Research Paper

Realizing orders as group rings ☆

H.W. Lenstra Jr. [a,*], A. Silverberg [b,*], D.M.H. van Gent [a,*]

[a] *Mathematisch Instituut, Universiteit Leiden, the Netherlands*
[b] *Department of Mathematics, University of California, Irvine, CA 92697, USA*

A R T I C L E   I N F O

A B S T R A C T

An order is a commutative ring that as an abelian group is finitely generated and free. A commutative ring is reduced if it has no non-zero nilpotent elements. In this paper we use a new tool, namely, the fact that every reduced order has a universal grading, to answer questions about realizing orders as group rings. In particular, we address the Isomorphism Problem for group rings in the case where the ring is a reduced order. We prove that any non-zero reduced order R can be written as a group ring in a unique "maximal" way, up to isomorphism. More precisely, there exist a ring A and a finite abelian group G, both uniquely determined up to isomorphism, such that $R \cong A[G]$ as rings, and such that if B is a ring and H is a group, then $R \cong B[H]$ as rings if and only if there is a finite abelian group J such that $B \cong A[J]$ as rings and $J \times H \cong G$ as groups. Computing A and G for given R can be done by means of an algorithm that is not quite polynomial-time. We also give a description of the automorphism group of R in terms of A and G.

* Corresponding authors.
E-mail addresses: hwl@math.leidenuniv.nl (H.W. Lenstra), asilverb@uci.edu (A. Silverberg), d.m.h.van.gent@math.leidenuniv.nl (D.M.H. van Gent).

1. Introduction

Consider the map

$$(\{\text{rings}\}/\cong) \times (\{\text{groups}\}/\cong) \to (\{\text{rings}\}/\cong)$$

that for each ring A and each group G sends the pair of isomorphism classes of (A, G) to the isomorphism class of the group ring $A[G]$. The *Isomorphism Problem for group rings* asks about the fibers of this map, i.e., given a ring R, what can one say about the pairs (A, G) with $A[G] \cong R$? There is a great deal of literature on this subject, starting with the 1940 paper by Higman [4], which solved the case where $A = \mathbb{Z}$ and G is a finite abelian group, and including [15, Chapter 14], [17, Chapters III and IV], [18], and the recent survey article [16] and the references therein.

The emphasis has been on results stating that the fibers of our map are often "small" in a suitable sense. For instance, it is a consequence of a theorem of May [11] that if G is an abelian group and $\mathbb{Z}[G] \cong \mathbb{Z}[H]$ then $G \cong H$. This contrasts with the complex case, where $\mathbb{C}[G] \cong \mathbb{C}[H]$, even as $\mathbb{C}$-algebras, whenever G and H are finite abelian groups of the same order.

One can slightly refine the question by not just asking for the existence of an isomorphism from $A[G]$ to R, but asking for the isomorphism as well. For a given non-zero ring R the object of study is thus the set of triples (A, G, ϕ), where A is a ring (always with 1), G is a group, and $\phi \colon A[G] \to R$ is a ring isomorphism. This essentially comes down to considering the set

$$\mathcal{D}(R) = \{(A, G) : A \subset R \text{ a subring}, \, G \subset R^* \text{ a subgroup, with}$$
$$A[G] \to R \text{ a ring isomorphism}\},$$

where R^* is the group of units of R, and $A[G] \to R$ is the natural group homomorphism.

One of the main contributions of the present paper is a new group-theoretic description of the set $\mathcal{D}(R)$ for an important class of rings R, namely for connected reduced orders; see below for definitions. These rings are commutative, so A is commutative and G is abelian. The case of commutative group rings has received special attention in the literature (for example [1,10–14]), an important tool being the abelian group $\mu = \mu(R) = \{\zeta \in R : (\exists n \in \mathbb{Z}_{\geq 1}) \, \zeta^n = 1\}$ of *roots of unity* in a commutative ring R.

For connected reduced orders R we add a new tool, namely the universal grading of R and the abelian group $\Gamma = \Gamma(R)$ by which it is graded. The existence of such a universal grading was recently established in [9], and it was proved there that it comes with a natural map $d = d_R \colon \mu \to \Gamma$. In one of our main theorems (Theorem 6.7 below) we exhibit, for connected reduced orders R, a natural bijection

$$\mathcal{D}(R) \xrightarrow{\sim} \{f \in \text{Hom}(\Gamma, \mu) : f \circ d \circ f = f\}.$$

Thus, the set of realizations of a connected reduced order as a group ring is parametrized by an easily defined set of homomorphisms from Γ to μ, both of which are finite abelian groups.

The theorem just stated has several striking consequences in the context of the Isomorphism Problem. For example, in Theorem 1.1 we prove that among reduced orders, group rings can only be isomorphic if they are so for obvious reasons. In Theorem 1.2 we show that each non-zero reduced order can in a unique "maximal" way be realized as a group ring. In Theorem 1.3 we establish a curious "cross-over" result. For the connected case, we describe in Theorem 1.5 the group of ring automorphisms of such a maximal group ring.

Deducing these results from our description of $\mathcal{D}(R)$ is surprisingly non-trivial, and has two features that may be unexpected in the context of commutative algebra. The first is the use of modules over non-commutative rings, and the second the use of techniques from number theory, taken from [7] and [9]. We next give precise statements of some of our main results, along with a brief introduction to our new tool and methods.

By an *order* we mean a commutative ring of which the additive group is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. A ring element x is *nilpotent* if $x^n = 0$ for some $n \in \mathbb{Z}_{>0}$. We call a commutative ring *reduced* if it has no non-zero nilpotent elements.

Obviously, if A is a ring and I and H are groups, then the group rings $A[I \times H]$ and $(A[I])[H]$ are isomorphic as rings. The following result expresses that, among reduced orders, group rings can only be isomorphic if they are so for this obvious reason.

Theorem 1.1. *Suppose A and B are reduced orders and G and H are finite abelian groups. Then the following are equivalent:*

(i) *$A[G] \cong B[H]$ as rings,*
(ii) *there exist an order C and finite abelian groups I and J such that $A \cong C[I]$ and $B \cong C[J]$ as rings and $I \times G \cong J \times H$ as groups.*

The proof is given in Section 8.

We call a commutative ring R *stark* if there do not exist a ring A and a non-trivial group G such that R is isomorphic to the group ring $A[G]$.

Theorem 1.2. *Let R be a non-zero reduced order. Then there exist a stark ring A, unique up to ring isomorphism, and a finite abelian group G, unique up to group isomorphism, such that $R \cong A[G]$ as rings.*

Theorem 1.2 is an immediate consequence of Theorem 1.1, and we give a proof in Section 8. We note that Theorem 1.1 may be deduced from Theorem 1.2 using that group rings of finite abelian groups over reduced orders are reduced (see Proposition 5.7(i)). There are many examples showing that A and G in Theorem 1.2 need not be uniquely determined as a subring of R and a subgroup of R^*, respectively (see Example 6.11).

Theorems 1.1 and 1.2 are closely related to known results about group rings of torsion abelian groups over integral domains of characteristic zero; see Corollary 5 in [1] and Theorem 8 in [14], which were proved by studying the group of torsion units in the group ring. Our new tool, namely the consideration of gradings, allows us in the case of orders to replace the condition that the base ring be a domain by the weaker condition that it be stark and reduced.

A ring element x is *idempotent* if $x^2 = x$. We call a commutative ring *connected* if it has precisely two idempotents, i.e., the ring is non-zero and 0 and 1 are the only idempotents. For a commutative ring R with a subring $A \subset R$ and a subgroup $G \subset R^*$ we write $A[G] = R$ when the natural map $A[G] \to R$ is a ring isomorphism.

If R, A, and G are as in Theorem 1.2, then A is isomorphic to a subring of R, and G is isomorphic to a subgroup of $\mu(R)$, but as we remarked, this subring and subgroup need not be uniquely determined. However, in the important special case where R is connected, there is a sense in which the set of subrings $A \subset R$ that can be used and the set of subgroups $G \subset \mu(R)$ that can be used are entirely independent. The following "cross-over" result, which we found surprising, formulates this more precisely.

Theorem 1.3. *Let R be a connected reduced order. Suppose that A and B are stark subrings of R and that G and H are subgroups of R^* such that $A[G] = B[H] = R$. Then $A[H] = B[G] = R$.*

Theorem 1.3 will follow immediately from Theorem 6.10, which is proved in Section 6 below. As can be seen in Example 6.12, we cannot drop the assumption that R be connected in Theorem 1.3.

We call a ring element x *autopotent* if $x^{n+1} = x$ for some $n \in \mathbb{Z}_{>0}$, or equivalently if it is the product of a root of unity and an idempotent that commute with each other (see Proposition 9.6.iv).

We have the following algorithmic result. All our algorithms will be deterministic.

Theorem 1.4. *There is an algorithm that, given a non-zero reduced order R, computes a stark subring $A \subset R$ and a subgroup $G \subset \mu(R)$ such that $A[G] = R$. This algorithm runs* (a) *in polynomial time when the additive group of R is generated by autopotents, and generally* (b) *in time $n^{O(m)}$ where n is the length of the input and m is the number of minimal prime ideals of R.*

The proof of Theorem 1.4, and a description of the algorithm and how its input and output are given, are found in Section 9. Note that the algorithm runs in polynomial time when m is bounded by a constant. The case $m = 1$ is precisely the case where R is a domain, in which case one necessarily has $A = R$ and $G = 1$. A notable special case for (a) is when R is the product of finitely many group rings over $\mathbb{Z}$. We do not know whether there exists a polynomial-time algorithm that decides whether a given reduced order is stark.

We next discuss the new tool that we announced. A *grading* of a commutative ring R is a pair $(\Delta, (R_\delta)_{\delta \in \Delta})$ where Δ is an abelian group and the R_δ are additive subgroups of R such that, first, for all $\gamma, \delta \in \Delta$ one has $R_\gamma \cdot R_\delta \subset R_{\gamma\delta}$, and, second, one has $\bigoplus_{\delta \in \Delta} R_\delta = R$ in the sense that the natural map $\bigoplus_{\delta \in \Delta} R_\delta \to R$ is bijective. For each commutative ring A and abelian group G the ring $A[G]$ has a natural grading $(G, (A\gamma)_{\gamma \in G})$.

Suppose now that R is a reduced order. Two recent results from [9] (Theorems 5.5 and 5.6 below) are of crucial importance to the present paper. The first states that R has a grading $(\Gamma, (R_\gamma)_{\gamma \in \Gamma})$ that is universal in the sense that giving a grading of R with group Δ is equivalent to giving a group homomorphism $\Gamma \to \Delta$ (see Definition 5.3). The abelian group $\Gamma = \Gamma(R)$ is finite, and by universality it is canonically defined, so that the group $\mathrm{Aut}(R)$ of ring automorphisms acts on it (see Remark 6.4). The second result states that, if R is also connected, then for each $\zeta \in \mu$ there is a unique $\gamma \in \Gamma$ such that $\zeta \in R_\gamma$, and we write $d(\zeta) = \gamma$; this gives rise to a group homomorphism $d \colon \mu \to \Gamma$, sometimes denoted d_R, which we call the *degree map*.

For each $(A, G) \in \mathcal{D}(R)$, the natural grading of $A[G]$ gives rise to the grading $(\mu, (A_\zeta)_{\zeta \in \mu})$ of R, where $A_\zeta = A\zeta$ if $\zeta \in G$ and $A_\zeta = 0$ otherwise. This grading corresponds to a homomorphism $f \colon \Gamma \to \mu$. We prove in Theorem 6.7 that in the connected case this construction induces a bijection from $\mathcal{D}(R)$ to the set of f such that $fdf = f$, so $\mathcal{D}(R)$ can be studied group-theoretically as mentioned above.

Our next result is on automorphism groups of orders. As we saw in Theorem 1.2, any non-zero reduced order R may be written as $A[G]$, where A is a stark subring of R and G is a subgroup of $\mu(R)$, but it is only up to the action of the automorphism group $\mathrm{Aut}(R)$ that the pair (A, G) is unique. Thus, a natural question is how to describe the group $\mathrm{Aut}(R)$ in terms of A and G. Restricting to connected orders, which is the main case of interest, we show in Theorem 1.5 that this group has a somewhat curious description in terms of 2×2 matrices.

We write $\mu = \mu(A)$ and $\Gamma = \Gamma(A)$. There is a left action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(G, \mu)$ given via the restriction $\mathrm{Aut}(A) \to \mathrm{Aut}(\mu)$, and a right action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(\Gamma, G)$ induced by its action on Γ. For abelian groups M and N we will, here and elsewhere, write the group $\mathrm{Hom}(M, N)$ additively, regardless of the notation used for N.

Theorem 1.5. *Let A be a stark connected reduced order with degree map $d_A \colon \mu \to \Gamma$ and let G be a finite abelian group. We equip the cartesian product*

$$M = \begin{pmatrix} \mathrm{Aut}(A) & \mathrm{Hom}(G, \mu) \\ \mathrm{Hom}(\Gamma, G) & \mathrm{Aut}(G) \end{pmatrix}$$

of $\mathrm{Aut}(A)$, $\mathrm{Hom}(G, \mu)$, $\mathrm{Hom}(\Gamma, G)$, and $\mathrm{Aut}(G)$ with the following multiplication:

$$\begin{pmatrix} \alpha_1 & s_1 \\ t_1 & \sigma_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & s_2 \\ t_2 & \sigma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 + s_1 t_2 & \alpha_1 s_2 + s_1 \sigma_2 \\ t_1 \alpha_2 + \sigma_1 t_2 & t_1 d_A s_2 + \sigma_1 \sigma_2 \end{pmatrix},$$

where the sum in $\mathrm{Aut}(A)$ is as in Lemma 7.7 and the sum in $\mathrm{Aut}(G)$ is taken inside $\mathrm{End}(G)$. For $x \in A$ and $g \in G$ write $\binom{x}{g}$ for the element $x \cdot g \in A[G]$. Then:

(i) M is a group;
(ii) there is a group isomorphism $M \xrightarrow{\sim} \mathrm{Aut}(A[G])$ such that the action of M on the ring $A[G]$ is given by

$$\begin{pmatrix} \alpha & s \\ t & \sigma \end{pmatrix} \begin{pmatrix} x \\ g \end{pmatrix} = \begin{pmatrix} \alpha(x) \cdot s(g) \\ t(\gamma) \cdot \sigma(g) \end{pmatrix}$$

for all $g \in G$, $\gamma \in \Gamma$, and $x \in A_\gamma$.

For the proof and additional results, we refer to Section 7.

Theorem 1.6. Let A be a stark connected reduced order with degree map $d_A \colon \mu \to \Gamma$ and let G be a finite abelian group. Let $\mathcal{A} = \{\bigoplus_{\gamma \in \Gamma} A_\gamma t(\gamma) : t \in \mathrm{Hom}(\Gamma, G)\}$, a set of subrings of $A[G]$. Let $\mathcal{G} = \{\{s(g)g : g \in G\} : s \in \mathrm{Hom}(G, \mu)\}$, a set of subgroups of $A[G]^*$. Then

$$\mathcal{A} \times \mathcal{G} = \{(B, H) \in \mathcal{D}(A[G]) : B \text{ is stark}\}.$$

The pairs (B, H) in Theorem 1.6 are exactly the pairs occurring in Theorem 1.3 with $R = A[G]$. Theorem 1.6 allows one, in the connected case, to read off the set of subrings $A \subset R$ and the set of subgroups $G \subset R^*$ that can be used in Theorem 1.2. At the end of Section 8 we show how Theorem 1.6 readily follows from Theorems 1.5 and 1.2.

Our results suggest several questions. Which other rings have a universal grading? Under what conditions is there a degree map? Once one has a degree map $d \colon \mu \to \Gamma$, are there consequences for the Isomorphism Problem for group rings, even if μ or Γ is infinite? Can we replace rings by algebras over base rings other than $\mathbb{Z}$? For preliminary results in these directions, see Theorem 6.21 in [19] (cf. Theorem 5.5), and [20] (cf. Theorem 5.6).

The structure of the paper is as follows. Section 2 contains generalities on modules of finite length over rings that need not be commutative. We show in Section 3 that a morphism of abelian groups, in particular the degree map defined above, can be interpreted as a module over a certain matrix ring. This enables us, in Section 4, to apply the theorem of Krull–Remak–Schmidt to morphisms of finite abelian groups. Additionally, we introduce, for any morphism of abelian groups, an important group U^* that acts on it. In Section 5 we treat generalities on graded rings and group rings. In Section 6 we apply the theory from the former sections to the degree map of a connected reduced order. It is an essential property of U^* that its action on the degree map can be lifted to an action on the order (see Lemma 6.5). We prove Theorem 1.3 by showing that the pairs (A, G), (B, H), (A, H), and (B, G) are in the same orbit under the action of U^*. This effectively proves Theorems 1.1 and 1.2 in the connected case. In Section 7 we prove Theorem 1.5. Here U^* will make a further appearance. In Section 8 we deduce Theorems 1.1 and 1.2 by reduction to the connected case. Finally, the algorithmic Theorem 1.4 is proved in Section 9.

2. Modules and decompositions

In this section we gather some results on modules, by which we mean left modules. Let R be a ring and M an R-module. We call an R-module D a *divisor* of M if $M \cong D \oplus N$ for some R-module N. If $(M_i)_{i \in I}$ is a family of submodules of M, then there is a natural map $\bigoplus_{i \in I} M_i \to M$, and we write $\bigoplus_{i \in I} M_i = M$ if this map is an isomorphism. Likewise, if C, D, N are submodules of M, we write $C \oplus D = N$ if the natural map $C \oplus D \to M$ is injective with image N.

Definition 2.1. Let R be a ring and M an R-module. A *decomposition* of M is a pair $(I, (M_i)_{i \in I})$ where I is a set and the M_i are submodules of M such that $\bigoplus_{i \in I} M_i = M$; in this case we also call $(M_i)_{i \in I}$ an *I-indexed decomposition* of M. We call M *indecomposable* if M is non-zero and there do not exist non-zero R-modules D and N with $M \cong D \oplus N$.

We abbreviate $(M_i)_{i \in I}$ to $(M_i)_i$ when the index set is understood.

Definition 2.2. For a ring R and an R-module M we define

$$\mathrm{Id}(R) = \{e \in R : e^2 = e\},$$
$$\mathrm{Dec}(M) = \{(D, N) : D, N \text{ are submodules of } M \text{ with } D \oplus N = M\}.$$

We equip $\mathrm{Id}(R)$ with a partial order given by $e \leq f$ if and only if $ef = fe = e$. We equip $\mathrm{Dec}(M)$ with a partial order given by $(D, N) \leq (D', N')$ if and only if there exists a submodule $C \subset M$ such that $D = D' \oplus C$ and $N \oplus C = N'$.

The following result, which we will use to prove Theorem 1.3, is easily verified.

Proposition 2.3. *Let R be a ring and M an R-module. Then we have a bijection $\Phi \colon \mathrm{Id}(\mathrm{End}(M)) \to \mathrm{Dec}(M)$ given by $e \mapsto (\ker(e), \mathrm{im}(e))$. If we let $\mathrm{Aut}(M)$ act naturally both on $\mathrm{Id}(\mathrm{End}(M))$ by conjugation and on $\mathrm{Dec}(M)$ coordinate-wise, then Φ is an isomorphism of partially ordered sets that respects the action of $\mathrm{Aut}(M)$.*

A module has *finite length* if every totally ordered set of submodules is finite, or equivalently if it is both Noetherian and Artinian.

Theorem 2.4 *(Krull–Remak–Schmidt; see Theorem X.7.5 of [5]). Suppose R is a ring and M is an R-module of finite length. Then there exists a decomposition of M into finitely many indecomposable submodules, and such a decomposition is unique up to automorphisms of M and relabeling of the indices.*

Remark 2.5. Let R be a ring, and let $\mathcal{M}$ be a non-empty set of R-modules of finite length. As a consequence of Theorem 2.4, there exists up to isomorphism exactly one R-module D that is a divisor of every $M \in \mathcal{M}$ such that every R-module that is a divisor of every

$M \in \mathcal{M}$ is a divisor of D; it is called a *greatest common divisor* of the set $\mathcal{M}$. Every such D is of finite length. We say R-modules M and N are *coprime* if the greatest common divisor of $\{M, N\}$ is 0. Likewise, if $\mathcal{M}$ is a finite set of R-modules of finite length, then there exists up to isomorphism exactly one R-module L of which each $M \in \mathcal{M}$ is a divisor such that L is a divisor of each R-module of finite length of which each $M \in \mathcal{M}$ is a divisor; it is called a *least common multiple* of $\mathcal{M}$. Every such L is of finite length.

Definition 2.6. Suppose R is a ring, M is an R-module, and $h \in \mathrm{End}(M)$. We define the R-modules

$$\mathrm{lim\,im}(h) = \bigcap_{n=1}^{\infty} h^n(M) \quad \text{and} \quad \mathrm{lim\,ker}(h) = \bigcup_{n=1}^{\infty} \ker(h^n).$$

Lemma 2.7 *(Fitting; see Theorem X.7.3 of [5]). Suppose R is a ring, M is an R-module of finite length, and $h \in \mathrm{End}(M)$. Then $M = \mathrm{lim\,im}(h) \oplus \mathrm{lim\,ker}(h)$, the restriction of h to $\mathrm{lim\,im}(h)$ is an automorphism, and the restriction of h to $\mathrm{lim\,ker}(h)$ is nilpotent.*

Lemma 2.8. *Suppose R is a ring, M and N are R-modules, and $f\colon M \to N$ and $g\colon N \to M$ are morphisms. Then f restricts to morphisms $i\colon \mathrm{lim\,im}(gf) \to \mathrm{lim\,im}(fg)$ and $k\colon \mathrm{lim\,ker}(gf) \to \mathrm{lim\,ker}(fg)$. If M and N have finite length, then i is an isomorphism.*

Proof. We have $f(gf)^n(M) = (fg)^n f(M) \subset (fg)^n(N)$ for all $n \geq 1$. Hence $f(\mathrm{lim\,im}(gf)) \subset \mathrm{lim\,im}(fg)$, so i is well-defined. As

$$f(\ker((gf)^{n+1})) \subset \ker(g(fg)^n) \subset \ker((fg)^{n+1})$$

for all $n \geq 1$ we also get $f(\mathrm{lim\,ker}(gf)) \subset \mathrm{lim\,ker}(fg)$, so k is well-defined. By symmetry we obtain a restriction $j\colon \mathrm{lim\,im}(fg) \to \mathrm{lim\,im}(gf)$ of g. Under the finite length assumption both ji and ij are automorphisms by Lemma 2.7, hence i is an isomorphism. $\square$

Proposition 2.9. *Suppose R is a ring, M is an R-module of finite length, and A_1, A_2, B_1, $B_2 \subset M$ are submodules such that A_1 and A_2 are coprime, $A_1 \oplus A_2 = B_1 \oplus B_2 = M$, and $A_1 \cong B_1$. Then $A_1 \oplus B_2 = B_1 \oplus A_2 = M$.*

Note that under the above assumptions it immediately follows that $A_1 \oplus B_2 \cong B_1 \oplus B_2 = M$. This is not equivalent to $A_1 \oplus B_2 = M$, as this concerns a specific map $A_1 \oplus B_2 \to M$. We need to show that the natural map $B_1 \to M \to A_1$ is an isomorphism.

Proof. From Theorem 2.4 it follows that $A_2 \cong B_2$ and thus B_1 and B_2 are coprime as well. By symmetry it therefore suffices to show $B_1 \oplus A_2 = M$. We consider the maps as in the following commutative diagram, where $\varphi\colon A_1 \to B_1$ is an isomorphism, the maps to and from M are the natural inclusions and projections, and the f_i and g_i are defined to make the diagram commute.

$$
\begin{array}{ccc}
 & \xrightarrow{f_1} & A_1 \\
 & & \uparrow p_1 \\
A_1 \xrightarrow{\varphi} B_1 \xrightarrow{e} M & & \\
 & & \downarrow p_2 \\
 & \xrightarrow{f_2} & A_2
\end{array}
\qquad
\begin{array}{ccc}
A_1 & \xrightarrow{g_1} & \\
e_1 \downarrow & & \\
M \xrightarrow{p} B_1 \xrightarrow{\varphi^{-1}} A_1 & & \\
e_2 \uparrow & & \\
A_2 & \xrightarrow{g_2} &
\end{array}
$$

Note that $\mathrm{id}_{B_1} = pe$ and $\mathrm{id}_M = e_1 p_1 + e_2 p_2$, so

$$
\mathrm{id}_{A_1} = \varphi^{-1} pe\varphi = \varphi^{-1} p(e_1 p_1 + e_2 p_2)e\varphi = \varphi^{-1} pe_1 \cdot p_1 e\varphi + \varphi^{-1} pe_2 \cdot p_2 e\varphi = g_1 f_1 + g_2 f_2.
$$

Lemma 2.8 shows that $D = \lim \mathrm{im}(g_2 f_2) \cong \lim \mathrm{im}(f_2 g_2)$, so D is a divisor of both A_1 and A_2 by Lemma 2.7. Since A_1 and A_2 are coprime, we must have that $D = 0$ and thus $g_2 f_2$ is nilpotent. We conclude that $g_1 f_1 = \mathrm{id}_{A_1} - g_2 f_2$ is an automorphism of A_1. Hence f_1 is injective, and since A_1 is of finite length it must be an automorphism. It follows that $p_1 e = f_1 \varphi^{-1} \colon B_1 \to A_1$ is an isomorphism, so $M = B_1 \oplus A_2$, as was to be shown. $\quad\square$

Definition 2.10. Let R be a ring. A class $\mathcal{S}$ of R-modules is *multiplicative* if $0 \in \mathcal{S}$ and for all R-modules M, N and D with $M \cong N \oplus D$ and N, $D \in \mathcal{S}$ one has $M \in \mathcal{S}$. We say a multiplicative class $\mathcal{S}$ of R-modules is *saturated* if for all $M \in \mathcal{S}$ and all divisors D of M one has $D \in \mathcal{S}$. For a multiplicative class $\mathcal{S}$ of R-modules and an R-module M, write $\mathrm{Dec}_{\mathcal{S}}(M) = \{(M_1, M_2) \in \mathrm{Dec}(M) : M_2 \in \mathcal{S}\}$, where $\mathrm{Dec}(M)$ is as in Definition 2.2. We equip $\mathrm{Dec}_{\mathcal{S}}(M)$ with the partial order inherited from $\mathrm{Dec}(M)$, and write $\max(\mathrm{Dec}_{\mathcal{S}}(M))$ for its set of maximal elements.

Proposition 2.11. *Let R be a ring, let $\mathcal{S}$ be a multiplicative class of R-modules, and let M and N be R-modules. Then*

(i) *if $M \cong N$ and $N \in \mathcal{S}$, then $M \in \mathcal{S}$;*
(ii) *the set $\mathrm{Dec}_{\mathcal{S}}(M)$ is non-empty.*

Suppose in addition that $\mathcal{S}$ is saturated and that M is of finite length, and let (A_1, A_2), $(B_1, B_2) \in \mathrm{Dec}_{\mathcal{S}}(M)$. Then

(iii) *one has $(A_1, A_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$ if and only if 0 is the only divisor of A_1 that is in $\mathcal{S}$;*
(iv) *the set $\max(\mathrm{Dec}_{\mathcal{S}}(M))$ is non-empty and consists of one orbit of $\mathrm{Dec}_{\mathcal{S}}(M)$ under the action of $\mathrm{Aut}(M)$;*
(v) *if (A_1, A_2), $(B_1, B_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$, then (A_1, B_2), $(B_1, A_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$.*

Proof. (i) Apply the definition of multiplicative with $D = 0$.

(ii) The trivial element $(M, 0)$ is in $\mathrm{Dec}_{\mathcal{S}}(M)$.

(iii) If (A_1, A_2) is maximal but $A_1 = D \oplus B_1$ for some $D \in \mathcal{S}$ and some B_1, then $(A_1, A_2) \leq (B_1, A_2 \oplus D) \in \mathrm{Dec}_{\mathcal{S}}(M)$ and thus $A_2 = A_2 \oplus D$ and $D = 0$. Conversely,

suppose 0 is the only divisor of A_1 that is in $\mathcal{S}$ and $(A_1, A_2) \leq (B_1, B_2)$. Then there is some C such that $A_1 = B_1 \oplus C$ and $B_2 = A_2 \oplus C$. Since $\mathcal{S}$ is saturated we have $C \in \mathcal{S}$, and since C is a divisor of A_1 we must have that $C = 0$. Hence $(A_1, A_2) = (B_1, B_2)$ is maximal.

(iv) Let $M = \bigoplus_{i \in I} M_i$ with each M_i indecomposable. If A_2, respectively A_1, is the direct sum of those M_i that are, respectively are not, in $\mathcal{S}$, then (A_1, A_2) is in $\text{Dec}_{\mathcal{S}}(M)$ and it is maximal by (iii). If (B_1, B_2) is also maximal, then B_2, respectively B_1, is a direct sum of indecomposables that are, respectively are not, in $\mathcal{S}$; this follows from the definition of $\text{Dec}_{\mathcal{S}}(M)$ and from (iii). Since together these decompositions give a decomposition of M into indecomposables, Theorem 2.4 implies that $A_1 \cong B_1$ and $A_2 \cong B_2$, so (B_1, B_2) belongs to the $\text{Aut}(M)$-orbit of (A_1, A_2). Because the action of $\text{Aut}(M)$ preserves the partial order, this orbit is conversely contained in $\max(\text{Dec}_{\mathcal{S}}(M))$.

(v) By (iii) we have that A_1 and A_2 are coprime and by (iv) we have $A_1 \cong B_1$ and $A_2 \cong B_2$. We may conclude from Proposition 2.9 that $(A_1, B_2), (B_1, A_2) \in \text{Dec}_{\mathcal{S}}(M)$. Applying (iii) again we may conclude they are maximal. $\quad\square$

3. Morphisms as modules

In this section we will interpret a morphism of (finite) abelian groups as a (finite length) module, as expressed by Proposition 3.3. We will then study decompositions of this module and what this decomposition corresponds to in terms of the original morphism. This will enable us in the next section to apply the Krull–Remak–Schmidt theorem to morphisms of finite abelian groups.

We write $\left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix} \right)$ for the ring of lower-triangular 2×2 matrices with integer coefficients, **Ab** for the category of abelian groups, and **ab** for the category of finite abelian groups.

Definition 3.1. Let $\mathcal{C}$ be a category. We define the category of $\mathcal{C}$-*morphisms*, written $\mathcal{C}\text{Hom}$, where the objects are the morphisms of $\mathcal{C}$ and for objects $f \colon A \to B$ and $g \colon C \to D$ the morphisms from f to g are the pairs $(\alpha, \beta) \in \text{Hom}_{\mathcal{C}}(A, C) \times \text{Hom}_{\mathcal{C}}(B, D)$ such that $\beta f = g\alpha$, as in the following diagram:

$$
\begin{array}{ccc}
A & \xrightarrow{\;f\;} & B \\
{\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\
C & \xrightarrow{\;g\;} & D.
\end{array}
$$

The composition of $\mathcal{C}$-morphisms $(\gamma, \delta) \colon g \to h$ and $(\alpha, \beta) \colon f \to g$ is $(\gamma\alpha, \delta\beta)$.

Remark 3.2. Let $d \colon A \to B$ be a morphism of abelian groups. Then the set $\text{End}(d) \subset \text{End}(A) \times \text{End}(B)$ of endomorphisms of d is a ring. Moreover, we have natural maps $\text{End}(d) \to \text{End}(A)$ and $\text{End}(d) \to \text{End}(B)$, turning A and B into $\text{End}(d)$-modules. Similarly we write $\text{Aut}(d)$ for the group of automorphisms of d, which equals $\text{End}(d) \cap (\text{Aut}(A) \times \text{Aut}(B))$.

The following proposition can be thought of as an explicit instance of Mitchell's embedding theorem for abelian categories.

Proposition 3.3. *There is an equivalence of categories, specified in the proof, between the category* **Ab**Hom *and the category* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$**-Mod** *of* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$*-modules. This equivalence restricts to an equivalence between the subcategory* **ab**Hom *and the subcategory of* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$*-modules of finite length.*

Proof. We will define functors $F\colon \textbf{Ab}\text{Hom} \to \left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$**-Mod** and $G\colon \left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$**-Mod** $\to \textbf{Ab}\text{Hom}$ such that FG and GF are naturally isomorphic to the identity functors of their respective categories. For an object $f\colon A \to B$ we take $F(f)$ to be $A \oplus B$, where the $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure is given by

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa \\ yf(a) + zb \end{pmatrix} \qquad (\text{for } x, y, z \in \mathbb{Z},\ a \in A,\ b \in B).$$

For a $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module M we take $G(M)$ to be the morphism $E_{11}M \to E_{22}M$ given by multiplication with E_{21}, where E_{ij} is the 2×2 matrix having a 1 at position (i,j) and zeros elsewhere. The remainder of this proposition is a straightforward verification. $\square$

Definition 3.4. Write $\mathcal{I}$ for the class of $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules that correspond to isomorphisms under the equivalence of categories of Proposition 3.3.

One readily checks that the class $\mathcal{I}$ is multiplicative and saturated in the sense of Definition 2.10. We observe that a $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module M belongs to $\mathcal{I}$ if and only if its $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure can be extended to a $\left(\begin{smallmatrix}\mathbb{Z} & \mathbb{Z}\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure. This fact will not be needed, and we omit the proof.

Remark 3.5. Using the equivalence of categories of Proposition 3.3, one can translate terminology related to modules into terminology about morphisms of abelian groups. We briefly go through what is most relevant to us:

(i) If $f\colon A \to B$ is a morphism of abelian groups, then a *submodule* of the $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module corresponding to f corresponds to a *restriction* of f, i.e., a morphism $f'\colon A' \to B'$ where $A' \subset A$ and $B' \subset B$ are subgroups and $f'(a') = f(a') \in B'$ for all $a' \in A'$.

(ii) For morphisms $f\colon A \to B$ and $g\colon C \to D$ of abelian groups and for $r = (\alpha, \beta) \in \text{Hom}(f, g)$, the image $\text{im}(r)$ equals the restriction $\text{im}(\alpha) \to \text{im}(\beta)$ of g, and the kernel $\ker(r)$ equals the restriction $\ker(\alpha) \to \ker(\beta)$ of f.

(iii) If $(f_i)_{i \in I}$ is a family of morphisms $f_i\colon A_i \to B_i$ of abelian groups, then we write $\bigoplus_{i \in I} f_i$ for the natural map $\bigoplus_{i \in I} A_i \to \bigoplus_{i \in I} B_i$ and we write f/f_i for the induced map $A/A_i \to B/B_i$. One verifies that $\bigoplus_{i \in I} f_i$ corresponds to the direct sum of the $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules that the f_i correspond to. If $f\colon A \to B$ is a morphism and

$f_i\colon A_i \to B_i$ is a family of restrictions of f then, just as we do for modules, we will write $\bigoplus_{i\in I} f_i = f$ if the natural map $\bigoplus_{i\in I} f_i \to f$ is an isomorphism.

(iv) For a morphism $f\colon A \to B$, the set $\mathrm{Dec}(f)$ is the set of all pairs (f_0, f_1) of restrictions of f such that $f_0 \oplus f_1 = f$, which is a partially ordered set as in Definition 2.2. The set $\mathrm{Dec}_{\mathcal{I}}(f)$ is the set of $(f_0, f_1) \in \mathrm{Dec}(f)$ such that f_1 is an isomorphism.

Definition 3.6. For a morphism $f\colon A \to B$ of abelian groups we denote the ring of morphisms from f to f in the category $\mathbf{Ab}\mathrm{Hom}$ by $\mathrm{End}(f)$, we define

$$\mathrm{Prj}(f) = \{e \in \mathrm{Id}(\mathrm{End}(f)) : \mathrm{im}(e) \text{ is an isomorphism}\},$$

and we equip $\mathrm{Prj}(f)$ with the partial order inherited from the partial order on $\mathrm{Id}(\mathrm{End}(f))$ from Definition 2.2.

We have the following corollary to Proposition 2.3.

Corollary 3.7. *Let $f\colon A \to B$ be a morphism of abelian groups. Then we have an isomorphism $\mathrm{Prj}(f) \to \mathrm{Dec}_{\mathcal{I}}(f)$ of partially ordered sets that respects the action of $\mathrm{Aut}(f)$.*

4. The group U^*

In this section we fix a morphism $d\colon A \to B$ of abelian groups. We will define a group U^* that acts on d and study some of its properties.

Definition 4.1. For $f, g \in \mathrm{Hom}(B, A)$, define $f \star g = f d g \in \mathrm{Hom}(B, A)$, and extend $\star$ to a ring multiplication on the additive group $Q = Q(d) = \mathbb{Z} \oplus \mathrm{Hom}(B, A)$ by

$$(m, f) \star (n, g) = (mn, mg + nf + fdg)$$

for $m, n \in \mathbb{Z}$ and $f, g \in \mathrm{Hom}(B, A)$. We define the multiplicative monoid

$$U = U(d) = 1 + \mathrm{Hom}(B, A) \subset \mathbb{Z} \oplus \mathrm{Hom}(B, A) = Q$$

and write $U^* = U^*(d) = U \cap Q^*$ for the intersection of U with the group of units of Q.

It is easy to check that Q is indeed a ring with unit element $1 = (1, 0)$, and that the projection map $Q \to \mathbb{Z}$ is a ring homomorphism with kernel $\mathrm{Hom}(B, A)$. The inverse image of 1 equals U, and U^* is a group because it is the kernel of the induced group homomorphism $Q^* \to \mathbb{Z}^*$. The following lemma is easy to verify.

Lemma 4.2. *We have a ring homomorphism $q\colon Q \to \mathrm{End}(d)$ defined by sending 1 to the identity id_d and $f \in \mathrm{Hom}(B, A)$ to (fd, df). It restricts to a group homomorphism $U^* \to \mathrm{Aut}(d)$.*

Remark 4.3. Recall from Remark 3.2 that A and B are $\mathrm{End}(d)$-modules. The map q makes A and B into Q-modules in such a way that d is Q-linear.

Definition 4.4. We write

$$\mathrm{Id}_0 = \mathrm{Id}_0(d) = \mathrm{Id}(Q) \cap \mathrm{Hom}(B, A) = \{f \in \mathrm{Hom}(B, A) : fdf = f\}$$

with Q as in Definition 4.1. We equip Id_0 with the partial order inherited from the partial order on $\mathrm{Id}(Q)$ as in Definition 2.2.

Remark 4.5. From Lemma 4.2 we get a map $U^* \to \mathrm{Aut}(d)$, i.e., U^* acts on d. In turn, since an isomorphism between d's induces a bijection between their Id_0's, the group $\mathrm{Aut}(d)$ acts on Id_0. However, U^* acts directly on Id_0 by conjugation within Q. Although we will not need it, both of the induced maps $U^* \to \mathrm{Aut}(\mathrm{Id}_0)$ are the same.

Recall the terminology $\mathrm{im}(r)$, $\ker(r)$, and $\bigoplus_{i \in I} f_i$ from Remark 3.5, and $\mathrm{Prj(d)}$ from Definition 3.6. If $e \in \mathrm{End}(d)$, we write $e = (e_A, e_B)$ with $e_A \in \mathrm{End}(A)$ and $e_B \in \mathrm{End}(B)$.

Proposition 4.6. *The map* $q \colon Q \to \mathrm{End}(d)$ *from Lemma 4.2 restricts to an isomorphism* $\mathrm{Id}_0(d) \xrightarrow{\sim} \mathrm{Prj(d)}$ *of partially ordered sets that respects the action of* $\mathrm{Aut}(d)$. *Its inverse is the map given by* $e \mapsto 0_e \oplus \mathrm{im}(e)^{-1}$, *where* $0_e \colon \ker(e_B) \to \ker(e_A)$ *is the zero map.*

Proof. Write $\Phi \colon \mathrm{Id}_0(d) \to \mathrm{End}(d)$ for the restriction of q, and write $\Psi \colon \mathrm{Prj(d)} \to \mathrm{Hom}(B, A)$ for the map $e \mapsto 0_e \oplus \mathrm{im}(e)^{-1}$. To see that Ψ is well defined, note that e and hence e_A and e_B are idempotents, so $A = \ker(e_A) \oplus \mathrm{im}(e_A)$ and likewise for B by Proposition 2.3.

Let $e \in \mathrm{Prj(d)}$ and $f = \Psi(e)$. Note that $fd = e_A$, by considering the restriction to $\mathrm{im}(e_A)$ and $\ker(e_A)$ separately, and similarly $df = e_B$ and $fe_B = f$. Hence $q(f) = e$ and $q \circ \Psi = \mathrm{id}_{\mathrm{Prj(d)}}$. For $g \in \mathrm{Hom}(B, A)$ we have $g \star f = gdf = ge_B$. In particular $f \star f = fe_B = f$, so $f \in \mathrm{Id}_0$. Thus Ψ restricts to $\mathrm{Prj(d)} \to \mathrm{Id}_0$.

Since q is a ring homomorphism, it maps idempotents to idempotents. For $f \in \mathrm{Id}_0$ it follows from $fdf = f$ that f and d are mutually inverse when restricted to $\mathrm{im}(df) \to \mathrm{im}(fd)$, respectively $\mathrm{im}(fd) \to \mathrm{im}(df)$. In particular $\mathrm{im}(q(f))$, which is precisely the restriction of d just mentioned, is an isomorphism. Hence Φ restricts to $\mathrm{Id}_0 \to \mathrm{Prj(d)}$. Moreover, the restriction of f to $\ker(df) \to \ker(fd)$ is zero since $fdf = f$, so $\Psi(\Phi(f)) = f$. We conclude that Φ and Ψ are mutually inverse.

All constructions are functorial in d and thus $\mathrm{Aut}(d)$ commutes with Φ. The definition of the partial order on idempotents is completely algebraic, so the partial order is preserved by Φ, which is the restriction of a ring homomorphism. If $e, e' \in \mathrm{Prj(d)}$ are such that $ee' = e = e'e$, then $\Psi(e) \star \Psi(e') = \Psi(e)e'_B = \Psi(e)e_Be'_B = \Psi(e)e_B = \Psi(e)$, and likewise $\Psi(e') \star \Psi(e) = \Psi(e)$, so Ψ preserves the partial order as well. $\quad\square$

In the following results, we use the terminology from Remark 3.5. We let U^* act on $\mathrm{Dec}(d)$ via the map $U^* \to \mathrm{Aut}(d)$ from Lemma 4.2.

Lemma 4.7. *Let $d_i \colon A_i \to B_i$ with $i \in \{-1, 0, 1\}$ be restrictions of d such that (d_0, d_1) and (d_0, d_{-1}) belong to $\mathrm{Dec}(d)$, and suppose that d_0 or d_1 is an isomorphism. Then $(d_0, d_{-1}) \in U^* \cdot (d_0, d_1)$.*

Proof. We have $A_0 \oplus A_1 \cong A \cong A_0 \oplus A_{-1}$. Hence the map $A_1 \to A_{-1}$ given by $x \mapsto x_{-1}$ where $x = x_0 + x_{-1}$ with $x_i \in A_i$ is an isomorphism. Similarly, we have a natural isomorphism $g_1 \colon d_1 \to d/d_0 \to d_{-1}$, and its extension $g = \mathrm{id}_{d_0} \oplus g_1 \in \mathrm{Aut}(d)$ maps (d_0, d_1) to (d_0, d_{-1}). Letting $r = \mathrm{id}_d - g \in \mathrm{End}(d)$, then $r(d_1) \subset d_0$ and $r(d_0) = 0$, so $r^2 = 0$. We first construct $f \in \mathrm{Hom}(B, A)$ that maps to r under $q \colon Q \to \mathrm{End}(d)$. Write $r = (r_A, r_B)$ with $r_A \in \mathrm{End}(A)$ and $r_B \in \mathrm{End}(B)$. Since d_0 or d_1 is invertible, there exists $f_1 \colon B_1 \to A_0$ such that the diagram

$$
\begin{array}{ccc}
A_1 & \xrightarrow{\ d_1\ } & B_1 \\
{\scriptstyle r_A}\downarrow & {\scriptstyle f_1} & \downarrow{\scriptstyle r_B} \\
A_0 & \xrightarrow[\ d_0\ ]{} & B_0
\end{array}
$$

commutes. Then $f = 0 \oplus f_1$ with $0 \colon B_0 \to A_1$ satisfies $(fd, df) = r$, so f does map to r under $q \colon Q \to \mathrm{End}(d)$. From $f \star f \star f = fdfdf = r_A^2 f = 0$ we see that f is nilpotent, so the element $1 - f \in U$ belongs to U^*. Since $1 - f$ maps to $\mathrm{id}_d - r = g$ via q, it sends (d_0, d_1) to (d_0, d_{-1}). $\square$

The proof of the following proposition, which can be considered a sharpening of Proposition 2.11.iv when $R = \left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix} \right)$, is the main reason for considering d as a module.

Proposition 4.8. *Assume A and B are finite. Then the set of maximal elements of $\mathrm{Dec}_{\mathcal{I}}(d)$ equals one orbit of $\mathrm{Dec}_{\mathcal{I}}(d)$ under the action of U^*.*

Proof. By Proposition 3.3 we may apply Proposition 2.11.iv. Thus, it suffices to show that any two maximal elements $(d_0, d_1), (e_0, e_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ are in the same U^*-orbit. Recall that $(d_0, e_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ by Proposition 2.11.v. Applying Lemma 4.7 we obtain $(d_0, e_1) \in U^* \cdot (d_0, d_1)$ since d_1 is an isomorphism, and $(e_0, e_1) \in U^* \cdot (d_0, e_1)$ since e_1 is an isomorphism. Thus $(e_0, e_1) \in U^* \cdot (d_0, e_1) = U^* \cdot (d_0, d_1)$. $\square$

5. Graded rings

In this section we consider gradings, which may be viewed as a generalization of group rings. In Section 6 we will use them to prove Theorem 1.3. We begin by giving the definitions as we need them, and state some results from [9].

Definition 5.1 *(Definition 1.1 and Lemma 7.1 in [9]).* Let R be a commutative ring. A *grading* of R is a pair $(\Delta, \mathcal{R})$ where Δ is a (multiplicatively written) abelian group and $\mathcal{R} = (R_\delta)_{\delta \in \Delta}$ is a Δ-indexed decomposition of R as a $\mathbb{Z}$-module, as defined in Definition 2.1, such that $R_\gamma R_\delta \subset R_{\gamma\delta}$ for all γ, $\delta \in \Delta$. For a grading $(\Delta, \mathcal{R})$ with $\mathcal{R} = (R_\delta)_{\delta \in \Delta}$ and a group homomorphism $f \colon \Delta \to \mathrm{E}$, we define $f_*(\mathcal{R})$ to be the E-indexed decomposition $(S_\epsilon)_{\epsilon \in \mathrm{E}}$ of R defined by $S_\epsilon = \sum_{\delta \in f^{-1}\epsilon} R_\delta$; then $(\mathrm{E}, f_*(\mathcal{R}))$ is a grading of R. We turn the class of gradings of R into a category by defining a morphism $(\Delta, \mathcal{R}) \to (\mathrm{E}, \mathcal{S})$ to be a group homomorphism $f \colon \Delta \to \mathrm{E}$ for which $f_*(\mathcal{R}) = \mathcal{S}$.

From now on, we will usually write $(R_\delta)_\delta$ instead of $(R_\delta)_{\delta \in \Delta}$.

Remark 5.2. Note that every non-zero commutative group ring $A[G]$ naturally comes with a grading $(G, (Ag)_g)$. Let R be a commutative ring. Analogously to writing $\bigoplus_{i \in I} M_i = M$ for submodules M_i of some R-module M when the natural map $\bigoplus_{i \in I} M_i \to M$ is an isomorphism, we write $R = A[G]$ for a subring A of R and subgroup G of R^* if the natural map $A[G] \to R$ is an isomorphism.

Definition 5.3 *(Definition 1.2 in [9]).* Let R be a commutative ring. A grading $(\Gamma, \mathcal{R})$ of R is called *universal* if it is an initial object of the category of gradings of R, or equivalently if for every grading $(\mathrm{E}, \mathcal{S})$ of R there is a unique group homomorphism $f \colon \Gamma \to \mathrm{E}$ such that $f_*(\mathcal{R}) = \mathcal{S}$. If a universal grading $(\Gamma, \mathcal{R})$ exists, then it is unique up to a unique isomorphism and we refer to it as *the* universal grading of R. We write $\Gamma(R) = \Gamma$ for the group of this grading.

Remark 5.4. If R and R' are commutative rings that have universal gradings, then any ring isomorphism $R \to R'$ induces a group isomorphism $\Gamma(R) \to \Gamma(R')$, so $\Gamma(R)$ behaves functorially under ring isomorphisms; in particular, the group $\mathrm{Aut}(R)$ of ring automorphisms of R acts in a natural way on $\Gamma(R)$.

Two important results on gradings of orders from [9] are fundamental to the present paper. The first concerns the existence of a universal grading. Recall a commutative ring is *reduced* if it has no non-zero nilpotent elements.

Theorem 5.5 *(Theorem 1.3 of [9]).* *If R is a reduced order, then R has a universal grading and $\Gamma(R)$ is finite.*

The second result relates to roots of unity. Recall that a commutative ring R is *connected* if it has exactly two idempotents and that $\mu(R)$ is the group of roots of unity in R.

Theorem 5.6 *(Theorem 1.5.iii in [9]).* *If R is a connected order and $(\Delta, (R_\delta)_\delta)$ is a grading of R, then $\mu(R) \subset \bigcup_{\delta \in \Delta} R_\delta$.*

The proofs of these two theorems as given in [9] are of a number-theoretic nature. For algebraic arguments one may refer to [19,20].

Another useful fact is that the properties of being reduced and being connected are preserved under construction of group rings. We write $\mathrm{nil}(R)$ for the set of nilpotent elements of a commutative ring R.

Proposition 5.7 *(Theorem 1.5 in [9]). Let A be an order and G a finite abelian group. Then:*

(i) $\mathrm{nil}(A[G]) = \mathrm{nil}(A)[G]$, *and A is reduced if and only if $A[G]$ is reduced;*

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

(iii) *If A is connected, then $\mu(A[G]) = \mu(A) \times G$.*

Proof. We apply the theory of gradings to the natural grading of $A[G]$. For (i) we apply Theorem 1.5.i in [9] so that $\mathrm{nil}(A[G]) = \bigoplus_{g \in G}(\mathrm{nil}(A[G]) \cap Ag) = \mathrm{nil}(A)[G]$. The remaining equivalence follows trivially. Theorem 1.5.ii and iii in [9] prove (ii) and (iii). □

Proposition 5.8. *Suppose $\overline{R} = (\Delta, (R_\delta)_\delta)$ is a grading of a commutative ring R and let*

$$\Delta' = \langle \delta \in \Delta : R_\delta \neq 0 \rangle.$$

Then:

(i) *We have that $\overline{R}' = (\Delta', (R_\delta)_\delta)$ is a grading of R.*

(ii) *The inclusion $i \colon \Delta' \to \Delta$ is a morphism $\overline{R}' \to \overline{R}$ of gradings.*

(iii) *If $\overline{S}$ is a grading of R and there exists a morphism $f \colon \overline{R} \to \overline{S}$, then there exists a unique morphism $f' \colon \overline{R}' \to \overline{S}$. It equals $f \circ i$.*

(iv) *If there exists a morphism from $\overline{R}'$ to a universal grading, then $\overline{R}'$ is universal.*

(v) *If $\overline{R}$ is universal, then $\Delta = \Delta'$.*

Proof. Both (i) and (ii) are trivial. For (iii), clearly $f \circ i$ is such a morphism. For uniqueness, it follows from the definitions that f' must equal f for all $\delta \in \Delta$ such that $R_\delta \neq 0$, and such δ generate Δ'. For (iv), we have a map from $\overline{R}'$ to any other grading by passing through the universal grading, and such a map is unique by (iii). For (v), if $\overline{R}$ is universal, then so is $\overline{R}'$ by (ii) and (iv), and then i is a bijection since universal objects are uniquely unique. □

Proposition 5.9. *Let S and T be orders, write $R = S \times T$, and let $\pi \colon R \to S$ be the natural projection.*

(i) *If $(\Delta, (R_\delta)_\delta)$ is a grading of R, then $(\Delta', (\pi(R_\delta))_\delta)$ with $\Delta' = \langle \delta \in \Delta : \pi(R_\delta) \neq 0 \rangle$ is a grading of S, and if the former is universal, then so is the latter.*

(ii) *If* $(E, (S_\epsilon)_\epsilon)$ *and* $(Z, (T_\zeta)_\zeta)$ *are gradings of* S, *respectively* T, *then* $(E \times Z, (R_{(\epsilon,\zeta)})_{(\epsilon,\zeta)})$ *with* $R_{1,1} = S_1 \times T_1$, $R_{\epsilon,1} = S_\epsilon \times \{0\}$ *for* $\epsilon \neq 1$, $R_{1,\zeta} = \{0\} \times T_\zeta$ *for* $\zeta \neq 1$, *and* $R_{(\epsilon,\zeta)} = \{(0,0)\}$ *for* $\epsilon \neq 1$, $\zeta \neq 1$, *is a grading of* R. *If the first two are universal, then so is the latter.*

Proof. (i) Clearly $S = \sum_{\delta \in \Delta'} \pi(R_\delta)$. We identify S with $S \times \{0\} \subset R$, so that $\pi(R_\delta) = (1,0) \cdot R_\delta$. As $(1,0) \in R_1$ by Theorem 1.5.ii in [9], we find $\pi(R_\delta) \subset R_\delta$, and hence the sum of the $\pi(R_\delta)$ is a direct sum. It follows that $(\Delta', (\pi(R_\delta))_\delta)$ is a grading of S.

Suppose that $(\Delta, (R_\delta)_\delta)$ is universal and let $(E, (S'_\epsilon)_\epsilon)$ be a grading of S. Then $(E, (S_\epsilon)_\epsilon)$ with $S_1 = S'_1 \times T$ and $S_\epsilon = S'_\epsilon \times \{0\}$ for $\epsilon \neq 1$ is a grading of R. By universality, there is a group homomorphism $f \colon \Delta \to E$ such that $f_*((R_\delta)_\delta) = (S_\epsilon)_\epsilon$. Its restriction f' to a map $\Delta' \to E$ is a morphism $(\Delta', (\pi(R_\delta))_\delta) \to (E, (S'_\epsilon)_\epsilon)$, and the map is unique by Proposition 5.8.iii. We conclude that $(\Delta', (\pi(R_\delta))_\delta)$ is universal.

(ii) The first statement is immediate. For universality, any grading $(\Delta, \mathcal{R})$ of R induces, as in (i), gradings of S and of T by the same group Δ, which come from unique group homomorphisms $E \to \Delta$ and $Z \to \Delta$. One readily checks that the induced group homomorphism $E \times Z \to \Delta$ is the unique morphism $(E \times Z, (R_{(\epsilon,\zeta)})_{(\epsilon,\zeta)}) \to (\Delta, \mathcal{R})$. The details are left to the reader. $\square$

Definition 5.10. When R is a commutative ring, we define the set

$$\mathcal{D}(R) = \{(A, G) : A \subset R \text{ a subring}, G \subset R^* \text{ a subgroup}, A[G] = R\},$$

and equip it with a partial order $\leq$ given by $(B, H) \leq (A, G)$ if and only if $H \subset G$ and $B \supset A$.

Note that $\mathrm{Aut}(R)$ naturally acts component-wise on $\mathcal{D}(R)$.

Lemma 5.11. *Suppose* R *is a non-zero order. Then for each* $(A, G) \in \mathcal{D}(R)$ *the order of* G *is at most the rank of* R *as a* $\mathbb{Z}$*-module, and* $\mathcal{D}(R)$ *contains a maximal element.*

Proof. By definition of $\mathcal{D}(R)$ the elements of G are linearly independent, from which the first claim follows. We have $(R, 1) \in \mathcal{D}(R)$, so $\mathcal{D}(R)$ is not empty. Thus if $(A, G) \in \mathcal{D}(R)$ and $\#G$ is maximal, then (A, G) is a maximal element of $\mathcal{D}(R)$. $\square$

Lemma 5.12. *Let* R *be a connected order and let* (A, G), $(B, H) \in \mathcal{D}(R)$ *be such that* $(B, H) \leq (A, G)$. *Then with* $J = G \cap \mu(B)$ *we have* $G = J \times H$ *and* $B = A[J]$.

Proof. By Lemma 5.11 the group H is finite, and by Proposition 5.7.iii the multiplication map $\mu(B) \times H \to \mu(R)$ is an isomorphism. Since the inverse image of G is $J \times H$, we have $G = J \times H$. Thus $A[J][H] = A[J \times H] = A[G] = B[H]$ and therefore $A[J] = B$. $\square$

Example 5.13. The conclusion to Lemma 5.12 does not hold in general for non-connected orders. Let p be prime and let $G = C_p \times C_p$ with C_p a group of order p. Then G is a

2-dimensional $\mathbb{F}_p$-vector space and thus there are precisely $p + 1$ subgroups $H_0, \dots, H_p$ of G of order p. We have $H_i \cdot H_j = G$ if and only if $i \neq j$. Let $R = \mathbb{Z}[G] \times \mathbb{Z}[G]$ and let $\Delta \colon G \to \mu(R)$ be the map given by $g \mapsto (g, g)$. Now consider the elements

$$(\mathbb{Z} \times \mathbb{Z}, \Delta(G)) \geq (\mathbb{Z}[H_0] \times \mathbb{Z}[H_1], \Delta(H_p))$$

of $\mathcal{D}(R)$. As Proposition 5.7.iii implies

$$\mu(\mathbb{Z}[H_0] \times \mathbb{Z}[H_1]) = \mu(\mathbb{Z}[H_0]) \times \mu(\mathbb{Z}[H_1]) = \{(\pm h_0, \pm h_1) : h_0 \in H_0,\, h_1 \in H_1\},$$

we get $J = \Delta(G) \cap \mu(\mathbb{Z}[H_0] \times \mathbb{Z}[H_1]) = 1$ and $(\mathbb{Z} \times \mathbb{Z})[J] \neq \mathbb{Z}[H_0] \times \mathbb{Z}[H_1]$.

Recall that we say a commutative ring R is *stark* if there do not exist a ring A and a non-trivial group G such that R is isomorphic to the group ring $A[G]$, or equivalently for R non-zero, if $\#\mathcal{D}(R) = 1$.

Lemma 5.14. *Let R be a non-zero commutative ring and let $(A, G) \in \mathcal{D}(R)$. If (A, G) is maximal, then A is stark. When R is a connected order, the converse also holds.*

Proof. If $A = B[J]$ for some $J \subset A^*$, then $(A, G) \leq (B, J \times G) \in \mathcal{D}(R)$. Hence if (A, G) is maximal we have $(A, G) = (B, J \times G)$ and thus $J = 1$, so A is stark. For connected orders, the converse follows from Lemma 5.12. $\quad\square$

Note that from Theorem 1.1 it follows that maximality of $(A, G) \in \mathcal{D}(R)$ for a non-zero reduced order R is equivalent to A being stark even when R is not connected. However, we have not proved this yet.

6. The degree map

In this section we extract from a connected reduced order R a morphism d of abelian groups. We will describe $\mathcal{D}(R)$ in terms of d using the theory in Section 4 and then prove Theorem 1.3.

Lemma 6.1. *Let R be a connected reduced order and let $(\Gamma(R), (R_\gamma)_\gamma)$ be its universal grading (see Definition 5.3). Then there exists a morphism of finite abelian groups $d \colon \mu(R) \to \Gamma(R)$ that sends $\zeta \in \mu(R)$ to the unique $\gamma \in \Gamma(R)$ such that $\zeta \in R_\gamma$.*

Proof. The group $\Gamma(R)$ is finite by Theorem 5.5, and $\mu(R)$ is finite by Lemma 3.3.ii in [7]. By Theorem 5.6, if $\zeta \in \mu(R)$, then there exists a $\gamma \in \Gamma(R)$ such that $\zeta \in R_\gamma$. The element γ is unique, since $R_\gamma \cap R_\delta = 0$ for all $\gamma \neq \delta$. That d is a homomorphism follows from the definitions. $\quad\square$

Definition 6.2. For a connected reduced order R we call the map $d = d_R \colon \mu(R) \to \Gamma(R)$ from Lemma 6.1 the *degree map* of R.

The above definition depends on the choice of universal grading. However, the universal grading of R is uniquely unique. Moreover, the proof of Theorem 1.3 of [9], which states that a reduced order has a universal grading, exhibited an explicit canonical choice of universal grading. Thus we can confidently refer to *the* degree map of a connected reduced order. We now describe the degree map $d_{A[G]}$ of $A[G]$.

Proposition 6.3. *Let A be a connected reduced order and let G be a finite abelian group. Let $(\Gamma(A), (A_\gamma)_\gamma)$ and $(\Gamma(A[G]), (R_\gamma)_\gamma)$ be the universal grading of A and $A[G]$, respectively. Then*

(i) *we have $\Gamma(A[G]) = \Gamma(A) \times G$, and $R_{(\gamma,g)} = A_\gamma \cdot g$ for all $\gamma \in \Gamma(A)$ and $g \in G$;*

(ii) *if we identify $\mu(A[G])$ with $\mu(A) \times G$ as in Proposition 5.7.iii, then the degree map*

$$d_{A[G]} \colon \mu(A) \times G \to \Gamma(A) \times G$$

equals $d_A \times \mathrm{id}_G$;

(iii) *we have $\Gamma(A) = \langle \gamma \in \Gamma(A[G]) : R_\gamma \cap A \neq 0 \rangle$.*

Proof. Let $\mathcal{A} = (\Gamma(A), (A_\gamma)_\gamma)$ and $\mathcal{R} = (\Gamma(A[G]), (R_\gamma)_\gamma)$ be the universal gradings of A and $A[G]$ respectively and define $\mathcal{A}[G] = (\Gamma(A) \times G, (A_\gamma \cdot g)_{(\gamma,g)})$. By universality there exists a unique morphism of gradings $\varphi \colon \mathcal{R} \to \mathcal{A}[G]$, which by Definition 5.1 is a group homomorphism $\Gamma(A[G]) \to \Gamma(A) \times G$, and we will show that it is an isomorphism. Let $\pi \colon \Gamma(A) \times G \to G$ be the projection and $\Delta = \ker(\pi\varphi)$. For $g \in G$ we have $g \in R_{d_{A[G]}(g)}$ and $g \in A_1 \cdot g$, so $\pi\varphi d_{A[G]}$ is the identity on G. It follows that $\Gamma(A[G]) = \Delta \times G$. Then $\mathcal{R}_A = (\Delta, (R_\delta)_\delta)$ is a grading of A, and φ restricts to a morphism of gradings $\varphi' \colon \mathcal{R}_A \to \mathcal{A}$ with $\varphi = \varphi' \times \mathrm{id}_G$. With $\Delta' = \langle \delta \in \Delta : R_\delta \neq 0 \rangle$ we have

$$\bigoplus_{(\delta,g)\in\Delta'\times G} R_\delta \cdot g = A[G],$$

so by Proposition 5.8.v we obtain $\Delta' \times G = \Gamma(A[G]) = \Delta \times G$. Hence $\Delta' = \Delta$, so $\mathcal{R}_A$ is universal by Proposition 5.8.iv. It follows that φ' and hence φ is an isomorphism, proving (i). Now (ii) and (iii) follow by inspection. $\square$

Proposition 6.3.ii expresses the degree map of $A[G]$ in terms of G and the degree map of A, but we will mainly use it in the opposite direction. Specifically, for a connected reduced order R, an element $(A, G) \in \mathcal{D}(R)$ corresponds to a certain decomposition $(d_A, \mathrm{id}_G) \in \mathrm{Dec}_\mathcal{I}(d)$ of the degree map d of R, as defined in Definition 2.10 and Definition 3.4. In Theorem 6.9 we will show it is in fact a bijective correspondence. This together with Proposition 4.8 will prove Theorem 1.3.

Remark 6.4. Let R be a connected reduced order with universal grading $(\Gamma, (R_\gamma)_\gamma)$ and degree map $d \colon \mu \to \Gamma$. Note that the group $\mathrm{Aut}(R)$ acts on the category of gradings of

R. Under this action, $\sigma \in \mathrm{Aut}(R)$ sends $(\Gamma, (R_\gamma)_\gamma)$ to $(\Gamma, (\sigma(R_\gamma))_\gamma)$, which is again a universal grading of R. Thus by universality, σ induces a unique isomorphism $\Gamma \xrightarrow{\sim} \Gamma$. It follows that $\mathrm{Aut}(R)$ acts on Γ. Clearly $\mathrm{Aut}(R)$ acts on μ, and it is easy to see the following diagram commutes

$$
\begin{array}{ccc}
\mu & \xrightarrow{\;d\;} & \Gamma \\
\sigma \downarrow & & \downarrow \sigma \\
\mu & \xrightarrow{\;d\;} & \Gamma,
\end{array}
$$

i.e., we obtain an action $\mathrm{Aut}(R) \to \mathrm{Aut}(d)$ of $\mathrm{Aut}(R)$ on d.

For a degree map $d \colon \mu \to \Gamma$ we define $U^*(d)$ as in Definition 4.1.

Lemma 6.5. *Let R be a connected reduced order with universal grading $(\Gamma, (R_\gamma)_{\gamma \in \Gamma})$ and corresponding degree map $d \colon \mu \to \Gamma$. Let $\varphi \colon U^*(d) \to \mathrm{Aut}(d)$ be as in Lemma 4.2 and $\chi \colon \mathrm{Aut}(R) \to \mathrm{Aut}(d)$ as in Remark 6.4. We then have a commutative diagram*

$$
\begin{array}{ccc}
& U^*(d) & \\
{\scriptstyle \psi} \swarrow & & \searrow {\scriptstyle \varphi} \\
\mathrm{Aut}(R) & \xrightarrow{\quad \chi \quad} & \mathrm{Aut}(d)
\end{array}
$$

where ψ is a morphism given by $1 + f \mapsto (x \in R_\gamma \mapsto f(\gamma) \cdot x)$.

Proof. Let $1 + f, 1 + g \in U^*$ and recall that their product equals $(1 + f) \star (1 + g) = 1 + f + g + fdg$ in U^*. It is easy to see that $\psi(1+f)$ is an endomorphism of R. For $\gamma \in \Gamma$ we have

$$
x \in R_\gamma \xmapsto{\;\psi(1+g)\;} g(\gamma) \cdot x \in R_{dg(\gamma)} \cdot R_\gamma \subset R_{dg(\gamma) \cdot \gamma}
$$

$$
\xmapsto{\;\psi(1+f)\;} f(dg(\gamma) \cdot \gamma) \cdot g(\gamma) \cdot x = f(\gamma)g(\gamma)fdg(\gamma) \cdot x,
$$

so indeed $\psi(1 + f) \circ \psi(1 + g) = \psi((1 + f) \star (1 + g))$. It follows that $\psi(1 + f) \in \mathrm{Aut}(R)$ and that ψ is a morphism.

Let $1 + f \in U^*$ and write $F = \psi(1 + f)$. For $\zeta \in \mu$ we have $F(\zeta) = f(d\zeta)\zeta$, so $F|_{\mu(R)} = \mathrm{id}_\mu + fd$. For $\gamma \in \Gamma$ and $x \in R_\gamma$ non-zero we have $F(x) = f(\gamma) \cdot x$, so the induced action on Γ sends γ to $df(\gamma)\gamma$. Hence $1 + f$ gets sent to $\mathrm{id}_\Gamma + df$, since $\{\gamma \in \Gamma : R_\gamma \neq 0\}$ is a generating set of Γ by Proposition 5.8.v. We conclude that $\chi(\psi(1 + f)) = (\mathrm{id}_\mu + fd, \mathrm{id}_\Gamma + df) = \varphi(1 + f)$, as was to be shown. $\quad\square$

Example 6.6. The map $\psi \colon U^* \to \mathrm{Aut}(R)$ need not be injective, even when R is stark. Consider the subring $R = \mathbb{Z} \cdot (1, 1) + 2S$ of $S = \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}]$ where $\mathrm{i}^2 = -1$, which is clearly connected, reduced, and has $\mu(R) = \{\pm 1\} \times \{\pm 1\}$. Let $\Gamma = \mu(R)$ and write

$$R_{1,1} = R \cap (\mathbb{Q} \times \mathbb{Q}) = \mathbb{Z} \cdot (1,1) + \mathbb{Z} \cdot (1,-1),$$

$$R_{1,-1} = 2\mathrm{i} \cdot (\mathbb{Z} \times \{0\}), \quad R_{-1,1} = 2\mathrm{i} \cdot (\{0\} \times \mathbb{Z}), \quad R_{-1,-1} = 0.$$

Then $(\Gamma, (R_\gamma)_\gamma)$ is the universal grading of R. Consider the identity $\mathrm{id}\colon \Gamma \to \mu$. Note that $2\mathrm{id} = 0$ and $d = 0$, hence $(1 + \mathrm{id})^2 = 1$ in Q and so $1 + \mathrm{id} \in U^*$. Moreover, $\psi(1 + \mathrm{id})$ is the identity of R, so ψ is not injective. To see R is stark, we can apply Lemma 7.1.vi below since $d = 0$.

For a degree map $d\colon \mu \to \Gamma$ we write $\mathrm{Id}_0(d)$ for the partially ordered set $\{f \in \mathrm{Hom}(\Gamma, \mu) : fdf = f\}$ corresponding to d, as defined in Definition 4.4.

Theorem 6.7. *Let R be a connected reduced order with universal grading $(\Gamma, (R_\gamma)_\gamma)$ and corresponding degree map $d\colon \mu \to \Gamma$. The map $\mathrm{Id}_0(d) \to \mathcal{D}(R)$ given by $f \mapsto (\bigoplus_{\gamma \in \ker(f)} R_\gamma, \mathrm{im}(f))$ is a well-defined isomorphism of partially ordered sets and respects the action of $\mathrm{Aut}(R)$ of Remark 6.4. Its inverse is the map given by $(A, G) \mapsto 0_{\Gamma(A) \to \mu(A)} \oplus d_{G \to d(G)}^{-1}$.*

Proof. Write Φ for the map $\mathrm{Id}_0(d) \to \mathcal{D}(R)$, which we first verify is well-defined. Suppose $f \in \mathrm{Id}_0(d)$. As $\ker(f)$ is a subgroup of Γ we have that $B = \bigoplus_{\gamma \in \ker(f)} R_\gamma$ is a subring of R. Furthermore, from $fdf = f$ it follows that the restriction of d to $\mathrm{im}(f) \to \mathrm{im}(df)$ is an isomorphism, with the restriction of f to $\mathrm{im}(df) \to \mathrm{im}(f)$ as inverse, and $\Gamma = \ker(f) \oplus \mathrm{im}(df)$. Thus

$$R = \bigoplus_{\gamma \in \Gamma} R_\gamma = \bigoplus_{\zeta \in \mathrm{im}(f)} \left(\bigoplus_{\gamma \in \ker(f) d(\zeta)} R_\gamma \right) = \bigoplus_{\zeta \in \mathrm{im}(f)} B\zeta = B[\mathrm{im}(f)].$$

Hence $\Phi(f) \in \mathcal{D}(R)$ and Φ is well-defined.

We next construct an inverse Ψ of Φ. Suppose $(A, G) \in \mathcal{D}(R)$. By Proposition 6.3 we may factor $\Gamma(R)$ and $\mu(R)$ such that d is given by $d\colon \mu(A) \times G \to \Gamma(A) \times d(G)$, where

$$\Gamma(A) = \langle \gamma \in \Gamma(R) : R_\gamma \cap A \neq 0 \rangle,$$

and the restriction d_1 of d to $G \to d(G)$ is an isomorphism. Now define $f\colon \Gamma(R) \to \mu(R)$ as the product of $0\colon \Gamma(A) \to \mu(A)$ and d_1^{-1}. Clearly $fdf = f$, so Ψ is well-defined.

For $(A, G) \in \mathcal{D}(R)$ we have $\ker(\Psi(A,G)) = \Gamma(A)$ and $\mathrm{im}(\Psi(A,G)) = G$, so indeed $\Phi \circ \Psi = \mathrm{id}$. Conversely, let $f \in \mathrm{Id}_0(d)$ and $f' = \Psi(\Phi(f))$. Restricted to $\mathrm{im}(df) \to \mathrm{im}(f)$, both f and f' equal the inverse of a restriction of d, and are 0 on a subgroup complementary to $\mathrm{im}(df)$. By Proposition 6.3.iii we have

$$\ker(f') = \Big\langle \gamma' \in \Gamma(R) : R_{\gamma'} \cap \bigoplus_{\gamma \in \ker(f)} R_\gamma \neq 0 \Big\rangle = \langle \gamma \in \ker(f) : R_\gamma \neq 0 \rangle \subset \ker(f),$$

so equality must hold and $f = f'$. Thus $\Psi \circ \Phi = \mathrm{id}$, and Φ and Ψ are bijections.

It follows easily from the definitions that Φ and Ψ respect the partial order and that the action of $\mathrm{Aut}(R)$ commutes with Φ. $\quad\square$

Remark 6.8. Recall that $U^*(d)$ was defined in Definition 4.1, and that it acts on R and hence on $\mathcal{D}(R)$ by Lemma 6.5. Moreover, $U^*(d)$ acts on d and hence on

$$\mathrm{Dec}_{\mathcal{I}}(d) = \{(d_0, d_1) : d_0 \oplus d_1 = d \text{ and } d_1 \text{ is an isomorphism}\}$$

as in Remark 3.5.iv. For $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ we will write μ_i and Γ_i for the finite abelian groups such that $d_i \colon \mu_i \to \Gamma_i$. Note that if $d_0 \oplus d_1 = d$, then $\mu_0 \oplus \mu_1 = \mu$ and $\Gamma_0 \oplus \Gamma_1 = \Gamma$.

Theorem 6.9. *Let R be a connected reduced order with degree map d and universal grading $(\Gamma, (R_\gamma)_\gamma)$. We have an isomorphism of partially ordered sets $\mathrm{Dec}_{\mathcal{I}}(d) \xrightarrow{\sim} \mathcal{D}(R)$ given by*

$$\big(d_0 \colon \mu_0 \to \Gamma_0, \, d_1 \colon \mu_1 \to \Gamma_1\big) \mapsto \Big(\bigoplus_{\gamma \in \Gamma_0} R_\gamma, \mu_1 \Big),$$

$$\big(d|_{\mu(A) \to \Gamma(A)}, \, d|_{G \to d(G)}\big) \leftarrow\!\shortmid \big(A, G\big),$$

that respects the action of $U^*(d)$, where $\Gamma(A) = \langle \gamma \in \Gamma : 0 \neq R_\gamma \subset A \rangle$.

Before we prove Theorem 6.9, we remark that the notation $\Gamma(A)$ used in the theorem was already reserved for the group of the universal grading of A. However, by Proposition 6.3.iii there is no ambiguity, as they are uniquely isomorphic. In fact, the map $d|_{\mu(A) \to \Gamma(A)}$ is the degree map of A.

Proof. Theorem 6.7, Proposition 4.6, and Corollary 3.7 give explicit isomorphisms of partially ordered sets $\mathcal{D}(R) \to \mathrm{Id}_0(d) \to \mathrm{Prj}(d) \to \mathrm{Dec}_{\mathcal{I}}(d)$, from which one readily reads off that their composition and its inverse are as given in the theorem. From Lemma 6.5 it follows that the isomorphisms respect the action of $U^*(d)$. $\quad\square$

Theorem 6.10. *Let R be a connected reduced order with degree map d, and suppose $(A, G), (B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then $A \cong B$ as rings, $G \cong H$ as groups, and (A, G), (A, H), (B, G) and (B, H) are all in the same $U^*(d)$-orbit of $\mathcal{D}(R)$.*

Proof. Let $\Phi \colon \mathrm{Dec}_{\mathcal{I}}(d) \to \mathcal{D}(R)$ be the isomorphism of Theorem 6.9. Suppose $(A, G), (B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then (A, G) and (B, H) are maximal elements of $\mathcal{D}(R)$ by Lemma 5.14, and thus $\Phi(A, G) = (d_0, d_1)$ and $\Phi(B, H) = (e_0, e_1)$ are maximal in $\mathrm{Dec}_{\mathcal{I}}(d)$. Then by Proposition 2.11.v and Proposition 4.8 all of (d_0, d_1), (d_0, e_1), (e_0, d_1), and (e_0, e_1) are maximal and in the same U^*-orbit. Since $\Phi(d_0, e_1) = (A, H)$ and $\Phi(e_0, d_1) = (B, G)$, and Φ respects the action of U^*, the last assertion of the theorem follows. As a consequence, (A, G) and (B, H) are in the same orbit of $\mathrm{Aut}(R)$, so $A \cong B$ as rings and $G \cong H$ as groups. $\quad\square$

Theorem 1.3 is an immediate consequence of Theorem 6.10. Note that in the connected case Theorem 1.2 also follows from Theorem 6.10. In Section 8 we shall see that the same applies for Theorem 1.1.

Example 6.11. Let $\langle \sigma \rangle$ be a group of order 2 and let $R = \mathbb{Z}[\mathrm{i}][\langle \sigma \rangle]$, where $\mathrm{i}^2 = -1$. We will compute $\mathcal{D}(R)$. By Proposition 5.7.i,ii the ring R is both reduced and connected. With $\Gamma = (\mathbb{Z}/2\mathbb{Z})^2$, consider the grading $(\Gamma, (R_{a,b})_{(a,b)})$ of R with $R_{a,b} = \mathbb{Z}\mathrm{i}^a \sigma^b$, where although i^a is not well-defined, $\mathbb{Z}\mathrm{i}^a$ is. Since a universal grading exists, and all $R_{a,b}$ are of rank 1 over $\mathbb{Z}$, this must be the universal grading. Let $d\colon \mu \to \Gamma$ be the degree map. It follows from Proposition 5.7.iii that $\mu = \langle \mathrm{i}, \sigma \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We will first compute $\mathrm{Dec}_{\mathcal{I}}(d)$.

Suppose we have $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ with $d_i\colon \mu_i \to \Gamma_i$ as in Remark 6.8. If $\mu_1 = 1$, then $d_0 = d$, and (d_0, d_1) corresponds via Theorem 6.9 to the trivial element $(R, 1)$ of $\mathcal{D}(R)$. Now suppose $\mu_1 \neq 1$. Since d_1 is an isomorphism, the groups μ_1 and Γ_1 are isomorphic, so μ_1 is isomorphic to a direct factor of μ and of Γ. Since $\mathbb{Z}/2\mathbb{Z}$ is the greatest common divisor of μ and Γ as $\mathbb{Z}$-modules (in the sense of Remark 2.5), we have that μ_1 is a direct factor of μ isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It follows that $\mu_1 = \langle (-1)^b \sigma \rangle$ for some $b \in \mathbb{Z}/2\mathbb{Z}$, and the corresponding group Γ_1 equals $\langle (0,1) \rangle$ in both cases. On the other hand $\mu_0 = \langle \mathrm{i}\sigma^a \rangle$ for some $a \in (\mathbb{Z}/2\mathbb{Z})$ since it must be a cyclic group of order 4, and $\Gamma_0 = \langle (1,a) \rangle$. Upon inspection, all pairs (a, b) do indeed give a decomposition $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$. The rings corresponding to the possible d_0 are $\mathbb{Z}[\mathrm{i}\sigma^a]$, and the groups corresponding to d_1 are $\langle (-1)^b \sigma \rangle$. This gives

$$\mathcal{D}(R) = \{(R, 1)\} \cup \{(\mathbb{Z}[\mathrm{i}\sigma^a], \langle (-1)^b \sigma \rangle) : a, b \in \mathbb{Z}/2\mathbb{Z}\}.$$

Interesting to note is that, although $(\mathbb{Z}[\mathrm{i}\sigma], \langle \sigma \rangle)$ differs from $(\mathbb{Z}[\mathrm{i}\sigma], \langle -\sigma \rangle)$, the corresponding gradings are isomorphic, since $\mathbb{Z}[\mathrm{i}\sigma] \cdot \sigma = \mathbb{Z}[\mathrm{i}\sigma] \cdot (-\sigma)$.

Example 6.12. The conclusion to Theorem 1.3 does not hold in general for non-connected reduced orders. Let C be a non-trivial finite abelian group and consider $R = \mathbb{Z}[C \times C] \times \mathbb{Z}[C]$. Let

$$A = \mathbb{Z}[C \times 1] \times \mathbb{Z}, \qquad G = \{((1, \gamma), \gamma) : \gamma \in C\},$$
$$B = \mathbb{Z}[1 \times C] \times \mathbb{Z}, \qquad H = \{((\gamma, 1), \gamma) : \gamma \in C\}.$$

Then A and B are stark, and $A[G] = R = B[H]$. However, the natural map $A[H] \to R$ has image $\mathbb{Z}[C \times 1] \times \mathbb{Z}[C] \neq R$.

7. Automorphisms of group rings

In this section we will describe $\mathrm{Aut}(A[G])$, for a stark connected reduced order A with degree map d and a finite abelian group G, in terms of $U^*(d)$, G, and $\mathrm{Aut}(A)$.

For a ring R, write $\mathrm{Jac}(R) = \{x \in R : 1 + RxR \subset R^*\}$ for the *Jacobson radical* of R. Recall the definitions of $\mathrm{Id}_0(d)$ from Definition 4.4 and $\Gamma(A)$ from Definition 5.3. In this section we write $\mathrm{Id}_0(A)$ for $\mathrm{Id}_0(d)$ and similarly for Q, U, and U^* as defined in Definition 4.1. In our context $U^*(A)$ is equal to $U(A)$ due to the following.

Lemma 7.1. *Let A be a connected reduced order with degree map $d\colon \mu \to \Gamma$. Then the following are equivalent:* (i) *A is stark;* (ii) *$\mathrm{Id}_0(A) = \{0\}$;* (iii) *the ideal $\mathrm{Hom}(\Gamma, \mu) \subset Q(A)$ consists of only nilpotent elements;* (iv) *$\mathrm{Hom}(\Gamma, \mu) = \mathrm{Jac}(Q(A))$;* (v) *$U^*(A) = U(A)$;* (vi) *for all abelian groups Ω and morphisms $f\colon \Omega \to \mu$ and $g\colon \Gamma \to \Omega$, the element $gdf \in \mathrm{End}(\Omega)$ is nilpotent.*

Proof. We will write $Q = Q(A)$ and similarly for U and U^*. (i $\Leftrightarrow$ ii) This follows from the bijection of Theorem 6.7. (ii $\Rightarrow$ iii) Let $f \in \mathrm{Hom}(\Gamma, \mu)$. Since the semigroup $\mathrm{Hom}(\Gamma, \mu)$ with the multiplication from Q is finite by Lemma 6.1, some power of f is idempotent and thus zero. (iii $\Rightarrow$ iv) It follows that $1 + \mathrm{Hom}(\Gamma, \mu) \subset Q^*$ and thus $\mathrm{Hom}(\Gamma, \mu) \subset \mathrm{Jac}(Q)$. The surjection $Q \twoheadrightarrow \mathbb{Z}$ must map $\mathrm{Jac}(Q)$ to $\mathrm{Jac}(\mathbb{Z}) = \{0\}$, so $\mathrm{Jac}(Q) \subset \mathrm{Hom}(\Gamma, \mu)$. (iv $\Rightarrow$ v) We have $U^* \subset U = 1 + \mathrm{Jac}(Q) \subset U^*$. (v $\Rightarrow$ ii) It follows that 1 is the only idempotent of U. The involution $x \mapsto 1 - x$ on Q shows that $\mathrm{Hom}(\Gamma, \mu)$ and $1 - \mathrm{Hom}(\Gamma, \mu) = U$ contain equally many idempotents, hence $\mathrm{Id}_0(A) = \{0\}$. (vi $\Rightarrow$ iii) It suffices to show that $df \in \mathrm{End}(\Gamma)$ is nilpotent for all $f \in \mathrm{Hom}(\Gamma, \mu)$, so take $\Omega = \Gamma$ and $g = \mathrm{id}_\Gamma$. (iii $\Rightarrow$ vi) As $(gdf)^{n+1} = g(dfg)^n df$ it holds that gdf is nilpotent if dfg is nilpotent. The latter holds because $fg \in \mathrm{Hom}(\Gamma, \mu) \subset Q$ is nilpotent. $\square$

A category $\mathcal{C}$ is *small* if the class of objects of $\mathcal{C}$ is a set and if for any two objects A and B of $\mathcal{C}$ the class $\mathrm{Hom}(A, B)$ is a set. A category $\mathcal{C}$ is *preadditive* (see Section 1.2 in [2]) if for any two objects A and B of $\mathcal{C}$ the class $\mathrm{Hom}(A, B)$ is an abelian group such that composition of morphisms is bilinear, i.e., for all objects A, B, and C and morphisms $f, f' : A \to B$ and $g, g' : B \to C$ we have

$$g \circ (f + f') = (g \circ f) + (g \circ f') \text{ and } (g + g') \circ f = (g \circ f) + (g' \circ f).$$

Lemma 7.2. *Let $\mathcal{C}$ be a preadditive small category with precisely two objects $\mathbf{0}$ and $\mathbf{1}$. Then:*

(i) *With $M_{ij} = \mathrm{Hom}(j, i)$ for $i, j \in \{\mathbf{0}, \mathbf{1}\}$ both $M_{\mathbf{00}}$ and $M_{\mathbf{11}}$ are rings and $M_{\mathbf{01}}$ and $M_{\mathbf{10}}$ are a $M_{\mathbf{00}}$-$M_{\mathbf{11}}$-bimodule and $M_{\mathbf{11}}$-$M_{\mathbf{00}}$-bimodule respectively.*

(ii) *The product of groups*

$$\mathrm{M}(\mathcal{C}) = \prod_{i,j \in \{\mathbf{0}, \mathbf{1}\}} M_{ij} = \begin{pmatrix} M_{\mathbf{00}} & M_{\mathbf{01}} \\ M_{\mathbf{10}} & M_{\mathbf{11}} \end{pmatrix}$$

is a ring with respect to the addition and multiplication implied by the matrix notation.

(iii) *If $M_{01} \cdot M_{10} = \mathrm{im}(M_{01} \otimes M_{10} \to M_{00}) \subset \mathrm{Jac}(M_{00})$, then $M_{10} \cdot M_{01} \subset \mathrm{Jac}(M_{11})$,*

$$\mathrm{Jac}(\mathrm{M}(\mathcal{C})) = \begin{pmatrix} \mathrm{Jac}(M_{00}) & M_{01} \\ M_{10} & \mathrm{Jac}(M_{11}) \end{pmatrix}, \quad and \quad \mathrm{M}(\mathcal{C})^* = \begin{pmatrix} M_{00}^* & M_{01} \\ M_{10} & M_{11}^* \end{pmatrix}.$$

Proof. That the M_{ij} are groups, and that the addition is compatible with the composition of morphisms, follows from the fact that $\mathcal{C}$ is preadditive. It is then easy to verify that the M_{ij} are rings and modules as claimed, and that $\mathrm{M}(\mathcal{C})$ is a ring, giving (i) and (ii).

Now suppose $M_{01} \cdot M_{10} \subset \mathrm{Jac}(M_{00})$. We will show that for all $m \in M_{01}$ and $n \in M_{10}$ we have $nm \in \mathrm{Jac}(M_{11})$. Let $s \in M_{11}$. Then $(ms)n \in M_{01} \cdot M_{10} \subset \mathrm{Jac}(M_{00})$, so $1 + msn$ has an inverse $r \in M_{00}$. Then

$$(1 - snrm)(1 + snm) = 1 - sn(r(1 + msn) - 1)m = 1 - sn(1 - 1)m = 1.$$

Hence $1 + snm$ has a left inverse $1 - snrm$, and similarly $1 - snrm$ is a right inverse of $1 + snm$. Thus $1 + snm \in M_{11}^*$ and $nm \in \mathrm{Jac}(M_{11})$. We conclude that $M_{10} \cdot M_{01} \subset \mathrm{Jac}(M_{11})$.

Consider $T = \begin{pmatrix} \mathrm{Jac}(M_{00}) & M_{01} \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ M_{10} & \mathrm{Jac}(M_{11}) \end{pmatrix}$ and write $J = T + B$. We will first show that $T \subset \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. For $x = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in T$ it suffices to show for all $y = \begin{pmatrix} r & m \\ n & s \end{pmatrix} \in \mathrm{M}(\mathcal{C})$ that $1 + xy \in \mathrm{M}(\mathcal{C})^*$. As $1 + xy = \begin{pmatrix} 1 + ar + bn & ma + bs \\ 0 & 1 \end{pmatrix}$ is upper diagonal, it is invertible if its diagonal elements are. The element $1 + ar + bn$ is invertible because $ar + bn \in \mathrm{Jac}(M_{00})$. So $T \subset \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. Analogously $B \subset \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. Thus we have a two-sided ideal $J \subset \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. To see equality, note that the ring

$$\mathrm{M}(\mathcal{C})/J \cong (M_{00}/\mathrm{Jac}(M_{00})) \times (M_{11}/\mathrm{Jac}(M_{11}))$$

has a trivial Jacobson radical.

An element of $\mathrm{M}(\mathcal{C})$ is a unit if and only if it maps to a unit in $\mathrm{M}(\mathcal{C})/\mathrm{Jac}(\mathrm{M}(\mathcal{C}))$, hence if and only if its diagonal elements are units, proving the final statement. □

Naturally, the construction $\mathrm{M}(\mathcal{C})$ can be generalized to categories $\mathcal{C}$ with any finite number of objects. We call $\mathrm{M}(\mathcal{C})$ the *matrix ring* of $\mathcal{C}$.

Remark 7.3. Given four abelian groups M_{ij} with $i, j \in \{0, 1\}$ together with compatible (i.e., associative) multiplications $M_{ij} \otimes M_{jk} \to M_{ik}$ for all $i, j, k \in \{0, 1\}$ with appropriate unit elements, we can construct the preadditive category $\mathcal{C}$ with two objects 0 and 1, with $\mathrm{Hom}(j, i) = M_{ij}$, and with composition being these multiplications. In particular, if M_{00} and M_{11} are rings, M_{01} is an M_{00}-M_{11}-bimodule, and M_{10} is an M_{11}-M_{00}-bimodule, then it remains only to specify the multiplications $M_{01} \otimes M_{10} \to M_{00}$ and $M_{10} \otimes M_{01} \to M_{11}$.

Let A be a connected reduced order and G a finite abelian group. Recall that $\mu(A)$ and $\Gamma(A)$ are $Q(A)$-modules by Remark 4.3, hence $\mathrm{Hom}(G, \mu(A))$ and $\mathrm{Hom}(\Gamma(A), G)$ are

respectively left and right $Q(A)$-modules. We next describe $U^*(A[G])$ in terms of A and G.

Proposition 7.4. *Let A be a connected reduced order and G a finite abelian group. Then:*

(i) *We have a matrix ring*

$$E = \begin{pmatrix} Q(A) & \mathrm{Hom}(G, \mu(A)) \\ \mathrm{Hom}(\Gamma(A), G) & \mathrm{End}(G) \end{pmatrix}$$

where $\mathrm{Hom}(G, \mu(A)) \otimes \mathrm{Hom}(\Gamma(A), G) \to \mathrm{Hom}(\Gamma(A), \mu(A)) \subset Q(A)$ is the composition map and $\mathrm{Hom}(\Gamma(A), G) \otimes \mathrm{Hom}(G, \mu(A)) \to \mathrm{End}(G)$ is given by $g \otimes f \mapsto gdf$.

(ii) *There is a natural ring isomorphism $E \xrightarrow{\sim} Q(A[G])$ that respects the action of $\mathrm{Aut}(A)$.*

(iii) *If A is stark, then the map in (ii) restricts to an isomorphism*

$$\begin{pmatrix} U^*(A) & \mathrm{Hom}(G, \mu(A)) \\ \mathrm{Hom}(\Gamma(A), G) & \mathrm{Aut}(G) \end{pmatrix} \xrightarrow{\sim} U^*(A[G]).$$

Proof. For (i), apply Remark 7.3 and Lemma 7.2.ii. Since all multiplications are defined in terms of compositions of morphisms, the associativity conditions are trivially satisfied.

Write $\Gamma = \Gamma(A)$ and $\mu = \mu(A)$. For (ii), we have by Proposition 6.3.ii that

$$Q(A[G]) \;=\; \mathbb{Z} \oplus \mathrm{Hom}(\Gamma \times G, \mu \times G) \;\cong\; \mathbb{Z} \oplus \begin{pmatrix} \mathrm{Hom}(\Gamma, \mu) & \mathrm{Hom}(G, \mu) \\ \mathrm{Hom}(\Gamma, G) & \mathrm{End}(G) \end{pmatrix},$$

where the isomorphism is one of abelian groups. Then the map $Q(A[G]) \to E$ with respect to the latter representation given by

$$\left(n, \begin{pmatrix} p & q \\ r & s \end{pmatrix}\right) \mapsto \begin{pmatrix} (n,p) & q \\ r & n+s \end{pmatrix}$$

is an isomorphism of rings that by functoriality respects the action of $\mathrm{Aut}(A)$.

For (iii), suppose A is stark. Then $\mathrm{Hom}(\Gamma, \mu) = \mathrm{Jac}(Q(A))$ by Lemma 7.1. It follows that the ideal $\mathrm{Hom}(G, \mu) \cdot \mathrm{Hom}(\Gamma, G) \subset \mathrm{Hom}(\Gamma, \mu)$ is contained in $\mathrm{Jac}(Q(A))$. Now apply Lemma 7.2.iii. $\square$

In Remark 7.5 and Proposition 7.6 we describe $\mathrm{Aut}(A[G])$ in terms of A and $U^*(A[G])$.

Remark 7.5. Let G be a finite abelian group. Then $-[G]$ and U^* act functorially on isomorphisms of connected reduced orders. Let A be a connected reduced order. From Proposition 6.3.ii we get a natural inclusion

$$\mathrm{Hom}(\Gamma(A), \mu(A)) \to \mathrm{Hom}(\Gamma(A[G]), \mu(A[G])),$$

which extends to an inclusion of rings $Q(A) \to Q(A[G])$. Then we have a commutative diagram

$$\begin{array}{ccccc}
U^*(A) & \xrightarrow{\text{Lemma } 6.5} & \text{Aut}(A) & \xrightarrow{U^*} & \text{Aut}(U^*(A)) \\
\downarrow & & \downarrow{\scriptstyle -[G]} & & \\
U^*(A[G]) & \xrightarrow{\text{Lemma } 6.5} & \text{Aut}(A[G]) & \xrightarrow{U^*} & \text{Aut}(U^*(A[G])),
\end{array}$$

and the composition $U^*(A) \to \text{Aut}(U^*(A))$ is the conjugation map.

Proposition 7.6. *Let A be a stark connected reduced order and G a finite abelian group. Then the maps and actions from Remark 7.5 fit in an exact sequence*

$$0 \to U^*(A) \xrightarrow{\iota} U^*(A[G]) \rtimes \text{Aut}(A) \xrightarrow{\pi} \text{Aut}(A[G]) \to 0,$$

where ι and π are homomorphisms such that $\iota(u) = (u^{-1}, u)$ and π maps each component to $\text{Aut}(A[G])$.

Proof. For all $u, v \in U^*(A)$ we have

$$\iota(u)\iota(v) = (u^{-1}, u)(v^{-1}, v) = (u^{-1}(uv^{-1}u^{-1}), uv) = \iota(uv)$$

by Remark 7.5, so ι is a homomorphism. Moreover, ι is injective because it maps injectively to the first factor. By the same remark π is a homomorphism.

We will now show that π is surjective. Suppose $\sigma \in \text{Aut}(A[G])$. By Theorem 6.10 there exists $1 + f \in U^*(A[G])$ that maps (A, G) to $(\sigma(A), \sigma(G))$, so without loss of generality we may assume $\sigma(A) = A$ and $\sigma(G) = G$. By applying the restriction $\sigma|_A \in \text{Aut}(A)$ we may assume σ is the identity on A. Consider the map $f \colon \Gamma(A) \times G \to \mu(A[G])$ given by $(\delta, g) \mapsto \sigma(g)g^{-1}$ and note that $1 + f \in U(A[G])$ gets mapped to σ. We similarly obtain the inverse of $1 + f$ in $U(A[G])$ from $(\delta, g) \mapsto \sigma^{-1}(g)g^{-1}$, so $1 + f \in U^*(A[G])$. It follows that σ is in the image of π and thus π is surjective.

To show the sequence is exact, it remains to show $\text{im}(\iota) = \ker(\pi)$. It is clear that $\text{im}(\iota) \subset \ker(\pi)$, so suppose $(1 + f, \alpha) \in \ker(\pi)$. As α^{-1} equals the restriction of $1 + f$ by assumption, it suffices to show that $1 + f \in U^*(A)$. For $g \in G$ we have $g = (1 + f)\alpha(g) = f(g)g$, and multiplying by g^{-1} we obtain $1 = f(g)$, i.e., $G \subset \ker(f)$. Moreover $\text{im}(f) \subset \mu(A)$, since multiplication by any unit $(\zeta, g) \in \mu(A) \times G = \mu(A[G])$ not in $\mu(A)$ sends A to $Ag \neq A$. Hence $f \in \text{Hom}(\Gamma(A), \mu(A))$ and $1 + f \in U(A)$. The same holds for the inverse $1 + e \in U^*(A[G])$ of $1 + f$, so $1 + e \in U(A)$ and thus $1 + f \in U^*(A)$. It now follows that $(1 + f, \alpha) = \iota(1 + e)$, so $\ker(\pi) \subset \text{im}(\iota)$, as was to be shown. $\square$

Proposition 7.4 and Proposition 7.6 combined gives us a description of $\text{Aut}(A[G])$ in terms of A and G. We now prove Theorem 1.5 and describe $\text{Aut}(A[G])$ by less canonical means.

Lemma 7.7. *Let A be a stark connected reduced order. Then the group $\mathrm{Hom}(\Gamma(A), \mu(A))$ has a (right) action on the set $\mathrm{Aut}(A)$, which for $\alpha \in \mathrm{Aut}(A)$ and $f \in \mathrm{Hom}(\Gamma(A), \mu(A))$ is given by*

$$(\alpha, f) \mapsto \alpha + f = \big(x \in A_\gamma \mapsto \alpha(x) \cdot f(\gamma)\big).$$

Proof. Let $\alpha \in \mathrm{Aut}(A)$ and $f, g \in \mathrm{Hom}(\Gamma(A), \mu(A))$. Note that

$$\alpha + f = \alpha \circ (1 + \alpha^{-1} f) \in \mathrm{Aut}(A),$$

where $1 + \alpha^{-1} f \in U(A) = U^*(A)$ by Lemma 7.1 and the composition is taken inside $\mathrm{Aut}(A)$ via Lemma 6.5. For $\gamma \in \Gamma(A)$ and $x \in A_\gamma$ we clearly have

$$[(\alpha + f) + g](x) = [\alpha + f](x) \cdot g(\gamma) = \alpha(x) \cdot f(\gamma) \cdot g(\gamma) = [\alpha + (f + g)](x),$$

so the action is well-defined. $\square$

Proof of Theorem 1.5. To check that M is a group it remains to verify that $t_1 d s_2 + \sigma_1 \sigma_2 \in \mathrm{Aut}(G)$. This follows from Lemma 7.1, namely $t_1 d s_2 \in \mathrm{Jac}(\mathrm{End}(G))$. Note that the map

$$\vartheta \colon M \to \mathrm{Aut}(A[G])$$

can be written as the composition of the homomorphism $\varphi \colon M \to U^*(A[G]) \rtimes \mathrm{Aut}(A)$ given by

$$\begin{pmatrix} \alpha & s \\ t & \sigma \end{pmatrix} \mapsto \begin{pmatrix} 1 & s \\ t\alpha^{-1} & \sigma \end{pmatrix} \cdot \alpha$$

where $U^*(A[G])$ is written in terms of the matrix representation of Proposition 7.4.iii, and the homomorphism $\pi \colon U^*(A[G]) \rtimes \mathrm{Aut}(A) \to \mathrm{Aut}(A[G])$ from Proposition 7.6.

The map π is still surjective when restricted to the image of φ. Namely any

$$\begin{pmatrix} u & s \\ t & \sigma \end{pmatrix} \cdot \alpha \in U^*(A[G]) \rtimes \mathrm{Aut}(A)$$

has the same image as $\begin{pmatrix} 1 & s \\ t\beta^{-1} & \sigma \end{pmatrix} \cdot \beta\alpha$, where β is the image of u in $\mathrm{Aut}(A)$. Hence the map ϑ is surjective. By Proposition 7.4.iii and Proposition 7.6, respectively, we have

$$\frac{\#M}{\#U^*(A[G])} = \frac{\#\mathrm{Aut}(A)}{\#U^*(A)} = \frac{\#\mathrm{Aut}(A[G])}{\#U^*(A[G])},$$

so the groups M and $\mathrm{Aut}(A[G])$ have the same (finite) cardinality, so ϑ is bijective.

8. Proofs of Theorems 1.1, 1.2, and 1.6

We will prove Theorems 1.1 and 1.2 by reducing to the connected case, where we can apply Theorem 6.10. Recall the definition of $\mathcal{D}$ from Definition 5.10.

Lemma 8.1. *Let S and T be orders with S non-zero, let $R = S \times T$ with projection map $\pi\colon R \to S$, and let $(A, G) \in \mathcal{D}(R)$. Then we have $(\pi(A), \pi(G)) \in \mathcal{D}(S)$ and the restriction $G \to \pi(G)$ of π is a group isomorphism.*

Proof. We have a natural map $\pi(A)[G] \twoheadrightarrow \pi(A)[\pi(G)] \to S$. Since S equals $\pi(A[G]) = \sum_{g \in G} \pi(A)\pi(g)$, this map is clearly surjective. Suppose $\sum_{g \in G} \pi(a_g)g$ is in its kernel. Writing $e = (1, 0) \in R$ and identifying S with $S \times \{0\}$, we have $\pi(x) = ex$ for all $x \in R$. By Proposition 5.7(ii) we have $e \in A$ and therefore $\sum_{g \in G} ea_g g = 0$ in $A[G]$. We conclude that for all $g \in G$ we have $\pi(a_g) = ea_g = 0$, so the map $\pi(A)[G] \to S$ is an isomorphism. Then the maps $\pi(A)[G] \to \pi(A)[\pi(G)]$ and $\pi(A)[\pi(G)] \to S$ are isomorphisms as well. Since $S \neq 0$, this implies that the map $G \to \pi(G)$ is an isomorphism and that $(\pi(A), \pi(G)) \in \mathcal{D}(S)$. $\quad\square$

Given a group ring structure on a product of orders, Lemma 8.1 constructs on each of the factors a group ring structure, with the same group. The following proposition does the opposite. For the definition of greatest common divisors, see Remark 2.5.

Proposition 8.2. *Let X be a finite non-empty set, let $(R_x)_{x \in X}$ be a collection of connected orders, and let $(A_x, G_x) \in \mathcal{D}(R_x)$ for all $x \in X$. Suppose that for all $x \in X$ we write $G_x = D_x \oplus E_x$ for some subgroups $D_x, E_x \subset G_x$ such that for all $x, y \in X$ we have $D_x \cong D_y$. Put $R = \prod_{x \in X} R_x$ and $A = \prod_{x \in X} A_x[E_x]$, and let $D \subset \prod_{x \in X} D_x$ be a subgroup for which all the projection maps $\pi_x\colon D \to D_x$ are isomorphisms. Then $(A, D) \in \mathcal{D}(R)$. If in addition (A_x, G_x) is maximal in $\mathcal{D}(R_x)$ for all $x \in X$, and D is a greatest common divisor of $\{G_x : x \in X\}$, then (A, D) is maximal in $\mathcal{D}(R)$.*

Proof. Clearly $A \subset R$ and $D \subset \mu(R)$. There is a sequence of ring isomorphisms

$$A[D] \cong \prod_{x \in X} (A_x[E_x][D]) \cong \prod_{x \in X} (A_x[E_x][D_x]) \cong \prod_{x \in X} A_x[G_x] = R,$$

where one obtains the first isomorphism by tensoring $A = \prod_{x \in X} A_x[E_x]$ with $\mathbb{Z}[D]$ over $\mathbb{Z}$ and the second isomorphism is induced by the group isomorphisms π_x. The resulting isomorphism $A[D] \to R$ restricts to the inclusion on both A and D, so $A[D] = R$ and indeed $(A, D) \in \mathcal{D}(R)$.

Now suppose that (A_x, G_x) is maximal in $\mathcal{D}(R_x)$ for all $x \in X$, and that D is a greatest common divisor of $\{G_x : x \in X\}$. Let $(B, H) \in \mathcal{D}(R)$ be such that $(A, D) \leq (B, H)$. For $x \in X$ let B_x and H_x be the projection of B, respectively H, to R_x, so by Lemma 8.1 we have $(B_x, H_x) \in \mathcal{D}(R_x)$ and $H \cong H_x$. Choose $(C_x, I_x) \in \mathcal{D}(R_x)$ to be maximal such that

$(B_x, H_x) \leq (C_x, I_x)$. Since R_x is connected, Lemma 5.12 implies that there exists a finite abelian group F_x such that $I_x \cong H_x \oplus F_x$. Since both (A_x, G_x) and (C_x, I_x) are maximal in $\mathcal{D}(R_x)$, we have $G_x \cong I_x$ by Theorem 6.10. Hence $G_x \cong I_x \cong H_x \oplus F_x \cong H \oplus F_x$. Thus H is a common divisor of all G_x, and H contains D. Since D is a greatest common divisor, we obtain $H = D$. From $A[D] = B[H] = B[D]$ and $A \supset B$ we see $A = B$, so $(A, D) = (B, H)$ and (A, D) is maximal. $\square$

Proof of Theorem 1.1. If $A = 0$ or $B = 0$, then Theorem 1.1 holds trivially. Hence assume A and B are non-zero.

(ii) $\Rightarrow$ (i) Assuming (ii), we have ring isomorphisms

$$A[G] \cong C[I][G] \cong C[I \times G] \cong C[J \times H] \cong C[J][H] \cong B[H].$$

(i) $\Rightarrow$ (ii) First assume $A[G]$ is connected. Let $(C, V) \geq (A, G)$ and $(D, W) \geq (B, H)$ be a maximal element of $\mathcal{D}(A[G])$, respectively $\mathcal{D}(B[H])$. By Lemma 5.14 the orders C and D are stark, so by Theorem 6.10 there exists a ring isomorphism $\sigma \colon B[H] \to A[G]$ that sends (D, W) to (C, V). It follows that $(C, V) \geq (\sigma(B), \sigma(H))$, so applying Lemma 5.12 twice, we find subgroups $I, J \subset V$ such that $I \times G = V = J \times \sigma(H) \cong J \times H$ and $C[I] = A$ and $C[J] = \sigma(B) \cong B$. This concludes the proof of the connected case.

Next consider the general case, where $A[G] = \prod_{x \in X} R_x$ is a non-empty product of connected reduced orders R_x. Without loss of generality we may assume $A[G] = B[H]$. Let $x \in X$. Write A_x and B_x for the image of A, respectively B, of the projection onto R_x. Then $A_x[G] \cong R_x \cong B_x[H]$ by Lemma 8.1. Since R_x is connected and we proved (i) $\Rightarrow$ (ii) in the connected case, there exist a reduced order C_x and finite abelian groups I_x and J_x such that $C_x[I_x] \cong A_x$ and $C_x[J_x] \cong B_x$ and $I_x \times G \cong J_x \times H = P_x$. Replacing C_x by $C_x[D_x]$ for some greatest common divisor D_x of I_x and J_x, we may assume that I_x and J_x are coprime. It follows that P_x is a least common multiple of G and H, as defined in Remark 2.5. In particular, when x ranges over X, the finite abelian groups P_x are pairwise isomorphic, and as a consequence the same holds for the groups I_x. Hence there exists a subgroup $I \subset \prod_{x \in X} I_x$ such that all projections $I \to I_x$ are isomorphisms, so from Proposition 8.2 it follows that $C[I] \cong A$ with $C = \prod_{x \in X} C_x$. Similarly we find a finite abelian group J that is isomorphic to all J_x such that $C[J] \cong B$. Now I and J together satisfy $I \times G \cong J \times H$, as desired. $\square$

Proof of Theorem 1.2. Let $(A, G) \in \mathcal{D}(R)$ be a maximal element (Lemma 5.11). Then A is stark by Lemma 5.14. Suppose B is a stark ring and H is a finite abelian group such that $B[H] \cong R$. By Theorem 1.1 there exist an order C and finite abelian groups I and J such that $A \cong C[I]$ and $B \cong C[J]$ and $I \times G \cong J \times H$. Since both A and B are stark we conclude that $I = J = 1$, so $G \cong H$ and $A \cong C \cong B$. Hence A and G are unique up to ring and group isomorphism, respectively. $\square$

Proof of Theorem 1.6. We use the notation of Theorem 1.6. By Remark 6.4, if $\alpha \in \mathrm{Aut}(A)$ and $\gamma \in \Gamma$ then $\alpha(A_\gamma) = A_{\alpha\gamma}$. It then follows readily from Theorem 1.5 that the

orbit of A under $\mathrm{Aut}(A[G])$ is $\mathcal{A}$ and the orbit of G under $\mathrm{Aut}(A[G])$ is $\mathcal{G}$. Theorem 1.6 now follows from Theorem 1.2. $\quad\square$

9. Algorithms

In this section we will prove Theorem 1.4, the algorithmic counterpart to Theorem 1.2. To state our theorems rigorously, we should specify how our data are encoded. We will continue the conventions used in [3,6–9,19], the results from which are therefore compatible. They can be briefly described as follows. Integers and rationals are encoded straightforwardly. Any finitely generated free module is specified by its rank, its elements are represented by vectors, and morphisms between such modules are represented by matrices. All rings we consider are Noetherian, so each finitely generated module is a cokernel of some morphism of finitely generated free modules, and it is encoded as such. Finally, a ring structure on a finitely generated abelian group is encoded as a collection of multiplication maps, one for every generator. For matrices with integer coefficients we can do multiplication and compute (bases for) kernels and images in polynomial time as described in [6].

Theorem 9.1 (*Theorem 4.1.1 in [3]*). *There exists a polynomial-time algorithm that, given a finite ring R and finite R-modules M_1 and M_2, computes a greatest common divisor D of M_1 and M_2 as defined in Remark 2.5, together with injections $\iota_i\colon D \to M_i$ and a complement $N_i \subset M_i$ such that $N_i \oplus \iota_i D = M_i$.*

Proposition 9.2. *For each of $R = \mathbb{Z}$ and $R = \left(\begin{smallmatrix}\mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$ there exists a polynomial-time algorithm that, given finite R-modules M_1 and M_2, computes a greatest common divisor D of M_1 and M_2, together with injections $\iota_i\colon D \to M_i$ and a complement $N_i \subset M_i$ such that $N_i \oplus \iota_i D = M_i$.*

Proof. By Theorem 2.6.9 in [3] we may compute the exponents of M_1 and M_2, and their least common multiple n, in polynomial time. Note that M_1 and M_2 are R/nR-modules and that replacing R by R/nR does not change the problem. Since R/nR is a finite ring, we can thus reduce to Theorem 9.1. $\quad\square$

Proposition 3.3 allows us to interpret a morphism of finite abelian groups as a finite length $\left(\begin{smallmatrix}\mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module. Although both types of objects are represented differently, one easily deduces from the proof of Proposition 3.3 that we can change representations in polynomial time.

In the following result, $\mathrm{Dec}_\mathcal{I}(d)$ is as defined in Definition 2.10, Remark 3.5.iv, and Definition 3.4.

Proposition 9.3. *There exists a polynomial-time algorithm that, given finite abelian groups A and B and a morphism $d\colon A \to B$, computes a maximal element of $\mathrm{Dec}_\mathcal{I}(d)$.*

Proof. By Proposition 9.2 we may compute in polynomial time a greatest common divisor D of A and B as $\mathbb{Z}$-modules. Similarly we may compute a greatest common divisor E of d and id_D as $\left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix}\right)$-modules. We also obtain submodules d_0 and d_1 of d such that $d_1 \cong E$ and $d = d_0 \oplus d_1$. We claim that (d_0, d_1) is a maximal element of $\mathrm{Dec}_{\mathcal{I}}(d)$. First note that d_1 is a divisor of id_D and thus must be an isomorphism. As $d = d_0 \oplus d_1$ we indeed have that $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$. Let $(e_0, e_1) \geq (d_0, d_1)$ be maximal in $\mathrm{Dec}_{\mathcal{I}}(d)$. Since e_1 is an isomorphism, it is isomorphic to id_F for some finite abelian group F. Since e_1 is a direct summand of d, the group F is a direct summand of both A and B, so F is a divisor of their greatest common divisor D. Thus e_1 is a divisor of id_D. It follows that e_1 is a divisor of $E \cong d_1$, so $(d_0, d_1) = (e_0, e_1)$ and thus (d_0, d_1) is maximal, as was to be shown. $\square$

In the following result, we represent a grading $(\Delta, (R_\delta)_{\delta \in \Delta})$ of an order R by a finitely generated abelian group Δ by specifying only those subgroups R_δ of R that are non-zero. This differs from the representation of gradings used in [19], which restricts to finite Δ and specifies *all* subgroups R_δ; the latter representation can readily be converted to the former in polynomial time, which is all we need.

Proposition 9.4. *There exists a polynomial-time algorithm that, given a reduced order R and a universal grading $(\Gamma, \mathcal{R})$ of R, computes a maximal element of $\mathcal{D}(R)$ as defined in Definition 5.10.*

Proof. First suppose R is connected. By Theorem 1.2 in [7] we may compute $\mu = \mu(R)$ in polynomial time and thus also the group homomorphism $d \colon \mu \to \Gamma$ as defined in Definition 6.2. We may compute a maximal element $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$, with $d_i \colon \mu_i \to \Gamma_i$ as in Remark 6.8, in polynomial time using Proposition 9.3. Under the isomorphisms of partially ordered sets of Theorem 6.9 this d corresponds to a maximal element $(A, G) \in \mathcal{D}(R)$, where $A = \sum_{\gamma \in \Gamma_0} R_\gamma$ and $G = \mu_1$, which we may compute in polynomial time.

Now consider the general case. By Theorem 1.1 in [7] we may compute in polynomial time connected reduced orders $(R_x)_{x \in X}$ for some index set X such that $R \cong \prod_{x \in X} R_x$, together with the projections $\pi_x \colon R \to R_x$. Using Proposition 5.9.i we may construct universal gradings for the R_x in polynomial time. Hence by the special case we may compute a maximal element of $\mathcal{D}(R_x)$ for all $x \in X$ in polynomial time. Finally, we may apply Proposition 8.2 to compute a maximal element of $\mathcal{D}(R)$, observing that the construction in Proposition 8.2 can be carried out in polynomial time using Proposition 9.2. $\square$

Computing a maximal element of $\mathcal{D}(R)$ for a reduced order R is now reduced to finding a universal grading of R.

Theorem 9.5 *(Theorem 1.4 in [19]). There is an algorithm that takes a reduced order R as input and produces a universal grading of R in time $n^{O(m)}$, where n is the length of the input and m is the number of minimal prime ideals of R.*

The above algorithm does not, in general, run in polynomial time; but when we bound m, or equivalently the number 2^m of idempotents of $R \otimes_{\mathbb{Z}} \mathbb{Q}$, by a constant it is guaranteed to finish in polynomial time.

We now consider the case where R is generated as a group by its autopotent elements. We recall that a ring element x is called autopotent if $x^{n+1} = x$ for some $n \in \mathbb{Z}_{>0}$. Write $\alpha(R)$ for the set of autopotents of R.

Proposition 9.6. *Let S and R be rings. Then:*

(i)   *The roots of unity and idempotents of R are autopotent.*
(ii) *The product of any two commuting autopotents of R is autopotent.*
(iii) *We have $\mu(R \times S) = \mu(R) \times \mu(S)$ and $\alpha(R \times S) = \alpha(R) \times \alpha(S)$.*
(iv) *Let $x \in R$. Then $x \in \alpha(R)$ if and only if there exist an idempotent $e \in R$ and a $\zeta \in \mu(R)$ such that $x = e\zeta = \zeta e$.*
(v)   *If R is commutative, then R is generated as a ring by $\alpha(R)$ if and only if its additive group is generated by $\alpha(R)$.*
(vi) *As groups, $R \times S$ is generated by autopotents if and only if each of R and S is generated by autopotents.*
(vii) *If R is connected, then $\alpha(R) = \mu(R) \cup \{0\}$.*

Proof. Statements (i), (ii) and (iii) are trivial. The 'if'-part of (iv) follows from (i) and (ii). 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 $x \in eR$ is an n-th root of unity, so is $\zeta = (x, 1) \in R$. Then $x = e\zeta = \zeta e$.

By (ii) the set of autopotents is closed under multiplication, and this gives (v). Part (vi) follows from (iii) combined with the fact that $0 \in \alpha(R)$ and $0 \in \alpha(S)$. Part (vii) follows from (iv). $\square$

The 'if'-part of (vi) is wrong when we replace 'autopotents' by 'roots of unity': As a group the connected ring $\mathbb{Z}$ is generated by its roots of unity $\{\pm 1\}$, but for $\mathbb{Z} \times \mathbb{Z}$ the group generated by the roots of unity does not contain $(1, 0)$. This is the main reason we introduce autopotents.

Lemma 9.7. *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. $\square$

Definition 9.8 *(Example 3.4 in [9])*. For an order R we define a bilinear map

$$\langle x, y \rangle_R = \langle x, y \rangle = \sum_{\sigma \colon R \to \mathbb{C}} \sigma(x) \cdot \overline{\sigma(y)},$$

where the sum ranges over all ring homomorphisms, of which there are only finitely many.

Remark 9.9. Following Example 3.4 in [9], the map from Definition 9.8 is non-degenerate when R is reduced, i.e., $\langle x, x \rangle = 0$ implies $x = 0$ for all $x \in R$. We have a bijective correspondence

$$\{\sigma \colon R \to \mathbb{C}\} \leftrightarrow \{(\mathfrak{p}, \sigma_{\mathfrak{p}}) : \mathfrak{p} \subset R \text{ a minimal prime ideal}, \ \sigma_{\mathfrak{p}} \colon R/\mathfrak{p} \to \mathbb{C}\}$$

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 $\langle x, y \rangle_R = \sum_{\mathfrak{p} \subset R} \langle \pi_{\mathfrak{p}}(x), \pi_{\mathfrak{p}}(y) \rangle_{R/\mathfrak{p}}$, where the sum ranges over all minimal prime ideals.

Lemma 9.10. *For all orders R that are generated as a group by $\alpha(R)$ we have $\langle R, R \rangle \subset \mathbb{Z}$. 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 $\langle x, y \rangle$.*

Proof. Note that R is reduced by Lemma 9.7. Let X be the set of minimal primes of R. Using Theorem 1.10 in [8] 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 9.9 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 Proposition 9.6.vii. 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 $\langle \zeta, \xi \rangle_R = \sum_{\sigma \colon R \to \mathbb{C}} \sigma(\zeta \xi^{-1})$, 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 $\langle R, R \rangle \subset \mathbb{Z}$ 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. $\quad\square$

For a ring R, an R-module M, and a subset $X \subset M$, we write $R \cdot X$ for the submodule of M generated by X.

Lemma 9.11. *There exists a polynomial-time algorithm that, given a finite-dimensional commutative $\mathbb{Q}$-algebra A and a finite set $X \subset A$, computes a $\mathbb{Q}$-basis Y of the subalgebra B of A generated by X, where each element in Y is a finite (possibly vacuous) product of elements of X.*

Proof. The algorithm proceeds as follows. Start with $Y = \{1\}$. Compute the set of products $Z = \{xy : x \in X, y \in Y\}$ and update Y to be a maximal $\mathbb{Q}$-linearly independent subset of $Z \cup Y$. Repeat this until $\mathbb{Q} \cdot Y$ is stable.

Suppose in some step $\mathbb{Q} \cdot Y = \mathbb{Q} \cdot (Z \cup Y)$. Then $Z \subset \mathbb{Q} \cdot Y$, so $\mathbb{Q} \cdot Y$ is closed under taking products with X. Since X generates B as a $\mathbb{Q}$-algebra and $1 \in \mathbb{Q} \cdot Y$ by the choice of initial Y, it follows that $\mathbb{Q} \cdot Y = B$. Note that $\#Y \leq \dim_{\mathbb{Q}}(B)$ and thus there are at most $\dim_{\mathbb{Q}}(B)$ 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. $\quad\square$

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

$$R = \{(a_i)_i \in \mathbb{Z}^n : (\forall i, j) \; a_i \equiv a_j \bmod 2\},$$

the set $\{-1, 1\}^n = \mu(R) \subset \alpha(R)$ is exponentially large. Theorem 1.4 of [7] gives a polynomial-time algorithm that, given an order R, produces a set of generators of $\mu(R)$.

Proposition 9.12. *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 [7]. Combined with Proposition 9.6.vii we may assume R is connected and $\alpha(R) = \mu(R) \cup \{0\}$.

Apply Theorem 1.2 in [7] to compute in polynomial time a set X of generators of the group $\mu(R)$. Using Lemma 9.11 we may compute a basis $Z \subseteq \mu(R)$ for the subalgebra $\mathbb{Q} \cdot \mu(R)$ of $R \otimes \mathbb{Q}$ as a $\mathbb{Q}$-vector space.

Denote the discriminant $\det((\mathrm{Tr}_{\mathbb{Q} \cdot \mu(R)/\mathbb{Q}}(xy))_{x,y \in Z})$ of $\mathbb{Z} \cdot Z$ by Δ_Z, and similarly let $\Delta_{\mu(R)}$ denote the discriminant of $\mathbb{Z} \cdot \mu(R)$. Let $n = \#Z = \dim_{\mathbb{Q}}(\mathbb{Q} \cdot \mu(R))$. We have $|\Delta_Z| \leq n^{3n/2}$ by Hadamard's inequality and the fact that $|\mathrm{Tr}(\zeta)| \leq n$ for $\zeta \in \mu(R)$. Thus,

$$\#(\mathbb{Z} \cdot \mu(R)/\mathbb{Z} \cdot Z)^2 = |\Delta_Z|/|\Delta_{\mu(R)}| \leq |\Delta_Z| \leq n^{3n/2}.$$

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. $\quad\square$

Roots of unity are homogeneous in any grading of a connected order, by Theorem 1.5 of [9]. The next result shows this is also true in any orthogonal decomposition of a connected reduced order, where orthogonal means with respect to the inner product in Definition 9.8.

Lemma 9.13. *Let $\mathcal{R}$ be an orthogonal decomposition of a connected reduced order R. Then the roots of unity of R are homogeneous in $\mathcal{R}$, i.e., for all $\zeta \in \mu(R)$ there exists some $M \in \mathcal{R}$ such that $\zeta \in M$.*

Proof. By Corollary 5.6 in [9] the element $1 \in R$ is *indecomposable*, i.e., for all $x, y \in R$ such that $x + y = 1$ and $\langle x, y \rangle \geq 0$ we have $x = 0$ or $y = 0$. Since $x \mapsto \zeta x$ is an isometry of R for all $\zeta \in \mu(R)$, we conclude that all $\zeta \in \mu(R)$ are indecomposable. Indecomposable elements are clearly homogeneous. $\quad\square$

Lemma 9.14. *Let R be a connected reduced order and $\overline{R} = (\Gamma, (R_\gamma)_\gamma)$ be the universal grading of R. Suppose $X \subset \mu(R)$ is a subset and $A \subset R$ is a subring such that $\bigoplus_{x \in X} Ax$ is an orthogonal decomposition of R. Write $\Delta = \mu(R)/\mu(A)$. Then the natural map $g \colon X \to \Delta$ is a bijection and $\overline{S} = (\Delta, (A \cdot g^{-1}(\delta))_\delta)$ is a grading of R. If also $A \subset R_1$, then $\overline{S}$ is universal.*

Proof. First we show g is a bijection. If $g(x) = g(y)$ for $x, y \in X$, then $Ax = Ay$ and thus $x = y$ by orthogonality. Hence g is injective. It follows from Lemma 9.13 that $\mu(R) = \bigcup_{x \in X}(Ax \cap \mu(R)) = \mu(A) \cdot X$, so g is surjective. It follows that $\overline{S}$ is a grading of R. Now assume $A \subset R_1$. Let $e \colon \Delta \to \Gamma$ be induced by the degree map $d \colon \mu(R) \to \Gamma$, which is well-defined because $\mu(A) \subset \ker(d)$ by assumption. Then $e_*(\overline{S}) = \overline{R}$, and $\overline{S}$ is universal by Proposition 5.8.iv. $\quad\square$

Theorem 9.15. *There exists a polynomial-time algorithm that, given a reduced order R that is generated as a group by $\alpha(R)$, computes the universal grading of R.*

Proof. We may write R as a product of connected orders in polynomial time using Algorithm 6.1 in [7]. Using Proposition 5.9.ii and Proposition 9.6.vi we may restrict ourselves to the connected case, so suppose R is connected and thus $\alpha(R) = \mu(R) \cup \{0\}$ by Proposition 9.6.vii. Let $\overline{R} = (\Gamma, (R_\gamma)_\gamma)$ be the universal grading of R, which is not part of the algorithm.

We will compute a subring $A \subset R$ and a sequence $s_1, \ldots, s_n \in \mu(R)$ having the following properties:

$$\text{(i)} \ \sum_{i=1}^{n} As_i = R; \quad \text{(ii)} \ A \subset R_1; \quad \text{(iii)} \ (\forall i \neq j) \ \langle As_i, As_j \rangle = 0.$$

It then follows from Lemma 9.14 that we have in fact computed the universal grading of R. The algorithm is as follows.

(1) Set $A = \mathbb{Z}$ and compute $\mathbb{Z}$-module generators $s_1, \ldots, s_n \in \mu(R)$ for R using Proposition 9.12.
(2) While there exist $i \neq j$ such that $\langle As_i, As_j \rangle \neq 0$, as computed by Lemma 9.10:
    (a) Choose any $i < j$ such that $\langle As_i, As_j \rangle \neq 0$;
    (b) Replace A by the ring generated by A and $s_i^{-1}s_j$;
    (c) Remove s_j from the list of generators.

Clearly, properties (i) and (ii) are satisfied after step (1), and (iii) is satisfied after step (2). Moreover, since the number of generators decreases each step, the number of iterations in step (2) is polynomially bounded and the algorithm terminates. It remains to show that (i) and (ii) are preserved by step (2). Property (i) is preserved because s_j is contained in As_i after updating A in step (2b). For (ii) it suffices to show that $s_i^{-1}s_j \in R_1$. As $s_i^{-1}s_j \in \mu(R)$ we have $s_i^{-1}s_j \in R_\gamma$ for $\gamma = d(s_i^{-1}s_j)$ by Lemma 6.1. Since $\langle A, As_i^{-1}s_j \rangle = \langle As_i, As_j \rangle \neq 0$ we conclude that $R_\gamma = R_1$ by Proposition 5.8 in [9], as was to be shown. Lastly, note that all operations can be carried out in polynomial time. $\square$

Proof of Theorem 1.4. By Proposition 9.4 it suffices to compute a universal grading of R. Apply Theorem 9.5 in the general case and Theorem 9.15 in the specific case of an order generated by its autopotents. $\square$

Data availability

No data was used for the research described in the article.

References

[1] I. Adjaero, E. Spiegel, Isomorphic group rings over domains, Can. Math. Bull. 32 (1989) 85–89, https://doi.org/10.4153/CMB-1989-012-6.
[2] F. Borceux, Handbook of Categorical Algebra 2: Categories and Structures, Encyclopedia of Mathematics and Its Applications, vol. 50, Cambridge University Press, 1994.
[3] I. Ciocănea-Teodorescu, Algorithms for finite rings, PhD thesis, Leiden University, 2016, https://hdl.handle.net/1887/40676.
[4] G. Higman, The units of group-rings, Proc. Lond. Math. Soc. 46 (2) (1940) 231–248.
[5] S. Lang, Algebra, 3rd edition, Graduate Texts in Mathematics, vol. 211, Springer, New York, 2005.
[6] H.W. Lenstra Lattices, in: J.P. Buhler, P. Stevenhagen (Eds.), Algorithmic Number Theory, in: MSRI Publications, vol. 44, Cambridge University Press, 2008, pp. 127–181, http://library.msri.org/books/Book44/.
[7] H.W. Lenstra, A. Silverberg, Roots of unity in orders, Found. Comput. Math. 17 (3) (Jun 2017) 851–877, https://doi.org/10.1007/s10208-016-9304-1.
[8] H.W. Lenstra, A. Silverberg, Algorithms for commutative algebras over the rational numbers, Found. Comput. Math. 18 (1) (2018) 159–180, https://doi.org/10.1007/s10208-016-9336-6.
[9] H.W. Lenstra, A. Silverberg, Universal gradings of orders, Arch. Math. 111 (6) (2018) 579–597, https://doi.org/10.1007/s00013-018-1228-3.

[10] W. May, Group algebras over finitely generated rings, J. Algebra 39 (2) (1976) 483–511, https://doi.org/10.1016/0021-8693(76)90049-1.
[11] W. May, Isomorphism of group algebras, J. Algebra 40 (1) (1976) 10–18, https://doi.org/10.1016/0021-8693(76)90083-1.
[12] W. May, Unit Groups and Isomorphism Theorems for Commutative Group Algebras, North-Holland Math. Stud., vol. 126, North-Holland, Amsterdam, 1986, pp. 163–178.
[13] W. May, The isomorphism problem for modular abelian p-group algebras, J. Algebra Appl. 13 (4) (2014).
[14] M.M. Parmenter, E. Spiegel, Isomorphic group rings over domains revisited, J. Algebra 129 (1990) 518–523, https://doi.org/10.1016/0021-8693(90)90234-F.
[15] D.S. Passman, The Algebraic Structure of Group Rings, Wiley–Interscience, 1977.
[16] C. Polcino Milies, Units of group rings and a conjecture of H.J. Zassenhaus, São Paulo J. Math. Sci. 16 (2022) 43–61, https://doi.org/10.1007/s40863-021-00267-8.
[17] S.K. Sehgal, Topics in Group Rings, 1st edition, Pure and Applied Mathematics, vol. 50, Marcel Dekker Inc., 1978.
[18] S.K. Sehgal, Units in Integral Group Rings, Harlow and John Wiley & Sons, Inc., New York, 1993.
[19] D.M.H. van Gent, Algorithms for finding the gradings of reduced rings, Master's thesis, Leiden University, 2019, https://arxiv.org/abs/1911.02957.
[20] D.M.H. van Gent, Decompositions in algebra, PhD thesis, Leiden University, 2024, in preparation.