UNIVERSAL GRADINGS OF ORDERS

H. W. LENSTRA, JR. AND A. SILVERBERG

ABSTRACT. For commutative rings, we introduce the notion of a *universal grading*, which can be viewed as the "largest possible grading". While not every commutative ring (or order) has a universal grading, we prove that every *reduced order* has a universal grading, and this grading is by a *finite* group. Examples of graded orders are provided by group rings of finite abelian groups over rings of integers in number fields. We also generalize known properties of nilpotents, idempotents, and roots of unity in such group rings to the case of graded orders; this has applications to cryptography. Lattices play an important role in this paper; a novel aspect is that our proofs use that the additive group of any reduced order can in a natural way be equipped with a lattice structure.

1. INTRODUCTION

In 1940, G. Higman [2, Theorem 3] proved the beautiful result that if Γ is a finite abelian group, then the torsion subgroup of the group of units of the group ring $\mathbb{Z}[\Gamma]$ equals $\pm\Gamma$. His proof was remarkable in that it depended on properties of the absolute value of complex numbers.

In recent work [5] on cryptography, the present authors needed to use a similar result on rings that are a bit more general than Higman's group rings, namely *graded orders*. Here an **order** is a commutative ring A of which the additive group A^+ is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$, and *graded* refers to the familiar notion recalled below; our gradings will always be by abelian groups. If the order A is **reduced** in the sense that its nilradical is 0, then the group A^+ carries a natural *lattice structure*. Replacing Higman's technique by this lattice structure, we were able to prove basic properties of nilpotents, idempotents, and torsion units in any graded order, as expressed in Theorem 1.5 below.

Much to our surprise, we discovered that the same lattice structure can be used to prove a far more fundamental result on graded orders. Namely, as our main theorem (Theorem 1.3) asserts, each reduced order A has a *universal grading*, which controls *all* gradings of A and can be thought of as its "finest possible" grading. The precise definition is given in Definition 1.2 below. This definition does not appear to occur in the literature, presumably because prior to our discovery no interesting class of examples was known; and indeed, many naturally occurring rings fail to have universal gradings.

Our main result suggests a number of promising avenues for further research. The first is to exhibit a larger class of commutative rings that have universal gradings. For Higman's original result, several far-reaching generalizations have been found, notably in the work of W. May [7]. Replacing our "archimedean" arguments by arguments with a p-adic flavor, one can probably identify algebraic conditions that ensure the existence of a universal grading.

Secondly, we hope to show in forthcoming work [6] that the existence of a universal grading on any reduced order has important consequences for the problem of how one may write a given commutative ring as a group ring, a problem that is closely related to the well-studied subject of isomorphisms between group rings. Roughly speaking, we prove that, up to isomorphism, there is a

unique "maximal" way of realizing a given reduced order as a group ring. Such results are probably also achievable over more general base rings than the ring of integers.

Third, there is the algorithmic question of designing an "efficient" method for computing the universal grading of a given reduced order, see [1].

Fourth, our main result may be rephrased by saying that there is, in a suitable sense, a "maximal" abelian group scheme "of multiplicative type" that acts on a given reduced order (see [9]). One may wonder whether a similar result holds for more general finite abelian group schemes.

In this paper all rings are supposed to be commutative.

Definition 1.1. Suppose Γ is a multiplicatively written abelian group with identity element 1. Then a Γ-**grading** of a ring A is a system $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ of additive subgroups $B_\gamma \subset A$ that satisfies:

  (i) $B_\gamma \cdot B_{\gamma'} \subset B_{\gamma\gamma'}$ for all $\gamma, \gamma' \in \Gamma$, and
  (ii) $A = \bigoplus_{\gamma \in \Gamma} B_\gamma$ in the sense that the additive group homomorphism $\bigoplus_{\gamma \in \Gamma} B_\gamma \to A$ sending $(x_\gamma)_{\gamma \in \Gamma}$ to $\sum_{\gamma \in \Gamma} x_\gamma$ is bijective.

We note that if R is a ring and Γ is an abelian group, then there is a natural Γ-grading of the group ring $R[\Gamma]$, given by $(R \cdot \gamma)_{\gamma \in \Gamma}$.

If $f : \Gamma \to \Delta$ is a homomorphism of abelian groups, then each Γ-grading $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ of a ring A gives rise to the Δ-grading $(\sum_{\gamma \in f^{-1}(\delta)} B_\gamma)_{\delta \in \Delta}$ of A, which we denote by $f_* \mathbf{B}$.

Definition 1.2. By a **universal grading** of a ring A we mean a pair $(\Gamma, \mathbf{B})$ consisting of an abelian group Γ and a Γ-grading $\mathbf{B}$ of A with the property that for each abelian group Δ and each Δ-grading $\mathbf{C}$ of A there is a unique group homomorphism $f : \Gamma \to \Delta$ such that $\mathbf{C} = f_* \mathbf{B}$.

If a universal grading of A exists, then by a standard argument it is, in an obvious sense, unique up to a unique isomorphism; and it exists if and only if the functor that assigns to an abelian group Δ the set of Δ-gradings of A is representable.

Many naturally occurring rings fail to have a universal grading; see Examples 7.3(i,ii,iii) for number fields and finite fields that have no universal grading. This makes the following result all the more unexpected.

Theorem 1.3. *Every reduced order has a universal grading, and its universal grading is by a finite abelian group.*

We prove Theorem 1.3 in section 9 (using lemmas given earlier in the paper).

It could be of interest to study non-reduced orders as well. In Examples 7.3(vi–viii) we show that they may have a universal grading by an infinite group, or by a finite group, or no universal grading at all. In particular, one cannot omit "reduced" from Theorem 1.3.

In section 10 we prove the following result, which answers a question posed by Kiran Kedlaya.

Theorem 1.4. *Let A be an order that is a Dedekind domain. Then the universal grading of A is by a finite cyclic group.*

Suppose A is a ring. The set of nilpotent elements of A is an ideal of A, denoted $\sqrt{0}$ or $\sqrt{0_A}$ and called the **nilradical**. We call $x \in A$ an **idempotent** if $x^2 = x$. We denote the set of idempotents by $\mathrm{Id}(A)$, and we call A **connected** if $\#\mathrm{Id}(A) = 2$ or, equivalently, if one has $\mathrm{Id}(A) = \{0, 1\}$ and $A \neq 0$. We call $x \in A$ a **root of unity** if $x^n = 1$ for some $n \in \mathbb{Z}_{>0}$. The set of roots of unity of A, which is a subgroup of the group A^* of units of A, is denoted by $\mu(A)$.

Let A be a ring and let $(B_\gamma)_{\gamma \in \Gamma}$ be a Γ-grading of A. Then the subgroup B_1 of A is a subring of A that contains the identity element of A (see Lemma 2.1). We shall call an additive subgroup $H \subset A$ **homogeneous** if for each $(x_\gamma)_{\gamma \in \Gamma} \in \bigoplus_{\gamma \in \Gamma} B_\gamma$ one has that $\sum_{\gamma \in \Gamma} x_\gamma$ is in H if and only if each x_γ is in H (i.e., $H = \bigoplus_{\gamma \in \Gamma} (H \cap B_\gamma)$ via the bijection in (ii) above). This terminology will in particular be applied to ideals and to subrings of A. An element of A is called **homogeneous** if it belongs to $\bigcup_{\gamma \in \Gamma} B_\gamma$.

Theorem 1.5. *Let Γ be an abelian group, and let A be an order with Γ-grading $(B_\gamma)_{\gamma\in\Gamma}$. Then:*

   (i) *the nilradical $\sqrt{0_A}$ is a homogeneous ideal of A;*

   (ii) $\mathrm{Id}(A) = \mathrm{Id}(B_1)$, *and A is connected if and only if B_1 is connected;*

   (iii) *if B_1 is connected, then each element of $\mu(A)$ is homogeneous.*

The three parts of Theorem 1.5 are proved in Propositions 4.1(iii), 5.9, and 6.3, respectively. Note that Theorem 1.5(iii) is clearly false if the connectedness assumption is dropped.

In the case that A is a group ring $B[\Gamma]$ with its natural Γ-grading, with B an order and Γ a finite abelian group, Theorem 1.5 was known and can be deduced from results in [7] (Proposition 2 of [7] for (i), the Corollary to Proposition 3 for (ii), and the Corollary to Proposition 10 for (iii)).

We end the introduction with two important classes of examples of graded rings.

Example 1.6 (*Kummer extensions*). Let $K \subset L$ be a field extension, and let W be the set of $a \in L^*$ for which there exists $n \in \mathbb{Z}_{>0}$ such that $a^n \in K^*$ and K contains a primitive n-th root of unity. Then W is a subgroup of L^* containing K^*, and the subfield $K(W)$ of L is graded by the group W/K^*; here the piece of degree $aK^* \in W/K^*$ is the one-dimensional K-vector space Ka. This example illustrates that finding a grading for a field extension is closely related to the classical problem of generating the field by means of radicals.

Example 1.7 (*Extended tensor algebras*). Suppose A is a commutative ring and L is a projective A-module of rank 1. For $i \in \mathbb{Z}$, let $L^{\otimes i}$ denote the i-th tensor power of L, where for negative values of i we define $L^{\otimes i} = \mathrm{Hom}_A(L^{\otimes -i}, A)$. Then the extended tensor algebra $\Lambda = \bigoplus_{i\in\mathbb{Z}} L^{\otimes i}$ is graded by an infinite cyclic group. If $r \in \mathbb{Z}_{>0}$ and $L^{\otimes r}$ is free, say $L^{\otimes r} = Ay$, then the ring $B = \Lambda/(y-1)\Lambda$ is graded by a cyclic group of order r, since $B = \bigoplus_{i=0}^{r-1} L^{\otimes i}$. This class of examples includes the graded orders that we encountered in lattice-based cryptography, and that play crucial roles in the proofs of the main results in [3, 5]. More precisely, Theorem 1.5(ii,iii) supplies the proof of Proposition 14.3(iv) of [5].

2. Graded rings

In this section we give some relatively straightforward lemmas that we will use to prove our main results. The proofs of Theorems 1.3 and 1.5 depend on two techniques. One, mentioned earlier, depends on the introduction of a natural lattice structure on any reduced order. The other (Lemma 2.5 below) consists of equipping a Γ-graded ring with an action by the dual of Γ, after a suitable cyclotomic base change; here Γ is finite.

Lemma 2.1. *Suppose A is a ring, Γ is an abelian group, and $(B_\gamma)_{\gamma\in\Gamma}$ is a Γ-grading of A. Then:*

   (i) $1 \in B_1$,

   (ii) B_1 *is a ring, and*

   (iii) *each B_γ is a B_1-module.*

Proof. Write $1 = (1_\gamma)_{\gamma\in\Gamma} \in A$. Take any $\delta \in \Gamma$ and $\alpha \in B_\delta$. Then $\alpha = 1 \cdot \alpha = (1_\gamma)_{\gamma\in\Gamma} \cdot (\alpha_\gamma)_{\gamma\in\Gamma}$ where $\alpha_\delta = \alpha$ and $\alpha_\gamma = 0$ for all $\gamma \neq \delta$. Comparing δ-coordinates we have $\alpha = 1_1 \cdot \alpha$, and likewise $\alpha = \alpha \cdot 1_1$. So 1_1 acts left and right as the identity on each B_δ, and hence on A. Thus, $1 = 1_1 \in B_1$, proving (i). Parts (ii) and (iii) are straightforward. $\square$

If Γ is an abelian group and $k \in \mathbb{Z}$, let $\Gamma^k = \{\gamma^k : \gamma \in \Gamma\}$. The following two lemmas will be used to prove Proposition 4.3 and Proposition 3.9, respectively.

Lemma 2.2. *Suppose Γ is an abelian group, $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of a commutative ring A, and the set $S = \{\gamma \in \Gamma : B_\gamma \neq 0\}$ is finite. Then there are a finite abelian group Δ and a Δ-grading $\mathbf{C} = (C_\delta)_{\delta \in \Delta}$ of A such that $\bigcup_{\gamma \in \Gamma} B_\gamma = \bigcup_{\delta \in \Delta} C_\delta$.*

Proof. We can and do replace Γ with $\langle S \rangle$. Since $\{1\} = \bigcap_{N \in \mathbb{Z}_{>0}} \Gamma^N$, if $s, t \in S$ with $s \neq t$ then there exists $N_{s,t} \in \mathbb{Z}_{>0}$ such that $st^{-1} \notin \Gamma^{N_{s,t}}$. Let $M = \mathrm{lcm}_{s,t \in S, s \neq t}\{N_{s,t}\}$, let $c : \Gamma \to \Gamma/\Gamma^M$ be the canonical projection map, and let $\mathbf{C} = c_*\mathbf{B} = (C_\delta)_{\delta \in \Gamma/\Gamma^M}$. By construction, the restriction of c to S is injective, and the desired result now follows with $\Delta = \Gamma/\Gamma^M$. $\qquad \square$

Lemma 2.3. *Suppose A is a commutative ring, Γ is an abelian group, $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, and $(\Gamma, \mathbf{B})$ is universal. Then $\Gamma = \langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle$.*

Proof. Put $\Delta = \Gamma/\langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle$, and let $t, c : \Gamma \to \Delta$ be the trivial and the canonical map, respectively. Then t and c agree on each γ with $B_\gamma \neq 0$, so $t_*\mathbf{B} = c_*\mathbf{B}$, and by universality one gets $t = c$ so $\Delta = \{1\}$. $\qquad \square$

We will use the next lemma to prove Lemma 3.8 and Proposition 4.3.

Lemma 2.4. *Suppose Γ is an abelian group, A is either a commutative $\mathbb{Q}$-algebra with $\dim_\mathbb{Q} A < \infty$ or an order, and $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A. Then $B_\gamma = 0$ for all but finitely many $\gamma \in \Gamma$.*

Proof. This holds since $A = \bigoplus_{\gamma \in \Gamma} B_\gamma$, and A has finite $\mathbb{Z}$-rank (if A is an order) or finite $\mathbb{Q}$-dimension (if A is a finite dimensional commutative $\mathbb{Q}$-algebra). $\qquad \square$

Suppose $k \in \mathbb{Z}_{>0}$. With Φ_k denoting the k-th cyclotomic polynomial and $\zeta_k = X + (\Phi_k)$, we have $\mathbb{Z}[\zeta_k] = \mathbb{Z}[X]/(\Phi_k) = \bigoplus_{i=0}^{\varphi(k)-1} \mathbb{Z} \cdot \zeta_k^i$, where φ is the Euler φ-function. Suppose A is a ring, Γ is an abelian group, and $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A. Then $B_\gamma[\zeta_k] = B_\gamma \otimes_\mathbb{Z} \mathbb{Z}[\zeta_k]$ is a module over $B_1[\zeta_k]$ for all $\gamma \in \Gamma$, and $A[\zeta_k] = A \otimes_\mathbb{Z} \mathbb{Z}[\zeta_k] = \bigoplus_{\gamma \in \Gamma}(B_\gamma[\zeta_k])$ is a Γ-graded ring that contains A. If Γ is finite of exponent dividing k, we let

$$\hat{\Gamma}_k = \mathrm{Hom}(\Gamma, \langle \zeta_k \rangle),$$

a multiplicative group with $\#\hat{\Gamma}_k = \#\Gamma$. We use the next lemma to prove Propositions 4.1 and 5.8.

Lemma 2.5. *Suppose A is a ring, Γ is a finite abelian group, $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, and k is a positive integer divisible by the exponent of Γ. For $\chi \in \hat{\Gamma}_k$, and $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in A[\zeta_k]$ with $\alpha_\gamma \in B_\gamma[\zeta_k]$, define*

$$\chi * \alpha = (\chi(\gamma) \cdot \alpha_\gamma)_{\gamma \in \Gamma} \in A[\zeta_k].$$

This defines an action of $\hat{\Gamma}_k$ on $A[\zeta_k]$ by ring automorphisms, and for all $\delta \in \Gamma$ and $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in A[\zeta_k]$ one has

$$\sum_{\chi \in \hat{\Gamma}_k} \chi * (\chi(\delta)^{-1}\alpha) = \#\Gamma \cdot \alpha_\delta \in B_\delta[\zeta_k] \subset A[\zeta_k].$$

Proof. The proof is an easy exercise. The last statement follows from the fact that if $\delta \in \Gamma$ then $\sum_{\chi \in \hat{\Gamma}_k} \chi(\delta)$ is $\#\Gamma$ if $\delta = 1$, and otherwise is 0. $\qquad \square$

3. Euclidean vector spaces, lattices, and orders

In a series of examples, we introduce the lattice structure on reduced orders that we will use in the proofs of our main results. We conclude the section with a result on gradings of reduced orders that we will use to prove Proposition 5.8 and Theorem 1.3.

If C is a $\mathbb{Z}$-module or $\mathbb{Z}$-algebra, we will write $C_\mathbb{Q}$ for $C \otimes_\mathbb{Z} \mathbb{Q}$.

A **Euclidean vector space** is a finite dimensional $\mathbb{R}$-vector space E equipped with a map $\langle \ , \ \rangle : E \times E \to \mathbb{R}$, $(x, y) \mapsto \langle x, y \rangle$ that is $\mathbb{R}$-bilinear, symmetric, and positive definite.

Example 3.1. Suppose E is a finite dimensional $\mathbb{R}$-vector space equipped with a map $\langle \, , \, \rangle :$ $E \times E \to \mathbb{R}$ that is $\mathbb{R}$-bilinear, symmetric, and positive semidefinite. Let

$$\mathrm{rad}(E) = \{x \in E : \langle x, E \rangle = 0\}.$$

Then $\mathrm{rad}(E) = \{x \in E : \langle x, x \rangle = 0\}$, and $\langle \, , \, \rangle$ makes $E/\mathrm{rad}(E)$ into a Euclidean vector space.

Example 3.2. Suppose E is a commutative $\mathbb{R}$-algebra with $\dim_{\mathbb{R}}(E) < \infty$. For all $x, y \in E$, let $\langle x, y \rangle = \sum_{\sigma:E \to \mathbb{C}} \sigma(x)\overline{\sigma(y)}$, where σ ranges over all $\mathbb{R}$-algebra homomorphisms from E to $\mathbb{C}$. Then $\mathrm{rad}(E) = \sqrt{0_E}$. (If $x \in \sqrt{0_E}$ then $\sigma(x) = 0$ for all σ, so $\langle x, y \rangle = 0$ for all y, so $x \in \mathrm{rad}(E)$. Conversely, $E/\sqrt{0_E}$ is a product of fields, and these fields are $\mathbb{R}$ and $\mathbb{C}$. Since the inner products on $\mathbb{R}$ and $\mathbb{C}$ are positive definite, so is the inner product on E. Thus $\mathrm{rad}(E/\sqrt{0_E}) = 0$, so $\mathrm{rad}(E) \subset \sqrt{0_E}$. Note that, as a consequence, the number of σ's equals $\dim_{\mathbb{R}}(E)$.)

Recall that a **lattice** is a finitely generated free abelian group L equipped with a positive definite symmetric $\mathbb{R}$-bilinear function $\langle \, , \, \rangle : L_{\mathbb{R}} \times L_{\mathbb{R}} \to \mathbb{R}$, where $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$.

If B and C are rings, we write $\mathrm{Rhom}(B, C)$ for the set of ring homomorphisms from B to C.

Example 3.3. Suppose A is an order. Then $E = A_{\mathbb{R}}$ is a finite dimensional $\mathbb{R}$-vector space equipped with an $\mathbb{R}$-bilinear, symmetric, positive semidefinite inner product $\langle \, , \, \rangle : E \times E \to \mathbb{R}$ as in Example 3.2. Further, $\mathrm{rad}(E) = \sqrt{0_E} = (\sqrt{0_A})_{\mathbb{R}}$, and thus $A/\sqrt{0_A}$ has a natural lattice structure. (That $(\sqrt{0_A})_{\mathbb{R}} \subset \sqrt{0_E}$ is clear. For the reverse inclusion, $A/\sqrt{0_A}$ is a reduced order, so $(A/\sqrt{0_A})_{\mathbb{Q}}$ is a product of finitely many number fields, so is a product of finitely many separable extensions of $\mathbb{Q}$. It follows that $(A/\sqrt{0_A})_{\mathbb{R}} = E/(\sqrt{0_A})_{\mathbb{R}}$ is a product of finitely many separable extensions of $\mathbb{R}$, so is reduced. It also follows that $\#\mathrm{Rhom}(A, \mathbb{C})$ equals $\mathrm{rank}(A/\sqrt{0_A})$, the rank of $A/\sqrt{0_A}$ as an abelian group.)

Example 3.4. Suppose A is a reduced order. Then $A/\sqrt{0_A} = A$, so by the previous example A has a natural lattice structure. It is given by

$$\langle x, y \rangle = \sum_{\sigma \in \mathrm{Rhom}(A, \mathbb{C})} \sigma(x)\overline{\sigma(y)}$$

for $x, y \in A$. Note that $\#\mathrm{Rhom}(A, \mathbb{C}) = \mathrm{rank}(A)$. It follows that one has

(3.4.1) $$\langle \zeta, \zeta \rangle = \mathrm{rank}(A) \qquad \text{for every } \zeta \in \mu(A).$$

Example 3.5. Let Γ be a finite abelian group, and let $A = \mathbb{Z}[\Gamma]$. A short computation shows that for $x = \sum_{\gamma \in \Gamma} x_{\gamma}\gamma$ (with $x_{\gamma} \in \mathbb{Z}$) one has

$$\langle x, x \rangle = \#\Gamma \cdot \sum_{\gamma \in \Gamma} x_{\gamma}^2.$$

Hence for $x \neq 0$ one has $\langle x, x \rangle \geq \#\Gamma$, with equality if and only if $x \in \pm\Gamma$. Combining this with (3.4.1), one obtains Higman's theorem $\mu(\mathbb{Z}[\Gamma]) = \pm\Gamma$.

Example 3.6. Let Γ be a finite abelian group, let I be the $\mathbb{Z}[\Gamma]$-ideal $\mathbb{Z} \cdot \sum_{\gamma \in \Gamma} \gamma$, and put $A = \mathbb{Z}[\Gamma]/I$. For $x = (\sum_{\gamma \in \Gamma} x_{\gamma}\gamma) + I \in A$ (with $x_{\gamma} \in \mathbb{Z}$), one computes

$$\langle x, x \rangle = \sum_{\substack{\gamma, \delta \in \Gamma \\ \gamma < \delta}} (x_{\gamma} - x_{\delta})^2,$$

where $<$ is any total ordering on Γ. One readily deduces that for $x \neq 0$ this is at least $\#\Gamma - 1 = \mathrm{rank}(A)$, with equality if and only if $x \in \pm\Gamma + I$. As before, one deduces $\mu(\mathbb{Z}[\Gamma]/I) = \pm\Gamma + I$.

Example 3.7. Contrary to what the previous two examples might suggest, it is not the case that $\langle x, x \rangle \geq \mathrm{rank}(A)$ for every non-zero x in a reduced order A, not even when A is connected. For example, let A be the subring of the product ring $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ consisting of those elements whose

coordinates have the same parity, and choose $x = (2, 0, 0, 0, 0)$. Then $\mathrm{rank}(A) = 5$ and $\langle x, x \rangle = 4$. We will refer to this example in Remark 6.1, concerning the proof of Theorem 1.5(iii).

Lemma 3.8. *Suppose Γ is an abelian group, A is either a commutative $\mathbb{Q}$-algebra with $\dim_{\mathbb{Q}} A < \infty$ or an order, $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, and A has no non-zero homogeneous nilpotent elements. Then:*

    (i) *if $\delta \in \Gamma$ and δ has infinite order, then $B_\delta = 0$;*
    (ii) *the subgroup $\langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle$ is finite.*

Proof. By Lemma 2.4, for all but finitely many $\gamma \in \Gamma$ we have $B_\gamma = 0$. Suppose $\delta \in \Gamma$ has infinite order. Then there exists $N \in \mathbb{Z}_{>0}$ such that $B_{\delta^N} = 0$. Suppose $x \in B_\delta$. Then $x^N \in (B_\delta)^N \subset B_{\delta^N} = 0$, so x is homogeneous and nilpotent. By our assumption, $x = 0$, proving (i). Thus the abelian group $\langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle$ is generated by finitely many elements of finite order, so this group is finite, proving (ii). $\qquad\square$

Proposition 3.9. *Suppose Γ is an abelian group, A is a reduced order, and $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A. Then:*

    (i) *the subgroup $\langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle$ is finite;*
    (ii) *if $(\Gamma, \mathbf{B})$ is universal, then Γ is finite.*

Proof. Since A is reduced, it has no non-zero nilpotent elements, so (i) follows from Lemma 3.8(ii). Part (ii) now follows from (i) and Lemma 2.3. $\qquad\square$

4. Nilpotent and separable elements

We next prove Theorem 1.5(i). If R is a ring and $m \in \mathbb{Z}_{>0}$, we write $R^+[m]$ for the m-torsion in the additive group R.

Proposition 4.1. *Suppose A is a ring, Γ is an abelian group, and $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A.*

    (i) *If Γ is finite and $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in \sqrt{0_A}$, then $\#\Gamma \cdot \alpha_\delta \in \sqrt{0_A}$ for all $\delta \in \Gamma$.*
    (ii) *If Γ is finite and $A^+[\#\Gamma] = 0$, then $\sqrt{0_A}$ is a homogeneous ideal.*
    (iii) *If A is an order, then $\sqrt{0_A}$ is a homogeneous ideal.*

Proof. We first prove (i). Let k denote the exponent of the finite group Γ and let $A' = A[\zeta_k]$. We have $\alpha \in \sqrt{0_A} \subset \sqrt{0_{A'}}$, and since $\sqrt{0_{A'}}$ is an ideal we have $\chi(\delta)^{-1} \alpha \in \sqrt{0_{A'}}$ for all $\chi \in \hat{\Gamma}_k$ and $\delta \in \Gamma$. Since $\hat{\Gamma}_k$ acts by ring automorphisms (Lemma 2.5), we have $\sum_{\chi \in \hat{\Gamma}_k} \chi * (\chi(\delta)^{-1} \alpha) \in \sqrt{0_{A'}}$ for all $\delta \in \Gamma$. By Lemma 2.5 we now have $\#\Gamma \cdot \alpha_\delta \in \sqrt{0_{A'}} \cap A = \sqrt{0_A}$ for all $\delta \in \Gamma$.

We next prove (ii). Clearly, $\bigoplus_{\gamma \in \Gamma} (\sqrt{0_A} \cap B_\gamma) \subset \sqrt{0_A}$. For the reverse inclusion, suppose $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in \sqrt{0_A}$ and $\delta \in \Gamma$. By (i) we have $(\#\Gamma \cdot \alpha_\delta)^N = 0$ for some $N \in \mathbb{Z}_{>0}$. But $(\#\Gamma \cdot \alpha_\delta)^N = (\#\Gamma)^N \alpha_\delta^N$. If $A^+[\#\Gamma] = 0$, then $\alpha_\delta^N = 0$, so $\alpha_\delta \in \sqrt{0_A}$ as desired.

For (iii), let $\mathcal{I}$ denote the ideal generated by the homogeneous nilpotent elements of A, i.e., $\mathcal{I}$ is the largest homogeneous ideal of A contained in $\sqrt{0_A}$. Then $A/\mathcal{I}$ has a Γ-grading $(C_\gamma)_{\gamma \in \Gamma}$ with $C_\gamma = B_\gamma/(\sqrt{0_A} \cap B_\gamma)$, and $A/\mathcal{I}$ is an order with no non-zero homogeneous nilpotent elements. By Lemma 3.8(ii), the subgroup $\langle \gamma \in \Gamma : C_\gamma \neq 0 \rangle$ is finite; we can and do replace Γ with this finite group. Since orders have no non-zero torsion, (iii) now follows from (ii). $\qquad\square$

The following example shows that the condition that $A^+[\#\Gamma] = 0$ cannot be dropped from Proposition 4.1(ii).

Example 4.2. Suppose p is a prime number and Γ is any finite abelian group of order divisible by p. Then $A = \mathbb{F}_p[\Gamma] = \bigoplus_{\gamma \in \Gamma} \mathbb{F}_p \cdot \gamma$ is a Γ-graded ring and $(\sum_{\gamma \in \Gamma} \gamma)^2 = \#\Gamma \sum_{\gamma \in \Gamma} \gamma = 0$. So $\sum_{\gamma \in \Gamma} \gamma \in \sqrt{0_A}$, but the coordinates γ of $\sum_{\gamma \in \Gamma} \gamma$ are units and thus are not nilpotent, so the ideal $\sqrt{0_A}$ is not homogeneous.

We call a polynomial $f \in \mathbb{Q}[X]$ **separable** if f is coprime to its derivative f'. If E is a commutative $\mathbb{Q}$-algebra with $\dim_{\mathbb{Q}} E < \infty$, then $\alpha \in E$ is called **separable** if there exists a separable polynomial $f \in \mathbb{Q}[X]$ with $f(\alpha) = 0$. We write E_{sep} for the set of separable elements of E. Note that E_{sep} is a sub-$\mathbb{Q}$-algebra of E (see for example Lemma 2.2 of [4]). We will use the next result to prove Theorem 1.5(iii).

Proposition 4.3. *If Γ is an abelian group and $E = \bigoplus_{\gamma \in \Gamma} E_\gamma$ is a Γ-graded commutative $\mathbb{Q}$-algebra with $\dim_{\mathbb{Q}} E < \infty$, then both E_{sep} and $\sqrt{0_E}$ are homogeneous.*

Proof. By Lemma 2.4 the set $\{\gamma \in \Gamma : E_\gamma \neq 0\}$ is finite, and by Lemma 2.2 we may assume Γ is finite. For $\sqrt{0_E}$, see Proposition 4.1(ii). For E_{sep}, the proof is the same. Namely, suppose $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in E_{\text{sep}}$ and let $E' = E \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_k]$ with k the exponent of Γ. Then $\chi(\delta)^{-1} \in \langle \zeta_k \rangle \subset (E')_{\text{sep}}$, and $(E')_{\text{sep}}$ is a ring that is stable under the ring automorphisms of E'. As in the proof of Proposition 4.1, we obtain $\#\Gamma \cdot \alpha_\delta \in (E')_{\text{sep}} \cap E = E_{\text{sep}}$ for all $\delta \in \Gamma$. Since $(\#\Gamma)^{-1} \in \mathbb{Q} \subset E_{\text{sep}}$, we have $\alpha_\delta \in E_{\text{sep}}$ for all $\delta \in \Gamma$, as desired. $\square$

5. IDEMPOTENTS IN GRADED ORDERS

In this section we prove Theorem 1.5(ii) (see Proposition 5.9). We will use Proposition 5.8 to prove both Theorem 1.3 and Theorem 1.5.

Suppose L is a lattice. If $z \in L$, then a **decomposition** of z in L is a pair $(x, y) \in L \times L$ such that $z = x + y$ and $\langle x, y \rangle \geq 0$. We say that such a decomposition is **non-trivial** if $x \neq 0$ and $y \neq 0$. Call z **indecomposable** (in L) if the number of decompositions of z equals 2, or equivalently, if $z \neq 0$ and z has no non-trivial decompositions.

Remark 5.1. If L is a lattice and $z = x + y$ with $x, y, z \in L$, then:
  (i) $\langle x, y \rangle \geq 0 \iff \langle z, z \rangle \geq \langle x, x \rangle + \langle y, y \rangle$,
  (ii) $\langle x, y \rangle = 0 \iff \langle z, z \rangle = \langle x, x \rangle + \langle y, y \rangle$.

Remarks 5.2. (i) If z is a shortest non-zero vector in a lattice L, then z is indecomposable.
  (ii) If L is a lattice, then L is generated by its set of indecomposable elements.

Recall that $\text{Id}(A)$ denotes the set of idempotents of a ring A. Below we use the natural lattice structure on a reduced order that was given in Example 3.4.

Lemma 5.3. *If A is a reduced order and $x \in A$, then $\langle x, x \rangle \geq \#\{\sigma \in \text{Rhom}(A, \mathbb{C}) : \sigma(x) \neq 0\}$.*

Proof. If $\sigma(x) = 0$ for all $\sigma \in \text{Rhom}(A, \mathbb{C})$, then $x = 0$ (see for example Lemma 3.1 of [5]), and the desired result holds. Assume that $x \neq 0$. Applying the arithmetic-geometric mean inequality to obtain the first inequality below, and using that $\prod_{\sigma(x) \neq 0} \sigma(x)\overline{\sigma(x)} \in \mathbb{Z}_{>0}$ for the second, we have

$$\langle x, x \rangle = \sum_{\substack{\sigma \in \text{Rhom}(A, \mathbb{C}) \\ \sigma(x) \neq 0}} \sigma(x)\overline{\sigma(x)} = \#\{\sigma : \sigma(x) \neq 0\} \cdot \frac{\sum_{\sigma(x) \neq 0} \sigma(x)\overline{\sigma(x)}}{\#\{\sigma : \sigma(x) \neq 0\}}$$

$$\geq \#\{\sigma : \sigma(x) \neq 0\} \cdot \left(\prod_{\sigma(x) \neq 0} \sigma(x)\overline{\sigma(x)}\right)^{1/\#\{\sigma : \sigma(x) \neq 0\}} \geq \#\{\sigma : \sigma(x) \neq 0\}.$$

$\square$

Lemma 5.4. *If A is a reduced order and $e \in \text{Id}(A)$, then $\langle e, 1 - e \rangle = 0$.*

Proof. Since $e \in \text{Id}(A)$, for all $\sigma \in \text{Rhom}(A, \mathbb{C})$ we have $\sigma(e) \in \{0, 1\}$, so $\sigma(e)\overline{\sigma(1 - e)} = 0$. Thus, $\langle e, 1 - e \rangle = \sum_{\sigma \in \text{Rhom}(A, \mathbb{C})} \sigma(e)\overline{\sigma(1 - e)} = 0$. $\square$

Proposition 5.5. *Suppose A is a reduced order. Then the map*

$$F : \mathrm{Id}(A) \to \{decompositions\ of\ 1\ in\ A\}$$

defined by $e \mapsto (e, 1 - e)$ is a bijection, and its inverse sends a decomposition (x, y) of 1 to x.

Proof. We first show that the map F is well-defined. Suppose $e \in \mathrm{Id}(A)$. By Lemma 5.4 we have $\langle e, 1 - e \rangle = 0$. Thus $(e, 1 - e)$ is a decomposition of 1 in A, as desired.

The map F is clearly injective. To see that it is surjective, suppose (x, y) is a decomposition of 1 in A. By Lemma 5.3 we have $\langle x, x \rangle \geq \#\{\sigma \in \mathrm{Rhom}(A, \mathbb{C}) : \sigma(x) \neq 0\}$, and the same with y in place of x. Using that $x + y = 1$ to obtain the third equality, it follows that

$$
\begin{aligned}
\#\mathrm{Rhom}(A, \mathbb{C}) = \mathrm{rank}_{\mathbb{Z}} A = \langle 1, 1 \rangle &\geq \langle x, x \rangle + \langle y, y \rangle \\
&\geq \#\{\sigma \in \mathrm{Rhom}(A, \mathbb{C}) : \sigma(x) \neq 0\} + \#\{\sigma \in \mathrm{Rhom}(A, \mathbb{C}) : \sigma(y) \neq 0\} \\
&= \#\mathrm{Rhom}(A, \mathbb{C}) + \#\{\sigma \in \mathrm{Rhom}(A, \mathbb{C}) : \sigma(x) \neq 0,\ \sigma(y) \neq 0\} \\
&= \#\mathrm{Rhom}(A, \mathbb{C}) + \#\{\sigma \in \mathrm{Rhom}(A, \mathbb{C}) : \sigma(xy) \neq 0\}.
\end{aligned}
$$

Thus for all $\sigma \in \mathrm{Rhom}(A, \mathbb{C})$ we have $\sigma(xy) = 0$. So $x(1 - x) = xy = 0$. Thus, $x \in \mathrm{Id}(A)$ so F is surjective. $\square$

Corollary 5.6. *Suppose A is a reduced order. Then A is connected if and only if 1 is indecomposable.*

Lemma 5.7. *Suppose A is a reduced order, Γ is a finite abelian group, and $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A. Let k denote the exponent of the group Γ and let $A' = A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_k]$. Then:*
  (i) *A' is reduced;*
  (ii) *$\mathrm{Rhom}(A', \mathbb{C}) \cong \mathrm{Rhom}(A, \mathbb{C}) \times \mathrm{Rhom}(\mathbb{Z}[\zeta_k], \mathbb{C})$;*
  (iii) *for all $\alpha, \beta \in A \subset A'$ we have $\langle \alpha, \beta \rangle_{A'} = \varphi(k) \langle \alpha, \beta \rangle_A$, where $\langle\ ,\ \rangle_{A'}$ and $\langle\ ,\ \rangle_A$ are the inner products of Example 3.4 for A' and A, respectively.*

Proof. Part (i) holds since $A'_{\mathbb{Q}} = A_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_k)$ is a separable algebra over $\mathbb{Q}$ (since $A_{\mathbb{Q}}$ and $\mathbb{Q}(\zeta_k)$ are). Part (ii) is immediate. Part (iii) follows from (ii) since $\#\mathrm{Rhom}(\mathbb{Z}[\zeta_k], \mathbb{C}) = \varphi(k)$, so each element of $\mathrm{Rhom}(A, \mathbb{C})$ has $\varphi(k)$ extensions to A'. $\square$

Proposition 5.8. *Suppose A is a reduced order, Γ is an abelian group, $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, and $\langle\ ,\ \rangle$ is the inner product of Example 3.4. Suppose $\gamma, \delta \in \Gamma$ and $\gamma \neq \delta$. Then $\langle B_\gamma, B_\delta \rangle = 0$.*

Proof. The conclusion is clear if $B_\gamma = 0$ or $B_\delta = 0$. Thus, we can (and do) replace Γ by the subgroup $\langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle$, which is finite by Proposition 3.9(i).

Let k denote the exponent of the group Γ and embed A in $A' = A[\zeta_k] = \bigoplus_{\gamma \in \Gamma} B'_\gamma$ where $B'_\gamma = B_\gamma \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_k]$. It suffices to show $\langle B'_\gamma, B'_\delta \rangle_{A'} = 0$. Let $\alpha \in B'_\gamma$ and $\beta \in B'_\delta$. Choose $\chi \in \hat{\Gamma}_k$ such that $\chi(\gamma) \neq \chi(\delta)$. Since χ acts on A' by a ring automorphism (Lemma 2.5) we have

$$\langle \alpha, \beta \rangle_{A'} = \langle \chi * (\alpha), \chi * (\beta) \rangle_{A'} = \langle \chi(\gamma)\alpha, \chi(\delta)\beta \rangle_{A'} = \langle \alpha, \chi(\gamma)^{-1}\chi(\delta)\beta \rangle_{A'}.$$

Thus,

(5.8.1) $$\langle B'_\gamma, (1 - \chi(\gamma)^{-1}\chi(\delta))B'_\delta \rangle_{A'} = 0.$$

We have $\chi(\gamma)^{-1}\chi(\delta) \in \langle \zeta_k \rangle \smallsetminus \{1\}$. Thus, $1 - \chi(\gamma)^{-1}\chi(\delta)$ divides $\prod_{i=1}^{k-1}(1 - \zeta_k^i) = k$ in $\mathbb{Z}[\zeta_k]$. By (5.8.1) we now have $0 = \langle B'_\gamma, kB'_\delta \rangle_{A'} = k\langle B'_\gamma, B'_\delta \rangle_{A'}$. Thus, $\langle B'_\gamma, B'_\delta \rangle_{A'} = 0$. $\square$

Proposition 5.9. *Suppose A is an order, Γ is an abelian group, and $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A. Then $\mathrm{Id}(A) = \mathrm{Id}(B_1)$, and A is connected if and only if B_1 is connected.*

Proof. The inclusion $\mathrm{Id}(B_1) \subset \mathrm{Id}(A)$ is clear. For the reverse inclusion, take $e = (e_\gamma)_{\gamma \in \Gamma} \in \mathrm{Id}(A)$.

We first assume A is reduced. By Lemma 2.1(i) we have $(1 - e)_\gamma = -e_\gamma$ if $\gamma \neq 1$, and $(1 - e)_1 = 1 - e_1$. By Lemma 5.4 and Proposition 5.8 we have

$$0 = \langle e, 1 - e \rangle = \sum_{\gamma \in \Gamma} \langle e_\gamma, (1 - e)_\gamma \rangle = \langle e_1, 1 - e_1 \rangle - \sum_{\gamma \neq 1} \langle e_\gamma, e_\gamma \rangle \leq \langle e_1, 1 - e_1 \rangle,$$

so $(e_1, 1 - e_1)$ is a decomposition of 1. Now Proposition 5.5 and Lemma 5.4 give $\langle e_1, 1 - e_1 \rangle = 0$ so $0 = \sum_{\gamma \neq 1} \langle e_\gamma, e_\gamma \rangle$, and all e_γ with $\gamma \neq 1$ are 0. Hence $e \in B_1$.

For the general case, the natural maps $\mathrm{Id}(A) \to \mathrm{Id}(A/\sqrt{0_A})$ and $\mathrm{Id}(B_1) \to \mathrm{Id}(B_1/\sqrt{0_{B_1}})$ are bijections (this follows, for example, from Theorem 1.5 of [4]). By the reduced case, the natural map $\mathrm{Id}(B_1/\sqrt{0_{B_1}}) \to \mathrm{Id}(A/\sqrt{0_A})$ is a bijection. It follows that the inclusion $\mathrm{Id}(B_1) \hookrightarrow \mathrm{Id}(A)$ is a bijection. In particular, A is connected if and only if B_1 is connected. $\qquad\square$

6. Roots of unity in graded orders

In this section we prove Theorem 1.5(iii).

Remark 6.1. If A is a reduced order with a Γ-grading and $\zeta = (\zeta_\gamma)_{\gamma \in \Gamma} \in \mu(A)$, then by (3.4.1) and Proposition 5.8 we have $\mathrm{rank}(A) = \langle \zeta, \zeta \rangle = \sum_\gamma \langle \zeta_\gamma, \zeta_\gamma \rangle$. If each non-zero term in the latter sum were at least $\mathrm{rank}(A)$, then there would be at most one such term, and Theorem 1.5(iii) would follow. However, Example 3.7 exhibits a connected reduced order A and $x \in A$ with $0 < \langle x, x \rangle < \mathrm{rank}(A)$. Thus, more is required to prove Theorem 1.5(iii).

Lemma 6.2. *If A is a reduced order, Γ is an abelian group, $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, and $\alpha \in A$ is indecomposable, then there exists $\delta \in \Gamma$ such that $\alpha \in B_\delta$.*

Proof. Pick $\delta \in \Gamma$ with $\alpha_\delta \neq 0$. Then $\alpha = \alpha_\delta + (\alpha - \alpha_\delta)$, and we have $\alpha_\delta \in B_\delta$ and $\alpha - \alpha_\delta \in \bigoplus_{\gamma \neq \delta} B_\gamma$, so $\langle \alpha_\delta, \alpha - \alpha_\delta \rangle = 0$ by Proposition 5.8. Since $(\alpha_\delta, \alpha - \alpha_\delta)$ cannot be a non-trivial decomposition of the indecomposable element α, we have $\alpha - \alpha_\delta = 0$ as desired. $\qquad\square$

Proposition 6.3. *If A is an order, Γ is an abelian group, $(B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, and B_1 is connected, then $\mu(A) \subset \bigcup_{\gamma \in \Gamma} B_\gamma$.*

Proof. Proposition 5.9 shows that A is connected. Take $\zeta = (\zeta_\gamma)_{\gamma \in \Gamma} \in \mu(A)$.

First suppose A is reduced. Then 1 is indecomposable in A by Corollary 5.6. The map $x \mapsto \zeta x$ is a lattice automorphism of A. Hence ζ is also indecomposable in A. By Lemma 6.2, there exists $\delta \in \Gamma$ such that $\zeta \in B_\delta$, as desired.

For the general case, applying Proposition 4.3 to $E = A_{\mathbb{Q}}$ shows that $\zeta_\gamma \in E_{\mathrm{sep}}$ for all $\gamma \in \Gamma$. Also, $\zeta \bmod \sqrt{0_A} \in A/\sqrt{0_A} = \bigoplus_{\gamma \in \Gamma} B_\gamma/(\sqrt{0_A} \cap B_\gamma)$ is a root of unity, so by the reduced case there is a unique $\delta \in \Gamma$ such that $(\zeta \bmod \sqrt{0_A})_\delta$ is a root of unity and for all $\gamma \neq \delta$ we have $0 = (\zeta \bmod \sqrt{0_A})_\gamma = \zeta_\gamma \bmod (\sqrt{0_A} \cap B_\gamma)$. Thus for all $\gamma \neq \delta$ we have $\zeta_\gamma \in \sqrt{0_E} \cap E_{\mathrm{sep}} = \{0\}$. $\qquad\square$

7. Universal gradings—lemmas and examples

The results in this section follow in a straightforward way from the definitions, and are left as exercises.

Lemma 7.1. *Suppose A is a ring and Γ is an abelian group.*

(i) *Suppose $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading of A, suppose Δ is an abelian group, suppose $f : \Gamma \to \Delta$ is a group homomorphism, and let $f_*(\mathbf{B}) = (\sum_{\gamma \in f^{-1}(\delta)} B_\gamma)_{\delta \in \Delta}$. Then $f_*(\mathbf{B})$ is a Δ-grading of A.*

(ii) *The map $\Gamma \mapsto \{\Gamma\text{-gradings of } A\}$ is a covariant functor from the category of abelian groups to the category of sets.*

An abelian group H is called **indecomposable** if $H \neq 1$ and whenever $H = H_1 \oplus H_2$ with abelian groups H_1 and H_2 then $H_1 = 1$ or $H_2 = 1$.

Lemma 7.2. *Suppose A is a ring.*

   (i) *If $(\Gamma_1, (B_\gamma)_{\gamma \in \Gamma_1})$ and $(\Gamma_2, (C_\gamma)_{\gamma \in \Gamma_2})$ are universal gradings of A, then there is a unique group isomorphism $\sigma : \Gamma_1 \to \Gamma_2$ such that for all $\gamma \in \Gamma_1$ we have $B_\gamma = C_{\sigma(\gamma)}$.*
   (ii) *If $(\Gamma, (A_\gamma)_{\gamma \in \Gamma})$ is a universal grading of A, and $(C_\delta)_{\delta \in \Delta}$ is a Δ-grading of A, then for each $\delta \in \Delta$ for which C_δ is an indecomposable abelian group there exists $\gamma \in \Gamma$ with $C_\delta = A_\gamma$.*

Examples 7.3. We leave verifications of the below statements as an exercise. A hint is to use Lemma 7.2(ii).

   (i) The cyclotomic field $\mathbb{Q}(\zeta_8)$ has a $\mathbb{Z}/4\mathbb{Z}$-grading $\bigoplus_{j=0}^{3} \mathbb{Q} \cdot \zeta_8^j$ and a $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$-grading $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}i\sqrt{2}$ and has no universal grading. For $t \geq 4$, the field $\mathbb{Q}(\zeta_{2^t})$ equals $\mathbb{Q}(\eta)$, where $\eta = \zeta_{2^t}\sqrt{2}$, it has the two gradings $\bigoplus_{j=0}^{2^{t-1}-1} \mathbb{Q} \cdot \zeta_{2^t}^j$ and $\bigoplus_{j=0}^{2^{t-1}-1} \mathbb{Q} \cdot \eta^j$ by a cyclic group of order 2^{t-1}, and it has no universal grading. This example is taken from [1].
   (ii) The field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ has three different $\mathbb{Z}/6\mathbb{Z}$-gradings in which all pieces have dimension one over $\mathbb{Q}$, and has no universal grading.
   (iii) A $\mathbb{Z}/2\mathbb{Z}$-grading of $\mathbb{F}_{5^6}$ is $\mathbb{F}_{5^3} \oplus \mathbb{F}_{5^3} \cdot \sqrt{2}$, a $\mathbb{Z}/3\mathbb{Z}$-grading of $\mathbb{F}_{5^6}$ is $\mathbb{F}_{5^2} \oplus \mathbb{F}_{5^2} \cdot \zeta_9 \oplus \mathbb{F}_{5^2} \cdot \zeta_9^2$, but $\mathbb{F}_{5^6}$ has no universal grading.
   (iv) If $d \in \mathbb{Z}$ and d is not a square, then the $\mathbb{Z}/2\mathbb{Z}$-grading $\mathbb{Z} \oplus \sqrt{d}\mathbb{Z}$ is the universal grading on $\mathbb{Z}[\sqrt{d}]$. If A is an order of rank 2 and odd discriminant, then the grading by the trivial group is the universal grading on A.
   (v) The ring $\mathbb{Z}[\sqrt[3]{2}, \zeta_3]$ has a universal grading $\bigoplus_{j=0}^{2} \mathbb{Z}[\zeta_3]\sqrt[3]{2}^j$ by a cyclic group of order 3.
   (vi) The ring $\mathbb{Z}[X]/(X^2) = \mathbb{Z}[\varepsilon]$ has a universal grading by an infinite cyclic group $\Gamma = \langle c \rangle$, with $\mathbb{Z}[\varepsilon]_1 = \mathbb{Z}$, and $\mathbb{Z}[\varepsilon]_c = \mathbb{Z}\varepsilon$, and $\mathbb{Z}[\varepsilon]_\gamma = 0$ for all $\gamma \in \Gamma \smallsetminus \{1, c\}$. This also gives a $\mathbb{Z}/n\mathbb{Z}$-grading on the ring for every $n \in \mathbb{Z}_{>1}$. This non-reduced graded order has no universal grading by a finite abelian group.
   (vii) Let A be the subring of $\mathbb{Z}[X]/(X^4)$ generated by the images of 1, $2X(1+X)$, and $2X^2(1+X)$. Then A is a non-reduced order, and the grading of A by the trivial group is the universal grading of A.
   (viii) The ring $\mathbb{Z}[X, Y]/(X, Y)^2 = \mathbb{Z}[\varepsilon, \eta]$, with $\varepsilon = X \bmod (X, Y)^2$ and $\eta = Y \bmod (X, Y)^2$, has no universal grading. If Γ is any group, and σ and τ are non-identity distinct elements of Γ, then one grading is given by $B_1 = \mathbb{Z}$, $B_\sigma = \mathbb{Z}\varepsilon$, $B_\tau = \mathbb{Z}\eta$ and another by $B_1 = \mathbb{Z}$, $B_\sigma = \mathbb{Z}(\varepsilon + \eta)$, $B_\tau = \mathbb{Z}(\varepsilon + 2\eta)$.
   (ix) If Γ is an abelian group, then the universal grading of the group ring $\mathbb{Z}[\Gamma]$ is the natural Γ-grading $(\mathbb{Z} \cdot \gamma)_{\gamma \in \Gamma}$.

8. S-DECOMPOSITIONS OF LATTICES

We give a result on S-decompositions of lattices that we will use in §9 to prove Theorem 1.3.

If L is a lattice and S is a set, then an S-**decomposition** of L is a system $(L_s)_{s \in S}$ of subgroups of L such that:

   (i) if $s, t \in S$ and $s \neq t$, then $\langle L_s, L_t \rangle = 0$, and
   (ii) $\sum_{s \in S} L_s = L$.

This implies that $L = \bigoplus_{s \in S} L_s$, in the sense that the map $\bigoplus_{s \in S} L_s \to L, (\alpha_s)_{s \in S} \mapsto \sum_{s \in S} \alpha_s$ is bijective.

An S-decomposition $(L_s)_{s \in S}$ of a lattice L is **universal** if for every set T and every T-decomposition $(M_t)_{t \in T}$ of L, there is a unique map $f : S \to T$ such that for all $t \in T$ we have $M_t = \sum_{s \in f^{-1}(t)} L_s$.

If a set S and a universal S-decomposition exist for a given lattice, then by a standard argument S and that decomposition are, in an obvious sense, unique up to a unique isomorphism.

Theorem 8.1. *Every lattice has a universal S-decomposition for some finite set S, and for that universal S-decomposition all L_s are non-zero.*

Theorem 8.1 is classical and due to Eichler, and can be easily proved using the proof of Theorem 6.4 on p. 27 of [8].

9. Proof of Theorem 1.3

We now prove Theorem 1.3. Since A is a reduced order, it has a lattice structure as in Example 3.4. By Theorem 8.1 the lattice A has a universal S-decomposition $A = \bigoplus_{s \in S} L_s$ for some finite set S, and each L_s is non-zero. Let Γ be the abelian group with generating set S and relations $s_1 \cdot s_2 = s_3$ whenever there are $x \in L_{s_1}$ and $y \in L_{s_2}$ such that when we write $xy = \sum_{s \in S} z_s$ with $z_s \in L_s$ we have $z_{s_3} \neq 0$. This produces a group Γ equipped with a map $h : S \to \Gamma$, $s \mapsto s$, and we obtain a Γ-decomposition $(B_\gamma)_{\gamma \in \Gamma}$ of A with $B_\gamma = \sum_{s \in h^{-1}(\gamma)} L_s$. If $s_1 \in h^{-1}(\gamma_1)$ and $s_2 \in h^{-1}(\gamma_2)$ with $\gamma_1, \gamma_2 \in \Gamma$, then

$$L_{s_1} \cdot L_{s_2} \subset \sum_{u \in S, u = s_1 s_2} L_u \subset \sum_{u \in h^{-1}(\gamma_1 \gamma_2)} L_u = B_{\gamma_1 \gamma_2}.$$

Thus $B_{\gamma_1} B_{\gamma_2} \subset B_{\gamma_1 \gamma_2}$, so the Γ-decomposition $\mathbf{B} = (B_\gamma)_{\gamma \in \Gamma}$ is a Γ-grading.

Since each L_s is non-zero, we have that $B_\gamma \neq 0$ for all $\gamma \in h(S)$, so $\Gamma \supset \langle \gamma \in \Gamma : B_\gamma \neq 0 \rangle \supset \langle h(S) \rangle \supset \Gamma$. It now follows from Proposition 3.9(i) that Γ is finite.

To show the Γ-grading $\mathbf{B}$ is universal, let $\mathbf{C} = (C_\delta)_{\delta \in \Delta}$ be a Δ-grading of A, with Δ an abelian group. By Proposition 5.8, we have that $\mathbf{C}$ is a Δ-decomposition of the lattice A, so there is a unique map $g : S \to \Delta$ such that for all $\delta \in \Delta$ we have $C_\delta = \sum_{s \in g^{-1}(\delta)} L_s$. If $s_1 s_2 = u$ is one of the relations for the group Γ, then for some $x \in L_{s_1} \subset C_{g(s_1)}$ and $y \in L_{s_2} \subset C_{g(s_2)}$ we have a product xy with L_u-coordinate non-zero, so with $C_{g(u)}$-coordinate non-zero. But $C_{g(s_1)} C_{g(s_2)} \subset C_{g(s_1)g(s_2)}$ so $g(u) = g(s_1)g(s_2)$. So there is a unique group homomorphism $f : \Gamma \to \Delta$ such that $f \circ h = g$. This implies that $f_* \mathbf{B} = \mathbf{C}$, so the map $f \mapsto f_* \mathbf{B}$ is surjective. To show it is injective, suppose $\tilde{f} : \Gamma \to \Delta$ is a group homomorphism such that $\tilde{f}_* \mathbf{B} = \mathbf{C}$. By the uniqueness of f we have $f \circ h = \tilde{f} \circ h$. Since $\Gamma = \langle h(S) \rangle$ it follows that $f = \tilde{f}$, so the map $f \mapsto f_* \mathbf{B}$ is injective.

10. Proof of Theorem 1.4

Lemma 10.1. *Suppose $E = \bigoplus_{\gamma \in \Gamma} D_\gamma$ is a finite étale $\mathbb{Q}$-algebra graded by a finite abelian group Γ, suppose $\Gamma = \langle \gamma \in \Gamma : D_\gamma \neq 0 \rangle$, and suppose D_1 is a field. Then $\dim_{D_1} D_\gamma = 1$ for all $\gamma \in \Gamma$.*

Proof. Each non-zero homogeneous element has a power in D_1. That power is non-zero, hence a unit. Thus all homogeneous elements are units. If $\gamma \in \Gamma$ and $0 \neq x \in D_\gamma$, then the map $D_1 \to D_\gamma$, $a \mapsto ax$ is an isomorphism of D_1-vector spaces.

To see that each D_γ is non-zero, take $\gamma \in \Gamma$ and write it as $\gamma = \prod_{i=1}^r \gamma_i$ with each $D_{\gamma_i} \neq 0$. For each i, choose $0 \neq x_i \in D_{\gamma_i}$. Then $0 \neq \prod_{i=1}^r x_i \in D_\gamma$. $\square$

Lemma 10.2. *Suppose A is a Dedekind order and $A = \bigoplus_{\gamma \in \Gamma} B_\gamma$ is a Γ-grading. Then the order B_1 is also Dedekind.*

Proof. We have $B_1 = A \cap (B_1)_{\mathbb{Q}}$. It follows that B_1 is the ring of integers of the number field $(B_1)_{\mathbb{Q}}$. $\square$

Next we prove Theorem 1.4. It suffices to prove that if p is prime and $A = \bigoplus_{\gamma \in \Gamma} B_\gamma$ is a Dedekind order graded by a finite abelian p-group Γ with each $(B_\gamma)_{\mathbb{Q}}$ one-dimensional over the field $(B_1)_{\mathbb{Q}}$, then Γ is cyclic. To see that this suffices, invoke Lemma 2.3, replace Γ by its p-primary component

(viewing that component either as a subgroup or as a quotient group), and apply Lemma 10.1 with $E = A_{\mathbb{Q}}$.

Let p, A, Γ, $(B_\gamma)_{\gamma \in \Gamma}$ be as above and let q be the exponent of the p-group Γ. By Lemma 10.2 we have that B_1 is a Dedekind order.

Let $\mathfrak{p}$ be a prime ideal of B_1 containing p. Define the ring homomorphism $\phi : A \to A/\mathfrak{p}A$ by $\phi(x) = (x^q + \mathfrak{p}A)$; this is the canonical map $A \to A/\mathfrak{p}A$ followed by the q-th powering map from $A/\mathfrak{p}A$ to itself, the latter being a ring homomorphism because $A/\mathfrak{p}A$ contains the finite field $B_1/\mathfrak{p}$ of characteristic p. The restriction of ϕ to B_1 is the canonical map $B_1 \to B_1/\mathfrak{p}$ followed by an automorphism of $B_1/\mathfrak{p}$. For each $\gamma \in \Gamma$ one has $(B_\gamma)^q \subset B_1$, so $\phi(B_\gamma)$ lands in the subring $B_1/\mathfrak{p}$ of $A/\mathfrak{p}A$. Since the B_γ generate A, the image of ϕ in fact lies in $B_1/\mathfrak{p}$, giving the following diagram.

$$\begin{array}{ccc} A & \xrightarrow{\ \phi\ } & A/\mathfrak{p}A \\ \cup & \searrow & \cup \\ B_1 & \longrightarrow\!\!\!\!\!\rightarrow & B_1/\mathfrak{p} \end{array}$$

Let $\mathfrak{r} = \ker \phi$. Then $\mathfrak{r}$ is a prime ideal of A with $A/\mathfrak{r} \xrightarrow{\sim} B_1/\mathfrak{p}$, so $\mathfrak{r}$ lies over $\mathfrak{p}$ with residue class field degree $f(\mathfrak{r}/\mathfrak{p}) = 1$. Now we consider the familiar formula

(10.2.1) $$\sum_{\mathfrak{q}} e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p}) = [A_{\mathbb{Q}} : (B_1)_{\mathbb{Q}}] = \#\Gamma,$$

the sum ranging over the prime ideals $\mathfrak{q}$ of A lying over $\mathfrak{p}$ and $e(\mathfrak{q}/\mathfrak{p})$ denoting the ramification index; the last equality follows from our assumption on the $(B_\gamma)_{\mathbb{Q}}$. Let $\mathfrak{q}$ be one of those prime ideals. For each $x \in \mathfrak{r}$ one has $x^q \in \mathfrak{p}A \subset \mathfrak{q}$, so $x \in \mathfrak{q}$. This proves $\mathfrak{r} \subset \mathfrak{q}$, hence $\mathfrak{r} = \mathfrak{q}$, since $\mathfrak{r}$ is maximal. Thus there is only one $\mathfrak{q}$, namely $\mathfrak{q} = \mathfrak{r}$. Formula (10.2.1) now becomes $e(\mathfrak{r}/\mathfrak{p}) = \#\Gamma$. For each $x \in \mathfrak{r}$ one has $x^q \in \mathfrak{p}A = \mathfrak{r}^{e(\mathfrak{r}/\mathfrak{p})} = \mathfrak{r}^{\#\Gamma}$, so $q \cdot \mathrm{ord}_{\mathfrak{r}}(x) \geq \#\Gamma$; here $\mathrm{ord}_{\mathfrak{r}}$ counts factors $\mathfrak{r}$. Picking $x \in A$ such that $\mathrm{ord}_{\mathfrak{r}}(x) = 1$, then $x \in \mathfrak{r}$ so $q \geq \#\Gamma$. But a finite abelian group whose exponent is at least its order is clearly cyclic. This gives the desired result.

Remark 10.3. Note that instead of requiring that A be Dedekind, it suffices that it be locally Dedekind at all primes dividing its $\mathbb{Z}$-rank.

References

[1] D. van Gent, Master's thesis, Mathematisch Instituut, Universiteit Leiden, in preparation.

[2] G. Higman, *The units of group-rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.

[3] H. W. Lenstra, Jr. and A. Silverberg, *Lattices with symmetry*, Journal of Cryptology **30** (2017), 760–804, `http://doi.org/10.1007/s00145-016-9235-7`.

[4] H. W. Lenstra, Jr. and A. Silverberg, *Algorithms for commutative algebras over the rational numbers*, Foundations of Computational Mathematics **18** (2018), 159–180, `http://doi.org/10.1007/s10208-016-9336-6`.

[5] H. W. Lenstra, Jr. and A. Silverberg, *Testing isomorphism of lattices over CM-orders*, submitted for publication, `https://www.math.uci.edu/~asilverb/bibliography/CMorders.pdf`.

[6] H. W. Lenstra, Jr. and A. Silverberg, *Realizing commutative rings as group rings*, in preparation.

[7] W. May, *Group algebras over finitely generated rings*, J. Algebra **39** (1976), 483–511.

[8] J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73, Springer-Verlag, New York-Heidelberg, 1973.

[9] J. Oesterlé, *Schémas en groupes de type multiplicatif*, in Autour des schémas en groupes, Vol. I, Panoramas et Synthèses **42/43**, Société Mathématique de France, Paris, 2014, 63–91.

Mathematisch Instituut, Universiteit Leiden, The Netherlands
Email address: `hwl@math.leidenuniv.nl`

Department of Mathematics, University of California, Irvine, CA 92697, USA
Email address: `asilverb@uci.edu`