UNIVERSAL GRADINGS OF ORDERS

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

Abstract. An *order* is a commutative ring of which the additive group is a finitely generated free abelian group, and a *graded order* is an order that is provided with a grading by some abelian group. Examples are provided by group rings of finite abelian groups over rings of integers in number fields. We generalize known properties of nilpotents, idempotents, and roots of unity in such group rings to the case of graded orders. Our main result is that every reduced order has a grading that is *universal* in a natural sense. Most of our proofs depend on the observation that the additive group of any reduced order can in a natural way be equipped with a lattice structure.

1. Introduction

In the present paper we are interested in gradings of orders. All rings are supposed to be *commutative*. A ring is *reduced* if it has no non-zero nilpotent elements, where an element x is called nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$. By an *order* we mean a ring A of which the additive group A^+ is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$.

Suppose A is a ring, and Γ is a multiplicatively written abelian group with identity element 1. Then a Γ-*grading of* 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.

One of our main results concerns *universal gradings.* 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 a Δ-grading $(\sum_{\gamma\in f^{-1}(\delta)} B_\gamma)_{\delta\in\Delta}$ of A. This Δ-grading is denoted $f_*\mathbf{B}$. 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–iii)). Remarkably, we have the following result.

Theorem 1.1. *Every reduced order has a universal grading by some finite abelian group.*

Theorem 1.1 has applications to isomorphism problems for commutative group rings [3]. For the proof, see section 9.

It seems likely that our "archimedean" proof of Theorem 1.1 can be replaced by a p-adic one that applies to algebras over more general base rings than $\mathbb{Z}$. While our proof of Theorem 1.1 readily implies that there is an algorithm that, when given a reduced order, computes its universal grading, it is doubtful whether this can be done in polynomial time.

2010 *Mathematics Subject Classification.* 13A02.

Key words and phrases. graded orders, graded rings, lattices.

Support for the research was provided by the Alfred P. Sloan Foundation.

We also prove a result (Theorem 1.2) concerning nilpotents, idempotents, and roots of unity in graded orders.

Let A be 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 1.2. *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 1.2 are proved in Propositions 4.1, 5.9, and 6.2, respectively. Part (iii) plays an important role in other recent work of the authors; see [2].

If B is an order and Γ is a finite abelian group, then a Γ-grading of the group ring $B[\Gamma]$ is given by $(B \cdot \gamma)_{\gamma\in\Gamma}$. The statements of Theorem 1.2 in this case are known and can be deduced from results in [4] (Proposition 2 of [4] for (i), the Corollary to Proposition 3 for (ii), and the Corollary to Proposition 10 for (iii)).

Our proofs depend on two techniques. The first, which is more or less standard, consists of equipping a Γ-graded ring with an action by the dual of Γ, after a suitable cyclotomic base change; here Γ is supposed to be finite. The second, which is of a less algebraic nature, depends on the introduction of a natural lattice structure on any reduced order.

Acknowledgments. We thank Warren May for providing the references to [4].

2. Graded rings

In this section we give some lemmas that we will use to prove our main results.

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. □

If Γ is an abelian group and $k \in \mathbb{Z}$, let $\Gamma^k = \{\gamma^k : \gamma \in \Gamma\}$.

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 $\Delta = \Gamma/\Gamma^M$. □

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 $\Delta=\{1\}$. □

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). □

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 a finite group whose exponent divides k, we let

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

a multiplicative group with $\#\hat{\Gamma}_k = \#\Gamma$.

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. □

3. Euclidean vector spaces, lattices, and orders

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 $\mathrm{rad}(E)\subset\sqrt{0_E}$.)

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 $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$.

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.)

Lemma 3.4. *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). □

Corollary 3.5. *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 3.4(ii). Part (ii) now follows from (i) and Lemma 2.3. □

4. Nilpotent and separable elements

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 3.4(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). □

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 [1]).

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. □

5. Idempotents in graded orders

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.

If B and C are rings, we write $\text{Rhom}(B, C)$ for the set of ring homomorphisms from B to C. 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 3.3.

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 [2]), 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

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

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

□

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

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

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

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

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. □

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 3.3 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'. □

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 3.3. 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 Lemma 3.5(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,

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

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, $\langle B'_\gamma, B'_\delta\rangle_{A'} = 0$. □

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 $\operatorname{Id}(A) = \operatorname{Id}(B_1)$, and A is connected if and only if B_1 is connected.*

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

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 $\operatorname{Id}(A) \to \operatorname{Id}(A/\sqrt{0_A})$ and $\operatorname{Id}(B_1) \to \operatorname{Id}(B_1/\sqrt{0_{B_1}})$ are bijections (this follows, for example, from Theorem 1.5 of [1]). By the reduced case, the natural map $\operatorname{Id}(B_1/\sqrt{0_{B_1}}) \to \operatorname{Id}(A/\sqrt{0_A})$ is a bijection. It follows that the inclusion $\operatorname{Id}(B_1) \hookrightarrow \operatorname{Id}(A)$ is a bijection. In particular, A is connected if and only if B_1 is connected. □

6. Roots of unity in graded orders

Lemma 6.1. *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. □

Proposition 6.2. *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 6.1, 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 $\zeta_\gamma \in E_{\text{sep}}$ 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 $\zeta_\gamma \in \sqrt{0_E} \cap E_{\text{sep}} = \{0\}$. □

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 $\mathbb{Q}\oplus\mathbb{Q}\mathrm{i}\oplus\mathbb{Q}\sqrt{2}\oplus\mathbb{Q}\mathrm{i}\sqrt{2}$ and has no universal grading.

(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) 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.

(v) If $0\neq d\in\mathbb{Z}$, 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.

(vi) 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.

(vii) 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 tau 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 $B_1=\mathbb{Z}$, $B_\sigma=\mathbb{Z}(\varepsilon+\eta)$, $B_\tau=\mathbb{Z}(\varepsilon+2\eta)$.

8. S-decompositions of lattices

We give a result on S-decompositions of lattices that we will use in §9 to prove Theorem 1.1.

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 $M_t=\sum_{s\in f^{-1}(t)}L_s$.

Theorem 8.1. *Every lattice has a unique 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 [5].

9. Proof of Theorem 1.1

We now prove Theorem 1.1. Since A is a reduced order, it has a lattice structure with

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

as in Example 3.3. 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

$$L_{s_1} \cdot L_{s_2} \subset \sum_{u\in S, u=s_1s_2} L_u \subset \sum_{u\in h^{-1}(\gamma_1\gamma_2)} L_u = B_{\gamma_1\gamma_2}.$$

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 Lemma 3.5(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 $s_1s_2 = u$ 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.

References

[1] H. W. Lenstra, Jr. and A. Silverberg, *Algorithms for commutative algebras over the rational numbers*, Foundations of Computational Mathematics, online October 24, 2016, http://rdcu.be/lR4C.

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

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

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

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

Mathematisch Instituut, Universiteit Leiden, The Netherlands
E-mail address: hwl@math.leidenuniv.nl

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: asilverb@uci.edu