D.M.H. van Gent

Algorithms for finding the gradings of reduced rings

Master thesis

3 July 2019

Thesis supervisor: Prof. Dr. H.W. Lenstra Jr

Leiden University
Mathematical Institute

Contents

1 Introduction

In this thesis we will study gradings of $\mathbb{Q}$-algebras and *orders*, which are commutative rings for which the additive group is isomorphic to $\mathbb{Z}^r$ for some $r \in \mathbb{Z}_{\geq 0}$. An element x of a ring R is called *nilpotent* if $x^n = 0$ for some integer $n \geq 1$, and R is called *reduced* if 0 is the only nilpotent of R. In [1], H.W. Lenstra and A. Silverberg showed that each reduced order has a universal grading, for which we also give an alternative proof (Theorem 6.21). Our goal is to present an algorithm to compute this universal grading in polynomial time once we bound the size of the minimal spectrum of the order.

Definition 1.1. Let k be a commutative ring. A *decomposition* of a k-module M is a family of k-submodules $\{M_s\}_{s\in S}$ indexed by some set S such that the natural map $\bigoplus_{s\in S} M_s \to M$ is an isomorphism. For any decomposition $\{M_s\}_{s\in S}$ and map $f : S \to T$ we define $f_*(\{M_s\}_{s\in S}) = \{\sum_{s\in f^{-1}t} M_s\}_{t\in T}$, which is again a decomposition of M. We say a decomposition $\mathcal{M}$ is a *refinement* of a decomposition $\mathcal{N}$, written $\mathcal{N} \preceq \mathcal{M}$, if there exists a map f such that $f_*\mathcal{M} = \mathcal{N}$. A *pre-grading* of a k-algebra R is a decomposition $\{R_s\}_{s\in S}$ of R as k-module such that for all $s, t \in S$ there exists some $u \in S$ such that $R_s \cdot R_t \subseteq R_u$.

With $R = k[X]$, an example of a pre-grading would be the decomposition $\{kX^i\}_{i\in\mathbb{Z}_{\geq 0}}$, since $kX^i \cdot kX^j \subseteq kX^{i+j}$. For the order $\mathbb{Z}[\sqrt{2}]$ one can take $\{\mathbb{Z}\sqrt{2^i}\}_{i\in\mathbb{Z}/2\mathbb{Z}}$, where $\mathbb{Z}\sqrt{2^i}$ is well defined since $\sqrt{2^2} \in \mathbb{Z}$. In both examples, the index set S comes equipped with a binary operator $* : S^2 \to S$ satisfying $R_s \cdot R_t \subseteq R_{s*t}$. This is not a surprise, since if $R_s \cdot R_t \neq 0$, then any $u \in S$ such that $R_s \cdot R_t \subseteq R_u$ must be unique if it exists.

Definition 1.2. Let k be a commutative ring and R be a (not necessarily commutative) k-algebra. A *group-grading of* R is a triple $\overline{R} = (R, G, \mathcal{R})$ with G a group and $\mathcal{R} = \{R_g\}_{g\in G}$ a G-indexed pre-grading of R, such that $1 \in R_1$ and for all $g, h \in G$ we have $R_g \cdot R_h \subseteq R_{gh}$. For brevity we call $\overline{R}$ a *G-grading* when $\overline{R}$ is a group-grading with the group G as index set. We call a G-grading an *abelian group-grading* if G is an abelian group. For any morphism of groups $\varphi : G \to H$ we define $\varphi_*(\overline{R}) = (R, H, \varphi_*(\mathcal{R}))$, which is again a grading. The class of gradings of R forms a category (see Appendix A) where the *morphisms* $\varphi : \overline{R} \to \overline{S}$ are simply the morphisms of groups such that $\varphi_*(\overline{R}) = \overline{S}$.

The pre-grading $\{\mathbb{Z}\sqrt{2^i}\}_{i\in\mathbb{Z}/2\mathbb{Z}}$ of $\mathbb{Z}[\sqrt{2}]$ trivially becomes a $\mathbb{Z}/2\mathbb{Z}$-grading. For $k[X]$ we may take $R_i = kX^i$ when $0 \leq i$ and $R_i = 0$ when $i < 0$ to turn $\{R_i\}_{i\in\mathbb{Z}}$ into a $\mathbb{Z}$-grading. We say a group-grading $\overline{U}$ of R is *universal* if it is an initial object in the category of group-gradings of R. Concretely, this means that $\overline{U}$ is the finest grading of R possible. By Yoneda's lemma, having a universal grading is equivalent to having a representation of the functor $F : \mathtt{Grp} \to \mathtt{Set}$ that sends each group G to the set of G-gradings of R. We analogously define a universal abelian group-grading by considering the category of abelian group gradings of R instead. We cannot expect in general that a universal grading exists (Example 2.15). However, for reduced orders a universal abelian group-grading always exists [1]. Since the grading of $\mathbb{Z}[\sqrt{2}]$ we gave earlier cannot be further refined, we must conclude that it is a universal abelian group-grading.

For our algorithms, k will either be $\mathbb{Z}$ or $\mathbb{Q}$, elements of which have an obvious binary encoding. Additionally, R will either be a reduced order or reduced commutative $\mathbb{Q}$-algebra, which both are free k-modules. Elements of k^n are simply represented by a list of n elements of k and a morphism of k-modules $f : k^m \to k^n$ is represented as a matrix in $k^{n\times m}$. Submodules M of k^n are represented by any injection $f : k^m \to k^n$ with image M. For k-algebras free of rank n as k-module we additionally encode the multiplicative structure by structure constants $(a_{hij})_{hij} \in k^{n\times n\times n}$ such that $e_h \cdot e_i := \sum_{j=1}^n a_{hij} e_j$ for all $1 \leq h, i \leq n$, with e_i the i-th standard basis vector of k^n. We encode a finite abelian group by its entire multiplication table and we then get an obvious encoding for our gradings. Now that we have specified our encoding we can formally talk about algorithmic complexity.

We call a prime ideal $\mathfrak{p}$ of a commutative ring R *minimal* if for all prime ideals $\mathfrak{q} \subseteq \mathfrak{p}$ we have $\mathfrak{p} = \mathfrak{q}$, and write $\operatorname{minspec} R$ for the set of minimal prime ideals of R.

Theorem 1.3. *There is a deterministic algorithm that takes a pair (E, q) as input, where E is a reduced commutative $\mathbb{Q}$-algebra and q is a prime power, and produces all $\mathbb{Z}/q\mathbb{Z}$-gradings of E in time $n^{O(m)}$, where n is the length of the input and $m = \# \operatorname{minspec} E$.*

Our main result is the following.

Theorem 1.4. *There is a deterministic algorithm that takes a reduced order R as input and produces a universal abelian group grading of R in time $n^{O(m)}$, where n is the length of the input and $m = \#\operatorname{minspec} R$.*

If we bound the size of the minimal spectrum by a constant, the above algorithms run in polynomial time. For example, when R is a domain, or equivalently an order in a number field, then $\#\operatorname{minspec} R = 1$ and thus is the algorithm polynomial. For the proof of Theorem 1.3 and Theorem 1.4, see Section 7.2 respectively Section 7.3.

Example 1.5. One might be tempted to think that all group-gradings of a commutative ring are abelian group-gradings. Indeed, for a G-grading $\overline{R}$ we have $R_g \cdot R_h \subseteq R_{gh} \cap R_{hg}$ for all $g, h \in G$, so if $R_g \cdot R_h \neq 0$ we have $R_{gh} = R_{hg} \neq 0$ and thus $gh = hg$. If R is not necessarily a domain, say $R = \mathbb{Z}[\sqrt{2}]^2$, we may provide a counterexample. Let $G = \operatorname{Aut}_{\texttt{Set}}(\{1, 2, 3\})$ be the symmetric group of degree 3 and define $R_1 = \mathbb{Z} \times \mathbb{Z}$, $R_{(1\,2)} = (\mathbb{Z}\sqrt{2}) \times 0$, $R_{(2\,3)} = 0 \times (\mathbb{Z}\sqrt{2})$ and $R_g = 0$ for all other $g \in G$. Then $(R, G, \{R_g\}_{g\in G})$ is a non-abelian group-grading of a commutative ring. We can give a $(\mathbb{Z}/2\mathbb{Z})^2$-grading $\overline{S}$ of R with $S_{(0,0)} = R_1$, $S_{(1,0)} = R_{(1\,2)}$, $S_{(0,1)} = R_{(2\,3)}$ and $S_{(1,1)} = 0$ that has the same non-zero components as $\overline{R}$ but has an abelian group. Moreover, there exists no morphism f between the groups G and $(\mathbb{Z}/2\mathbb{Z})^2$ in either direction such that $f_*\overline{R} = \overline{S}$ or $f_*\overline{S} = \overline{R}$.

We consider Example 1.5 as evidence that there perhaps is a structure that is better suited to grade a ring than a group. Another piece of evidence is Example 2.16.

Definition 1.6. A *grid* is a quadruple $G = (S, 1, D, *)$, where S is a set containing 1, such that $D \subseteq S^2$ satisfies $(1, s), (s, 1) \in D$ for all $s \in S$ and $* : D \to S$ is a binary operator such that for all $s \in S$ we have $s * 1 = 1 * s = s$, and $s * s = s$ implies $s = 1$. Through abuse of notation we will often write $g \in G$ where we mean $g \in S$. We say G is *abelian* when for all $(s, t) \in D$ we have $(t, s) \in D$ and $s * t = t * s$. With $H = (T, 1, E, \star)$ another grid, a *morphism* from G to H is a map $f : S \to T$ such that for all $(s, t) \in D$ we have $(f(s), f(t)) \in E$ and $f(s * t) = f(s) \star f(t)$.

It follows immediately that $f(1) = 1$ for all grid morphisms f from the fact that 1 is the only idempotent. The class of grids forms a category `Grd`, which contains the category of groups as a full subcategory.

Example 1.5 (continued)**.** An example of a grid would be the grid V on the elements $\{1, a, b\}$ such that $a * a = b * b = 1$ and $a * b$ and $b * a$ are undefined. One can informally view this grid as $(\mathbb{Z}/2\mathbb{Z})^2 = \{1, a, b, ab\}$ with ab and all products resulting in ab removed. We have grid morphisms $f : V \to (\mathbb{Z}/2\mathbb{Z})^2$ given by $a \mapsto (1, 0)$ and $b \mapsto (0, 1)$, and $g : V \to G = \operatorname{Aut}_{\texttt{Set}}(\{1, 2, 3\})$ given by $a \mapsto (1\,2)$ and $b \mapsto (2\,3)$. The ring $\mathbb{Z}[\sqrt{2}]^2$ similarly has a V-grading $\overline{T}$ under the proper definition of a grid-grading, which extends the definition of a group-grading, and the $(\mathbb{Z}/2\mathbb{Z})^2$-grading $\overline{S}$ and G-grading $\overline{R}$ of $\mathbb{Z}[\sqrt{2}]^2$ can be obtained as $f_*\overline{T}$ and $g_*\overline{T}$.

Definition 1.7. Let k be a commutative ring and R a k-algebra. A *grid-grading* of R is a triple $\overline{R} = (R, G, \mathcal{R})$ with G a grid and $\mathcal{R} = \{R_g\}_{g\in G}$ a G-indexed pre-grading of R, which satisfies $1 \in R_1$ and additionally for all $g, h \in G$ such that $R_g \cdot R_h \neq 0$ we have that $g * h$ is defined and $R_g \cdot R_h \subseteq R_{g*h}$. We call $\overline{R}$ an *abelian grid-grading* if G is an abelian grid. For any morphism of grids $f : G \to H$ we define $f_*(\overline{R}) = (R, H, f_*(\mathcal{R}))$, which is again a grading.

The proof of [1] generalizes effortlessly, which we present in Section 6.3.

Theorem 1.8. *Let R be a reduced order. Then R has a universal abelian group-grading* [1]*, a universal group-grading and a universal grid-grading.*

Using this theorem it is now not difficult to see that $\overline{T}$ from Example 1.5 is a universal grid-grading. For Theorem 1.8 to work we require the somewhat artificial property of grids that 1 is the only idempotent. If we drop this property, then the pre-grading $\{R_s\}_{s\in\{0,1\}}$ of $\mathbb{Z}^2$ with $R_1 = (1, 1)\mathbb{Z}$ and $R_0 = (1, 0)\mathbb{Z}$ can be turned into a 'grid'-grading $\overline{R}$. If a universal grading should still exist, then $\overline{R}$ must be it since it cannot be refined, but reversing the coordinates of $\mathbb{Z}^2$ gives a different 'grid'-grading $\overline{R}'$ of $\mathbb{Z}^2$ between the two of which no mapping exists.

With some more effort, we also generalize Theorem 1.4.

Theorem 1.9. *There is a deterministic algorithm that takes a reduced order R as input and produces a universal grid grading $\overline{U} = (R, \Upsilon, \{U_v\}_{v \in \Upsilon})$ of R in time $n^{O(m)}$, where n is the length of the input and $m = \#\operatorname{minspec} R$. There is a deterministic algorithm that takes this $\overline{U}$ as input and produces a finite presentation of a group Γ and a morphism of grids $f : \Upsilon \to \Gamma$ such that $f_*\overline{U}$ is a universal group grading of R in time $n^{O(1)}$.*

Note that the algorithm of Theorem 1.9 does not compute $f_*\overline{U}$. The finitely presented group Γ will generally not be finite, as for $\mathbb{Z}[\sqrt{2}]^2$ as in Example 1.5 it is $\langle a, b \mid a^2 = b^2 = 1 \rangle$ by Proposition 6.7. Hence the algorithm only returns a presentation. More importantly, we are thus far unable to explicitly compute the decomposition of R corresponding to the grading $f_*\overline{U}$ as it requires us to solve the word problem in Γ, which for general groups is undecidable [2]. We know of no algorithm that given f, $\overline{U}$ and $x \in R$ decides whether x is homogeneous in $f_*\overline{U}$, i.e. there is some $\gamma \in \Gamma$ such that $x \in \sum_{v \in f^{-1}\gamma} U_v$.

2 Graded rings

In this section we derive some properties of grids and gradings and introduce some tools to construct gradings from smaller gradings. This is followed by some examples highlighting the difference between gradings graded with grids, groups and abelian groups.

2.1 Basic properties

In this section k will be a commutative ring and R will be a (not necessarily commutative) k-algebra. For each grid-grading $\overline{R} = (R, G, \{R_g\}_{g\in G})$ the k-module R_1 is closed under multiplication and contains 1, and is thus a k-subalgebra of R. Similarly R_g is an R_1-R_1-bimodule for all $g \in G$. We will use this fact without reference.

Definition 2.1. Let $G = (S, 1, D, *)$ be a grid. We call a $(T, 1, E, \star)$ a *subgrid* of G if it is a grid such that $T \subseteq S$, $E = D \cap T^2$ and $s \star t = s * t$ for all $(s,t) \in E$. For $X \subseteq S$ we write $\langle X\rangle_{\texttt{Grd}}$ or simply $\langle X\rangle$ for the smallest subgrid of G containing X.

We similarly write $\langle X\rangle_{\texttt{Grp}}$ and $\langle X\rangle_{\texttt{Ab}}$ for the smallest subgroup respectively abelian subgroup containing X. Note that if G is a group, the notation $\langle X\rangle$ has become ambiguous. For $G = \mathbb{Z}$, we have $\langle 1\rangle_{\texttt{Grd}} = \mathbb{Z}_{\geq 0}$ while $\langle 1\rangle_{\texttt{Grp}} = \mathbb{Z}$.

Definition 2.2. Let $\mathcal{C} \in \{\texttt{Grd}, \texttt{Grp}, \texttt{Ab}\}$ and let $\overline{R} = (R, G, \mathcal{R})$ be a $\mathcal{C}$-grading of R. We say $\overline{R}$ is *efficient* if $G = \langle g \in G \,|\, R_g \neq 0\rangle_{\mathcal{C}}$ and say $\overline{R}$ is *loose* if $R_g \cdot R_h \neq 0$ for all $g, h \in G$ such that $\{g, h\} \neq \{1\}$ and $g * h$ is defined.

Note that whether a grading is efficient depends on the underlying category. By the same argument as before a group-grading can be efficient as group-grading but be not efficient as grid-grading. Note that a loose grading is necessarily efficient.

Lemma 2.3. *Let $\mathcal{C} \in \{\texttt{Grd}, \texttt{Grp}, \texttt{Ab}\}$ and let $\overline{R} = (R, G, \{R_g\}_{g\in G})$ be an efficient $\mathcal{C}$-grading. If $H \in \operatorname{obj}(\mathcal{C})$ and morphisms $\varphi, \psi : G \to H$ satisfy $\varphi_*\overline{R} = \psi_*\overline{R}$, then $\varphi = \psi$.*

Proof. Since $\varphi_*\overline{R} = \psi_*\overline{R}$, we must have that φ and ψ agree on $X = \{g \in G \,|\, R_g \neq 0\}$. Let $K = \{x \in G \,|\, \varphi(x) = \psi(x)\} \supseteq X$. For $x, y \in K$ such that $x * y$ is defined we have $\varphi(x * y) = \varphi(x)\varphi(y) = \psi(x)\psi(y) = \psi(x * y)$, so $x * y \in K$ and K is a subgrid of G. Additionally, if G is a group K is also closed under taking inverses, making K a subgroup of G. It follows that $K \subseteq G = \langle X\rangle_{\mathcal{C}} \subseteq K$ since $X \subseteq K$, so $\varphi = \psi$. □

Proposition 2.4. *Let $\mathcal{C} \in \{\texttt{Grd}, \texttt{Grp}, \texttt{Ab}\}$ and let $\overline{R} = (R, G, \{R_g\}_{g\in G})$ be a $\mathcal{C}$-grading. Let $H = \langle g \in G \,|\, R_g \neq 0\rangle_{\mathcal{C}}$ and let $\varphi : H \to G$ be the inclusion. Then $\overline{S} = (R, H, \{R_h\}_{h\in H})$ is an efficient $\mathcal{C}$-grading such that $\varphi_*\overline{S} = \overline{R}$. If for each $\mathcal{C}$-grading $\overline{T}$ there exists a morphism $\psi_* : \overline{R} \to \overline{T}$, then $\overline{S}$ is a universal grading. Moreover, universal $\mathcal{C}$-gradings are efficient.*

Proof. It is an easy verification that $\overline{S}$ is a grading and that $\varphi_*\overline{S} = \overline{R}$. If morphisms $\psi_* : \overline{R} \to \overline{T}$ exist for all $\mathcal{C}$-gradings $\overline{T}$, then the same holds for $\overline{S}$ by composition with φ_*. Then by Lemma 2.3 such a map is unique, hence $\overline{S}$ is universal. If $\overline{R}$ was already universal, then there exists a morphism $\psi : G \to H$ such that $(\varphi \circ \psi)_*\overline{R} = \overline{R}$, hence $\varphi \circ \psi = \mathrm{id}_G$ by uniqueness of morphisms. Similarly $\psi \circ \varphi = \mathrm{id}_H$, hence $\overline{R} = \overline{S}$ and $\overline{R}$ is efficient. □

Proposition 2.4 allows us to restrict ourselves to the category of efficient gradings when looking for a universal grading, since each grading is the image of an efficient grading under some morphism.

Remark 2.5. Note that by the definition of a grid grading, if $R_{\gamma_1} \cdots R_{\gamma_m} \neq 0$ for $\gamma_1, \ldots, \gamma_m \in \Gamma$, then $\gamma_1 * \cdots * \gamma_m$ is uniquely defined regardless of grouping of factors. In particular, if $x \in R_\gamma$ is not nilpotent then $0 \neq R_\gamma \cdots R_\gamma$ and thus γ^n is uniquely defined for all $n \geq 0$.

We call an element x of a ring R *regular* if for all $y \in R$ such that $xy = 0$ or $yx = 0$ we have $y = 0$. Any $x \in R$ that is not regular is called a *zero-divisor*.

Proposition 2.6. *Let $\overline{R} = (R, \Gamma, \{R_\gamma\}_{\gamma\in\Gamma})$ be a grid-grading of a reduced (not necessarily commutative) algebra R over a commutative ring k such that $X = \{\gamma \in \Gamma \mid R_\gamma \neq 0\}$ is finite. Then the following holds.*

1. *For each $\gamma \in X$ we have that $\langle\gamma\rangle_{\mathtt{Grd}} \subseteq X$ is a finite cyclic group.*
2. *If R_1 is a domain, then for each $\gamma \in \Gamma$ all non-zero $x \in R_\gamma$ are regular, and $X = \langle X\rangle_{\mathtt{Grd}}$ is a group. If additionally R is commutative, then X is abelian.*
3. *If R_1 is a field, then for each $\gamma \in \Gamma$ all non-zero $x \in R_\gamma$ are invertible with $x^{-1} \in R_{\gamma^{-1}}$. Additionally, $\dim_{R_1} R_\gamma = 1$ for all $\gamma \in X$.*

Proof. (1) Let $\gamma \in \Gamma$ be such that $R_\gamma \neq 0$. Then γ^n is uniquely defined for all $n \in \mathbb{Z}_{\geq 0}$ by Remark 2.5, and since $\{1, \gamma, \gamma^2, \dots\} \subseteq X$ is finite we must have $\gamma^n = \gamma^m$ for some $0 \leq n < m$. Now $\gamma^{2m(m-n)} = \gamma^{(2m-1)(m-n)} = \dots = \gamma^{m(m-n)}$ since $(2m-a)(m-n) \geq m$ for all $a \leq m$. Hence $\gamma^{m(m-n)}$ is idempotent and $\gamma^{m(m-n)} = 1$. It follows that $\langle\gamma\rangle_{\mathtt{Grd}}$ is a finite group.

(2) Assume R_1 is a domain. Let $\gamma_1, \dots, \gamma_n \in X$ and for each i let $x_i \in R_{\gamma_i}$ be non-zero. Applying induction to n we show that $x_1 \cdots x_n \neq 0$. Assume $0 \neq x := x_1 \cdots x_n$, then $x \in R_\delta$ for some $\delta \in X$. Using (1) we get $0 \neq x_{n+1}^{\mathrm{ord}(\gamma_{n+1})}, x^{\mathrm{ord}(\delta)} \in R_1$ and thus $0 \neq x^{\mathrm{ord}(\delta)} x_{n+1}^{\mathrm{ord}(\gamma_{n+1})}$ since R_1 is a domain. In particular, $x_1 \cdots x_{n+1} = x \cdot x_{n+1} \neq 0$. It follows from Remark 2.5 that $\gamma = \gamma_1 * \dots * \gamma_n$ is uniquely defined regardless of grouping of factors and that $0 \neq R_\gamma$, so $\gamma \in X$. We conclude that $X = \langle X\rangle_{\mathtt{Grd}}$ and that X is a monoid. It then follows from (1) that X is a group. If R is commutative, $0 \neq R_\gamma R_\delta \cap R_\delta R_\gamma \subseteq R_{\gamma*\delta} \cap R_{\delta*\gamma}$ implies $\gamma * \delta = \delta * \gamma$ for all $\gamma, \delta \in X$, making X abelian.

Let $x \in R_\delta$ be non-zero and $y \in R$ such that $xy = 0$. Write $y = \sum_\gamma y_\gamma$ with $y_\gamma \in R_\gamma$ for all $\gamma \in \Gamma$. Then $xy = \sum_\gamma xy_\gamma = \sum_\gamma xy_{\delta^{-1}*\gamma}$ with $xy_\gamma \in R_{\delta*\gamma}$. By uniqueness of decomposition $xy_\gamma = 0$ and by the above $y_\gamma = 0$ for all $\gamma \in \Gamma$. It follows that $y = 0$, hence x is not a left zero-divisor. Analogously x is not a right zero-divisor, so x is regular.

(3) Let $\gamma \in X$ with $n = \mathrm{ord}(\gamma)$ and let $x \in R_\gamma$ be non-zero. As $x^n \in R_1$ is invertible, we have $y = (x^n)^{-1} \cdot x^{n-1} \in R_{\gamma^{n-1}}$ such that $xy = yx = 1$. Hence x is invertible with $x^{-1} = y \in R_{\gamma^{-1}}$. Consider R_γ as left R_1-module. Then we have R_1-linear maps $R_1 \to R_\gamma$ and $R_\gamma \to R_1$ given by $z \mapsto zx$ and $z \mapsto zx^{-1}$. We note that they are mutually inverse, implying that $R_1 \cong_{R_1\text{-}\mathtt{Mod}} R_\gamma$, from which it follows that $\dim_{R_1} R_\gamma = 1$. □

2.2 Coproduct gradings and joint gradings

A basic tool in our study of gradings is the ability to construct complex gradings from small building blocks, which we will treat in this section. The following lemma is an exercise in elementary algebra left to the reader.

Lemma 2.7. *Let $\mathcal{G} = \{G_i\}_{i\in I}$ be a family of grids with $G_i = (S_i, 1_i, D_i, *_i)$. Then $\mathcal{G}$ has a product $\prod_{i\in I} G_i$, where the underlying set is $\prod_{i\in I} S_i$ and the product $(a_i)_{i\in I} * (b_i)_{i\in I} := (a_i *_i b_i)_{i\in I}$ is defined precisely when it is for all components. Additionally $\mathcal{G}$ has a coproduct $\coprod_{i\in I} G_i$ where the underlying set is $S = \{1\} \amalg \coprod_{i\in I}(S_i \setminus \{1_i\})$ with 1 the unit. For $a, b \in S \setminus \{1\}$ we define $a * b = a *_i b$ if and only if there is some $i \in I$ such that $(a, b) \in D_i$.* □

Definition 2.8. Let $G = (S, 1, D, *)$ be a grid. We define the *groupification of G*, symbolically G^{grp}, to be the group with presentation

$$\langle [g] \text{ for } g \in G \mid [1] = 1,\ [g] \cdot [h] = [g * h] \text{ for } (g, h) \in D\rangle.$$

Lemma 2.9. *Groupification defines a functor $\_^{\mathrm{grp}} : \mathtt{Grd} \to \mathtt{Grp}$. This functor is the left adjoint of the forgetful functor $\mathtt{Grp} \to \mathtt{Grd}$.*

Proof. The proof is straightforward and amounts to showing that for any grid G and group H any morphism of grids $g : G \to H$ factors uniquely through G^{grp}. Let F be the free group with set of symbols G, let $N \subseteq F$ be the normal subgroup such that $F/N = G^{\mathrm{grp}}$ as in Definition 2.8 and let $f : G \to F/N$ be the natural map. We combine the universal property of the free group and the homomorphism theorem to obtain the unique $h : F/N \to H$ as follows

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr] \arrow[ddr, "g"'] & & F/N \arrow[ddl, dashed, "\exists! h"] \\
& F \arrow[ur] \arrow[d, dashed, "\exists! i"] & \\
& H &
\end{tikzcd}$$

where we use that always $N \subseteq \ker(i)$. □

Groupification $\_^{\mathtt{grp}}$ is to grids what abelianization $\_^{\mathtt{ab}}$ is to groups. Since the forgetful functors $\mathtt{Ab} \to \mathtt{Grp}$ and $\mathtt{Grp} \to \mathtt{Grd}$ are right adjoint they commute with limits. In particular, the product of groups taken in the category of groups is canonically isomorphic to the same product taken in the category of grids instead. The same holds for products of abelian groups in the category of groups. Therefore, when we take products of groups or abelian groups we do not have to specify the underlying category. However, the coproduct for each category is, in general, fundamentally different, so here we need to be careful. The most notable difference we encounter is that a coproduct of finitely many finite grids is finite, just like in the category of abelian groups, while a coproduct in the category of groups will only be finite if all but possibly one of the groups is trivial.

Definition 2.10. Let $\mathcal{R} = \{\overline{R^i}\}_{i \in I}$ be a finite family of grid-gradings with $\overline{R^i} = (R_i, G_i, \{R_{i,g}\}_{g \in G_i})$. Then $R = \prod_{i \in I} R_i$ has a grading $\coprod_{i \in I} \overline{R^i} = (R, G, \{R_g\})$ called the *coproduct of* $\mathcal{R}$, with $G = \coprod_{i \in I} G_i$ taken in the category of grids and $R_g = R_{i,g}$ if $g \in G_i \setminus \{1\}$ and $R_1 = \prod_{i \in I} R_{i,1}$.

One can verify that the coproduct of efficient gradings is again an efficient grading. Another construction is the joint grading, which uses the product instead of the coproduct.

Lemma 2.11. *Let k be a commutative ring and R be a k-algebra. Let I be a set and let $\{\overline{R}_i\}_{i \in I}$ with $\overline{R}_i = (R, \Gamma_i, \{R_{i,\gamma}\}_{\gamma \in \Gamma_i})$ be a collection of grid-gradings. Let $S_\delta = \bigcap_{i \in I} R_{i,\delta(i)}$ for all $\delta \in \Delta = \prod_{i \in I} \Gamma_i$. If the natural map $\bigoplus_{\delta \in \Delta} S_\delta \to R$ is surjective, then $\bigcap_{i \in I} \overline{R}_i := (R, \Delta, \{S_\delta\}_{\delta \in \Delta})$ is a grid-grading.*

Proof. Clearly the natural map $\bigoplus_{\delta \in \Delta} S_\delta \to R$ is injective and thus an isomorphism. It suffices to note that $S_\delta S_{\delta'} \subseteq R_{\delta(i)} R_{\delta'(i)} \subseteq R_{(\delta\delta')(i)}$ for all $\delta, \delta' \in \Delta$ and $i \in I$ hence $S_\delta S_{\delta'} \subseteq \bigcap_{i \in I} R_{(\delta\delta')(i)} = S_{\delta\delta'}$. As $1 \in S_1$ we have that $\bigcap_{i \in I} \overline{R}_i$ is a grading. □

Definition 2.12. Using the same notation as in Lemma 2.11, we call $\bigcap_{i \in I} \overline{R}_i$ the *joint grading* of $\{\overline{R}_i\}_{i \in I}$ when it is a grading.

Remark 2.13. If R has a universal grading $\overline{U} = (R, \Upsilon, \{U_\upsilon\}_{\upsilon \in \Upsilon})$, then $\overline{R} \cap \overline{S}$, with $\overline{R}$ and $\overline{S}$ gradings of R, is always a grading. Namely the (unique) maps $f : \Upsilon \to \Gamma$ and $g : \Upsilon \to \Delta$ such that $f_* \overline{U} = \overline{R}$ and $g_* \overline{U} = \overline{S}$ give a map $h : \Upsilon \to \Gamma \times \Delta$ and a $\Gamma \times \Delta$-grading $\overline{T} = h_* \overline{U}$. The projection maps $\pi_\Gamma : \Gamma \times \Delta \to \Gamma$ and $\pi_\Delta : \Gamma \times \Delta \to \Delta$ then satisfy $\pi_{\Gamma *} \overline{T} = \overline{R}$ and $\pi_{\Delta *} \overline{T} = \overline{S}$. One then easily verifies $\overline{T} = \overline{R} \cap \overline{S}$. This argument trivially extends to joint gradings of infinitely many gradings. To show that R does not have a universal grading, it suffices to give gradings $\overline{R}$ and $\overline{S}$ such that $\overline{R} \cap \overline{S}$ is not a grading. As Proposition 3.35 will show, under mild finiteness conditions the existence of such $\overline{R}$ and $\overline{S}$ is also necessary. If we drop these finiteness conditions, Example 6.6 provides a counter-example.

2.3 Examples

In this section we consider some examples of gradings.

Example 2.14. Let Γ be a finite group and let k be a commutative ring which is connected, meaning it is not isomorphic to the product of two non-zero rings. Consider k^Γ, which is a k-module of which we denote the elements as $\sum_{\gamma \in \Gamma} x_\gamma \gamma$ for some $x_\gamma \in k$. Then k^Γ can be equipped with a k-algebra structure by defining the multiplication as the k-linear continuation of the multiplication of Γ. We write $k[\Gamma]$ for this ring, which we call the *group ring of* Γ. The group ring comes with a natural Γ-grading $\overline{U} = (k[\Gamma], \Gamma, \{k \cdot \gamma\}_{\gamma \in \Gamma})$. Note that $\overline{U}$ cannot be further refined by connectedness of k. As $\overline{U}$ is also efficient it must be the universal grading of $k[\Gamma]$ whenever a universal grading exists. If $k = \mathbb{Z}$ and Γ is abelian, then $k[\Gamma]$ is a reduced order and $\overline{U}$ must be the universal grading of $k[\Gamma]$ since it exists by Theorem 1.8.

If Γ and Δ are finite abelian groups, then $k[\Gamma \times \Delta] \cong k[\Gamma] \otimes_k k[\Delta]$. Then by the structure theorem for finite abelian groups we may study the structure of $k[\Gamma]$ through that of $k[C_{p^n}]$, where p is a prime, $n \geq 1$ and C_r is the cyclic group of order r. Additionally, $k[\Gamma] \cong k \otimes_{\mathbb{Z}} \mathbb{Z}[\Gamma]$. We have

$$\mathbb{Q}[C_{p^n}] \cong \mathbb{Q}[X]/(X^{p^n} - 1) \cong \mathbb{Q}[X]/(X^{p^{n-1}} - 1) \times \mathbb{Q}[X]/\left(\frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}\right) \cong \mathbb{Q}[C_{p^{n-1}}] \times \mathbb{Q}(\zeta_{p^n}).$$

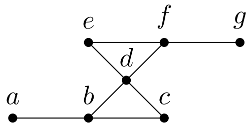
As $\mathbb{Q}(\zeta_a) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_b) \cong \mathbb{Q}(\zeta_{ab})$ for $a, b \in \mathbb{Z}_{>0}$ coprime, we have that for $k = \mathbb{Q}$ the group rings are isomorphic to products of cyclotomic fields.

By Example 2.14 we may consider products of cyclotomic rings as the first generalization of group rings. It gives us motivation to study the gradings of cyclotomic fields, which we will do more thoroughly in Section 5.

Example 2.15. Consider the ring $K = \mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive 8-th root of unity. Since it is a field, all its efficient gradings are graded with abelian groups of size dividing $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$ by Proposition 2.6. It has an obvious grading $\overline{A} = (K, \mathbb{Z}/4\mathbb{Z}, \{A_n\}_{n \in \mathbb{Z}/4\mathbb{Z}})$ with $A_n = \zeta_8^n \cdot \mathbb{Q}$, which is well defined since $\zeta_8^4 \in \mathbb{Q}$. The natural projection $\pi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ then induces the grading $\overline{B} = \pi_* \overline{A} = (K, \mathbb{Z}/2\mathbb{Z}, \{B_n\}_{n \in \mathbb{Z}/2\mathbb{Z}})$ with $B_n = \zeta_8^n \cdot \mathbb{Q}(\zeta_4)$. Two other $\mathbb{Z}/2\mathbb{Z}$-gradings of K are $\overline{C}$ and $\overline{D}$ with $C_n = \sqrt{2}^n \cdot \mathbb{Q}(\zeta_4 \cdot \sqrt{2}) = \zeta_4^n \cdot \mathbb{Q}(\zeta_4 \cdot \sqrt{2})$ and $D_n = \zeta_4^n \cdot \mathbb{Q}(\sqrt{2})$ as $\zeta_8 = (1 + \zeta_4)/\sqrt{2}$. As we will show in Section 5, we have in fact listed all efficient gradings of K with a cyclic group, up to group isomorphism. Of these we can construct a joint grading $\overline{E} = \overline{C} \cap \overline{D} = (K, (\mathbb{Z}/2\mathbb{Z})^2, \{E_{m,n}\}_{(m,n) \in (\mathbb{Z}/2\mathbb{Z})^2})$ with $E_{m,n} = \sqrt{2^{m+n}} \cdot \zeta_4^n \cdot \mathbb{Q}$. However, $\overline{A}$ and $\overline{E}$ have no joint grading, as $\sum_{k,m,n} A_k \cap E_{m,n} = \mathbb{Q}(\zeta_4) \neq K$. Thus K has no universal grading by Remark 2.13.

Now consider $R = \mathbb{Z}[\zeta_8]$, which is a reduced order. It certainly has $\overline{U} := (R, \mathbb{Z}/4\mathbb{Z}, \{A_n \cap R\}_{n \in \mathbb{Z}/4\mathbb{Z}})$ as grading. On the other hand, $\zeta_8 = (\frac{1}{2}\sqrt{2}) + (\frac{1}{2}\zeta_4\sqrt{2}) \notin \bigoplus_{(m,n) \in (\mathbb{Z}/2\mathbb{Z})^2} (E_{m,n} \cap R)$ as $\sqrt{2}/2 \notin R$, so $\overline{E}$ does not similarly produce a grading of R. Hence the non-existence of a joint grading of $\overline{A}$ and $\overline{E}$ does not contradict that R should have a universal grading. Moreover, since $\overline{U}$ cannot be further refined, it must be the universal grading provided by Theorem 1.8.

The following two examples highlight the difference between grid-gradings, group-gradings and abelian group-gradings. Specifically, in Example 2.16 we construct a ring A and a grid-grading $\overline{A}$ of A such that there exists no group-grading $\overline{B}$ of A with the same non-zero homogeneous components as $\overline{A}$. We do the same in Example 2.17 for groups and abelian groups.



Example 2.16. Grids need not be associative. Consider the following figure consisting of seven points $S = \{a, \ldots, g\}$ and 4 lines each containing exactly three points. We define multiplication on $G = \{1\} \cup S$ such that $\{1\} \cup L$ is a Klein four-group for each line L, and all other products are undefined. Then G is a grid, and $(bd)e = fe = g$ while $b(de) = bc = a$. Hence G is not associative.

Now consider the efficient grading $\overline{R} = (\mathbb{Q}(\sqrt{2}, \sqrt{3}), (\mathbb{Z}/2\mathbb{Z})^2, \{\sqrt{2^u 3^v} \cdot \mathbb{Q}\}_{(u,v) \in (\mathbb{Z}/2\mathbb{Z})^2})$. For each line L we have an injective morphism of grids $\varphi_L : (\mathbb{Z}/2\mathbb{Z})^2 \cong (\{1\} \cup L) \to G$ and the coproduct of these morphisms gives a surjection $\varphi : \coprod_L (\mathbb{Z}/2\mathbb{Z})^2 \to G$. Now $\overline{A} = \varphi_* \coprod_L \overline{R}$ gives a G-grading of $A = \mathbb{Q}(\sqrt{2}, \sqrt{3})^4$ without any zero homogeneous components. Then for any grading $\overline{B} = (A, H, \{B_h\}_{h \in H})$ of A with the same non-zero homogeneous components as $\overline{A}$ there exists a unique injective morphism $\psi : G \to H$ such that $\psi_* \overline{A} = \overline{B}$. If H is a group, then H is certainly associative, so $\psi(g) = \psi(f)\psi(e) = \psi(b)\psi(d)\psi(e) = \psi(b)\psi(c) = \psi(a)$, a contradiction. Thus the decomposition of $\overline{A}$ can be turned into a grading with a grid but not with a group.

Example 2.17. A commutative ring can be efficiently graded with a finite non-abelian group, as seen in Example 1.5. However, for this ring there exists a grading with an abelian group which has the same non-zero homogeneous components. Here we will construct a grading with a non-abelian group for which this is not the case.

For $n \in \mathbb{Z}_{\geq 1}$ consider the groups $N = \{\pm 1\}^{n+1} = \langle z, x_1, \dots, x_n \rangle$ and $G = \{\pm 1\}^n = \langle x_{n+1}, \dots, x_{2n} \rangle$. On the generators of G define an action $\varphi : G \to \operatorname{Aut}(N)$ as

$$x_{n+i} \mapsto \big(x_j \mapsto x_j z^{\delta_{ij}},\ z \mapsto z\big) \quad \text{for all } 1 \leq i, j \leq n,$$

where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise, and define $\mathrm{ES}_n = N \rtimes_\varphi G$. Although we do not use this fact, we note that ES_n is an *extra special* 2*-group* [3], as its center is $\langle z \rangle \cong \mathbb{F}_2$, and $\mathrm{ES}_n/\langle z \rangle \cong \mathbb{F}_2^{2n}$. Consider the ES_2-valued matrix

$$M = \begin{array}{c@{}c} \begin{array}{ccc} 1 & 2 & 3 \end{array} & \\ \begin{pmatrix} x_1 & x_2 & x_1x_2 \\ x_4 & x_3 & x_3x_4 \\ x_1x_4 & x_2x_3 & x_1x_2x_3x_4 \end{pmatrix} & \begin{array}{c} 4 \\ 5 \\ 6 \end{array} \end{array}$$

together with a labeling of its rows and columns. Consider the $(\mathbb{Z}/2\mathbb{Z})^3$-grading $\overline{R}$ of $R = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ with $R_{(a,b,c)} = \sqrt{2^a 3^b 5^c} \cdot \mathbb{Q}$. For each i let Δ_i be the group generated by z and the entries of row/column i of M and note that we have an isomorphism $f_i : (\mathbb{Z}/2\mathbb{Z})^3 \to \Delta_i$. Consider the Δ_i-grading $\overline{R^i} = f_{i*}\overline{R}$ of R. Then we grade $A = R^6$ with $\Delta = \coprod_{i=1}^6 \Delta_i$ as the coproduct (in the category of grids) of $\overline{R^1}, \dots, \overline{R^6}$, and let $\overline{A}$ be the image of this coproduct under the natural map $g : \Delta \to \mathrm{ES}_2$. Since the Δ_i generate ES_2 the grading $\overline{A}$ is efficient. Thus the commutative ring A can be efficiently graded with a non-commutative group.

Assume there is a Γ-grading $\overline{B}$ of A with the same non-zero components as $\overline{A}$ and with Γ an abelian group. Let $D = \bigcup_i \Delta_i$ and note that $A_\delta \neq 0$ for all $\delta \in D$. Thus there exists a (unique) injective map $\psi : D \to \Gamma$ such that $A_\delta = B_{\psi(\delta)}$ for all $\delta \in D$. Moreover, the restriction $\psi|_{\Delta_i}$ is a morphism of groups for each i, as $\{0\} \subsetneq A_\delta A_{\delta'} \cap A_{\delta\delta'} = B_{\psi(\delta)} B_{\psi(\delta')} \cap B_{\psi(\delta\delta')}$ implies $\psi(\delta)\psi(\delta') = \psi(\delta\delta')$ for all $\delta, \delta' \in \Delta_i$. Let p_i be the product of the three entries of row/column i of M for each i, and note $p_i = 1$ for $i \in \{1, \dots, 5\}$, while $p_6 = z$. As Γ is abelian, we get

$$1 = \prod_{i=1}^{3} \psi(p_i) = \prod_{a=1}^{3} \prod_{b=1}^{3} \psi(M_{ab}) = \prod_{i=4}^{6} \psi(p_i) = \psi(z),$$

so ψ is not injective, a contradiction. Hence there is no abelian group-grading with the same non-zero components as $\overline{A}$.

3 Gradings as ring automorphisms

3.1 Cyclotomic number fields and Steinitz numbers

In this section we will define cyclotomic rings and derive some properties.

Definition 3.1. The *Steinitz numbers* are the formal products $\prod_p p^{n_p}$ with p ranging over the primes and $n_p \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ for all p. We denote the set of Steinitz numbers by $\mathbb{S}$. We define multiplication on Steinitz numbers as $(\prod_p p^{n_p}) \cdot (\prod_p p^{m_p}) := \prod_p p^{n_p+m_p}$, with the convention that $x + \infty = \infty + x = \infty$ for all $x \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$. For $x = \prod_p p^{n_p} \in \mathbb{S}$ we define *the order of x at the prime p* as $\operatorname{ord}_p(x) := n_p$. We say $x \in \mathbb{S}$ *divides* $y \in \mathbb{S}$, symbolically $x \mid y$, if there exists some $z \in \mathbb{S}$ such that $xz = y$, or equivalently if $\operatorname{ord}_p(x) \leq \operatorname{ord}_p(y)$ for all primes p. We also write ∞ for the Steinitz number $\prod_p p^\infty$.

Remark 3.2. Note that $\mathbb{Z}_{>0}$ is naturally embedded in $\mathbb{S}$ as the set of all Steinitz numbers $\prod_p p^{n_p}$ for which only finitely many n_p are non-zero and none are infinity. For this subset of $\mathbb{S}$ the defined concepts of multiplication, divisibility and order agree with those defined for $\mathbb{Z}_{>0}$. Hence we will interpret this embedding as a true inclusion. Each definition in this thesis involving Steinitz numbers will generalize similar definitions on $\mathbb{Z}_{>0}$ if such exist. We will leave it to the reader to verify this.

Definition 3.3. Consider the natural projections $\pi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$ integers. Note that $\mathbb{Z}_{>0}$ is a partially ordered set with respect to divisibility, such that $\{\pi_{mn}\}_{m \mid n \in \mathbb{Z}_{>0}}$ becomes an inverse system of homomorphisms. Then we define the *ring of profinite integers* as the inverse limit $\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{Z}_{>0}} \mathbb{Z}/n\mathbb{Z}$ of this system.

Remark 3.4. We may interpret Steinitz numbers as special ideals of $\hat{\mathbb{Z}}$. Taking $e = \prod_p p^{n_p} \in \mathbb{S}$, we define through abuse of notation its ideal $e\hat{\mathbb{Z}} = \bigcap_{d \in \mathbb{Z}_{>0},\ d \mid e} d\hat{\mathbb{Z}}$. Note that for $e \in \mathbb{Z}_{>0}$ we have that $e\hat{\mathbb{Z}}$ is unambiguous, as the ideal is the same when e is interpreted as a Steinitz number. We have a Chinese remainder theorem $\hat{\mathbb{Z}}/(\prod_p p^{n_p})\hat{\mathbb{Z}} \cong_{\texttt{Rng}} \prod_p \hat{\mathbb{Z}}/p^{n_p}\hat{\mathbb{Z}}$ and also that for $n \in \mathbb{Z}_{>0}$ the projection $\hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ induces an isomorphism $\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \cong_{\texttt{Rng}} \mathbb{Z}/n\mathbb{Z}$.

Definition 3.5. For $N \subseteq \mathbb{S}$ we define the *greatest common divisor* and *least common multiple* of the elements of N as the Steinitz numbers

$$\gcd(N) := \prod_p p^{\inf\{\operatorname{ord}_p(x) \,\mid\, x \in N\}} \quad \text{and} \quad \operatorname{lcm}(N) := \prod_p p^{\sup\{\operatorname{ord}_p(x) \,\mid\, x \in N\}}$$

respectively. In particular, we have a definition of gcd and lcm on infinite subsets of $\mathbb{Z}_{>0}$.

Definition 3.6. Let G be a group for which each element has finite order, i.e. G is *torsion*. We define the *exponent* of G as the Steinitz number $e(G) := \operatorname{lcm}\{\operatorname{ord}(g) \mid g \in G\}$. Additionally, when we say G has exponent $e \in \mathbb{S}$, we implicitly assume G is torsion.

Remark 3.7. The profinite integers form a ring, so in particular a multiplicative monoid. If G is torsion we have a right action $G \times \hat{\mathbb{Z}} \to G$ of $\hat{\mathbb{Z}}$ as monoid given by $(g, \underline{n}) \mapsto g^n$, where n is any integer such that $n \equiv \underline{n} \mod \operatorname{ord}(g)$. It satisfies $1^n = 1 = g^0$, $g^1 = g$, $g^{n+m} = g^n g^m$ and $g^{nm} = (g^n)^m$ for all $g \in G$ and $n, m \in \hat{\mathbb{Z}}$. When G is abelian $\hat{\mathbb{Z}}$ even respects the group structure as $(gh)^n = g^n h^n$, making G a $\hat{\mathbb{Z}}$-module. The map $\hat{\mathbb{Z}} \to \operatorname{End}_{\texttt{Set}}(G)$ has kernel $e(G)\hat{\mathbb{Z}}$, so even $\hat{\mathbb{Z}}/e(G)\hat{\mathbb{Z}}$ acts on G.

Definition 3.8. A *topological group* is a group G equipped with a topology such that the multiplication $G \times G \to G$ and inversion $G \to G$ are continuous maps, where $G \times G$ is equipped with the product topology. We call a topological group *locally compact* if the underlying topology is Hausdorff and locally compact. We write `LCA` for the category of locally compact abelian groups with as morphisms the continuous group homomorphisms. We have a natural inclusion `Ab` → `LCA` where we equip each group with the discrete topology. For topological spaces X and Y the *compact-open topology* on Y^X is the topology with subbase $\{V(K, U) \mid K \subseteq X \text{ compact}, U \subseteq Y \text{ open}\}$, where

$V(K,U) = \{f \in Y^X \mid f(K) \subseteq U\}$. For any $\Gamma, \Delta \in \mathrm{obj}(\mathtt{LCA})$ we equip $\mathrm{Hom}_{\mathtt{LCA}}(\Gamma, \Delta)$ with a group structure given by point-wise multiplication and with the subspace topology from Δ^Γ with the compact-open topology, making it a topological abelian group.

Definition 3.9. Let $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$, which is a compact abelian group. For $e \in \mathbb{S}$ we write $\mu_e \subseteq \mathbb{T}$ for its e-torsion subgroup, which we equip with the discrete topology. For a locally compact abelian group Γ we define $\widehat{\Gamma} = \mathrm{Hom}_{\mathtt{LCA}}(\Gamma, \mathbb{T})$ as the *dual group* of Γ, which is a locally compact abelian group as well (Theorem 1.2.6 of [4]). For $f \in \mathrm{Hom}_{\mathtt{LCA}}(\Gamma, \Delta)$ we write $\widehat{f} \in \mathrm{Hom}_{\mathtt{LCA}}(\widehat{\Delta}, \widehat{\Gamma})$ for the map given by $\chi \mapsto \chi \circ f$. Then $\widehat{\cdot} : \mathtt{LCA} \to \mathtt{LCA}$ is a contravariant functor.

Remark 3.10. For $e \in \mathbb{S}$ and $\chi \in \widehat{\mu}_e$ we have $\chi(\mu_e) \subseteq \mu_e$. Hence $\widehat{\mu}_e$ is closed under composition and this composition is continuous. This turns $\widehat{\mu}_e$ into a topological ring where the addition is pointwise multiplication and multiplication is composition.

Lemma 3.11. *For all $e \in \mathbb{S}$ the natural action $\varphi_e : \hat{\mathbb{Z}}/e\hat{\mathbb{Z}} \to \mathrm{End}_{\mathtt{Ab}}(\mu_e) \cong \widehat{\mu}_e$ as in Remark 3.7 is an isomorphism of rings.*

Proof. First assume $e \in \mathbb{Z}_{>0}$. Then μ_e is the zero set of $X^e - 1$ in $\mathbb{C}[X]$, a polynomial which has precisely e distinct roots, so $\#\mu_e = e$. If $d \mid e$ is the exponent of μ_e, then $X^d - 1$ has at least e distinct roots and thus $d \geq e$ because $\mathbb{C}$ is a domain. Hence $d = e$ and thus μ_e is cyclic. If we fix any generator $\zeta \in \mu_e$, then $\chi \in \widehat{\mu}_e$ is uniquely defined by $\chi(\zeta)$. As $\varphi_e(x)(\zeta) = \zeta^x$ for all $x \in \hat{\mathbb{Z}}/e\hat{\mathbb{Z}}$ we have that φ_e is surjective, and since $\zeta^x = \zeta^y$ implies $x = y$ for $x, y \in \hat{\mathbb{Z}}/e\hat{\mathbb{Z}}$ it is also injective. For general $e \in \mathbb{S}$ we note that with $d \mid e$ an integer the diagram

$$\begin{tikzcd}
\hat{\mathbb{Z}}/e\hat{\mathbb{Z}} \arrow[r] \arrow[d] & \widehat{\mu}_e \arrow[d] \\
\mathbb{Z}/d\mathbb{Z} \arrow[r, "\sim"] & \widehat{\mu}_d
\end{tikzcd}$$

is commutative, hence

$$\hat{\mathbb{Z}}/e\hat{\mathbb{Z}} = \varprojlim_{d \mid e} \mathbb{Z}/d\mathbb{Z} \cong \varprojlim_{d \mid e} \mathrm{Hom}_{\mathtt{LCA}}(\mu_d, \mathbb{T}) \cong \mathrm{Hom}_{\mathtt{LCA}}\Big(\varinjlim_{d \mid e} \mu_d, \mathbb{T}\Big) = \mathrm{Hom}_{\mathtt{LCA}}(\mu_e, \mathbb{T}) = \widehat{\mu}_e$$

□

Corollary 3.12. *Let $e \in \mathbb{S}$. Then $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^* \cong \mathrm{Aut}_{\mathtt{Ab}}(\mu_e) \cong \mathrm{Aut}_{\mathtt{Rng}}(\mathbb{Q}(\mu_e)) \cong \mathrm{Aut}_{\mathtt{Rng}}(\mathbb{Z}[\mu_e])$.*

Proof. The first isomorphism is a direct consequence of Lemma 3.11. For $k \in \{\mathbb{Z}, \mathbb{Q}\}$ and e an integer the isomorphism $\mathrm{Aut}_{\mathtt{Grp}}(\mu_e) \cong \mathrm{Aut}_{\mathtt{Rng}}(k[\mu_e])$ is proved in Theorem 3.1 in [5], and the general case follows from $\mu_e = \varinjlim_{d \mid e} \mu_d$ and $k[\mu_e] = \varinjlim_{d \mid e} k[\mu_d]$. □

Lemma 3.13. *Let $e \in \mathbb{Z}_{>0}$, $\zeta \in \mu_e$ primitive and $\pi = 1 - \zeta \in \mathbb{Z}[\mu_e]$.*

1. *For all $a \in \mathbb{Z}$ there exist $x \in \mathbb{Z}[\mu_e]$ such that $x\pi = 1 - \zeta^a$. If $\gcd(a, e) = 1$, then x is a unit.*
2. *If $\eta, \theta \in \mu_e$ are distinct, then $e = x(\eta - \theta)$ for some $x \in \mathbb{Z}[\mu_e]$.*
3. *If $e = p^n$ for some $n \in \mathbb{Z}_{>0}$ and prime p, then we may write $x\pi^m = p$ with $m = p^n - p^{n-1}$ and $x \in \mathbb{Z}[\mu_{p^n}]^*$.*

Proof. Recall the following basic algebraic identities in $\mathbb{Z}[\mu_e][X]$ with $b, c \in \mathbb{Z}_{>0}$.

$$\sum_{i=0}^{b-1} X^{ci} = \frac{X^{bc} - 1}{X^c - 1} = \prod_{\xi \in \mu_{bc} \setminus \mu_c} (X - \xi).$$

(1) Fix $c = 1$. Taking $b = a$ and $X = \zeta$ in the above identities we obtain $x\pi = 1 - \zeta^a$ with $x = \sum_{i=0}^{a-1} \zeta^i$. If $\gcd(a, e) = 1$, then there exists a $b \in \mathbb{Z}_{>0}$ such that $ab \equiv 1 \mod e$. From the first identity with this b and $X = \zeta^a$ it follows that x is invertible.

(2) Let $x = \eta^{-1} \cdot \prod_{\xi \in \mu_e \setminus \{1, \eta^{-1}\theta\}} (1 - \xi)$. From the above identities with $b = e$, $c = 1$ and $X = 1$ we obtain $x(\eta - \theta) = \prod_{\xi \in \mu_e \setminus \mu_1} (X - \xi) = \sum_{i=0}^{e-1} X = e$.

(3) Each $\xi \in \mu_e$ may be written $\xi = \zeta^a$ for some $a \in \mathbb{Z}$, and $\xi \notin \mu_{p^{n-1}}$ if and only if $\gcd(a, e) = 1$. Then by (1) for all $\xi \in \mu_{p^n} \setminus \mu_{p^{n-1}}$ there exist $x_\xi \in \mathbb{Z}[\mu_{p^n}]^*$ such that $1 - \xi = \pi x_\xi$. Taking $b = p$, $c = p^{n-1}$ and $X = 1$ it follows that $x = \prod_{\xi \in \mu_{p^n} \setminus \mu_{p^{n-1}}} x_\xi$ satisfies $x\pi^m = p$. □

Lemma 3.14. *For $n = \prod_p p^{n_p} \in \mathbb{Z}_{>0}$ write $\operatorname{rad}(n) = \prod_p p^{\min\{n_p, 1\}}$ and $\omega(n) = \#\{p \mid n_p \geq 1\}$. Then $\operatorname{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{\operatorname{rad}(n)}) = (-1)^{\omega(n)} \cdot n/\operatorname{rad}(n)$ for any primitive $\operatorname{rad}(n)$-th root of unity $\zeta_{\operatorname{rad}(n)}$.*

Proof. Consider the map ψ given by $n \mapsto \operatorname{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{\operatorname{rad}(n)})$. Let $n, m \in \mathbb{Z}_{>0}$ be coprime. We have $(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ by the Chinese Remainder Theorem. Writing $\zeta_{\operatorname{rad}(nm)} = \zeta_{\operatorname{rad}(n)}\zeta_{\operatorname{rad}(m)}$ and using Corollary 3.12 we get

$$\psi(nm) = \sum_{a \in (\mathbb{Z}/nm\mathbb{Z})^*} \zeta_{\operatorname{rad}(nm)}^a = \sum_{a \in (\mathbb{Z}/nm\mathbb{Z})^*} \zeta_{\operatorname{rad}(n)}^a \zeta_{\operatorname{rad}(m)}^a = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ b \in (\mathbb{Z}/m\mathbb{Z})^*}} \zeta_{\operatorname{rad}(n)}^a \zeta_{\operatorname{rad}(m)}^b = \psi(n)\psi(m).$$

Thus ψ is a multiplicative function, and so is $n \mapsto (-1)^{\omega(n)} \cdot n/\operatorname{rad}(n)$. Because of this we may assume without loss of generality that $n = p^k$. Here

$$\psi(n) = \sum_{a \in (\mathbb{Z}/p^k\mathbb{Z})^*} \zeta_p^a = p^{k-1} \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \zeta_p = -p^{k-1} = (-1)^{\omega(n)} \cdot n/\operatorname{rad}(n),$$

as was to be shown. □

Proposition 3.15. *Let $e \in \mathbb{S}$ and let M be a $\mathbb{Z}$-module on which multiplication by integer divisors of e is injective. Define $N = M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ and consider the action ψ of $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^* \cong \operatorname{Aut}_{\mathbb{Z}\text{-}\mathtt{Alg}}(\mathbb{Z}[\mu_e])$ on N via the second component. Then multiplication with integer divisors of e is injective on N and the natural map $M \to N$ is injective with as image the $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$-invariant submodule $N^{(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*}$ of N.*

Proof. Recall that we have a functor $M \otimes_{\mathbb{Z}} \_$ on $\mathbb{Z}$-modules. Then $\varinjlim_{d \mid e}(M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d]) = N$ and the action of $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ on $M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d]$ commutes with the direct limit. Assuming the proposition holds for integers $d \mid e$ in place of e, we get

$$N^{(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*} = \big(\varinjlim_{d \mid e}(M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d])\big)^{(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*} = \varinjlim_{d \mid e} \big((M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d])^{(\hat{\mathbb{Z}}/d\hat{\mathbb{Z}})^*}\big) = \varinjlim_{d \mid e} M = M.$$

For $c \mid d \mid e$ with c and d integer we have an exact sequence $0 \to M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d] \xrightarrow{c\cdot} c(M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d])$ because multiplication by c is injective, so $0 \to \varinjlim_{d \mid e}(M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d]) \to \varinjlim_{d \mid e} c(M \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d])$ is an exact sequence. It follows that multiplication by c is injective on N. It remains to prove the proposition assuming $e \in \mathbb{Z}_{>0}$.

Note that $\mathbb{Z}[\mu_e]$ is a free $\mathbb{Z}$-module with a basis $\mathcal{B} = \{1, \zeta_e, \ldots, \zeta_e^{\varphi(e)-1}\}$ containing 1, so the natural map $M^{\mathcal{B}} \to N$ is an isomorphism of $\mathbb{Z}$-modules. In particular, $M \hookrightarrow M \otimes 1 \hookrightarrow N$ and multiplication by e is injective on M. Obviously $M \otimes 1 \subseteq N^{(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*}$ since $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ acts via the second component. For the reverse inclusion, let $x \in N^{(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*}$ be given. Consider as in Lemma 3.14 the trace function $\operatorname{Tr} = \operatorname{Tr}_{\mathbb{Q}(\mu_e)/\mathbb{Q}}$ and note that $\operatorname{Tr}(\mathbb{Z}[\mu_e]) \subseteq \mathbb{Z}$. Write $x = \sum_{b \in \mathcal{B}} x_b \otimes b$ with $x_b \in M$ and let $d = \operatorname{rad}(e)$. Then

$$\begin{aligned}\operatorname{Tr}(\zeta_d)x &= \sum_{\tau \in \operatorname{Aut}(\mu_e)} \tau(\zeta_d)x = \sum_{\tau \in \operatorname{Aut}(\mu_e)} \tau(\zeta_d x) = \sum_{\substack{\tau \in \operatorname{Aut}(\mu_e) \\ b \in \mathcal{B}}} \tau(x_b \otimes \zeta_d b) = \sum_{b \in \mathcal{B}} \Big(x_b \otimes \sum_{\tau \in \operatorname{Aut}(\mu_e)} \tau(\zeta_d b)\Big) \\ &= \sum_{b \in \mathcal{B}} x_b \otimes \operatorname{Tr}(\zeta_d b) = \Big(\sum_{b \in \mathcal{B}} x_b \operatorname{Tr}(\zeta_d b)\Big) \otimes 1 \in M \otimes 1.\end{aligned}$$

It follows that $\operatorname{Tr}(\zeta_d)x_b = 0$ for all $b \neq 1$. We have that $\operatorname{Tr}(\zeta_d) \mid e$ by Lemma 3.14, hence multiplication by $\operatorname{Tr}(\zeta_d)$ is injective on M. Thus $x_b = 0$ for all $b \neq 1$, so $x = x_1 \otimes 1 \in M \otimes 1$. Hence $N^{(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*} = M \otimes 1$, as was to be shown. □

3.2 Diagonalizable maps

Definition 3.16. Let k be a commutative ring, let M be a k-module and let $f \in \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$. For $\lambda \in k$ and $N \subseteq M$ we define the *eigenspace of f in N at eigenvalue λ* to be $N(f,\lambda) = \{x \in N \mid f(x) = \lambda x\}$. We say f is *S-diagonalizable* for some subset $S \subseteq k$ if the natural map $\bigoplus_{\lambda \in S} M(f,\lambda) \to M$ is an isomorphism.

Lemma 3.17. *Let $f \in \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ be S-diagonalizable and $g \in \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ be T-diagonalizable. Then f and g commute if and only if the natural map*

$$\bigoplus_{\lambda \in S, \mu \in T} (M(f,\lambda) \cap M(g,\mu)) \to M \tag{1}$$

is an isomorphism.

Proof. Assume f and g commute. For all $y \in M(g,\mu)$ we have $(gf)(y) = (fg)(y) = f(\mu y) = \mu f(y)$, hence $f(y) \in M(g,\mu)$ and $fM(g,\mu) \subseteq M(g,\mu)$. Let $x \in M(f,\lambda)$ be given. Since g is T-diagonalizable, we may uniquely write $x = \sum_{\mu \in T} x_\mu$ with $x_\mu \in M(g,\mu)$ for all $\mu \in T$. Now $\sum_{\mu \in T} \lambda x_\mu = \lambda x = f(x) = \sum_{\mu \in T} f(x_\mu)$ and $f(x_\mu) \in M(g,\mu)$. Hence by uniqueness of decomposition we have $f(x_\mu) = \lambda x_\mu$, so $x_\mu \in M(f,\lambda) \cap M(g,\mu)$. Therefore $M(f,\lambda) = \bigoplus_{\mu \in T}(M(f,\lambda) \cap M(g,\mu))$. That (1) is an isomorphism then follows from S-diagonalizability of f.

Assume (1) is an isomorphism. Then for $x \in M(f,\lambda) \cap M(g,\mu)$ we have $f(g(x)) = \lambda\mu x = g(f(x))$, so by k-linearity we have $f(g(x)) = g(f(x))$ for all $x \in \sum_{\lambda \in S,\, \mu \in T}(M(f,\lambda) \cap M(g,\mu)) = M$. Thus f and g commute. □

Lemma 3.18. *Let M be a k-module and let $S \subseteq k$ be such that multiplication by $\lambda - \mu$ is injective on M for all pairwise distinct $\lambda, \mu \in S$. Then for all $f \in \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ the natural map $\bigoplus_{\lambda \in S} M(f,\lambda) \to M$ is injective.*

Proof. Assume the map is not injective. Then there exists a minimal finite non-empty $I \subseteq S$ such that $\sum_{\lambda \in I} m_\lambda = 0$ for some non-zero $m_\lambda \in M(f,\lambda)$. Let $\mu \in I$ and consider $J = I \setminus \{\mu\}$. Then $0 = \mu m_\mu - f(m_\mu) = \sum_{\lambda \in J}(f(m_\lambda) - \mu m_\lambda) = \sum_{\lambda \in J}(\lambda - \mu) m_\lambda$. By minimality of I we must have that $(\lambda - \mu) m_\lambda = 0$ for some $\lambda \in J$, hence $m_\lambda = 0$, a contradiction. Thus the map is injective. □

Corollary 3.19. *Let $f, g \in \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ be respectively S-diagonalizable and T-diagonalizable and let $U = \{\lambda\mu \mid \lambda \in S,\ \mu \in T\}$. If f and g commute and U satisfies the conditions to Lemma 3.18, then $f \circ g$ is U-diagonalizable.*

Proof. By Lemma 3.18 the natural map $\varphi : \bigoplus_{\nu \in U} M(fg,\nu) \to M$ is injective. Note $M(f,\lambda) \cap M(g,\mu) \subseteq M(fg,\lambda\mu)$ for all $\lambda \in S$ and $\mu \in T$, so by Lemma 3.17 we have $\sum_{\nu \in U} M(fg,\nu) \supseteq \sum_{\lambda \in S,\, \lambda \in T} M(f,\lambda) \cap M(g,\mu) = M$, so φ is surjective. We conclude that fg is U-diagonalizable. □

Remark 3.20. Each S-diagonalizable $f \in \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ gives a decomposition $\{M(f,s)\}_{s \in S}$ of M and conversely each decomposition $\{E_s\}_{s \in S}$ of M gives a morphism that sends $x \in E_s$ to sx. If we assume multiplication by $\lambda - \mu$ is injective for all distinct $\lambda, \mu \in S \subseteq k$, then this is a bijective correspondence. The monoid $G = \mathrm{End}_{\mathtt{Set}}(S)$ acts on the set of S-decompositions of M given by $(g, \{E_s\}_{s \in S}) \mapsto g_*\{E_s\}_{s \in S} = \{\sum_{t \in g^{-1}s} E_t\}_{s \in S}$ and consequently G acts on the set $D \subseteq \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ of S-diagonalizable morphisms. If $S = \mu_e$, then $\hat{\mathbb{Z}}/e\hat{\mathbb{Z}} \hookrightarrow G$ acts on D, which we will write as f^a for $f \in D$ and $a \in \hat{\mathbb{Z}}/e\hat{\mathbb{Z}}$.

3.3 Cyclic group gradings

In this section we take $e \in \mathbb{S}$ and let R be a not necessarily commutative algebra over a commutative ring k such that multiplication in R by integer divisors of e is injective. If k is a $\mathbb{Z}[\mu_e]$-algebra we can interpret μ_e-gradings of R as μ_e-diagonalizable k-algebra automorphisms as Proposition 3.21 will show. In the remainder of this section we work towards a generalization for when k is not necessarily a $\mathbb{Z}[\mu_e]$-algebra.

Proposition 3.21. *Assume k is a $\mathbb{Z}[\mu_e]$-algebra. Then we have mutually inverse bijections*

$$\begin{array}{lrcl} & \{\mu_e\text{-gradings of } R \text{ as a } k\text{-algebra}\} & \leftrightarrow & \{\sigma \in \mathrm{Aut}_{k\text{-}\mathtt{Alg}}(R) \,|\, \sigma \text{ is } \mu_e\text{-diagonalizable}\} \\ \textit{given by} & (R, \mu_e, \{R_\zeta\}_{\zeta\in\mu_e}) & \mapsto & \Big(r_\zeta \in R_\zeta \mapsto \zeta r_\zeta\Big) \\ \textit{and} & (R, \mu_e, \{R(\sigma,\zeta)\}_{\zeta\in\mu_e}) & \leftarrow\!\shortmid & \sigma. \end{array}$$

Proof. First we show both maps are well-defined.

($\leftarrow$) By μ_e-diagonalizability of σ we have that $\{R(\sigma,\zeta)\}_{\zeta\in\mu_e}$ is a decomposition of R as a k-module. Because $\sigma(1) = 1$ we have $1 \in R(\sigma, 1)$. For $x \in R(\sigma,\zeta)$ and $y \in R(\sigma,\xi)$ we have $\sigma(xy) = \sigma(x)\sigma(y) = (\zeta\xi)(xy)$ so also $R(\sigma,\zeta)\cdot R(\sigma,\xi) \subseteq R(\sigma,\zeta\xi)$. Hence $(R,\mu_e,\{R(\sigma,\zeta)\}_{\zeta\in\mu_e})$ is a grading of R as a k-algebra.

($\rightarrow$) Let σ be the k-module homomorphism given by $r_\zeta \mapsto \zeta r_\zeta$ for all $r_\zeta \in R_\zeta$, which is well defined since $\{R_\zeta\}_{\zeta\in\mu_e}$ is a decomposition of R. For $r_\zeta \in R_\zeta$ and $r_\xi \in R_\xi$ we have $r_\zeta r_\xi \in R_{\zeta\xi}$ so $\sigma(r_\zeta r_\xi) = \zeta\xi r_\zeta r_\xi = \sigma(r_\zeta)\sigma(r_\xi)$ and $\sigma(1) = 1$ as $1 \in R_1$. Hence σ is a k-algebra homomorphism by linearity. For distinct $\zeta, \xi \in \mu_e$ multiplication by $\zeta - \xi$ is injective on R by Lemma 3.13.2. Then by Lemma 3.18 the natural map $\bigoplus_{\zeta\in\mu_e} R(\sigma,\zeta) \to R$ is injective. Because $R_\zeta \subseteq R(\sigma,\zeta)$ for all ζ we have $R = \sum_{\zeta\in\mu_e} R_\zeta \subseteq \sum_{\zeta\in\mu_e} R(\sigma,\zeta)$, so the map must in fact be an isomorphism. We conclude that σ is μ_e-diagonalizable.

It follows trivially from Remark 3.20 that the given maps are each other's inverse. □

We now consider the ring $R' = R \otimes_\mathbb{Z} \mathbb{Z}[\mu_e]$, which is a $k' = k \otimes_\mathbb{Z} \mathbb{Z}[\mu_e]$-algebra. Multiplication by integer divisors of e is injective on R' by Proposition 3.15, so R' satisfies the conditions to Proposition 3.21. For $a \in (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ let τ_a be the the image of a in $\mathrm{Aut}_{k\text{-}\mathtt{Alg}}(R')$ under the action defined in Proposition 3.15. Now $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ has a left action on $\mathrm{Aut}_{k'\text{-}\mathtt{Alg}}(R')$ given by $(a,\sigma) \mapsto {}^a\sigma = \tau_a\sigma\tau_a^{-1}$. Furthermore, $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ has a right action on the set of μ_e-diagonalizable k'-module homomorphisms by Remark 3.20. Hence we may define the following.

Definition 3.22. We define

$$X_e(R) = \{\sigma \in \mathrm{Aut}_{k'\text{-}\mathtt{Alg}}(R') \,|\, \sigma \text{ is } \mu_e\text{-diagonalizable and } (\forall a \in (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*)\, {}^a\sigma = \sigma^a\}.$$

We will show that the $\sigma \in X_e(R)$, under the bijection of Proposition 3.21 applied to R', correspond to the k'-algebra gradings of R' obtained from gradings $(R,\mu_e,\{R_\zeta\}_{\zeta\in\mu_e})$ of R as $(R',\mu_e,\{R_\zeta \otimes_\mathbb{Z} \mathbb{Z}[\mu_e]\}_{\zeta\in\mu_e})$.

Lemma 3.23. *Let $\sigma \in X_e(R)$ be given. Then*

(1) *For each $a \in (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ and $\zeta \in \mu_e$ we have $\tau_a R'(\sigma,\zeta) = R'(\sigma,\zeta)$.*

(2) *For each $b \in \hat{\mathbb{Z}}/e\hat{\mathbb{Z}}$ also $\sigma^b \in X_e(R)$.*

Proof. (1) Let $x \in R'(\sigma,\zeta)$ and let $d\,|\,e$ be an integer such that $x, \tau_a(x) \in D = R'(\sigma^d, 1)$. Let $b \in \mathbb{Z}_{>0}$ be such that $ab \equiv 1 \mod d$. Then

$$\zeta\tau_a(x) = \tau_a(\zeta^b x) = \tau_a\sigma^b(x) = \sigma^a\tau_a\sigma^{b-1}(x) = \cdots = \sigma^{ab}\tau_a(x) = \sigma\tau_a(x)$$

as $\sigma^{ab}|_D = \sigma|_D$. Thus $\tau_a(x) \in R'(\sigma,\zeta)$ and $\tau_a R'(\sigma,\zeta) \subseteq R'(\sigma,\zeta)$. From this fact applied to $\tau_a^{-1} = \tau_{a^{-1}}$ instead we obtain $R'(\sigma,\zeta) = \tau_a\tau_{a^{-1}}R'(\sigma,\zeta) \subseteq \tau_a R'(\sigma,\zeta)$, proving equality.

(2) Now let $b \in \hat{\mathbb{Z}}/e\hat{\mathbb{Z}}$ be given. By definition σ^b is diagonalizable with $R'(\sigma^b,\zeta) = \sum_{\xi:\xi^b=\zeta} R'(\sigma,\xi)$ for all $\zeta \in \mu_e$. For all $\zeta \in \mu_e$, $a \in (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ and $x \in R'(\sigma,\zeta)$ we have using (1) that $\tau_a\sigma^b(x) = \tau_a(\zeta^b x) = \zeta^{ab}\tau_a(x) = \sigma^{ab}\tau_a(x)$, so $\tau_a\sigma^b = \sigma^{ab}\tau_a$ by linearity. Hence $\sigma^b \in X_e(R)$. □

A consequence of (2) which we will use later is that $X_e(R)$ is closed under exponentiation and taking inverses. We may now prove the following.

Lemma 3.24. *Let Y be the set of k'-algebra gradings $(R',\Gamma,\{R'_\gamma\}_{\gamma\in\Gamma})$ such that $\tau_a R'_\gamma = R'_\gamma$ for all $a \in (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$. Then we have mutually inverse bijections*

$$\begin{array}{lrcl} & \{\text{gradings of } R \text{ as } k\text{-algebra}\} & \leftrightarrow & Y \\ \textit{given by} & (R,\Gamma,\{R_\gamma\}_{\gamma\in\Gamma}) & \mapsto & (R',\Gamma,\{R_\gamma \otimes_\mathbb{Z} \mathbb{Z}[\mu_e]\}_{\gamma\in\Gamma}) \\ \textit{and} & (R,\Gamma,\{R'_\gamma \cap R\}_{\zeta\in\mu_e}) & \leftarrow\!\shortmid & (R',\Gamma,\{R'_\gamma\}_{\gamma\in\Gamma}). \end{array}$$

Proof. We show both maps are well-defined.

($\to$) For each grading $\overline{R}$ its image $\overline{R'}$ is a grading of R' simply by the distributivity of the tensor product over the direct sum. That it satisfies the additional conditions follows from the fact that τ_a is an isomorphism and acts on the second component of each homogeneous component. Hence the mapping is well-defined.

($\leftarrow$) Let $G = (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$. For each grading $\overline{R'} = (R', \Gamma, \{R'_\gamma\}_{\gamma\in\Gamma}) \in Y$ the group G respects the homogeneous components, so by Proposition 3.15 we have

$$R = (R')^G = \Big(\bigoplus_{\gamma\in\Gamma} R'_\gamma\Big)^G = \bigoplus_{\gamma\in\Gamma}(R'_\gamma)^G = \bigoplus_{\gamma\in\Gamma}(R'_\gamma \cap R).$$

Thus the image of $\overline{R'}$ is in fact a k-algebra grading of R and the mapping is well-defined.

That the maps are each other's inverse follows readily from the fact that the natural map $R \to R'$ is injective by Proposition 3.15. □

Theorem 3.25. *Let $e \in \mathbb{S}$, k a commutative ring and R a k-algebra in which multiplication by integer divisors of e is injective. Then we have mutually inverse bijections*

$$\begin{array}{lrcl} & \{\mu_e\text{-gradings of } R \text{ as } k\text{-algebra}\} & \leftrightarrow & X_e(R) \\ \textit{given by} & (R, \mu_e, \{R_\zeta\}_{\zeta\in\mu_e}) & \mapsto & \Big(r_\zeta \otimes 1 \in R_\zeta \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e] \mapsto r_\zeta \otimes \zeta\Big) \\ \textit{and} & (R, \mu_e, \{R(\sigma,\zeta)\}_{\zeta\in\mu_e}) & \leftarrow\!\shortmid & \sigma. \end{array}$$

Proof. Let Y be as in Lemma 3.24. Using Lemma 3.23, one easily verifies that the image of Y in $\mathrm{Aut}_{k\otimes_{\mathbb{Z}}\mathbb{Z}[\mu_e]\text{-}\mathtt{Alg}}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e])$ under the correspondence of Proposition 3.21 is precisely $X_e(R)$. Now the given maps are simply a composition of those of Proposition 3.21 and Lemma 3.24, making them well-defined and each other's inverse. □

Corollary 3.26. *Assume k is a field with $\mathrm{char}(k) \neq 2$. If $k \subseteq L$ is a field extension of degree 2, then L has exactly one non-trivial efficient k-algebra grading.*

Proof. By Proposition 2.6 the k-algebra L can (up to unique isomorphism) only be non-trivially efficiently graded with μ_2. Since $\mathrm{char}(k) \neq 2$ the extension $k \subseteq L$ is Galois. Hence $X_2(L) = \mathrm{Aut}_{k\text{-}\mathtt{Alg}}(L)$ contains $[L : k] = 2$ elements, one of which induces the trivial grading. □

Example 3.27. The correspondence from Theorem 3.25 is not powerful enough to find μ_p-gradings of fields of characteristic p. Let $\mathbb{F}_{p^n}$ be the unique finite field extension of degree n of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. If $(\mathbb{F}_{p^n}, \mu_p, \{R_\zeta\}_{\zeta\in\mu_p})$ is a non-trivial grading, then $p \,|\, n$ and $R_1 = \mathbb{F}_{p^{n/p}}$ by Proposition 2.6. For $\alpha \in R_\zeta$ we have $\alpha^p \in R_1 = \mathbb{F}_{p^{n/p}}$, hence $\alpha \in \mathbb{F}_{p^{n/p}}$ as the Frobenius automorphism $x \mapsto x^p$ of $\mathbb{F}_{p^n}$ sends $\mathbb{F}_{p^{n/p}}$ to itself. Thus $\alpha \in R_\zeta \cap R_1$ implies $\alpha = 0$ if $\zeta \neq 1$, hence $R_\zeta = 0$, which is a contradiction. Thus no non-trivial μ_p-grading of $\mathbb{F}_{p^n}$ exists.

Example 3.28. Consider $K_n = \mathbb{Q}(\sqrt[n]{p})$ for p prime and $n \geq 1$ and note that $[K_n : \mathbb{Q}] = n$ since $X^n - p$ is an irreducible polynomial over $\mathbb{Q}$ by Eisenstein's Criterion. Hence to compute all cyclic gradings of K_n it suffices to consider μ_n-gradings.

Assume n is odd or $\sqrt{p} \notin \mathbb{Q}(\zeta_n)$. We then have that $K'_n := K_n \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_n] \cong \mathbb{Q}(\sqrt[n]{p}, \zeta_n)$ by Theorem A of Jacobson and Vélez [6]. Hence $\mathrm{Aut}_{\mathbb{Z}[\mu_n]\text{-}\mathtt{Alg}}(K'_n) = \{\sigma_i = (\sqrt[n]{p} \mapsto \zeta_n^i \cdot \sqrt[n]{p}) \,|\, i \in \mathbb{Z}/n\mathbb{Z}\}$. The grading corresponding to σ_1 by Theorem 3.25 is $\overline{R} = (K_n, \mu_n, \{p^{i/n} \cdot \mathbb{Q}\}_{\zeta_n^i\in\mu_n})$ and the grading corresponding to σ_i is simply $f_*\overline{R}$ with $f : \mu_n \to \mu_n$ given by $\zeta \mapsto \zeta^i$. It follows that these are all efficient gradings of K_n and thus $\overline{R}$ is the universal abelian group grading. In fact, by Proposition 2.6 it is the universal grid-grading.

3.4 Abelian torsion group gradings

In this section we generalize Theorem 3.25 to gradings with arbitrary abelian e-torsion groups. This relies on a theorem of Pontryagin on dual groups, as defined in Definition 3.9.

Theorem 3.29 (Pontryagin, Theorem 1.7.2 of [4]). *There is a natural isomorphism* $\Phi : \mathrm{id}_{\mathtt{LCA}} \to \widehat{\widehat{\cdot}}$ *with the component* $\Phi(\Gamma)$ *at* $\Gamma \in \mathrm{obj}(\mathtt{LCA})$ *given by* $\gamma \mapsto \mathrm{ev}_\gamma$*, where* $\mathrm{ev}_\gamma \in \widehat{\widehat{\Gamma}}$ *is evaluation map* $\chi \mapsto \chi(\gamma)$*.* □

Corollary 3.30. *The functor* $\widehat{\cdot}$ *is self-adjoint, i.e. there is a natural isomorphism between the two bifunctors* $\mathtt{LCA}^2 \to \mathtt{Set}$ *given by* $(\Gamma, \Delta) \mapsto \mathrm{Hom}_{\mathtt{LCA}}(\widehat{\Gamma}, \Delta)$ *respectively* $(\Gamma, \Delta) \mapsto \mathrm{Hom}_{\mathtt{LCA}}(\widehat{\Delta}, \Gamma)$*.* □

Remark 3.31. Let $e \in \mathbb{S}$, let k be a commutative ring and R be a k-algebra on which multiplication by integer divisors of e is injective. We then equip $R' = R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ with the discrete topology and $A = \mathrm{Aut}_{k\otimes_{\mathbb{Z}}\mathbb{Z}[\mu_e]\text{-}\mathtt{Alg}}(R')$ with the compact-open topology, making it a topological group. Note that since R' is discrete, $\{v(x,y) \,|\, x, y \in R'\}$ with $v(x,y) = \{f \in A \,|\, f(x) = y\}$ is a subbase of A.

Proposition 3.32. *Let* e*,* k *and* R *be as in Remark 3.31. Let* $\Delta \subseteq X_e(R)$ *be a compact abelian subgroup of* A*. Then* $\overline{R} = (R, \widehat{\Delta}, \{R_\chi\}_{\chi\in\widehat{\Delta}})$ *with* $R_\chi = \bigcap_{\delta\in\Delta} R(\delta, \chi(\delta))$ *is a grading.*

Proof. If we replace $\widehat{\Delta}$ by μ_e^Δ in the definition of $\overline{R}$, then the resulting grading is simply the joint grading of the gradings corresponding to the $\delta \in \Delta$ under the bijection of Theorem 3.25. To show $\overline{R}$ is a grading it suffices by Lemma 2.11 to verify that the natural map $f : \bigoplus_{\chi\in\widehat{\Delta}} R'_\chi \to R'$ is surjective, with $R'_\chi = \bigcap_{\delta\in\Delta} R'(\delta, \chi(\delta))$.

Let $x \in R'$ be given. Then $\{v(x,y) \,|\, y \in R'\}$ is an open cover of Δ so by compactness it has a finite subcover. Hence Δx is finite and the evaluation map $\mathrm{ev}_x : \Delta \to \Delta x$ has only finitely many fibers. For each $y \in \Delta x$ take a representative $\delta_y \in \mathrm{ev}_x^{-1}\{y\}$ and note that since the δ_y commute pair-wise we may write $x = \sum_{a\in\mu_e^{\Delta x}} x_a$ with $x_a \in S_a = \bigcap_{y\in\Delta x} R'(\delta_y, a(y))$ by Lemma 3.17. It now suffices to show that $x_a \in \sum_{\chi\in\widehat{\Delta}} R'_\chi$. Fix some $a \in \mu_e^{\Delta x}$ such that $x_a \neq 0$ and let $\chi = a \circ \mathrm{ev}_x : \Delta \to \mu_e$. We have $(\chi(\delta\gamma) - \chi(\delta)\chi(\gamma))x_a = (\delta\gamma)(x_a) - \delta(\gamma(x_a)) = 0$ hence $\chi(\delta\gamma) = \chi(\delta)\chi(\gamma)$ by Lemma 3.13.2. As $\chi(1) = 1$ we have that χ is a group homomorphism. Similarly, since $\chi^{-1}\{\zeta\} = v(x_a, \zeta x_a) \cap \Delta$ is open for all $\zeta \in \mu_e$ we even have $\chi \in \widehat{\Delta}$. Each $\delta \in \Delta$ commutes with all representatives δ_v so $\delta(x_a) \in S_a$. Then from $\sum_{a\in\mu_e^{\Delta x}} \delta(x_a) = \delta(x) = \delta_{\delta(x)}(x) = \sum_{a\in\mu_e^{\Delta x}} \chi(\delta) \cdot x_a$ it follows that $x_a \in R_\chi$. Hence f is surjective. We conclude that $\overline{R}$ is a grading. □

Remark 3.33. Theorem 3.25 can be considered a special case of Proposition 3.32. Let e, k and R be as in Remark 3.31. For any $\sigma \in X_e(R)$ consider $\Delta = \{\sigma^a \,|\, a \in \hat{\mathbb{Z}}/e\hat{\mathbb{Z}}\}$, which is a compact abelian subgroup of $X_e(R)$ by Lemma 3.23.2. Then the map $f_\sigma \in \mathrm{Hom}_{\mathtt{LCA}}(\widehat{\mu}_e, \Delta)$ given by $(\zeta \mapsto \zeta^a) \mapsto \sigma^a$ is continuous and surjective. Corollary 3.30 applied to $\widehat{f_\sigma}$ gives a injective morphism of groups $\varphi : \widehat{\Delta} \to \mu_e$. The μ_e-grading corresponding to σ by Theorem 3.25 is simply $\varphi_*\overline{R}$, with $\overline{R}$ the $\widehat{\Delta}$-grading corresponding to Δ by Proposition 3.32.

Theorem 3.34. *Let* e*,* k*,* R *and* A *be as in Remark 3.31. Write* $\mathtt{Ab}_e \subseteq \mathtt{Ab}$ *for the full subcategory of* e*-torsion groups. Let* $G : \mathtt{Ab}_e \to \mathtt{Set}$ *be the functor that sends* Γ *to the set of* Γ*-gradings and* $H : \mathtt{Ab}_e \to \mathtt{Set}$ *the functor that sends* Γ *to* $\{\varphi \in \mathrm{Hom}_{\mathtt{TGrp}}(\widehat{\Gamma}, A) \,|\, \mathrm{im}(\varphi) \subseteq X_e(R)\}$*. Then we have a natural isomorphism* $\Phi : G \to H$ *where the component at* $\Gamma \in \mathrm{obj}(\mathtt{Ab}_e)$ *is given by*

$$\begin{aligned}
\Phi(\Gamma) : \{\Gamma\text{-}\textit{gradings of } R \textit{ as } k\text{-}\textit{algebra}\} &\to \{\varphi \in \mathrm{Hom}_{\mathtt{TGrp}}(\widehat{\Gamma}, A) \mid \mathrm{im}(\varphi) \subseteq X_e(R)\} \\
\overline{R} = (R, \Gamma, \{R_\gamma\}_{\gamma\in\Gamma}) &\mapsto \Big(\chi \mapsto (x \in R_\gamma \mapsto \chi(\gamma) \cdot x)\Big) \\
\left(R, \Gamma, \Big\{ \bigcap_{\chi\in\widehat{\Gamma}} R(\varphi(\chi), \chi(\gamma)) \Big\}_{\gamma\in\Gamma}\right) &\mapsfrom \varphi.
\end{aligned}$$

Proof. We show that for fixed $\Gamma \in \mathrm{obj}(\mathtt{Ab}_e)$ the maps $G(\Gamma) \to H(\Gamma)$ and $H(\Gamma) \to G(\Gamma)$ are well-defined, as it then easily follows that the maps are mutually inverse and that Φ is a natural transformation.

($\to$) Note that since Γ is e-torsion we have $\chi(\Gamma) \subseteq \mu_e$ for all $\chi \in \widehat{\Gamma}$. For a Γ-grading $\overline{R}$ it is then clear that the corresponding φ is a well-defined $k \otimes \mathbb{Z}[\mu_e]$-algebra isomorphism with $\varphi(\chi) \in X_e(R)$ for all $\chi \in \widehat{\Gamma}$. It remains to show that it is continuous. By Remark 3.31 it suffices to show that $\varphi^{-1}v(x,y)$ is open for all $x, y \in R'$. Write $x = \sum_{\gamma\in\Gamma} x_\gamma \otimes u_\gamma$ with $x_\gamma \in R_\gamma$ and $u_\gamma \in \mathbb{Z}[\mu_e]$ for all $\gamma \in \Gamma$. If $y \notin \sum_{\gamma\in\Gamma} \mu_e \cdot (x_\gamma \otimes u_\gamma)$, then $\varphi^{-1}v(x,y) = \emptyset$ is open. Otherwise we may write $y = \sum_{\gamma\in\Gamma} x_\gamma \otimes (\zeta_\gamma \cdot u_\gamma)$ for some $\zeta_\gamma \in \mu_e$ and $\varphi^{-1}v(x,y) = \bigcap_{\gamma : x_\gamma \neq 0} \varphi^{-1}v(x_\gamma \otimes u_\gamma, x_\gamma \otimes (\zeta_\gamma u_\gamma))$. Thus without loss of generality we have $x = x_\gamma \otimes u_\gamma \neq 0$ and $y = \zeta_\gamma x$. By Pontryagin the evaluation map $\mathrm{ev}_\gamma : \widehat{\Gamma} \to \mathbb{T}$ is continuous. Since $x \neq 0$ and multiplication by $\chi(\gamma) - \zeta_\gamma$ is injective when $\chi(\gamma) \neq \zeta_\gamma$ for all $\chi \in \widehat{\Gamma}$ by Lemma 3.13.2 we get that

$$\varphi^{-1}(x, \zeta_\gamma x) = \{\chi \in \widehat{\Gamma} \mid \varphi(\chi)(x) = \zeta_\gamma x\} = \{\chi \in \widehat{\Gamma} \mid (\chi(\gamma) - \zeta_\gamma)x = 0\} = \mathrm{ev}_\gamma^{-1}(\zeta_\gamma)$$

is open. Hence φ is continuous, as was to be shown.

($\leftarrow$) Let $\varphi \in H(\Gamma)$ be given and let $\Delta = \mathrm{im}(\varphi)$, which is a compact abelian group. Since φ factors through Δ we get a morphism $f : \widehat{\Gamma} \to \Delta$ and thus by Pontryagin a morphism $g : \widehat{\Delta} \to \Gamma$. Then $\overline{S} = (R, \widehat{\Delta}, S_\chi)$ with $S_\chi = \bigcap_{\delta\in\Delta} R(\delta, \chi(\delta))$ is a grading by Proposition 3.32, and the grading corresponding to φ is precisely $g_*\overline{S}$. Hence $\Phi(\Gamma)$ is well-defined and bijective, as was to be shown. □

Theorem 3.34 essentially states that each grading of R with an abelian e-torsion group can be realized as the joint gradings of several μ_e-gradings. These joint gradings exist precisely when all involved $\sigma \in X_e(R)$ commute pair-wise, motivating the following theorem.

Theorem 3.35. *Let $e \in \mathbb{S}$, let k be a commutative ring and let R be a k-algebra on which multiplication by integer divisors of e is injective. Then R has a universal abelian e-torsion grading if and only if $X_e(R)$ is a compact abelian group. If these equivalent conditions hold, then the universal grading is given by Proposition 3.32 applied to $\Delta = X_e(R)$.*

Proof. By Theorem 3.34 the functors G and H as defined there are naturally isomorphic. Thus R has a universal grading if and only if H is representable.

Assume $X_e(R)$ is a compact abelian group. Then $\mathrm{Y} = \widehat{X_e(R)}$ is a discrete group such that $\widehat{\mathrm{Y}} \cong X_e(R)$ by Pontryagin. Corollary 3.30 now provides the natural isomorphism $\mathrm{Hom}_{\mathtt{Ab}}(\mathrm{Y}, \_) \cong \mathrm{Hom}_{\mathtt{LCA}}(\widehat{\_}, X_e(R)) = H$. Hence H is representable.

Assume H is representable, so that we have an $\mathrm{Y} \in \mathrm{obj}(\mathtt{Ab})$ and natural isomorphism $\Phi : \mathrm{Hom}_{\mathtt{LCA}}(\mathrm{Y}, \_) \to H$. By Yoneda's lemma Φ corresponds to $\varphi = \Phi(\mathrm{Y})(\mathrm{id}_\mathrm{Y}) \in H(\mathrm{Y})$, and since Φ is an isomorphism we have that for all $\Gamma \in \mathrm{obj}(\mathtt{Ab})$ and $\psi \in H(\Gamma)$ there exists a unique $f \in \mathrm{Hom}_{\mathtt{Ab}}(\mathrm{Y}, \Gamma)$ such that $\psi = \Phi(\Gamma)(f)(\varphi)$. Let $\sigma \in X_e(R)$ be given and define $\psi : \widehat{\mu_e} \to X_e(R)$ by $(\zeta \mapsto \zeta^a) \mapsto \sigma^a$ as in Remark 3.33. Then $\psi \in H(\mu_e)$, so there exists a $f \in \mathrm{Hom}_{\mathtt{Ab}}(\mathrm{Y}, \mu_e) = \widehat{\mathrm{Y}}$ such that $\psi = \widehat{f}_*(\varphi)$. Hence $\sigma = \psi(\mathrm{id}) = \varphi(\widehat{f}(\mathrm{id})) = \varphi(f)$, so $X_e(R) = \varphi\widehat{\mathrm{Y}}$. Since φ is a morphism of topological groups and $\widehat{\mathrm{Y}}$ is compact, we have that $X_e(R)$ is a compact abelian group. □

If $\mathrm{Aut}_{k'\text{-}\mathtt{Alg}}(R')$ is finite, as is the case when R is a finite product of number fields as will follow from Proposition 4.12, then it certainly is compact. In this case R has a universal abelian group grading if and only if the elements of $X_\infty(R)$ commute pair-wise. In Example 6.6 we construct a ring R such that $X_\infty(R)$ is abelian though no universal abelian torsion group-grading of R exists.

3.5 Computing joint gradings

The correspondence from Theorem 3.34 reduces the problem of Theorem 1.3, finding all gradings with cyclic groups of prime power order, to the problem of finding a specific subset of some automorphism group. For this reduction to be of practical use we need to show that computing the grading corresponding to the automorphism can be done in polynomial time.

Let k be either $\mathbb{Z}$ or $\mathbb{Q}$. If R and S are free k-modules represented by a basis $\mathcal{A}$ respectively $\mathcal{B}$, then we have a canonical basis $\{a \otimes b \mid a \in \mathcal{A},\, b \in \mathcal{B}\}$ for $R \otimes_k S$. Computationally, if $A = (a_{hij})_{h,i,j\in I}$ and $B = (b_{hij})_{h,i,j\in J}$ are structure constants for commutative k-algebras R respectively S, we construct $R \otimes_k S$ as the k-algebra defined by the structure constants $A \otimes B := (a_{hij} \cdot b_{h'i'j'})_{(h,h'),(i,i'),(j,j')\in I\times J}$. Note that the length of $A \otimes B$ is bounded by a polynomial in the length of (A, B). If 1 is in the basis of S, or equivalently for some $h' \in J$ we have $b_{h'i'j'} = \mathbb{1}(i' = j')$, then we can easily construct the natural morphism $\epsilon : R \to R \otimes_k S$ as the map sending the h-th basis vector e_h to $e_{(h,h')}$ for all $h \in I$. Similarly, we can construct a left inverse k-module homomorphism $\pi : R \otimes_k S \to R$ of ϵ by sending $e_{(i,i')}$ to e_i and $e_{(i,j')}$ to zero when $j' \neq i'$. In particular we can do this for the natural map $R \to R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ when we are free to choose $\{1, \zeta, \zeta^2, \dots, \zeta^{\varphi(e)-1}\}$ as basis of $\mathbb{Z}[\mu_e]$.

Using the kernel algorithm from [7], we may compute a basis of the kernel of any k-module homomorphism σ in polynomial time with respect to the length of the matrix σ. If $\sigma_1, \dots, \sigma_l : M \to N$ are k-module homomorphism we may compute $\bigcap_{i=1}^{l} \ker(\sigma_i)$ as the kernel of the map $x \mapsto (\sigma_1(x), \dots, \sigma_l(x))$, which can then be done in polynomial time with respect to the length of $(\sigma_1, \dots, \sigma_l)$.

Proposition 3.36. *Let $e \in \mathbb{Z}_{\geq 1}$, let $k \in \{\mathbb{Z}, \mathbb{Q}\}$ and let R be a free k-algebra represented by structure constants. Let $\sigma_1, \dots, \sigma_l$ be a sequence of $k[\mu_e]$-algebra endomorphisms of $R' = R \otimes_k k[\mu_e]$ represented by k-valued matrices. Write $K_{(\zeta_1,\dots,\zeta_l)} = \bigcap_{i=1}^{l} R(\sigma_i, \zeta_i)$ for $\zeta_1, \dots, \zeta_l \in \mu_e^l$. We can compute the sets $Z = \{z \in \mu_e^l \mid K_z \neq 0\}$ and $\mathcal{K} = \{K_z\}_{z \in Z}$ and verify that $\mathcal{K}$ is a decomposition of R in polynomial time with respect to the length of the input $(R, e, \sigma_1, \dots, \sigma_l)$.*

Proof. Let $\epsilon : R \to R'$ and $\pi : R' \to R$ be as before and for $\zeta \in \mu_e$ let $A_\zeta : R' \to R'$ be the multiplication by ζ, all which can be computed in polynomial time. Then for $i \leq l$ and $\zeta \in \mu_e$ define $M_{i,\zeta} = (\sigma_i - A_\zeta) \cdot \epsilon$ and note that $\ker(M_{i,\zeta}) = R(\sigma_i, \zeta)$. Let $Z_m = \{(\zeta_1, \dots, \zeta_m) \in \mu_e^m \mid \bigcap_{i=1}^{m} R(\sigma_i, \zeta_i) \neq 0\}$. Note that $\#Z_m$ is at most the rank of R, which in turn is bounded by the length of its encoding. We can thus compute Z_{m+1} recursively from Z_m by computing $\bigcap_{i=1}^{m+1} R(\sigma_i, \zeta_i)$ for all $(\zeta_1, \dots, \zeta_m) \in Z_m$ and $\zeta_{m+1} \in \mu_e$. Computation of $\bigcap_{i=1}^{m+1} R(\sigma_i, \zeta_i)$ can be done in polynomial time as discussed before using the kernel algorithm applied to the map $x \mapsto (M_{i,\zeta_1} x, \dots, M_{m+1,\zeta_{m+1}} x)$, so we may compute Z_{m+1} from Z_m in polynomial time. Hence we may compute $Z = Z_l$ in polynomial time, as well as K_z for all $z \in Z$, as was to be shown. For each K_z we have a basis, together giving a basis of $\sum_{z \in Z} K_z$. To verify $\sum_{z \in Z} K_z = R$ we simply check whether the matrix associated to the map $B : \bigoplus_{z \in Z} K_z \to R$ has $\det(B) \in k^*$, which we may compute using Theorem 6.6 from [8]. □

4 Automorphisms and wreaths

In order to understand gradings of rings in terms of Theorem 3.25, we first need to understand the automorphism group $\mathrm{Aut}_{\mathbb{Z}[\mu_e]}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e])$. We describe this group using a general construction involving wreaths in the case R is a product of fields.

4.1 Wreaths

In this subsection we assume $\mathcal{C}$ to be a small groupoid. We will define morphisms on subsets of $\mathrm{obj}(\mathcal{C})$, which collectively form a new small groupoid, called the power groupoid. This gives us a group $\mathrm{wr}(\mathcal{C})$ which later turns up as the automorphism group of a product of fields.

Definition 4.1. We define the *power category* $2^{\mathcal{C}}$ *of* $\mathcal{C}$ as follows. Take $\mathrm{obj}(2^{\mathcal{C}}) = \{X \mid X \subseteq \mathrm{obj}(\mathcal{C})\}$ the power set of $\mathrm{obj}(\mathcal{C})$ and for $X, Y \in \mathrm{obj}(2^{\mathcal{C}})$ let

$$\mathrm{Hom}_{2^{\mathcal{C}}}(X,Y) = \big\{ \big((\sigma_K)_{K\in X}, s\big) \,\big|\, s \in \mathrm{Iso}_{\mathtt{Set}}(X,Y),\ (\forall K \in X)\, \sigma_K \in \mathrm{Hom}_{\mathcal{C}}(K, s(K)) \big\}.$$

For $\rho = ((\rho_K)_{K\in X}, r) \in \mathrm{Hom}_{2^{\mathcal{C}}}(X,Y)$ and $\sigma = ((\sigma_K)_{K\in Y}, s) \in \mathrm{Hom}_{2^{\mathcal{C}}}(Y,Z)$ with $X,Y,Z \in \mathrm{obj}(2^{\mathcal{C}})$ define the composition

$$\sigma \circ \rho := \big((\sigma_{r(K)} \circ \rho_K)_{K\in X}, s \circ r\big) \in \mathrm{Hom}_{2^{\mathcal{C}}}(X,Z).$$

For $X \in \mathrm{obj}(2^{\mathcal{C}})$ we have $\mathrm{id}_X = ((\mathrm{id}_K)_{K\in X}, \mathrm{id}) \in \mathrm{Hom}_{2^{\mathcal{C}}}(X,X)$ as identity. For $W, X, Y \in \mathrm{obj}(2^{\mathcal{C}})$ such that $W \subseteq X$ and $\sigma = ((\sigma_K)_{K\in X}, s) \in \mathrm{Hom}_{2^{\mathcal{C}}}(X,Y)$ we define $\sigma|_W = ((\sigma_K)_{K\in W}, s|_W) \in \mathrm{Hom}_{2^{\mathcal{C}}}(W, s(W))$ as the *restriction of* σ *to* W, where $s|_W \in \mathrm{Iso}_{\mathtt{Set}}(W, s(W))$ is the restriction of s to W.

It is easy to verify that $2^{\mathcal{C}}$ is a category.

Lemma 4.2. *The category* $2^{\mathcal{C}}$ *is a groupoid. Specifically, each* $\sigma = ((\sigma_K)_K, s) \in \mathrm{Hom}_{2^{\mathcal{C}}}(X,Y)$ *has an inverse*

$$\sigma^{-1} = \big(((\sigma_{s^{-1}(L)})^{-1})_{L\in Y}, s^{-1}\big) \in \mathrm{Hom}_{2^{\mathcal{C}}}(Y,X) \qquad \square$$

If we let $\mathtt{SGd}$ be the category of small groupoids with as morphisms the functors which are bijective on the set of objects, then $\mathtt{SGd}$ is a groupoid and $2^{-} : \mathtt{SGd} \to \mathtt{SGd}$ is a functor. Namely, for each $F \in \mathrm{Iso}_{\mathtt{SGd}}(\mathcal{C}, \mathcal{D})$ we obtain $2^F : 2^{\mathcal{C}} \to 2^{\mathcal{D}}$ by applying F 'coordinate-wise'.

Definition 4.3. Define the *wreath of* $\mathcal{C}$ as $\mathrm{wr}(\mathcal{C}) = \mathrm{End}_{2^{\mathcal{C}}}(\mathrm{obj}(\mathcal{C}))$, which is a group by Lemma 4.2.

For the sake of clarity, we will use the Latin alphabet for permutations in $\mathrm{Aut}_{\mathtt{Set}}(\mathrm{obj}(\mathcal{C}))$ and the Greek alphabet for elements of $\hom(\mathcal{C})$ in the context of $\mathrm{wr}(\mathcal{C})$, as in Definition 4.1. For the sake of brevity, we will assume the following questionable correspondence between characters

Latin	a	b	o	r	s	t	u
Greek	α	β	ω	ρ	σ	τ	υ

such that for example $\alpha = ((\alpha_K)_{K\in\mathrm{obj}(\mathcal{C})}, a)$ is implicit when we take $\alpha \in \mathrm{wr}(\mathcal{C})$.

Lemma 4.4. *If* $\mathcal{C}$ *is connected, then for any* $K \in X = \mathrm{obj}(\mathcal{C})$ *we have an isomorphism of groups* $\mathrm{wr}(\mathcal{C}) \cong \mathrm{Aut}_{\mathcal{C}}(K)^X \rtimes \mathrm{Aut}_{\mathtt{Set}}(X)$*, where the action of* $\mathrm{Aut}_{\mathtt{Set}}(X)$ *on* $\mathrm{Aut}_{\mathcal{C}}(K)^X$ *is given by* ${}^s(\sigma_L)_{L\in X} = (\sigma_{s^{-1}(L)})_{L\in X}$.

Proof. Since all $L \in X$ are isomorphic, we can choose isomorphisms $f_L \in \mathrm{Hom}_{\mathcal{C}}(L,K)$ for all $L \in X$. Then define the map

$$\begin{aligned} F : \mathrm{Aut}_{\mathcal{C}}(K)^X \rtimes \mathrm{Aut}_{\mathtt{Set}}(X) &\to \mathrm{wr}(\mathcal{C}) \\ (\sigma_L)_{L\in X} \cdot s &\mapsto \big((f_{s(L)}^{-1} \sigma_{s(L)} f_L)_{L\in X}, s\big). \end{aligned}$$

It is routine verification that this is in fact an isomorphism. $\square$

In the general case, we can decompose $\mathcal{C}$ into connected components.

Proposition 4.5. *If the elements of $S \subseteq \mathrm{obj}(2^{\mathcal{C}})$ are pair-wise disconnected, then $\mathrm{Aut}_{2^{\mathcal{C}}}(\bigcup_{X\in S} X) \cong \prod_{X\in S} \mathrm{Aut}_{2^{\mathcal{C}}}(X)$. If $S = \mathrm{obj}(\mathcal{C})/{\cong}$ is the set of isomorphism classes of $\mathcal{C}$, then*

$$\mathrm{wr}(\mathcal{C}) \cong \prod_{X\in S} \mathrm{Aut}_{2^{\mathcal{C}}}(X) \cong \prod_{[K]\in S} \Big(\mathrm{Aut}_{\mathcal{C}}(K)^{[K]} \rtimes \mathrm{Aut}_{\mathtt{Set}}([K]) \Big). \qquad \square$$

By definition, an action of a group Γ on an object A in some category $\mathcal{D}$ is simply a homomorphism $\Gamma \to \mathrm{Aut}_{\mathcal{D}}(A)$ in the category of groups. If we take $A = \mathcal{C}$ to be an object in the category $\mathcal{D} = \mathtt{Cat}$ of small categories, then $\mathrm{Aut}_{\mathtt{Cat}}(\mathcal{C})$ is the set of all invertible functors $F : \mathcal{C} \to \mathcal{C}$. In particular, a group can act on a category. Note that each $F \in \mathrm{Aut}(\mathcal{C})$ induces a unique pair of permutations φ of $\hom(\mathcal{C})$ and f of $\mathrm{obj}(\mathcal{C})$. Hence if Γ acts on $\mathcal{C}$, it induces an action on the set of objects of $\mathcal{C}$. As we will show, a nice property of $\mathrm{wr}(\mathcal{C})$ is that it acts on $\mathcal{C}$, and that any action of Γ on $\mathcal{C}$ induces an action of Γ on $\mathrm{wr}(\mathcal{C})$.

Lemma 4.6. *There is a natural action $\mathrm{wr}(\mathcal{C}) \to \mathrm{Aut}_{\mathtt{SGd}}(\mathcal{C})$ given by sending $\sigma \in \mathrm{wr}(\mathcal{C})$ to the functor defined by*

$$A \mapsto s(A) \quad \text{and} \quad f \mapsto \sigma_B \circ f \circ (\sigma_A)^{-1}$$

for all $A, B \in \mathrm{obj}(\mathcal{C})$ and $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. $\square$

If we take $\mathcal{C}$ to be a group, which is a groupoid with a single object, then $\mathrm{wr}(\mathcal{C}) \cong \mathrm{aut}(\mathcal{C})$ and the action of Lemma 4.6 is simply conjugation, such that the image of $\mathrm{wr}(\mathcal{C})$ in $\mathrm{Aut}_{\mathtt{SGd}}(\mathcal{C})$ equals the group of inner automorphisms of $\mathcal{C}$.

Remark 4.7. If we have a group action $\varphi : \Gamma \to \mathrm{Aut}_{\mathtt{SGd}}(\mathcal{C})$, then we also have an action $(2{-})_{\mathcal{C},\mathcal{C}} \circ \varphi$ of Γ on $2^{\mathcal{C}}$, with $(2{-})_{\mathcal{C},\mathcal{C}}$ the restriction of $2{-}$ to $\mathrm{Hom}_{\mathtt{SGd}}(\mathcal{C}, \mathcal{C})$. This induces an action $\Gamma \to \mathrm{wr}(\mathcal{C})$ and in particular ensures $\mathrm{wr}(\mathcal{C}) \rtimes \Gamma$ is defined.

Instead of letting Γ act on $\mathcal{C}$ after taking its wreath, we can also combine $\mathcal{C}$ and Γ into a single category first.

Definition 4.8. Let Γ be a group with an action on $\mathcal{C}$. We define the *semi-direct product* $\mathcal{C} \rtimes \Gamma$ of $\mathcal{C}$ and Γ as the category with $\mathrm{obj}(\mathcal{C} \rtimes \Gamma) = \mathrm{obj}(\mathcal{C})$ and

$$\mathrm{Hom}_{\mathcal{C}\rtimes\Gamma}(A, B) = \{(\sigma, \gamma) \mid \gamma \in \Gamma,\ \sigma \in \mathrm{Hom}_{\mathcal{C}}(\gamma(A), B)\}.$$

Composition for $(\rho, \gamma) \in \mathrm{Hom}_{\mathcal{C}\rtimes\Gamma}(A, B)$ and $(\sigma, \delta) \in \mathrm{Hom}_{\mathcal{C}\rtimes\Gamma}(B, C)$ is defined as

$$(\sigma, \delta) \circ (\rho, \gamma) := \big(\sigma \cdot {}^{\delta}\rho, \delta\gamma\big) \in \mathrm{Hom}_{\mathcal{C}\rtimes\Gamma}(A, C).$$

Remark 4.9. Let Γ be a group acting on $\mathcal{C}$. We have an monomorphism of groupoids $F : \mathcal{C} \to \mathcal{C} \rtimes \Gamma$ given by $A \mapsto A$ and $\sigma \mapsto (\sigma, 1)$ for all $A \in \mathrm{obj}(\mathcal{C})$ and $\sigma \in \hom(\mathcal{C})$. By functoriality of $2{-}$ we get a monomorphism $2^F : 2^{\mathcal{C}} \to 2^{\mathcal{C}\rtimes\Gamma}$ and thus a monomorphism $f = (2^F)_{\mathrm{obj}(\mathcal{C}),\mathrm{obj}(\mathcal{C})} : \mathrm{wr}(\mathcal{C}) \to \mathrm{wr}(\mathcal{C} \rtimes \Gamma)$. The action of Γ gives a map $G : \Gamma \to \mathrm{Aut}_{\mathtt{SGd}}(\mathcal{C})$ which induces a map $g : \Gamma \to \mathrm{wr}(\mathcal{C} \rtimes \Gamma)$ given by $\gamma \mapsto (((\mathrm{id}_{G(\gamma)(K)}, \gamma))_{K\in\mathrm{obj}(\mathcal{C}\rtimes\Gamma)}, G(\gamma)|_{\mathrm{obj}(\mathcal{C}\rtimes\Gamma)})$. The maps f and g induce a map $h : \mathrm{wr}(\mathcal{C}) \rtimes \Gamma \to \mathrm{wr}(\mathcal{C} \rtimes \Gamma)$ such that the following diagram commutes.

$$\begin{tikzcd}
& \mathrm{wr}(\mathcal{C}) \rtimes \Gamma \arrow[dd, dashed, tail, "h"] & \\
\mathrm{wr}(\mathcal{C}) \arrow[ur, tail] \arrow[dr, tail, "f"'] & & \Gamma \arrow[ul, tail] \arrow[dl, "g"] \\
& \mathrm{wr}(\mathcal{C} \rtimes \Gamma) &
\end{tikzcd}$$

When $\mathcal{C}$ is not the empty groupoid g and thus h is injective.

We can also use actions to define invariant categories.

Definition 4.10. Let $\mathcal{C}$ be a small groupoid with Γ a group acting on $\mathcal{C}$ and consider the induced action of Γ on $2^{\mathcal{C}}$. We define the Γ-*invariant of* $\mathcal{C}$ as the groupoid $\mathcal{C}^\Gamma$ with $\operatorname{obj}(\mathcal{C}^\Gamma) = \operatorname{obj}(\mathcal{C})/\Gamma$ and for $\Gamma A, \Gamma B \in \operatorname{obj}(\mathcal{C}/\Gamma)$

$$\operatorname{Hom}_{\mathcal{C}^\Gamma}(\Gamma A, \Gamma B) = \{\sigma \in \operatorname{Hom}_{2^{\mathcal{C}}}(\Gamma A, \Gamma B) \mid (\forall \gamma \in \Gamma)\ {}^\gamma\sigma = \sigma\}.$$

It follows from the definition that we have a natural inclusion $\operatorname{wr}(\mathcal{C}^\Gamma) \to \operatorname{wr}(\mathcal{C})$, and its image is precisely $\operatorname{wr}(\mathcal{C})^\Gamma$.

4.2 Automorphisms of products of fields

Now we show how we can consider the automorphism group of a product of fields as a wreath.

Lemma 4.11. *Let k be a commutative ring and let E be a commutative k-algebra.*

(1) *If k is a field and* $\dim_k E < \infty$, *then* $\operatorname{minspec} E = \operatorname{spec} E = \operatorname{maxspec} E$ *and* $\# \operatorname{spec} E < \infty$.

(2) *If E is reduced, then the natural k-algebra homomorphism*

$$\varphi : E \to \prod_{\mathfrak{p} \in \operatorname{minspec} E} E/\mathfrak{p}$$

is injective.

(3) *If E is reduced,* $\operatorname{minspec} E = \operatorname{maxspec} E$ *and* $\# \operatorname{spec} E < \infty$, *then φ is an isomorphism.*

Proof. (1) Note that E is an Artinian ring being finitely generated as module over the Artinian ring k. Hence this is a special case of Theorem 2.14 in [9]. (2) The kernel of φ is $\bigcap_{\mathfrak{p} \in \operatorname{minspec} E} \mathfrak{p}$, which is the nilradical of E by Corollary 2.12 in [9], which is trivial when E is reduced. (3) All minimal prime ideals are maximal and hence pair-wise coprime. Thus φ is an isomorphism by (2) and by the Chinese remainder theorem for rings, which is Exercise 2.6 in [9]. □

Let k be a commutative ring. If a k-algebra E is isomorphic to a finite product of fields $\varphi : E \xrightarrow{\sim} \prod_{i \in I} K_i$, then this family $\{K_i\}_{i \in I}$ is determined up to isomorphism. Namely, there is a bijection $f : I \to \operatorname{spec} E$ such that $E/f(i) \cong K_i$ for all $i \in I$. Hence when we say E is a finite product of fields we simply mean that $\# \operatorname{minspec} E = \# \operatorname{spec} E = \# \operatorname{maxspec} E < \infty$ and that the natural map $E \to \prod_{\mathfrak{p} \in \operatorname{spec} E} E/\mathfrak{p}$ is an isomorphism. Similarly, each automorphism of E induces a permutation on $\operatorname{spec} E$.

Now to such E we may associate the following groupoid $\mathcal{C}$: Take $\operatorname{obj}(\mathcal{C}) = \operatorname{spec} E$ and $\operatorname{Hom}_{\mathcal{C}}(\mathfrak{m}, \mathfrak{n}) = \operatorname{Iso}_{k\texttt{-Alg}}(E/\mathfrak{m}, E/\mathfrak{n})$ for all $\mathfrak{m}, \mathfrak{n} \in \operatorname{spec} E$. Each $\varphi \in \operatorname{Aut}_{k\texttt{-Alg}}(E)$ induces $\varphi_{\mathfrak{p}} \in \operatorname{Iso}_{k\texttt{-Alg}}(E/\mathfrak{p}, E/\varphi(\mathfrak{p}))$ and $f \in \operatorname{Aut}_{\texttt{Set}}(\operatorname{spec} E)$. Hence, we have a map $\Phi : \operatorname{Aut}_{k\texttt{-Alg}}(E) \to \operatorname{wr}(\mathcal{C})$ given by $\varphi \mapsto ((\varphi_{\mathfrak{p}})_{\mathfrak{p} \in \operatorname{obj}(\mathcal{C})}, f)$. Conversely, each element of $\operatorname{wr}(\mathcal{C})$ induces an automorphism of $\prod_{\mathfrak{p} \in \operatorname{spec} E} E/\mathfrak{p}$ using the universal property of the direct product, which in turn gives an automorphism of E by Lemma 4.11. Thus we get a map $\Psi : \operatorname{wr}(\mathcal{C}) \to \operatorname{Aut}_{k\texttt{-Alg}}(E)$. We leave the routine verification as an exercise to the reader.

Proposition 4.12. *The maps Φ and Ψ are mutually inverse group homomorphisms, giving a natural isomorphism* $\operatorname{Aut}_{k\texttt{-Alg}}(E) \cong \operatorname{wr}(\mathcal{C})$. □

Example 4.13. A special case we consider will be the following. Let $E \neq 0$ be a finite dimensional reduced $\mathbb{Q}$-algebra and let $\mathbb{Q}' = \mathbb{Q}(\mu_e)$ for some $e \in \mathbb{S}$. Then $E' = E \otimes_{\mathbb{Q}} \mathbb{Q}'$ for $e \in \mathbb{S}$ is both a $\mathbb{Q}$-algebra and a $\mathbb{Q}'$-algebra. Moreover, E' is a finite product of fields by Lemma 4.11 as it is finite dimensional over $\mathbb{Q}'$ and reduced by Theorem A1.3 in [9].

In the context of Definition 3.22 we have three relevant groups: $A = \operatorname{Aut}_{\mathbb{Q}\texttt{-Alg}}(E')$, $B = \{\sigma \in A \mid \sigma\mathbb{Q}' = \mathbb{Q}'\}$ and $C = \operatorname{Aut}_{\mathbb{Q}'\texttt{-Alg}}(E')$. Let $\Gamma = \operatorname{Aut}_{\mathbb{Q}\texttt{-Alg}}(\mathbb{Q}')$ and consider its natural action $\varphi : \Gamma \to A$ on E'. Here $X_e(E) \subseteq C$ while C is generally too small to contain $\varphi(\Gamma)$. However, we do have $\varphi(\Gamma) \subseteq B$. We even have that $B \cong C \rtimes \Gamma$.

Now construct the groupoids $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{E}$ as in Proposition 4.12 for E' as $\mathbb{Q}'$-algebra, E' as $\mathbb{Q}$-algebra and E as $\mathbb{Q}$-algebra respectively. Then $\mathcal{C}$ is a wide subgroupoid of $\mathcal{D}$. We may also construct $\mathcal{D}$ and $\mathcal{E}$ using $\mathcal{C}$, as $\mathcal{D} \cong \mathcal{C} \rtimes \Gamma$ and $\mathcal{E} \cong \mathcal{C}^\Gamma$. Under the same natural inclusions as in Remark 4.9 for the wreaths we get the following commutative diagram.

$$\begin{tikzcd}
C \arrow[r, tail] \arrow[d, leftrightarrow] & B \arrow[r, tail] \arrow[d, leftrightarrow] & A \arrow[d, leftrightarrow] \\
\mathrm{wr}(\mathcal{C}) \arrow[r, tail] & \mathrm{wr}(\mathcal{C}) \rtimes \Gamma \arrow[r, tail] & \mathrm{wr}(\mathcal{C} \rtimes \Gamma)
\end{tikzcd}$$

4.3 Conjugacy in wreaths

In this section we generalize a well-known theorem (Theorem 4.15), relating conjugacy of permutations to their cycle type, to wreaths. For the remainder of this section $\mathcal{C}$ will be a groupoid with only finitely many objects and $\mathcal{D}$ will be a wide subgroupoid of $\mathcal{C}$.

Definition 4.14. Let Ω be a finite set and let $s \in \mathrm{Aut}_{\mathtt{Set}}(\Omega)$ be a permutation of Ω. Define $c_k(s)$ to be the number of orbits of $\langle s \rangle$ of length k. Then we call $c(s) := (c_1(s), c_2(s), \dots)$ the *cycle type* of s.

Theorem 4.15. *Let $r, s \in \mathrm{Aut}_{\mathtt{Set}}(\Omega)$. Then r and s are conjugate in $\mathrm{Aut}_{\mathtt{Set}}(\Omega)$ if and only if $c(r) = c(s)$. Furthermore, if those equivalent conditions hold the number of $a \in \mathrm{Aut}_{\mathtt{Set}}(\Omega)$ such that $ar = sa$ is*

$$\prod_{k \geq 1} \left(c_k(s)! \cdot k^{c_k(s)} \right) \leq (\#\Omega)^{\#(\Omega/\langle s \rangle)}. \qquad \square$$

The idea of the proof is the following: For each orbit of $\langle r \rangle$ one chooses an orbit of $\langle s \rangle$ to send it to, which must necessarily be of the same length k, and one notes that this can be done in exactly k ways. In a wreath, it is generally not sufficient to consider only the length of the cycle to be able to decide where to send it.

Definition 4.16. For $K, L \in \mathrm{obj}(\mathcal{C})$ we call $\rho \in \mathrm{Aut}_{\mathcal{C}}(K)$ and $\sigma \in \mathrm{Aut}_{\mathcal{C}}(L)$ *$\mathcal{D}$-conjugate*, written $\rho \sim_{\mathcal{D}} \sigma$, if there exists an $\alpha \in \mathrm{Hom}_{\mathcal{D}}(K, L)$ such that $\alpha\rho = \sigma\alpha$.

Note that if $K = L$ and $\mathcal{C} = \mathcal{D}$ in the above definition, our definition of conjugacy coincides with that of conjugacy in the group $\mathrm{Aut}_{\mathcal{C}}(K)$, hence this is a generalization. For this generalization it is easy to see that $\sim_{\mathcal{D}}$ is also an equivalence relation.

Definition 4.17. For $K \in X \subseteq \mathrm{obj}(\mathcal{C})$ and $\sigma = ((\sigma_L)_{L \in X}, s) \in \mathrm{Aut}_{2^{\mathcal{C}}}(X)$ define

$$\lambda_\sigma(K) = (\sigma^{\#(\langle\sigma\rangle K)})_K = \sigma_{s^{-1}(K)} \circ \sigma_{s^{-2}(K)} \circ \cdots \circ \sigma_{s(K)} \circ \sigma_K \in \mathrm{Aut}_{\mathcal{C}}(K).$$

Lemma 4.18. *Let $K, L \in X \subseteq \mathrm{obj}(\mathcal{C})$ and $\sigma \in \mathrm{Aut}_{2^{\mathcal{C}}}(X)$. If $\langle\sigma\rangle K = \langle\sigma\rangle L$, then $\lambda_\sigma(K) \sim_{\mathcal{C}} \lambda_\sigma(L)$.*

Proof. Let $n = \#(\langle\sigma\rangle K)$ and let $m \geq 0$ be such that $s^m(K) = L$. Consider $\alpha = (\sigma^m)_K \in \mathrm{Hom}_{\mathcal{C}}(K, L)$. Then $\lambda_\sigma(L) \circ \alpha = (\sigma^{n+m})_K = \alpha \circ \lambda_\sigma(K)$, so $\lambda_\sigma(K) \sim_{\mathcal{C}} \lambda_\sigma(L)$. $\square$

Definition 4.19. We define $\mathscr{F}(\mathcal{C}) = \mathrm{aut}(\mathcal{C})/{\sim_{\mathcal{C}}}$. For $X \subseteq \mathrm{obj}(\mathcal{C})$ and $\sigma \in \mathrm{Aut}_{2^{\mathcal{C}}}(X)$ the map $X \xrightarrow{\lambda_\sigma} \mathrm{aut}(\mathcal{C}) \to \mathscr{F}(\mathcal{C})$ factors through $X/\langle\sigma\rangle$ by Lemma 4.18 and we write Λ_σ for the factor $X/\langle\sigma\rangle \to \mathscr{F}(\mathcal{C})$.

For a fixed σ we treat the map Λ_σ as a labeling of the orbits of σ. Then analogously to Definition 4.14 we may define the type of an element $\sigma \in \mathrm{wr}(\mathcal{C})$.

Definition 4.20. For $\sigma \in \mathrm{wr}(\mathcal{C})$, $k \in \mathbb{Z}_{\geq 1}$ and $\gamma \in \mathscr{F}(\mathcal{C})$, let $c(\sigma, k, \gamma)$ be the number of orbits O of $\langle s \rangle$ of length k and label $\Lambda_\sigma(O) = \gamma$. We then define $c(\sigma) = (c(\sigma, k, \gamma))_{k \in \mathbb{Z}_{\geq 1}, \gamma \in \mathscr{F}(\mathcal{C})}$ to be the *type* of σ.

This generalization of cycle type allows us to formulate the right analogue to Theorem 4.15. For $K \in \mathrm{obj}(\mathcal{C})$ and $\sigma \in \mathrm{Aut}_{\mathcal{C}}(K)$ write $C_{\mathcal{D}}(\sigma) = \{\alpha \in \mathrm{Aut}_{\mathcal{D}}(K) \mid \alpha\sigma = \sigma\alpha\}$ for the centralizer of γ in $\mathrm{Aut}_{\mathcal{D}}(K)$.

Theorem 4.21. *Let $\mathcal{C}$ be a finite groupoid and let $\rho, \sigma \in \mathrm{wr}(\mathcal{C})$ be given. Then ρ and σ are conjugate in $\mathrm{wr}(\mathcal{C})$ if and only if $c(\rho) = c(\sigma)$. If these equivalent conditions hold, then the number of $\alpha \in \mathrm{wr}(\mathcal{C})$ such that $\alpha\rho = \sigma\alpha$ is*

$$\prod_{\substack{k \in \mathbb{Z}_{\geq 1} \\ [\gamma] \in \digamma}} \left(c(\rho, k, [\gamma])! \cdot \big(k \cdot \# C_{\mathcal{C}}(\gamma)\big)^{c(\rho,k,[\gamma])} \right).$$

With $\mathcal{D}$ a wide subgroupoid of $\mathcal{C}$, the number of $\alpha \in \mathrm{wr}(\mathcal{D})$ such that $\alpha\rho = \sigma\alpha$ is at most $(\# \operatorname{aut}(\mathcal{D}))^{\#(\mathrm{obj}(\mathcal{D})/\langle\rho\rangle)}$.

We prove this theorem using the following lemma.

Lemma 4.22. *Let $X, Y \subseteq \mathrm{obj}(\mathcal{C})$ and let $\rho \in \mathrm{Aut}_{2^{\mathcal{C}}}(X)$ and $\sigma \in \mathrm{Aut}_{2^{\mathcal{C}}}(Y)$ be such that $\langle\rho\rangle$ and $\langle\sigma\rangle$ act transitively on X respectively Y. If $\rho \sim_{2^{\mathcal{D}}} \sigma$, then $A = \{\alpha \in \mathrm{Hom}_{2^{\mathcal{D}}}(X, Y) \mid \alpha\rho = \sigma\alpha\}$ contains at most $\sum_{L \in Y} \# C_{\mathcal{D}}(\lambda_\rho(L))$ elements, with equality when $\mathcal{C} = \mathcal{D}$.*

Proof. Assume $\rho \sim_{2^{\mathcal{D}}} \sigma$, hence $\#X = \#Y =: n$. Fix $K \in X$ and define

$$B = \{(L, \omega) \mid L \in Y,\ \omega \in \mathrm{Hom}_{\mathcal{D}}(K, L),\ \omega \circ \lambda_\rho(K) = \lambda_\sigma(L) \circ \omega\}.$$

If $\lambda_\rho(K) \sim_{\mathcal{D}} \lambda_\sigma(L)$ for some $L \in Y$, then there are precisely $\# C_{\mathcal{D}}(\lambda_\rho(L))$ elements ω such that $(L, \omega) \in B$, and otherwise there are none. Thus $\#B \leq \sum_{L \in Y} \# C_{\mathcal{D}}(\lambda_\rho(L))$, with equality when $\mathcal{C} = \mathcal{D}$ by Lemma 4.18. Now consider the map $\Phi : A \to B$ given by $\alpha \mapsto (a(K), \alpha_K)$. It is well-defined, since for each $\alpha \in A$ we have $\alpha_K \lambda_\rho(K) \alpha_K^{-1} = (\alpha\rho^n\alpha^{-1})_L = (\sigma^n)_K = \lambda_\sigma(L)$. It suffices to show Φ is injective in general and a bijection when $\mathcal{C} = \mathcal{D}$. For all $\alpha \in A$ and $k \geq 0$ we have the relations

$$a(r^k(K)) = s^k(a(K)) \quad \text{and} \quad \alpha_{r^k(K)} = (\sigma^k)_{a(K)} \circ \alpha_K \cdot (\rho^{-k})_{r^k(K)} \tag{1}$$

We claim that given $(L, \omega) \in B$ the equations of (1) with $k \in \{0, \dots, n-1\}$ uniquely define an element α of $\mathrm{Hom}_{2^{\mathcal{C}}}(X, Y)$ satisfying $a(K) = L$, $\alpha_K = \omega$ and $\alpha\rho = \sigma\alpha$, giving a left inverse $\Psi : B \to \mathrm{Hom}_{2^{\mathcal{C}}}(X, Y)$ of Φ. By transitivity of $\langle r\rangle$ the map a is determined entirely in terms of $a(K) = L$, meaning a is unique, and by transitivity of $\langle s\rangle$ in fact $a \in \mathrm{Iso}_{\mathtt{Set}}(X, Y)$. From $\alpha_K = \omega$ and $\langle r\rangle$ being transitive it follows analogously that α is uniquely and well-defined. Thus Ψ is a well-defined injection, proving the general case.

Assume $\mathcal{C} = \mathcal{D}$. To prove Ψ is a right inverse of Φ it remains to be shown that $\mathrm{im}(\Psi) \subseteq A$. Let $(L, \omega) \in B$ and let $\alpha = \Psi(L, \omega)$. Let $J \in X$, which we may write as $J = r^m(K)$ for some $m \in \{0, \dots, n-1\}$. When $m \neq n-1$ the relations $ar(J) = sa(J)$ and $\alpha_{r(J)} \circ \rho_J = \sigma_{a(J)} \circ \alpha_J$ follow directly from the defining relations (1) with $k \in \{0, \dots, n-1\}$. If $m = n-1$ we also have $ar(J) = a(K) = s^n a(K) = sar^m(K) = sa(J)$, hence $ar = sa$. Then,

$$\begin{aligned} \alpha_{r(J)} \circ \rho_J = \omega \circ \rho_J = \omega \circ \lambda_\rho(K) \circ (\rho^m)_{r^m(K)} &= \lambda_\sigma(L) \circ \omega \circ (\rho^m)_{r^m(K)} \\ = \sigma_{a(J)} \circ (\sigma^m)_{a(K)} \circ \omega \circ (\rho^m)_{r^m(K)} &= \sigma_{a(J)} \circ \alpha_J. \end{aligned}$$

Hence $\alpha\rho = \sigma\alpha$ and $\alpha \in A$, as was to be shown. Thus Φ and Ψ are mutually inverse. □

Proof of Theorem 4.21:
Assume $\rho = \alpha\sigma\alpha^{-1}$ for some $\alpha \in \mathrm{wr}(\mathcal{C})$, then we certainly have $r = asa^{-1}$. Hence a induces a bijection on the orbits of r and s. By basic algebra paired orbits are equally large, and by Lemma 4.18 these orbits must have conjugate labels. In particular, $c(\rho, k, \gamma) = c(\sigma, k, \gamma)$ for all $k \in \mathbb{Z}_{\geq 0}$ and $\gamma \in \digamma$, so ρ and σ are of the same type.

If ρ and σ are of the same type, we may choose a bijection f between the set of orbits $\mathcal{O}$ of ρ and those of σ that preserves length and label. Then by Lemma 4.22, for each $O \in \mathcal{O}$ there exists $\alpha_O \in \mathrm{Hom}_{2^{\mathcal{C}}}(O, f(O))$ such that $\sigma|_{f(O)} \circ \alpha_O = \alpha_O \circ \rho|_O$. Then the concatenation $\alpha := \prod_{O \in \mathcal{O}} \alpha_O \in \mathrm{wr}(\mathcal{C})$ satisfies $\alpha\rho = \sigma\alpha$, so $\rho \sim_{2^{\mathcal{C}}} \sigma$. Note that for different choices of f and α_O

we obtain different α. Conversely, each α induces a bijection f and parts $\alpha_O \in \mathrm{Hom}_{2\mathcal{C}}(O, f(O))$ for all $O \in \mathcal{O}$. Basic combinatorics and Lemma 4.22 then show that the number of α is

$$\Bigg(\prod_{\substack{k\in\mathbb{Z}_{\geq 0}\\ [\gamma]\in\mathcal{F}}} c(\rho,k,[\gamma])!\Bigg)\cdot\Bigg(\prod_{\substack{k\in\mathbb{Z}_{\geq 0}\\ [\gamma]\in\mathcal{F}}} (k\cdot\#C_{\mathcal{C}}(\gamma))^{c(\rho,k,[\gamma])}\Bigg), \tag{2}$$

as was to be shown.

Consider a wide subgroupoid $\mathcal{D}$ of $\mathcal{C}$. Note that $\sum_{k\in\mathbb{Z}_{\geq 0},\,[\gamma]\in\mathcal{F}} c(\rho,k,[\gamma]) = \#\mathcal{O} = \#\operatorname{obj}(\mathcal{D})/\langle\rho\rangle$. Then from Lemma 4.22 we get a upper bound on the number of $\alpha \in \mathrm{wr}(\mathcal{D})$ such that $\alpha\rho = \sigma\alpha$ similarly as for (1), namely

$$\Bigg(\prod_{\substack{k\in\mathbb{Z}_{\geq 0}\\ [\gamma]\in\mathcal{F}}} c(\rho,k,[\gamma])!\Bigg)\cdot\Bigg(\prod_{O\in\mathcal{O}}\sum_{K\in O}\#\operatorname{Aut}_{\mathcal{D}}(K)\Bigg) \leq \Bigg(\sum_{K\in\operatorname{obj}(\mathcal{D})}\#\operatorname{Aut}_{\mathcal{D}}(K)\Bigg)^{\#(\operatorname{obj}(\mathcal{D})/\langle\rho\rangle)},$$

as was to be shown. □

Corollary 4.23. *Let $\mathcal{D}$ be a finite groupoid and Γ a group acting on $\mathcal{D}$. If $\sigma\gamma, \tau\gamma' \in \mathrm{wr}(\mathcal{D}) \rtimes \Gamma \subseteq \mathrm{wr}(\mathcal{D} \rtimes \Gamma)$ are $\mathrm{wr}(\mathcal{D})$-conjugate, then $\gamma = \gamma'$ and the number of $\alpha \in \mathrm{wr}(\mathcal{D})$ such that $\alpha\sigma\gamma = \rho\gamma\alpha$ is at most $(\#\operatorname{aut}(\mathcal{D}))^{\#(\operatorname{obj}(\mathcal{D})/\langle\sigma\gamma\rangle)}$.*

Proof. If $\alpha\sigma\gamma = \rho\gamma'\alpha$ for some $\alpha \in \mathrm{wr}(\mathcal{D})$, then $\gamma = \pi_\Gamma(\alpha\sigma\gamma) = \pi_\Gamma(\rho\gamma'\alpha) = \gamma'$. For the second claim we simply apply Theorem 4.21 to the categories $\mathcal{C} = \mathcal{D} \rtimes \Gamma$ and $\mathcal{D} \subseteq \mathcal{C}$. □

4.4 Computation

If we want to do computations on groupoids and wreaths we first need to specify an encoding. In our applications, the objects of $\mathcal{C}$ are number fields as in Example 4.13. For both the objects and morphisms of $\mathcal{C}$ we already made a choice of how to encode them in Section 1, namely by structure constants and matrices respectively. We then encode $\mathcal{C}$ as a sequence $K_1, \ldots, K_n$ of objects followed by $n \times n$ sequences of morphisms $\sigma_{ij1}, \ldots, \sigma_{ijm_{ij}} \in \mathrm{Hom}_{\mathcal{C}}(K_i, K_j)$. Then $\sigma \in \mathrm{wr}(\mathcal{C})$ can be encoded as a permutation s of $\{1, \ldots, n\}$ and a sequence of n morphisms in the obvious way. There may exist some more practical or efficient encodings, we may pre-compute all inverses of the matrices for example or work with multiplication tables instead of actual matrices. This simple encoding however already satisfies our requirements, namely that composition and inversion in both $\mathcal{C}$ and $\mathrm{wr}(\mathcal{C})$ can be done in polynomial time with respect to the length of the encoding.

One may verify that Lemma 4.22 implicitly gives a polynomial time algorithm to compute A. Thus we may turn Theorem 4.21 into an algorithm as well.

Corollary 4.24. *There is an algorithm that takes as input a quadruple $(\mathcal{C}, \mathcal{D}, \rho, \sigma)$, where $\mathcal{C}$ is a groupoid, $\mathcal{D} \subseteq \mathcal{C}$ is a wide subgroupoid and $\sigma, \rho \in \mathrm{wr}(\mathcal{C})$, and outputs all $\alpha \in \mathrm{wr}(\mathcal{D})$ such that $\alpha\rho = \sigma\alpha$ in time $n^{O(\#\operatorname{obj}(\mathcal{D})/\langle\rho\rangle)}$, where n is the length of the input.* □

5 Gradings of cyclotomic number fields

In this section we will use the acquired theory to compute the gradings of cyclotomic fields $\mathbb{Q}(\mu_e)$ with $e \in \mathbb{Z}_{>0}$ a prime power. We simply list the gradings of $\mathbb{Q}(\mu_e)$ with the torsion subgroup μ_∞ of $\mathbb{C}^*$ and later prove that these must be all such gradings. The sections beyond this one do not depend on any of the results proven here and thus this section can be skipped by a reader that is only interested in the proof Theorem 1.4.

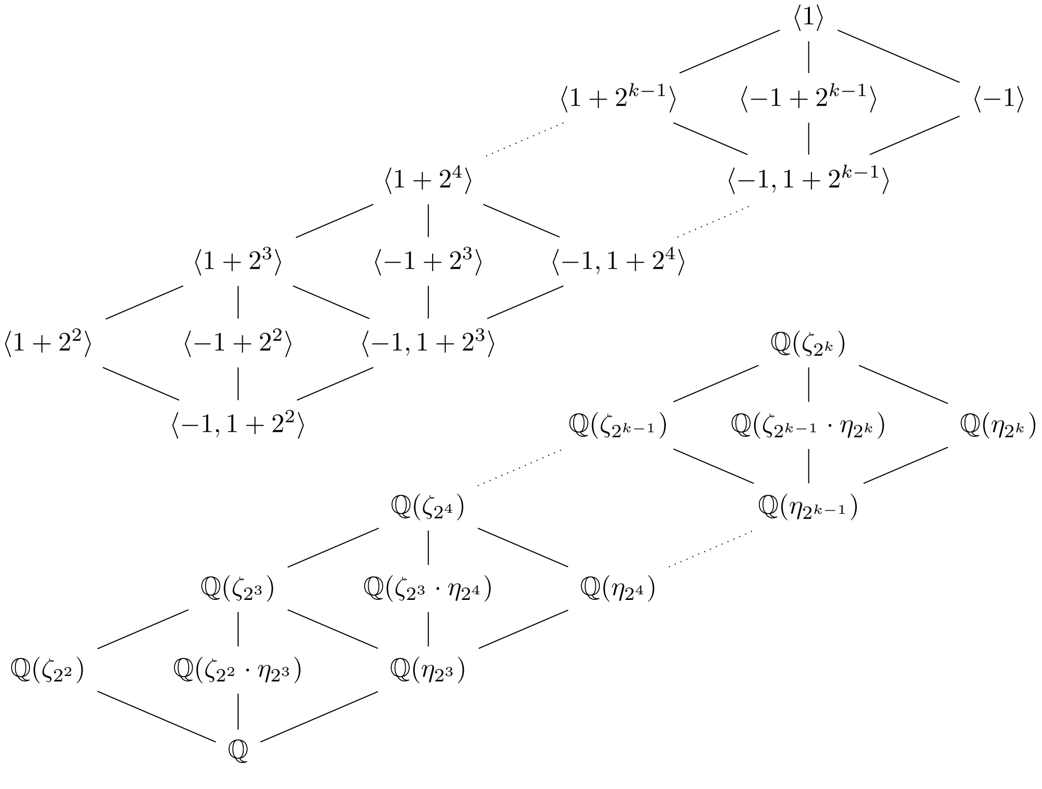
Theorem 5.1. *Let p be prime and $k \geq 1$. Then the μ_∞-gradings of $\mathbb{Q}(\mu_{p^k})$ are precisely the gradings in Example 5.4.*

For now, we not only fix the ring $\mathbb{Q}(\mu_{p^k})$ we grade, but also the group μ_∞ we grade it with. By nature of the definitions we use, if $\overline{E}$ is a μ_∞-grading and $\varphi \in \mathrm{End}(\mu_\infty)$, then we have $\varphi_*\overline{E} = \overline{E}$ only when φ restricted to $\langle \zeta \in \mu_\infty \mid E_\zeta \neq 0\rangle$ is the identity, not simply when this restriction is an isomorphism. This is an important aspect to the counting argument we use in the proof of the theorem.

Lemma 5.2. *Let p be prime and $k \geq 1$. Then $1 \to 1+p\mathbb{Z}/p^k\mathbb{Z} \to (\mathbb{Z}/p^k\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \to 1$ is an exact sequence. When $p \neq 2$ the group $1 + p^n\mathbb{Z}/p^k\mathbb{Z} = \langle 1 + p^n\rangle$ is a cyclic group of order p^{k-n} for $1 \leq n \leq k$. If $p = 2$ and $k \geq 2$, then $1+p\mathbb{Z}/p^k\mathbb{Z} = \langle -1\rangle \times (1+4\mathbb{Z}/2^k\mathbb{Z})$, and $1+2^n\mathbb{Z}/2^k\mathbb{Z} = \langle 1+2^n\rangle$ is a cyclic group of order 2^{k-n} for $2 \leq n \leq k$.*

Proof. Standard. It follows from Proposition 2' in [10]. □

Corollary 5.3. *For each $n \geq 1$ let ζ_n be a primitive n-th root of unity and let $\eta_n = \zeta_n + \zeta_n^{-1}$. For $k \geq 2$, the subgroups of $(\mathbb{Z}/2^k\mathbb{Z})^*$ and subfields of $\mathbb{Q}(\mu_{2^k})$ are as follows, where lines indicate subgroups of index 2 respectively field extensions of degree 2.*


$\langle 1\rangle$
$\langle 1+2^{k-1}\rangle$
$\langle -1+2^{k-1}\rangle$
$\langle -1\rangle$
$\langle -1, 1+2^{k-1}\rangle$
$\langle 1+2^4\rangle$
$\langle 1+2^3\rangle$
$\langle -1+2^3\rangle$
$\langle -1, 1+2^4\rangle$
$\langle 1+2^2\rangle$
$\langle -1+2^2\rangle$
$\langle -1, 1+2^3\rangle$
$\langle -1, 1+2^2\rangle$
$\mathbb{Q}(\zeta_{2^k})$
$\mathbb{Q}(\zeta_{2^{k-1}})$
$\mathbb{Q}(\zeta_{2^{k-1}} \cdot \eta_{2^k})$
$\mathbb{Q}(\eta_{2^k})$
$\mathbb{Q}(\eta_{2^{k-1}})$
$\mathbb{Q}(\zeta_{2^4})$
$\mathbb{Q}(\zeta_{2^3})$
$\mathbb{Q}(\zeta_{2^3} \cdot \eta_{2^4})$
$\mathbb{Q}(\eta_{2^4})$
$\mathbb{Q}(\zeta_{2^2})$
$\mathbb{Q}(\zeta_{2^2} \cdot \eta_{2^3})$
$\mathbb{Q}(\eta_{2^3})$
$\mathbb{Q}$

Proof. The subgroups follow directly from Lemma 5.2. For the fields we note that the extension $\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}$ is Galois, so we apply Galois correspondence and Corollary 3.12 to the diagram of groups. □

Example 5.4. Let $E = \mathbb{Q}(\mu_{p^k})$ with p prime and $k \geq 1$, let $\zeta \in \mu_{p^k}$ be primitive and let $G = \mathbb{Z}/p^{k-1}\mathbb{Z}$.

a. Note that $\{\zeta^0, \dots, \zeta^{p^{k-1}-1}\}$ forms a $\mathbb{Q}(\mu_p)$-basis of E and that $\zeta^{p^{k-1}} \in \mathbb{Q}(\mu_p)$. With $C_n = \zeta^n \cdot \mathbb{Q}(\mu_p)$ for all $n \in G$, we get a grading $\overline{C} = (E, G, \{C_n\}_{n \in G})$. There are p^{k-1} morphisms $G \to \mu_\infty$, giving p^{k-1} distinct μ_∞-gradings of E, including the trivial grading.

b. Assume $p \neq 2$ or $k \geq 3$. Consider $R_1 = \mathbb{Q}(\alpha)$ and $R_{-1} = \beta \cdot \mathbb{Q}(\alpha)$ with $\alpha = \zeta + \zeta^{-1}$ and $\beta = \zeta - \zeta^{-1}$. By Corollary 5.3 we have $[E : R_1] = 2$. Because $\zeta = (\alpha + \beta)/2 \in R_1 + R_{-1}$, we must have $E = R_1 \oplus R_{-1}$. Furthermore, we have $\beta^2 = \zeta^2 + \zeta^{-2} - 2 = -4 + \alpha^2 \in R_1$, hence $R_{-1}R_{-1} \subseteq R_1$. We conclude $\overline{R} = (E, \mu_2, \{R_s\}_{s \in \mu_2})$ is a grading, which in turn gives a new μ_∞-grading of E under the natural inclusion $\mu_2 \to \mu_\infty$. If $p = 2$, we can additionally decompose E into $I_1 = \mathbb{Q}(\beta)$ and $I_{-1} = \alpha \cdot \mathbb{Q}(\beta)$ yielding another μ_2-grading $\overline{I}$, using that $\mathbb{Q}(\beta)$ is the $\langle -1 + 2^{k-1} \rangle$-invariant subfield of E.

c. Assume $p = 2$ and $k \geq 4$. Note that $\sqrt{2} = \zeta_8 + \zeta_8^{-1} \in E$ and consider $\alpha = \zeta\sqrt{2} \in E$. We have $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(\alpha^2)$, so $\zeta = \alpha/\sqrt{2} \in \mathbb{Q}(\alpha)$ and $E = \mathbb{Q}(\alpha)$. Moreover, $\alpha^{2^{k-1}} = -2^{2^{k-2}} \in \mathbb{Q}$. Thus with $S_n = \alpha^n \cdot \mathbb{Q}$ we get a grading $\overline{S} = (E, G, \{S_n\}_{n \in G})$. Note that α and ζ^i are $\mathbb{Q}$-linearly independent for each $i \in \mathbb{Z}$. Hence for any of the 2^{k-2} injections $\varphi : G \to \mu_\infty$ the grading $\varphi_* \overline{S}$ is not listed in (a), nor is it listed in (b). For any non-injective $\varphi \in \operatorname{End}(G)$ we have $\varphi_* \overline{S} = \varphi_* \overline{C}$. Thus we get exactly 2^{k-2} new μ_∞-gradings of E.

d. Assume $p = 2$ and $k \geq 4$. Consider $\alpha = \zeta^2 + \zeta^{-2}$ and $\beta = \zeta_8(\zeta + \zeta^{-1})$. By Corollary 5.3 the field $\mathbb{Q}(\alpha)$ is the $\langle -1, 1 + 2^{k-1} \rangle$-invariant subfield of E and we have $[E : \mathbb{Q}(\alpha)] = 4$. Since β is neither invariant under $\zeta \mapsto \zeta^{-1}$, $\zeta \mapsto \zeta^{-1+2^{k-1}}$ nor $\zeta \mapsto \zeta^{1+2^{k-1}}$, we have that $\mathbb{Q}(\alpha, \beta) = E$. Moreover $\beta^4 = (\zeta_4(2 + \alpha))^2 = -(2 + \alpha)^2 \in \mathbb{Q}(\alpha)$. Then with $W_n = \beta^n \cdot \mathbb{Q}(\alpha)$ we get a grading $\overline{W} = (E, \mathbb{Z}/4\mathbb{Z}, \{W_n\}_{\mathbb{Z}/4\mathbb{Z}})$. The injective morphisms $\mathbb{Z}/4\mathbb{Z} \to \mu_\infty$ give two new μ_∞-gradings of E. Since $\mathbb{Q}(\alpha, \beta^2) = \mathbb{Q}(\zeta^2)$ the others coincide with gradings of (a) by Corollary 3.26.

First we show that besides a single possible exception, all μ_∞-gradings of $\mathbb{Q}(\mu_{p^k})$ are μ_{p^∞}-gradings.

Lemma 5.5. *Let p and q be prime and let $E = \mathbb{Q}(\mu_{p^k})$ for some $k \geq 1$. If E has an efficient μ_{q^n}-grading for some $n \geq 1$, then $q^n = 2$ or $p = q$. Moreover, if $p \neq 2$ then E has exactly one efficient μ_2-grading and no efficient μ_{2p}-gradings.*

Proof. Let q be such that E has an efficient μ_{q^n}-grading $\overline{E}$ and assume $p \neq q$. Using Theorem 3.25, this grading corresponds to some non-trivial $\sigma \in \operatorname{Aut}_{\mathbb{Z}[\mu_{q^n}]}(E \otimes_\mathbb{Z} \mathbb{Z}[\mu_{q^n}]) \cong \operatorname{Aut}_{\mathbb{Q}(\mu_{q^n})}(\mathbb{Q}(\mu_{q^n p^k}))$ such that $\sigma^{q^n} = 1$ and $\tau_a \sigma = \sigma^a \tau_a$ for all $a \in (\mathbb{Z}/q^n\mathbb{Z})^*$, where τ_a is the image of a under $(\mathbb{Z}/q^n\mathbb{Z})^* \to \operatorname{Aut}(\mathbb{Z}[\mu_{q^n}]) \to \operatorname{Aut}(E \otimes_\mathbb{Z} \mathbb{Z}[\mu_{q^n}])$. Note that τ_a and σ commute as $\operatorname{Aut}(\mathbb{Q}(\mu_{q^n p^k}))$ is abelian. Then for all $a \in (\mathbb{Z}/q^n\mathbb{Z})^*$ we have $\sigma^a = \tau_a \sigma \tau_a^{-1} = \tau_a \tau_a^{-1} \sigma = \sigma$, so $a = 1$. Thus $(\mathbb{Z}/q^n\mathbb{Z})^* = \{1\}$ and $q^n = 2$. It follows that E can only have a non-trivial efficient μ_{q^n}-grading if $q^n = 2$ or $p = q$.

Assume $p \neq 2$. Then $\operatorname{Aut}_{\mathbb{Z}[\mu_2]}(E \otimes_\mathbb{Z} \mathbb{Z}[\mu_2]) \cong \operatorname{Aut}(E) \cong (\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic of even order by Lemma 5.2. Hence it contains exactly one σ of order 2, and it trivially satisfies $\tau_a \sigma = \sigma^a \tau_a$ for all $a \in (\mathbb{Z}/2\mathbb{Z})^*$. The corresponding efficient μ_2-grading of E is then unique. If $\overline{E}$ is an efficient μ_{2p}-grading of E, then we get an efficient μ_p-grading of the unique subfield $E' = \sum_{\zeta \in \mu_p} E_\zeta$ of E of degree two. In particular, we may write $E' = F(\alpha)$ for some $\alpha \in E'$ and subfield $F \subseteq E'$ of degree p such that $\alpha^p \in F$. The minimal polynomial of α must then be $f = X^p - \alpha^p$, but $\zeta_p \alpha$ is a root of f while $\zeta_p = \zeta_p \alpha / \alpha \notin E'$, so E'/F is not normal. However, $E/\mathbb{Q}$ is a Galois extension, so this is a contradiction and no efficient $2p$-grading exists. □

Lemma 5.5 shows that, besides a single μ_2-grading in the case $p \neq 2$, all μ_∞-gradings of $\mathbb{Q}(\mu_{p^k})$ are μ_{p^∞}-gradings. Since the order of $\langle \gamma \in \Gamma \mid E_\gamma \neq 0 \rangle$ divides $[\mathbb{Q}(\mu_{p^k}) : \mathbb{Q}] = (p-1)p^{k-1}$ for any Γ-grading $\overline{E}$ of $\mathbb{Q}(\mu_{p^k})$ by Proposition 2.6, we may even restrict to the group μ_{p^k}.

Lemma 5.6. *Let $p^k > 1$ be a prime power and let $A = \mathbb{Z}/p^k\mathbb{Z}$ and $M = (\mathbb{Z}/p^k\mathbb{Z})^*$. Then M acts on A by multiplication and we let $G = A \rtimes M$ be the corresponding semi-direct product. Then there is a bijection*

$$\{\mu_{p^k}\text{-gradings of } \mathbb{Q}(\mu_{p^k})\} \leftrightarrow Z = \{H \subseteq G \mid H \text{ a group, the natural map } M \to G/H \text{ is a bijection}\}.$$

Proof. By Theorem 3.25, the set of μ_{p^k}-gradings of $E = \mathbb{Q}(\mu_{p^k})$ is in bijection with $X_{p^k}(E)$ as defined in Definition 3.22. Then by Proposition 4.12, we have $\mathrm{Aut}_{\mathbb{Z}[\mu_{p^k}]\text{-}\mathtt{Alg}}(E') \cong \mathrm{wr}(\mathcal{C})$ with $E' = E \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_{p^k}]$ and $\mathcal{C}$ the category with $\mathrm{obj}(\mathcal{C}) = \mathrm{spec}\, E'$ and $\mathrm{Hom}_{\mathcal{C}}(\mathfrak{m}, \mathfrak{n}) = \mathrm{Hom}_{\mathbb{Z}[\mu_{p^k}]\text{-}\mathtt{Alg}}(E'/\mathfrak{m}, E'/\mathfrak{n})$ for all $\mathfrak{m}, \mathfrak{n} \in \mathrm{obj}(\mathcal{C})$. We have an injection $\mathbb{Q}(\mu_{p^k}) \hookrightarrow E'/\mathfrak{m}$ since $E'/\mathfrak{m}$ is a $\mathbb{Q}(\mu_{p^k})$-algebra and morphisms of fields are injective and an injection of $E'/\mathfrak{m}$ into a compositum of the factors of E', which is $\mathbb{Q}(\mu_{p^k})$. Therefore $E'/\mathfrak{m} \cong \mathbb{Q}(\mu_{p^k})$ for all $\mathfrak{m} \in \mathrm{spec}\, E'$, so $\mathrm{wr}(\mathcal{C}) \cong \mathrm{Aut}_{\mathtt{Set}}(\mathrm{obj}(\mathcal{C}))$ by Proposition 4.5. Moreover, $M \cong \mathrm{Aut}(\mathbb{Q}(\mu_{p^k}))$ acts regularly on $\mathrm{obj}(\mathcal{C})$, so we have a canonical isomorphism $\mathrm{Aut}_{\mathtt{Set}}(\mathrm{obj}(\mathcal{C})) \cong \mathrm{Aut}_{\mathtt{Set}}(M)$ such that the induced action $C_M : M \to \mathrm{Aut}_{\mathtt{Set}}(M)$ is the Cayley-action. Then $X_{p^k}(\mathbb{Q}(\mu_{p^k}))$ is in natural bijection with $X = \{\gamma \in \mathrm{Aut}_{\mathtt{Set}}(M) \,|\, \gamma^{p^k} = 1,\ (\forall a \in M)\, C_M(a) \cdot \gamma \cdot C_M(a^{-1}) = \gamma^a\}$. With $Y = \{\varphi \in \mathrm{Hom}(G, \mathrm{Aut}_{\mathtt{Set}}(M)) \,|\, \varphi|_M = C_M\}$ we have a bijection $X \to Y$ given by $\gamma \mapsto [\sigma^n \tau_a \mapsto \gamma^n C_M(a)]$, where σ and τ_a are the image of $1 \in A$ respectively $a \in M$ in G.

Now consider the map $\Phi : Y \to Z$ given by $\varphi \mapsto \{g \in G \,|\, \varphi(g)(1) = 1\}$. To show that it is well-defined, consider $\varphi \in Y$ and let $H = \Phi(\varphi)$, which is clearly a group. If $\tau_a \in H$ then $1 = \varphi(\tau_a)(1) = a$ hence $\tau_a = 1$, so $M \to G/H$ is injective. For each $\sigma^n \in A$ we may take $a = \varphi(\sigma^n)(1)$ such that $\varphi(\tau_a^{-1}\sigma^n)(1) = 1$ hence $\tau_a^{-1}\sigma^n \in H$. Thus $\#A \leq \#H$ and $\#G/H \leq \#M$, so $M \to G/H$ is also surjective. Hence $H \in Z$ and Φ is well-defined.

For $H \in Z$ we have a natural action $G \to \mathrm{Aut}_{\mathtt{Set}}(G/H)$ and using the natural bijection $G/H \to M$ an action $\varphi_H : G \to \mathrm{Aut}_{\mathtt{Set}}(M)$. Note that $\varphi_H|_M = C_M$ and $\Phi(\varphi_H) = H$. Hence the map $\Psi : Z \to Y$ given by $H \mapsto \varphi_H$ is a right inverse of Φ. For $\varphi \in Y$, $g \in G$ and $a \in M$ we may uniquely write $g\tau_a = \tau_b h$ for some $h \in \Phi(\varphi)$ and $b \in M$, hence $(\Psi \circ \Phi)(\varphi)(g)(a) = (\Psi \circ \Phi)(\tau_b h)(1) = b = \varphi(\tau_b h)(1) = \varphi(g)(a)$, hence Ψ is a left inverse of Φ. Thus Φ is bijective and the lemma follows. □

Lemma 5.7. *Let p prime, $0 < n < k$ and consider $G = A \rtimes M$ as in Lemma 5.6. Assume $\alpha, \beta \in A$ and $\langle \tau \rangle = 1 + p^{k-n}\mathbb{Z}/p^k\mathbb{Z} \subseteq M$.*

1. *If $\alpha^{p^{n-1}} \in \langle \beta \rangle$, then $\langle \beta, \alpha\tau \rangle \cap M \neq 1$.*
2. *If $p = 2$, $\beta^2 \neq 1$ and $2 \leq n$, then $\langle \beta, \alpha\eta\tau \rangle \cap M \neq 1$ with $\eta = -1 \in M$.*

Proof. (1) Consider $S_r = \sum_{i=0}^{r-1} \tau^i$ and note that $(\alpha\tau)^r = \alpha^{S_r}\tau^r$ for all $r \geq 0$. We have

$$S_{p^{n-1}} = \sum_{i=0}^{p^{n-1}-1} \tau^i \equiv \sum_{i=0}^{p^{n-1}-1} (1 + ip^{k-n}) \equiv p^{n-1}\left(1 + \frac{p^{k-n}(p^{n-1}-1)}{2}\right) \mod p^{k-1},$$

using that both sums range over all elements of $1 + p^{k-n}\mathbb{Z}/p^{k-1}\mathbb{Z}$ and $n < k$. Hence $p^{n-1} \,|\, S_{p^{n-1}}$. When $\alpha^{p^{n-1}} \in \langle \beta \rangle$ we have $\alpha^{S_{p^{n-1}}} = \beta^r$ for some r, so $1 \neq \tau^{p^{n-1}} = \beta^{-r}(\alpha\tau)^{p^{n-1}} \in \langle \beta, \alpha\tau \rangle$, as was to be shown.

(2) Assume $p = 2$, $\beta \neq 1$ and $2 \leq n$. Then $(\alpha\eta\tau)^2 = \alpha^{1-\tau}\tau^2$ and note that $1 \neq \tau^2$ generates $1 + 2^{k-n+1}\mathbb{Z}/2^k\mathbb{Z}$ since $2 \leq n$. We have $(\alpha^{1-\tau})^{2^{n-2}} \in 2^{k-2}\mathbb{Z}/2^k\mathbb{Z} \subseteq \langle \beta \rangle$ because $\beta^2 \neq 1$. The claim now follows from (1) applied to $\alpha^{1-\tau}$ and τ^2. □

Proof of Theorem 5.1. Using Lemma 5.5, with the same notation as in Lemma 5.6, it suffices to bound $|Z|$ from above by the number of μ_{p^k}-gradings of $\mathbb{Q}(\mu_{p^k})$ listed in Example 5.4. The group G induces an exact sequence $1 \to A \to G \to M \to 1$, and any subgroup $H \subseteq G$ induces an exact sequence $1 \to H_A \to H \to H_M \to 1$ where $H_A = H \cap A$ and $H_M = \pi_M(H)$ is the projection to M. Since $A = \langle \sigma \rangle$ is cyclic of order p^k, $H_A = \langle \sigma^{p^n} \rangle$ is uniquely determined by its size p^{k-n}. If $H \in Z$, then by $p^k = |H| = |H_A| \cdot |H_M| = p^{k-n}|H_M|$ we have $|H_M| = p^n$. In particular, $H_M \subseteq 1 + p\mathbb{Z}/p^k\mathbb{Z}$ and $n < k$ using Lemma 5.2. By the same lemma, if $p \neq 2$, then $H_M = 1 + p^{k-n}\mathbb{Z}/p^k\mathbb{Z} = \langle 1 + p^{k-n} \rangle$, which is cyclic. From Corollary 5.3 it follows that, in general, we may distinguish between the following mutually exclusive cases.

(1)	$H_M = \langle 1 + p^{k-n} \rangle$	for $0 \leq n \leq k-1$ and if $p = 2$ also $n \leq k-2$
(2)	$H_M = \langle -1 + p^{k-n} \rangle$	for $p = 2$ and $1 \leq n \leq k-2$
(3)	$H_M = \langle 1 + p^{k-n+1}, -1 \rangle$	for $p = 2$ and $1 \leq n \leq k-1$

Case (1): Here $H = \langle \sigma^{p^n}, \sigma^r \tau \rangle$ for some $r \in \mathbb{Z}/p^n\mathbb{Z}$, where τ is the image of $1 + p^{k-n} \in M$ in G. If $n = 0$, then $H = A$, which is a single solution. Now assume $n > 0$. If $p \,|\, r$, then $H \cap M \neq 1$ by Lemma 5.7.1. Thus $r \in (\mathbb{Z}/p^n\mathbb{Z})^*$, meaning that given n there are at most $p^n - p^{n-1}$ possible groups H in this case.

Case (2): Here $H = \langle \sigma^{2^n}, \sigma^r \eta\tau \rangle$ for some $r \in \mathbb{Z}/2^n\mathbb{Z}$, $\eta = -1$ and $\tau = 1 + 2^{k-n}$. If $n = 1$, then $r = 1$ as $\eta\tau \notin H$, which yields one possible H. For larger n we have $\sigma^{2^{n+1}} \neq 1$ hence there are no possible subgroups H by Lemma 5.7.2.

Case (3): Here $H = \langle \sigma^{2^n}, \sigma^r \tau, \sigma^s \eta \rangle$ for $r, s \in \mathbb{Z}/2^n\mathbb{Z}$, $\eta = -1$ and $\tau = 1 + 2^{k-n+1}$. If $n = 1$, then $r = 0$ and $s = 1$, giving a single subgroup. If $n = 2$, then $r, s \neq 0$ and $r \neq s$ as $\sigma^{s-t}\eta\tau \in H$ while $1 \neq \eta\tau \in M$. Moreover $(\sigma^r\tau)^2 = \sigma^{r(2+2^{k-1})} \in H$ implies $2 \,|\, r$. Thus $(r, s) \in \{(2, 1), (2, 3)\}$ gives two possible subgroups. If $3 \leq n < k - 1$, we consider $\sigma^{s-r}\eta\tau = \sigma^s\eta\sigma^r\tau \in H$ and note that by Lemma 5.7.2 no subgroups exist. Hence assume $n = k - 1$. Then $\sigma^{2r+4s} = [\sigma^r\tau, \sigma^s\eta] \in H$, meaning that $2^{k-2} \,|\, r + 2s$. We have that $4 \nmid r$ by applying Lemma 5.7 to $\sigma^r\tau$, so $2 \nmid s$. There are then 2^{k-2} possible values of s, and for each only two possible r, giving at most 2^{k-1} subgroups H.

If $p \neq 2$, then summing over all n in case (1) gives $|Z| \leq 1 + \sum_{i=1}^{k-1}(p^i - p^{i-1}) = p^{k-1}$, the right hand side of which equals the number of μ_{p^k}-gradings of $\mathbb{Q}(\mu_{p^k})$ listed in Example 5.4. If $p = 2$, then $|Z| \leq 2$ if $k = 2$, $|Z| \leq 6$ if $k = 3$ and $|Z| \leq 4 + 2^{k-2} + 2^{k-1}$ if $4 \leq k$, which is again precisely the number of distinct μ_{2^k}-gradings of $\mathbb{Q}(\mu_{2^k})$ listed in Example 5.4, as was to be shown. □

6 Existence of universal gradings

In this section we present two proofs for the existence of universal gradings of reduced orders.

6.1 Primitive idempotents and factorization of gradings

Definition 6.1. Let R be a commutative ring. Then $e \in R$ is called *idempotent* if $e^2 = e$. We call e a *primitive idempotent* if $e \neq 0$ and $ee' \in \{e, 0\}$ for all idempotents e'. We write $\operatorname{prid}(R)$ for the set of primitive idempotents of R. We say R is *connected* when $1 \in \operatorname{prid} R$.

Note that for each commutative ring R and idempotent $e \in R$ we get a ring eR.

Lemma 6.2. *Let R be a commutative ring. If $\# \operatorname{minspec} R < \infty$, then R has only finitely many idempotents. If R has only finitely many idempotents, then $\sum_{e \in \operatorname{prid} R} e = 1$ and the natural morphism of abelian groups $\prod_{e \in \operatorname{prid} R} eR \to R$ is an isomorphism of rings.*

Proof. The natural map $R/\sqrt{0} \to \prod_{\mathfrak{p} \in \operatorname{minspec} R} R/\mathfrak{p}$ is injective by Lemma 4.11. The idempotents of $\prod_{\mathfrak{p}} R/\mathfrak{p}$ are $\{0,1\}^{\operatorname{minspec} R}$ since each $R/\mathfrak{p}$ is a domain. If $\# \operatorname{minspec} R < \infty$, then $\prod_{\mathfrak{p}} R/\mathfrak{p}$ and therefore $R/\sqrt{0}$ have only finitely many idempotents. Assume $e, f \in R$ are idempotents such that $e - f \in \sqrt{0}$. Then for some $n \in \mathbb{Z}_{\geq 0}$ we have

$$0 = (e-f)^{2n+1} = \sum_{i=0}^{2n+1} \binom{2n+1}{i} e^i (-f)^{2n+1-i} = e - f + ef \sum_{i=1}^{2n} \binom{2n}{i} (-1)^i = e - f,$$

hence $e = f$. Hence R has only finitely many idempotents as well.

Assume R has only finitely many idempotents. Note that the primitive idempotents are simply the minimal elements among the non-zero idempotents of R under the partial order $\preceq$ given by $e \preceq e'$ if and only if $ee' = e$. Now let $x = \sum_{e \in \operatorname{prid} R} e$ and assume $x \neq 1$. Then $y = 1 - x \neq 0$ is an idempotent, so there exists some $e' \in \operatorname{prid} R$ such that $e' \preceq y$ by finiteness. Then $e' = e'y = e' - \sum_{e \in \operatorname{prid} R} ee' = e' - e' = 0$ since $ee' = 0$ for all $e' \neq e \in \operatorname{prid} R$, which is a contradiction. Hence $x = 1$.

Now consider the natural map $\varphi : \prod_{e \in \operatorname{prid} R} eR \to R$ and the map $\psi : R \to \prod_{e \in \operatorname{prid} R} eR$ given by $r \mapsto (er)_{e \in \operatorname{prid} R}$. Clearly $\psi\varphi = \mathrm{id}$ since $ee' = 0$ for distinct $e, e' \in \operatorname{prid} R$, while $\varphi\psi = \mathrm{id}$ additionally requires that $\sum_{e \in \operatorname{prid} R} e = 1$. Hence φ is an isomorphism. □

Corollary 6.3. *Let R be a commutative reduced $\mathbb{Q}$-algebra of finite dimension as $\mathbb{Q}$-module. Then R is connected if and only if it is a field, and* $\operatorname{spec} R = \{(1-e)R \mid e \in \operatorname{prid}(R)\}$.

Proof. Use the facts that $eR \cong R/(1-e)R$ for idempotents e, that $R \cong \prod_{\mathfrak{m} \in \operatorname{spec} R} R/\mathfrak{m}$ and that $\operatorname{prid} \prod_{\mathfrak{m}} R/\mathfrak{m} = \{e_{\mathfrak{n}} \mid \mathfrak{n} \in \operatorname{spec} R\}$ with $e_{\mathfrak{n}} = (\mathbb{1}_{\mathfrak{m}=\mathfrak{n}})_{\mathfrak{m} \in \operatorname{spec} R}$. □

In Lemma 6.2 we used the primitive idempotents to factor our rings. We can apply the same technique to gradings. For this, recall that we have defined a coproduct of gradings in Definition 2.10.

Definition 6.4. Let R be a commutative ring with only finitely many idempotents and let $\overline{R} = (R, \Gamma, \{R_\gamma\}_{\gamma \in \Gamma})$ be a grid-grading. For each $e \in \operatorname{prid} R_1$ we define $\Gamma_e = \langle \gamma \in \Gamma \mid eR_\gamma \neq 0 \rangle$ and $\overline{eR} = (eR, \Gamma_e, \{eR_\gamma\}_{\gamma \in \Gamma_e})$.

Lemma 6.5. *Let R be a commutative ring with only finitely many idempotents and let $\overline{R} = (R, \Gamma, \{R_\gamma\}_{\gamma \in \Gamma})$ be a grid-grading. Then $\overline{eR}$ and $\overline{R'} := \coprod_{e \in \operatorname{prid} R_1} \overline{eR}$ are efficient gradings of R and the natural map $\varphi : \coprod_{e \in \operatorname{prid} R_1} \Gamma_e \to \Gamma$ satisfies $\varphi_* \overline{R'} = \overline{R}$.*

Proof. Clearly $1_{eR} = e \in eR_1$ and $eR_\gamma \cdot eR_{\gamma'} = eR_\gamma R_{\gamma'} \subseteq eR_{\gamma\gamma'}$, so $\overline{eR}$ is a grading. Then $\overline{R'}$ is a grading of R by Lemma 6.2, and $\varphi_* \overline{R'} = \overline{R}$ follows trivially. Additionally $\overline{eR}$ and $\overline{R'}$ are efficient by construction. □

Lemma 6.5 will allow us to assume that the trivial components of our gradings are connected in some of the proofs, most notably Proposition 6.12. In the case of finite-dimensional reduced $\mathbb{Q}$-algebras we even have that each factor $\overline{eR}$ of $\overline{R}$ is an abelian group-grading by Corollary 6.3 and Proposition 2.6.

Example 6.6. In this example we construct a ring R for which $X_\infty(R)$ as defined in Definition 3.22 is an abelian group but is not compact, meaning that any pair of abelian group-gradings of R have a joint grading as follows from Theorem 3.34, while no universal grading exists by Theorem 3.35. Consider $R = \mathbb{Z}[\sqrt{2}]^{\mathbb{Z}}$ and let p be prime. Note that $\sqrt{2} \in \mathbb{Q}(\zeta_8) \setminus \mathbb{Q}(\zeta_4)$ hence $\sqrt{2} \notin \mathbb{Q}(\zeta_{p^2})$. Thus $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p^2}] \cong \mathbb{Z}[\sqrt{2}, \zeta_{p^2}]$ is a domain. Now consider $R' = \mathbb{Z}[\sqrt{2}, \zeta_{p^2}]^{\mathbb{Z}}$ and note that we have a natural map $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p^2}] \to R'$. Since $\mathbb{Z}[\zeta_{p^2}]$ is free of finite rank as $\mathbb{Z}$-module, we even have that this map is an isomorphism. We have that each automorphism of R' must permute the primitive idempotents, which are the elements $e_i = (\mathbb{1}(j = i))_{j\in\mathbb{Z}}$ of R'. Thus we have a natural map $\mathrm{Aut}_{\mathbb{Z}[\zeta_{p^2}]\text{-}\mathtt{Alg}}(R') \to \mathrm{Aut}_{\mathbb{Z}[\zeta_{p^2}]\text{-}\mathtt{Alg}}(\mathbb{Z}[\sqrt{2}, \zeta_{p^2}])^{\mathbb{Z}} \rtimes \mathrm{Aut}_{\mathtt{Set}}(\mathbb{Z})$. Using the universal property of the product one can show that this map is an isomorphism as well.

Now let $\sigma \in X_{p^2}(R)$ and $i \in \mathbb{Z}$. Let $n = \#(\langle\sigma\rangle e_i)$ and assume $n \neq 1$. Because $n \mid \mathrm{ord}(\sigma) \mid p^2$ we have $\zeta_n \in \mathbb{Z}[\zeta_{p^2}]$. For $0 \le m < n$ let $a_m = \sum_{j=0}^{n-1} \zeta_n^{-mj}\sigma^j(e_i)$ and note that $a_m \in R'(\sigma, \zeta_n^m)$. Then

$$\sum_{m=0}^{n-1} a_m = \sum_{j=0}^{n-1} \sigma^j(e_i) \sum_{m=0}^{n-1} \zeta_n^{-mj} = \sum_{j=0}^{n-1} \sigma^j(e_i) \cdot n\mathbb{1}(j = 0) = ne_i.$$

We have $a_m/n \notin R'$ since $\zeta_n/n \notin \mathbb{Z}[\zeta_n]$, but $e_i \in \bigoplus_{j=0}^{p^2-1} R'(\sigma, \zeta_{p^2}^j)$ by μ_{p^2}-diagonalizability of σ, a contradiction. Thus $n = 1$. It follows that $X_{p^2}(R) \subseteq \mathrm{Aut}_{\mathbb{Z}[\zeta_{p^2}]\text{-}\mathtt{Alg}}(\mathbb{Z}[\sqrt{2}, \zeta_{p^2}])^{\mathbb{Z}}$. Since the latter has exponent 2, we only obtain non-trivial gradings when $p = 2$, and the only efficient gradings of R with μ_e for $e \in \mathbb{S}$ have $e \mid 2$. We conclude that $X_\infty(R) \cong X_2(R) \cong \mathrm{Aut}(\mathbb{Z}[\sqrt{2}])^{\mathbb{Z}}$, which is abelian. However, it is not compact since $(\sqrt{2})_{i\in\mathbb{Z}}$ has an infinite orbit under $X_\infty(R)$. Hence for any two abelian torsion group-gradings of R a joint-grading exists, while no universal abelian torsion group-grading of R exists.

6.2 Hierarchy of categories

We consider gradings of a ring R with a grid G. In this section we show that if R has a universal grid-grading, then it has a universal group-grading. Similarly the existence of a universal abelian group-grading follows from the existence of a universal group-grading.

Proposition 6.7. *Let k be a commutative ring, let R be a k-algebra and let $\overline{U} = (R, \mathrm{Y}, \mathcal{R})$ be a grading. If $\overline{U}$ is a universal grid-grading, then $f_*\overline{U}$ is a universal group-grading, with $f : \mathrm{Y} \to \mathrm{Y}^{\mathtt{grp}}$ the groupification map as in Lemma 2.9. If $\overline{U}$ is a universal group-grading, then $f_*\overline{U}$ is a universal group-grading, with $f : \mathrm{Y} \to \mathrm{Y}^{\mathtt{ab}}$ the abelianization map.*

Proof. We have forgetful functors $M_{\mathtt{Grp}} : \mathtt{Grp} \to \mathtt{Grd}$ and $M_{\mathtt{Ab}} : \mathtt{Ab} \to \mathtt{Grp}$ which are right adjoints of $\_^{\mathtt{grp}}$ (Lemma 2.9) respectively $\_^{\mathtt{ab}}$. For $\mathcal{C} \in \{\mathtt{Grd}, \mathtt{Grp}, \mathtt{Ab}\}$, there exists a universal $\mathcal{C}$-grading of R if and only if the functor $F_{\mathcal{C}} : \mathcal{C} \to \mathtt{Set}$ given by $\Gamma \mapsto \{\Gamma\text{-gradings of } R\}$ is representable. Note that $F_{\mathtt{Ab}} \cong F_{\mathtt{Grp}} \circ M_{\mathtt{Ab}}$ and $F_{\mathtt{Grp}} \cong F_{\mathtt{Grd}} \circ M_{\mathtt{Grp}}$. If we have categories $\mathcal{C}$ and $\mathcal{D}$, a right adjoint functor $M : \mathcal{D} \to \mathcal{C}$ and a representable functor $F : \mathcal{C} \to \mathtt{Set}$, then $F \circ M$ is representable. Namely, let L be a left adjoint of M and assume F is representable. Then there exists an $A \in \mathrm{obj}(\mathcal{C})$ and natural isomorphism $\mathrm{Hom}_{\mathcal{C}}(A, \_) \cong F$. Hence $F \circ M \cong \mathrm{Hom}_{\mathcal{D}}(A, M(\_)) \cong \mathrm{Hom}_{\mathcal{C}}(L(A), \_)$ so $F \circ R$ is representable. Moreover, we obtain a universal element of $F \circ M$ from a universal element of F by applying L to it, from which the lemma follows. □

Proposition 6.8. *Let k be a commutative ring and R be a k-algebra with a decomposition $\mathcal{M}$ not containing $\{0\}$. Then the functor $F : \mathtt{Grd} \to \mathtt{Set}$ given by*

$$\Gamma \mapsto \{\textit{grid-gradings } (R, \Gamma, \mathcal{R}) \textit{ such that } \mathcal{M} \preceq \mathcal{R}\}$$

is representable, where $\preceq$ is as defined in Definition 1.1.

Proof. Write $\mathcal{M} = \{M_i\}_{i\in I}$ and let X be the set of equivalence relations $\sim$ on I such that $\{N_j\}_{j\in I/\sim} := \pi^{\sim}_* \mathcal{M}$, where $\pi^{\sim} : I \to I/{\sim}$ is the quotient map, is a pre-grading of R such that $1 \in N_e$ for some unique $e \in I/{\sim}$ and if $N_j N_j \subseteq N_j$ for $j \in I/{\sim}$ we have $j = e$. Now define an equivalence relation $\simeq$ on I such that for $i, j \in I$ we have $i \simeq j$ if and only if $i \sim j$ for all $\sim \in X$. It is a straightforward verification that $\simeq \in X$. Let $S = I/{\simeq}$ and $\mathcal{U} = \{U_s\}_{s\in S} := \pi^{\simeq}_* \mathcal{M}$.

If $R = 0$ then $I = \emptyset$ and $F \cong \mathrm{Hom}_{\mathtt{Grd}}(\{1\}, \_)$ is representable. Hence assume $R \neq 0$. Let $e \in S$ be the unique element such that $1 \in U_e$. Let $\Upsilon = (S, e, D, *)$ with $D = \{(s,t) \in S \,|\, U_s \cdot U_t \neq 0\}$ and $s * t$ the unique $u \in S$ such that $U_s \cdot U_t \subseteq U_u$ for all $(s,t) \in D$. Note that $(e,s), (s,e) \in D$ and $s = s * 1 = 1 * s$ for all $s \in S$ since $0 \neq 1 \in U_e$ and $U_s \neq 0$ so $U_s \cap (U_e U_s) \cap (U_s U_e) \neq 0$. Then Υ is a grid and $\overline{U} = (R, \Upsilon, \mathcal{U})$ is a loose grid-grading.

Now let $\overline{R} = (R, \Gamma, \mathcal{R})$ be any grid-grading such that $\mathcal{M} \preceq \mathcal{R} =: \{R_\gamma\}_{\gamma\in\Gamma}$. Then there exists a map $f : I \to \Gamma$ such that $f_*\mathcal{M} = \mathcal{R}$, and f induces an equivalence relation $\sim$ on I where $i \sim j$ if and only if $f(i) = f(j)$. Note that $\sim \in X$, hence $\pi^{\sim} = q \circ \pi^{\simeq}$ for some unique q by definition of $\simeq$. Then $f = g \circ \pi^{\simeq}$ for some unique $g : S \to \Gamma$. We note that g as map of grids $G \to \Gamma$ is in fact a morphism, hence $\overline{R} = g_*\overline{U}$. Thus $\overline{U}$ is a universal object of F and F is representable. □

6.3 A proof using lattices

We prove the existence of universal grid gradings using a generalization of the proof in [1], Section 9.

Definition 6.9. Let R be a subring of a finite product of number fields. We then define the map $R^2 \to \mathbb{C}$ given by

$$(x, y) \mapsto \langle x, y\rangle_R := \sum_{\sigma\in\mathrm{Hom}_{\mathtt{Rng}}(R,\mathbb{C})} \sigma(x)\overline{\sigma(y)}.$$

Remark 6.10. Note that $\langle \_, \_\rangle_R$ as in Definition 6.9 is in fact real valued. For $\sigma \in \mathrm{Hom}_{\mathtt{Rng}}(R, \mathbb{C})$ the map $x \mapsto \overline{\sigma(x)}$ is also an element of $\mathrm{Hom}_{\mathtt{Rng}}(R, \mathbb{C})$, so complex conjugation of $\langle x, y\rangle_R$ for $x, y \in R$ simply permutes the terms of the sum defining $\langle \_, \_\rangle_R$. Hence $\overline{\langle x, y\rangle_R} = \langle x, y\rangle_R$ must be real. Additionally, for all $x, y \in R$ we have the following properties: (1) $\langle \_, y\rangle_R$ is $\mathbb{Z}$-linear; (2) $\langle x, y\rangle_R = \langle y, x\rangle_R$ and (3) $\langle x, x\rangle_R \in \mathbb{R}_{\geq 0}$ with $\langle x, x\rangle_R = 0$ if and only if $x = 0$. If R is a $\mathbb{Q}$-module, we would call $\langle \_, \_\rangle_R$ an inner product.

Lemma 6.11. *Let R be a finite product of number fields. Then for all $n \in \mathbb{Z}_{\geq 0}$, $x, y \in R$ and $e \in R$ idempotent we have $\langle ex, ey\rangle_R = \langle ex, ey\rangle_{eR}$ and $\langle x, y\rangle_{R\otimes_{\mathbb{Q}}\mathbb{Q}(\mu_n)} = \varphi(n) \cdot \langle x, y\rangle_R$, where φ is Euler's totient function.*

Proof. For each idempotent $e \in R$ a map $eR \to \mathbb{C}$ extends to a map $R \to \mathbb{C}$ by composing with the projection. We have an isomorphism $R \cong eR \times (1-e)R$ and from this it follows the natural map $\mathrm{Hom}_{\mathtt{Rng}}(eR, \mathbb{C}) \sqcup \mathrm{Hom}_{\mathtt{Rng}}((1-e)R, \mathbb{C}) \to \mathrm{Hom}_{\mathtt{Rng}}(R, \mathbb{C})$ is a bijection. Then $\langle ex, ey\rangle_R = \langle ex, ey\rangle_{eR}$ for all $x, y \in R$ follows trivially.

Let $n \in \mathbb{Z}_{\geq 0}$. By the universal property of the tensor product we have mutually inverse maps

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Q}\text{-}\mathtt{Alg}}(R, \mathbb{C}) \times \mathrm{Hom}_{\mathbb{Q}\text{-}\mathtt{Alg}}(\mathbb{Q}(\mu_n), \mathbb{C}) &\to \mathrm{Hom}_{\mathbb{Q}\text{-}\mathtt{Alg}}(R \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_n), \mathbb{C}) \\ (f, g) &\mapsto f \otimes g = \big[x \otimes y \mapsto f(x) \otimes g(y)\big] \\ \big[x \mapsto f(x \otimes 1),\ y \mapsto f(1 \otimes y)\big] &\mapsfrom f \end{aligned}$$

From Corollary 3.12 it follows that $\#\,\mathrm{Hom}_{\mathbb{Q}\text{-}\mathtt{Alg}}(\mathbb{Q}(\mu_n), \mathbb{C}) = \varphi(n)$. Let $\sigma \in \mathrm{Hom}_{\mathtt{Rng}}(R, \mathbb{C})$. Now $(\sigma \otimes \chi)(x) = \sigma(x)$ for all $\chi \in \mathrm{Hom}_{\mathtt{Rng}}(\mathbb{Q}(\mu_n), \mathbb{C})$ and $x \in R$. Hence

$$\sum_{\chi\in\mathrm{Hom}_{\mathtt{Rng}}(\mathbb{Q}(\mu_n),\mathbb{C})} (\sigma \otimes \chi)(x)\overline{(\sigma \otimes \chi)(y)} = \varphi(n) \cdot \sigma(x)\overline{\sigma(y)}$$

for all $x, y \in R$, from which it follows that $\langle x, y\rangle_{R\otimes_{\mathbb{Q}}\mathbb{Q}(\mu_n)} = \varphi(n) \cdot \langle x, y\rangle_R$. □

Proposition 6.12. *Let R be a product of number fields with $\dim_{\mathbb{Q}}(R) < \infty$, let Γ be a grid and let $\overline{R}$ be a Γ-grading of R. Then $\langle R_\gamma, R_\delta\rangle_R = 0$ if and only if $\gamma \neq \delta$ or $R_\gamma = 0$.*

Proof. ($\Rightarrow$) If $R_\gamma \neq 0$ and $\gamma = \delta$, then for any non-zero $x \in R_\gamma$ we have $0 < \langle x, x\rangle \in \langle R_\gamma, R_\delta\rangle$.

($\Leftarrow$) Let $J = \mathrm{prid}(R_1)$ as in Definition 6.1 and note that the elements of J are orthogonal and sum to 1 by Lemma 6.2. Thus for all $x, y \in R$ we have $\langle x, y\rangle_R = \sum_{e\in J}\langle ex, ey\rangle_R$. Hence to show $\langle R_\gamma, R_\delta\rangle_R = 0$ it suffices to show that $\langle eR_\gamma, eR_\delta\rangle_R = 0$ for all $e \in J$. By Lemma 6.11 we have $\langle eR_\gamma, eR_\delta\rangle_R = \langle eR_\gamma, eR_\delta\rangle_{eR}$. Thus we may assume without loss of generality that $\overline{R} = \overline{eR}$. Then R_1 is connected, so it is a field by Corollary 6.3. Thus Γ is a finite abelian group by Proposition 2.6.2. If $R_\gamma = 0$ then $\langle R_\gamma, R_\delta\rangle = 0$ and we are done. Hence assume $\delta \neq \gamma$, so there exists a character $\chi \in \widehat{\Gamma}$ such that $\chi(\gamma) \neq \chi(\delta)$ by Theorem 3.29. Let n be the exponent of Γ and write $R'_\alpha = R_\alpha \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_n)$ for all $\alpha \in \Gamma$. Note that $\widehat{\Gamma}$ acts on $R' = R \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_n)$, where $\chi \in \widehat{\Gamma}$ acts by sending $x \in R'_\alpha$ to $\chi(\alpha)x$ for all $\alpha \in \Gamma$. Then $\langle \chi * x, \chi * y\rangle_{R'} = \langle x, y\rangle_{R'}$ for all $x, y \in R'$, as applying χ just results in a reordering of the sum defining the inner product. Then for any $x \in R'_\gamma$ and $y \in R'_\delta$, we have

$$\langle x, y\rangle_{R'} = \langle \chi * x, \chi * y\rangle_{R'} = \langle \chi(\gamma)\cdot x, \chi(\delta)\cdot y\rangle_{R'} = \langle \chi(\gamma\delta^{-1})\cdot x, y\rangle_{R'}.$$

As $s = 1 - \chi(\gamma\delta^{-1}) \neq 0$ there exists some $t \in \mathbb{Z}[\mu_n]$ such that $st = n$ by Lemma 3.13.2. Thus

$$0 = \langle sR'_\gamma, R'_\delta\rangle_{R'} \supseteq \langle stR'_\gamma, R'_\delta\rangle_{R'} = n\langle R'_\gamma, R'_\delta\rangle_{R'}$$

Then from Lemma 6.11 it follows that $\langle R_\gamma, R_\delta\rangle_R = 0$, as was to be shown. □

Corollary 6.13. *Let R be a reduced order and let $\overline{R}$ be a Γ-grading of R. Then $\langle R_\gamma, R_\delta\rangle_R = 0$ if and only if $\gamma \neq \delta$ or $R_\gamma = 0$.*

Proof. Since R is a reduced order, $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product of number fields and $\overline{E} = \overline{R} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a Γ-grading of E such that $E_\gamma \cap R = R_\gamma$. Any $\sigma : R \to \mathbb{C}$ naturally extends to a morphism $\sigma' : E \to \mathbb{C}$ and each $\rho : E \to \mathbb{C}$ restricts to a map $\rho' : R \to \mathbb{C}$, hence $\langle x, y\rangle_E = \langle x, y\rangle_R$ for all $x, y \in R$. The claim then follows from Proposition 6.12. □

Proof of Theorem 1.8: Since R is a reduced order, it has a lattice structure with inner product $\langle \_, \_ \rangle_R$ as in Definition 6.9. Then Theorem 2 in [11] states that R has a decomposition $\mathcal{E} = \{E_s\}_{s\in S}$ such that $\langle E_s, E_t\rangle = 0$ when $s, t \in S$ are distinct, and such that $\mathcal{E}$ is universal with this property, i.e. for any other such decomposition $\mathcal{F} = \{F_t\}_{t\in T}$ of R there exists a unique map $f : S \to T$ such that $f_*\mathcal{E} = \mathcal{F}$. We then obtain a universal grid grading of R by applying Proposition 6.8 to $\mathcal{E}$, because Corollary 6.13 ensures all gradings of R have $\mathcal{E}$ as refinement. A universal group grading and abelian group grading then exist by Proposition 6.7.

□

6.4 A proof using automorphism groups

Instead of generalizing groups to grids, we will now focus on generalizing reduced orders to a broader class of rings. To show R has a universal abelian group-grading, it suffices to show that $X_\infty(R)$ as defined in Definition 3.22 is a finite abelian group by Theorem 3.35.

Definition 6.14. Let k be a commutative ring with $p \in k$ and let M be a k-module. A k-subalgebra $A \subseteq \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ is called *p-good* if $p(1 - ps)$ is injective for all $s \in A$.

Lemma 6.15. *Let k be a commutative ring, let M be a k-module and let $A \subseteq \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$ be a k-subalgebra. Let $p \in k$, $u \in k^*$ and $n \in \mathbb{Z}_{>0}$. If A is up^n-good, then A is p-good.*

Proof. Since multiplication by up^n is injective, so is multiplication p. If $(1 - ps)(x) = 0$ for $s \in A$ and $x \in M$, then $x = ps(x)$ so $x = (ps)^n(x) = p^n s^n(x)$. Then $r = u^{-1}s^n \in A$ and A is up^n-good. Because $up^n(1 - up^n r)(x) = 0$ we get that $x = 0$ and thus A is p-good. □

Proposition 6.16. *Let p and q be (not necessarily distinct) primes, let $k = \mathbb{Z}[\zeta_p, \zeta_q]$ and let M be a k-module. Write $E = \mathrm{End}_{k\text{-}\mathtt{Mod}}(M)$, $\pi = 1 - \zeta_p$ and $\tau = 1 - \zeta_q$ and let $A \subseteq E$ be a p-good and q-good k-subalgebra.*

(1) *If $\langle 1 + \pi\tau s\rangle \subseteq A^*$ for some $s \in A$ is torsion, then $s = 0$.*

(2) *If $\langle 1 + \pi s, 1 + \tau r\rangle \subseteq A^*$ for some $s, r \in A$ is torsion, then $1 + \pi s$ and $1 + \tau r$ commute.*

Proof. Note that by Lemma 3.13.1 and Lemma 6.15 a p-good algebra is π-good.

(1) Write $T = 1 + \tau k[X] \subseteq k[X]$. Recall that $\pi^{p-1} \in pk$ by Lemma 3.13 and that $p \mid \binom{p}{i}$ for $0 < i < p$. Hence

$$(1 + \pi\tau TX)^p \subseteq 1 + p\pi\tau T \left(1 + \tau \sum_{i=2}^{p} \frac{\binom{p}{i}\pi^{i-1}\tau^{i-2}}{p}(XT)^{i-1}\right) X \subseteq 1 + p\pi\tau TX. \tag{6.16.1}$$

Then inductively we have $(1 + \pi\tau TX)^{p^n} \subseteq (1 + p^{n-1}\pi\tau TX)^p \subseteq 1 + p^n\pi\tau TX$, where we obtain the second inclusion by substituting $p^{n-1}X$ for X in (6.16.1).

Consider $\sigma = 1 + \pi\tau s$. By assumption we have $\sigma^n = 1$ for some $n \in \mathbb{Z}_{>0}$. If $n = p^m$ for some $m \in \mathbb{Z}_{\geq 0}$, then $1 = \sigma^n = 1 + p^m\pi\tau(1 + \tau e)s$ for some $e \in A$ by what we have shown before. We have $p^m\pi\tau(1 + \tau e)s = 0$ while $p^m\pi\tau(1 + \tau e)$ is injective by p-goodness and q-goodness, hence $s = 0$. Thus we assume n and p are coprime, in which case there exists some $m > 0$ such that $n \mid p^m - 1$. Then $1 + \pi\tau s = \sigma = \sigma^{p^m} = 1 + p^m\pi\tau(1 + \tau e)s$ and thus $\pi\tau(1 - p^m(1 + \tau e))s = 0$. As $\pi\tau(1 - p^m(1 + \tau e))$ is injective we again have $s = 0$, as was to be shown.

(2) Let $\sigma = 1 + \pi s$ and $\rho = 1 + \tau r$. By assumption $\sigma^{-1} \in A$ hence $s' = -\sigma^{-1}s \in A$ and $\sigma(1 + \pi s') = 1 = (1 + \pi s')\sigma$, so $\sigma^{-1} = 1 + \pi s'$. As $1 = \sigma\sigma^{-1} = 1 + \pi(s + s' + \pi ss')$ we get $\pi(s + s' + \pi ss') = 0$. Similarly $\tau(r + r' + \tau rr') = 0$ for $\rho^{-1} = 1 + \tau r'$. Now

$$[\sigma, \rho] \equiv (1 + \pi s)(1 + \tau r)(1 + \pi s')(1 + \tau r') \equiv 1 + \pi(s + s' + \pi ss') + \tau(r + r' + \tau rr') \equiv 1 \mod \pi\tau.$$

The group $\langle[\sigma, \rho]\rangle \subseteq \langle\sigma, \rho\rangle$ is torsion, hence we have $[\sigma, \rho] = 1$ by (1). □

Proposition 6.17. *Let $e \in \mathbb{S}$, let $k = \mathbb{Z}[\mu_e]$, let M be a k-module and let $A \subseteq E = \operatorname{End}_{k\text{-}\mathtt{Mod}}(M)$ be p-good k-subalgebra such that $(1 - \zeta_p)A = A \cap (1 - \zeta_p)E$ for all primes $p \mid e$. If $\rho, \sigma \in A$ are μ_e-diagonalizable and $\langle\rho, \sigma\rangle$ is torsion, then ρ and σ commute.*

Proof. By the Chinese remainder theorem we may write $\sigma = \sigma_1 \cdots \sigma_s$ with $[\sigma_i, \sigma_j] = 1$ and $\sigma_i \in \langle\sigma\rangle$ of prime power order for all $1 \leq i, j \leq s$, and similarly we write $\rho = \rho_1 \cdots \rho_r$. To show $[\sigma, \rho] = 1$ it suffices to show that $[\sigma_i, \rho_j] = 1$ for all i and j. Thus we may assume without loss of generality that $\operatorname{ord}(\sigma) = p^a$ and $\operatorname{ord}(\rho) = q^b$ for $a, b \in \mathbb{Z}_{\geq 0}$ and primes $p, q \mid e$.

We apply induction to $n = a + b$. First assume $a, b \leq 1$. Consider $\pi = 1 - \zeta_p$ and recall that $1 - \zeta_p^i \equiv 0 \mod \pi$ for all $i \in \mathbb{Z}$ by Lemma 3.13. Thus $1 - \sigma \equiv 0 \mod \pi$ by μ_p-diagonalizability. Hence $\sigma = 1 + \pi s$ for some $s \in E$ and thus $s \in A$ by $\pi A = A \cap \pi E$. Similarly $\rho = 1 + \tau r$ with $\tau = 1 - \zeta_q$, hence $[\sigma, \rho] = 1$ by Proposition 6.16.2. Otherwise we may assume without loss of generality that $a \geq 2$. Then $[\sigma^p, \rho] = 1$ by the induction hypothesis. Fix $\zeta \in \mu_{p^a}$ and consider $N = M(\sigma^p, \zeta^p)$ and the k-subalgebra $B = \{\sigma \in A \mid \sigma N \subseteq N\} \subseteq A$. Then $\sigma \in B$ by construction of N and $\rho \in B$ by Lemma 3.17. Since N is a direct summand of M we get that $C = B|_N \subseteq \operatorname{End}_{k\text{-}\mathtt{Mod}}(N)$ is r-good and $(1 - \zeta_r)C = C \cap (1 - \zeta_r)\operatorname{End}_{k\text{-}\mathtt{Mod}}(N)$ for all primes $r \mid e$. Let $\alpha = \rho|_N$ and $\beta = (\zeta^{-1}\sigma)|_N$, which are respectively μ_{p^a}-diagonalizable and μ_q-diagonalizable. Moreover, $\langle\alpha, \beta\rangle \subseteq C^*$ is a torsion subgroup. We have $\operatorname{ord}(\alpha) = 1 < \operatorname{ord}(\sigma)$ and $\operatorname{ord}(\beta) \leq \operatorname{ord}(\rho)$, so we may apply the induction hypothesis to conclude α and β commute. In particular, ρ and σ commute when restricted to $M(\sigma^p, \zeta^p)$ for each ζ, so σ and ρ commute on M by $\mu_{p^{a-1}}$-diagonalizability of σ^p. Hence $\langle\rho, \sigma\rangle$ is abelian when it is torsion. □

Lemma 6.18. *Let $e \in \mathbb{S}$ and let R be a commutative ring such that multiplication by integer divisors of e is injective on R. If R is reduced, then $R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ is reduced.*

Proof. Since $R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e] = \lim_{\to d \in \mathbb{Z}_{>0},\ d \mid e} R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_d]$ we may assume without loss of generality that $e \in \mathbb{Z}_{>0}$. With $S = \{e^m \mid m \in \mathbb{Z}_{\geq 0}\}$ we consider the localization $S^{-1}R$, which is reduced, and note that R injects into $S^{-1}R$ since multiplication by e is injective. Since $(S^{-1}R) \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e] \cong S^{-1}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e])$, we may also assume without loss of generality that $R = S^{-1}R$. Let $\mathfrak{p} \in \operatorname{minspec} R$, let $K_{\mathfrak{p}}$ be a field containing $R/\mathfrak{p}$ and note that $\operatorname{char}(K_{\mathfrak{p}}) \nmid e$ as e is invertible in $R/\mathfrak{p}$. We have that $X^e - 1$ and thus Φ_e, the e-th cyclotomic polynomial, is separable over $K_{\mathfrak{p}}$ since its derivative eX^{e-1} only has 0 as root. Hence $K_{\mathfrak{p}} \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e] \cong K_{\mathfrak{p}}[X]/\Phi_e$ is reduced by Theorem A1.3 in [9]. By Lemma 4.11 we have an injection

$$R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e] \to \left(\prod_{\mathfrak{p} \in \operatorname{minspec} R} K_{\mathfrak{p}}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e] \cong \prod_{\mathfrak{p} \in \operatorname{minspec} R} (K_{\mathfrak{p}} \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]),$$

where the isomorphism follows from the fact that $\mathbb{Z}[\mu_e]$ is a free $\mathbb{Z}$-module of finite rank. It follows that $R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ is reduced as well. □

Lemma 6.19. *Let k be a commutative Noetherian ring and let R be a reduced commutative k-algebra that is finitely generated as a module. Then $\operatorname{Aut}_{k\text{-}\mathtt{Alg}}(R)$ is a finite group.*

Proof. Since R is reduced we have an injection $R \to \prod_{\mathfrak{p} \in \operatorname{minspec} R} R/\mathfrak{p}$ by Lemma 4.11 and thus an injection $\operatorname{Aut}_{k\text{-}\mathtt{Alg}}(R) \to \operatorname{wr}(\mathcal{C})$ with $\mathcal{C}$ constructed similarly as in Proposition 4.12. We have by Corollary 1.3 in [9] that R is a Noetherian ring and thus $\# \operatorname{minspec} R < \infty$ by Exercise 1.2 in [9], hence it suffices to show that $\operatorname{Aut}_{k\text{-}\mathtt{Alg}}(R/\mathfrak{p})$ is finite for all $\mathfrak{p} \in \operatorname{minspec} R$. As $R/\mathfrak{p}$ is a finitely generated k-algebra, we may then assume without loss of generality that R is a domain.

It suffices to show that each element $x \in R$ has a finite orbit under $\operatorname{Aut}_{k\text{-}\mathtt{Alg}}(R)$, because we may then apply this fact to the finite number of generators of R. Note that we may replace k by its image in R and thus assume that k is a domain. Because R is finitely generated, x is the root of some non-zero polynomial $f \in k[X]$. As $\operatorname{Aut}_{k\text{-}\mathtt{Alg}}(R)$ must permute the roots of this polynomial and f has only finitely many roots because R is a domain, we may conclude that the orbit of x is finite, as was to be shown. □

Lemma 6.20. *Let k be a commutative Noetherian ring and let M be a finitely generated k-module. There exists some constant $c \in \mathbb{Z}_{\geq 0}$ such that if $\mathcal{M}$ is a decomposition of M, then $\mathcal{M}$ contains at most c non-zero elements.*

Proof. Let $n \in \mathbb{Z}_{\geq 0}$ be such that M can be generated by n elements. First assume k is a local ring with maximal ideal $\mathfrak{m}$. If $N/\mathfrak{m}N = 0$ for some submodule $N \subseteq M$, then $N = 0$ by Nakayama's lemma. Hence if $\mathcal{M} = \{M_i\}_{i \in I}$ is a decomposition of M, then

$$n \geq \dim_{k/\mathfrak{m}\text{-}\mathtt{Vec}}(M/\mathfrak{m}M) = \sum_{i \in I} \dim_{k/\mathfrak{m}\text{-}\mathtt{Vec}}(M_i/\mathfrak{m}M_i)$$

implies $M_i/\mathfrak{m}M_i = 0$ and thus $M_i = 0$ for all but at most n elements $i \in I$.

Now consider the general case. Let $A = \operatorname{Ass}_k(M)$ be the set of associated primes of M, which is finite by Theorem 3.1 in [9] since M is finitely generated over a Noetherian ring. We have an injection $M \to \prod_{\mathfrak{p} \in A} M_{\mathfrak{p}}$ by Corollary 3.5.a in [9] and for any submodule $N \subseteq M$ we have $\operatorname{Ass}_k(N) \subseteq \operatorname{Ass}_k(M)$. Let $\mathcal{M} = \{M_i\}_{i \in I}$ be a decomposition of M. For each $\mathfrak{p} \in A$ we have a decomposition $\{M_{i,\mathfrak{p}}\}_{i \in I}$ of the $k_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ and thus $M_{i,\mathfrak{p}} = 0$ for all but at most n elements $i \in I$ as shown before. For each $i \in I$ such that $M_i \neq 0$ there must exist some $\mathfrak{p} \in A$ such that $M_{i,\mathfrak{p}} \neq 0$, hence there are at most $c := n \cdot \# A$ non-zero elements in $\mathcal{M}$. □

Theorem 6.21. *Let $e \in \mathbb{S}$, let k be a commutative Noetherian ring and let R be a reduced commutative k-algebra that is finitely generated as k-module, such that for each prime $p \mid e$ we have $\bigcap_{n \geq 0} p^n R = \{0\}$ and that multiplication by p is injective on R. Then R has a universal abelian e-torsion grading.*

Proof. By Lemma 6.20 there exists some $c \in \mathbb{Z}_{\geq 0}$ such that each grading of R has at most c non-zero homogenous components. Hence any efficient abelian group-grading of R has exponent dividing $c!$. By replacing e with $\gcd(e, c!)$ we may assume that $e \in \mathbb{Z}_{>0}$. Then $k' = k \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ is a Noetherian ring because $\mathbb{Z}[\mu_e]$ is a finitely generated $\mathbb{Z}$-algebra, and thus $R' = R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$ is a Noetherian ring because it is finitely generated over k'. Since $\mathbb{Z}[\mu_e]$ is a free $\mathbb{Z}$-module, we also have that $\bigcap_{n \geq 0} p^n R' = \{0\}$ and that multiplication by p is injective on R' for all primes $p \mid e$. Let $s \in \operatorname{End}_{k'\text{-}\mathtt{Mod}}(R')$ and assume $p(1 - ps)(x) = 0$ for some $x \in R'$ and prime $p \mid e$. Then $x = ps(x)$ by injectivity of p, so $x = p^n s^n(x)$ for all $n \in \mathbb{Z}_{\geq 0}$. Thus $x \in \bigcap_{n \geq 0} p^n R' = \{0\}$ so $x = 0$ and thus $p(1 - ps)$ is injective. It follows that $\operatorname{End}_{k'\text{-}\mathtt{Mod}}(R')$ is p-good for all primes $p \mid e$. By Lemma 6.18 have that R' is reduced and thus by Lemma 6.19 we have that $\operatorname{Aut}_{k'\text{-}\mathtt{Alg}}(R')$ is a finite group. In particular, all μ_e-diagonalizable elements of $\operatorname{Aut}_{k'\text{-}\mathtt{Alg}}(R')$ commute by Proposition 6.17. It follows that $X_e(R)$ as definined in Definition 3.22 is a finite abelian group. Hence by Theorem 3.35 there exists a universal abelian e-torsion grading of R, as was to be shown. □

Note that reduced orders satisfy the conditions to Theorem 6.21 for all $e \in \mathbb{S}$ and thus have a universal abelian-group grading. The condition that k be a Noetherian ring is rather strong, but Example 6.6 shows that theorem becomes false when we drop it.

7 Universal abelian group grading

In this section we present a proof of Theorem 1.3 and derive Theorem 1.4 for abelian groups.

7.1 Combinatorial algorithm

In this section we consider a finite groupoid $\mathcal{C}$ and a Steinitz number $e \in \mathbb{S}$ such that the group $(\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ acts on $\mathcal{C}$. Our goal is to study the following set, specifically its size and how to list its elements.

Definition 7.1. Let $\mathcal{C}$ be a finite groupoid, $e \in \mathbb{S}$ and $G \subseteq (\hat{\mathbb{Z}}/e\hat{\mathbb{Z}})^*$ a subgroup that has a left action on $\mathcal{C}$. Then G has an induced left-action on $\mathrm{wr}(\mathcal{C})$ by Remark 4.7 and a right action on the e-torsion of $\mathrm{wr}(\mathcal{C})$ by exponentiation. With respect to these actions we define

$$X_e(\mathcal{C}, G) = \{\sigma \in \mathrm{wr}(\mathcal{C}) \mid \sigma^e = 1,\ (\forall a \in G)\ {}^a\sigma = \sigma^a\}.$$

Beware that this notation hides the left action of G on $\mathcal{C}$, which will remain unchanged throughout this section.

In this section we will derive the following result.

Theorem 7.2. *There is a deterministic algorithm that takes a quadruple $(\mathcal{C}, e, G, *)$, where $\mathcal{C}$ is a finite groupoid encoded as in Section 4.4, where $e > 1$ is a prime power encoded in base 1, where $G \subseteq (\mathbb{Z}/e\mathbb{Z})^*$ is a subgroup and $*$ is an action of G on $\mathcal{C}$ which we encode by associating to each element of G a permutation on the morphisms of $\mathcal{C}$, and computes $X_e(\mathcal{C}, G)$ in $n^{O(m)}$ time, where n is the length of the input and $m = \#(\mathrm{obj}(\mathcal{C})/G)$. With $a = \#\,\mathrm{aut}(\mathcal{C})$ as defined in Definition A.2 and $c = 2 + \mathbb{1}(4 \mid e)$ we have the bound $\#X_e(\mathcal{C}, G) \leq (2ma^c)^m$.*

We will prove this using various reductions. First we reduce to the case where all objects of $\mathcal{C}$ are $(\mathcal{C} \rtimes G)$-isomorphic.

Lemma 7.3. *With the same setting as in Definition 7.1, consider the group $\mathrm{wr}(\mathcal{C}) \rtimes G$ and let $\mathcal{P}$ be the set of orbits of $\mathrm{wr}(\mathcal{C}) \rtimes G$ acting on $\mathrm{obj}(\mathcal{C})$. Then with $\mathcal{C}|_P$ the full subcategory of $\mathcal{C}$ with objects $P \subseteq \mathrm{obj}(\mathcal{C})$ we have*

$$X_e(\mathcal{C}, G) = \prod_{P \in \mathcal{P}} X_e(\mathcal{C}|_P, G). \tag{7.3.1}$$

Proof. All $P \in \mathcal{P}$ are G-invariant by definition, hence the action of G does in fact restrict to $\mathcal{C}|_P$, making the right hand side of (7.3.1) well-defined. It follows directly from the definition that the right hand side of (7.3.1) is contained in the left hand side. For the converse, it suffices to note that each element $\sigma \in X_e(\mathcal{C}, G)$ has orbits refining $\mathcal{P}$ and that the relations $\sigma^e = 1$ and ${}^a\sigma = \sigma^a$ also hold for the restrictions $\sigma|_P \in \mathrm{wr}(\mathcal{C}|_P)$ for $P \in \mathcal{P}$. Hence $\sigma|_P \in X_e(\mathcal{C}|_P, G)$ and $\sigma \in \prod_{P \in \mathcal{P}} X_e(\mathcal{C}|_P, G)$. □

We may thus assume the groups we consider are ‘sufficiently transitive’, i.e. $\mathrm{wr}(\mathcal{C}) \rtimes G$ acts transitively on $\mathrm{obj}(\mathcal{C})$. In the next reduction we will strengthen this property to the individual elements of $\mathrm{wr}(\mathcal{C})$. Namely, we note that for $\sigma \in X_e(\mathcal{C}, G)$ the group G acts on $\langle\sigma\rangle$ by exponentiation, hence we may define the following.

Definition 7.4. With the same setting as in Definition 7.1, define

$$X_e^!(\mathcal{C}, G) = \{\sigma \in X_e(\mathcal{C}, G) \mid \langle\sigma\rangle \rtimes G \text{ acts transitively on } \mathrm{obj}(\mathcal{C})\}.$$

For partitions $\mathcal{P}$ and $\mathcal{O}$ of a set Ω we write $\mathcal{P} \succeq \mathcal{O}$ if and only if $P \cap O \in \{\emptyset, O\}$ for all $O \in \mathcal{O}$ and $P \in \mathcal{P}$, i.e. when $\mathcal{O}$ refines $\mathcal{P}$.

Lemma 7.5. *Consider the same setting as in Definition 7.1. Assume $\mathrm{wr}(\mathcal{C}) \rtimes G$ acts transitively on $\mathrm{obj}(\mathcal{C})$ and let $\mathcal{O} = \mathrm{obj}(\mathcal{C})/G$. Then*

$$X_e(\mathcal{C}, G) = \bigsqcup_{\mathcal{P} \succeq \mathcal{O}} \prod_{P \in \mathcal{P}} X_e^!(\mathcal{C}|_P, G). \tag{7.5.1}$$

Proof. For all $P \in \mathcal{P} \succeq \mathcal{O}$ the set P is G-stable, hence the action of G restricts to $\mathcal{C}|_P$, making $X_e^!(\mathcal{C}|_P, G)$ well-defined. Write $X(\mathcal{P}) = \prod_{P\in\mathcal{P}} X_e^!(\mathcal{C}|_P, G) \subseteq \mathrm{wr}(\mathcal{C})$ for all partitions $\mathcal{P} \succeq \mathcal{O}$. For $\sigma \in X(\mathcal{P})$ one clearly has that the set of orbits of $\langle\sigma\rangle \rtimes G$ is precisely $\mathcal{P}$. Hence for distinct partitions $\mathcal{P}$ and $\mathcal{Q}$ one has that $X(\mathcal{P}) \cap X(\mathcal{Q}) = \emptyset$ and the union on the right side of (7.5.1) is indeed disjoint. It follows directly from the definition that $X(\mathcal{P}) \subseteq X_e(\mathcal{C}, G)$, so the right hand side of (7.5.1) is contained in the left. Conversely, for any $\sigma \in X_e(\mathcal{C}, G)$ the partition $\mathcal{P} = \mathrm{obj}(\mathcal{C})/(\langle\sigma\rangle \rtimes G)$ must have $\mathcal{O}$ as refinement. As for all $P \in \mathcal{P}$ the group $\langle\sigma|_P\rangle \rtimes G$ acts transitively on P, we have that $\sigma|_P \in X_e^!(\mathcal{C}|_P, G)$ and $\sigma \in X(\mathcal{P})$, so the reverse inclusion also holds. □

A final reduction step will restrict to the case where $\langle\sigma\rangle$ itself is transitive. Here we will use that G is abelian.

Definition 7.6. With the same setting as in Definition 7.1, define

$$X_e^{!!}(\mathcal{C}, G) = \{\sigma \in X_e(\mathcal{C}, G) \mid \langle\sigma\rangle \text{ acts transitively on } \mathrm{obj}(\mathcal{C})\}.$$

We will now show for $\sigma \in X_e(\mathcal{C}, G)$ that the restriction of σ to a single orbit of $\langle\sigma\rangle$ defines it in its entirety.

Proposition 7.7. *Consider the same setting as in Definition 7.1. Let $\mathcal{O} = \mathrm{obj}(\mathcal{C})/G$, let $I_O \trianglelefteq G$ be the pointwise stabiliser of $O \in \mathcal{O}$ and let $I = \langle I_O \mid O \in \mathcal{O}\rangle$. Write $\mathcal{H} = \{H \mid I \trianglelefteq H \trianglelefteq G\}$ and fix some $x \in \mathrm{obj}(\mathcal{C})$. For any $H \in \mathcal{H}$ let*

$$\mathcal{P}(H) = \{P \subseteq \mathrm{obj}(\mathcal{C}) \mid x \in P,\ (\forall O \in \mathcal{O})\, P \cap O \in \mathrm{obj}(\mathcal{C})/H\}.$$

Then for all $\sigma \in X_e^!(\mathcal{C}, G)$ we have that $P = \langle\sigma\rangle x \in \mathcal{P}(H_P)$, where $H_P \trianglerighteq I$ is the setwise stabiliser of P. Moreover, the map

$$\begin{aligned} \varphi : X_e^!(\mathcal{C}, G) &\to \bigsqcup_{H\in\mathcal{H}} \bigsqcup_{P\in\mathcal{P}(H)} X_e^{!!}(\mathcal{C}|_P, H) \\ \sigma &\mapsto \sigma|_{\langle\sigma\rangle x} \in X_e^{!!}(\mathcal{C}|_{\langle\sigma\rangle x}, H_{\langle\sigma\rangle x}) \end{aligned}$$

is well-defined and bijective.

Proof. We break up the proof into several parts.

Well-definedness: Let $\sigma \in X_e^!(\mathcal{C}, G)$ be given, let $P = \langle\sigma\rangle x$ be the orbit of x under σ and let $H \trianglelefteq G$ be the setwise stabilizer of P. Note that H acts on P and thus $X_e^{!!}(\mathcal{C}|_P, H)$ is well-defined and $\sigma|_P \in X_e^{!!}(\mathcal{C}|_P, H)$. First we show that $H \in \mathcal{H}$ and $P \in \mathcal{P}(H)$, from which it follows that $\sigma|_P$ is in fact an element of the codomain of φ. Since G normalizes $\langle\sigma\rangle$ it permutes the orbits of σ. As $P \cap O \neq \emptyset$ for all $O \in \mathcal{O}$ by definition of $X_e^!(\mathcal{C}, G)$, we have that since I_O stabilises a point $y \in P \cap O$, it must stabilise the entire orbit P setwise. Hence $I_O \trianglelefteq H$ for all $O \in \mathcal{O}$, so $H \in \mathcal{H}$. Let $O \in \mathcal{O}$ be given. Note that $HP = P$ by definition and $HO = O$ as $H \subseteq G$, and thus $H(P \cap O) = P \cap O$. Furthermore, for all $y, z \in P \cap O$ there exists some $t \in G$ such that $ty = z$ by transitivity. By the same argument as before we have $tP = P$, and thus $t \in H$ and $Hy = Hz$. Thus $P \cap O$ is an orbit of H acting on $\mathrm{obj}(\mathcal{C})$ for all $O \in \mathcal{O}$, so $P \in \mathcal{P}(H)$.

For the well-definedness of φ it remains to show that the union defining the codomain of φ is indeed disjoint. If $P, P' \subseteq \mathrm{obj}(\mathcal{C})$ are distinct, then clearly $X_e^{!!}(\mathcal{C}|_P, H) \cap X_e^{!!}(\mathcal{C}|_{P'}, H') = \emptyset$ for any $H, H' \trianglelefteq G$ for which this is defined. Thus we need to show that for distinct $H, H' \in \mathcal{H}$ we have $\mathcal{P}(H) \cap \mathcal{P}(H') = \emptyset$. We have $I_O \trianglelefteq H, H'$ for $O = Gx \in \mathcal{O}$, so $H/I_O \neq H'/I_O$. As G/I_O acts regularly on O, we have that $(H/I_O)x \neq (H'/I_O)x$, hence for any $P \in \mathcal{P}(H)$ and $P' \in \mathcal{P}(H')$ we have $P \cap O = Hx \neq H'x = P' \cap O$. So $P \neq P'$, from which the claim follows. We conclude that φ is well-defined.

Injectivity: Let $\sigma \in X_e^!(\mathcal{C}, G)$ and $\omega = \varphi(\sigma) \in X_e^{!!}(\mathcal{C}|_P, H)$ for $P = \langle\sigma\rangle x$ and $H = H_P$. For all $y \in \mathrm{obj}(\mathcal{C})$ there exists some $z \in P$ and $\tau = \tau_a \in G$ such that $ty = z$. We use the convention of Section 4.1 that $\sigma = ((\sigma_y)_{y\in\mathrm{obj}(\mathcal{C})}, s)$ and similarly for τ and ω is implicit. We have

$$s(y) = st^{-1}(z) = t^{-1}s^a(z) = t^{-1}o^a(z) \quad \text{and} \tag{7.7.1}$$

$$\sigma_y = (\tau^{-1}\sigma^a\tau)_y = (\tau_{s(y)})^{-1} \circ (\omega^a)_z \circ \tau_y. \tag{7.7.2}$$

Hence σ is uniquely determined by $\varphi(\sigma)$ and φ is injective.

Note that equations (7.7.1) and (7.7.2) in fact give us a way to construct, for any $\omega \in X_e^{!!}(\mathcal{C}|_P, H)$, an element $\sigma \in \mathrm{wr}(\mathcal{C})$. This construction a priori depends on the choice of τ and z. If we choose for each class $gH \in G/H$ a representative τ_{gH} and require that τ in (7.7.1) and (7.7.2) be taken in $R = \{\tau_{gH} \,|\, gH \in G/H\}$, then for each $y \in \mathrm{obj}(\mathcal{C})$ both τ and z exist and are unique. Now we obtain a map $\psi_{H,P} : X_e^{!!}(\mathcal{C}|_P, H_P) \to \mathrm{wr}(\mathcal{C})$, and a combined map $\psi : \bigsqcup_{H\in\mathcal{H}} \bigsqcup_{P\in\mathcal{P}(H)} X_e^{!!}(\mathcal{C}|_P, H_P) \to \mathrm{wr}(\mathcal{C})$ which is a left inverse of φ.

Surjectivity: For surjectivity of φ, it remains to show that ψ is also a right inverse of φ. This is, however, clearly the case when $\mathrm{im}(\psi) \subseteq X_e^{!}(\mathcal{C}, G)$. Let $H \in \mathcal{H}$, $P \in \mathcal{P}(H)$ and $\omega \in X_e^{!!}(\mathcal{C}|_P, H)$. By definition, $\sigma := \psi(\omega)$ has P as an orbit. For all $y \in \mathrm{obj}(\mathcal{C})$ with corresponding τ_a and z we have

$$\begin{aligned} &s^e(y) = t^{-1}o^{ae}(z) = t^{-1}z = y \quad \text{and} \\ &(\sigma^e)_y = \tau_{t^{-1}s(y)} \circ (\omega^{ae})_z \circ (\tau^{-1})_y = \tau_{t^{-1}(y)} \circ (\tau^{-1})_y = \mathrm{id}_y, \end{aligned}$$

so $\sigma^e = 1$. Now let additionally $\tau_b \in G$ be given. Then there exists some $\tau_c \in R$ and $\tau_d \in H$ such that $\tau_b\tau_a^{-1} = \tau_c\tau_d$. Hence

$$\begin{aligned} &t_b s(y) = t_b t_a^{-1} o^a(z) = t_c t_d o^a(z) = t_c o^{ad} t_d(z) = s^{adc} t_c t_d(z) = s^b t_b(y) \quad \text{and} \\ &(\tau_b\sigma)_y = (\tau_b\tau_a\omega^a\tau_a^{-1})_y = (\tau_c\tau_d\omega^a\tau_a^{-1})_y = (\tau_c\omega^{ad}\tau_d\tau_a^{-1})_y = (\sigma^{adc})_{t_d(y)} \circ (\tau_d)_y = (\sigma^b\tau_d)_y. \end{aligned}$$

Thus $\sigma \in X_e^{!}(\mathcal{C}, G)$, as was to be shown. Therefore ψ is a right inverse of φ. It follows that φ is surjective. □

Lemma 7.8. *Consider the same setting as in Definition 7.1, let $a = \#\,\mathrm{aut}(\mathcal{C})$ as defined in Definition A.2 and let m be the number of orbits of G acting on* $\mathrm{obj}(\mathcal{C})$*. If G is cyclic, then $\#X_e^{!!}(\mathcal{C}, G) \leq a^{m+1}$. In this case, we may compute $X_e^{!!}(\mathcal{C}, G)$ in $n^{O(m)}$ time with n the length of the input $(\mathcal{C}, e, G, *)$, where $e \in \mathbb{Z}_{>0}$ and $*$ is the action of G on $\mathcal{C}$.*

Proof. Write $G = \langle b \rangle$ and take any $x \in \mathrm{obj}(\mathcal{C})$. Consider $\sim_{\mathcal{C}}$ as in Definition 4.16 and λ as in Definition 4.17. Let

$$S = \{\sigma \in \mathrm{wr}(\mathcal{C}) \,|\, \sigma \text{ acts transitively on } \mathrm{obj}(\mathcal{C}),\ \sigma^e = 1 \text{ and } {}^b\lambda_\sigma(x) \sim_{\mathcal{C}} \lambda_\sigma(x)^b\}$$

and note that it is closed under conjugation. Moreover, we have that $X_e^{!!}(\mathcal{C}, G) \subseteq S$. Let Φ be the set of $\mathrm{wr}(\mathcal{C})$-conjugacy classes of S, which corresponds to some subset of the set of conjugacy classes of $\mathrm{Aut}_{\mathcal{C}}(x)$ by Theorem 4.21. Fix some representative $\sigma_\varphi \in \varphi$ for each $\varphi \in \Phi$. Let $\Gamma = \mathrm{wr}(\mathcal{C}) \rtimes G$, let τ_b be the image of b in Γ and let $U_\varphi = \{\upsilon \in \mathrm{wr}(\mathcal{C}) \circ \tau_b \subseteq \Gamma \,|\, \upsilon\sigma_\varphi\upsilon^{-1} = \sigma_\varphi^b\}$. If $\upsilon_\varphi \in U_\varphi$, then all permutations $\alpha \in \mathrm{wr}(\mathcal{C})$ such that $\alpha\upsilon_\varphi\alpha^{-1} = \tau_b$ give rise to an element $\alpha\sigma_\varphi\alpha^{-1} \in X_e^{!!}(\mathcal{C}, G)$, and we claim that we obtain all elements of $X_e^{!!}(\mathcal{C}, G)$ in this way. Each $\sigma \in X_e^{!!}(\mathcal{C}, G)$ is conjugate to some σ_φ, so there exists some $\alpha \in \mathrm{wr}(\mathcal{C})$ such that $\alpha\sigma_\varphi\alpha^{-1} = \sigma$, while $\alpha^{-1}\tau_b\alpha = \alpha^{-1}({}^b\alpha)\tau_b \in U_\varphi$. Hence these are in fact all elements of $X_e^{!!}(\mathcal{C}, G)$.

It remains to count these elements. Given φ, we have that

$$U_\varphi = \{\beta \in \mathrm{wr}(\mathcal{C}) \,|\, \beta({}^b\sigma_\varphi)\beta^{-1} = \sigma_\varphi^b\} \circ \tau_b.$$

We may compute U_φ using Theorem 4.21 in time $n^{O(m)}$ and it contains $\#\,\mathrm{obj}(\mathcal{C}) \cdot \#C(\lambda_{\sigma_\varphi}(x))$ elements. Furthermore $\sum_{\varphi\in\Phi} \#C(\lambda_{\sigma_\varphi}(x)) \leq \#\,\mathrm{Aut}_{\mathcal{C}}(x)$, so $\sum_{\varphi\in\Phi} \#U_\varphi \leq \#\,\mathrm{obj}(\mathcal{C}) \cdot \#\,\mathrm{Aut}_{\mathcal{C}}(x) = a$. Let then $V(\upsilon) = \{\alpha \in \mathrm{wr}(\mathcal{C}) \,|\, \alpha\upsilon\alpha^{-1} = \tau_b\}$, which for any $\upsilon \in \Gamma$ may be computed using Corollary 4.23 in time $n^{O(m)}$ and contains at most a^m elements. Hence, counting the number of elements we get

$$\#X_e^{!!}(\mathcal{C}, G) \leq \sum_{\varphi\in\Phi} \sum_{\upsilon\in U_\varphi} \#V(\upsilon) \leq a^m \cdot \sum_{\varphi\in\Phi} \#U_\varphi \leq a^{m+1},$$

as was to be shown. □

Proof of Theorem 7.2.
Write $e = p^k$ for some prime p and let $d = 1 + \mathbb{1}(4 \,|\, e)$. By Lemma 5.2 the group $G \subseteq (\mathbb{Z}/p^k\mathbb{Z})^*$ has a cyclic subgroup $G' \trianglelefteq G$ such that $[G : G'] \leq d$. Note that $X_e^{!!}(\mathcal{C}, G) \subseteq X_e^{!!}(\mathcal{C}, G')$ and $\#\operatorname{obj}(\mathcal{C})/G' \leq dm$. Then by Lemma 7.8 we have

$$\#X_e^{!!}(\mathcal{C}, G) \leq \#X_e^{!!}(\mathcal{C}, G') \leq a^{dm+1}. \tag{7.2.1}$$

We combine (7.2.1) with Proposition 7.7. For $H \in \mathcal{H}$ we have $\#\mathcal{P}(H) = [G : H]^{m-1}$ and assuming all objects of $\mathcal{C}$ are $\mathcal{C} \rtimes G$-isomorphic we get $\#\operatorname{aut}(\mathcal{C}|_P) = a/[G : H]$ for all $P \in \mathcal{P}(H)$. Thus

$$\#X_e^{!}(\mathcal{C}, G) \leq \sum_{H \in \mathcal{H}} \sum_{P \in \mathcal{P}(H)} \left(\frac{a}{[G : H]} \right)^{dm+1} = a^{dm+1} \sum_{H \in \mathcal{H}} [G : H]^{-2-(d-1)m} \leq 2a^{dm+1}. \tag{7.2.2}$$

In the last inequality we use $S = \sum_{H \trianglelefteq G} [G : H]^{-2} \leq 2$. Namely, if $p > 2$ then G is cyclic and H is uniquely determined by its size, so we have $S \leq \sum_{i=1}^{\infty} i^{-2} = \pi^2/6 \leq 2$. If $p = 2$, then for each index greater than 1 there are at most 3 subgroups of G of this index, so $S \leq 1 + 3\sum_{i=1}^{\infty} 2^{-2i} = 2$.

Still assuming all objects of $\mathcal{C}$ are $\mathcal{C} \rtimes G$-isomorphic we combine (7.2.2) with Lemma 7.5. Then we get for fixed $\mathcal{P} \succeq \operatorname{obj}(C)/G$ that

$$\# \prod_{P \in \mathcal{P}} X_e^{!}(\mathcal{C}|_P, G) \leq \prod_{P \in \mathcal{P}} 2(\#\operatorname{aut}(\mathcal{C}|_P))^{d \cdot \#(P/G)+1} \leq 2^m a^{\sum_{P \in \mathcal{P}} (d\#(P/G)+1)} = (2a^c)^m.$$

There are at most m^m such $\mathcal{P} \succeq \operatorname{obj}(\mathcal{C})/G$, hence

$$\#X_e(\mathcal{C}, G) \leq \sum_{\mathcal{P} \succeq \operatorname{obj}(\mathcal{C})/G} (2a^c)^m \leq (2ma^c)^m. \tag{7.2.3}$$

If we drop the assumption that all objects of $\mathcal{C}$ are $\mathcal{C} \rtimes G$-isomorphic we obtain the same inequality by applying Lemma 7.3.

What remains is to show we can compute $X_e(\mathcal{C}, G)$ in $n^{O(m)}$ time. The counting argument we used simply consists of chaining together various explicit bijections from the lemmata in this section. The reader should verifiy that for any such bijection φ computing $\varphi(\sigma)$ takes $n^{O(m)}$ time. This is trivial for all steps except possibly Proposition 7.7, where we have to note it is easy to solve the equations (7.7.1) and (7.7.2). Hence we get a $(2ma^c)^m \cdot n^{O(m)} \subseteq n^{O(m)}$ time algorithm, since both m and a are bounded by n. □

7.2 Computing cyclic gradings of reduced rational algebras

Using Theorem 7.2 we can finally prove Theorem 1.3.

Remark 7.9. Given two number fields K and L represented by structure constants we may compute $\alpha \in K$ and $\beta \in L$ together with minimal polynomials $f_\alpha, f_\beta \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$, for example using Theorem 1.7 from [12]. Then $K \cong L$ precisely when f_α and f_β have the same degree and f_α has a linear factor over L. Moreover, an isomorphism $\varphi : K \to L$ is uniquely determined by the image of α, which must be a root of f_α in L. Hence we may use Theorem 4.5 of [13] to compute the isomorphisms between two number fields in polynomial time with respect to the length of the input.

Algorithm 7.10. Let E be an n-dimensional reduced $\mathbb{Q}$-algebra, let p be prime and let $k \geq 0$.

1. Let replace k by $\min\{k, \lfloor \log_p n \rfloor\}$. If $k = 0$ simply output the trivial grading of E and terminate. Compute $E' = E \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_{p^k})$ as in Section 3.5. Using Algorithm 7.2 in [12], we compute $\operatorname{spec} E'$, $E'/\mathfrak{m}$ for $\mathfrak{m} \in \operatorname{spec} E'$ and the isomorphism $\varphi : E' \to \prod_{\mathfrak{m} \in \operatorname{spec} E'} E'/\mathfrak{m}$.
2. For each pair $\mathfrak{m}, \mathfrak{n} \in \operatorname{spec} E'$ compute $\operatorname{Iso}_{\mathbb{Q}(\mu_{p^k})\texttt{-Alg}}(E'/\mathfrak{m}, E'/\mathfrak{n})$ using Remark 7.9, such that we can construct the concrete category $\mathcal{C}$ with $\operatorname{obj}(\mathcal{C}) = \operatorname{spec} E'$ and $\operatorname{Hom}_{\mathcal{C}}(\mathfrak{m}, \mathfrak{n}) = \operatorname{Iso}_{\mathbb{Q}(\mu_{p^k})\texttt{-Alg}}(E'/\mathfrak{m}, E'/\mathfrak{n})$ as in Section 4.4. Let $G = (\mathbb{Z}/p^k\mathbb{Z})^*$ and compute its left action on $\mathcal{C}$ via $G \to \operatorname{Aut}(\mathbb{Q}(\mu_{p^k})) \to \operatorname{Aut}(E')$ as in Corollary 3.12.

3. Using Theorem 7.2 compute $X_{p^k}(\mathcal{C}, G)$.
4. For each $\sigma \in X_{p^k}(\mathcal{C}, G)$ compute the corresponding $f_\sigma \in \operatorname{Aut}(E')$ as in Proposition 4.12 using φ. Then compute the grading $\overline{E}_\sigma$ corresponding to f_σ by Theorem 3.25 using Proposition 3.36 and output $\overline{E}_\sigma$.

Proof of Theorem 1.3. We need to show the correctness of Algorithm 7.10 and that its runtime is in $n^{O(m)}$. By Proposition 2.6, an efficient grading with a cyclic group of prime power order must have a group of size at most $\dim_{\mathbb{Q}}(E) = n$. Hence we may replace k by $k = \min\{k, \lfloor \log_p n \rfloor\}$ in step (1). By the correctness of the various algorithms we use up to step (3), we correctly compute $X_{p^k}(\mathcal{C}, G)$. By definition of $X_{p^k}(\mathcal{C}, G)$ each $\sigma \in X_{p^k}(\mathcal{C}, G)$ corresponds to an element $f_\sigma \in \operatorname{Aut}(E')$ which is also an element of $X_{p^k}(E)$ as defined in Definition 3.22. Then by Theorem 3.25 each such f_σ encodes a μ_{p^k}-grading we obtain by computing the eigenspaces, which we all output. Hence the algorithm is correct.

Step (1) takes time polynomial in n by Theorem 1.10 in [12]. For each pair $\mathfrak{m}, \mathfrak{n} \in \operatorname{spec} A$ computation of $\operatorname{Iso}(A/\mathfrak{m}, A/\mathfrak{n})$ is polynomial in n as well by Remark 7.9, and thus so is step (2). In step (3) computation of $X_{p^k}(\mathcal{C}, G)$ takes $n^{O(m)}$ time by Theorem 7.2. For each σ we require only $n^{O(1)}$ time in step (4), meaning that Algorithm 7.10 terminates in $n^{O(m)}$ time. □

7.3 Computing universal abelian group gradings of reduced orders

Let R be a reduced order and write $E = R \otimes_{\mathbb{Z}} \mathbb{Q}$. We have a natural inclusion $R \to E$ which for any $e \in \mathbb{S}$ induces an injection $X_e(R) \to X_e(E)$, where X_e is as in Definition 3.22. Moreover, E is a reduced $\mathbb{Q}$-algebra with $\#\operatorname{spec} E = \#\operatorname{minspec} E = \#\operatorname{minspec} R$ and $\#\operatorname{spec} E' = \#\operatorname{minspec} R'$ with $E' = E \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_e)$ and $R' = R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$. With a slight modification to Algorithm 7.10 we can compute the cyclic gradings of R.

Algorithm 7.11. Let R be a reduced order of rank r.

1. Let $\mathcal{P} = \{p^{\lfloor \log_p r \rfloor} \mid p \text{ prime}, p \leq r\}$. Let $E = R \otimes_{\mathbb{Z}} \mathbb{Q}$ be the reduced $\mathbb{Q}$-algebra with the same structure constants as R.
2. For each $q \in \mathcal{P}$ compute $X_q(E)$ using Algorithm 7.10 and then compute $X_q(R)$ as the subset of $X_q(E)$ of morphisms for which the corresponding matrices have integer coefficients. Let $S = \bigcup_{q \in \mathcal{P}} X_q(R)$.
3. Using Proposition 3.36 compute the set Z of all $z = \{\zeta_s\}_{s \in S} \in \mu_\infty^S$ such that $U_z = \bigcap_{s \in S} R(s, \zeta_s) \neq 0$ and for each $z \in Z$ compute U_z.
4. Compute the group $\Upsilon = \langle Z \rangle$ and return $\overline{U} = (R, \Upsilon, \{U_v\}_{v \in \Upsilon})$.

Proof of Theorem 1.4: We show that Algorithm 7.11 correctly computes a universal abelian group-grading of R in time $n^{O(m)}$, where n is the length of the input R and $m = \#\operatorname{minspec} R = \#\operatorname{spec} E$. The inclusion $R \to E$ induces an inclusion $X_q(R) \to X_q(E)$ when we interpret $X_q(R)$ as the automorphisms of $X_q(E)$ that restrict to an automorphism of $R' = R \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_e]$. These are precisely the matrices with integer coefficients, since R and E have the same structure constants. By Theorem 1.8 the reduced order R has a universal abelian group grading and by Remark 2.13 all joint gradings of gradings of R exist. Thus $\overline{U}$ is in fact a grading of R. Moreover, its computation can be done in time $n^{O(m)}$ by Theorem 1.3 and Proposition 3.36. It remains to show that $\overline{U}$ is in fact the universal abelian group-grading of R.

By Theorem 3.34 each efficient grading $\overline{R} = (R, \Gamma, \{R_\gamma\}_{\gamma \in \Gamma})$ can be written as the joint grading of some gradings with cyclic groups of prime power order using the structure theorem for finite abelian groups applied to Γ. For each efficient abelian group grading the group Γ has exponent at most r, so it has exponent dividing $e = \prod_{q \in \mathcal{P}} q$. Hence all cyclic gradings of prime power order that can occur are the gradings associated to the elements of S. Thus there exists a map $f : \Upsilon \to \Gamma$ such that $f_* \overline{U} = \overline{R}$. Since $\overline{U}$ is efficient by construction, this f is unique and $\overline{U}$ is universal by Proposition 2.4. Hence the algorithm is correct. □

8 Universal grid grading

In this section we present an algorithm to compute the universal grid grading of a reduced order.

8.1 Restricting decompositions of finitely generated abelian groups

Definition 8.1. Let k be a ring, let $B \subseteq A$ be k-modules and let $\mathcal{A} = \{A_i\}_{i \in I}$ be a decomposition of A. We say $\mathcal{A}$ *restricts* to B if $\mathcal{B} = \{A_i \cap B\}_{i \in I}$ is a decomposition of B, and we call $\mathcal{B}$ the restriction of $\mathcal{A}$ to B.

In this section we will write $S/T = \{T\} \cup \{\{s\} \mid s \in S \setminus T\}$ for sets $T \subseteq S$, which comes with a natural map $S \to S/T$ for which the set of fibres is precisely S/T.

Proposition 8.2. *Let k be a ring, let $B \subseteq A$ be k-modules and let $\mathcal{A} = \{A_i\}_{i \in I}$ be a decomposition of A with I finite. Then there exists a map $u : I \to U$ for some set U that such that $u_*\mathcal{A}$ restricts to B and such that it is universal with respect to this property, i.e. each map $f : I \to J$ such that $f_*\mathcal{A}$ restricts to B factors uniquely through u.*

Proof. We apply induction to $n = \#I$. If $n = 0$ we clearly have $u = \mathrm{id}_\emptyset$ as universal map.

Now assume that $n > 0$ and that universal maps exist for all decompositions of A with less than n components. For $b \in B$ we may uniquely write $b = \sum_{i \in I} a_i$ with $a_i \in A_i$ and we define the support $\mathrm{supp}_{\mathcal{A}}(b) = \{i \in I \mid a_i \notin B\}$ and weight $w_{\mathcal{A}}(b) = \# \mathrm{supp}_{\mathcal{A}}(b)$ of b. If $\mathcal{A}$ restricts to B, or equivalently each element of B has zero weight, we take $u = \mathrm{id}_I$ and are done. Otherwise, there exists some $b \in B$ with $2 \leq w_{\mathcal{A}}(b)$, because having $w_{\mathcal{A}}(b) = 1$ is clearly impossible. We may choose $b \in B$ such that $\mathrm{supp}_{\mathcal{A}}(c) \subsetneq \mathrm{supp}_{\mathcal{A}}(b)$ for some $c \in B$ implies $w_{\mathcal{A}}(c) = 0$. Consider $J = I/\mathrm{supp}_{\mathcal{A}}(b)$ together with the natural map $q : I \to J$ and let $\mathcal{A}' = q_*\mathcal{A}$. By the induction hypothesis there exists a universal map $v : J \to U$ such that $v_*\mathcal{A}'$ restricts to B and we claim that $u = v \circ q$ is a universal map for $\mathcal{A}$. Let $f : I \to K$ be such that $f_*\mathcal{A}$ restricts to B. To show that f factors uniquely through u it suffices to show it factors uniquely through q by universality of v, which is precisely the case when $\#f(\mathrm{supp}_{\mathcal{A}}(b)) = 1$. Since $f_*\mathcal{A} = \mathcal{C} = \{C_k\}_{k \in K}$ restricts to B we may uniquely write $b = \sum_{k \in K} c_k$ with $c_k \in B \cap C_k$. We may also uniquely write $b = \sum_{i \in I} a_i$ with $a_i \in A_i$ and note that $c_k = \sum_{i \in f^{-1}k} a_i$. Hence $\{i\} \subseteq \mathrm{supp}_{\mathcal{A}}(c_{f(i)}) \subseteq \mathrm{supp}_{\mathcal{A}}(b)$ for all $i \in \mathrm{supp}_{\mathcal{A}}(b)$, so $\mathrm{supp}_{\mathcal{A}}(c_{f(i)}) = \mathrm{supp}_{\mathcal{A}}(b)$ by choice of b. As all $c_{f(i)}$ have the same non-empty support they must be equal and thus $f(i) = f(j)$ for all $i, j \in \mathrm{supp}_{\mathcal{A}}(b)$, as was to be shown. □

We now set out to turn Proposition 8.2 into an algorithm. Note that by the structure theorem of finitely generated groups, we may represent a finitely generated abelian group A by a matrix $M_A \in \mathbb{Z}^{n \times n}$ for some $n \in \mathbb{Z}_{\geq 0}$ such that $A \cong \mathbb{Z}^n / M_A \mathbb{Z}^n$, which we call a *matrix representation* of A. A subgroup B of A is represented by a *generator matrix* $G_B \in \mathbb{Z}^{n \times k}$ for some $k \in \mathbb{Z}_{\geq 0}$ such that $B = G_B \mathbb{Z}^k / M_A \mathbb{Z}^n$. We will prove the following theorem.

Theorem 8.3. *There is a deterministic algorithm that takes a quadruple $(n, A, \mathcal{A}, B)$ with $n \in \mathbb{Z}_{\geq 0}$, with A a finitely generated group given in matrix representation M_A, with $\mathcal{A} = \{A_i\}_{i \in I}$ a decomposition of A with each A_i given by a generator matrix G_i and with B a subgroup of A given by a generator matrix G_B, and computes a universal map $u : I \to U$ such that $f_*\mathcal{A}$ lifts to B in polynomial time with respect to the input.*

Lemma 8.4. *For matrices $A \in \mathbb{Z}^{n \times a}$ and $B \in \mathbb{Z}^{n \times b}$ for $a, b, n \in \mathbb{Z}_{\geq 0}$ we may compute a basis for $A\mathbb{Z}^a + B\mathbb{Z}^b$ and $A\mathbb{Z}^a \cap B\mathbb{Z}^b$ and we can verify whether $A\mathbb{Z}^a \subseteq B\mathbb{Z}^b$, in polynomial time with respect to the length of the input (A, B).*

Proof. We may compute the image and kernel of integer matrices in polynomial time using using the image and kernel algorithm from [7] and compute determinants using Theorem 6.6 from [8]. Then a basis for $A\mathbb{Z}^a + B\mathbb{Z}^b$ can be computed as a basis for the image of the matrix $(A|B)$. We may compute a basis matrix $K \in \mathbb{Z}^{(a+b) \times k}$ of the kernel of $(A|B)$ for some $k \in \mathbb{Z}_{\geq 0}$. A basis for $A\mathbb{Z}^a \cap B\mathbb{Z}^b$ we then obtain as a basis for the image of $(A|0_{n \times b}) \cdot K$, where $0_{n \times b} \in \mathbb{Z}^{n \times b}$ is the all-zero matrix. We may replace A by a basis for the image of A such that A becomes injective. For the inclusion $A\mathbb{Z}^a \subseteq B\mathbb{Z}^b$ we compute a basis matrix M for the image of $(\mathbb{I}_a|0_{a \times b}) \cdot K$. We have that $A\mathbb{Z}^a \subseteq B\mathbb{Z}^b$ precisely when M is invertible, which we may check by computing its determinant. □

Algorithm 8.5. Let $n \in \mathbb{Z}_{\geq 0}$, let $M_A \in \mathbb{Z}^{n \times n}$, let $\mathcal{A} = \{A_i\}_{i \in I}$ a sequence of matrices with $A_i \in \mathbb{Z}^{n \times k_i}$ for some $k_i \in \mathbb{Z}_{\geq 0}$ and let $G_B \in \mathbb{Z}^{n \times m}$ for some $m \in \mathbb{Z}_{\geq 0}$.

1. Let $J = I$ and replace G_B by a basis matrix for $G_B\mathbb{Z}^m + M_A\mathbb{Z}^n$.
2. For $S \subseteq J$ write A_S for the matrix with as columns the columns of the matrices A_j for $j \in S$ and let $k_S = \sum_{j \in S} k_j$. Let $S = J$.
3. For each $i \in J$, let $T = S \setminus \{i\}$ and if $G_B\mathbb{Z}^m \cap \sum_{j \in T} A_j\mathbb{Z}^{k_j} \not\subseteq \sum_{j \in T}(G_B\mathbb{Z}^m \cap A_j\mathbb{Z}^{k_j})$ then update $S = T$.
4. If $S = J$, return the natural map $I \to J$ and terminate. Otherwise update $J = J/S$ and $\mathcal{A} = \{A_j\}_{j \in J}$ and go to step 2.

Proof of Theorem 8.3: We show that Algorithm 8.5 satisfies the requirements. Correctness follows from the proof of Proposition 8.2, where we note that in step 4 of the algorithm S is an non-empty set that is minimal with respect to inclusion for which there exists an element of B with support S. With regards to runtime, the only non-trivial step in the algorithm is step 3, which can be executed in polynomial time by Lemma 8.4. Then, since the size of J strictly decreases in step 4 we enter this step at most $\#I$ times. Thus the algorithm runs in polynomial time. □

8.2 Restricting gradings of orders

Definition 8.6. Let k be a commutative ring, let R be a k-algebra and let $S \subseteq R$ be a subalgebra. We say a grading $\overline{R} = (R, G, \mathcal{R})$ *restricts* to S when $\mathcal{R}$ restricts to S and hence $\overline{S} = (S, G, \mathcal{S})$ is a grading, where $\mathcal{S}$ is the restriction of $\mathcal{R}$ to S. We then call $\overline{S}$ the restriction of $\overline{R}$ to S.

Lemma 8.7. *Let k be a commutative ring, let R be a k-algebra and let $S \subseteq R$ be a subalgebra. For each loose grid-grading $\overline{R} = (R, G, \mathcal{R})$ there exists a universal morphism of grids $u : G \to H$ such that $u_*\overline{R}$ restricts to S.*

Proof. Let $u_1 : G \to I$ be the universal map such that $u_{1*}\mathcal{R}$ restricts to S, which exists by Proposition 8.2. Consider the functor $F : \texttt{Grd} \to \texttt{Set}$ that sends Γ to the set of Γ-gradings of R of which $u_{1*}\mathcal{R}$ is a refinement. By Proposition 6.8 there then exists a universal grid H and map $u_2 : I \to H$ such that $\overline{U} = u_{2*}u_{1*}\overline{R}$ is a grid grading. Note that $\overline{U}$ restricts to S by construction, and since $\overline{R}$ is loose we have that $u = u_2 \circ u_1$ is a morphism of grids. It follows from universality that u satisfies the additional requirements. □

Proposition 8.8. *There is an algorithm that takes a pair $(R, \overline{E})$, where R is a reduced order represented by structure constants and $\overline{E}$ is a loose grid-grading of $E = R \otimes_{\mathbb{Z}} \mathbb{Q}$, the $\mathbb{Q}$-algebra with the same structure constants as R, and which computes both a universal morphism of grids u such that $u_*\overline{E}$ restricts to R and the restriction of $u_*\overline{R}$ to R, in polynomial time with respect to the length of the input.*

Proof. Let n be the rank of R and write $\overline{E} = (E, G, \{E_g\}_{g \in G})$. Compute integer bases for $S_g = E_g \cap \mathbb{Z}^n$ and let $S = \sum_{g \in G} S_g$. Then the determinant d of the basis matrix of S satisfies $d\mathbb{Z}^n \subseteq S$. Applying a change of basis to the basis matrix of dR we may assume that $S = \mathbb{Z}^n$. Now apply Theorem 8.3 to the decomposition $\mathcal{S} = \{S_g\}_{g \in G}$ of the finitely generated abelian group $\mathbb{Z}^n$ and the subgroup R. This gives a universal map $u_1 : G \to I$ such that $\{E_g\}_{g \in G}$ restricts to R and let $\mathcal{T} = \{T_i\}_{i \in I}$ be this restriction. Write $\pi_i : R \to T_i$ be the natural projection. Now construct a graph $\mathcal{G}$ on the vertices I where $\{i, j\} \in \binom{I}{2}$ is an edge if and only if there are $a, b \in I$ such that $\pi_i(T_a \cdot T_b) \neq 0$ and $\pi_j(T_a \cdot T_b) \neq 0$, which we may compute in polynomial time. Then with C the set of connected components of $\mathcal{G}$ we obtain a map $u_2 : I \to C$ such $\mathcal{U} = u_{2*}\mathcal{T}$ is a pre-grading. We can now easily define a grid structure on C such that $\overline{U} = (R, C, \mathcal{U})$ is a loose grid grading and $u = u_2 \circ u_1$ satisfies the requirements. □

8.3 Computing universal grid gradings of reduced orders

We can now present our final algorithm.

Algorithm 8.9. Let R be a reduced order.

1. Let $E = R \otimes_{\mathbb{Z}} \mathbb{Q}$ and compute $\operatorname{spec} E$, $E_P = \prod_{\mathfrak{m} \in P} E/\mathfrak{m}$ and maps $\pi_P : E \to E_P$ for each $P \subseteq \operatorname{spec} E$, as well as $R_P = \pi_P(R)$ using Theorem 1.10 from [12].
2. For each $P \subseteq \operatorname{spec} E$ compute a universal abelian group grading $\overline{A}_P$ of R_P using Algorithm 7.11 and let $\overline{E}_P$ be the corresponding grading of E_P.
3. For each partition $\mathcal{P}$ of $\operatorname{spec} E$ such that $\overline{E}_P$ is loose for each $P \in \mathcal{P}$, compute $\overline{E}_{\mathcal{P}} = \coprod_{P \in \mathcal{P}} \overline{E}_P$ and the corresponding universal $u_{\mathcal{P}}$ such that $u_{\mathcal{P}*}\overline{E}_{\mathcal{P}}$ restricts to R using Proposition 8.8, and let $\overline{R}_{\mathcal{P}}$ be that restriction.
4. Return any grading $\overline{R}_{\mathcal{P}}$ with the most homogeneous components among all partitions $\mathcal{P}$.

Proof of Theorem 1.9 for grids: We show that Algorithm 8.9 computes the universal grid grading of R in $n^{O(m)}$ time, where $m = \# \operatorname{minspec} R = \# \operatorname{spec} E$. First we note that there are 2^m subsets $P \subseteq \operatorname{spec} E$ and at most m^m partitions $\mathcal{P}$ of $\operatorname{spec} E$. For each $P \subseteq \operatorname{spec} E$ we take at most $n^{O(m)}$ time and for each $\mathcal{P}$ only $n^{O(1)}$ time. Thus the total complexity becomes $n^{O(m)}$, as was to be shown.

Let $\overline{U} = (R, \mathrm{Y}, \{U_v\}_{v \in \mathrm{Y}})$ be a universal grid grading of R and let $\overline{V}$ be the corresponding grading of E. Consider $\operatorname{prid}(V_1)$, which induces a partition of $\operatorname{prid}(E)$, which in turn induces a partition $\mathcal{P}$ of $\operatorname{spec} E$ by Corollary 6.3. For $P \in \mathcal{P}$ let $\overline{V}_P = (\pi_P(E), \mathrm{Y}, \{\pi_P(V_v)\}_{v \in \mathrm{Y}})$, which form the factors of $\overline{V}$ as in Lemma 6.5. Note that each $\overline{V}_P$ restricts to R_P and let $\overline{U}_P$ be this restriction. Because $\overline{A}_P = (R_P, G_P, \{A_{P,g}\}_{g \in G_P})$ is a universal abelian group grading of R_P, there exists a unique morphism $f_P : G_P \to \mathrm{Y}$ such that $f_{P*}\overline{A}_P = \overline{U}_P$ and thus $f_{P*}\overline{E}_P = \overline{V}_P$. Then the combined map $f : \coprod_{P \in \mathcal{P}} G_P \to \mathrm{Y}$ satisfies $f_*\overline{E}_{\mathcal{P}} = \overline{V}$. Since $\overline{V}$ restricts to R, there exists a unique g such that $f = g \circ u_{\mathcal{P}}$ and $g_*\overline{R}_{\mathcal{P}} = \overline{U}$ by universality of $u_{\mathcal{P}}$. As $\overline{U}$ is a universal grid grading of R, so must be $\overline{R}_{\mathcal{P}}$ as it is loose. Hence a universal grid grading of R is among the possible gradings returned by the algorithm in step (4).

Assume there is some partition $\mathcal{Q}$ of $\operatorname{spec} E$ such $\overline{E}_Q$ is loose for all $Q \in \mathcal{Q}$ and such that $\overline{R}_{\mathcal{Q}}$ has at least as many homogeneous components as $\overline{R}_{\mathcal{P}}$. Then there exists a unique morphism $g_* : \overline{R}_{\mathcal{P}} \to \overline{R}_{\mathcal{Q}}$ which is surjective on the underlying grid by universality and must be bijective as the grid of $\overline{R}_{\mathcal{Q}}$ is at least as large as the grid of $\overline{R}_{\mathcal{P}}$ and both are finite. Since $\overline{R}_{\mathcal{Q}}$ is loose it must be universal as well. Thus the algorithm is correct. □

We get the final part of Theorem 1.9 as a corollary.

Proof of Theorem 1.9 for groups: We compute the universal grid grading $\overline{U} = (R, \mathrm{Y}, \{U_v\}_{v \in \mathrm{Y}})$ using Algorithm 8.9. We may take $G = \mathrm{Y}^{\mathrm{grp}}$ by Proposition 6.7 and a finite presentation of G and a map $f : \mathrm{Y} \to G$ can be obtained as in Lemma 2.9 in clearly polynomial time. □

References

[1] H. W. Lenstra Jr. and A. Silverberg. Universal gradings of orders. *Archiv der Mathematik*, 111(6):579–597, Dec 2018.

[2] William W. Boone. The word problem. *Annals of Mathematics*, 70(2):207–265, 1959.

[3] Daniel Gorenstein. Classifying the finite simple groups. *Bull. Amer. Math. Soc. (N.S.)*, 14(1):1–98, 01 1986.

[4] W. Rudin. *Fourier Analysis on Groups*. Dover Books on Mathematics. Dover Publications, 2017.

[5] Serge Lang. *Algebra*. Springer, 3 edition, 2002.

[6] Eliot T. Jacobson and William Y. Vélez. The galois group of a radical extension of the rationals. *manuscripta mathematica*, 67(1):271–284, Dec 1990.

[7] H. W. Lenstra, Jr. Lattices. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44:127–181, 2008. http://library.msri.org/books/Book44/files/06hwl.pdf#page=36.

[8] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The design and analysis of computer algorithms*. Addison-Wesley, 1 edition, 1974.

[9] David Eisenbud. *Commutative Algebra*. Springer, 1 edition, 1995.

[10] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 2 edition, 1990.

[11] Martin Eichler. Note zur Theorie der Kristallgitter. *Mathematische Annalen*, 125(1):51–55, Dec 1952. `https://doi.org/10.1007/BF01343106`.

[12] H. W. Lenstra Jr. and A. Silverberg. Algorithms for commutative algebras over the rational numbers. *Foundations of Computational Mathematics*, 18(1):159–180, Feb 2018.

[13] A. K. Lenstra. Factoring polynomials over algebraic number fields. In J. A. van Hulzen, editor, *Computer Algebra*, pages 245–254, Berlin, Heidelberg, 1983. Springer Berlin Heidelberg.

[14] Saunders Mac Lane. *Categories for the Working Mathematician*. Springer, 2 edition, 1978.

A Category theory

We provide a brief summary of the category theoretical terminology we employ. Most of this can be found in [14] albeit with some possible notational differences.

Definition A.1. A *category* $\mathcal{C}$ consists of a class $\text{obj}(\mathcal{C})$ of *objects* and a class $\text{hom}(\mathcal{C})$ of *morphisms*. Each $f \in \text{hom}(\mathcal{C})$ has a unique associated *source* $s(f)$ and *target* $t(f)$ in $\text{obj}(\mathcal{C})$, written $f : s(f) \to t(f)$, and we write $\text{Hom}_{\mathcal{C}}(A, B)$ for the subclass of morphisms $f \in \text{hom}(\mathcal{C})$ such that $s(f) = A$ and $t(f) = B$. For $f \in \text{Hom}_{\mathcal{C}}(A, B)$ and $g \in \text{Hom}_{\mathcal{C}}(B, C)$ we have a *composition* $g \circ f \in \text{Hom}_{\mathcal{C}}(A, C)$, and the operation $\circ$ is associative. Furthermore, $\text{Hom}_{\mathcal{C}}(A, A)$ contains a (unique) *identity* element id_A such that for all $f \in \text{hom}(\mathcal{C})$ we have $\text{id}_A \circ f = f$ if $t(f) = A$ and $f \circ \text{id}_A = f$ if $s(f) = A$. We say $f \in \text{Hom}_{\mathcal{C}}(A, B)$ is *invertible* if there exists some $g \in \text{Hom}_{\mathcal{C}}(B, A)$ such that $g \circ f = \text{id}_A$ and $f \circ g = \text{id}_B$. A category $\mathcal{D}$ is a *subcategory* of $\mathcal{C}$ if $\text{obj}(\mathcal{D}) \subseteq \text{obj}(\mathcal{C})$, $\text{hom}(\mathcal{D}) \subseteq \text{hom}(\mathcal{C})$ and $\mathcal{D}$ has the same composition law and identity elements as $\mathcal{C}$. Any $A \in \text{obj}(\mathcal{C})$ is called *initial* if for all $B \in \text{obj}(\mathcal{C})$ there exists a unique morphism $f : A \to B$.

We write `Set` for the category of sets, `Grp` for the category of groups and `Ab` for the category of abelian groups. For any commutative ring k we write k-`Mod` for the category of k-modules and k-`Alg` for the category of k-algebras.

Definition A.2. For a category $\mathcal{C}$ we define the classes of *endomorphisms* and *isomorphisms* of $\mathcal{C}$ as

$$\text{end}(\mathcal{C}) = \{f \in \text{hom}(\mathcal{C}) \mid s(f) = t(f)\} \quad \text{and} \quad \text{iso}(\mathcal{C}) = \{f \in \text{hom}(\mathcal{C}) \mid f \text{ is invertible}\}$$

respectively. We also write $\text{aut}(\mathcal{C}) = \text{end}(\mathcal{C}) \cap \text{iso}(\mathcal{C})$ for the class of *automorphisms* of $\mathcal{C}$. For given $A, B \in \text{obj}(\mathcal{C})$ we additionally define the classes

$$\text{End}_{\mathcal{C}}(A) = \text{Hom}_{\mathcal{C}}(A, A), \quad \text{Iso}_{\mathcal{C}}(A, B) = \text{Hom}_{\mathcal{C}}(A, B) \cap \text{iso}(\mathcal{C}), \quad \text{Aut}_{\mathcal{C}}(A) = \text{Iso}_{\mathcal{C}}(A, A).$$

Definition A.3. Let $\mathcal{C}$ be a subcategory of $\mathcal{D}$. Then

1. $\mathcal{C}$ is *locally small* if $\text{Hom}_{\mathcal{C}}(A, B)$ is a set for all $A, B \in \text{obj}(\mathcal{C})$.
2. $\mathcal{C}$ is *small* if it is locally small and $\text{obj}(\mathcal{C})$ is a set.
3. $\mathcal{C}$ is *finite* if $\text{obj}(\mathcal{C})$ and $\text{Hom}_{\mathcal{C}}(A, B)$ are finite sets for all $A, B \in \text{obj}(\mathcal{C})$.
4. $\mathcal{C}$ is a *wide subcategory of* $\mathcal{D}$ if $\text{obj}(\mathcal{C}) = \text{obj}(\mathcal{D})$.
5. $\mathcal{C}$ is a *full subcategory of* $\mathcal{D}$ if $\text{Hom}_{\mathcal{C}}(A, B) = \text{Hom}_{\mathcal{D}}(A, B)$ for all $A, B \in \text{obj}(\mathcal{D})$.
6. $\mathcal{C}$ is a *monoid* if $\# \text{obj}(\mathcal{C}) = 1$.
7. $\mathcal{C}$ is a *groupoid* if $\text{hom}(\mathcal{C}) = \text{iso}(\mathcal{C})$, i.e. all morphisms of $\mathcal{C}$ are invertible.
8. subclasses $X, Y \subseteq \text{obj}(\mathcal{C})$ are *disconnected* if for all $K \in X$ and $L \in Y$ there are no morphisms $K \to L$ or $L \to K$.
9. a subclass $Z \subseteq \text{obj}(\mathcal{C})$ is *connected* if $Z \neq \emptyset$ and for all disconnected subclasses $X, Y \subseteq \text{obj}(\mathcal{C})$ such that $X \cup Y = Z$ we have $X = Z$ or $Y = Z$.

Definition A.4. Let $\mathcal{C}, \mathcal{D}$ be categories. A *functor* $F : \mathcal{C} \to \mathcal{D}$ is a mapping that assigns to each $A \in \text{obj}(\mathcal{C})$ an object $F(A) \in \text{obj}(\mathcal{D})$ and to each morphism $f \in \text{Hom}_{\mathcal{C}}(A, B)$ a morphism $F(f) \in \text{Hom}_{\mathcal{D}}(F(A), F(B))$ such that

$$F(\text{id}_A) = \text{id}_{F(A)} \quad \text{and} \quad F(g \circ f) = F(g) \circ F(f)$$

for all $A, B, C \in \text{obj}(\mathcal{C})$, $f \in \text{Hom}_{\mathcal{C}}(A, B)$ and $g \in \text{Hom}_{\mathcal{C}}(B, C)$. If $\mathcal{C}$ and $\mathcal{D}$ are small categories and $A, B \in \text{obj}(\mathcal{C})$ we write $F_{A,B} : \text{Hom}_{\mathcal{C}}(A, B) \to \text{Hom}_{\mathcal{D}}(F(A), F(B))$ for the map given by $f \mapsto F(f)$. The class of all small categories forms a category `Cat`, in which the functors are the morphisms.