Decompositions in algebra

Gent, D.M.H. van

CHAPTER 5

Group rings

5.1 Introduction

This chapter is based on [35], the authors of which include H.W. Lenstra and A. Silverberg. Given a ring A and a (multiplicatively written) group G we may construct the *group ring* $A[G]$, a ring whose additive group is simply the free A-module with basis G, and multiplication is given by $ag\cdot bh = (ab)(gh)$ for $a, b \in A$ and $g, h \in G$. This construction describes a functor

$$\underline{\mathrm{Ring}} \times \underline{\mathrm{Group}} \to \underline{\mathrm{Ring}}.$$

The *Isomorphism Problem for Group Rings* asks to describe the fibers of this map up to isomorphism, i.e. given a ring R, what can one say about the pairs (A, G) such that $A[G] \cong R$? We will refine this question by not just asking for the existence of an isomorphism, but asking for the isomorphism as well, meaning we study the triples (A, G, ϕ) such that $\phi\colon A[G] \to R$ is an isomorphism. We will specialize to the case where A and G, and hence R, are commutative. Equivalently, for non-zero rings R, we study the set

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

where $A[G] = R$ is to mean that the natural map $A[G] \to R$ is an isomorphism of rings. We say a ring R is *stark* if it is non-zero, commutative and can only be written as a group ring in the trivial way, i.e. $\#\mathcal{D}(R) = 1$. Our main result reads as follows.

Theorem 5.6.4. *Let R be a non-zero reduced order. Then there exist a stark ring A, unique up to ring isomorphism, and a finite abelian group G, unique up to group isomorphism, such that $R \cong A[G]$ as rings.*

Clearly, if A is a ring and I and H are groups, then $A[I \times H]$ and $(A[I])[H]$ are isomorphic as rings. The following result, which is more or less equivalent to Theorem 5.6.4, expresses that, among reduced orders, group rings can only be isomorphic if they are so for this obvious reason.

Theorem 5.6.3. *Suppose A and B are reduced orders and G and H are finite abelian groups. Then the following are equivalent:*

(i) *$A[G] \cong B[H]$ as rings,*

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

If R, A and G are as in Theorem 5.6.4, then A is isomorphic to a subring of R, and G is isomorphic to a subgroup of $\mu(R)$, but as Example 5.5.20 shows, this subring and subgroup need not be uniquely determined. However, the following theorem shows that in an important special case there is a sense in which the subrings and subgroups that can be used are entirely independent. To a connected reduced order R we associate a group $U^*(R)$ acting on R by ring automorphisms (Definition 5.5.16), and $\mathrm{Aut}(R)$ in turn clearly acts on $\mathcal{D}(R)$.

Theorem 5.5.19. *Let R be a connected reduced order and suppose (A, G), $(B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then $A \cong B$ as rings, $G \cong H$ as groups, and (A, G), (A, H), (B, G) and (B, H) are all in $\mathcal{D}(R)$ and in particular in the same $U^*(R)$-orbit.*

As can be seen in Example 5.5.21, we cannot drop the assumption that R be connected in Theorem 5.5.19.

We will prove Theorem 5.5.19 using the theory of gradings from Chapter 4. For a non-zero commutative ring R and $(A, G) \in \mathcal{D}(R)$ we have a natural grading $\mathcal{R} = \{R_\zeta\}_{\zeta \in \mu(R)}$ where $R_\zeta = A\zeta$ if $\zeta \in G$ and $R_\zeta = 0$ otherwise. If R has a universal grading, we write $\Gamma(R)$ for the group of this grading, and we obtain a homomorphism $f \colon \Gamma(R) \to \mu(R)$ corresponding to $\mathcal{R}$. For a connected reduced order R we also get a homomorphism $d_R \colon \mu(R) \to \Gamma(R)$, the *degree map*, from Proposition 4.6.5. It turns out that the morphisms $f \colon \Gamma(R) \to \mu(R)$ for which the induced grading comes from a group ring are precisely those for which $f d_R f = f$. We proceed to study d_R by commutative algebra on the Mitchell embedding.

Throughout this chapter, for abelian groups M and N we write the group $\mathrm{Hom}(M, N)$ additively, regardless of the notation used for N. Let A be a connected reduced order and G a finite abelian group. We have a left action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(G, \mu(A))$ given via the restriction $\mathrm{Aut}(A) \to \mathrm{Aut}(\mu(A))$ and a right action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(\Gamma(A), G)$ via the natural map $\mathrm{Aut}(A) \to \mathrm{Aut}(\Gamma(A))$. This is used implicitly in the following theorem, where we describe the automorphism group of a group ring over a stark reduced connected order.

Theorem 5.7.8. *Let A be a stark connected reduced order with degree map $d_A \colon \mu \to \Gamma$ and let G be a finite abelian group. We equip the cartesian product*

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

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

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

where the sum in $\mathrm{Aut}(A)$ *is as in Lemma 5.7.7 and the sum in* $\mathrm{Aut}(G)$ *is taken inside* $\mathrm{End}(G)$*. For* $x \in A$ *and* $g \in G$ *write* $\left(\begin{smallmatrix} x \\ g \end{smallmatrix}\right)$ *for the element* $x \cdot g \in A[G]$*. Then:*

1. *M is a group;*
2. *there is a natural isomorphism* $M \xrightarrow{\sim} \mathrm{Aut}(A[G])$ *such that the evaluation map* $M \times A[G] \to A[G]$ *is given by*

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

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

We also have an algorithmic result. We call a ring element x *autopotent* if $x^{n+1} = x$ for some $n \geq 1$.

Theorem 5.8.4. *There is an algorithm that, given a non-zero reduced order R, computes a stark subring $A \subseteq R$ and a subgroup $G \subseteq \mu(R)$ such that $A[G] = R$. This algorithm runs* (a) *in polynomial time when the additive group of R is generated by autopotents, and generally* (b) *in time $n^{O(m)}$ where n is the length of the input and m is the number of minimal prime ideals of R.*

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

5.2 Modules and decompositions

In this section we gather some results on modules, by which we mean left modules.

Definition 5.2.1. Let R be a ring and M an R-module. We write $\mathrm{Dec}(M)$ for the set

$$\mathrm{Dec}(M) = \{(D, N) \mid D,\, N \text{ are submodules of } M \text{ with } D \oplus N = M\},$$

or equivalently the set of $\{1,2\}$-indexed decompositions of M. We equip $\mathrm{Dec}(M)$ with a partial order given by $(D, N) \leq (D', N')$ if and only if there exists a submodule $C \subseteq M$ such that $D = D' \oplus C$ and $N \oplus C = N'$.

Theorem 5.2.2 (Krull–Remak–Schmidt; see Theorem X.7.5 of [30]). *Suppose R is a ring and M is an R-module of finite length. Then there exists a decomposition of M into finitely many indecomposable submodules, and such a decomposition is unique up to automorphisms of M and relabeling of the indices.* □

Definition 5.2.3. Let R be a ring, and let $\mathcal{M}$ be a non-empty set of R-modules of finite length. For an R-module M we call an R-module D a *divisor* of M if $M \cong D \oplus N$ for some R-module N. As a consequence of Theorem 5.2.2, there exists up to isomorphism exactly one R-module D that is a divisor of every $M \in \mathcal{M}$ with the property that every R-module that is a divisor of every $M \in \mathcal{M}$ is also a divisor of D; it is called a *greatest common divisor* of the set $\mathcal{M}$. Every such D is of finite length. We say R-modules M and N are *coprime* if the greatest common divisor of $\{M, N\}$ is 0. Likewise, if $\mathcal{M}$ is a finite set of R-modules of finite length, then there exists up to isomorphism exactly one R-module L of which each $M \in \mathcal{M}$ is a divisor with the property that L is a divisor of each R-module of finite length of which each $M \in \mathcal{M}$ is a divisor; it is called a *least common multiple* of $\mathcal{M}$. Every such L is of finite length.

Definition 5.2.4. Suppose R is a ring, M is an R-module, and $h \in \operatorname{End}(M)$. We define the R-modules

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

Lemma 5.2.5 (Fitting; see Theorem X.7.3 of [30]). *Suppose R is a ring, M is an R-module of finite length, and $h \in \operatorname{End}(M)$. Then $M = \lim \operatorname{im}(h) \oplus \lim \ker(h)$, the restriction of h to $\lim \operatorname{im}(h)$ is an automorphism, and the restriction of h to $\lim \ker(h)$ is nilpotent.* □

Lemma 5.2.6. *Suppose R is a ring, M and N are R-modules, and $f\colon M \to N$ and $g\colon N \to M$ are morphisms. Then f restricts to morphisms*

$$i\colon \lim \operatorname{im}(gf) \to \lim \operatorname{im}(fg) \quad \textit{and} \quad k\colon \lim \ker(gf) \to \lim \ker(fg).$$

If M and N have finite length, then i is an isomorphism.

Proof. For all $n \geq 1$ we have

$$f(\operatorname{im}((gf)^n)) = \operatorname{im}((fg)^n f) \subseteq \operatorname{im}((fg)^n).$$

Hence $f(\lim \operatorname{im}(gf)) \subseteq \lim \operatorname{im}(fg)$, so i is well-defined. As

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

for all $n \geq 1$ we also get $f(\lim \ker(gf)) \subseteq \lim \ker(fg)$, so k is well-defined. By symmetry we obtain a restriction $j\colon \lim \operatorname{im}(fg) \to \lim \operatorname{im}(gf)$ of g. Under the finite length assumption both ji and ij are automorphisms by Lemma 5.2.5, hence i is an isomorphism. □

Proposition 5.2.7. *Suppose R is a ring, M is an R-module of finite length, and A_1, A_2, B_1, $B_2 \subseteq M$ are submodules such that A_1 and A_2 are coprime, $A_1 \oplus A_2 = B_1 \oplus B_2 = M$, and $A_1 \cong B_1$. Then $A_1 \oplus B_2 = B_1 \oplus A_2 = M$.*

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

Proof. From Theorem 5.2.2 it follows that $A_2 \cong B_2$ and thus B_1 and B_2 are coprime as well. By symmetry it therefore suffices to show $B_1 \oplus A_2 = M$. We consider the maps as in the following commutative diagram, where $\varphi\colon A_1 \to B_1$ is an isomorphism, the maps to and from M are the natural inclusions and projections, and the f_i and g_i are defined to make the diagram commute.

$$\begin{tikzcd}
& & A_1 & & A_1 \arrow[d, "e_1"'] \arrow[rrd, bend left, "g_1"] & & \\
A_1 \arrow[rru, bend left, "f_1"] \arrow[r, "\varphi"] \arrow[rrd, bend right, "f_2"'] & B_1 \arrow[r, "e"] & M \arrow[u, "p_1"'] \arrow[d, "p_2"] & & M \arrow[r, "p"] & B_1 \arrow[r, "\varphi^{-1}"] & A_1 \\
& & A_2 & & A_2 \arrow[u, "e_2"] \arrow[rru, bend right, "g_2"'] & &
\end{tikzcd}$$

Note that $\mathrm{id}_{B_1} = pe$ and $\mathrm{id}_M = e_1p_1 + e_2p_2$, so

$$\begin{aligned}
\mathrm{id}_{A_1} &= \varphi^{-1}pe\varphi = \varphi^{-1}p(e_1p_1 + e_2p_2)e\varphi \\
&= \varphi^{-1}pe_1 \cdot p_1e\varphi + \varphi^{-1}pe_2 \cdot p_2e\varphi = g_1f_1 + g_2f_2.
\end{aligned}$$

Lemma 5.2.6 shows that $D = \lim \operatorname{im}(g_2f_2) \cong \lim \operatorname{im}(f_2g_2)$, so D is a divisor of both A_1 and A_2 by Lemma 5.2.5. Since A_1 and A_2 are coprime, we must have that $D = 0$ and thus g_2f_2 is nilpotent. We conclude that $g_1f_1 = \mathrm{id}_{A_1} - g_2f_2$ is an automorphism of A_1. Hence f_1 is injective, and since A_1 is of finite length it must be an automorphism. It follows that $p_1e = f_1\varphi^{-1}\colon B_1 \to A_1$ is an isomorphism, so $M = B_1 \oplus A_2$, as was to be shown. □

Definition 5.2.8. Let R be a ring. A class $\mathcal{S}$ of R-modules is *multiplicative* if $0 \in \mathcal{S}$ and for all R-modules M, N and D with $M \cong N \oplus D$ and N, $D \in \mathcal{S}$ one has $M \in \mathcal{S}$. We say a multiplicative class $\mathcal{S}$ of R-modules is *saturated* if for all $M \in \mathcal{S}$ and all divisors D of M one has $D \in \mathcal{S}$. For a multiplicative class $\mathcal{S}$ of R-modules and an R-module M, write

$$\mathrm{Dec}_{\mathcal{S}}(M) = \{(M_1, M_2) \in \mathrm{Dec}(M) \mid M_2 \in \mathcal{S}\},$$

where $\mathrm{Dec}(M)$ is as in Definition 5.2.1. We equip $\mathrm{Dec}_{\mathcal{S}}(M)$ with the partial order inherited from $\mathrm{Dec}(M)$, and write $\max(\mathrm{Dec}_{\mathcal{S}}(M))$ for its set of maximal elements.

Proposition 5.2.9. *Let R be a ring, let $\mathcal{S}$ be a multiplicative class of R-modules, and let M and N be R-modules. Then:*

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

Suppose also that $\mathcal{S}$ is saturated and $(A_1, A_2) \in \mathrm{Dec}_{\mathcal{S}}(M)$. Then

3. *one has $(A_1, A_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$ if and only if 0 is the only divisor of A_1 that is in $\mathcal{S}$;*

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

4. *the set $\max(\mathrm{Dec}_{\mathcal{S}}(M))$ is non-empty and consists of one orbit of $\mathrm{Dec}_{\mathcal{S}}(M)$ under the action of $\mathrm{Aut}(M)$;*
5. *if (A_1, A_2), $(B_1, B_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$, then (A_1, B_2), $(B_1, A_2) \in \max(\mathrm{Dec}_{\mathcal{S}}(M))$.*

Proof. 1. Apply the definition of multiplicative with $D = 0$.

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

3. If (A_1, A_2) is maximal but $A_1 = D \oplus B_1$ for some $D \in \mathcal{S}$ and some B_1, then $(A_1, A_2) \leq (B_1, A_2 \oplus D) \in \mathrm{Dec}_{\mathcal{S}}(M)$ and thus $A_2 = A_2 \oplus D$ and $D = 0$. Conversely, suppose 0 is the only divisor of A_1 that is in $\mathcal{S}$ and $(A_1, A_2) \leq (B_1, B_2)$. Then there is some C such that $A_1 = B_1 \oplus C$ and $B_2 = A_2 \oplus C$. Since $\mathcal{S}$ is saturated we have $C \in \mathcal{S}$, and since C is a divisor of A_1 we must have that $C = 0$. Hence $(A_1, A_2) = (B_1, B_2)$ is maximal.

4. Let $M = \bigoplus_{i \in I} M_i$ with each M_i indecomposable. If A_2, respectively A_1, is the direct sum of those M_i that are, respectively are not, in $\mathcal{S}$, then (A_1, A_2) is in $\mathrm{Dec}_{\mathcal{S}}(M)$ and it is maximal by 3. If (B_1, B_2) is also maximal, then B_2, respectively B_1, is a direct sum of indecomposables that are, respectively are not, in $\mathcal{S}$; this follows from the definition of $\mathrm{Dec}_{\mathcal{S}}(M)$ and from 3. Since together these decompositions give a decomposition of M into indecomposables, Theorem 5.2.2 implies that $A_1 \cong B_1$ and $A_2 \cong B_2$, so (B_1, B_2) belongs to the $\mathrm{Aut}(M)$-orbit of (A_1, A_2). Because the action of $\mathrm{Aut}(M)$ preserves the partial order, this orbit is conversely contained in $\max(\mathrm{Dec}_{\mathcal{S}}(M))$.

5. By 3 we have that A_1 and A_2 are coprime and by 4 we have $A_1 \cong B_1$ and $A_2 \cong B_2$. We may conclude from Proposition 5.2.7 that $(A_1, B_2), (B_1, A_2) \in \mathrm{Dec}_{\mathcal{S}}(M)$. Applying 3 again we may conclude they are maximal. □

5.3 Morphisms as modules

In this section we will interpret a morphism of (finite) abelian groups as a (finite length) module, as expressed by Proposition 5.3.2. We will then study decompositions of this module and what this decomposition corresponds to in terms of the original morphism. This will enable us in the next section to apply the Krull–Remak–Schmidt theorem to morphisms of finite abelian groups.

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

Definition 5.3.1. Let $\mathcal{C}$ be a category. We define the *arrow category* of $\mathcal{C}$, written $\mathrm{Arr}(\mathcal{C})$, to be the category where the objects are the morphisms of $\mathcal{C}$ and for objects $f\colon A \to B$ and $g\colon C \to D$ the morphisms from f to g are the pairs $(\alpha, \beta) \in \mathrm{Hom}_{\mathcal{C}}(A, C) \times \mathrm{Hom}_{\mathcal{C}}(B, D)$ such that $\beta f = g\alpha$.

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

Proposition 5.3.2. *There is an equivalence of categories, specified in the proof, between the category* $\mathrm{Arr}(\underline{\mathrm{Ab}})$ *and the category of* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$*-modules. This equivalence restricts to an equivalence of categories between the subcategory* $\mathrm{Arr}(\underline{\mathrm{ab}})$ *and the subcategory of* $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$*-modules of finite length.*

Proof. Write $\mathcal{M}$ for the category of $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules. We will define functors

$$F\colon \mathrm{Arr}(\underline{\mathrm{Ab}}) \to \mathcal{M} \quad \text{and} \quad G\colon \mathcal{M} \to \mathrm{Arr}(\underline{\mathrm{Ab}})$$

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

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa \\ yf(a) + zb \end{pmatrix},$$

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

Definition 5.3.3. Write $\mathcal{I}$ for the class of $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-modules that correspond to isomorphisms under the equivalence of categories of Proposition 5.3.2.

One readily checks that the class $\mathcal{I}$ is multiplicative and saturated in the sense of Definition 5.2.8. We observe that a $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module M belongs to $\mathcal{I}$ if and only if its $\left(\begin{smallmatrix}\mathbb{Z} & 0\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure can be extended to a $\left(\begin{smallmatrix}\mathbb{Z} & \mathbb{Z}\\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$-module structure. This fact will not be needed, and we omit the proof.

Remark 5.3.4. Using the equivalence of categories of Proposition 5.3.2, one can translate terminology related to modules into terminology about morphisms of abelian groups. We briefly go through what is most relevant to us:

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

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

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

4. For a morphism $f\colon A \to B$, the set $\operatorname{Dec}(f)$ is the set of all pairs (f_0, f_1) of restrictions of f such that $f_0 \oplus f_1 = f$, which is a partially ordered set as in Definition 5.2.1. The set $\operatorname{Dec}_{\mathcal{I}}(f)$ is the set of $(f_0, f_1) \in \operatorname{Dec}(f)$ such that f_1 is an isomorphism.

Definition 5.3.5. Let $f\colon A \to B$ be a morphism of abelian groups. We say f is *nil* if for all morphisms $g\colon B \to A$ the element $fg \in \operatorname{End}(B)$ is nilpotent, or equivalently $gf \in \operatorname{End}(A)$ is nilpotent.

Lemma 5.3.6. *Suppose $f\colon A \to B$ is a morphism of abelian groups.*

1. *If f is a nil isomorphism, then $A = B = 0$.*
2. *If f is nil, then every divisor of f is nil.*

Proof. 1. If f is a nil isomorphism, then $ff^{-1} = \mathrm{id}_B$ is nilpotent, hence $A = B = 0$. 2. Suppose $f = f_0 \oplus f_1$ for morphisms $f_i\colon A_i \to B_i$. Let $g_1\colon B_1 \to A_1$ be a morphism. Then $g = g_1 \oplus 0 : B_1 \oplus B_2 \to A_1 \oplus A_2$ is a morphism such that fg is nilpotent if and only if $f_1 g_1$ is nilpotent. Hence f_1 is nil if f is nil. □

Lemma 5.3.7. *Let $f\colon A \to B$ be a morphisms of finite abelian groups.*

1. *Then f is nil if and only if all isomorphisms dividing f are trivial.*
2. *Suppose $f = f_0 \oplus f_1$. Then f is nil if and only if f_0 and f_1 are nil.*
3. *We may uniquely, up to automorphisms of f, write $f = f_0 \oplus f_1$ with f_0 nil and f_1 an isomorphism.*
4. *Suppose $(f_0, f_1) \in \mathrm{Dec}_{\mathcal{I}}(f)$. Then (f_0, f_1) is maximal if and only if f_0 is nil.*

Proof. 1. If f is nil, then every divisor is nil and the only nil isomorphism is trivial by Lemma 5.3.6. Suppose all isomorphisms dividing f are trivial. Let $g\colon B \to A$ be a morphism. Then $\lim \operatorname{im} fg = 0$ by Lemma 5.2.6, otherwise the restriction of f to $\lim \operatorname{im} fg \to \lim \operatorname{im} gf$ is an isomorphism and a nontrivial divisor of f. Hence fg is nilpotent by Lemma 5.2.5 and f is nil.

Both 2 and 3 follow from 1 combined with Theorem 5.2.2, while 4 follows from 1 and Proposition 5.2.9.3. □

5.4 The group U^*

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

Definition 5.4.1. For $f, g \in \mathrm{Hom}(B, A)$, we define $f \star g = fdg$ and extend $\star$ to a ring multiplication on the additive group $Q = Q(d) = \mathbb{Z} \oplus \mathrm{Hom}(B, A)$ by

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

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

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

and write $U^* = U^*(d) = U \cap Q^*$.

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

Lemma 5.4.2. *We have a ring homomorphism $q\colon Q \to \mathrm{End}(d)$ defined by sending 1 to the identity id_d and $f \in \mathrm{Hom}(B, A)$ to (fd, df). It restricts to a group homomorphism $U^* \to \mathrm{Aut}(d)$.* □

Remark 5.4.3. Note that A and B are $\mathrm{End}(d)$-modules. The map q makes A and B into Q-modules in such a way that d is Q-linear.

In the following results, we use the terminology from Remark 5.3.4. We let U^* act on $\mathrm{Dec}(d)$ via the map $U^* \to \mathrm{Aut}(d)$ from Lemma 5.4.2.

Lemma 5.4.4. *Let $d_i \colon A_i \to B_i$ with $i \in \{-1, 0, 1\}$ be restrictions of d such that (d_0, d_1) and (d_0, d_{-1}) belong to $\mathrm{Dec}(d)$, and suppose that d_0 or d_1 is an isomorphism. Then $(d_0, d_{-1}) \in U^* \cdot (d_0, d_1)$.*

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

$$\begin{tikzcd}
A_1 \arrow[r, "d_1"] \arrow[d, "r_A"'] & B_1 \arrow[d, "r_B"] \arrow[dl, dotted, "f_1"'] \\
A_0 \arrow[r, "d_0"'] & B_0
\end{tikzcd}$$

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

The proof of the following proposition, which can be considered a sharpening of Proposition 5.2.9.4 when $R = \left(\begin{smallmatrix}\mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z}\end{smallmatrix}\right)$, is the main reason for considering d as a module.

Proposition 5.4.5. *Assume A and B are finite. Then the set of maximal elements of $\mathrm{Dec}_{\mathcal{I}}(d)$ equals one orbit of $\mathrm{Dec}_{\mathcal{I}}(d)$ under the action of U^*.*

Proof. By Proposition 5.3.2 we may apply Proposition 5.2.9.4. Thus it suffices to show that any two maximal elements $(d_0, d_1), (e_0, e_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ are in the same U^*-orbit. Recall that $(d_0, e_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ by Proposition 5.2.9.5. Applying Lemma 5.4.4 we obtain $(d_0, e_1) \in U^* \cdot (d_0, d_1)$ since d_1 is an isomorphism, and $(e_0, e_1) \in U^* \cdot (d_0, e_1)$ since e_1 is an isomorphism. Thus $(e_0, e_1) \in U^* \cdot (d_0, e_1) = U^* \cdot (d_0, d_1)$. □

5.5 The degree map

In this section we will prove facts about group rings and interpret them as a special case of gradings. We will rely heavily on [34].

Definition 5.5.1. For a ring A and a group G the *group ring* $A[G]$ is an A-algebra with as underlying group the free A-module with basis G where multiplication is given by

$$\Big(\sum_{g\in G} a_g g\Big)\cdot\Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G}\Big(\sum_{h\in G} a_h b_{h^{-1}g}\Big) g.$$

We associate with $A[G]$ its natural grading $\{Ag\}_{g\in G}$.

First we observe that that the properties of being reduced and being connected are preserved under construction of group rings, as a consequence of Theorem 1.5 in [34] or Theorem 4.6.6.

Corollary 5.5.2. *Let A be an order and G a finite abelian group. Then:*

1. *We have* $\mathrm{nil}(A[G]) = \mathrm{nil}(A)[G]$, *and A is reduced if and only if $A[G]$ is reduced;*
2. *We have* $\mathrm{Id}(A[G]) = \mathrm{Id}(A)$, *and A is connected if and only if $A[G]$ is connected;*
3. *If A is connected, then $\mu(A[G]) = \mu(A) \times G$.* □

Definition 5.5.3. Let R be a reduced order. By Theorem 1.3 in [34] or Theorem 6.21 in [17] the ring R has a universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ (see Definition 4.2.1). We will write $\Gamma(R)$ for this group Γ.

Remark 5.5.4. If R and R' are commutative rings that have universal gradings, then any ring isomorphism $R \to R'$ induces a group isomorphism $\Gamma(R) \to \Gamma(R')$, so $\Gamma(R)$ behaves functorially under ring isomorphisms; in particular, the group $\mathrm{Aut}(R)$ of ring automorphisms of R acts in a natural way on $\Gamma(R)$.

Lemma 5.5.5. *Let R be a connected reduced order and let $\{R_\gamma\}_{\gamma\Gamma(R)}$ be its universal grading. Then there exists a morphism of finite abelian groups $d\colon \mu(R) \to \Gamma(R)$ that sends $\zeta \in \mu(R)$ to the unique $\gamma \in \Gamma(R)$ such that $\zeta \in R_\gamma$.*

Proof. The group $\Gamma(R)$ is finite by Theorem 1.3 of [34], and $\mu(R)$ is finite by Lemma 3.3.ii in [32]. By Theorem 1.5.iii of [34], if $\zeta \in \mu(R)$, then there exists a $\gamma \in \Gamma(R)$ such that $\zeta \in R_\gamma$. The element γ is unique, since $R_\gamma \cap R_\delta = 0$ for all $\gamma \neq \delta$. That d is a homomorphism follows from the definitions. □

Definition 5.5.6. For a connected reduced order R we call the map $d\colon \mu(R) \to \Gamma(R)$ from Lemma 5.5.5 the *degree map* of R.

The above definition depends on the choice of universal grading. However, the universal grading of R is uniquely unique. Moreover, the proof of Theorem 1.3 of [34], which states that a reduced order has a universal grading, exhibited an explicit canonical choice of universal grading. Thus we can confidently refer to *the* degree map of a connected reduced order. We now describe the degree map $d_{A[G]}$ of $A[G]$.

Proposition 5.5.7. *Let A be a connected reduced order and let G be a finite abelian group. Let $(\Gamma(A), (A_\gamma)_\gamma)$ and $(\Gamma(A[G]), (R_\gamma)_\gamma)$ be the universal grading of A and $A[G]$ respectively. Then*

1. *we have $\Gamma(A[G]) = \Gamma(A) \times G$, and $R_{(\gamma,g)} = A_\gamma \cdot g$ for all $\gamma \in \Gamma(A)$ and $g \in G$;*
2. *if we identify $\mu(A[G])$ with $\mu(A) \times G$ as in Proposition 5.5.2.iii, then the degree map $d_{A[G]}\colon \mu(A) \times G \to \Gamma(A) \times G$ equals $d_A \times \mathrm{id}_G$;*
3. *we have $\Gamma(A) = \langle \gamma \in \Gamma(A[G]) : R_\gamma \cap A \neq 0 \rangle$.*

Proof. Let $\mathcal{A} = (\Gamma(A), (A_\gamma)_\gamma)$ and $\mathcal{R} = (\Gamma(A[G]), (R_\gamma)_\gamma)$ be the universal gradings of A and $A[G]$ respectively and write $\mathcal{A}[G] = (\Gamma(A) \times G, (A_\gamma \cdot g)_{(\gamma,g)})$. By universality there exists a unique morphism of gradings $\varphi\colon \mathcal{R} \to \mathcal{A}[G]$, which by Definition 4.2.1 is a group homomorphism $\Gamma(A[G]) \to \Gamma(A) \times G$, and we will show that it is an isomorphism. Let $\pi\colon \Gamma(A) \times G \to G$ be the projection and $\Delta = \ker(\pi\varphi)$. For $g \in G$ we have $g \in R_{d_{A[G]}(g)}$ and $g \in A_1 \cdot g$, so $\pi\varphi d_{A[G]}$ is the identity on G. It follows that $\Gamma(A[G]) = \Delta \times G$. Then $\mathcal{R}_A = (\Delta, (R_\delta)_\delta)$ is a grading of A, and φ restricts to a morphism of gradings $\varphi'\colon \mathcal{R}_A \to \mathcal{A}$ with $\varphi = \varphi' \times \mathrm{id}_G$. With $\Delta' = \langle \delta \in \Delta : R_\delta \neq 0 \rangle$ we have

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

so by Lemma 4.2.4.5 we obtain $\Delta' \times G = \Gamma(A[G]) = \Delta \times G$. Hence $\Delta' = \Delta$, so $\mathcal{R}_A$ is universal by Lemma 4.2.4.4. It follows that φ' and hence φ is an isomorphism, proving 1. Now 2 and 3 follow by inspection. □

Proposition 5.5.7.2 expresses the degree map of $A[G]$ in terms of G and the degree map of A, but we will mainly use it in the opposite direction. Specifically, for a connected reduced order R, an element $(A, G) \in \mathcal{D}(R)$ corresponds to a certain decomposition $(d_A, \mathrm{id}_G) \in \mathrm{Dec}_{\mathcal{I}}(d)$ of the degree map d of R, as defined in Definition 5.2.1 and Definition 5.3.3.

Example 5.5.8. Note that the conclusion to Proposition 5.5.7 becomes false when we drop the assumption that A be connected.

Let $A = \mathbb{Z} \times \mathbb{Z}$, which has a trivial universal grading $\mathcal{A}$ by Proposition 4.2.6.2, and let G be a non-trivial finite abelian group. Because $A[G] \cong \mathbb{Z}[G] \times \mathbb{Z}[G]$ we get $\Gamma(A[G]) = G \times G$ by Proposition 4.2.6.2, while $\mathcal{A}[G]$ is G-indexed. Hence $\mathcal{A}[G]$ is not universal.

Definition 5.5.9. Suppose R is a commutative ring. We define the set

$$\mathcal{D}(R) = \left\{ (A,G) \;\middle|\; \begin{array}{l} A \subseteq R \text{ is a subring,} \\ G \subseteq R^* \text{ is a subgroup,} \\ A[G] = R \end{array} \right\}$$

which we equip with a partial order $\leq$ given by $(B,H) \leq (A,G)$ if and only if $H \subseteq G$ and $B \supseteq A$.

Lemma 5.5.10. *Suppose R is a non-zero order. Then for each $(A,G) \in \mathcal{D}(R)$ the order of G is at most the rank of R as $\mathbb{Z}$-module, and $\mathcal{D}(R)$ contains a maximal element.*

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

Lemma 5.5.11. *Let R be a connected order and let $(A,G),(B,H) \in \mathcal{D}(R)$. Then $(B,H) \leq (A,G)$ if and only if there exists some subgroup $J \subseteq \mu(R)$ such that $B = A[J]$ and $G = J \times H$.*

Proof. The implication ($\Leftarrow$) is obvious, so it remains to prove ($\Rightarrow$). By Lemma 5.5.10 the group H is finite, and by Proposition 5.5.2.3 the multiplication map $\mu(B) \times H \to \mu(R)$ is an isomorphism. Since the inverse image of G is $J \times H$, we have $G = J \times H$. Thus $A[J][H] = A[J \times H] = A[G] = B[H]$ and therefore $A[J] = B$. □

Example 5.5.12. The conclusion to Lemma 5.5.11 does not hold in general for non-connected orders. Let p be prime and let $G = C_p \times C_p$ with C_p a group of order p. Then G is a 2-dimensional $\mathbb{F}_p$-vector space and thus there are precisely $p+1$ subgroups $H_0, \ldots, H_p$ of G of order p. We have $H_i \cdot H_j = G$ if and only if $i \neq j$. Let $R = \mathbb{Z}[G] \times \mathbb{Z}[G]$ and let $\Delta\colon G \to \mu(R)$

be the map given by $g \mapsto (g, g)$. Now consider the elements $(\mathbb{Z}\times\mathbb{Z}, \Delta(G)) \geq (\mathbb{Z}[H_0] \times \mathbb{Z}[H_1], \Delta(H_p))$ of $\mathcal{D}(R)$. As Proposition 5.5.2 implies

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

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

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

Lemma 5.5.13. *Let R be a non-zero commutative ring and let $(A, G) \in \mathcal{D}(R)$. If (A, G) is maximal, then A is stark. When R is a connected order, the converse also holds.*

Proof. If $A = B[J]$ for some $J \subseteq \mu(A)$, then $(A, G) \leq (B, J \times G) \in \mathcal{D}(R)$. Hence if (A, G) is maximal we have $(A, G) = (B, J\times G)$ and thus $J = 1$, so A is stark. For connected orders, the converse follows from Lemma 5.5.11. □

Note that from Theorem 5.6.3 it follows that maximality of $(A, G) \in \mathcal{D}(R)$ for a non-zero reduced order R is equivalent to A being stark even when R is not connected. However, we have not proved this yet.

Remark 5.5.14. Let R be a connected reduced order with universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ and degree map $d\colon \mu \to \Gamma$. Note that the group $\mathrm{Aut}(R)$ acts on the category of gradings of R. Under this action, $\sigma \in \mathrm{Aut}(R)$ sends $\{R_\gamma\}_{\gamma\in\Gamma}$ to $\{\sigma(R_\gamma)\}_{\gamma\in\Gamma}$, which is again a universal grading of R. Thus, by universality this induces a unique isomorphism $f\colon \Gamma \to \Gamma$ between them. It follows that $\mathrm{Aut}(R)$ acts on Γ. Clearly $\mathrm{Aut}(R)$ acts on $\mu(R)$, and it is then easy to see that the combination of these actions gives an action $\mathrm{Aut}(R) \to \mathrm{Aut}(d)$. Through this map the group $\mathrm{Aut}(R)$ acts on $\mathrm{Dec}_{\mathcal{I}}(d)$.

Theorem 5.5.15. *Let R be a connected reduced order. We have a natural isomorphism*

$$\mathcal{D}(R) \to \mathrm{Dec}_{\mathcal{I}}(d_R)$$

of partially ordered $\mathrm{Aut}(R)$*-sets given by*

$$\begin{aligned}(A, G) &\mapsto (d_A\colon \Gamma(A) \to \mu(A);\ \mathrm{id}_G\colon G \to G)\\ \Big(\bigoplus_{\gamma\in\Gamma_0} R_\gamma, \mu_1\Big) &\leftarrow\!\shortmid (d_0\colon \Gamma_0 \to \mu_0;\ d_1\colon \Gamma_1 \to \mu_1),\end{aligned}$$

where the first map is as induced by Proposition 5.5.7.2 and $\{R_\gamma\}_{\gamma\in\Gamma(R)}$ is the universal grading of R.

Proof. That the maps are well-defined and mutually inverse can be easily deduced from Proposition 5.5.7. Both maps are functorial, and thus commute with the action of $\mathrm{Aut}(R)$. That they respect the partial order follows from Lemma 5.5.11. □

Definition 5.5.16. For a connected reduced order R with degree map $d\colon \mu \to \Gamma$ we write $U^*(R)$ or $U^*(d)$ for the group as in Definition 5.4.1.

Lemma 5.5.17. *Let R be a connected reduced order with degree map d. Let $\varphi\colon U^*(d) \to \mathrm{Aut}(d)$ be as in Lemma 5.4.2 and $\chi\colon \mathrm{Aut}(R) \to \mathrm{Aut}(d)$ as in Remark 5.5.14. We then have a commutative diagram*

$$\begin{tikzcd}
& U^*(d) \arrow[dl, "\psi"'] \arrow[dr, "\varphi"] & \\
\mathrm{Aut}(R) \arrow[rr, "\chi"] & & \mathrm{Aut}(d)
\end{tikzcd}$$

where ψ is a morphism given in terms of the universal grading $\{R_\gamma\}_{\gamma\in\Gamma}$ of R by $1 + f \mapsto (x \in R_\gamma \mapsto f(\gamma) \cdot x)$.

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

$$\begin{aligned}
x \in R_\gamma &\xmapsto{\psi(1+g)} g(\gamma)\cdot x \in R_{dg(\gamma)} \cdot R_\gamma \subseteq R_{dg(\gamma)\cdot\gamma} \\
&\xmapsto{\psi(1+f)} f(dg(\gamma)\cdot\gamma)\cdot g(\gamma)\cdot x = f(\gamma)g(\gamma)fdg(\gamma)\cdot x,
\end{aligned}$$

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

Let $1+f \in U^*$ and write $F = \psi(1+f)$. For $\zeta \in \mu$ we have $F(\zeta) = f(d\zeta)\zeta$, so $F|_{\mu(R)} = \mathrm{id}_\mu + fd$. For $\gamma \in \Gamma$ and $x \in R_\gamma$ non-zero we have $F(x) = f(\gamma)\cdot x$, so the induced action on Γ sends γ to $df(\gamma)\gamma$. Hence $1 + f$ gets sent to $\mathrm{id}_\Gamma + df$, since $\{\gamma \in \Gamma \mid R_\gamma \neq 0\}$ is a generating set of Γ by Lemma 4.2.4.5. We conclude that $\chi(\psi(1 + f)) = (\mathrm{id}_\mu + fd, \mathrm{id}_\Gamma + df) = \varphi(1 + f)$, as was to be shown. □

Example 5.5.18. The map $\psi\colon U^* \to \mathrm{Aut}(R)$ need not be injective, even when R is stark. Consider the subring $R = \mathbb{Z}\cdot(1, 1) + 2S$ of $S = \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}]$ where $\mathrm{i}^2 = -1$, which is clearly connected, reduced, and has $\mu(R) = \{\pm 1\} \times \{\pm 1\}$. Let $\Gamma = \mu(R)$ and write

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

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

Then $(\Gamma, (R_\gamma)_\gamma)$ is the universal grading of R. Consider the identity $\mathrm{id}\colon \Gamma \to \mu$. Note that $2\,\mathrm{id} = 0$ and $d = 0$, hence $(1+\mathrm{id})^2 = 1$ in Q and so $1+\mathrm{id} \in U^*$. Moreover, $\psi(1+\mathrm{id})$ is the identity of R, so ψ is not injective. To see R is stark, we can apply Lemma 5.7.1 below since $d = 0$.

Note that $U^*(R)$ acts on $\mathcal{D}(R)$ through $\mathrm{Aut}(R)$.

Theorem 5.5.19. *Let R be a connected reduced order and suppose (A, G), $(B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then $A \cong B$ as rings, $G \cong H$ as groups, and (A, G), (A, H), (B, G) and (B, H) are all in $\mathcal{D}(R)$ and in particular in the same $U^*(R)$-orbit.*

Proof. Let d be the degree map of R and let $\Phi\colon \mathrm{Dec}_{\mathcal{I}}(d) \to \mathcal{D}(R)$ be the map from Theorem 5.5.15. Suppose $(A, G), (B, H) \in \mathcal{D}(R)$ are such that A and B are stark. Then (A, G) and (B, H) are maximal elements of $\mathcal{D}(R)$ by Lemma 5.5.13, and thus $\Phi(A, G) = (d_0, d_1)$ and $\Phi(B, H) = (e_0, e_1)$ are maximal in $\mathrm{Dec}_{\mathcal{I}}(d)$. Then by Proposition 5.2.9.5 and Proposition 5.4.5 all of (d_0, d_1), (d_0, e_1), (e_0, d_1), and (e_0, e_1) are maximal and in the same U^*-orbit. Note that the action of U^* on $\mathrm{Dec}_{\mathcal{I}}(d)$ factors through $\mathrm{Aut}(R)$ by Lemma 5.5.17, so Φ respects the action of U^*. Since $\Phi(d_0, e_1) = (A, H)$ and $\Phi(e_0, d_1) = (B, G)$, the last assertion of the theorem follows. As a consequence, (A, G) and (B, H) are in the same orbit of $\mathrm{Aut}(R)$, so $A \cong B$ as rings and $G \cong H$ as groups. □

Example 5.5.20. Let $C_2 = \langle \sigma \rangle$ be a group of order 2 and let $R = \mathbb{Z}[\mathrm{i}][C_2]$, where $\mathrm{i}^2 = -1$. We will compute $\mathcal{D}(R)$.

By Proposition 5.5.2 the ring R is both reduced and connected. With $\Gamma = (\mathbb{Z}/2\mathbb{Z})^2$, consider the grading $(\Gamma, (R_{a,b})_{(a,b)})$ of R with $R_{a,b} = \mathbb{Z}\mathrm{i}^a\sigma^b$, where although i^a is not well-defined, $\mathbb{Z}\mathrm{i}^a$ is. Since a universal grading exists, and all $R_{a,b}$ are of rank 1 over $\mathbb{Z}$, this must be the universal grading. Let $d\colon \mu \to \Gamma$ be the degree map. It follows from Proposition 5.5.2.3 that $\mu = \langle \mathrm{i}, \sigma \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We will first compute $\mathrm{Dec}_{\mathcal{I}}(d)$. Suppose we have $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ with $d_i\colon \mu_i \to \Gamma_i$. If $\mu_1 = 1$, then $d_0 = d$, and (d_0, d_1) corresponds via Theorem 5.5.15 to the trivial element $(R, 1)$ of $\mathcal{D}(R)$. Now suppose $\mu_1 \neq 1$. Since d_1 is an isomorphism, the groups μ_1 and Γ_1 are isomorphic, so μ_1 is isomorphic to a direct summand of μ and of Γ. Since $\mathbb{Z}/2\mathbb{Z}$ is the greatest common divisor of μ and Γ as $\mathbb{Z}$-modules (in the sense of Definition 5.2.3), we have that μ_1 is a direct summand of μ isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It follows that $\mu_1 = \langle (-1)^b\sigma \rangle$ for some $b \in \mathbb{Z}/2\mathbb{Z}$, and the corresponding group Γ_1 equals $\langle (0,1) \rangle$ in both cases. On the other hand $\mu_0 = \langle \mathrm{i}\sigma^a \rangle$ for some $a \in (\mathbb{Z}/2\mathbb{Z})$ since it must be a cyclic group of order 4, and $\Gamma_0 = \langle(1, a)\rangle$. Upon inspection, all pairs (a, b) do indeed give a decomposition $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$. The rings corresponding to the possible d_0 are $\mathbb{Z}[\mathrm{i}\sigma^a]$, and the groups corresponding to d_1 are $\langle(-1)^b\sigma\rangle$. This gives

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

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

Example 5.5.21. The conclusion to Theorem 5.5.19 does not hold in general for non-connected reduced orders. Let C be a non-trivial finite abelian group and consider $R = \mathbb{Z}[C \times C] \times \mathbb{Z}[C]$. Let

$$\begin{aligned} A &= \mathbb{Z}[C \times 1] \times \mathbb{Z}, & G &= \{((1, \gamma), \gamma) \mid \gamma \in C\}, \\ B &= \mathbb{Z}[1 \times C] \times \mathbb{Z}, & H &= \{((\gamma, 1), \gamma) \mid \gamma \in C\}. \end{aligned}$$

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

5.6 Proofs of main theorems

In this section we prove Theorems 5.6.3 and 5.6.4 by reducing to the connected case, where we can apply Theorem 5.5.19. Recall the definition of $\mathcal{D}$ from Definition 5.5.9.

Lemma 5.6.1. *Let S and T be orders with S non-zero, let $R = S \times T$ with projection map $\pi\colon R \to S$, and let $(A, G) \in \mathcal{D}(R)$. Then we have $(\pi(A), \pi(G)) \in \mathcal{D}(S)$ and the restriction $G \to \pi(G)$ of π is a group isomorphism.*

Proof. We have a natural map $\pi(A)[G] \twoheadrightarrow \pi(A)[\pi(G)] \to S$. Since S equals $\pi(A[G]) = \sum_{g\in G} \pi(A)\pi(g)$, this map is clearly surjective. Suppose $\sum_{g\in G} \pi(a_g)g$ is in its kernel. Writing $e = (1, 0) \in R$ and identifying S with $S \times \{0\}$, we have $\pi(x) = ex$ for all $x \in R$. By Proposition 5.5.2.2 we have $e \in A$ and therefore $\sum_{g\in G} ea_g g = 0$ in $A[G]$. We conclude that for all $g \in G$ we have $\pi(a_g) = ea_g = 0$, so the map $\pi(A)[G] \to S$ is an isomorphism. Then the maps $\pi(A)[G] \to \pi(A)[\pi(G)]$ and $\pi(A)[\pi(G)] \to S$ are isomorphisms as well. Since $S \neq 0$, this implies that the map $G \to \pi(G)$ is an isomorphism and that $(\pi(A), \pi(G)) \in \mathcal{D}(S)$. □

Given a group ring structure on a product of orders, Lemma 5.6.1 constructs on each of the factors a group ring structure, with the same group. The following proposition does the opposite. For the definition of greatest common divisors, see Definition 5.2.3.

Proposition 5.6.2. *Let X be a finite non-empty set. For all $x \in X$ let R_x be a connected order, let $(A_x, G_x) \in \mathcal{D}(R_x)$, and suppose we write $G_x = D_x \oplus E_x$ for some subgroups $D_x, E_x \subseteq G_x$ such that for all $y, z \in X$ we have $D_y \cong D_z$. Consider*

$$R = \prod_{x\in X} R_x \quad \textit{and} \quad A = \prod_{x\in X} A_x[E_x], \quad \textit{and let} \quad D \subseteq \prod_{x \in X} D_x$$

be a subgroup for which all the projection maps $\pi_x \colon D \to D_x$ are isomorphisms. Then $(A, D) \in \mathcal{D}(R)$. If in addition (A_x, G_x) is maximal in $\mathcal{D}(R_x)$ for all $x \in X$, and D is a greatest common divisor of $\{G_x \,|\, x \in X\}$, then (A, D) is maximal in $\mathcal{D}(R)$.

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

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

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

Now suppose that (A_x, G_x) is maximal in $\mathcal{D}(R_x)$ for all $x \in X$, and that D is a greatest common divisor of $\{G_x \,|\, x \in X\}$. Let $(B, H) \in \mathcal{D}(R)$ be such that $(A, D) \leq (B, H)$. For $x \in X$ let B_x and H_x be the projection of B and H to R_x respectively. By Lemma 5.6.1 we have $(B_x, H_x) \in \mathcal{D}(R_x)$ and $H \cong H_x$. Choose $(C_x, I_x) \in \mathcal{D}(R_x)$ to be maximal such that $(B_x, H_x) \leq (C_x, I_x)$. Since R_x is connected, Lemma 5.5.11 implies that there exists a finite abelian group F_x such that $I_x \cong H_x \oplus F_x$. Since both (A_x, G_x) and (C_x, I_x) are maximal in $\mathcal{D}(R_x)$, we have $G_x \cong I_x$ by Theorem 5.5.19. Hence $G_x \cong I_x \cong H_x \oplus F_x \cong H \oplus F_x$. Thus H is a common divisor of all G_x, and H contains D. Since D is a greatest common divisor, we obtain $H = D$. From $A[D] = B[H] = B[D]$ and $A \supseteq B$ we see $A = B$, so $(A, D) = (B, H)$ and (A, D) is maximal. □

Theorem 5.6.3. *Suppose A and B are reduced orders and G and H are finite abelian groups. Then the following are equivalent:*

(i) *$A[G] \cong B[H]$ as rings,*

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

Proof. If $A = 0$ or $B = 0$, then Theorem 5.6.3 holds trivially. Hence assume A and B are non-zero. (ii ⇒ 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 ⇒ ii) First assume $A[G]$ is connected. Let $(C, V) \geq (A, G)$ and $(D, W) \geq (B, H)$ be a maximal element of $\mathcal{D}(A[G])$, respectively $\mathcal{D}(B[H])$. By Lemma 5.5.13 the orders C and D are stark, so by Theorem 5.5.19 there exists a ring isomorphism $\sigma\colon B[H] \to A[G]$ that sends (D, W) to (C, V). It follows that $(C, V) \geq (\sigma(B), \sigma(H))$, so applying Lemma 5.5.11 twice, we find subgroups I, $J \subseteq V$ such that $I \times G = V = J \times \sigma(H) \cong J \times H$ and $C[I] = A$ and $C[J] = \sigma(B) \cong B$. This concludes the proof of the connected case.

Next consider the general case, where $A[G] = \prod_{x \in X} R_x$ is a non-empty product of connected reduced orders R_x. Without loss of generality we may assume $A[G] = B[H]$. Let $x \in X$. Write A_x and B_x for the image of A, respectively B, of the projection onto R_x. Then $A_x[G] \cong R_x \cong B_x[H]$ by Lemma 5.6.1. Since R_x is connected and we proved (i ⇒ ii) in the connected case, there exist a reduced order C_x and finite abelian groups I_x and J_x such that $C_x[I_x] \cong A_x$ and $C_x[J_x] \cong B_x$ and $I_x \times G \cong J_x \times H = P_x$. Replacing C_x by $C_x[D_x]$ for some greatest common divisor D_x of I_x and J_x, we may assume that I_x and J_x are coprime. It follows that P_x is a least common multiple of G and H, as defined in Definition 5.2.3. In particular, when x ranges over X, the finite abelian groups P_x are pairwise isomorphic, and as a consequence the same holds for the groups I_x. Hence there exists a subgroup $I \subseteq \prod_{x \in X} I_x$ such that all projections $I \to I_x$ are isomorphisms, so from Proposition 5.6.2.1 it follows that $C[I] \cong A$ with $C = \prod_{x \in X} C_x$. Similarly we find a finite abelian group J that is isomorphic to all J_x such that $C[J] \cong B$. Now I and J together satisfy $I \times G \cong J \times H$, as desired. □

Theorem 5.6.4. *Let R be a non-zero reduced order. Then there exist a stark ring A, unique up to ring isomorphism, and a finite abelian group G, unique up to group isomorphism, such that $R \cong A[G]$ as rings.*

Proof. Let $(A, G) \in \mathcal{D}(R)$ be a maximal element (Lemma 5.5.10). Then A is stark by Lemma 5.5.13. Suppose B is a stark ring and H is a finite abelian group such that $B[H] \cong R$. By Theorem 5.6.3 there exist an order C and finite abelian groups I and J such that $A \cong C[I]$ and $B \cong C[J]$ and $I \times G \cong J \times H$. Since both A and B are stark we conclude that $I = J = 1$, so $G \cong H$ and $A \cong C \cong B$. Hence A and G are unique up to ring and group isomorphism, respectively. □

5.7 Automorphisms of group rings

In this section we will describe $\mathrm{Aut}(A[G])$, for a stark connected reduced order A with degree map d and a finite abelian group G, in terms of $U^*(d)$, G, and $\mathrm{Aut}(A)$. In this section we write $Q(A)$ for $Q(d)$ and similarly for U and U^* as defined in Definition 5.4.1. In our context $U^*(A)$ is equal to $U(A)$ due to the following.

Lemma 5.7.1. *Let A be a connected reduced order with degree map $d\colon \Gamma \to \mu$. Then the following are equivalent:*

(i) *A is stark;*

(ii) *d is nil;*

(iii) $\mathrm{Hom}(\Gamma, \mu) = \mathrm{nil}(Q(A))$*;*

(iv) $\mathrm{Hom}(\Gamma, \mu) = \mathrm{Jac}(Q(A))$*;*

(v) $U^*(A) = U(A)$*;*

Proof. We will write $Q = Q(A)$ and similarly for U and U^*.

(i $\Leftrightarrow$ ii) This follows from Theorem 5.5.15 and Lemma 5.3.7.4.

(ii $\Leftrightarrow$ iii) This follows immediately from the definition of nil and the multiplication on Q, and the fact that in general $\mathrm{nil}(Q) \subseteq \mathrm{Hom}(\Gamma, \mu)$.

(iii $\Rightarrow$ iv) Since $\mathrm{nil}(Q)$ is a nil two-sided ideal we have $\mathrm{Hom}(\Gamma, \mu) \subseteq \mathrm{nil}(Q) \subseteq \mathrm{Jac}(Q)$. The surjection $Q \twoheadrightarrow \mathbb{Z}$ must map $\mathrm{Jac}(Q)$ to $\mathrm{Jac}(\mathbb{Z}) = 0$, so in general $\mathrm{Jac}(Q) \subseteq \mathrm{Hom}(\Gamma, \mu)$, hence we have equality.

(iv $\Rightarrow$ v) We have $U = 1 + \mathrm{Jac}(Q) \subseteq Q^*$, so $U = U^*$.

(v $\Rightarrow$ iii) The involution $x \mapsto 1 - x$ on Q maps U to $\mathrm{Hom}(\Gamma, \mu)$. Hence both sets have the same number of idempotents, which by assumption is only 1 for U. Since $\mathrm{Hom}(\Gamma, \mu)$ is finite, every element has some power which is idempotent and hence 0, so $\mathrm{Hom}(\Gamma, \mu) \subseteq \mathrm{nil}(Q)$. The reverse inclusion holds in general. □

A category $\mathcal{C}$ is *small* if the class of objects of $\mathcal{C}$ is a set, and for any two objects A and B of $\mathcal{C}$ the class $\mathrm{Hom}(A, B)$ is a set. A category $\mathcal{C}$ is *preadditive* (see Section 1.2 in [4]) if for any two objects A and B of $\mathcal{C}$ the class $\mathrm{Hom}(A, B)$ is an abelian group such that composition of morphisms is bilinear, i.e. for all objects A, B, and C and morphisms $f, f'\colon A \to B$ and $g, g'\colon B \to C$ we have $g \circ (f + f') = (g \circ f) + (g \circ f')$ and $(g + g') \circ f = (g \circ f) + (g' \circ f)$.

Lemma 5.7.2. *Let $\mathcal{C}$ be a preadditive small category with precisely two objects $\mathbf{0}$ and $\mathbf{1}$. Then:*

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

2. *The product of groups*

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

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

3. *If* $M_{\mathbf{01}} \cdot M_{\mathbf{10}} = \mathrm{im}(M_{\mathbf{01}} \otimes M_{\mathbf{10}} \to M_{\mathbf{00}}) \subseteq \mathrm{Jac}(M_{\mathbf{00}})$*, then*

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

Proof. That the M_{ij} are groups, and that the addition is compatible with the composition of morphisms, follows from the fact that $\mathcal{C}$ is preadditive. It is then easy to verify that the M_{ij} are rings and modules as claimed, and that $\mathrm{M}(\mathcal{C})$ is a ring, giving 1 and 2.

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

$$\begin{aligned} (1 - snrm)(1 + snm) &= 1 - sn(r(1 + msn) - 1)m \\ &= 1 - sn(1 - 1)m = 1. \end{aligned}$$

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

$$T = \begin{pmatrix} \mathrm{Jac}(M_{\mathbf{00}}) & M_{\mathbf{01}} \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 \\ M_{\mathbf{10}} & \mathrm{Jac}(M_{\mathbf{11}}) \end{pmatrix}$$

and write $J = T + B$. We will first show that $T \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. For $x = \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \in T$ it suffices to show for all $y = \left(\begin{smallmatrix} r & m \\ n & s \end{smallmatrix}\right) \in \mathrm{M}(\mathcal{C})$ that $1 + xy \in \mathrm{M}(\mathcal{C})^*$. As $1 + xy = \left(\begin{smallmatrix} 1+ar+bn & ma+bs \\ 0 & 1 \end{smallmatrix}\right)$ is upper triangular, it is invertible if its diagonal elements are. The element $1 + ar + bn$ is invertible because $ar + bn \in \mathrm{Jac}(M_{\mathbf{00}})$, so $T \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. Analogously $B \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. Thus we have a two-sided ideal $J \subseteq \mathrm{Jac}(\mathrm{M}(\mathcal{C}))$. To see equality, note that the ring $\mathrm{M}(\mathcal{C})/J \cong (M_{\mathbf{00}}/\mathrm{Jac}(M_{\mathbf{00}})) \times (M_{\mathbf{11}}/\mathrm{Jac}(M_{\mathbf{11}}))$ has a trivial Jacobson radical. An element of $\mathrm{M}(\mathcal{C})$ is a unit if and only if it maps to a unit in $\mathrm{M}(\mathcal{C})/\mathrm{Jac}(\mathrm{M}(\mathcal{C}))$, hence if and only if its diagonal elements are units, proving the final statement. □

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

Remark 5.7.3. Given four abelian groups M_{ij} with $i, j \in \{0,1\}$ together with compatible (i.e. associative) multiplications $M_{ij} \otimes M_{jk} \to M_{ik}$ for all $i, j, k \in \{0,1\}$ with appropriate unit elements, we can construct the preadditive category $\mathcal{C}$ with two objects 0 and 1, with $\mathrm{Hom}(j,i) = M_{ij}$, and with composition being these multiplications. In particular, if M_{00} and M_{11} are rings, M_{01} is an M_{00}-M_{11}-bimodule, and M_{10} is an M_{11}-M_{00}-bimodule, then it remains only to specify the multiplications $M_{01} \otimes M_{10} \to M_{00}$ and $M_{10} \otimes M_{01} \to M_{11}$.

Let A be a connected reduced order and G a finite abelian group. Recall that $\mu(A)$ and $\Gamma(A)$ are $Q(A)$-modules by Remark 5.4.3, hence $\mathrm{Hom}(G, \mu(A))$ and $\mathrm{Hom}(\Gamma(A), G)$ are respectively left and right $Q(A)$-modules. We next describe $U^*(A[G])$ in terms of A and G.

Proposition 5.7.4. *Let A be a connected reduced order and G a finite abelian group. Then:*

1. *We have a matrix ring*

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

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

2. *There is a natural ring isomorphism $E \xrightarrow{\sim} Q(A[G])$ that respects the action of* $\mathrm{Aut}(A)$.
3. *If A is stark, then the map in 2 restricts to an isomorphism*

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

Proof. 1. Apply Remark 5.7.3 and Lemma 5.7.2.2. Since all multiplications are defined in terms of compositions of morphisms, the associativity conditions are trivially satisfied.

2. Write $\Gamma = \Gamma(A)$ and $\mu = \mu(A)$. We have by Proposition 5.5.7.ii that

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

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

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

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

3. Suppose A is stark. Then $\mathrm{Hom}(\Gamma,\mu) = \mathrm{Jac}(Q(A))$ by Lemma 5.7.1. It follows that the ideal $\mathrm{Hom}(G,\mu) \cdot \mathrm{Hom}(\Gamma,G) \subseteq \mathrm{Hom}(\Gamma,\mu)$ is contained in $\mathrm{Jac}(Q(A))$. Now apply Lemma 5.7.2.3. □

In Remark 5.7.5 and Proposition 5.7.6 we describe $\mathrm{Aut}(A[G])$ in terms of A and $U^*(A[G])$.

Remark 5.7.5. Let G be a finite abelian group. Then $-[G]$ and U^* act functorially on isomorphisms of connected reduced orders. Let A be a connected reduced order. From Proposition 5.5.7.ii we get a natural inclusion $\mathrm{Hom}(\Gamma(A), \mu(A)) \to \mathrm{Hom}(\Gamma(A[G]), \mu(A[G]))$, which extends to an inclusion of rings $Q(A) \to Q(A[G])$. Then we have a commutative diagram

$$\begin{tikzcd}
U^*(A) \arrow[r, "\text{Lem 5.5.17}"] \arrow[d, tail] & \mathrm{Aut}(A) \arrow[r, "U^*"] \arrow[d, tail, "-[G]"] & \mathrm{Aut}(U^*(A)) \\
U^*(A[G]) \arrow[r, "\text{Lem 5.5.17}"] & \mathrm{Aut}(A[G]) \arrow[r, "U^*"] & \mathrm{Aut}(U^*(A[G])),
\end{tikzcd}$$

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

Proposition 5.7.6. *Let A be a stark connected reduced order and G a finite abelian group. Then the maps and actions from Remark 5.7.5 fit in an exact sequence*

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

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

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

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

by Remark 5.7.5, so ι is a homomorphism. Moreover, ι is injective because it maps injectively to the first factor. By the same lemma π is a homomorphism.

We will now show that π is surjective. Suppose $\sigma \in \mathrm{Aut}(A[G])$. By Theorem 5.5.19 there exists $1+f \in U^*(A[G])$ that maps (A, G) to $(\sigma(A), \sigma(G))$, so without loss of generality we may assume $\sigma(A) = A$ and $\sigma(G) = G$. By applying the restriction $\sigma|_A \in \mathrm{Aut}(A)$ we may assume σ is the identity on A. Consider the map $f\colon \Gamma(A) \times G \to \mu(A[G])$ given by $(\delta, g) \mapsto \sigma(g)g^{-1}$ and note that $1 + f \in U(A[G])$ gets mapped to σ. We similarly obtain the inverse of $1 + f$ in $U(A[G])$ from $(\delta, g) \mapsto \sigma^{-1}(g)g^{-1}$, so $1 + f \in U^*(A[G])$. It follows that σ is in the image of π and thus π is surjective.

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

Proposition 5.7.4 and Proposition 5.7.6 combined gives us a description of $\mathrm{Aut}(A[G])$ in terms of A and G. We now prove Theorem 5.7.8 and describe $\mathrm{Aut}(A[G])$ by less canonical means.

Lemma 5.7.7. *Let A be a stark connected reduced order. Then the group $\mathrm{Hom}(\Gamma(A), \mu(A))$ has a (right) action on the set $\mathrm{Aut}(A)$, which for $\alpha \in \mathrm{Aut}(A)$ and $f \in \mathrm{Hom}(\Gamma(A), \mu(A))$ is given by*

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

Proof. Let $\alpha \in \mathrm{Aut}(A)$ and $f, g \in \mathrm{Hom}(\Gamma(A), \mu(A))$. Note that $\alpha + f = \alpha \circ (1 + \alpha^{-1}f) \in \mathrm{Aut}(A)$, where $1 + \alpha^{-1}f \in U(A) = U^*(A)$ by Lemma 5.7.1 and the composition is taken inside $\mathrm{Aut}(A)$ via Lemma 5.5.17. For $\gamma \in \Gamma(A)$ and $x \in A_\gamma$ we clearly have

$$\begin{aligned}[(\alpha + f) + g](x) &= [\alpha + f](x) \cdot g(\gamma)\\ &= \alpha(x) \cdot f(\gamma) \cdot g(\gamma)\\ &= [\alpha + (f + g)](x),\end{aligned}$$

so the action is well-defined. □

Theorem 5.7.8. *Let A be a stark connected reduced order with degree map $d_A\colon \mu \to \Gamma$ and let G be a finite abelian group. We equip the cartesian product*

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

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

$$\begin{pmatrix} \alpha_1 & s_1 \\ t_1 & \sigma_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & s_2 \\ t_2 & \sigma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 + s_1t_2 & \alpha_1 s_2 + s_1\sigma_2 \\ t_1\alpha_2 + \sigma_1 t_2 & t_1 d_A s_2 + \sigma_1\sigma_2 \end{pmatrix},$$

where the sum in $\mathrm{Aut}(A)$ *is as in Lemma 5.7.7 and the sum in* $\mathrm{Aut}(G)$ *is taken inside* $\mathrm{End}(G)$*. For $x \in A$ and $g \in G$ write $\left(\begin{smallmatrix} x \\ g \end{smallmatrix}\right)$ for the element $x \cdot g \in A[G]$. Then:*

1. *M is a group;*
2. *there is a natural isomorphism $M \xrightarrow{\sim} \mathrm{Aut}(A[G])$ such that the evaluation map $M \times A[G] \to A[G]$ is given by*

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

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

Proof. To check that M is a group it remains to verify that $t_1 d s_2 + \sigma_1\sigma_2 \in \mathrm{Aut}(G)$. This follows from Lemma 5.7.1, namely $t_1 d s_2 \in \mathrm{Jac}(\mathrm{End}(G))$. Note that the map $\vartheta\colon M \to \mathrm{Aut}(A[G])$ can be written as the composition of the homomorphism $\varphi\colon M \to U^*(A[G]) \rtimes \mathrm{Aut}(A)$ given by

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

where $U^*(A[G])$ is written in terms of the matrix representation of Proposition 5.7.4, and the homomorphism $\pi\colon U^*(A[G]) \rtimes \mathrm{Aut}(A) \to \mathrm{Aut}(A[G])$ from Proposition 5.7.6. The map π is still surjective when restricted to the image of φ. Namely any $\left(\begin{smallmatrix} u & s \\ t & \sigma \end{smallmatrix}\right) \cdot \alpha \in U^*(A[G]) \rtimes \mathrm{Aut}(A)$ has the same image as $\left(\begin{smallmatrix} 1 & s \\ t\beta^{-1} & \sigma \end{smallmatrix}\right) \cdot \beta\alpha$, where β is the image of u in $\mathrm{Aut}(A)$. Hence the map ϑ is surjective. By Proposition 5.7.4.3 and Proposition 5.7.6, respectively, we have

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

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

5.8 Algorithms

In this section we will prove Theorem 5.8.4, the algorithmic counterpart to Theorem 5.6.4.

Lemma 5.8.1. *For each of $R = \mathbb{Z}$ and $R = \left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix}\right)$ there exists a polynomial-time algorithm that, given finite R-modules M_1 and M_2, computes a greatest common divisor D of M_1 and M_2 as defined in Definition 5.2.3, together with injections $\iota_i\colon D \to M_i$ and a complement $N_i \subseteq M_i$ such that $N_i \oplus \iota_i D = M_i$.*

Proof. By Theorem 2.6.9 in [5] we may compute the exponents of M_1 and M_2, and their least common multiple n, in polynomial time. Note that M_1 and M_2 are R/nR-modules and that replacing R by R/nR does not change the problem. Since R/nR is a finite ring, the problem reduces to Theorem 4.1.1 in [5]. □

Proposition 5.3.2 allows us to interpret a morphism of finite abelian groups as a finite length $\left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix}\right)$-module. Although both types of objects are represented differently, one easily deduces from the proof of Proposition 5.3.2 that we can change representations in polynomial time.

In the following result, $\operatorname{Dec}_{\mathcal{I}}(d)$ is as defined in Definition 5.2.8, Remark 5.3.4, and Definition 5.3.3.

Proposition 5.8.2. *There exists a polynomial-time algorithm that, given finite abelian groups A and B and a morphism $d\colon A \to B$, computes a maximal element of $\operatorname{Dec}_{\mathcal{I}}(d)$.*

Proof. By Lemma 5.8.1 we may compute in polynomial time a greatest common divisor D of A and B as $\mathbb{Z}$-modules. Similarly we may compute a greatest common divisor E of d and id_D as $\left(\begin{smallmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{smallmatrix}\right)$-modules. We also obtain submodules d_0 and d_1 of d such that $d_1 \cong E$ and $d = d_0 \oplus d_1$. We claim that (d_0, d_1) is a maximal element of $\operatorname{Dec}_{\mathcal{I}}(d)$.

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 $(d_0, d_1) \in \operatorname{Dec}_{\mathcal{I}}(d)$. Let $(e_0, e_1) \geq (d_0, d_1)$ be maximal in $\operatorname{Dec}_{\mathcal{I}}(d)$. Since e_1 is an isomorphism, it is isomorphic to id_F for some finite abelian group F. Since e_1 is a direct summand of d, the group F is a direct summand of both A and B, so F is a divisor of their greatest common divisor D. Thus e_1 is a divisor of id_D. It follows that e_1

is a divisor of $E \cong d_1$, so $(d_0, d_1) = (e_0, e_1)$ and thus (d_0, d_1) is maximal, as was to be shown. □

Recall that we have specified an encoding for gradings of orders in Section 4.7.

Proposition 5.8.3. *There exists a polynomial-time algorithm that, given a reduced order R and a universal grading of R, computes a maximal element of $\mathcal{D}(R)$ as defined in Definition 5.5.9.*

Proof. First suppose R is connected. By Theorem 1.2 in [32] we may compute $\mu = \mu(R)$ in polynomial time and thus also the group homomorphism $d\colon \mu \to \Gamma$ as defined in Definition 5.5.6. We may compute a maximal element $(d_0, d_1) \in \mathrm{Dec}_{\mathcal{I}}(d)$ with $d_i\colon \mu_i \to \Gamma_i$ in polynomial time using Proposition 5.8.2. Under the isomorphisms of partially ordered sets of Theorem 5.5.15 this d corresponds to a maximal element $(A, G) \in \mathcal{D}(R)$, where $A = \sum_{\gamma \in \Gamma_0} R_\gamma$ and $G = \mu_1$, which we may compute in polynomial time.

Now consider the general case. By Theorem 1.1 in [32] we may compute in polynomial time connected reduced orders $\{R_x\}_{x \in X}$ for some index set X such that $R \cong \prod_{x \in X} R_x$, together with the projections $\pi_x\colon R \to R_x$. Using Proposition 4.2.6 we may construct universal gradings for the R_x in polynomial time. Hence by the special case we may compute a maximal element of $\mathcal{D}(R_x)$ for all $x \in X$ in polynomial time. Finally, we may apply Proposition 5.6.2 to compute a maximal element of $\mathcal{D}(R)$, observing that the construction in Proposition 5.6.2 can be carried out in polynomial time using Lemma 5.8.1. □

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

Theorem 5.8.4. *There is an algorithm that, given a non-zero reduced order R, computes a stark subring $A \subseteq R$ and a subgroup $G \subseteq \mu(R)$ such that $A[G] = R$. This algorithm runs* (a) *in polynomial time when the additive group of R is generated by autopotents, and generally* (b) *in time $n^{O(m)}$ where n is the length of the input and m is the number of minimal prime ideals of R.*

Proof. We compute the universal grading of R. For (a), we use Theorem 4.7.13, while for (b) we use Theorem 1.4 in [17]. The theorem now follows from Proposition 5.8.3. □