$ that respects the action of $\mathrm{Aut}(A)$.*
3. *If A is stark, then the map in 2 restricts to an isomorphism*

$$\begin{pmatrix} U^*(A) & \mathrm{Hom}(G, \mu(A)) \\ \mathrm{Hom}(\Gamma(A), G) & \mathrm{Aut}(G) \end{pmatrix} \xrightarrow{\sim} U^*(A[G]).$$

Proof. 1. Apply Remark 5.7.3 and Lemma 5.7.2.2. Since all multiplications are defined in terms of compositions of morphisms, the associativity conditions are trivially satisfied.

2. Write $\Gamma = \Gamma(A)$ and $\mu = \mu(A)$. We have by Proposition 5.5.7.ii that

$$Q(A[G]) \;=\; \mathbb{Z} \oplus \mathrm{Hom}(\Gamma \times G, \mu \times G) \;\cong\; \mathbb{Z} \oplus \begin{pmatrix} \mathrm{Hom}(\Gamma,\mu) & \mathrm{Hom}(G,\mu) \\ \mathrm{Hom}(\Gamma,G) & \mathrm{End}(G) \end{pmatrix},$$

where the isomorphism is one of abelian groups. Then the map $Q(A[G]) \to E$ with respect to the latter representation given by

$$\Big(n, \begin{pmatrix} p & q \\ r & s \end{pmatrix}\Big) \mapsto \begin{pmatrix} (n,p) & q \\ r & n+s \end{pmatrix}$$

is an isomorphism of rings that by functoriality respects the action of $\mathrm{Aut}(A)$.

3. Suppose A is stark. Then $\mathrm{Hom}(\Gamma,\mu) = \mathrm{Jac}(Q(A))$ by Lemma 5.7.1. It follows that the ideal $\mathrm{Hom}(G,\mu) \cdot \mathrm{Hom}(\Gamma, G) \subseteq \mathrm{Hom}(\Gamma,\mu)$ is contained in $\mathrm{Jac}(Q(A))$. Now apply Lemma 5.7.2.3. □

In Remark 5.7.5 and Proposition 5.7.6 we describe $\mathrm{Aut}(A[G])$ in terms of A and $U^*(A[G])$.

Remark 5.7.5. Let G be a finite abelian group. Then $-[G]$ and U^* act functorially on isomorphisms of connected reduced orders. Let A be a connected reduced order. From Proposition 5.5.7.ii we get a natural inclusion $\mathrm{Hom}(\Gamma(A),\mu(A)) \to \mathrm{Hom}(\Gamma(A[G]),\mu(A[G]))$, which extends to an inclusion of rings $Q(A) \to Q(A[G])$. Then we have a commutative diagram

$$\begin{array}{ccccc} U^*(A) & \xrightarrow{\text{Lem 5.5.17}} & \mathrm{Aut}(A) & \xrightarrow{\quad U^*\quad} & \mathrm{Aut}(U^*(A)) \\ \big\downarrow & & \big\downarrow{\scriptstyle -[G]} & & \\ U^*(A[G]) & \xrightarrow{\text{Lem 5.5.17}} & \mathrm{Aut}(A[G]) & \xrightarrow{\quad U^*\quad} & \mathrm{Aut}(U^*(A[G])), \end{array}$$

and the composition $U^*(A) \to \mathrm{Aut}(U^*(A))$ is the conjugation map.

Proposition 5.7.6. *Let A be a stark connected reduced order and G a finite abelian group. Then the maps and actions from Remark 5.7.5 fit in an exact sequence*

$$0 \to U^*(A) \xrightarrow{\iota} U^*(A[G]) \rtimes \mathrm{Aut}(A) \xrightarrow{\pi} \mathrm{Aut}(A[G]) \to 0,$$

where ι and π are homomorphisms such that $\iota(u) = (u^{-1}, u)$ and π maps each component to $\mathrm{Aut}(A[G])$.

Proof. For all $u, v \in U^*(A)$ we have

$$\iota(u)\iota(v) = (u^{-1}, u)(v^{-1}, v) = (u^{-1}(uv^{-1}u^{-1}), uv) = \iota(uv)$$

by Remark 5.7.5, so ι is a homomorphism. Moreover, ι is injective because it maps injectively to the first factor. By the same lemma π is a homomorphism.

We will now show that π is surjective. Suppose $\sigma \in \mathrm{Aut}(A[G])$. By Theorem 5.5.19 there exists $1+f \in U^*(A[G])$ that maps (A, G) to $(\sigma(A), \sigma(G))$, so without loss of generality we may assume $\sigma(A) = A$ and $\sigma(G) = G$. By applying the restriction $\sigma|_A \in \mathrm{Aut}(A)$ we may assume σ is the identity on A. Consider the map $f\colon \Gamma(A) \times G \to \mu(A[G])$ given by $(\delta, g) \mapsto \sigma(g)g^{-1}$ and note that $1 + f \in U(A[G])$ gets mapped to σ. We similarly obtain the inverse of $1 + f$ in $U(A[G])$ from $(\delta, g) \mapsto \sigma^{-1}(g)g^{-1}$, so $1 + f \in U^*(A[G])$. It follows that σ is in the image of π and thus π is surjective.

To show the sequence is exact, it remains to show $\mathrm{im}(\iota) = \ker(\pi)$. It is clear that $\mathrm{im}(\iota) \subseteq \ker(\pi)$, so suppose $(1 + f, \alpha) \in \ker(\pi)$. As α^{-1} equals the restriction of $1 + f$ by assumption, it suffices to show that $1 + f \in U^*(A)$. For $g \in G$ we have $g = (1 + f)\alpha(g) = f(g)g$, and since g is a unit we have $f(g) = 1$, i.e. $G \subseteq \ker(f)$. Moreover $\mathrm{im}(f) \subseteq \mu(A)$, since multiplication by any unit $(\zeta, g) \in \mu(A) \times G = \mu(A[G])$ not in $\mu(A)$ sends A to $Ag \neq A$. Hence $f \in \mathrm{Hom}(\Gamma(A), \mu(A))$ and $1 + f \in U(A)$. The same holds for the inverse $1 + e \in U^*(A[G])$ of $1 + f$, so $1 + e \in U(A)$ and thus $1 + f \in U^*(A)$. It now follows that $(1 + f, \alpha) = \iota(1 + e)$, so $\ker(\pi) \subseteq \mathrm{im}(\iota)$, as was to be shown. □

Proposition 5.7.4 and Proposition 5.7.6 combined gives us a description of $\mathrm{Aut}(A[G])$ in terms of A and G. We now prove Theorem 5.7.8 and describe $\mathrm{Aut}(A[G])$ by less canonical means.

Lemma 5.7.7. *Let A be a stark connected reduced order. Then the group $\mathrm{Hom}(\Gamma(A), \mu(A))$ has a (right) action on the set $\mathrm{Aut}(A)$, which for $\alpha \in \mathrm{Aut}(A)$ and $f \in \mathrm{Hom}(\Gamma(A), \mu(A))$ is given by*

$$(\alpha, f) \mapsto \alpha + f = \big(x \in A_\gamma \mapsto \alpha(x) \cdot f(\gamma)\big).$$

Proof. Let $\alpha \in \mathrm{Aut}(A)$ and $f, g \in \mathrm{Hom}(\Gamma(A), \mu(A))$. Note that $\alpha + f = \alpha \circ (1 + \alpha^{-1}f) \in \mathrm{Aut}(A)$, where $1 + \alpha^{-1}f \in U(A) = U^*(A)$ by Lemma 5.7.1 and the composition is taken inside $\mathrm{Aut}(A)$ via Lemma 5.5.17. For $\gamma \in \Gamma(A)$ and $x \in A_\gamma$ we clearly have

$$\begin{aligned}[(\alpha + f) + g](x) &= [\alpha + f](x) \cdot g(\gamma) \\ &= \alpha(x) \cdot f(\gamma) \cdot g(\gamma) \\ &= [\alpha + (f + g)](x),\end{aligned}$$

so the action is well-defined. □

Theorem 5.7.8. *Let A be a stark connected reduced order with degree map $d_A\colon \mu \to \Gamma$ and let G be a finite abelian group. We equip the cartesian product*

$$M = \begin{pmatrix} \mathrm{Aut}(A) & \mathrm{Hom}(G,\mu) \\ \mathrm{Hom}(\Gamma, G) & \mathrm{Aut}(G) \end{pmatrix}$$

of $\mathrm{Aut}(A)$, $\mathrm{Hom}(G,\mu)$, $\mathrm{Hom}(\Gamma,G)$, *and* $\mathrm{Aut}(G)$ *with the following multiplication:*

$$\begin{pmatrix} \alpha_1 & s_1 \\ t_1 & \sigma_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & s_2 \\ t_2 & \sigma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 + s_1 t_2 & \alpha_1 s_2 + s_1\sigma_2 \\ t_1\alpha_2 + \sigma_1 t_2 & t_1 d_A s_2 + \sigma_1\sigma_2 \end{pmatrix},$$

where the sum in $\mathrm{Aut}(A)$ *is as in Lemma 5.7.7 and the sum in* $\mathrm{Aut}(G)$ *is taken inside* $\mathrm{End}(G)$. *For $x \in A$ and $g \in G$ write $\left(\begin{smallmatrix} x \\ g \end{smallmatrix}\right)$ for the element $x \cdot g \in A[G]$. Then:*

1. *M is a group;*
2. *there is a natural isomorphism $M \xrightarrow{\sim} \mathrm{Aut}(A[G])$ such that the evaluation map $M \times A[G] \to A[G]$ is given by*

$$\begin{pmatrix} \alpha & s \\ t & \sigma \end{pmatrix} \begin{pmatrix} x \\ g \end{pmatrix} = \begin{pmatrix} \alpha(x) \cdot s(g) \\ t(\gamma) \cdot \sigma(g) \end{pmatrix}$$

for all $g \in G$, $\gamma \in \Gamma$ and $x \in A_\gamma$.

Proof. To check that M is a group it remains to verify that $t_1 d s_2 + \sigma_1\sigma_2 \in \mathrm{Aut}(G)$. This follows from Lemma 5.7.1, namely $t_1 d s_2 \in \mathrm{Jac}(\mathrm{End}(G))$. Note that the map $\vartheta\colon M \to \mathrm{Aut}(A[G])$ can be written as the composition of the homomorphism $\varphi\colon M \to U^*(A[G]) \rtimes \mathrm{Aut}(A)$ given by

$$\begin{pmatrix} \alpha & s \\ t & \sigma \end{pmatrix} \mapsto \begin{pmatrix} 1 & s \\ t\alpha^{-1} & \sigma \end{pmatrix} \cdot \alpha$$

where $U^*(A[G])$ is written in terms of the matrix representation of Proposition 5.7.4, and the homomorphism $\pi\colon U^*(A[G]) \rtimes \mathrm{Aut}(A) \to \mathrm{Aut}(A[G])$ from Proposition 5.7.6. The map π is still surjective when restricted to the image of φ. Namely any $\left(\begin{smallmatrix} u & s \\ t & \sigma \end{smallmatrix}\right) \cdot \alpha \in U^*(A[G]) \rtimes \mathrm{Aut}(A)$ has the same image as $\left(\begin{smallmatrix} 1 & s \\ t\beta^{-1} & \sigma \end{smallmatrix}\right) \cdot \beta\alpha$, where β is the image of u in $\mathrm{Aut}(A)$. Hence the map ϑ is surjective. By Proposition 5.7.4.3 and Proposition 5.7.6, respectively, we have

$$\frac{\#M}{\#U^*(A[G])} = \frac{\#\,\mathrm{Aut}(A)}{\#U^*(A)} = \frac{\#\,\mathrm{Aut}(A[G])}{\#U^*(A[G])},$$

so the groups M and $\mathrm{Aut}(A[G])$ have the same (finite) cardinality, so ϑ is bijective. □

5.8 Algorithms

In this section we will prove Theorem 5.8.4, the algorithmic counterpart to Theorem 5.6.4.

Lemma 5.8.1. *For each of $R = \mathbb{Z}$ and $R = \left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$ there exists a polynomial-time algorithm that, given finite R-modules M_1 and M_2, computes a greatest common divisor D of M_1 and M_2 as defined in Definition 5.2.3, together with injections $\iota_i \colon D \to M_i$ and a complement $N_i \subseteq M_i$ such that $N_i \oplus \iota_i D = M_i$.*

Proof. By Theorem 2.6.9 in [5] we may compute the exponents of M_1 and M_2, and their least common multiple n, in polynomial time. Note that M_1 and M_2 are R/nR-modules and that replacing R by R/nR does not change the problem. Since R/nR is a finite ring, the problem reduces to Theorem 4.1.1 in [5]. □

Proposition 5.3.2 allows us to interpret a morphism of finite abelian groups as a finite length $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module. Although both types of objects are represented differently, one easily deduces from the proof of Proposition 5.3.2 that we can change representations in polynomial time.

In the following result, $\mathrm{Dec}_{\mathcal{I}}(d)$ is as defined in Definition 5.2.8, Remark 5.3.4, and Definition 5.3.3.

Proposition 5.8.2. *There exists a polynomial-time algorithm that, given finite abelian groups A and B and a morphism $d \colon A \to B$, computes a maximal element of $\mathrm{Dec}_{\mathcal{I}}(d)$.*

Proof. By Lemma 5.8.1 we may compute in polynomial time a greatest common divisor D of A and B as $\mathbb{Z}$-modules. Similarly we may compute a greatest common divisor E of d and id_D as $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules. We also obtain submodules d_0 and d_1 of d such that $d_1 \cong E$ and $d = d_0 \oplus d_1$. We claim that (d_0, d_1) is a maximal element of $\mathrm{Dec}_{\mathcal{I}}(d)$.

First note that d_1 is a divisor of id_D and thus must be an isomorphism. As $d = d_0 \oplus d_1$ we indeed have that $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$. Let $(e_0, e_1) \geq (d_0, d_1)$ be maximal in $\mathrm{Dec}_{\mathcal{I}}(d)$. Since e_1 is an isomorphism, it is isomorphic to id_F for some finite abelian group F. Since e_1 is a direct summand of d, the group F is a direct summand of both A and B, so F is a divisor of their greatest common divisor D. Thus e_1 is a divisor of id_D. It follows that e_1

is a divisor of $E \cong d_1$, so $(d_0, d_1) = (e_0, e_1)$ and thus (d_0, d_1) is maximal, as was to be shown. □

Recall that we have specified an encoding for gradings of orders in Section 4.7.

Proposition 5.8.3. *There exists a polynomial-time algorithm that, given a reduced order R and a universal grading of R, computes a maximal element of $\mathcal{D}(R)$ as defined in Definition 5.5.9.*

Proof. First suppose R is connected. By Theorem 1.2 in [32] we may compute $\mu = \mu(R)$ in polynomial time and thus also the group homomorphism $d\colon \mu \to \Gamma$ as defined in Definition 5.5.6. We may compute a maximal element $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ with $d_i\colon \mu_i \to \Gamma_i$ in polynomial time using Proposition 5.8.2. Under the isomorphisms of partially ordered sets of Theorem 5.5.15 this d corresponds to a maximal element $(A, G) \in \mathcal{D}(R)$, where $A = \sum_{\gamma \in \Gamma_0} R_\gamma$ and $G = \mu_1$, which we may compute in polynomial time.

Now consider the general case. By Theorem 1.1 in [32] we may compute in polynomial time connected reduced orders $\{R_x\}_{x \in X}$ for some index set X such that $R \cong \prod_{x \in X} R_x$, together with the projections $\pi_x\colon R \to R_x$. Using Proposition 4.2.6 we may construct universal gradings for the R_x in polynomial time. Hence by the special case we may compute a maximal element of $\mathcal{D}(R_x)$ for all $x \in X$ in polynomial time. Finally, we may apply Proposition 5.6.2 to compute a maximal element of $\mathcal{D}(R)$, observing that the construction in Proposition 5.6.2 can be carried out in polynomial time using Lemma 5.8.1. □

Computing a maximal element of $\mathcal{D}(R)$ for a reduced order R is now reduced to finding a universal grading of R.

Theorem 5.8.4. *There is an algorithm that, given a non-zero reduced order R, computes a stark subring $A \subseteq R$ and a subgroup $G \subseteq \mu(R)$ such that $A[G] = R$. This algorithm runs* (a) *in polynomial time when the additive group of R is generated by autopotents, and generally* (b) *in time $n^{O(m)}$ where n is the length of the input and m is the number of minimal prime ideals of R.*

Proof. We compute the universal grading of R. For (a), we use Theorem 4.7.13, while for (b) we use Theorem 1.4 in [17]. The theorem now follows from Proposition 5.8.3. □

CHAPTER 6

Roots of ideals in number rings

6.1 Introduction

Let R be an order, not necessarily in a number field. A *fractional ideal* of R is a finitely generated R-submodule $\mathfrak{a} \subseteq \mathbb{Q}R$ such that $\mathbb{Q}\mathfrak{a} = \mathbb{Q}R$. For fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R we write $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a} \cdot \mathfrak{b}$ for the R-submodule of $\mathbb{Q}R$ given by $\{a + b \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ and generated by $\{ab \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ respectively. We say a fractional ideal $\mathfrak{a}$ of R is *invertible* if there exists a fractional ideal $\mathfrak{a}^{-1}$ of R such that $\mathfrak{a}\mathfrak{a}^{-1} = R$, and we write $\mathcal{I}(R)$ for the group of invertible fractional ideals of R.

Any fractional ideal of R is a free abelian group of the same rank as R, and we will encode a fractional ideal of R by a $\mathbb{Z}$-basis in $\mathbb{Q}R$. Using standard techniques as in [5], it is possible to compute $\mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{b}$ and $\mathfrak{a}^{-1}$ in polynomial time on input R, $\mathfrak{a}$ and $\mathfrak{b}$. This chapter we dedicate to the computation of another elementary operation, namely taking roots of fractional ideals.

A fractional R-ideal can have multiple n-th roots as $\mathcal{I}(R)$ can have non-trivial torsion, while if R is the maximal order the n-th root is unique if it exists. This makes it impossible to produce such a root functorially under isomorphisms; see Example 6.7.6. Instead we solve the following problem.

Theorem 6.7.3. *There exists a polynomial-time algorithm that, given an order R in a number field and fractional ideal $\mathfrak{a}$ of R, computes the maximal $n \in \mathbb{Z}_{\geq 0}$ with respect to divisibility for which there exist an order $R \subseteq S \subseteq \mathbb{Q}R$ and fractional ideal $\mathfrak{b}$ of S such that $\mathfrak{b}^n = S\mathfrak{a}$, where $\mathfrak{b}^0 := S$, and additionally computes such S and $\mathfrak{b}$. The output of this algorithm is functorial under isomorphisms of R.*

If a fractional R-ideal $\mathfrak{a}$ has an n-th root say $\mathfrak{b}$, then the S-ideal $S\mathfrak{a}$ also has an n-th root, namely $S\mathfrak{b}$, for any order $R \subseteq S \subseteq \mathbb{Q}R$. However, if $S\mathfrak{a}$ has an n-th root for some S, then $\mathfrak{a}$ does not need to have an n-th root; see Example 6.7.5.

A maximal order in a number field has unique prime factorization of ideals. However, we cannot expect to compute in polynomial time, given an ideal $\mathfrak{a}$ of a number ring R, the set of prime ideals $\mathfrak{a} \subseteq \mathfrak{p}$ of R, for the same reason that factorization of integers is considered hard. An often good enough substitute is a coprime factorization: For a set X of ideals of R, we compute a set C of pairwise coprime invertible proper ideals so that every ideal of X is a (necessarily unique) product of ideals of C, potentially enlarging the order R in the process as in Theorem 6.7.3. We say C is *reduced* if $\langle C \rangle$ is a direct summand of $\mathcal{I}(R)$. For finite C this is equivalent to the elements of C having no proper roots in $\mathcal{I}(R)$. For orders $R \subseteq S \subseteq \mathbb{Q}R$ and a set X of fractional ideals of R we write $S \cdot X = \{S\mathfrak{a} \mid \mathfrak{a} \in X\}$, and we say

C is *strongly reduced* if $S \cdot C$ is reduced for every order $R \subseteq S \subseteq \mathbb{Q}R$. Using the previous theorem we may compute strongly reduced coprime bases.

Theorem 6.8.5. *There exists a polynomial-time algorithm that, given a order R in a number field and a finite set X of fractional ideals contained in R, computes an order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S \cdot X$ has a strongly reduced coprime basis and computes such a coprime basis. The output of this algorithm is functorial under isomorphisms of R.*

For both theorems we produce an order S functorially, so one can wonder whether this S has a compact definition other than it being the output of the algorithm, as will be the case in Theorem 6.2.5 and Theorem 6.4.8. However, we were unable to find such a description.

6.2 Fractional ideals

Let R be a commutative ring. We say $x \in R$ is *regular* if multiplication by x is injective and *invertible* if it is surjective. Let S be the set of regular elements of R. Then S is a multiplicatively closed set, and we write $\mathrm{Q}(R) = S^{-1}R$, the localization of R by S, for the *total ring of fractions* of R. The natural map $R \to \mathrm{Q}(R)$ is an injective ring homomorphism, and we treat it as an inclusion. If R is a reduced order, then $\mathrm{Q}(R) = \mathbb{Q}R$. If $R \subseteq S \subseteq \mathrm{Q}(R)$ are (sub)rings, then $\mathrm{Q}(S) = \mathrm{Q}(R)$.

For R-submodules $\mathfrak{a}, \mathfrak{b} \subseteq \mathrm{Q}(R)$ we write $\mathfrak{a} + \mathfrak{b} = \{a + b \,|\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$, write $\mathfrak{a} \cdot \mathfrak{b}$ or $\mathfrak{a}\mathfrak{b}$ for the additive group generated by $\{ab \,|\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ and write $\mathfrak{a} : \mathfrak{b} = \{x \in \mathrm{Q}(R) \,|\, x\mathfrak{b} \subseteq \mathfrak{a}\}$. A *fractional ideal* of R, which is not necessarily an ideal of R, is a finitely generated R-submodule $\mathfrak{a} \subseteq \mathrm{Q}(R)$ such that $\mathrm{Q}(R) \cdot \mathfrak{a} = \mathrm{Q}(R)$. An *invertible ideal* of R is a fractional ideal $\mathfrak{a}$ of R for which there exists an R-submodule $\mathfrak{b} \subseteq \mathrm{Q}(R)$ such that $\mathfrak{a}\mathfrak{b} = R$.

Lemma 6.2.1. *Let R be a commutative ring with fractional ideal $\mathfrak{a}$. Then $\mathfrak{a}$ contains a regular element of R.*

Proof. Since $\mathrm{Q}(R)\mathfrak{a} = \mathrm{Q}(R)$ we may write $\sum_{k=1}^{n}(r_k/s_k) \cdot a_k = 1$ for some $n \in \mathbb{Z}_{\geq 0}$, $r_k, s_k \in R$ and $a_k \in \mathfrak{a}$ with s_k regular. Multiplying this equation by the regular element $s = \prod_{k=1}^{n} s_k$ we obtain $\mathfrak{a} \ni \sum_{k=1}^{n} r_k(s/s_k)a_k = s$. □

Lemma 6.2.2. *Let R be a commutative ring and suppose $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ are fractional ideals of R. Then*

1. *R, $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$ are fractional ideals of R;*
2. *$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$ and $\mathfrak{a} : R = \mathfrak{a}$;*
3. *If $\mathfrak{b} \subseteq \mathfrak{c}$, then $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{c}$, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{c}$, $\mathfrak{b} : \mathfrak{a} \subseteq \mathfrak{c} : \mathfrak{a}$ and $\mathfrak{a} : \mathfrak{b} \supseteq \mathfrak{a} : \mathfrak{c}$;*
4. *We have $\mathfrak{c}(R : \mathfrak{c}) = R$ if and only if $\mathfrak{c}$ is invertible;*

5. *If* $\mathfrak{c}$ *is invertible, then* $\mathfrak{ac} : \mathfrak{bc} = \mathfrak{a} : \mathfrak{b}$, $\mathfrak{a} : \mathfrak{c} = \mathfrak{a}(R : \mathfrak{c})$, *and* $\mathfrak{ac} \subseteq \mathfrak{bc}$ *implies* $\mathfrak{a} \subseteq \mathfrak{b}$*;*
6. *If* R *is Noetherian or* $\mathfrak{c}$ *is invertible, then* $\mathfrak{a} : \mathfrak{c}$ *is a fractional ideal;*
7. *If* $\mathfrak{a}$ *is of the form* Ra *for some unit* $a \in \mathrm{Q}(R)$*, then* $\mathfrak{a}$ *is invertible. If* R *is semi-local, then the converse also holds.* □

Proof. We will prove the non-trivial parts.

4. If $\mathfrak{cd} = R$ for some $\mathfrak{d}$, then $\mathfrak{d} \subseteq R : \mathfrak{c}$ and $R = \mathfrak{cd} \subseteq \mathfrak{c}(R : \mathfrak{c}) \subseteq R$, so we have equality throughout. Suppose $\mathfrak{c}(R : \mathfrak{c}) = R$. It suffices to show that $R : \mathfrak{c}$ is finitely generated. We have $1 = \sum_{i \in I} c_i d_i$ for some finite set I and $c_i \in \mathfrak{c}$ and $d_i \in R : \mathfrak{c}$. If $x \in R : \mathfrak{c}$, then $x = \sum_{i \in I}(c_i x)d_i \in \sum_{i \in I} Rd_i$, so the d_i generate $R : \mathfrak{c}$.

5. Write $\mathfrak{d} = R : \mathfrak{c}$. Note that $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{ae} : \mathfrak{be}$ for all $\mathfrak{e}$. Hence $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{ac} : \mathfrak{bc} \subseteq \mathfrak{acd} : \mathfrak{bcd} = \mathfrak{a} : \mathfrak{b}$, so we have equality throughout. Using this we have $\mathfrak{a} : \mathfrak{c} = \mathfrak{ad} : \mathfrak{cd} = \mathfrak{ad} : R = \mathfrak{ad}$. Note that $\mathfrak{e} \subseteq \mathfrak{f}$ is equivalent to $R \subseteq \mathfrak{f} : \mathfrak{e}$, from which one then deduces the last statement.

6. We have $cR \subseteq \mathfrak{c}$ for some $c \in \mathrm{Q}(R)^*$ by Lemma 6.2.1, so $\mathfrak{a} : \mathfrak{c} \subseteq \mathfrak{a} : cR = \frac{1}{c}\mathfrak{a}$. Assuming R is Noetherian, $\mathfrak{a} : \mathfrak{c}$ is Noetherian because $\frac{1}{c}\mathfrak{a} \cong \mathfrak{a}$ is Noetherian. If $\mathfrak{c}$ is invertible, then $\mathfrak{a} : \mathfrak{c} = \mathfrak{a}(R : \mathfrak{c})$ is fractional.

7. For all maximal ideals $\mathfrak{m}$ choose $a_\mathfrak{m} \in \mathfrak{a}$ and $b_\mathfrak{m} \in R : \mathfrak{a}$ so that $a_\mathfrak{m} b_\mathfrak{m} \in R \setminus \mathfrak{m}$, and choose $\lambda_\mathfrak{m} \in R \setminus \mathfrak{m}$ with $\lambda_\mathfrak{m} \in \mathfrak{n}$ for all maximal $\mathfrak{n} \neq \mathfrak{m}$. Then $a = \sum_\mathfrak{m} \lambda_\mathfrak{m} a_\mathfrak{m} \in \mathfrak{a}$ and $b = \sum_\mathfrak{m} \lambda_\mathfrak{m} b_\mathfrak{m} \in R : \mathfrak{a}$ satisfy $ab \equiv \lambda_\mathfrak{m}^2 a_\mathfrak{m} b_\mathfrak{m} \not\equiv 0 \pmod{\mathfrak{m}}$ for all $\mathfrak{m}$. Hence $ab \in R^*$ and $a \in \mathrm{Q}(R)^*$. Finally $\mathfrak{a} = ab\mathfrak{a} \subseteq a(R : \mathfrak{a})\mathfrak{a} = aR \subseteq \mathfrak{a}$ and we have equality throughout. □

If $\mathfrak{a}$ is an invertible ideal of R, we write $\mathfrak{a}^{-1} = R : \mathfrak{a}$ for the unique R-submodule of $\mathrm{Q}(R)$ such that $\mathfrak{a}\mathfrak{a}^{-1} = R$. We write $\mathcal{I}(R)$ for the set of invertible ideals of R, which by Lemma 6.2.2 is closed under taking inverses, and is thus a group under multiplication.

Example 6.2.3. The group $\mathcal{I}(R)$ can contain non-trivial torsion for an order R in a number field.

Consider $R = \mathbb{Z}[2\mathrm{i}]$. Then $\mathrm{i} \in \mathbb{Q}R \setminus R$ is a fourth root of unity, hence $\mathrm{i}R \in \mathcal{I}(R)$ is non-trivial torsion. More generally, for orders $R \subseteq S \subseteq \mathbb{Q}R$ the group S^*/R^* is torsion and the natural map to $\mathcal{I}(R)$ is injective.

Lemma 6.2.4. *Let* $R \subseteq S \subseteq \mathrm{Q}(R)$ *be commutative (sub)rings. There is a map from the set of fractional ideals of* R *to the set of fractional ideals of* S *that sends* $\mathfrak{a}$ *to* $S\mathfrak{a}$*, and it preserves inverses of invertible ideals and respects addition and multiplication.* □

Theorem 6.2.5. *There exists a polynomial-time algorithm that, given an order R in a number field and a fractional R-ideal $\mathfrak{a}$, computes the unique minimal order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S\mathfrak{a}$ is invertible.*

Proof. In [8] it is shown that $S\mathfrak{a}$ is invertible for the order $S = \mathfrak{a}^n : \mathfrak{a}^n$ with $n = [K : \mathbb{Q}] - 1$. Any order $R \subseteq T \subseteq \mathbb{Q}R$ where $T\mathfrak{a}$ is invertible satisfies $S = \mathfrak{a}^n : \mathfrak{a}^n \subseteq T(\mathfrak{a}^n : \mathfrak{a}^n) \subseteq (T\mathfrak{a}^n) : (T\mathfrak{a}^n) = T$, so S is the unique minimum. □

Theorem 6.2.5 probably also holds when R is any order, with essentially the same proof. This generalization would be sufficient to prove generalizations to general orders for all algorithmic theorems in this chapter.

6.3 Lengths of modules

Let R be a commutative ring and M a R-module. A *chain* in M is a set of submodules of M that is totally ordered by inclusion. We define the *length* of M to be

$$\ell_R(M) = \sup\{\#C \mid C \text{ a chain in } M\} - 1 \in \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

Note that we do not distinguish between infinite cardinal numbers. Similarly we define the *Krull dimension* of R to be

$$\dim(R) = \sup\{\#C \mid C \text{ a chain in } R \text{ of prime ideals}\} - 1.$$

Note that $\ell_R(0) = 0$ and $\dim(0) = -1$. We say M has finite length if $\ell_R(M) < \infty$, which is equivalent to M being both Noetherian and Artinian. For a prime ideal $\mathfrak{p} \subseteq R$ write $R_\mathfrak{p}$ for the localization of R at $\mathfrak{p}$ and $M_\mathfrak{p} = R_\mathfrak{p} \otimes_R M$. If M has finite length we write

$$[M]_R = \left(\ell_{R_\mathfrak{m}}(M_\mathfrak{m})\right)_\mathfrak{m} \in \mathbb{Z}_{\geq 0}^{(\max \operatorname{spec} R)}.$$

where $\max \operatorname{spec} R$ is the set of maximal ideals of R.

Lemma 6.3.1 (Theorem 2.13 in [12])**.** *Let R be a commutative ring and $N \subseteq M$ be R-modules. Then $\ell_R(M) = \ell_R(N) + \ell_R(M/N)$ and*

$$\ell_R(M) = \sum_{\mathfrak{m} \subseteq R} \ell_{R_\mathfrak{m}}(M_\mathfrak{m}),$$

where the sum ranges over all maximal ideals $\mathfrak{m}$. □

Lemma 6.3.2. *Let R be a Noetherian commutative ring. If $\dim(R) \leq 1$, then for every fractional R-ideal $\mathfrak{a} \subseteq R$ the R-module $R/\mathfrak{a}$ has finite length.*

Proof. Write $\mathrm{chain}(R)$ for the set of chains of prime ideals of R. The primes of $R/\mathfrak{a}$ correspond to the primes of R containing $\mathfrak{a}$, so we get a surjective map $f\colon \mathrm{chain}(R) \to \mathrm{chain}(R/\mathfrak{a})$ that discards primes not containing $\mathfrak{a}$. Minimal prime ideals contain no regular elements (Theorem 3.1 in [12]), while $\mathfrak{a}$ does (Lemma 6.2.1). Maximal elements of $\mathrm{chain}(R)$ contain a minimal prime, which gets discarded by f. Hence $\dim(R/\mathfrak{a}) \leq \dim(R) - 1 \leq 0$. It then follows from Corollary 9.1 in [12] that $R/\mathfrak{a}$ has finite length. □

Examples of a Noetherian commutative ring with Krull dimension at most 1 include any order and its localizations.

Proposition 6.3.3. *Let $R \subseteq S \subseteq \mathrm{Q}(R)$ be commutative (sub)rings. If $\dim(R) \leq 1$ and $\ell_R(S/R) < \infty$, then for all invertible ideals $\mathfrak{a} \subseteq R$ we have $[S/S\mathfrak{a}]_R = [R/\mathfrak{a}]_R$.*

Proof. It suffices to prove for local R that $\ell(S/S\mathfrak{a}) = \ell(R/\mathfrak{a})$. In this case $\mathfrak{a} = \alpha R$ for some regular $\alpha \in R$. Note that the map $S/R \to S\mathfrak{a}/\mathfrak{a}$ given by $x \mapsto \alpha x$ is an isomorphism since α is regular in S. We conclude that $\ell(S\mathfrak{a}/\mathfrak{a}) = \ell(S/R) < \infty$. We have exact sequences of R-modules

$$0 \to R/\mathfrak{a} \to S/\mathfrak{a} \to S/R \to 0 \quad \text{and} \quad 0 \to S\mathfrak{a}/\mathfrak{a} \to S/\mathfrak{a} \to S/S\mathfrak{a} \to 0.$$

Hence $\ell(R/\mathfrak{a}) + \ell(S/R) = \ell(S\mathfrak{a}/\mathfrak{a}) + \ell(S/S\mathfrak{a})$ by Lemma 6.3.2. □

Example 6.3.4. With the notation as in Proposition 6.3.3, the R-modules $R/\mathfrak{a}$ and $S/S\mathfrak{a}$ need not be isomorphic. In fact, if R and S are orders, then the modules need not even be isomorphic over $\mathbb{Z}$.

Take $R = \mathbb{Z}[2\mathrm{i}]$ and $S = \mathbb{Z}[\mathrm{i}]$ with $\mathfrak{a} = 2\mathrm{i}R$, which is clearly invertible. Then $R/\mathfrak{a} \cong \mathbb{Z}/4\mathbb{Z}$ and $S/S\mathfrak{a} \cong (\mathbb{Z}/2\mathbb{Z})^2$ as $\mathbb{Z}$-modules, which are non-isomorphic.

Lemma 6.3.5. *Let R be a commutative ring with fractional ideals $\mathfrak{a} \subseteq \mathfrak{b}$. Then there exists some regular $r \in R$ such that $r\mathfrak{b} \subseteq \mathfrak{a}$. If R is Noetherian with $\dim(R) \leq 1$, then $\ell_R(\mathfrak{b}/\mathfrak{a}) < \infty$.*

Proof. We may choose generators $r_1/s_1, \ldots, r_n/s_n \in \mathrm{Q}(R)$ of $\mathfrak{b}$. Then $y = \prod_i s_i$ is regular and satisfies $y\mathfrak{b} \subseteq R$. By Lemma 6.2.1 there exists some regular $x \in R$ such that $xR \subseteq \mathfrak{a}$. Hence we may take $r = xy$. We have a surjection $\mathfrak{b}/xR \to \mathfrak{b}/\mathfrak{a}$, so it suffices to show $\ell_R(\mathfrak{b}/xR) < \infty$. The injection $\mathfrak{b}/xR \to \frac{1}{y}R/xR$ and the fact that $\frac{1}{y}R/xR \cong R/xyR$ has finite length by Lemma 6.3.2 finish the proof. □

As a consequence of Lemma 6.3.5, every fractional ideal $\mathfrak{a}$ of R can be written as $\mathfrak{b} : \mathfrak{c}$ for some ideals $\mathfrak{b}, \mathfrak{c} \subseteq R$ with $\mathfrak{c}$ invertible: As $r\mathfrak{a} \subseteq R$ for some regular r we may take $\mathfrak{b} = r\mathfrak{a}$ and $\mathfrak{c} = rR$. Under additional invertibility assumptions we may even take $\mathfrak{b}$ and $\mathfrak{c}$ coprime.

Lemma 6.3.6. *Let R be a commutative ring and let $\mathfrak{a}$ be a fractional R-ideal such that $\mathfrak{a}$ and $R + \mathfrak{a}$ are invertible. Then $R + \mathfrak{a}^{-1}$ is invertible and $\mathfrak{b} = (R + \mathfrak{a}^{-1})^{-1}$ and $\mathfrak{c} = (R + \mathfrak{a})^{-1}$ satisfy (1) $\mathfrak{b}, \mathfrak{c} \subseteq R$; (2) $\mathfrak{b} + \mathfrak{c} = R$ and (3) $\mathfrak{a} = \mathfrak{b} : \mathfrak{c}$.*

Proof. Note that $R + \mathfrak{a}^{-1} = \mathfrak{a}^{-1}(R + \mathfrak{a})$ is invertible. Rearranging gives $\mathfrak{a} = (R + \mathfrak{a}) : (R + \mathfrak{a}^{-1}) = \mathfrak{b} : \mathfrak{c}$. We have $\mathfrak{b} + \mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{c} = (\mathfrak{a} + R)\mathfrak{c} = R$. In particular, we have $\mathfrak{b}, \mathfrak{c} \subseteq R$. □

Proposition 6.3.7. *There exists a polynomial-time algorithm that, given an order R in a number field and an invertible ideal $\mathfrak{a}$ of R, decides whether $\mathfrak{a}$ is torsion, and if so computes the minimal order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S\mathfrak{a} = S$.*

Proof. We compute using Theorem 6.2.5 the minimal order $R \subseteq S \subseteq \mathbb{Q}R$ where $R + \mathfrak{a}$ becomes invertible. We claim $\mathfrak{a}$ is torsion if and only if $S\mathfrak{a} = S$.

($\Rightarrow$) As $S\mathfrak{a}$ is the quotient of $\mathfrak{b} = (S + (S\mathfrak{a})^{-1})^{-1}$ and $\mathfrak{c} = (S + S\mathfrak{a})^{-1}$ as in Lemma 6.3.6 with $\mathfrak{b} + \mathfrak{c} = S$, the ideal $S\mathfrak{a}$ is torsion if and only if $\mathfrak{b}$ and $\mathfrak{c}$ are. However, since $\mathfrak{b}, \mathfrak{c} \subseteq S$, this is only possible if $\mathfrak{b} = \mathfrak{c} = S$. Hence $S\mathfrak{a} = S : S = S$.

($\Leftarrow$) Let $k \in \mathbb{Z}_{>0}$. For $x \in R : S$ we have $xS = xS\mathfrak{a}^k \subseteq R\mathfrak{a}^k = \mathfrak{a}^k$, so $x \in \mathfrak{a}^k$. Hence $R : S \subseteq \mathfrak{a}^k \subseteq S$. By Lemma 6.3.5 the R-module $S/(R : S)$ has finite length, so in particular it is a finite group. Thus $\mathfrak{a}^k$ can take only finitely many values, so by invertibility $\mathfrak{a}$ must be torsion.

Finally, suppose that $\mathfrak{a}$ is torsion and $R \subseteq T \subseteq \mathbb{Q}R$ is an order such that $T\mathfrak{a} = T$. Then $T(R + \mathfrak{a}) = T$ is invertible, so $S \subseteq T$. Hence S is the unique minimal order where $S\mathfrak{a} = S$. □

6.4 Coprime bases

It is easy to see that for a set C of pairwise coprime invertible proper ideals of a commutative ring R the natural map $\mathbb{Z}^{(C)} \to \mathcal{I}(R)$ is injective with image $\langle C \rangle$ and that $\langle C \rangle$ is closed under addition. In fact, $\mathbb{Z}^{(C)} \to \langle C \rangle$ is an isomorphism of partially ordered groups.

Lemma 6.4.1. *There exists a polynomial-time algorithm that, given a reduced order R and a finite set C of pairwise coprime invertible proper ideals*

of R and some invertible ideal $\mathfrak{a}$ of R, decides whether $\mathfrak{a}$ is in the image of the injection $\mathbb{Z}^{(C)} \to \mathcal{I}(R)$ and if so computes the preimage.

Proof. First verify whether $R+\mathfrak{a}$ is invertible, as it should be if $\mathfrak{a} \in \langle C \rangle$. If so, then by Lemma 6.3.6 we may write $\mathfrak{a} = \mathfrak{b} : \mathfrak{c}$ for invertible $\mathfrak{b}, \mathfrak{c} \subseteq R$. We then proceed using trial division. □

Definition 6.4.2. Given a commutative ring R and a set X of fractional ideals contained in R, we write $\langle\langle X \rangle\rangle$ for the multiplicative monoid generated by X with unit R, and we define the *closure of* X, written $\mathrm{cl}_R(X)$ or simply $\mathrm{cl}(X)$, to be the smallest set of fractional ideals in R such that $\langle\langle X \rangle\rangle \subseteq \mathrm{cl}(X)$ and for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{cl}(X)$ we have $\mathfrak{ab}, \mathfrak{a}+\mathfrak{b} \in \mathrm{cl}(X)$, and if $\mathfrak{b}$ is invertible and $\mathfrak{a} : \mathfrak{b} \subseteq R$ also $\mathfrak{a} : \mathfrak{b} \in \mathrm{cl}(X)$.

From Lemma 6.2.4 we deduce the following.

Lemma 6.4.3. *Let $R \subseteq S \subseteq \mathrm{Q}(R)$ be commutative (sub)rings and let X be a set of fractional ideals contained in R. Writing $S \cdot X = \{S\mathfrak{a} \mid \mathfrak{a} \in X\}$, we have $S \cdot \mathrm{cl}_R(X) \subseteq \mathrm{cl}_S(S \cdot X)$.* □

Lemma 6.4.4. *Let R be a commutative ring R and C a set of invertible ideals contained in R which are pairwise coprime. Then* $\mathrm{cl}(C) = \langle\langle C \rangle\rangle$.

Proof. Clearly $\langle\langle C \rangle\rangle \subseteq \mathrm{cl}(C)$. For all $\mathfrak{a}, \mathfrak{b} \in \langle\langle C \rangle\rangle$ we may write $\mathfrak{a} = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{a_\mathfrak{c}}$ and $\mathfrak{b} = \prod_{\mathfrak{c}} \mathfrak{c}^{b_\mathfrak{c}}$ with $a_\mathfrak{c}, b_\mathfrak{c} \in \mathbb{Z}_{\geq 0}$. Then

$$\mathfrak{a} + \mathfrak{b} = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{\min\{a_\mathfrak{c}, b_\mathfrak{c}\}} \quad \text{and} \quad \mathfrak{a} : \mathfrak{b} = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{a_\mathfrak{c} - b_\mathfrak{c}}.$$

Hence $\mathfrak{a}+\mathfrak{b} \in \langle\langle C \rangle\rangle$, and $\mathfrak{a} : \mathfrak{b} \in \langle\langle C \rangle\rangle$ if $\mathfrak{a} : \mathfrak{b} \subseteq R$. Thus $\langle\langle C \rangle\rangle = \mathrm{cl}(C)$. □

Definition 6.4.5. Let R be a commutative ring and X a set of fractional ideals contained in R. A *coprime basis* for X is a set C of invertible proper ideals of R, which are pairwise coprime and satisfy $X \subseteq \langle\langle C \rangle\rangle$.

Note that a coprime basis need not exist for every X. At the very least, the ideals in X should be invertible.

Lemma 6.4.6. *For a commutative ring R and a set X of fractional ideals contained in R we may equip the set of coprime bases of X with a partial order where $C \leq D$ if and only if $\langle\langle C \rangle\rangle \subseteq \langle\langle D \rangle\rangle$.*

Proof. It suffices to verify for coprime bases C and D that $\langle\langle C \rangle\rangle = \langle\langle D \rangle\rangle$ implies $C = D$. Let $m_{\mathfrak{cd}} \in \mathbb{Z}_{\geq 0}$ be such that $\mathfrak{c} = \prod_{\mathfrak{d} \in D} \mathfrak{d}^{m_{\mathfrak{cd}}}$. Since the elements of C are pairwise coprime, there is for every $\mathfrak{d} \in D$ at most one

$\mathfrak{c} \in C$ such that $m_{\mathfrak{c}\mathfrak{d}} > 0$. Because $\langle\langle D \rangle\rangle \subseteq \langle\langle C \rangle\rangle$, there is no $\mathfrak{d} \in D$ such that for all $\mathfrak{c} \in C$ we have $m_{\mathfrak{c}\mathfrak{d}} = 0$.

Let $\mathfrak{d} \in D$. Then there exist $\mathfrak{c} \in C$ and $m > 0$ such that $\mathfrak{c} = \mathfrak{d}^m$ and in turn by symmetry $\mathfrak{e} \in D$ and $n > 0$ such that $\mathfrak{e} = \mathfrak{c}^n$. Then $\mathfrak{e} = \mathfrak{d}^{mn}$, so $\mathfrak{e} = \mathfrak{d}$ and $m = n = 1$. Thus $\mathfrak{d} = \mathfrak{c} \in C$ and $D \subseteq C$. By symmetry we have $C = D$. □

Proposition 6.4.7. *Let R be a Noetherian commutative ring and X a set of fractional ideals contained in R. Then:*

1. *X has a coprime basis if and only if $\mathrm{cl}(X) \subseteq \mathcal{I}(R)$;*
2. *if X has a coprime basis, then it has a unique minimal one;*
3. *if C is a coprime basis of X, then C is minimal if and only if $C \subseteq \mathrm{cl}(X)$.*

Proof. (1) Suppose X has a coprime basis D. Then $X \subseteq \langle\langle D \rangle\rangle = \mathrm{cl}(D)$ by Lemma 6.4.4, so $\mathrm{cl}(X) \subseteq \mathrm{cl}(D) = \langle\langle D \rangle\rangle \subseteq \mathcal{I}(R)$. Suppose instead that $\mathrm{cl}(X) \subseteq \mathcal{I}(R)$. We will show that

$$C = \{\mathfrak{a} \in \mathrm{cl}(X) \mid \forall\, \mathfrak{b} \in \mathrm{cl}(X),\ \mathfrak{a} \subsetneq \mathfrak{b} \Leftrightarrow \mathfrak{b} = R\}$$

is a coprime basis of X.

First, note that the elements of C are pairwise coprime: For $\mathfrak{a}, \mathfrak{b} \in C$ we have $\mathfrak{a} + \mathfrak{b} \in \mathrm{cl}(X)$. If $\mathfrak{a} \subsetneq \mathfrak{a} + \mathfrak{b}$, then $\mathfrak{a} + \mathfrak{b} = R$ by definition of C, and similarly when $\mathfrak{b} \subsetneq \mathfrak{a} + \mathfrak{b}$. Otherwise $\mathfrak{a} = \mathfrak{a} + \mathfrak{b} = \mathfrak{b}$. Second, we show $\mathrm{cl}(X) \subseteq \langle\langle C \rangle\rangle$ using Noetherian induction: Certainly $R \in \langle\langle C \rangle\rangle$. Now let $\mathfrak{a} \in \mathrm{cl}(X) \setminus \{R\}$ and suppose $\mathfrak{c} \in \langle\langle C \rangle\rangle$ for all $\mathfrak{c} \in \mathrm{cl}(X)$ with $\mathfrak{a} \subsetneq \mathfrak{c}$. Either $\mathfrak{a} \in C$, or there is some $\mathfrak{b} \in \mathrm{cl}(X)$ such that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$, in which case $\mathfrak{b}, (\mathfrak{a} : \mathfrak{b}) \in \langle\langle C \rangle\rangle$ by the induction hypothesis and hence $\mathfrak{a} \in \langle\langle C \rangle\rangle$. Thus C is a coprime basis for X, as was to be shown.

(2) Suppose now that X has a coprime basis. We will show that C as in (1) is the unique minimal coprime basis. Let D be any coprime basis of X. We have $C \subseteq \mathrm{cl}(X)$, so $\mathrm{cl}(C) \subseteq \mathrm{cl}(X)$. On the other hand, $X \subseteq \mathrm{cl}(C)$, so $\mathrm{cl}(C) = \mathrm{cl}(X)$. Similarly for D we have $\mathrm{cl}(X) \subseteq \mathrm{cl}(D)$. Hence $\langle\langle C \rangle\rangle = \mathrm{cl}(C) = \mathrm{cl}(X) \subseteq \mathrm{cl}(D) = \langle\langle D \rangle\rangle$ by Lemma 6.4.4. Thus $C \leq D$, as was to be shown.

(3) It is clear that the minimal coprime basis from (2) satisfies $C \subseteq \mathrm{cl}(X)$. Let D be any coprime basis of X such that $D \subseteq \mathrm{cl}(X)$. Then as before we obtain $\langle\langle D \rangle\rangle = \mathrm{cl}(D) = \mathrm{cl}(X)$. Hence $\langle\langle C \rangle\rangle = \mathrm{cl}(X) = \langle\langle D \rangle\rangle$ and $C = D$ by Lemma 6.4.6. Hence D is minimal. □

Theorem 6.4.8. *There exists a polynomial-time algorithm that, given a order R in a number field and a finite set X of fractional ideals contained*

in R, computes the unique minimal order S such that $R \subseteq S \subseteq \mathbb{Q}R$ and $\mathrm{cl}(S \cdot X) \subseteq \mathcal{I}(S)$, and then computes the minimal coprime basis of $S \cdot X$.

Note that the output of this algorithm is clearly functorial under isomorphisms of R.

Proof. Start with S equal to the minimal order $R \subseteq S \subseteq \mathrm{Q}(R)$ where the elements of X become invertible using Theorem 6.2.5, and let $C = X$.

Iteratively compute $\mathfrak{c} = S\mathfrak{a} + S\mathfrak{b}$ for distinct $\mathfrak{a}, \mathfrak{b} \in C$. If $\mathfrak{c} \neq S$, replace S by the unique minimal order $S \subseteq T \subseteq \mathrm{Q}(R)$ where $T\mathfrak{c}$ is invertible using Theorem 6.2.5, replace $\mathfrak{a}$ and $\mathfrak{b}$ in C by $T\mathfrak{a} : T\mathfrak{c}$ and $T\mathfrak{b} : T\mathfrak{c}$, and add $T\mathfrak{c}$ to C. Once $S\mathfrak{a} + S\mathfrak{b} = S$ for all distinct $\mathfrak{a}, \mathfrak{b} \in C$ we terminate and return the order S and coprime basis $S \cdot C$.

Polynomial run time follows from the fact that $\sum_{\mathfrak{a} \in C} \ell_R(S/\mathfrak{a}S)$, which is bounded by the length of the input, decreases by at least 1 after every iteration where $\mathfrak{c} \neq S$. For this, the fact that S changes throughout the algorithm is irrelevant by Proposition 6.3.3. This also gives a polynomial bound on $\#C$ and hence the number of pairs $\mathfrak{a}, \mathfrak{b} \in C$ to check for coprimality every iteration.

It remains to show correctness. With induction on the number of steps one shows that during the algorithm $S \cdot X \subseteq \langle\!\langle S \cdot C \rangle\!\rangle$, so that $S \cdot C$ is indeed a coprime basis for $S \cdot X$, and $S \cdot C \subseteq \mathrm{cl}(S \cdot X)$, so it is minimal by Proposition 6.4.7. Suppose $R \subseteq T \subseteq \mathrm{Q}(R)$ be such that $\mathrm{cl}(TX) \subseteq \mathcal{I}(T)$. Then at every point of the algorithm we could replace S by $S \cap T$ and preserve invertibility, so $S \subseteq T$ at every step by minimality of S guaranteed by Theorem 6.2.5. Hence S is minimal such that $\mathrm{cl}(SX) \subseteq \mathcal{I}(S)$, and the algorithm is correct. □

In the above algorithm, once $S\mathfrak{a} + S\mathfrak{b} = S$ for some S, we will also have $T\mathfrak{a} + T\mathfrak{b} = T$ for any $S \subseteq T \subseteq \mathrm{Q}(R)$. Keeping track of which pairs are coprime could speed up the iterative algorithm in practice. Moreover, once we compute $S\mathfrak{a}$ we may replace $\mathfrak{a}$ in C by $S\mathfrak{a}$ to potentially speed up later computations.

6.5 Fitting ideals

Let R be a commutative ring and M a finitely generated R-module. Then there exists an exact sequence

$$R^{(I)} \xrightarrow{f} R^n \to M \to 0$$

for some set I and $n \in \mathbb{Z}_{\geq 0}$, where we interpret f as a matrix. Note that I can be infinite, as M need not be finitely presentable. For $k \leq n$ we define the *k-th Fitting ideal of M*, written $\mathrm{Fit}_k(M)$, to be the R-ideal generated by the determinants of all $(n-k) \times (n-k)$ minors of the matrix f, which is 0 when no such minors exist. Note that $\mathrm{Fit}_k(M) = 0$ for $k < 0$, and vacuously $\mathrm{Fit}_n(M) = R$ as the determinant of a 0×0 matrix is 1. It is clear that $\mathrm{Fit}_i(M) \subseteq \mathrm{Fit}_j(M)$ for $i \leq j \leq n$. We extend the definition of $\mathrm{Fit}_k(M)$ to arbitrary $k \in \mathbb{Z}$ where $\mathrm{Fit}_k(M) = R$ for $k > n$. By a theorem of Fitting [14] the Fitting ideals do not depend on the choice of exact sequence.

Lemma 6.5.1. *Let R be a non-zero Artinian commutative ring, M a finitely generated R-module and $k \in \mathbb{Z}_{\geq 0}$. Then:*

1. *M can be generated by k elements if and only if $\mathrm{Fit}_k(M) = R$;*
2. *M is free of rank k if and only if $\mathrm{Fit}_{k-1}(M) = 0$ and $\mathrm{Fit}_k(M) = R$;*
3. *if M is free of rank k, then every set of generators of M of cardinality k is a basis.*

Proof. The first two follow from Propositions 20.6 and 20.8 in [12], while the third is elementary. □

Proposition 6.5.2. *There exists a polynomial time algorithm that, given a finite commutative ring R and a finitely generated R-module M, computes the minimal number of generators n for M, and $\mathrm{Fit}_{n-1}(M)$.*

Proof. Using Theorem 4.1.3 from [5] we may compute such minimal n and generators $m_1, \ldots, m_n$ of M. We may then compute an exact sequence $R^m \xrightarrow{f} R^n \to M \to 0$, so that $\mathrm{Fit}_{n-1}(M)$ is the ideal generated by the coefficients of f. □

It is very possible a more direct proof of Proposition 6.5.2 can be given.

6.6 Finite-étale algebras

Let R be a commutative ring and S an R-algebra. We write S^{o} for the opposite ring of S. Then $S^{\mathrm{e}} = S \otimes_R S^{\mathrm{o}}$ is a ring and S is an S^{e}-module where the module structure is given by $(s \otimes s') \cdot t = sts'$. We say S is *separable* if S is projective as S^{e}-module. We say S is *finite-étale* over R if S is commutative and S is projective and separable over R.

Lemma 6.6.1. *Let R be a commutative ring and S a finite-étale R-algebra. Then*

1. *for all ideals $\mathfrak{a} \subseteq R$ the $R/\mathfrak{a}$-algebra $S/\mathfrak{a}S$ is finite-étale;*
2. *for all maximal ideals $\mathfrak{m} \subseteq R$ the $R_{\mathfrak{m}}$-algebra $S_{\mathfrak{m}}$ is finite-étale;*

3. *if R is a field, then S is a product of fields.*

Proof. For 1 and 2 it suffices to verify separability. For 1 it is trivial that $R/\mathfrak{a}$ is separable over R, hence $S/\mathfrak{a}S$ is separable over $R/\mathfrak{a}$ by Proposition III.1.7 of [28]. For 2 we have Proposition III.2.5 of [28]. Finally, 3 is a consequence of Theorem III.3.1 of [28]. □

Proposition 6.6.2. *There exists a polynomial-time algorithm that, given a finite commutative ring R and a finite commutative R-algebra S, decides whether S is finite-étale over R and if not, computes either some ideal $0 \subsetneq \mathfrak{a} \subsetneq R$ or some ideal $0 \subsetneq \mathfrak{b} \subsetneq S$. The output of this algorithm is functorial under isomorphisms.*

Proof. Projectivity over finite rings can be tested using Theorem 5.4.1 from [5], hence the finite-étale property can be tested. Suppose S is not finite-étale. If S is not free over R, then the ideal $\mathfrak{a}$ we obtain from Proposition 6.5.2 satisfies $0 \subsetneq \mathfrak{a} \subsetneq R$ by Lemma 6.5.1. If S is not separable over $\mathbb{Z}$, we obtain a ideal $0 \subsetneq \mathfrak{b} \subsetneq S$ from Proposition 6.1.3 from [5] which is functorial under isomorphisms.

Suppose S is free over R and separable over $\mathbb{Z}$. Then certainly S is projective over R. Hence S is separable over R by Proposition 6.2.14.ii from [5], so S is finite-étale over R. □

6.7 Roots of ideals

In this section we will prove the main theorems on taking roots in orders.

Proposition 6.7.1. *Let $Z \subseteq R \subseteq S \subseteq \mathrm{Q}(R)$ be commutative (sub)rings such that Z is Dedekind and S is finitely generated as a Z-module. Let $\mathfrak{a} \subseteq R$ be an invertible ideal. Write $a = \mathfrak{a} \cap Z$ and suppose $R/\mathfrak{a}$ is finite-étale over Z/a. If $m \in \mathbb{Z}_{\geq 0}$ is such that there exists an ideal $\mathfrak{b} \subseteq S$ with $S\mathfrak{a} = \mathfrak{b}^m$, then there exists an ideal $b \subseteq Z$ with $a = b^m$.*

In this proposition one can think of Z as $\mathbb{Z}$ and S as the maximal order of a number field $\mathrm{Q}(R)$.

Proof. It suffices to prove the proposition for local Z: All conditions on the rings and ideals are preserved by localization at a prime of Z, which for the finite-étale property is Lemma 6.6.1.2, and the conclusion holds if it holds everywhere locally. If Z is a field, then $Z = R = S = \mathrm{Q}(R)$ and the proposition holds trivially. Thus we may assume Z is a discrete valuation ring with maximal ideal $p = \pi Z$. Note that Z is Noetherian, hence S and consequently R are Noetherian Z-modules and in particular Noetherian

rings. Hence because Z is semi-local and of dimension 1, so are both R and S.

Suppose $\mathfrak{b} \subseteq S$ is such that $S\mathfrak{a} = \mathfrak{b}^m$. Write $a = p^k$ for some $k \geq 0$. To show there exists an ideal b with $a = b^m$, it suffices to show that $m \mid k$. We may assume that $k > 0$, otherwise this is trivial. Because $\mathfrak{a}$ and $\mathfrak{b}$ are invertible ideals of a semi-local ring, we have $\mathfrak{a} = \alpha R$ and $\mathfrak{b} = \beta S$ for some regular $\alpha \in R$ and $\beta \in S$ by Lemma 6.2.2.7.

By Lemma 6.3.5 we have $\ell_R(S/R) < \infty$, so by Proposition 6.3.3 we have $[R/\alpha R]_R = [S/\alpha S]_R$. We have inclusions

$$S \supseteq \beta S \supseteq \cdots \supseteq \beta^m S = \alpha S.$$

For all i we have an isomorphism $S/\beta S \to \beta^i S/\beta^{i+1} S$ since β^i is regular, so

$$[R/\alpha R]_R = [S/\alpha S]_R = m \cdot [S/\beta S]_R.$$

Write $A_i = \pi^i \cdot (R/\alpha R)$. We have inclusions

$$A_0 \supseteq A_1 \supseteq \cdots \supseteq A_k = 0.$$

Because $R/\alpha R$ as $Z/\pi^k Z$-algebra is finite-étale by assumption, it is projective and hence free. Therefore multiplication by π^i for $0 \leq i < k$ is an isomorphism $A_0/A_1 \to A_i/A_{i+1}$ of Z-modules and hence of R-modules. We conclude that

$$k \cdot [A_0/A_1]_R = [R/\alpha R]_R = m \cdot [S/\beta S]_R.$$

Note that A_0/A_1 is finite-étale over $Z/\pi Z$ by Lemma 6.6.1, and that $Z/\pi Z$ is a field. Hence $A_0/A_1 = R/(\alpha R + \pi R)$ is a product of fields. In particular, if we choose any maximal $\mathfrak{m} \subset R$ containing $\alpha R + \pi R$ we obtain $[A_0/A_1]_R(\mathfrak{m}) = \ell_{R_\mathfrak{m}}((A_0/A_1)_\mathfrak{m}) = 1$. It follows that $k = m \cdot [S/\beta S]_R(\mathfrak{m})$, as was to be shown. □

Example 6.7.2. Under the assumptions of Proposition 6.7.1 it need not be the case that $\mathfrak{a}$ itself be an m-th power in $\mathcal{I}(R)$.

Let $R = \mathbb{Z}[2\sqrt{2}]$ and $\mathfrak{a} = (2 + 2\sqrt{2})R$. Then $R/\mathfrak{a} \cong \mathbb{Z}/a$ as $\mathbb{Z}/a$-algebra for $a = \mathfrak{a} \cap \mathbb{Z} = 4\mathbb{Z}$, so $R/\mathfrak{a}$ is certainly étale. Since $1 + \sqrt{2}$ is a unit in the maximal order $S = \mathbb{Z}[\sqrt{2}]$, we have that $S\mathfrak{a} = (S\sqrt{2})^2$. Suppose $\mathfrak{c} \in \mathcal{I}(R)$ satisfies $\mathfrak{c}^2 = \mathfrak{a}$. Square roots of ideals in S are unique, so $S\mathfrak{c} = S\sqrt{2}$ and $\mathfrak{c} \subseteq S\sqrt{2}$. On the other hand we have

$$\mathfrak{c} = \mathfrak{a} \cdot (R : \mathfrak{c}) \supseteq \mathfrak{a} \cdot (S2 : S\sqrt{2}) = 2\sqrt{2}S.$$

Thus $\mathfrak{c}$ corresponds to some R-submodule $\mathfrak{d}$ of $S/2S$ with square $(1+\sqrt{2})R+2S$. Clearly $\mathfrak{d} \neq S/2S$, so $\mathfrak{d} = dR + 2S$ for some $d \in S/2S$. As $d^2 \in \{0, 1\}$ we conclude that $\mathfrak{d}^2 \neq (1 + \sqrt{2})R + 2S$, so no such $\mathfrak{c}$ exists.

Theorem 6.7.3. *There exists a polynomial-time algorithm that, given an order R in a number field and fractional ideal $\mathfrak{a}$ of R, computes the maximal $n \in \mathbb{Z}_{\geq 0}$ with respect to divisibility for which there exist an order $R \subseteq S \subseteq \mathbb{Q}R$ and fractional ideal $\mathfrak{b}$ of S such that $\mathfrak{b}^n = S\mathfrak{a}$, where $\mathfrak{b}^0 := S$, and additionally computes such S and $\mathfrak{b}$. The output of this algorithm is functorial under isomorphisms of R.*

Note that $n = 0$ corresponds to the case where $\mathfrak{a}$ is torsion.

Proof. First compute some order $R \subseteq S \subseteq \mathrm{Q}(R)$ such that $S\mathfrak{a}$ and $S+S\mathfrak{a}$ are invertible using Theorem 6.2.5. Then write $S\mathfrak{a} = \mathfrak{a}_+ : \mathfrak{a}_-$ with $\mathfrak{a}_+, \mathfrak{a}_- \subseteq S$ invertible and coprime as in Lemma 6.3.6, and apply the algorithm recursively to $\mathfrak{a}_+$ and $\mathfrak{a}_-$ separately with S in the place of R. Since the ideals are coprime, we may obtain a solution $n = \gcd(n_+, n_-)$ from solutions n_+ and n_- for $\mathfrak{a}_+$ and $\mathfrak{a}_-$ respectively, and similarly we may construct S and $\mathfrak{b}$. Hence we may now assume that $\mathfrak{a} \subsetneq R$.

Suppose that at some point during the algorithm we obtain an ideal $\mathfrak{a} \subsetneq \mathfrak{d} \subsetneq R$. Then compute some extension T and a coprime basis C for $\{T\mathfrak{a}, T\mathfrak{d}\}$ using Theorem 6.4.8. Using Lemma 6.4.1 we may write $T\mathfrak{a} = \prod_{\mathfrak{c} \in C} (T\mathfrak{c})^{m_\mathfrak{c}}$ for some $m_\mathfrak{c} \in \mathbb{Z}_{\geq 0}$. As before we may solve the problem by applying the algorithm recursively to all $\mathfrak{c} \in C$. By the assumption on $\mathfrak{d}$ we have $\mathfrak{a} \subsetneq \mathfrak{c}$ for all $\mathfrak{c} \in C$, so the recursion is well-founded.

Now we proceed to the actual algorithm. Compute $a \in \mathbb{Z}_{>1}$ such that $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$. By Proposition 6.6.2 we may assume that $R/\mathfrak{a}$ is finite-étale over $\mathbb{Z}/a\mathbb{Z}$, otherwise we can proceed recursively as above. Then write $a = b^m$ for some $b, m \in \mathbb{Z}_{>0}$ with m maximal. If $b \notin \mathfrak{a}$, then we may proceed recursively with $\mathfrak{d} = bR + \mathfrak{a}$. Otherwise $b \in a\mathbb{Z}$, so $a = b$ and $m = 1$, in which case the solution is $n = 1$ and $\mathfrak{b} = \mathfrak{a}$ by Proposition 6.7.1.

That the algorithm runs in polynomial time follows from all theorems applied. □

Corollary 6.7.4. *There exists a polynomial-time algorithm that, given an order R in a number field, a fractional ideal $\mathfrak{a}$ of R and a positive integer n, decides whether there exist an order $R \subseteq S \subseteq \mathbb{Q}R$ and fractional ideal $\mathfrak{b}$ of S such that $\mathfrak{b}^n = S\mathfrak{a}$ and if so computes such S and $\mathfrak{b}$. The output of this algorithm is functorial under isomorphisms of R.* □

Example 6.7.5. A fractional ideal of an order R can have a square root in an order $R \subseteq S \subseteq \mathbb{Q}R$, while not having such a square root in R, even when R is a domain.

Let $R = \mathbb{Z}[2\mathrm{i}]$ and $\mathfrak{a} = 2R$. For $S = \mathbb{Z}[\mathrm{i}]$ and $\mathfrak{c} = (1 + \mathrm{i})S$ we have $\mathfrak{c}^2 = 2\mathrm{i}S = \mathfrak{a}S$, so $\mathfrak{a}$ has a square root in a larger order. Since S is Dedekind, the group $\mathcal{I}(S)$ is torsion-free, so $\mathfrak{c}$ is even the unique square root of $\mathfrak{a}S$.

Suppose $\mathfrak{b}$ is some fractional ideal of R such that $\mathfrak{b}^2 = \mathfrak{a}$. Then $\mathfrak{b}S = \mathfrak{c}$ by uniqueness of $\mathfrak{c}$, so $\mathfrak{b} \subseteq \mathfrak{c} \subseteq S$. Let $x \in \mathfrak{b}$. Then $x = s + t\mathrm{i}$ for $s, t \in \mathbb{Z}$. As

$$2R = \mathfrak{b}^2 \ni x^2 = (s^2 - t^2) + 2st\mathrm{i},$$

we conclude that $s, t \in 2\mathbb{Z}$. Hence $\mathfrak{b} \subseteq 2S$. But then $2R = \mathfrak{b}^2 \subseteq 4S$, which is false. Hence $\mathfrak{b}$ does not exist.

Example 6.7.6. It is impossible to functorially take square roots of ideals in arbitrary number rings without passing to a larger order.

Consider $R = \mathbb{Z}[2\mathrm{i}]$ with invertible fractional ideals $\mathfrak{b} = 2(1 + \mathrm{i})R \subseteq R$ and $\mathfrak{c} = 2(1 - \mathrm{i})R \subseteq R$. We have $\mathfrak{b}^2 = 8\mathrm{i}R = \mathfrak{c}^2$. Note that $8\mathrm{i}R$ is invariant under the automorphism group of R, so likewise should a functorially chosen square root of it be invariant. Since $\mathfrak{b}$ and $\mathfrak{c}$ are distinct conjugates, there should be a third square root of $8\mathrm{i}R$. We will show that the 2-torsion subgroup $\mathcal{I}(R)[2]$ of $\mathcal{I}(R)$ has cardinality 2, giving a contradiction.

Suppose $\mathfrak{a} \in \mathcal{I}(R)$ satisfies $\mathfrak{a}^2 = R$. Write $S = \mathbb{Z}[\mathrm{i}]$ for the maximal order. Then $(S\mathfrak{a})^2 = S$, and because S is Dedekind also $S\mathfrak{a} = S$, so $\mathfrak{a} \subseteq S$. On the other hand we have $\mathfrak{a} \supseteq \mathfrak{a}^2(R : \mathfrak{a}) \supseteq R(R : S) = 2S$. Hence $\mathfrak{a}$ corresponds to some subgroup of $S/2S$. Clearly $\mathfrak{a}$ is neither S nor $2S$, leaving 3 possible subgroups. However, the order of $\mathcal{I}(R)[2]$ is a non-trivial power of 2, so this power must be 2, as was to be shown.

6.8 Reduced coprime bases

Now that we can take roots of ideals we will use this to give a variation on the coprime basis algorithm (Theorem 6.4.8).

Definition 6.8.1. Let G be a group. We say a subgroup $H \subseteq G$ is *pure* if for all $h \in H$ and $k \in \mathbb{Z}_{>0}$ for which there exists a $g \in G$ such that $g^k = h$, such a g exists in H.

Lemma 6.8.2. *Let R be a reduced order. Suppose $H \subseteq \mathcal{I}(R)$ is a finitely generated torsion-free subgroup, then H is a direct summand of $\mathcal{I}(R)$ if and only if it is a pure subgroup.*

Proof. We have a natural isomorphism $\mathcal{I}(R) \cong \bigoplus_{\mathfrak{p}} \mathcal{I}(R_{\mathfrak{p}})$ and H is a subgroup of some direct summand $G = \bigoplus_{\mathfrak{p} \in \mathcal{P}} \mathcal{I}(R_{\mathfrak{p}})$ for a finite set of maximal ideals $\mathcal{P}$. Note that H is pure in $\mathcal{I}(R)$ if and only if it is pure in G. Since G is finitely generated and H is torsion free, the equivalence follows. □

Definition 6.8.3. Let R be a commutative ring, X a set of fractional ideals contained in R and C a coprime basis of X. We say that C is *reduced* if $\langle C \rangle$ is

a pure subgroup of $\mathcal{I}(R)$. Let $\mathcal{O}$ be the integral closure of R in $\mathrm{Q}(R)$. We say that C is *strongly reduced* if $S \cdot C$ is reduced for every subring $R \subseteq S \subseteq \mathcal{O}$.

Equivalently, C is strongly reduced if $\mathcal{O} \cdot C$ is reduced.

Example 6.8.4. Not every X that admits a coprime basis also admits a reduced coprime basis.

Consider $R = \mathbb{Z}[\sqrt[2]{2}, \sqrt[3]{2}]$ and $X = \{2R\}$ and suppose C is a reduced coprime basis of X. As $(\sqrt[2]{2}R)^2 = 2R = (\sqrt[3]{2}R)^3$ the group $\langle C \rangle$ should include a second and third root of $2R$. If we uniquely express $2R = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{k_\mathfrak{c}}$, then $6 \mid k_\mathfrak{c}$ for all $\mathfrak{c}$. In particular, $2R = \mathfrak{b}^6$ for some $\mathfrak{b} \subseteq R$. Since $R/2R \cong (\mathbb{Z}/2\mathbb{Z})^6$ as group, we must have that $\ell_{\mathbb{Z}/2\mathbb{Z}}(R/\mathfrak{b}) = 1$ and $R/\mathfrak{b} \cong \mathbb{Z}/2\mathbb{Z}$ as ring. Hence $\mathfrak{b}$ is a prime above 2, which must be $\mathfrak{b} = \sqrt[2]{2}R + \sqrt[3]{2}R$. As $\mathfrak{b}^5 \subseteq 2R$ we have that $\mathfrak{b}^6 \neq 2R$, so we arrive at a contradiction.

Theorem 6.8.5. *There exists a polynomial-time algorithm that, given a order R in a number field and a finite set X of fractional ideals contained in R, computes an order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S \cdot X$ has a strongly reduced coprime basis and computes such a coprime basis. The output of this algorithm is functorial under isomorphisms of R.*

Proof. Compute an order $R \subseteq S \subseteq \mathbb{Q}R$ and a minimal coprime basis C for $S \cdot X$ using Theorem 6.4.8. Then compute an order $S \subseteq T \subseteq \mathbb{Q}R$ where every $T\mathfrak{c}$ for $\mathfrak{c} \in C$ has a maximal root $\mathfrak{b}_\mathfrak{c}$ and compute $B = \{\mathfrak{b}_\mathfrak{c} \mid \mathfrak{c} \in C\}$ using Theorem 6.7.3. From the fact that the elements of B are pairwise coprime we may deduce that $\langle B \rangle$ is pure, even for larger orders in $\mathbb{Q}R$. Hence B is strongly reduced. One easily verifies that B is minimal. □

Cover

The cover of this thesis features abstract sunflowers, each of which is constructed as the Voronoi tesselation of a spiral of points that is subsequently projected onto the surface of revolution of a hyperbolic spiral. The image was created in the Python API of Blender (v3.5.1) using the SciPy library (v1.10.1). It is produced by the following code, which is optimized for compactness.

```
import bpy, bmesh, numpy as np; from scipy.spatial import Voronoi
nm,a2,col=np.linalg.norm,np.arctan2,bpy.data.collections.new('c')
def make_cell(vs,fs,cs,s):
  r,i=[a if a >= 0 else len(cs) for a in s],len(vs)
  l=[cs[a] for a in s if a>=0]; c=sum(l)/len(l); cs+=[c*3/nm(c)]
  x=sorted([(nm(cs[a]),cs[a]) for a in r]); d=(x[0][1]+x[-1][1])/2
  t=min(nm(d)*.2,.15); t=0 if t<.03 else t
  l=[(1-t)*cs[a]+t*c for a in r]; vs+=[list(d)+[0]]
  for c,d in zip(l,l[1:]+[l[0]]):
    for t in np.linspace(0,1,max(2,int(10*nm(c-d))))[1:]:
      vs+=[list(t*d+(1-t)*c)+[0]]; fs+=[[i,len(vs)-1,len(vs)]]
  fs[-1][-1]=i+1; return (vs,fs,cs)
def make_object(name,mesh,colors,location,cuts):
  l,m=bpy.data.meshes.new(name),bpy.data.materials.new(name)
  m.use_nodes=True; n=m.node_tree.nodes
  x=[n.get('Material_Output')]+list(map(lambda s:n.new('ShaderNode'
    +s),2*['BsdfDiffuse']+['MixShader','NewGeometry']))
  for i,a,j,b in [(0,0,3,0),(3,1,1,0),(3,2,2,0),(3,0,4,6)]:
    m.node_tree.links.new(x[i].inputs[a],x[j].outputs[b])
  for i in [0,1]: x[i+1].inputs[0].default_value=colors[i]
  l.from_pydata(mesh[0],[],mesh[1]); l.update()
  o=bpy.data.objects.new(name,l); o.data.materials.append(m)
  col.objects.link(o); o.location,m=(location,0,0),bmesh.new()
  m.from_mesh(o.data); bmesh.ops.subdivide_edges(m,edges=m.edges,
    use_grid_fill=1, cuts=cuts); m.to_mesh(o.data); o.data.update()
  for v in o.data.vertices:
    t=nm(v.co); p=(v.co/t)*(1.-np.sin(4*t)/4/t)
    v.co=[p[0],p[1],-np.cos(4*t)/4/t]
def mkflower(offset,rad=.65,exp=.6,cell=350):
  p=2*np.pi; ct=lambda a,r:r*np.array([np.cos(p*a),np.sin(p*a)])
  points=[ct(.6180339*c,rad*(c/cell)**exp) for c in range(cell)]
  v=Voronoi(points); m=[[[],[],list(v.vertices)] for i in [0,1]]
  for j in filter(lambda j:j+3>2<len(v.regions[j]),v.point_region):
    s=v.regions[j]; l=[m[1][2][a] for a in s if a>=0]; c=sum(l)/len(l)
    f=lambda:[a2(*(m[1][2][i]-c if i>=0 else c)[:2]) for i in s]
    k=np.argmin(f()); s=[s[(i+k)%len(s)] for i in range(len(s))]
    if all(x<=y for (x,y) in zip(f(),f()[1:])): s.reverse()
    b=all(i>=0 for i in s) and nm(c)<=.75; m[b]=make_cell(*m[b],s)
  make_object('p',m[0],((1,.72,0,1),(1,.45,0,1)),offset,25)
  make_object('s',m[1],((.7,.16,0,1),(.11,.45,0,1)),offset,7)
c,d=bpy.context.scene.collection,bpy.data.cameras.new('v')
d.lens=55; v=bpy.data.objects.new('v',d); c.children.link(col)
v.location,v.rotation_euler=(3.1,1.6,5.6),(.55,-.55,2.65)
c.objects.link(v); mkflower(0); mkflower(-3.1); mkflower(-6.2)
mkflower(-9.3); mkflower(-12.4); mkflower(-15.5);
```

Tables

Table 1: A table of minimal polynomials f_α together with a minimal polynomial g_β of degree 2 over $\mathbb{Q}(\alpha)$ such that $(\beta, \alpha - \beta)$ is a non-trivial decomposition of α.

$q(\alpha)$	f_α	g_β
2.2844	$x^3 - x^2 + 3x + 1$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 + 1)$
2.5198	$x^3 + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2$
2.6178	$x^3 + 2x^2 + 4x + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2$
2.7246	$x^3 + 2x + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2$
2.7850	$x^3 - 2x^2 + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2$
2.8582	$x^3 + 2x^2 - x + 2$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 + \alpha)$
2.8657	$x^3 - 2x^2 + 3x + 2$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 - \alpha)$
2.9073	$x^3 + 2x^2 - 2x + 1$	$x^2 - \alpha x - \alpha$
2.9379	$x^3 + 2x^2 + x + 4$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 + \alpha)$
2.9380	$x^3 - x^2 - x + 5$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 - 1)$
2.9516	$x^3 + x^2 + x + 5$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 + 1)$
3	$x^3 + x^2 - 4x + 1$	$x^2 - (\alpha + 1)\, x + 1$
3.1102	$x^3 + x^2 - 2x + 4$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 + \alpha)$
3.2714	$x^3 + 2x^2 + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2$
3.2849	$x^3 - 2x^2 + 2x + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2$
3.2981	$x^3 + 2x^2 - 2x + 2$	$x^2 - (\alpha - 1)\, x - (\alpha - 1)$
3.3321	$x^3 + 3x + 5$	$x^2 - \alpha x + \frac{1}{3}(\alpha^2 + \alpha + 1)$
3.3333	$x^3 - 2x^2 - 3x + 1$	$x^2 - (\alpha - 1)\, x + 1$
3.3378	$x^3 + x^2 - 4x + 3$	$x^2 - (\alpha - 1)\, x - (\alpha - 1)$
3.3853	$x^3 + 4x + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2 + 1$
3.4436	$x^3 - 2x^2 - x + 6$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 - \alpha)$
3.5716	$x^3 + 2x^2 + 6x + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2 + 1$
3.6432	$x^3 + 2x^2 + 6x + 2$	$x^2 - (\alpha + 1)\, x - 1$
3.6830	$x^3 + x^2 - 4x + 4$	$x^2 - \alpha x + \frac{1}{2}\alpha^2 + \frac{1}{2}\alpha - 1$
3.6839	$x^3 - x^2 - 3x + 7$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 - 1)$
3.7159	$x^3 + x^2 + 3x + 7$	$x^2 - \alpha x + \frac{1}{2}(\alpha^2 + 1)$
3.7362	$x^3 + 2x^2 - 3x + 2$	$x^2 - \alpha x - \alpha$
3.7962	$x^3 + 2x^2 + 6x + 1$	$x^2 - (\alpha - 1)\, x - \alpha - 1$
3.8854	$x^3 - 3x + 7$	$x^2 - \alpha x + \frac{1}{3}(\alpha^2 - \alpha + 1)$
3.9111	$x^3 - 2x^2 + 5x + 2$	$x^2 - (\alpha - 1)\, x - 1$
3.9938	$x^3 + x^2 - 5x + 4$	$x^2 - (\alpha + 1)\, x + 1$
4	$x^3 - 2x^2 - 4x + 1$	$x^2 - \alpha x + \alpha$

Table 2: A table of minimal polynomials f_α together with a minimal polynomial g_β of degree greater than 2 over $\mathbb{Q}(\alpha)$ such that $(\beta, \alpha - \beta)$ is a non-trivial decomposition of α.

$q(\alpha)$	f_α	g_β
2.9240	$x^3 + 5$	$x^4 - 2\alpha x^3 + 2\alpha^2 x^2 + 5x - \alpha$
3.0103	$x^3 - x^2 + 5$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (-3\alpha^2 - 2\alpha + 15)x^3 + (3\alpha^2 - 7\alpha - 6)x^2 + (\alpha^2 + \alpha + 5)x - \alpha + 1$
3.2595	$x^3 + 2x^2 - x + 3$	$x^4 - 2\alpha x^3 + (2\alpha^2 + \alpha - 1)x^2 + (\alpha^2 + 3)x - \alpha + 1$
3.2624	$x^3 - 2x^2 + 3x + 3$	$x^4 - 2\alpha x^3 + (2\alpha^2 - \alpha + 1)x^2 + (-\alpha^2 + 2\alpha + 3)x - \alpha$
3.3019	$x^3 + 6$	$x^6 - 3\alpha x^5 + 4\alpha^2 x^4 + 18x^3 - 8\alpha x^2 + 2\alpha^2 x + 1$
3.3378	$x^3 + x + 6$	$x^4 - 2\alpha x^3 + (\frac{3}{2}\alpha^2 - \frac{1}{2}\alpha)x^2 + (\frac{1}{2}\alpha^2 + \frac{1}{2}\alpha + 3)x + 1$
3.3656	$x^3 - 2x^2 + 4x + 2$	$x^4 - 2\alpha x^3 + (2\alpha^2 - \alpha + 2)x^2 + (-\alpha^2 + 2\alpha + 2)x - \alpha$
3.3709	$x^3 - x^2 + 2x + 5$	$x^6 - 3\alpha x^5 + 4\alpha^2 x^4 + (-3\alpha^2 + 6\alpha + 15)x^3 + (-\alpha^2 - 10\alpha - 5)x^2 + 3\alpha^2 x + 3$
3.3863	$x^3 + x^2 - 3x + 4$	$x^8 - 4\alpha x^7 + 7\alpha^2 x^6 + (7\alpha^2 - 21\alpha + 28)x^5 + (18\alpha^2 - 30\alpha + 17)x^4 + (19\alpha^2 - 30\alpha + 32)x^3 + (13\alpha^2 - 24\alpha + 19)x^2 + (6\alpha^2 - 9\alpha + 8)x + \alpha^2 - 2\alpha + 2$
3.3895	$x^3 - x^2 + 6$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (-3\alpha^2 - 2\alpha + 18)x^3 + (3\alpha^2 - 8\alpha - 7)x^2 + (\alpha^2 + \alpha + 6)x - \alpha + 1$
3.4190	$x^3 - 2x + 6$	$x^6 - 3\alpha x^5 + (4\alpha^2 - 1)x^4 + (-4\alpha + 18)x^3 + (\alpha^2 - 8\alpha)x^2 + 2\alpha^2 x + 1$
3.4338	$x^3 - x^2 + 4x + 3$	$x^8 - 4\alpha x^7 + (7\alpha^2 - 1)x^6 + (-7\alpha^2 + 31\alpha + 21)x^5 + (-17\alpha^2 - 30\alpha - 13)x^4 + (19\alpha^2 - 27\alpha - 24)x^3 + (4\alpha^2 + 26\alpha + 13)x^2 + (-5\alpha^2 + 3\alpha + 3)x - 2\alpha - 1$
3.4438	$x^3 + x^2 + 6$	$x^{10} - 5\alpha x^9 + 11\alpha^2 x^8 + (14\alpha^2 + 84)x^7 + (11\alpha^2 - 69\alpha + 68)x^6 + (44\alpha^2 - 36\alpha + 30)x^5 + (29\alpha^2 - 5\alpha + 99)x^4 + (5\alpha^2 - 24\alpha + 42)x^3 + (3\alpha^2 - 6\alpha)x^2 - 1$
3.4537	$x^3 + 2x + 6$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (4\alpha + 18)x^3 + (-\alpha^2 - 8\alpha)x^2 + 2\alpha^2 x + 1$

Table 2: Continued.

$q(\alpha)$	f_α	g_β
3.4767	x^3+x^2-2x+5	$x^{14}-7\alpha x^{13}+23\alpha^2x^{12}+(47\alpha^2-94\alpha+235)x^{11}+(200\alpha^2-467\alpha+333)x^{10}+(695\alpha^2-761\alpha+1040)x^9+(1143\alpha^2-1912\alpha+2739)x^8+(1840\alpha^2-3030\alpha+3435)x^7+(2256\alpha^2-3290\alpha+4258)x^6+(1960\alpha^2-3100\alpha+3990)x^5+(1343\alpha^2-2101\alpha+2601)x^4+(667\alpha^2-1022\alpha+1300)x^3+(226\alpha^2-354\alpha+447)x^2+(49\alpha^2-75\alpha+95)x+5\alpha^2-8\alpha+10$
3.4858	x^3+2x^2+2x+6	$x^6-3\alpha x^5+(4\alpha^2+1)x^4+(6\alpha^2+4\alpha+18)x^3+(4\alpha^2-3\alpha+16)x^2+(3\alpha^2-2\alpha+6)x+\alpha^2+2$
3.5833	x^3-2x^2+6	$x^8-4\alpha x^7+(7\alpha^2+\alpha)x^6+(-17\alpha^2+42)x^5+(25\alpha^2-26\alpha-75)x^4+(-14\alpha^2+36\alpha+72)x^3+(-\alpha^2-22\alpha-29)x^2+(4\alpha^2+5\alpha)x-\alpha^2+2$
3.6133	x^3+x^2-x+6	$x^6-3\alpha x^5+(4\alpha^2+\alpha)x^4+(\alpha^2-3\alpha+18)x^3+(\alpha^2-8\alpha-1)x^2+(2\alpha^2+\alpha)x+1$
3.6361	x^3+2x^2-x+4	$x^6-3\alpha x^5+(4\alpha^2-1)x^4+(6\alpha^2-\alpha+12)x^3+(5\alpha^2-8\alpha+11)x^2+(4\alpha^2-4\alpha+4)x+\alpha^2-\alpha+2$
3.6370	x^3-2x^2+3x+4	$x^6-3\alpha x^5+(4\alpha^2+1)x^4+(-6\alpha^2+7\alpha+12)x^3+(3\alpha^2-14\alpha-10)x^2+(2\alpha^2+5\alpha+4)x-\alpha^2+1$
3.6521	x^3+2x^2+5	$x^6-3\alpha x^5+4\alpha^2x^4+(6\alpha^2+15)x^3+(5\alpha^2-7\alpha+13)x^2+(4\alpha^2-3\alpha+5)x+\alpha^2+2$
3.6593	x^3+7	$x^3-2\alpha x^2+\alpha^2x+1$
3.6785	x^3-x^2-x+7	$x^{10}-5\alpha x^9+(11\alpha^2+1)x^8+(-14\alpha^2-18\alpha+98)x^7+(30\alpha^2-68\alpha-81)x^6+(16\alpha^2+27\alpha+140)x^5+(-13\alpha^2-70\alpha+18)x^4+(24\alpha^2+8\alpha-14)x^3+(-8\alpha^2-5\alpha+31)x^2+(2\alpha^2-2\alpha-7)x+1$
3.6878	x^3-x+7	$x^6-3\alpha x^5+4\alpha^2x^4+(-3\alpha+21)x^3+(\alpha^2-9\alpha)x^2+2\alpha^2x+1$
3.6915	x^3+x+7	$x^6-3\alpha x^5+4\alpha^2x^4+(3\alpha+21)x^3+(-\alpha^2-9\alpha)x^2+2\alpha^2x+1$
3.6939	x^3+x^2+x+7	$x^6-3\alpha x^5+(4\alpha^2+\alpha+1)x^4+(\alpha^2+\alpha+21)x^3+(-9\alpha-1)x^2+(2\alpha^2+\alpha)x+1$
3.7123	x^3-2x^2+4x+3	$x^6-3\alpha x^5+4\alpha^2x^4+(-6\alpha^2+12\alpha+9)x^3+(-15\alpha-7)x^2+(4\alpha^2+\alpha)x-\alpha^2+2\alpha+1$
3.7228	x^3+2x^2+x+6	$x^6-3\alpha x^5+4\alpha^2x^4+(6\alpha^2+3\alpha+18)x^3+(4\alpha^2-5\alpha+16)x^2+(3\alpha^2-3\alpha+6)x+\alpha^2+2$

3.7238	$x^3 - x^2 + 2x + 6$	$x^8 - 4\alpha x^7 + 7\alpha^2 x^6 + (-7\alpha^2 + 14\alpha + 42)x^5 + (-4\alpha^2 - 35\alpha - 26)x^4 + (15\alpha^2 + 8\alpha - 6)x^3 + (-6\alpha^2 + 6\alpha + 20)x^2 + (\alpha^2 - 4\alpha - 6)x + \alpha + 1$
3.7345	$x^3 + x^2 - 3x + 5$	$x^3 - 2\alpha x^2 + (\frac{3}{2}\alpha^2 - \frac{1}{2})x + \frac{1}{2}\alpha^2 - \alpha + \frac{3}{2}$
3.7479	$x^3 - x^2 + 7$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (-3\alpha^2 - 2\alpha + 21)x^3 + (3\alpha^2 - 9\alpha - 9)x^2 + (\alpha^2 + 2\alpha + 7)x - \alpha$
3.7664	$x^3 - 2x + 7$	$x^6 - 3\alpha x^5 + (4\alpha^2 - 1)x^4 + (-4\alpha + 21)x^3 + (\alpha^2 - 9\alpha)x^2 + 2\alpha^2 x + 1$
3.7771	$x^3 - 2x^2 + x + 6$	$x^6 - 3\alpha x^5 + 4\alpha^2 x^4 + (-6\alpha^2 + 3\alpha + 18)x^3 + (4\alpha^2 - 10\alpha - 15)x^2 + (4\alpha + 6)x - \alpha - 1$
3.7949	$x^3 + 2x + 7$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (4\alpha + 21)x^3 + (-\alpha^2 - 9\alpha)x^2 + 2\alpha^2 x + 1$
3.7995	$x^3 + x^2 + 7$	$x^6 - 3\alpha x^5 + (4\alpha^2 + \alpha)x^4 + (\alpha^2 + 21)x^3 + (-9\alpha - 1)x^2 + (2\alpha^2 + \alpha)x + 1$
3.8253	$x^3 + x^2 - 2x + 6$	$x^6 - 3\alpha x^5 + 4\alpha^2 x^4 + (3\alpha^2 - 6\alpha + 18)x^3 + (4\alpha^2 - 10\alpha + 9)x^2 + (3\alpha^2 - 5\alpha + 6)x + \alpha^2 - \alpha + 1$
3.8560	$x^3 + 2x^2 + 2x + 7$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (6\alpha^2 + 4\alpha + 21)x^3 + (4\alpha^2 - 4\alpha + 19)x^2 + (3\alpha^2 - 3\alpha + 7)x + \alpha^2 + 2$
3.8739	$x^3 - x^2 + x + 7$	$x^3 - 2\alpha x^2 + (\frac{3}{2}\alpha^2 + \frac{1}{2})x - \frac{1}{2}\alpha^2 + \frac{5}{2}$
3.9466	$x^3 - 2x^2 + 7$	$x^6 - 3\alpha x^5 + (4\alpha^2 - 1)x^4 + (-6\alpha^2 + 2\alpha + 21)x^3 + (4\alpha^2 - 10\alpha - 19)x^2 + (\alpha^2 + 5\alpha + 7)x - \alpha^2 - \alpha + 1$
3.9928	$x^3 + 2x^2 - x + 5$	$x^6 - 3\alpha x^5 + (4\alpha^2 - 1)x^4 + (6\alpha^2 - \alpha + 15)x^3 + (5\alpha^2 - 9\alpha + 13)x^2 + (4\alpha^2 - 4\alpha + 5)x + \alpha^2 - \alpha + 1$
3.9948	$x^3 - x^2 + 3x + 6$	$x^6 - 3\alpha x^5 + (4\alpha^2 + 1)x^4 + (-3\alpha^2 + 7\alpha + 18)x^3 + (-\alpha^2 - 12\alpha - 9)x^2 + (3\alpha^2 + 3\alpha)x - \alpha^2 + \alpha + 1$

Table 3: A table of minimal polynomials f_α together with a polynomial g over $\mathbb{Q}(\alpha)$ such that $g(x+\alpha/2)$ is exponentially bounded at radius $\sqrt{q(\alpha/2)}$, proving α is indecomposable.

$q(\alpha)$	f_α	g
2	x^3-2x^2-x+1	$\left(\alpha^2-2\alpha\right)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\alpha^2-\alpha-1)$
2.0347	x^3+x^2+3x+2	$x^2\cdot(x-\alpha)^2\cdot(x^2-\alpha x-1)$
2.0780	x^3-2x^2+x+2	$(x-1)\cdot(x-\alpha+1)\cdot x^2\cdot(x-\alpha)^2$
2.0801	x^3+3	$x^2\cdot(x-\alpha)^2\cdot(x^4-2\alpha x^3+2\alpha^2x^2-3x+\alpha)$
2.0826	x^3+2x^2+3x+3	$\left(\alpha^2+\alpha+1\right)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2)$
2.0872	x^3-x^2-x+3	$(\alpha+1)\cdot x\cdot(x-\alpha)\cdot(x^4-2\alpha x^3+\left(2\alpha^2-\alpha+1\right)x^2+(-2\alpha+3)\,x+\frac{1}{2}\alpha^2-\alpha+\frac{1}{2})$
2.0905	x^3-x^2-2x+3	$\alpha\cdot x\cdot(x-\alpha)\cdot(x^4-2\alpha x^3+\left(2\alpha^2-1\right)x^2+\left(-\alpha^2-\alpha+3\right)x+\frac{1}{3}\alpha^2-\frac{1}{3}\alpha-\frac{2}{3})$
2.0967	x^3+x^2+x+3	$\alpha\cdot x^2\cdot(x-\alpha)^2\cdot(x^4-2\alpha x^3+\left(\frac{5}{3}\alpha^2-\frac{1}{3}\alpha-\frac{1}{3}\right)x^2+\left(\alpha^2+\alpha+2\right)x+1)$
2.1102	x^3+x^2+2x+3	$x\cdot(x-\alpha)\cdot(x^4-2\alpha x^3+2\alpha^2x^2+\left(\alpha^2+2\alpha+3\right)x+1)$
2.1279	x^3-x+3	$x^2\cdot(x-\alpha)^2\cdot(x^4-2\alpha x^3+2\alpha^2x^2+(-\alpha+3)\,x-\alpha)$
2.1390	x^3+x+3	$2\cdot x\cdot(x-\alpha)\cdot(x^6-3\alpha x^5+\left(4\alpha^2+\frac{1}{2}\right)x^4+(2\alpha+9)\,x^3+\left(-\frac{1}{2}\alpha^2-4\alpha\right)x^2+\alpha^2x+\frac{1}{2})$
2.1626	x^3-x^2+3	$(\alpha-1)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2)$
2.1815	x^3-2x^2-x+3	$x\cdot(x-\alpha)\cdot(x^2-\alpha x+1)$
2.1904	x^3-x^2+2x+2	$(\alpha-1)\cdot x\cdot(x-\alpha)\cdot(x^4-2\alpha x^3+\frac{3}{2}\alpha^2x^2+\left(-\frac{1}{2}\alpha^2+\alpha+1\right)x-\frac{1}{4}\alpha^2-\frac{1}{2})$
2.1973	x^3+2x^2+2x+3	$(\alpha+1)\cdot x^2\cdot(x-\alpha)^2\cdot(x^4-2\alpha x^3+2\alpha^2x^2+\left(2\alpha^2+2\alpha+3\right)x+\frac{1}{2}\alpha^2+\frac{1}{2}\alpha+\frac{3}{2})$
2.2230	x^3+2x^2+4x+2	$\left(\alpha^2+\alpha+1\right)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2+\frac{1}{3})\cdot(x^2-\alpha x+\alpha^2+\alpha+2)$
2.2309	x^3+x^2+3	$(\alpha+1)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2)$
2.2512	x^3-2x+3	$\alpha\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2+\frac{1}{3})\cdot(x^4-2\alpha x^3+\left(\alpha^2-\alpha\right)x^2+\alpha^2x+1)$

2.3044	x^3+x^2-2x+2	$(\alpha+2)\cdot x^3\cdot(x-\alpha)^3\cdot(x^2-\alpha x+\frac{1}{2}\alpha^2+\frac{1}{2}\alpha)$
2.3681	x^3+2x^2+4x+1	$\left(\alpha^2+\alpha+4\right)\cdot x\cdot(x+1)\cdot(x-\alpha-1)\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{2}\alpha^2+\frac{1}{2}\alpha+\frac{1}{2})\cdot(x^4-2\alpha x^3+\left(\frac{7}{5}\alpha^2-\frac{2}{5}\alpha-\frac{1}{5}\right)x^2+\left(\frac{6}{5}\alpha^2+\frac{9}{5}\alpha+\frac{2}{5}\right)x+\frac{1}{5}\alpha^2+\frac{4}{5}\alpha+\frac{2}{5})$
2.4206	x^3+2x^2+2	$(\alpha+1)\cdot x^2\cdot(x-\alpha)^2\cdot(x^4-2\alpha x^3+\left(\frac{4}{3}\alpha^2-\frac{2}{3}\alpha-\frac{1}{3}\right)x^2+\left(\frac{4}{3}\alpha^2+\frac{1}{3}\alpha+\frac{2}{3}\right)x+\frac{2}{3}\alpha^2+\frac{2}{3}\alpha+\frac{1}{3})\cdot(x^4-2\alpha x^3+\left(2\alpha^2+\alpha\right)x^2+\left(\alpha^2+2\right)x-\alpha)$
2.4239	x^3+2x^2-x+1	$\left(\alpha^2+2\alpha-2\right)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2+\frac{1}{3}\alpha+\frac{1}{3})\cdot(x^4-2\alpha x^3+\left(2\alpha^2+\alpha-1\right)x^2+\left(\alpha^2+1\right)x-\alpha)$
2.4300	x^3-2x^2+2x+2	$(\alpha-1)\cdot x\cdot(x-\alpha)\cdot(x^2-\alpha x+\frac{1}{3}\alpha^2-\frac{1}{3}\alpha+\frac{1}{3})\cdot(x^8-4\alpha x^7+\left(7\alpha^2+\alpha\right)x^6+\left(-17\alpha^2+14\alpha+14\right)x^5+\left(17\alpha^2-35\alpha-24\right)x^4+\left(-2\alpha^2+30\alpha+20\right)x^3+\left(-7\alpha^2-11\alpha-3\right)x^2+\left(5\alpha^2-\alpha-2\right)x-\alpha^2+\alpha+1)$
2.4436	x^3-2x^2+3x+1	$x\cdot(x-\alpha)\cdot(x^4-2\alpha x^3+\left(2\alpha^2-\alpha+2\right)x^2+\left(-\alpha^2+\alpha+1\right)x-1)\cdot(x^6-3\alpha x^5+\left(4\alpha^2-\alpha\right)x^4+\left(-4\alpha^2+9\alpha+3\right)x^3+\left(-2\alpha^2-4\alpha-1\right)x^2+\left(2\alpha^2-3\alpha-1\right)x+\alpha)$
2.4517	x^3+x^2-x+3	$\left(\alpha^2+2\alpha-2\right)\cdot x^2\cdot(x-\alpha)^2\cdot(x^2-\alpha x+\frac{1}{2}\alpha^2-\frac{1}{2})\cdot(x^6-3\alpha x^5+\left(\frac{179}{46}\alpha^2+\frac{6}{23}\alpha+\frac{1}{46}\right)x^4+\left(\frac{52}{23}\alpha^2-\frac{65}{23}\alpha+\frac{192}{23}\right)x^3+\left(\frac{44}{23}\alpha^2-\frac{101}{23}\alpha+\frac{51}{23}\right)x^2+\left(\frac{67}{46}\alpha^2-\frac{16}{23}\alpha+\frac{51}{46}\right)x+\frac{4}{23}\alpha^2-\frac{5}{23}\alpha+\frac{13}{23})$
2.4960	x^3+2x^2+x+3	$\left(3\alpha^2+9\alpha+5\right)\cdot x^3\cdot(x-\alpha)^3\cdot(x^4-2\alpha x^3+\left(\alpha^2-1\right)x^2+\alpha x-\alpha^2-1)\cdot(x^4-2\alpha x^3+\left(2\alpha^2+\alpha\right)x^2+\left(\alpha^2+\alpha+3\right)x-\alpha)\cdot(x^4-2\alpha x^3+\left(\frac{10}{7}\alpha^2-\frac{2}{7}\alpha-\frac{1}{7}\right)x^2+\left(\frac{8}{7}\alpha^2+\frac{4}{7}\alpha+\frac{9}{7}\right)x+\frac{2}{7}\alpha^2+\frac{1}{7}\alpha+\frac{4}{7})^2$
2.5248	x^3-x^2-2x+4	$\left(\frac{1}{2}\alpha^2-\frac{1}{2}\alpha+1\right)\cdot x\cdot(x-\alpha)\cdot(x-\frac{1}{2}\alpha)^2\cdot(x^2+\left(-\alpha-1\right)x+\frac{1}{2}\alpha^2+\frac{1}{2}\alpha)\cdot(x^2-\alpha x+1)\cdot(x^2+\left(-\alpha+1\right)x+\frac{1}{2}\alpha^2-\frac{1}{2}\alpha)$
2.5324	x^3+x^2+2x+4	$(-\alpha+1)\cdot x\cdot(x-\alpha)\cdot(x-\frac{1}{2}\alpha)^2\cdot(x^2-\alpha x+\frac{1}{2}\alpha^2)\cdot(x^4-2\alpha x^3+\left(\frac{3}{2}\alpha^2-\frac{1}{2}\alpha\right)x^2+\left(\alpha^2+\alpha+2\right)x+1)$

Table 3: Continued.

$q(\alpha)$	f_α	g
2.5426	x^3+x^2+x+4	$\alpha\cdot x^3\cdot(x-\alpha)^3\cdot(x^4-2\alpha x^3+2\alpha^2x^2+\left(\alpha^2+\alpha+4\right)x-\alpha+1)\cdot(x^4-2\alpha x^3+\left(\frac{3}{2}\alpha^2-\frac{1}{2}\alpha-\frac{1}{2}\right)x^2+\left(\alpha^2+\alpha+2\right)x+1)^2$
2.5601	x^3-x+4	$\left(-\frac{1}{2}\alpha^2-\frac{3}{2}\alpha\right)\cdot x\cdot(x-\alpha)\cdot(x^4-2\alpha x^3+\left(\frac{3}{2}\alpha^2-\frac{1}{2}\alpha\right)x^2+\left(\frac{1}{2}\alpha^2-\frac{1}{2}\alpha+2\right)x-\frac{1}{2}\alpha+\frac{1}{2})\cdot(x^4-2\alpha x^3+\left(\frac{3}{2}\alpha^2+\frac{1}{2}\alpha\right)x^2+\left(-\frac{1}{2}\alpha^2-\frac{1}{2}\alpha+2\right)x-1)\cdot(x^4-2\alpha x^3+\left(\frac{8}{5}\alpha^2+\frac{1}{5}\alpha-\frac{1}{5}\right)x^2+\left(-\frac{1}{5}\alpha^2-\frac{2}{5}\alpha+\frac{12}{5}\right)x+\frac{1}{10}\alpha^2-\frac{3}{10}\alpha-\frac{1}{5})$
2.6335	x^3+x^2-3x+2	$\left(\alpha^2+2\alpha\right)\cdot x^2\cdot(x-\alpha)^2\cdot(x^2+\left(-\alpha-1\right)x+1)\cdot(x^2+\left(-\alpha+1\right)x-\alpha+1)\cdot(x^2-\alpha x+\frac{1}{2}\alpha^2+\frac{1}{2}\alpha-\frac{1}{2})^2\cdot(x^4-2\alpha x^3+\left(\frac{3}{2}\alpha^2-\frac{1}{2}\alpha-\frac{1}{2}\right)x^2+\left(\alpha^2-\alpha+1\right)x+\frac{1}{2}\alpha^2-\frac{1}{2}\alpha-\frac{1}{2})$
2.6377	x^3-2x^2-x+4	$\left(-\alpha^2+\alpha\right)\cdot x^2\cdot(x-\alpha)^2\cdot(x^2-\alpha x+1)^2\cdot(x^2-\alpha x+\frac{1}{2}\alpha^2-\frac{1}{2})^2\cdot(x^8-4\alpha x^7+\left(7\alpha^2-1\right)x^6+\left(-14\alpha^2-4\alpha+28\right)x^5+\left(18\alpha^2-9\alpha-35\right)x^4+\left(-8\alpha^2+8\alpha+24\right)x^3+\left(-\alpha^2-3\alpha-3\right)x^2+\left(2\alpha^2-4\right)x-\frac{1}{2}\alpha^2+\frac{1}{2}\alpha+1)$

Bibliography

[1] L. V. Ahlfors. *Complex Analysis*. McGraw-Hill, 3rd edition, 1979.

[2] M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Addison–Wesley, 1969.

[3] M. J. H. van den Bergh, S. T. Castelein, and D. M. H. van Gent. Order versus chaos. In *2020 IEEE Conference on Games (CoG)*, pages 391–398, 2020. https://doi.org/10.1109/CoG47356.2020.9231895.

[4] F. Borceux. Handbook of categorical algebra 2: Categories and structures. In *Encyclopedia of Mathematics and its Applications*, volume 50. Cambridge University Press, 1994. https://doi.org/10.1017/CBO9780511525865.

[5] I. Ciocănea-Teodorescu. *Algorithms for finite rings*. PhD thesis, Leiden University, 2016. https://hdl.handle.net/1887/40676.

[6] J. B. Conway. *A Course in Functional Analysis*. Springer, 2007. https://doi.org/10.1007/978-1-4757-4383-8.

[7] Z. Cvetkovski. *Inequalities: Theorems, Techniques and Selected Problems*. Springer, 2012. https://doi.org/10.1007/978-3-642-23792-8_11.

[8] E. C. Dade, O. Taussky, and H. Zassenhaus. On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field. *Math. Annalen*, 148:31–64, 1962. https://doi.org/10.1007/BF01438389.

[9] M. DeVos. *Flows on Graphs*. PhD thesis, Princeton Univ., 2000.

[10] R. Diestel. *Graph Theory*. Springer, 5th edition, 2017. https://doi.org/10.1007/978-3-662-53622-3.

[11] M. Eichler. Note zur Theorie der Kristallgitter. *Mathematische Annalen*, 125:51–55, 1952. https://doi.org/10.1007/BF01343106.

[12] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Ge-*

ometry, volume 150 of *Lecture Notes in Mathematics*. Springer, 1995. https://doi.org/10.1007/978-1-4612-5350-1.

[13] I. Fáry. On straight line representation of planar graphs. *Acta Univ. Szeged. Sect. Sci. Math.*, 11:229–233, 1948.

[14] H. Fitting. Die determinantenideale eines moduls. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 46:195–228, 1936.

[15] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022. https://www.gap-system.org.

[16] R. J. Gardner. The Brunn–Minkowski inequality. *Bull. Amer. Math. Soc.*, 39:355–405, 2002. https://doi.org/10.1090/S0273-0979-02-00941-2.

[17] D. M. H. van Gent. Algorithms for finding the gradings of reduced rings. Master's thesis, Leiden University, 2019. https://arxiv.org/abs/1911.02957.

[18] D. M. H. van Gent. Indecomposable algebraic integers, 2021. https://arxiv.org/abs/2111.00499.

[19] D. M. H. van Gent. IndecomposableAlgebraicIntegers. https://github.com/MadPidgeon/IndecomposableAlgebraicIntegers, 2023.

[20] D. M. H. van Gent. Nonabelian flows in networks. *Journal of Graph Theory*, 104(1):245–256, 2023. https://doi.org/10.1002/jgt.22958.

[21] D. M. H. van Gent. NonabelianFlowsInGraphs. https://github.com/MadPidgeon/NonabelianFlowsInGraphs, 2023.

[22] A. Goodall, T. Krajewski, G. Regts, and L. Vena. A Tutte polynomial for maps. *Combinatorics, Probability and Computing*, 27(6):913–945, 2018. https://doi.org/10.1017/S0963548318000081.

[23] G. Hanrot, X. Pujol, and D. Stehlé. Algorithms for the shortest and closest lattice vector problems. In *Coding and Cryptology*, pages 159–190. Springer, 2011. https://doi.org/10.1007/978-3-642-20901-7_10.

[24] J. Hopcroft and R. Tarjan. Efficient planarity testing. *J. ACM*, 21(4):549–568, Oct. 1974. https://doi.org/10.1145/321850.321852.

[25] J. Hubbard, D. Schleicher, and S. Sutherland. How to find all roots of complex polynomials by Newton's method. *Inventiones mathematicae*, 146:1–33, 2001. https://doi.org/10.1007/s002220100149.

[26] P. Jordan and J. von Neumann. On inner products in linear, metric spaces. *Annals of Mathematics*, 36(3):719–723, 1935. https://doi.org/10.2307/1968653.

[27] I. Kaplansky. *Infinite Abelian Groups*. University of Michigan Press, 1954.

[28] M.-A. Knus and M. Ojanguren. *Théorie de la Descente et Algèbres d'Azumaya*, volume 389 of *Lecture Notes in Mathematics*. 1974. https:

//doi.org/10.1007/BFb0057799.

[29] E. Kreyszig. *Introductory Functional Analysis With Applications*. John Wiley & Sons, 1989.

[30] S. Lang. Algebra. In *Graduate Texts in Mathematics*, volume 211. Springer, 3rd edition, 2005. https://doi.org/10.1007/978-1-4613-0041-0.

[31] A. K. Lenstra. Factoring polynomials over algebraic number fields. *Lecture Notes in Computer Science*, 162, 1983. https://doi.org/10.1007/3-540-12868-9_108.

[32] H. W. Lenstra Jr. and A. Silverberg. Roots of unity in orders. *Foundations of Computational Mathematics*, 17(3):851–877, Jun 2017. https://doi.org/10.1007/s10208-016-9304-1.

[33] H. W. Lenstra Jr. and A. Silverberg. Algorithms for commutative algebras over the rational numbers. *Foundations of Computational Mathematics*, 18(1):159–180, 2018. http://doi.org/10.1007/s10208-016-9336-6.

[34] H. W. Lenstra Jr. and A. Silverberg. Universal gradings of orders. *Archiv der Mathematik*, 111(6):579–597, Dec 2018. https://doi.org/10.1007/s00013-018-1228-3.

[35] H. W. Lenstra Jr., A. Silverberg, and D. M. H. van Gent. Realizing orders as group rings. *Journal of Algebra*, 2023. https://doi.org/10.1016/j.jalgebra.2023.11.017.

[36] B. Litjens. On dihedral flows in embedded graphs. *Journal of graph theory*, 91(2):174–191, 2019. https://doi.org/10.1002/jgt.22427.

[37] S. Mac Lane. *Categories for the working mathematician*. Springer, 1978. https://doi.org/10.1007/978-1-4757-4721-8.

[38] J. S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.

[39] J. Milnor and D. Husemoller. *Symmetric Bilinear Forms*. Springer, 1973. https://doi.org/10.1007/978-3-642-88330-9.

[40] R. S. Rumely. *Capacity Theory on Algebraic Curves*. Springer, 1989. https://doi.org/10.1007/BFb0084525.

[41] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. https://www.sagemath.org.

Index

Acknowledgments

First and foremost I would like to thank my advisor and copromotor Hendrik Lenstra, for his many interesting problems and the time we spent trying to solve them. In the 6 years I have worked with you, you were always available and happy to answer my questions. It was a delight and an honor to be your student.

For their help, one way or another, in bringing this thesis to fruition, I would like to thank my promotor, Ronald van Luijk; the members of my doctorate committee, Gianne Derks, David Holmes, Peter Stevenhagen, Alex Bartel, and Ted Chinburg; my coauthors, Mark van den Bergh, Sipke Castelein, Hendrik Lenstra, and Alice Silverberg; and my office mates, Onno Berrevoets, George Politopoulos, Pim Spelier, and Jesse Vogel.

I would like to thank Dion Gijswijt for providing references to literature for Chapter 1, Onno Berrevoets and Borys Kadets for their help in proving Proposition 2.3.18, Ted Chinburg for his proof of Corollary 3.6.7, and Wessel van Woerden for his support in implementing the lattice algorithms from Chapter 3.

Finally, I would like to thank my friends and family, for their support and confidence. It really meant a lot to me.

Curriculum Vitae

Daniël Martinus Herman van Gent is geboren op 10 september 1995 te Leiden en opgegroeid in Voorhout. Hij behaalde in 2013 zijn vwo-diploma aan het Northgo College in Noordwijk.

In 2016 behaalde hij cum laude zijn bachelorgraden in Wiskunde en Informatica aan de Universiteit Leiden. Hij schreef zijn bachelorscriptie, getiteld *"Graph-isomorphism in quasi-polynomial time"*, onder begeleiding van Owen Biesel en Hendrik Jan Hoogeboom. In 2019 verdedigde hij zijn masterscriptie, getiteld *"Algorithms for finding the gradings of reduced rings"*, aan de Universiteit Leiden onder begeleiding van Hendrik Willem Lenstra. Hij behaalde hierbij cum laude zijn mastergraad Wiskunde.

Tijdens zijn bachelor- en masterstudie is hij werkzaam geweest als studentassistent bij de Universiteit Leiden. Ook vormde hij met Onno Bernardus Berrevoets en Wessel Pieter Jacobus van Woerden een team voor verscheidene internationale programmeerwedstrijden. Zij wonnen in 2017 de *"Catalyst Coding Contest"*. In 2019 behaalde hij in een team met Berrevoets en Pim Spelier de finale van de *"International Collegiate Programming Contest"*.

In 2019 begon hij zijn promotietraject aan de Universiteit Leiden onder begeleiding van Lenstra. Sindsdien vormt hij met Berrevoets de redactie van de probleemrubriek van het vakblad *"Nieuw Archief voor Wiskunde"*.