



Finite representation type and direct-sum cancellation

Ryan Karr¹

Department of Mathematics and Statistics, University of Nebraska–Lincoln, Lincoln, NE 68588-0323, USA

Received 17 January 2003

Abstract

Consider the notion of *finite representation type* (FRT for short): An integral domain R has FRT if there are only finitely many isomorphism classes of indecomposable finitely generated torsion-free R -modules. Now specialize: Let R be of the form $D + c\mathcal{O}$ where D is a principal ideal domain whose residue fields are finite, $c \in D$ is a nonzero nonunit, and \mathcal{O} is the ring of integers of some finite separable field extension of the quotient field of D . If the D -rank of R is at least four then R does not have FRT. In this case we show that cancellation of finitely generated torsion-free R -modules is valid if and only if every unit of $\mathcal{O}/c\mathcal{O}$ is liftable to a unit of \mathcal{O} . We also give a complete analysis of cancellation for some rings of the form $D + c\mathcal{O}$ having FRT. We include some examples which illustrate the difficult cubic case.

© 2004 Elsevier Inc. All rights reserved.

Keywords: Cancellation; Lattice; Order

1. Introduction

In its most general terms, the cancellation question for modules asks whether $L \oplus M \cong L \oplus N$ implies $M \cong N$. Here, L , M and N are modules, usually assumed to be finitely generated, over a ring. Until the mid-seventies, research on the cancellation question focused mainly on finitely generated projective modules over polynomial rings and, more generally, coordinate rings of algebraic varieties. The reason for this focus was the

E-mail address: rkarr@math.unl.edu.

¹ This research forms part of the author's PhD dissertation at the University of Nebraska–Lincoln. Part of the research was supported by a grant from the National Science Foundation.

celebrated question raised by J.-P. Serre [21] in 1955: If R is the polynomial ring in a finite number of variables over a field, is every finitely generated projective module free? This question reduces to the cancellation question: If P and Q are finitely generated R -modules such that $P \oplus R \cong Q \oplus R$, are P and Q necessarily isomorphic? Serre's question inspired a huge amount of research on the cancellation question for projective modules, from the Bass Cancellation Theorem [2, Chapter IV, (3.5)] (which gives a positive answer if the rank of P is greater than the number of variables) to the eventual solution by Quillen [19] and Suslin [23].

Efforts to answer Serre's problem resulted in many important results on cancellation and failure of cancellation for projective modules over more general rings; see [17,26,27]. Moreover, research on these questions continued long after the solution of Serre's problem; see [3,13,22,24,35].

The modules we will consider in this paper will not in general be projective. Much less is known about cancellation in general. Among the first results was the theorem, due to Vasconcelos [29], that says cancellation holds for finitely generated modules over commutative semilocal rings. Other early results on cancellation can be found in [7,28].

The rings we will consider are Noetherian integral domains, and the modules are finitely generated and torsion-free. The first result on cancellation in this context (beyond the classical result for Dedekind domains, due to Steinitz) was due to Chase [4], who proved that torsion-free cancellation holds over the polynomial ring $K[x, y]$, provided K is an algebraically closed field of characteristic zero. In [32] R. Wiegand began a systematic study of cancellation for torsion-free modules over Noetherian rings of dimension one and two. This work was continued in joint work with S. Wiegand in [33,34], and in [25] Swan applied the Wiegands' methods in a non-commutative setting. More recently, in [8,9] Guralnick and Levy also considered the cancellation problem for torsion-free modules over one-dimensional rings.

Definitive results pertaining to cancellation for orders in quadratic number fields were obtained in [32]. In this paper, we extend the study of cancellation to orders in number fields of higher degree. When the degree is at least four, we give a complete answer to the cancellation question for a large family of orders. Number fields of degree three pose the greatest difficulties and hence our results are less conclusive. All the results we obtain in this paper are valid not only for number fields but also for algebraic function fields in one variable over a finite field of constants.

2. Definitions and preliminary results

All rings in this paper are commutative. If R is a ring then the group of units of R is denoted by R^\times . If M is an R -module then $M^{(r)}$ denotes the direct sum of r copies of M . If R is a local ring with maximal ideal \mathfrak{m} then the \mathfrak{m} -adic completion of R is denoted by \widehat{R} . All local rings in this paper will be Noetherian.

Definition 1. Suppose R is a one-dimensional Noetherian domain. We say that *cancellation holds for R* provided the implication $L \oplus M \cong L \oplus N \Rightarrow M \cong N$ holds for all finitely generated torsion-free R -modules L , M and N ; otherwise we say *cancellation fails for R* .

Remark 2. For a one-dimensional Noetherian domain R , a finitely generated torsion-free R -module is sometimes referred to as an R -lattice in the literature.

Definition 3. An *Artinian pair* consists of an Artinian ring A contained in a commutative ring B such that B is finitely generated as an A -module. Such a pair will be denoted $A \hookrightarrow B$. An $A \hookrightarrow B$ *module* consists of a finitely generated projective B -module W and an A -submodule V of W such that $BV = W$. Such a module will be denoted $V \hookrightarrow W$. An $A \hookrightarrow B$ -morphism from $V_1 \hookrightarrow W_1$ to $V_2 \hookrightarrow W_2$ is defined to be a B -linear map $\alpha : W_1 \rightarrow W_2$ such that $\alpha(V_1) \subseteq V_2$. We say that the $A \hookrightarrow B$ -module $V \hookrightarrow W$ has *constant rank* provided W is a free B -module.

All of the modules we will construct will have constant rank. We mention that there is a well-defined notion of direct-sum decomposition in the category of modules over $A \hookrightarrow B$. For the remainder of this section, let $A \hookrightarrow B$ denote any Artinian pair. We now describe some matrix constructions that can be used to build constant-rank modules over $A \hookrightarrow B$. Most of the material in this section appears either in [31, Section 2] or in [34, Section 3].

Definition 4. Let r be any positive integer. Let ν denote the r -by- r nilpotent matrix having 1's on the super-diagonal and 0's elsewhere. Let 1_r denote the r -by- r identity matrix. Suppose τ is an r -by- r matrix over a (commutative) ring T having entries τ_{ij} . We say τ is *striped* if $\tau_{i,j} = \tau_{i+1,j+1}$ for all i, j . We say τ is *upper triangular* if $\tau_{i,j} = 0$ whenever $i > j$.

The matrices ν and 1_r will continue to appear throughout the rest of this section. The next lemma is easy to prove and is well known for matrices over a field k . See [10, III.15, Ex. 1].

Lemma 5. Let ν be the matrix given in Definition 4. Suppose τ is an r -by- r matrix over a ring T . If $\tau\nu = \nu\tau$ then τ is an upper triangular striped matrix. \square

The following construction is taken from [34, Section 3].

Construction 6. Let $W := B^{(r)}$ and represent elements of W as column vectors. Let X be any r -by- s matrix over B , where $s \geq r$. Let x_j denote the j th column of X and let V denote the A -submodule of W generated by the x_j 's. If $BV = W$ then $V \hookrightarrow W$ is a constant-rank $A \hookrightarrow B$ -module. Usually, we will take the left r -by- r submatrix of X to be identity matrix 1_r ; then $BV = W$ is automatic.

More generally, suppose we can represent B as a direct product: $B = \prod_{i=1}^t B_i$. Then $W = \bigoplus_{i=1}^t B_i^{(r)}$. For each i from 1 to t , let X_i be any r -by- s matrix over B_i . We let x_j be the element of W whose i th component is the j th column of X_i . Let V denote the A -submodule of W generated by the x_j 's. Again, if $BV = W$ then $V \hookrightarrow W$ is a constant-rank $A \hookrightarrow B$ -module.

We collect some information regarding the endomorphisms of $V \hookrightarrow W$. The following is a consequence of a general fact concerning endomorphisms of modules over Artinian pairs (see [34, the remarks preceding Proposition 3.2]).

Lemma 7. *Suppose $V \hookrightarrow W$ is a (constant-rank) $A \hookrightarrow B$ -module produced by Construction 6. A sequence of matrices $(\varphi_1, \dots, \varphi_t)$, where each φ_i is an r -by- r matrix over B_i , represents an endomorphism of $V \hookrightarrow W$ if and only if there is one s -by- s matrix λ over A such that $\varphi_i X_i = X_i \lambda$ holds simultaneously for all i .*

We take $t = 1$, specialize the matrix X , and analyze the endomorphisms of the resulting module $V \hookrightarrow W$. The following corollary is a generalization of part of an argument used in [31, Proposition 2.6].

Corollary 8. *Suppose a positive integer r is given. Let $a, b \in B$ and set $X := (1_r | a1_r + bv)$. Build V and W as in Construction 6 above. Suppose the r -by- r matrix φ represents an endomorphism of $V \hookrightarrow W$. Then $\varphi = \sigma + ar + bv\tau$ and*

$$a\sigma + b\sigma v + a^2\tau + ab(v\tau + \tau v) + b^2v\tau v = \mu + a\varrho + bv\varrho \quad (1)$$

for suitable r -by- r matrices σ, τ, μ and ϱ over A .

As above, let $A \hookrightarrow B$ be any Artinian pair. We need a definition which appears in [34, Section 1].

Definition 9. Suppose $V \hookrightarrow W$ is a constant-rank $A \hookrightarrow B$ -module. The *delta group* of $V \hookrightarrow W$ in B , denoted $\Delta(V \hookrightarrow W)$, is defined to be the subgroup of B^\times consisting of the determinants of all automorphisms of $V \hookrightarrow W$. We will often use the plain symbol Δ in contexts where the dependence on $V \hookrightarrow W$ is clear.

It is useful to know the delta group is well behaved with respect to direct sums. The next lemma is the same as [34, Lemma 1.7] except that our notation here is slightly different from the notation there.

Lemma 10. *Suppose $V_1 \hookrightarrow W_1$ and $V_2 \hookrightarrow W_2$ are two constant-rank $A \hookrightarrow B$ -modules. Let Δ_1 and Δ_2 be the corresponding delta groups. Then the delta group of $(V_1 \hookrightarrow W_1) \oplus (V_2 \hookrightarrow W_2)$ is $\Delta_1 \cdot \Delta_2$.*

The following proposition extends part of the proof of [31, Proposition 2.6]. In the statement of the proposition below, note that A^\times is assumed to be finite. A proof of the proposition may be found in [12].

Proposition 11. *Let $A \hookrightarrow B$ be an Artinian pair with A^\times finite. Suppose there are $a, b \in B$ such that $\{1, a, a^2, b\}$ is linearly independent over A . Then there is a constant-rank $A \hookrightarrow B$ -module $V \hookrightarrow W$ with delta group $\Delta = 1$.*

3. Orders and cancellation

Suppose D is a principal ideal domain having the property that all of its residue fields are finite. Denote the quotient field of D by F . Next, suppose K is a finite separable field extension of F . Let \mathcal{O} be the integral closure of D in K . Our assumptions on K imply, in particular, that each residue field of \mathcal{O} is a finite field extension of some residue field of D . We use d to denote the degree $[K : F]$ of K over F . *The notation and assumptions introduced in this paragraph will remain in force throughout the rest of this paper.*

Since D is integrally closed in F we have $\mathcal{O} \cap F = D$. More generally, $(I\mathcal{O}) \cap D = I$ for each ideal $I \subseteq D$. We let $\{\omega_1, \dots, \omega_d\}$ be a basis of the free D -module \mathcal{O} . It is often desirable to have an integral basis of the form $\omega_i := \theta^{i-1}$ for some $\theta \in \mathcal{O}$. However, Dedekind found an example of a cubic number field in which the integral closure of \mathbb{Z} does not have a basis of this form. In any case, the following lemma allows us to assume $\omega_1 = 1$.

Lemma 12. *With notation as above, there is a D -basis $\omega_1, \dots, \omega_d$ of \mathcal{O} such that $\omega_1 = 1$.*

Proof. We want to show that D is a direct summand of \mathcal{O} . It suffices to show that \mathcal{O}/D is torsion-free (and hence free) as a D -module. Given $\alpha \in \mathcal{O}$, if $b\alpha \in D$ for some nonzero $b \in D$ then $\alpha \in \mathcal{O} \cap F = D$. \square

Definition 13. Recall that F is the quotient field of D . A subring R of \mathcal{O} containing D is called a D -order, or an order for short, if $FR = K$. Now suppose R is an order and consider the R -ideal $\mathfrak{c}_R := (R :_R \mathcal{O})$. It is the largest \mathcal{O} -ideal contained in R and is called the *conductor* of R . The image of \mathcal{O}^\times in $(\mathcal{O}/\mathfrak{c}_R)^\times$ under the quotient map is denoted by Λ_R and is called the group of liftable units $\mathcal{O}/\mathfrak{c}_R$.

One of the main techniques in studying an order R is to kill the conductor in both R and \mathcal{O} and work with the bottom line of the resulting pullback square:

$$\begin{array}{ccc} R & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ R/\mathfrak{c}_R & \longrightarrow & \mathcal{O}/\mathfrak{c}_R \end{array} \quad (2)$$

Sometimes it is easier to work with a larger order S which contains the given order R .

Lemma 14. *Suppose $R \subseteq S \subseteq \mathcal{O}$ where R and S are orders. If cancellation fails for S then cancellation fails for R .*

Proof. If M and N are S -lattices then of course every S -linear map $\varphi : M \rightarrow N$ is R -linear. We claim the converse is true. Suppose $\varphi : M \rightarrow N$ is R -linear. Take a nonzero element $c \in \mathfrak{c}_R$. Then $c \in R$ and $cs \in R$ for all $s \in S$. For all $x \in M$ we have $c\varphi(sx) = \varphi(cs x) = cs\varphi(x)$. Since N is torsion-free, $\varphi(sx) = s\varphi(x)$ and thus φ is S -linear. Therefore

$\varphi: M \rightarrow N$ is an S -homomorphism if and only if it is an R -homomorphism. The rest is clear. \square

We now establish a general criterion for cancellation. See Section 2 for the definitions related to delta groups. The next proposition is based on results in [34].

Proposition 15. *Let R be any proper order in \mathcal{O} . Let $A := R/\mathfrak{c}_R$ and $B := \mathcal{O}/\mathfrak{c}_R$. Then cancellation fails for R if and only if there is an $A \hookrightarrow B$ -module $V \hookrightarrow W$ with constant rank and with delta group Δ such that $\Delta \cdot \Lambda_R \neq B^\times$.*

Proof. If $\Delta \cdot \Lambda_R \neq B^\times$ for some $A \hookrightarrow B$ -module $V \hookrightarrow W$ with ${}_B W$ free of rank r , choose $u \in B^\times - \Delta \cdot \Lambda_R$. Referring to item (i) on p. 432 of [34], we take $C := \mathcal{O}$ and $P := \mathcal{O}^{(r)}$. We define M to be the pullback of P and V over W . In the notation of [34, (1.3)] we put $N := M^u$ (M “twisted” by u). By [34, Proposition 1.4] we have $M \oplus \mathcal{O} \cong N \oplus \mathcal{O}$, whereas $M \not\cong N$ by [34, Lemma 1.6]. Hence cancellation fails.

Conversely, suppose we have $\Delta \cdot \Lambda_R = B^\times$ for all constant-rank $A \hookrightarrow B$ -modules $V \hookrightarrow W$, where Δ is the delta group of $V \hookrightarrow W$. Let L, M and N be R -lattices. If $M \oplus L \cong N \oplus L$ then $M^u \cong N$ for some $u \in B^\times$ by [34, Proposition 1.4]. By assumption, $\Delta_M \cdot \Lambda_R = B^\times$, where Δ_M denotes the delta group of the $A \hookrightarrow B$ -module $M/\mathfrak{c}_R M \hookrightarrow \mathcal{O}M/\mathfrak{c}_R M$. Note that $\mathcal{O}M/\mathfrak{c}_R M$ is a free $\mathcal{O}/\mathfrak{c}_R$ -module since R is a domain. Since $u \in \Delta_M \cdot \Lambda_R$, we gather from [34, Lemma 1.6] that $M \cong N$. Hence cancellation holds. \square

4. A family of orders and finite representation type

We keep the notation and assumptions introduced at the beginning of Section 3. It is a well-known fact that every order R in a quadratic number field has the form $R = \mathbb{Z} + c\mathcal{O}$ for some $c \in \mathbb{Z}$. While this fact is no longer true for orders in higher-degree fields, we will restrict most of our attention in this paper to orders having the form $D + c\mathcal{O}$.

Consider an element $c \in D$. We assume throughout that c is a nonzero nonunit of D . Let $R := D + c\mathcal{O}$; then R is an order properly contained in \mathcal{O} . By Lemma 12 we can write $R = D \oplus Dc\omega_2 \oplus \cdots \oplus Dc\omega_d$. The conductor \mathfrak{c}_R can be determined quite explicitly.

Lemma 16. *With the notation above, $\mathfrak{c}_R = c\mathcal{O}$.*

Proof. Since $c\mathcal{O} \subseteq R$ it follows that $c \in \mathfrak{c}_R$ and hence $c\mathcal{O} \subseteq \mathfrak{c}_R$. For the reverse inclusion, suppose $r \in \mathfrak{c}_R$. Set $M := D\omega_2 \oplus \cdots \oplus D\omega_d$. Recall that we have assumed $d \neq 1$. We can write $r = b + cm$, where $b \in D$ and $m \in M$. It suffices to show $b \in cD$. Since $b \in \mathfrak{c}_R$, $b\omega_2$ is an element of R . Therefore $b\omega_2 \in Dc\omega_2$ and hence b is a multiple of c . \square

Since $(D + c\mathcal{O})/c\mathcal{O} \cong D/(c\mathcal{O} \cap D) = D/cD$, the pullback for $R := D + c\mathcal{O}$ has the following form:

$$\begin{array}{ccc} D + c\mathcal{O} & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ D/cD & \longrightarrow & \mathcal{O}/c\mathcal{O} \end{array} \quad (3)$$

Definition 17. Suppose R is a one-dimensional Noetherian domain. We say R has *finite representation type* if there are only finitely many isomorphism classes of indecomposable finitely generated torsion-free R -modules.

The next lemma follows immediately from the proof of Lemma 14.

Lemma 18. Suppose $R \subseteq S \subseteq \mathcal{O}$ where R and S are orders. If R has finite representation type then S has finite representation type.

We can decide when $R := D + c\mathcal{O}$ has finite representation type.

Proposition 19. Assume D is a principal ideal domain, all the residue fields of D are finite, F is the quotient field of D , K is a finite separable field extension of F having degree $d > 1$, and \mathcal{O} is the integral closure of D in K . Let $R := D + c\mathcal{O}$, where $c \in D$ is a nonzero nonunit. Then $R := D + c\mathcal{O}$ has finite representation type if and only if either (1) $d = 2$ or (2) $d = 3$ and c is squarefree.

Proof. Set $A := D/cD$ and $B := \mathcal{O}/c\mathcal{O}$. It follows from [31, Corollary 5.2 and Remark 1.10.1] that R has finite representation type if and only if the following two conditions hold: (DR1) the A -module B can be generated by 3 elements; (DR2) the A -module $(JB + A)/A$ is trivial or is cyclic, where $J := \text{rad } A$. These conditions were introduced by Drozd and Roĭter in [6]. Note that $d = 2$ or $d = 3$ ensures that (DR1) holds and hence it suffices to consider (DR2) in each case. If $d = 2$ then B/A is a cyclic A -module; since A is a principal ideal ring, (DR2) holds. If $d = 3$ and c is squarefree then $J := \text{rad } A = 0$ and condition (DR2) holds.

Conversely, suppose $d = 3$ and there is a prime $p \in D$ such that $p^2 | c$; then R is contained in the order $D + p^2\mathcal{O}$. By the proof of Lemma 14 it is enough to show that $D + p^2\mathcal{O}$ does not have finite representation type. In other words, we can assume $c = p^2$. Thus A is local, $J = pA$ and $J^2 = 0$; denote the residue field of A by k . Note that the annihilator of the A -module $(JB + A)/A$ is J and hence $(JB + A)/A$ is naturally a k -module. Since $B = A \oplus A\overline{\omega}_2 \oplus A\overline{\omega}_3$, we have $(JB + A)/A = Ap\overline{\omega}_2 \oplus Ap\overline{\omega}_3$ and hence $(JB + A)/A$ has k -dimension equal to 2. Thus (DR2) fails. Finally, if $d \geq 4$ then (DR1) fails. \square

In the proof above, when $d = 3$ we see that $(JB + A)/A$ is either trivial or has k -dimension 2, depending on whether or not c is squarefree. The reader might wonder about the absence of dimension 1. As we have seen, $(JB + A)/A$ cannot have dimension

1 when R has the form $D + c\mathcal{O}$, but one can build examples of orders having the form $D[c\theta] = D + Dc\theta + Dc^2\theta^2$ so that $(JB + A)/A$ has dimension 1. However, I do not yet have any general results for orders having the form $D[c\theta]$.

5. Main results

Suppose D is a complete discrete valuation ring with finite residue field. As above, denote the quotient field of D by F . Then the valuation on the quotient field F of D extends uniquely to a valuation of K . The following fact comes from [30, Proposition 3.3.3].

Lemma 20. *Suppose D is a complete discrete valuation ring having a finite residue field. Let K be a finite separable extension of the quotient field of D and let \mathcal{O} be the integral closure of D in K . Then there is a unit $u \in \mathcal{O}^\times$ such that $\{1, u, \dots, u^{d-1}\}$ is a D -basis for \mathcal{O} .*

Now suppose D is any principal ideal domain having all of its residue fields finite. Since we will be dealing later on with rings of the form $D/p^m D$, where $p \in D$ is a prime element, it will be useful to examine the completion $\widehat{D}_{\mathfrak{p}}$ of D localized at $\mathfrak{p} := pD$. Let the prime factorization of $\mathfrak{p}\mathcal{O}$ be written as $\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$, where the prime ideals $\mathfrak{q}_i \subset \mathcal{O}$ are distinct and $e_i \geq 1$ for each i . For ease of notation, we write \mathcal{O}_i for the localization $\mathcal{O}_{\mathfrak{q}_i}$. For all positive integers m we have

$$D/\mathfrak{p}^m = \widehat{D}_{\mathfrak{p}}/\mathfrak{p}^m \widehat{D}_{\mathfrak{p}} \quad \text{and} \quad \mathcal{O}_i/\mathfrak{q}_i^{me_i} \mathcal{O}_i = \widehat{\mathcal{O}_i}/\mathfrak{q}_i^{me_i} \widehat{\mathcal{O}_i}; \quad (4)$$

we also have

$$(\mathfrak{q}_i^{me_i} \mathcal{O}_i) \cap D_{\mathfrak{p}} = (\mathfrak{p}^m \mathcal{O}_i) \cap D_{\mathfrak{p}} = \mathfrak{p}^m D_{\mathfrak{p}}. \quad (5)$$

Let f_i be the degree of \mathfrak{q}_i over \mathfrak{p} ; that is, $f_i := [\mathcal{O}/\mathfrak{q}_i : D/\mathfrak{p}]$. For the rest of this section, we set $d_i := e_i f_i$.

Proposition 21. *For each i there is a unit $u_i \in \widehat{\mathcal{O}_i}^\times$ such that*

$$\{1, u_i, u_i^2, \dots, u_i^{d_i-1}\}$$

is a $\widehat{D}_{\mathfrak{p}}$ -basis for $\widehat{\mathcal{O}_i}$.

Proof. The quotient field K_i of each $\widehat{\mathcal{O}_i}$ is a finite extension of the quotient field of the complete discrete valuation ring $\widehat{D}_{\mathfrak{p}}$. It is well known that the degree of the extension is $e_i f_i$ and that $\widehat{\mathcal{O}_i}$ is the integral closure of $\widehat{D}_{\mathfrak{p}}$ in K_i . Now we apply Lemma 20. \square

Let m be a positive integer and set $A := D/\mathfrak{p}^m$ and $B := \mathcal{O}/\mathfrak{p}^m \mathcal{O}$. By the Chinese Remainder Theorem we have an A -isomorphism $B \cong \prod_{i=1}^g B_i$, where we have set $B_i := \mathcal{O}/\mathfrak{q}_i^{me_i}$ for each i . Consideration of $\widehat{\mathcal{O}_i} \otimes_D D/\mathfrak{p}^m$ with respect to (4) and (5) leads immediately from the preceding proposition to the following result.

Proposition 22. For each i there is a unit $v_i \in B_i^\times$ such that

$$\{1, v_i, v_i^2, \dots, v_i^{d_i-1}\}$$

is an A -basis for B_i .

Remark 23. Recall that $d_i := e_i f_i$. If some $d_i = 1$ then we will set $v_i := 1$.

In particular, each B_i is a free A -module of rank $e_i f_i$, B is a free A -module of rank $d = e_1 f_1 + \dots + e_g f_g$ and every nonempty subproduct of $\prod_{i=1}^g B_i$ contains A as a subring in an obvious way.

We now return to the situation given pictorially by the diagram (3). Proposition 11 is the primary tool we need in order to begin building the proof of the next theorem.

Theorem 24. Suppose D is a principal ideal domain, all the residue fields of D are finite, F is the quotient field of D , K is a finite separable field extension of F having degree d , and \mathcal{O} is the integral closure of D in K . Let $R := D + c\mathcal{O}$, where $c \in D$ is a nonzero nonunit. Let $A := D/cD$ and $B := \mathcal{O}/c\mathcal{O}$. If $d \geq 4$ then there is a constant-rank $A \hookrightarrow B$ -module having a trivial delta group.

Proof. Take $A := D/cD$ and $B := \mathcal{O}/c\mathcal{O}$ as in the statement of the theorem. Note that A^\times is finite. In order to get a constant-rank $A \hookrightarrow B$ -module having a trivial delta group, we know by Proposition 11 it suffices to find $a, b \in B$ such that $\{1, a, a^2, b\}$ is A -independent. We can most easily find such elements if we assume A is local, so we begin by imposing that assumption. Thus we can write $c = p^n$ for some prime element $p \in D$.

Write the prime factorization of $p\mathcal{O}$ as $q_1^{e_1} \cdots q_g^{e_g}$. Let f_i denote the degree of q_i . By the Chinese Remainder Theorem we have an A -isomorphism $B \cong \prod_{i=1}^g B_i$, where $B_i := \mathcal{O}/q_i^{e_i}$ for each i . Therefore, to give $a, b \in B$ such that $\{1, a, a^2, b\}$ is A -independent it will suffice to work in $\prod_{i=1}^g B_i$ instead of in B . Hence we identify B with $\prod_{i=1}^g B_i$ for the rest of this section. In what follows we will use repeatedly the fact, from above, that each B_i is a free A -module with basis $\{v_i^{j-1} : 1 \leq j \leq e_i f_i\}$, where each $v_i \in B_i^\times$. Also, if the A -rank of B_i is 1 then $v_i := 1$ (see Remark 23). Below, the word “rank” will mean A -rank.

Here is some new notation. For each i let $\varepsilon_i \in B$ denote the primitive idempotent corresponding to B_i . Also, let us set $v := (v_1, \dots, v_g) \in B^\times$. We now continue with the assumption that A is local and $d \geq 4$.

First, suppose $g = 1$. Since $d \geq 4$ we know that $B = B_1$ has rank at least 4. Set $a := v$ and $b := v^3$. Then $\{1, a, a^2, b\} = \{1, v, v^2, v^3\}$ is A -independent.

Next, suppose $g = 2$. If B_1 has rank at least 3 we take $a := v\varepsilon_1$ and $b := \varepsilon_2$ so that $\{1, a, a^2, b\} = \{1, v\varepsilon_1, v^2\varepsilon_1, \varepsilon_2\}$. We claim this set is A -independent. Suppose we have a relation in B of the form $w + xv\varepsilon_1 + yv^2\varepsilon_1 + z\varepsilon_2 = 0$, where $w, x, y, z \in A$. Project to B_1 ; we find out that $w = x = y = 0$. Now project to B_2 and see that $z = 0$. Thus $\{1, a, a^2, b\}$ is A -independent.

By symmetry, if B_2 has rank at least 3 then $\{1, v\varepsilon_2, v^2\varepsilon_2, \varepsilon_1\}$ is A -independent. Now assume both B_1 and B_2 have rank 2. We claim that $\{1, v\varepsilon_1, v^2\varepsilon_1, v\varepsilon_2\}$ is A -independent. Suppose we have a relation in B of the form $w + xv\varepsilon_1 + yv^2\varepsilon_1 + zv\varepsilon_2 = 0$, where

$w, x, y, z \in A$. Projection to B_2 shows us that $w = z = 0$. Projection to B_1 gives us $xv_1 + yv_1^2 = 0$. Since v_1 is a unit in B_1 we see that $x = y = 0$. The claim is established.

Suppose $g = 3$. Then there is some i such that the rank of B_i is at least 2. Without loss of generality, we may assume $i = 1$. We claim $\{1, v\varepsilon_1, v^2\varepsilon_1, \varepsilon_2\}$ is A -independent. Suppose we have a relation in B of the form $w + xv\varepsilon_1 + yv^2\varepsilon_1 + z\varepsilon_2 = 0$, where $w, x, y, z \in A$. Projection to B_3 shows us that $w = 0$, and then projection to B_2 reveals that $z = 0$. Projection to B_1 gives us $xv_1 + yv_1^2 = 0$. Since v_1 is a unit in B_1 we see that $x = y = 0$. The claim is established.

Finally, suppose $g \geq 4$. If there is an i such that the rank of B_i is at least 2 then we can proceed exactly as in the case $g = 3$. Hence it now suffices to assume that B is a direct product of g copies of A . Suppose there exists $u \in A^\times$ such that $u - 1 \in A^\times$. Set $a := \varepsilon_1 + u\varepsilon_2$. We claim $\{1, a, a^2, \varepsilon_3\}$ is A -independent. Suppose we have a relation in B of the form $w + xa + ya^2 + z\varepsilon_3 = 0$. Projection to B_4 and B_3 gives us $w = 0$ and $z = 0$, respectively. Projection to B_2 and B_1 gives us $ux + u^2y = 0$ and $x + y = 0$, respectively. Therefore $u(1 - u)x = 0$ and hence $x = y = 0$.

We are now left with a product B of four or more copies of the local ring A and for all $u \in A$ either u or $u - 1$ is a nonunit (for an example of this situation consider $A = \mathbb{Z}/2\mathbb{Z}$). It is *not* possible to find an A -independent set of the form $\{1, a, a^2, b\}$ in some rings B of the type that we have left. Fortunately, it turns out that a construction by E.C. Dade can be used in order to build an $A \hookrightarrow B$ -module having a trivial delta group. For a proof of Dade's Theorem see [31, Theorem 2.9]. Before completing the proof of Theorem 24 in the local case, we state and prove a result using the same construction as in [31].

Theorem 25. *Let A and B be defined as in the statement of Theorem 24. Suppose A is local and $B = \prod_{i=1}^g A$, where $g \geq 4$. Then there exists a constant-rank $A \hookrightarrow B$ -module having a trivial delta group.*

Proof. We will use the general construction of a $V \hookrightarrow W$ -module given above in Construction 6. To allow for the case $g > 4$, we take $B_i := A$ for $i \leq 3$ and put $B_4 := \prod_{i=4}^g A$. The action of A on B_4 is given by the diagonal embedding of A into B_4 .

Let $r := |A^\times|$ and let $W := B^{(r)}$. We use $t := 4$ in our construction; in other words, we write $B = \prod_{i=1}^4 B_i$ and take $W := \bigoplus_{i=1}^4 B_i^{(r)}$. Set $X_1 := (1_r | 0)$, $X_2 := (0 | 1_r)$, $X_{32} := (1_r | 1_r)$ and $X_4 := (1_r | v)$, where 1_r is the r -by- r identity matrix over A and, as before, v is the r -by- r nilpotent matrix over A having 1's on the super-diagonal and 0's elsewhere. Note that $s = 2r$ in this construction.

Let x_j be the column vector in W whose i th component (in $(B_i^{(r)})$) is the j th column of X_i . We take as generators of the A -module V the column vectors x_j . One can check that $BV = W$; thus $V \hookrightarrow W$ is an $A \hookrightarrow B$ -module. Consider an arbitrary B -endomorphism φ of W ; we can represent φ as a 4-tuple $(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, where each φ_i is an r -by- r matrix over B_i . By fact 7 we know that φ represents an endomorphism of $V \hookrightarrow W$ if and only if there is a single s -by- s matrix λ over A that simultaneously satisfies $\varphi_i X_i = X_i \lambda$ for all i .

Since λ is a $2r$ -by- $2r$ matrix over A we have $\lambda = \begin{pmatrix} \sigma & \mu \\ \tau & \varrho \end{pmatrix}$ for suitable r -by- r matrices σ, τ, μ , and ϱ over A . Now consider each φ_i in turn. From the equation $\varphi_1 X_1 = X_1 \lambda$ we get $\varphi_1 = \sigma$ and $\mu = 0$. Since $\varphi_2 X_2 = X_2 \lambda$ we get $\tau = 0$ and $\varphi_2 = \varrho$. Next, the equation $\varphi_3 X_3 = X_3 \lambda$ implies that $(\varphi_3 | \varphi_3) = (\sigma + \tau | \mu + \varrho)$ and hence $\varphi_3 = \sigma = \varrho$. Finally, since

$\varphi_4 X_4 = X_4 \lambda$ we have $(\varphi_4 | \varphi_4 v) = (\sigma + v\tau | \mu + v\varrho)$, and thus $\varphi_4 = \sigma$. It follows that $\sigma v = v\varrho = v\sigma$. The equality $\sigma v = v\sigma$ implies that σ is an upper triangular striped matrix, by Lemma 5.

We conclude that φ has the form $(\sigma, \sigma, \sigma, \sigma)$. If φ is an *automorphism* of $V \hookrightarrow W$ then we see that the determinant of the r -by- r matrix σ is 1 and hence the determinant of φ is equal to 1. \square

Now we can finish the proof of Theorem 24. We still write $A := D/cD$ and $B := \mathcal{O}/c\mathcal{O}$. We have just completed our construction of a constant-rank $A \hookrightarrow B$ -module having a trivial delta group when A is local, that is, when $c = p^n$ for some prime $p \in D$. Now suppose $c \in D$ is any nonzero nonunit. The Artinian ring $A := D/cD$ is a product of local rings, say $A = \prod_1^m A_s$. We get a corresponding decomposition $B = \prod_1^m B_s$ having the property that each $A_s \hookrightarrow B_s$ is an Artinian pair. To construct a constant-rank $A \hookrightarrow B$ -module having a trivial delta group, it is not difficult to see that it suffices to build, for each s , a constant-rank $A_s \hookrightarrow B_s$ -module $V_s \hookrightarrow W_s$ having a trivial delta group. We take $r := |A^\times|$ and build a rank r module $V_s \hookrightarrow W_s$ over each pair $A_s \hookrightarrow B_s$ using the constructions we have just described. Note that $|A_s^\times|$ divides r for each s ; therefore, for each s we get a constant-rank $A_s \hookrightarrow B_s$ -module that has a trivial delta group. Together, these modules yield a constant-rank $A \hookrightarrow B$ -module having a trivial delta group. \square

When $d < 4$ it can happen that every constant-rank $A \hookrightarrow B$ -module has a nontrivial delta group. For example, suppose $d = 2$. Then every ideal of $R := D + c\mathcal{O}$ is 2-generated, so a result of Bass [1] implies that every R -lattice is a direct sum of R -ideals (see [32, p. 444] for a more thorough statement in this situation). With $A := D/cD$ and $B := \mathcal{O}/c\mathcal{O}$, it follows that every constant-rank $A \hookrightarrow B$ -module is a direct sum of $A \hookrightarrow B$ -modules of rank 1. The remarks preceding [34, Lemma 1.6], coupled with Lemma 10, imply that the delta group of every constant-rank $A \hookrightarrow B$ -module contains the group $(D/cD)^\times$, which certainly need not be trivial.

Here is our main result concerning cancellation for the order $R = D + c\mathcal{O}$.

Theorem 26. *Suppose D is a principal ideal domain, all the residue fields of D are finite, F is the quotient field of D , K is a finite separable field extension of F having degree d , and \mathcal{O} is the integral closure of D in K . Let $R := D + c\mathcal{O}$, where $c \in D$ is a nonzero nonunit. Assume $d \geq 4$. The order $D + c\mathcal{O}$ has cancellation if and only if every unit of $(\mathcal{O}/c\mathcal{O})^\times$ is liftable.*

Proof. By Theorem 24 there is a constant-rank $A \hookrightarrow B$ -module $V \hookrightarrow W$ with delta group Δ such that $\Delta = 1$. By Lemma 16, $c_R = c\mathcal{O}$. Now apply Proposition 15. \square

6. Cubic orders without finite representation type

In this section we still hold onto the assumptions and notation from Section 3. In particular, $d := [K : F]$. What happens when $d = 3$? Since Proposition 11 works only when $d \geq 4$ we need a new construction to build modules having a trivial delta group when

$d = 3$. The following proposition brings us close to that end. The set $\{\omega_1 = 1, \omega_2, \omega_3\}$ is a D -basis of \mathcal{O} .

Proposition 27. *Suppose $d = 3$ and $R = D + p^2\mathcal{O}$, where $p \in D$ is prime. Let $A := D/p^2D$ and $B := \mathcal{O}/p^2\mathcal{O}$. Then there is a constant-rank $A \hookrightarrow B$ -module having delta group Δ such that the image $\overline{\Delta}$ of Δ in $(B/pB)^\times$ is trivial.*

Proof. Set $a := p\overline{\omega_2} \in B$ and $b := p\overline{\omega_3} \in B$, where $\overline{\omega_2}$ and $\overline{\omega_3}$ are the images of the integral basis elements ω_2, ω_3 in $\mathcal{O}/p^2\mathcal{O}$. Take $r := |(A/pA)^\times|$ and build $V \hookrightarrow W$ as described in Construction 6 by setting $X := (1_r | a1_r + bv)$. Suppose φ is an automorphism of $V \hookrightarrow W$. By Corollary 8 we have $\varphi = \sigma + a\tau + bv\tau$ and

$$a\sigma + b\sigma v + a^2\tau + ab(v\tau + \tau v) + b^2v\tau v = \mu + a\varrho + bv\varrho$$

for suitable r -by- r matrices σ, τ, μ and ϱ over A . Since $p^2 = 0$ in B we have

$$a\sigma + b\sigma v = \mu + a\varrho + bv\varrho.$$

Hence all the entries of μ are in pB . Since $pB \cap A = pA$ we may write $\mu = p\lambda$ for some matrix λ over A .

Now we have

$$p(\lambda + \overline{\omega_2}(\varrho - \sigma) + \overline{\omega_3}(v\varrho - \sigma v)) = 0,$$

that is,

$$\lambda + \overline{\omega_2}(\varrho - \sigma) + \overline{\omega_3}(v\varrho - \sigma v) \equiv 0 \pmod{pB}.$$

By the A/pA -linear independence of the images of $\{1, \overline{\omega_2}, \overline{\omega_3}\}$ in B/pB we gather that $p = \sigma \pmod{pA}$, and then that $v\sigma \equiv \sigma v \pmod{pA}$. Thus $\sigma v \equiv v\sigma \pmod{pA}$ and hence the images of the entries of σ in A/pA give us an upper triangular striped matrix, by Lemma 5. Since σ is an r -by- r matrix, the image of the determinant of σ , and hence that of $\varphi = \sigma + p\overline{\omega_2}\tau + p\overline{\omega_3}v\tau$, is equal to 1 in B/pB . Therefore, the image of Δ in $(B/pB)^\times$ is indeed trivial. \square

The preceding proposition leads to the following partial result on cancellation for cubic orders.

Corollary 28. *Suppose $d = 3$ and $R = D + p^2\mathcal{O}$, where $p \in D$ is prime. If the image $\overline{\Lambda_R}$ of \mathcal{O}^\times in $(\mathcal{O}/p\mathcal{O})^\times$ is proper then cancellation fails for R .*

Proof. Let $A := D/p^2D$ and $B := \mathcal{O}/p^2\mathcal{O}$. By Proposition 27 there is a constant-rank $A \hookrightarrow B$ -module having delta group Δ such that the image $\overline{\Delta}$ of Δ in $(B/pB)^\times$ is trivial. If the image $\overline{\Lambda_R}$ of \mathcal{O}^\times in $(\mathcal{O}/p\mathcal{O})^\times = (B/pB)^\times$ is proper then of course $\overline{\Delta} \cdot \overline{\Lambda_R} = \overline{\Lambda_R}$ is a proper subgroup of $(\mathcal{O}/p\mathcal{O})^\times$. Thus $\Delta \cdot \overline{\Lambda_R} \neq (\mathcal{O}/p^2\mathcal{O})^\times$. By Proposition 15, cancellation fails for R . \square

Let $A := D/p^2D$ and $B := \mathcal{O}/p^2\mathcal{O}$. Unfortunately, I do not know at present if it is possible to build an $A \hookrightarrow B$ -module having a trivial delta group under the hypotheses of Proposition 27. If there is such an $A \hookrightarrow B$ -module having $\Delta = 1$ in $B^\times = (\mathcal{O}/p^2\mathcal{O})^\times$ then cancellation holds for $R := D + p^2\mathcal{O}$ if and only if $\Delta_R = (\mathcal{O}/p^2\mathcal{O})^\times$ (by Proposition 15). It is desirable to find a module having a trivial delta group since it can happen that some unit in $(\mathcal{O}/p^2\mathcal{O})^\times$ may not be liftable to \mathcal{O}^\times even when every unit in $(\mathcal{O}/p\mathcal{O})^\times$ is liftable to \mathcal{O}^\times (see Example 32).

7. Cubic orders with finite representation type

Now we consider some special cubic orders R of the form $D + p\mathcal{O}$. Again, suppose $d = 3$. Let $k := D/pD$, where $p \in D$ is a prime. For the remainder of this section, suppose $p\mathcal{O}$ is a prime ideal in \mathcal{O} . Then the field $\ell := \mathcal{O}/p\mathcal{O}$ is an extension of k of degree 3. Let σ and τ be the distinct nontrivial elements of the Galois group of ℓ/k . Let us consider indecomposable modules over the Artinian pair $k \hookrightarrow \ell$. The structure of these modules is described in [33]. From [33, Theorem 3.9] we have the diagram

$$\begin{array}{ccc} \ell & \xrightarrow{\delta} & \ell \times \ell \times \ell \\ \uparrow & & \uparrow \gamma \\ k & \longrightarrow & \ell \end{array} \quad (6)$$

where δ is the diagonal embedding, γ is given by $\gamma(x) := (x, x^\sigma, x^\tau)$ and the other two maps are the inclusions. This diagram represents “change of rings” between the “bottom” Artinian pair $k \hookrightarrow \ell$ and the “top” Artinian pair $\delta: \ell \hookrightarrow \ell \times \ell \times \ell$. From [33, Theorem 3.9 and Proposition 2.10] we have the following fact.

Lemma 29. *Every indecomposable $k \hookrightarrow \ell$ -module is isomorphic to some direct summand of some indecomposable $\ell \hookrightarrow \ell \times \ell \times \ell$ -module. Furthermore, every indecomposable $\ell \hookrightarrow \ell \times \ell \times \ell$ -module is isomorphic to either $\ell \hookrightarrow 0 \times 0 \times \ell$, $\ell \hookrightarrow 0 \times \ell \times \ell$, $\ell \hookrightarrow \ell \times \ell \times \ell$ or one of the four others obtained by permuting the factors. (In each case, the map is the diagonal embedding δ followed by projection.) Finally, $\ell \hookrightarrow \ell \times \ell \times \ell$ itself is isomorphic as a $k \hookrightarrow \ell$ -module to the direct sum of three copies of $k \hookrightarrow \ell$.*

In particular, every indecomposable $k \hookrightarrow \ell$ -module has rank 1 or 2. It is not hard to see that the delta group of every $k \hookrightarrow \ell$ -module of rank 1 contains k^\times . For the $k \hookrightarrow \ell$ -module $\ell \hookrightarrow 0 \times \ell \times \ell$ given in Lemma 29 we have the following result.

Proposition 30. *With the notation and assumptions related to diagram (6) above, the delta group of the $k \hookrightarrow \ell$ -module $\ell \hookrightarrow 0 \times \ell \times \ell$ is $(\ell^\times)^2$.*

Proof. We resort to matrix reduction techniques. First we write $\ell = k(\theta)$ for some $\theta \in \ell$ with $\theta^3 - s\theta^2 + t\theta - u = 0$, where $s, t, u \in k$. Without loss of generality, we may assume

$s = 0$. (If k has characteristic $\neq 3$, we can eliminate the quadratic term by a change of variable; in characteristic 3 we can actually take $s = 0$ and $t = 1$; see [14, Theorem 6.4] for example.) We have

$$\theta^3 = u - t\theta \quad \text{and} \quad \theta^4 = u\theta - t\theta^2; \quad (7)$$

we also have

$$\begin{aligned} \theta^\sigma + \theta^\tau &= -\theta, & \theta^\sigma \theta^\tau &= t + \theta^2, \\ \theta^{2\sigma} + \theta^{2\tau} &= -2t - \theta^2, & \theta^{2\sigma} \theta^{2\tau} &= t^2 + u\theta + t\theta^2; \end{aligned}$$

and finally

$$\theta^{2\sigma} \theta^{2\tau} + \theta^{2\tau} \theta^{2\sigma} = -u.$$

Since we are viewing $\ell \hookrightarrow 0 \times \ell \times \ell$ as a $k \hookrightarrow \ell$ -module via the vertical maps in (6), the ℓ -module structure on $0 \times \ell \times \ell$ is given by $z \cdot (0, x, y) = (0, z^\sigma x, z^\tau y)$. Let $W := \ell \times \ell$ with the *usual* ℓ -module structure, and note that the map $\Phi : W \rightarrow 0 \times \ell \times \ell$ taking (x, y) to $(0, x^\sigma, y^\tau)$ is an ℓ -module isomorphism. Thus we can simply replace the $k \hookrightarrow \ell$ -module $\ell \hookrightarrow 0 \times \ell \times \ell$ by the more tractable $k \hookrightarrow \ell$ -module $\varepsilon : \ell \hookrightarrow W$, where the map ε takes z to $\Phi^{-1}((0, z, z)) = (z^\tau, z^\sigma)$.

We have thus replaced our $k \hookrightarrow \ell$ -module by an isomorphic copy $V \hookrightarrow W$, where V is the k -subspace of W spanned by the columns of the matrix

$$X := \begin{pmatrix} 1 & \theta^\tau & \theta^{2\tau} \\ 1 & \theta^\sigma & \theta^{2\sigma} \end{pmatrix}.$$

Note that we can do column operations over k without changing $V \hookrightarrow W$; we can also do row operations over ℓ without changing the isomorphism class of $V \hookrightarrow W$. Using row operations over ℓ , we replace X by

$$X' := \begin{pmatrix} 1 & 0 & -\theta^\sigma \theta^\tau \\ 0 & 1 & \theta^\sigma + \theta^\tau \end{pmatrix} = \begin{pmatrix} 1 & 0 & -t - \theta^2 \\ 0 & 1 & -\theta \end{pmatrix}.$$

Now using column operations over k , we can replace X' by the matrix

$$X'' := \begin{pmatrix} 1 & 0 & \theta \\ 0 & 1 & \theta^2 \end{pmatrix}.$$

Thus we may assume that V is generated by the columns of X'' .

Suppose φ is an endomorphism of $V \hookrightarrow W$. By Lemma 7 we have $\varphi X'' = X''\lambda$, where

$$\lambda = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

is a 3-by-3 matrix over k . Use the first two columns of X'' to get

$$\varphi = \begin{pmatrix} a + c\theta & d + f\theta \\ b + c\theta^2 & e + f\theta^2 \end{pmatrix}.$$

Now the last column of X'' gives

$$\varphi((\theta, \theta^2)^T) = \begin{pmatrix} fu + (a - ft)\theta + (c + d)\theta^2 \\ cu + (b - ct + fu)\theta + (e - ft)\theta^2 \end{pmatrix}.$$

This vector must have the form $(g + j\theta, h + j\theta^2)^T$. Thus $a = e$, $b = ct - fu$, and $d = -c$. Conversely, the validity of these equations implies that φ is an endomorphism of $V \hookrightarrow W$ (by Lemma 7 again). Now φ has the form

$$\varphi = \begin{pmatrix} e + c\theta & -c + f\theta \\ ct - fu + c\theta^2 & e + f\theta^2 \end{pmatrix}.$$

Set $\varepsilon := e - ft - c\theta - f\theta^2$. We claim that the eigenvalues of φ are precisely ε^σ and ε^τ . In other words, $\varepsilon^\sigma + \varepsilon^\tau$ is the trace of φ and $\varepsilon^\sigma \varepsilon^\tau$ is the determinant of φ . The trace of φ is $2e + c\theta + f\theta^2$ and the determinant of φ is

$$(e^2 + c^2t - cfu) + (ec - cft + f^2u)\theta + (ef + c^2)\theta^2.$$

At this point we'll use the relations in (7) to verify the claim directly.

First, we have

$$\begin{aligned} \varepsilon^\sigma + \varepsilon^\tau &= (e - ft - c\theta^\sigma - f\theta^{2\sigma}) + (e - ft - c\theta^\tau - f\theta^{2\tau}) \\ &= 2e - 2ft - c(\theta^\sigma + \theta^\tau) - f(\theta^{2\sigma} + \theta^{2\tau}) \\ &= 2e - 2ft - c(-\theta) - f(-2t - \theta^2) \\ &= 2e + c\theta + f\theta^2 \end{aligned}$$

and hence $\varepsilon^\sigma + \varepsilon^\tau$ is the trace of φ . Next, $\varepsilon^\sigma \varepsilon^\tau$ is equal to

$$\begin{aligned} (e - ft)^2 - c(e - ft)(\theta^\sigma + \theta^\tau) - f(e - ft)(\theta^{2\sigma} + \theta^{2\tau}) \\ + c^2(\theta^\sigma \theta^\tau) + cf(\theta^{2\sigma} \theta^\tau + \theta^{2\tau} \theta^\sigma) + f^2(\theta^{2\sigma} \theta^{2\tau}), \end{aligned}$$

and in turn is equal to

$$\begin{aligned} (e - ft)^2 - c(e - ft)(-\theta) - f(e - ft)(-2t - \theta^2) \\ + c^2(t + \theta^2) + cf(-u) + f^2(t^2 + u\theta + t\theta^2). \end{aligned}$$

Collecting coefficients gives us

$$\begin{aligned} & ((e - ft)^2 + 2eft - 2f^2t^2 + c^2t - cfu + f^2t^2) \\ & + (c(e - ft) + f^2u)\theta + (f(e - ft) + c^2 + f^2t)\theta^2, \end{aligned}$$

and hence $\varepsilon^\sigma \varepsilon^\tau$ is equal to the determinant of φ , as claimed.

Note that e can be made to equal any given element of ℓ by choosing c , e and f correctly. Thus the delta group Δ consists of the images of $\delta^\sigma \delta^\tau$ as δ ranges over all elements of ℓ^\times . We claim this image is equal to $(\ell^\times)^2$.

Let $q := |D/pD| = |k|$. After swapping σ and τ if necessary, we may assume that $\delta^\sigma = \delta^q$ and $\delta^\tau = \delta^{q^2}$. Then $\delta^\sigma \delta^\tau = \delta^{q^2+q} = (\delta^{(q^2+q)/2})^2 \in (\ell^\times)^2$. Conversely, let ξ be a generator of ℓ^\times . We want to find $\delta \in \ell^\times$ so that $\delta^\sigma \delta^\tau = \xi^2$. The order of ℓ^\times is $q^3 - 1$ and thus it suffices to find an integer t so that (with $\delta := \xi^t$)

$$q(q+1)t \equiv 2 \pmod{(q-1)(q^2+q+1)}.$$

If q is odd, one can easily check that $q(\frac{q+1}{2})$ and $(\frac{q-1}{2})(q^2+q+1)$ are relatively prime. If q is even one easily checks that $q(q+1)$ and q^3-1 are relatively prime. \square

Proposition 30 leads us to another partial result on cancellation for cubic orders.

Theorem 31. *Keep the notation and assumptions above. Suppose $d = 3$ and $p\mathcal{O}$ is a prime ideal. Then cancellation holds for $R := D + p\mathcal{O}$ if and only if $(D/pD)^\times \cdot \Lambda_R = (\mathcal{O}/p\mathcal{O})^\times$ and $((\mathcal{O}/p\mathcal{O})^\times)^2 \cdot \Lambda_R = (\mathcal{O}/p\mathcal{O})^\times$.*

Proof. Suppose $k^\times \cdot \Lambda_R = \ell^\times$ and $(\ell^\times)^2 \cdot \Lambda_R = \ell^\times$, where $k := D/pD$ and $t = \mathcal{O}/p\mathcal{O}$. By Lemma 29 and Proposition 30 above, the delta subgroup of every indecomposable $k \hookrightarrow \ell$ -module contains either k^\times or $(\ell^\times)^2$. By Lemma 10, the same holds for $k \hookrightarrow \ell$ -module, indecomposable or not. By Proposition 15 cancellation holds.

Conversely, suppose $(\ell^\times)^2 \cdot \Lambda_R \neq \ell^\times$. Since the $k \hookrightarrow \ell$ -module $V \hookrightarrow W$ of constant rank 2 constructed in Proposition 30 has $\Delta = (\ell^\times)^2$, cancellation fails by Proposition 15. Finally, suppose $k^\times \cdot \Lambda_R \neq \ell^\times$. The pair $k \hookrightarrow \ell$ itself has its delta group equal to k^\times and again cancellation fails by Proposition 15. \square

If $k^\times \cdot \Lambda_R \neq \ell^\times$ then by results in [32] there exists an invertible ideal I of R such that $I \oplus \mathcal{O} \cong R \oplus \mathcal{O}$ but $I \not\cong R$. This situation gives us a somewhat boring failure of cancellation. However, we will show in Section 8 that there exist orders R as above such that $k^\times \cdot \Lambda_R = \ell^\times$ and $(\ell^\times)^2 \cdot \Lambda_R \neq \ell^\times$ (see Example 33).

In the cases where $d = 3$ and $p\mathcal{O}$ is not prime one can probably carry out an analysis similar to the one above and obtain an explicit condition for cancellation to hold for $R = D + p\mathcal{O}$. However, such an analysis still remains to be completed. Finally, we remark that explicit conditions which settle the $d = 2$ case appeared in [32].

8. Examples

Here is an example of a cubic order $R := \mathbb{Z} + p\mathcal{O}$ having the property that all units of $\mathcal{O}/p\mathcal{O}$ are liftable. The cubic order R in the following example has finite representation type, by Proposition 19.

Example 32. Let θ be a root of the polynomial $f(x) := x^3 + x + 1$ and let $K := \mathbb{Q}(\theta)$. This K corresponds to the complex cubic number field of discriminant -31 which appears in [18, Table 3.2]. Let \mathcal{O} be the ring of integers of K . The table shows that $\mathcal{O} = \mathbb{Z}[\theta]$. Also, the table gives $\varepsilon := \theta$ as a fundamental unit.

Take $p := 2$ and let ξ denote the image of θ in $\mathcal{O}/p\mathcal{O}$. Let Λ be the image of \mathcal{O}^\times in $\mathcal{O}/p\mathcal{O}$. We claim $\Lambda = (\mathcal{O}/p\mathcal{O})^\times$. The polynomial f is irreducible modulo 2 and thus $p\mathcal{O}$ is prime by [18, Chapter 6, (2.27)]. Hence $\mathcal{O}/p\mathcal{O}$ is a finite field \mathbb{F} with 8 elements. Since ξ is nontrivial in \mathbb{F}^\times it necessarily generates \mathbb{F}^\times . This proves the claim. Finally, let $R := \mathbb{Z} + p\mathcal{O}$. By Proposition 15, cancellation holds for R since $\Lambda = (\mathcal{O}/p\mathcal{O})^\times$.

By the way, one can show directly that the image of \mathcal{O}^\times in $(\mathcal{O}/p^2\mathcal{O})^\times$ has order 28, whereas $(\mathcal{O}/p^2\mathcal{O})^\times$ itself has order 56. Thus $\mathcal{O}/p^2\mathcal{O}$ has units which do not lift to \mathcal{O}^\times even though all units of $\mathcal{O}/p\mathcal{O}$ lift to \mathcal{O}^\times .

In the example above we obtained cancellation for R “cheaply” since all the units of $\mathcal{O}/p\mathcal{O}$ were liftable—a condition which can arise only if p is small enough (see [12, Corollary 7.1]). Example 34 below is much more typical.

Our next two examples involve more cubic orders R of the form $\mathbb{Z} + p\mathcal{O}$. In the next example, we show how cancellation can fail for R even when the map $\text{Pic}(R) \rightarrow \text{Pic}(\mathcal{O})$ is injective. This example stands in sharp contrast with the quadratic orders Q studied in [32], where it is shown that the injectivity of $\text{Pic } Q \rightarrow \text{Pic } \mathcal{O}$ is equivalent to cancellation holding for Q .

Example 33. As in the previous example, let θ be a root of the polynomial $f(x) = x^3 + x + 1$ and let $K := \mathbb{Q}(\theta)$. From [18, Table 3.2] we find $\mathcal{O} = \mathbb{Z}[\theta]$ and θ is a fundamental unit. It follows that \mathcal{O}^\times is generated by -1 and θ .

Take $p = 5$ and let Λ denote the image of \mathcal{O}^\times in $\mathcal{O}/p\mathcal{O}$. Since f is irreducible modulo 5, it follows from [18, Chapter 6, (2.27)] that $p\mathcal{O}$ is a prime ideal. Set $k := \mathbb{Z}/p\mathbb{Z}$ and $\ell := \mathcal{O}/p\mathcal{O}$. Let ξ be the image of θ in $\mathcal{O}/p\mathcal{O}$.

We have $|\ell^\times| = 31 \cdot 4$ and, by a direct computation, the image Λ of the subgroup generated by -1 and ξ in ℓ^\times has index 2. Thus $\Lambda = (\ell^\times)^2$ and hence $(\ell^\times)^2 \cdot \Lambda \neq \ell^\times$. By Theorem 31, cancellation fails for $R := \mathbb{Z} + p\mathcal{O}$. However, $k^\times \cdot \Lambda = \ell^\times$ since k^\times has a nonsquare. From the Mayer–Vietoris exact sequence (see [16])

$$1 \rightarrow R^\times \rightarrow (R/\mathfrak{c}_R)^\times \times \mathcal{O}^\times \rightarrow (\mathcal{O}/\mathfrak{c}_R)^\times \rightarrow \text{Pic}(R) \rightarrow \text{Pic}(\mathcal{O}) \rightarrow 1$$

it follows that $\text{Pic}(R) \rightarrow \text{Pic}(\mathcal{O})$ is injective.

This time we show how cancellation can hold for an order even in the presence of nonliftable units. By Theorem 26, it is necessary that the number field containing the order under consideration has degree at most 3.

Example 34. Keep the same setup from Example 33 but take $p = 59$; then $p\mathcal{O}$ is a prime ideal. Again, set $k := \mathbb{Z}/p\mathbb{Z}$ and $\ell := \mathcal{O}/p\mathcal{O}$. The order of $\ell^\times := (\mathcal{O}/p\mathcal{O})^\times$ is $3541 \cdot 29 \cdot 2$. A direct computation shows the image Λ of the subgroup generated by -1 and ξ in ℓ^\times has order $3541 \cdot 2$. Since $|(k^\times)^2| = 29$ and $\gcd(29, 3541 \cdot 2) = 1$ it follows that $(k^\times)^2 \cdot \Lambda = \ell^\times$ and thus $k^\times \cdot \Lambda = (\ell^\times)^2 \cdot \Lambda = \ell^\times$. By Theorem 31, cancellation holds for $R := \mathbb{Z} + p\mathcal{O}$, even though $\mathcal{O}/p\mathcal{O}$ has nonliftable units.

Acknowledgment

The author thanks Roger Wiegand for his assistance and guidance while the author's research was in progress.

References

- [1] H. Bass, On the ubiquity of Gorenstein rings, *Math. Z.* 82 (1963) 8–28.
- [2] H. Bass, *Algebraic K-Theory*, Benjamin, New York–Amsterdam, 1968.
- [3] S.M. Bhatwadekar, A. Roy, Some cancellation theorems about projective modules over polynomial rings, *J. Algebra* 111 (1) (1987) 166–176.
- [4] S.U. Chase, Torsion-free modules over $K[x, y]$, *Pacific J. Math.* 12 (1962) 437–447.
- [5] E.C. Dade, Some indecomposable group representations, *Ann. of Math.* (2) 77 (1963) 406–412.
- [6] Ju.A. Drozd, A.V. Roĭter, Commutative rings with a finite number of indecomposable integral representations, *Izv. Akad. Nauk. SSSR Ser. Mat.* 31 (1967) 783–798, in Russian.
- [7] E.G. Evans Jr., Krull–Schmidt and cancellation over local rings, *Pacific J. Math.* 46 (1973) 115–121.
- [8] R.M. Guralnick, L.S. Levy, Cancellation and direct summands in dimension 1, *J. Algebra* 142 (2) (1991) 310–347.
- [9] R.M. Guralnick, L.S. Levy, R.B. Warfield Jr., Cancellation counterexamples in Krull dimension 1, *Proc. Amer. Math. Soc.* 109 (2) (1990) 323–326.
- [10] N. Jacobson, *Lectures in Abstract Algebra*, vol. II, Van Nostrand, Princeton, NJ, 1964.
- [11] N. Jacobson, *Lectures in Abstract Algebra*, vol. III, Van Nostrand, Princeton, NJ, 1964.
- [12] R. Karr, Failure of cancellation for quartic and higher-degree orders, *J. Algebra Appl.*, in press.
- [13] N. Mohan Kumar, M.P. Murty, A. Roy, A cancellation theorem for protective modules over finitely generated rings, in: *Algebraic Geometry and Commutative Algebra*, vol. I, Kinokuniya, Tokyo, 1988, pp. 281–287.
- [14] S. Lang, *Algebra*, 3rd Edition, Addison–Wesley, 1993.
- [15] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, Cambridge, UK, 1989.
- [16] J. Milnor, *Introduction to Algebraic K-Theory*, Princeton University Press, Princeton, NJ, 1971.
- [17] M.P. Murty, R. Swan, Vector bundles over affine surfaces, *Invent. Math.* 36 (1976) 125–165.
- [18] M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, UK, 1989.
- [19] D. Quillen, Projective modules over polynomial rings, *Invent. Math.* 36 (1976) 167–171.
- [20] P. Samuel, About Euclidean rings, *J. Algebra* 19 (1971) 282–301.
- [21] J.-P. Serre, Faisceaux algébriques cohérents, *Ann. of Math.* (2) 61 (1955) 197–278, in French.
- [22] A.A. Suslin, The cancellation problem for projective modules, and related questions, in: *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)*, Acad. Sci. Fennica, Helsinki, 1980, pp. 323–330, in Russian.
- [23] A.A. Suslin, Projective modules over polynomial rings are free, *Dokl. Akad. Nauk SSSR* 229 (5) (1976) 1063–1066, in Russian.
- [24] R. Swan, Failure of cancellation for direct sums of line bundles, *Trans. Amer. Math. Soc.* 336 (2) (1993) 581–605.
- [25] R. Swan, Torsion free cancellation over orders, *Illinois J. Math.* 32 (3) (1988) 329–360.

- [26] R. Swan, Serre's problem, in: Conference on Commutative Algebra, 1975 (Queen's Univ., Kingston, ON, 1975), in: Queen's Papers on Pure and Applied Math., vol. 42, 1975, pp. 1–60.
- [27] R. Swan, A cancellation theorem for projective modules in the metastable range, *Invent. Math.* 27 (1974) 23–43.
- [28] W.V. Vasconcelos, Ideals and cancellation, *Math. Z.* 102 (1967) 353–355.
- [29] W.V. Vasconcelos, On local and stable cancellation, *An. Acad. Brazil. Ciênc.* 37 (1965) 389–393.
- [30] E. Weiss, *Algebraic Number Theory*, McGraw–Hill, New York, 1963.
- [31] R. Wiegand, Noetherian rings of bounded representation type, in: *Commutative Algebra, Proceedings of a Microprogram (June 15–July 2, 1987)*, Springer-Verlag, New York, 1989, pp. 497–516.
- [32] R. Wiegand, Cancellation over commutative rings of dimension one and two, *J. Algebra* 88 (1984) 438–459.
- [33] R. Wiegand, S. Wiegand, Bounds for one-dimensional rings of finite Cohen–Macaulay type, *J. Pure Appl. Algebra* 93 (1994) 311–342.
- [34] R. Wiegand, S. Wiegand, Stable isomorphism of modules over one-dimensional rings, *J. Algebra* 107 (1987) 425–435.
- [35] A. Weimers, Cancellation properties of projective modules over Laurent polynomial rings, *J. Algebra* 156 (1) (1993) 108–124.