Decompositions in algebra

Gent, D.M.H. van

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 $\text{indec}(R)$ with an edge between $x, y \in \text{indec}(R)$ 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 $\text{supp}(u) = \{i \in I \mid u_i \neq 0\}$. Now consider the free abelian group $\mathbb{Z}^{(I)}$ and let Γ be the group obtained from it by dividing out

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

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 $R = \mathbb{Z}[p^x \,|\, p \in \mathcal{P},\, x \in \mathbb{Q}_{\geq 0}] \subseteq \overline{\mathbb{Z}}$ 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 $\alpha \in \operatorname{indec}(\overline{\mathbb{Z}})$ 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 $x^\perp = \{y \in K \,|\, \langle x, y\rangle = 0\}$, 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 Υ. By universality we get a morphism of gradings and thus a morphism of groups $\Upsilon \to \Delta$. 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 $\{\gamma \in \Gamma \mid x_\gamma \neq 0\}$. 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

$$\begin{aligned} 0 &\equiv (p+1)\sum_{i=0}^{p-1} iX_ie_{-i} = (p+1)\sum_{i=0}^{p-1} iX_i \sum_{\substack{\mathrm{wt}(\vec{m})=p \\ \deg(\vec{m})=-i}} \binom{p}{\vec{m}} X^{\vec{m}} \\ &= \sum_{\substack{\mathrm{wt}(\vec{n})=p+1 \\ \deg(\vec{n})=0}} \binom{p+1}{\vec{n}} \Big(\sum_{i=0}^{p-1} n_i i\Big) X^{\vec{n}} \pmod{J}, \end{aligned}$$

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 $p^2 I \subseteq J$. The remaining p terms equal

$$0 \equiv \binom{p+1}{p+1} 0 X_0^{p+1} + \binom{p+1}{p} \sum_{i=1}^{p-1} piX_0X_i^p \equiv pX_0 \sum_{i=0}^{p-1} iX_i^p \pmod{J}.$$

We now apply the affine transformations $a \mapsto a$ and $a \mapsto 1-a$ to this equality, so that

$$\begin{aligned} 0 &\equiv X_1\Big(pX_0\sum_{i=0}^{p-1} iX_i^p\Big) + X_0\Big(pX_1\sum_{i=0}^{p-1}(1-i)X_i^p\Big) \\ &= pX_0X_1\sum_{i=0}^{p-1} X_i^p \equiv pX_0X_1e_0 \pmod{J} \end{aligned}$$

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 $\mathrm{nil}(R)$ 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.*

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 $x \in \mathrm{nil}(R)$, 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 $p^k \equiv 1 \pmod{n}$. 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*

$$\sqrt[p]{B} := \{x \in C \mid (\exists\, n \in \mathbb{Z}_{\geq 0})\ x^{p^n} \in B\}$$

generates C as a B-module and contains $C^G = \{c \in C \mid (\forall g \in G)\ gc = c\}$. 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 $M = \{\prod_{s \in S} s \mid S \subseteq O\}$ 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 $G = \operatorname{Hom}(\Gamma, \langle\zeta\rangle)$, 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. □