2009

Algebras Having Bases Consisting Entirely of Units

Jeremy Moore
Otterbein University, JMoore@otterbein.edu

Contemporary Mathematics
Volume 499, 2009

Algebras Having Bases Consisting Entirely of Units

Sergio López-Permouth, Jeremy Moore, and Steve Szabo

ABSTRACT. We introduce a hierarchy of notions about algebras having a basis $\mathcal{B}$ consisting entirely of units. Such a basis is called an invertible basis and algebras that have invertible bases are said to be invertible algebras. The other conditions considered in the said hierarchy include the requirement that for an invertible basis $\mathcal{B}$, the set of inverses $\mathcal{B}^{-1}$ be itself a basis, the notion that $\mathcal{B}$ be closed under inverses and the idea that $\mathcal{B}$ be closed under products. It is shown that the last property is unique of group rings. Many examples are considered and it is determined that the hierarchy is for the most part strict. For any field $F \neq F_2$, all semisimple F-algebras are invertible. Semisimple invertible F_2-algebras are fully characterized. Likewise, the question of which single-variable polynomials over a field yield invertible quotient rings of the F-algebra $F[x]$ is completely answered. Connections between invertible algebras and S-rings (rings generated by units) are also explored.

1. Introduction

If an algebra A over a (not necessarily commutative) ring R has a basis $\mathcal{B}$ consisting entirely of units then we say that $\mathcal{B}$ is an invertible basis and A is an invertible R-algebra. The archetypes of this notion are group rings and field extensions. The purpose of this paper is to initiate the study of invertible algebras.

Note that throughout this paper the definition of an algebra A over R will only require that for $r \in R, a, b \in A, r(ab) = (ra)b$ and not the common additional requirement that $r(ab) = a(rb)$ which makes the action of R on A ambidextrous. We do this to allow group rings RG and matrix rings $M_n(R)$ over a non-commutative ring R to be R-algebras. In lieu of this requirement we sometimes focus on bases $\mathcal{B}$ such that R commutes with the elements of $\mathcal{B}$, a property that does hold for RG with basis $\mathcal{B} = G$ and for matrix rings $M_n(R)$ with, for example, the (non-invertible) standard basis $\mathcal{B}$ consisting of the unit matrices. So, in principle, the algebras considered in this paper are free as left modules and all bases considered are, in fact, *left* bases.

For terminology and basic results on group rings, the reader is pointed in the direction of the standard references [5] and [6].

We start out by introducing a hierarchy of properties (invertible-2, invertible-3, and invertible-4) that strengthen the notion of invertibility and show that, for the most part, the hierarchy is strict (Section 2). Exploring the possibility that an invertible basis may be closed under products leads us to show that such property is unique of group rings. In turn, that result yields an alternative proof of results

of Mabry [4] and Kuczma [3] stating that Hamel bases of proper field extensions are not multiplicatively closed.

In the case when R is a field, invertible algebras are S-rings in the sense of [7], i.e. a ring in which every element can be expressed as the sum of units. In fact, it is not hard to see that invertible algebras over S-rings are themselves S-rings; this is the content of Proposition 2.2.

In Section 3 we study the behavior of the various invertibility properties with respect to standard constructions such as direct sums and rings of matrices, and conclude that with few exceptions, semisimple algebras are invertible. Also in Section 3 we characterize those single-variable polynomials over a field which induce invertible quotient rings.

2. Definitions and Preliminary Results

A group ring $A = RG$ is an R-algebra exhibiting the interesting property of having a basis $\mathcal{B} = G$ whose every element is invertible. Similarly, if $A = E$ is a field extension (or even a division ring extension) of a field $R = F$ then any basis of E over F consists entirely of units. That property reasonably leads to the following definition.

DEFINITION 2.1. Given an algebra A over a ring R, an *invertible basis* $\mathcal{B}$ is an R-basis $\mathcal{B}$ such that each element of $\mathcal{B}$ is invertible in A. If A has an invertible basis, A is called an *invertible algebra.*

It is easy to see that not all algebras are invertible, even when they are free R modules. Consider, for example, the polynomial ring $A = F[x]$ over an arbitrary field F or, for a finite dimensional example, $A = F_2 \oplus F_2$ which has dimension 2 as a free module over F_2 but only one invertible element.

The purpose of this paper is to investigate the basic properties of invertible algebras over rings and fields.

We notice that in the case $R = F$ is a field, every invertible F-algebra A is an S-ring (see the Introduction). Notice, however that $\mathbb{Z}$ is not an invertible algebra over any field, yet $\mathbb{Z}$ is an S-ring. So, we extend our observation as follows.

PROPOSITION 2.2. *An invertible algebra A over an S-ring R is itself an S-ring.*

PROOF. Straightforward from the definitions. □

A group ring also satisfies the property that the collection $\mathcal{B}^{-1}$ of inverses of the elements of the basis $\mathcal{B} = G$ equals G. This motivates the remaining three definitions in this section.

DEFINITION 2.3. Given an algebra A over a ring R, an *invertible-2 basis* is an invertible R-basis $\mathcal{B}$ such that the collection $\mathcal{B}^{-1}$ of the inverses of the elements of $\mathcal{B}$ also constitutes a basis. If A has an invertible-2 basis, A is called an *invertible-2 algebra.*

PROPOSITION 2.4. *Let $F \subset E$ be a finite degree field extension, i.e. $|E : F| < \infty$. Then there is a basis $\mathcal{B}$ for E over F such that $\mathcal{B}$ is invertible-2.*

PROOF. Since $|E : F| < \infty$, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for $\alpha_i \in E$ such that $F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}) \neq F(\alpha_1, \alpha_2, \ldots, \alpha_i)$. Let $\mathcal{B}_i = \{\alpha_i, \alpha_i^2, \ldots, \alpha_i^{k_i}\}$ be a basis for the extension $F(\alpha_1, \alpha_2, \ldots, \alpha_i)$ over $F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$. Then $\mathcal{B} = \{\alpha_1^{j_1}\alpha_2^{j_2}\ldots\alpha_n^{j_n} | 1 \leq$

$j_i \leq k_i\}$ is a basis for E over F. Let $\mathcal{B}^{-1} = \{\alpha_1^{-j_1}\alpha_2^{-j_2}\dots\alpha_n^{-j_n} | 1 \leq j_i \leq k_i\}$. Consider $\sum_{\lambda\in\mathcal{B}^{-1}} \beta_\lambda \lambda = 0$. Multiplying by $\alpha_1^{k_1}\alpha_2^{k_2}\dots\alpha_n^{k_n}$ gives $\sum_{\lambda\in\mathcal{B}} \beta_\lambda \lambda = 0$ which shows $\mathcal{B}^{-1}$ is a linearly independent set. Since $|\mathcal{B}^{-1}| = |\mathcal{B}|$, $\mathcal{B}^{-1}$ is a basis and thus $\mathcal{B}$ is an invertible-2 basis. □

Next, we introduce two other properties of group rings that invertible algebras may or may not have in general.

DEFINITION 2.5. Given an algebra A over a ring R, an *invertible-3 basis* is an invertible R-basis $\mathcal{B}$ such that $\mathcal{B}$ is closed under inverses. If A has an invertible-3 basis, A is called an *invertible-3 algebra.* Notice that if $\mathcal{B}$ is an invertible-3 basis then it follows easily that $\mathcal{B} = \mathcal{B}^{-1}$.

LEMMA 2.6. *Let A be an invertible algebra. Then A has an invertible basis $\mathcal{B}$ with $1 \in \mathcal{B}$.*

PROOF. Let $\mathcal{A} = \{v_1, v_2, \dots, v_n, \dots\}$ be an invertible basis for A. Now multiply each element of $\mathcal{A}$ by v_1^{-1} to obtain a new set $\mathcal{B}$ containing 1. Let $w \in A$. Then $wv_1 = \sum_{j=1}^m \alpha_j v_j$. Multiply by v_1^{-1} to obtain $w = \sum_{j=1}^m \alpha_j v_j v_1^{-1}$. Therefore, any element in A can be represented as a linear combination of elements from $\mathcal{B}$. Let $\sum_i \alpha_i v_i v_1^{-1} = 0$. Then multiplying by v_1 we get $\sum_i \alpha_i v_i = 0$ which implies that $\alpha_i = 0$ for all i as $\mathcal{A}$ is a basis. Therefore $\mathcal{B}$ is a linearly independent set and thus a basis. □

While, by the previous lemma, the existence of an invertible basis guarantees the existence of an invertible basis containing 1 the same is not true in general of invertible-3 bases, (see Example 2.9). For that reason we coin the following definition.

DEFINITION 2.7. Given an algebra A over a ring R, an *invertible-4 basis* is an invertible-3 R-basis which includes the identity. If A has an invertible-4 basis, A is called an *invertible-4 algebra.*

The following hierarchy for algebras is obvious.

group rings $\subset$ invertible-4 $\subset$ invertible-3 $\subset$ invertible-2 $\subseteq$ invertible

The following three examples show that the first three inclusions are indeed proper. However, while we show below an algebra with an invertible base that is not invertible-2, we do not know yet an invertible algebra which is not invertible-2. That is the subject of our fourth example below.

EXAMPLE 2.8 (Invertible-4 not Group Algebra). Consider $A = \frac{F_2[x,y]}{\langle x,y\rangle^2}$. Then A has 4 invertible elements, namely $\{1, 1+x, 1+y, 1+x+y\}$. To form an invertible-4 basis, $\mathcal{B}$, we must have $1 \in \mathcal{B}$. Therefore, we must have two of the other three remaining invertible elements. Since $(1+x)(1+y) = (1+x+y)$ we see that any invertible-4 basis we form cannot be closed under products.

EXAMPLE 2.9 (Invertible-3 not Invertible-4). Consider $A = \frac{F_3[x]}{\langle x^2\rangle}$. Then the group of units of A is $U(A) = \{1, -1, 1+x, 1-x, -1+x, -1-x\}$. Now, $\mathcal{B} = \{1+x, 1-x\}$ is an invertible-3 basis for A over F. Hence, A is invertible-3. Since a basis contains two elements and an invertible-4 basis contains the identity, if A had an invertible-4 basis, it would have two elements $\{1, a\}$ where a is self-invertible. Besides the identity, -1 is the only self-invertible element. Since $\{1, -1\}$ does not form a basis, A is not invertible-4.

EXAMPLE 2.10 (Invertible-2 not Invertible-3). Consider $A = \frac{F_3[x,y]}{\langle x,y\rangle^2}$. Let $U(A)$ be the group of units of A. Then $U(A) = \{\alpha+\beta x+\gamma y \mid \alpha,\beta,\gamma \in F_3, \alpha \neq 0\}$. Note that for $a = \alpha+\beta x+\gamma y \in U(A)$, $a^{-1} = (\alpha+\beta x+\gamma y)^{-1} = \alpha-\beta x-\gamma y$. An invertible-2 F-basis for A is $\{1+x, 1+y, 1+x+y\}$. So A is invertible-2. Let $\mathcal{B}$ be an invertible F-basis for A. Assume $a \in \mathcal{B} \cap F$. We know $a^{-1} = ba$ for some $b \in F$. So, any invertible-3 basis for A does not have constants in it. Since non-constant units are not self-invertible in A, any invertible-3 basis for A has an even number of elements. Since $|\mathcal{B}| = 3$ it cannot be invertible-3. Hence, A is not invertible-3

The following example guarantees the existence of invertible bases that are not invertible-2.

EXAMPLE 2.11. Let F be an algebraic extension of a finite field. Consider the F-algebra $A = F(x)$ of rational functions as a sub-algebra of the field of formal Laurent series $F((x))$. By Corollary 2.3 of [1], A consists precisely of those Laurent series that are (eventually) periodic. Since a periodic power series is of the form $\frac{p(x)}{1-x^j} = p(x)(1+x^j+x^{2j}+\cdots)$ for $p(x)$ a polynomial of degree less than j, where $j \in \mathbb{Z}^+$, then periodic power series are linear combinations of elements of the form $\frac{x^i}{1-x^j}$ with $0 \leq i < j$. It follows that eventually periodic Laurent series are generated by $\mathcal{G} = \{x^k \mid k \in \mathbb{Z}\} \cup \{\frac{x^i}{1-x^j} \mid j \in \mathbb{Z}^+, 0 \leq i \leq j-1\}$. Notice, however, that $\mathcal{G}^{-1} \subset F[x,x^{-1}]$ (the ring of Laurent polynomials). In particular, $\mathcal{G}^{-1}$ does not generate A. Any basis $\mathcal{B}$ contained in $\mathcal{G}$ will be an invertible basis that is not invertible-2.

An alternate direction in which to explore properties of a group ring RG is by considering the fact that G is an invertible basis which is closed under products. It turns out that this property completely characterizes group rings.

PROPOSITION 2.12. *If the R-algebra A has an invertible basis $\mathcal{B}$ which is closed under products then $\mathcal{B}$ is a group G. If, in addition, R commutes with $\mathcal{B}$ then A is a group ring.*

PROOF. Let A have basis $\mathcal{B} = \{v_1, \ldots, v_n, \ldots\}$. Then $\sum_k \alpha_k v_k = 1$. Let $v \in \mathcal{B}$. Then multiply through by v. So we have $\sum_k \alpha_k v_k v = v$. But each $v_k v \in \mathcal{B}$ as $\mathcal{B}$ is closed under products. Therefore there exists i such that $\alpha_k = 0$ for all $k \neq i$ and $v_i = 1$. Thus $1 \in \mathcal{B}$.

Now let $v \in \mathcal{B}$. We claim $v^{-1} \in \mathcal{B}$. Let $\sum_k \alpha_k v_k = v^{-1}$. Multiply through by v to obtain $\sum_k \alpha_k v_k v = 1$. Then there exists i such that $\alpha_k = 0$ for all $k \neq i$ and $v_i = v^{-1}$. But $v_i \in \mathcal{B}$ and so $v^{-1} \in \mathcal{B}$. Therefore $\mathcal{B}$ is a group. □

Proposition 2.12 has as a corollary which strengthens a result about field extensions reported in [3] for reals over rationals and in general in [4]. Namely, Corollary 2.13 extends the result that no proper field extension has a basis that is closed under multiplication.

COROLLARY 2.13. *If a simple ring A is an invertible R-algebra with invertible basis $\mathcal{B} \neq 1$ then $\mathcal{B}$ is not closed under products.*

PROOF. If such a basis existed then A would be a group algebra over R by the above Proposition. But then A would have a proper ideal I (the augmentation ideal). □

3. General Results and Some Families of Invertible Algebras

In this section we study the behavior of the invertibility properties with respect to standard constructions such as matrix rings and direct sums. We then apply those results to characterize certain families of invertible algebras.

PROPOSITION 3.1. *Let R be an arbitrary ring and $n \in \mathbb{Z}^+$. Then $M_n(R)$ is invertible-2 over R.*

PROOF. Consider the following: Let v_{nn} be the identity matrix and $\mathcal{A} = \{e_{ij} | i, j = 1, \ldots, n\}$ where e_{ij} is the matrix unit with 1 in the $i^{th}j^{th}$ coordinate and zeros elsewhere. For $i \neq j$, let $v_{ij} = v_{nn} + e_{ij}$. For $1 \leq i \leq n-2$, let $v_{ii} = v_{nn} + \sum_{l=i+1}^{n} e_{l,i+1+(l-i) \pmod{n-i}} - e_{ll}$. Let $v_{n-1,n-1} = v_{nn} - e_{nn} + e_{n-1,n} + e_{n,n-1}$. Now let $\mathcal{B} = \{v_{ij} | i, j = 1, \ldots, n\}$. It is easy to see that $\mathcal{B}$ spans $\mathcal{A}$. We will show that $\mathcal{B}$ is also linearly independent. Let $\sum_{i,j=1}^{n} \alpha_{ij} v_{ij} = 0$. Now $\alpha_{i1} = \alpha_{1i} = 0$ for $i = 2, \ldots, n$. As there is only one element with a 1 in each of these coordinates. Similarly we have $\alpha_{il} = 0$ for $2 \leq l \leq n-2$, and $i = l+1, \ldots, n-1$ and $\alpha_{kj} = 0$ for $2 \leq k \leq n-2$, and $j = k+2, \ldots, n$. The diagonal coordinates from the positions $nn, \ldots, 22$ give the following equations

$$\sum_{i \neq j} \alpha_{ij} + \alpha_{nn} = 0,$$

$$\sum_{i \neq j} \alpha_{ij} + \alpha_{n-1,n-1} + \alpha_{nn} = 0,$$

$$\vdots$$

$$\sum_{i \neq j} \alpha_{ij} + \sum_{k=1}^{n} \alpha_{kk} = 0.$$

These equations imply $\alpha_{ii} = 0$ for $i = 1, 2, \ldots, n-1$. Then $\alpha_{n,i+1} + \alpha_{ii} = 0$ for $i = 1, 2, \ldots, n-2$ gives $\alpha_{n,i+1} = 0$ for $i = 1, 2, \ldots, n-2$. Also for $k = 2, \ldots, n-2$ we have $\alpha_{k,k+1} + \sum_{i=1}^{k-1} \alpha_{ii} = 0$. Since $\alpha_{ii} = 0$ for $i = 1, 2, \ldots, n-1$ we have $\alpha_{k,k+1} = 0$ for $k = 2, \ldots, n-2$. For the $n-1, n$ and $n, n-1$ coordinates we obtain the equations

$$\alpha_{n-1,n} + \sum_{i=1}^{n-1} \alpha_{ii} = 0,$$

$$\alpha_{n,n-1} + \alpha_{n-2,n-2} + \alpha_{n,n-1} = 0.$$

Therefore, $\alpha_{n-1,n} = \alpha_{n,n-1} = 0$. Finally from the 1, 1 position we have the equation $\sum_{i,j=1}^{n} \alpha_{ij} = 0$, and since all entries are zero except for α_{nn} we conclude $\alpha_{nn} = 0$. Hence, $\mathcal{B}$ is an R-basis for $M_n(R)$.

Now we have the inverses for v_{ij} are as follows. If $i \neq j$ then $v_{ij}^{-1} = v_{nn} - e_{ij}$. If $i = j$ and $i < n-1$ then $v_{ij}^{-1} = v_{ij}^{T}$. Also $v_{n-1,n-1}^{-1} = v_{nn} - e_{n-1,n-1} + e_{n-1,n} + e_{n,n-1} - 2e_{nn}$. It is easy to see that these inverses form a basis also. □

The following example illustrates the bases for matrix rings introduced in Proposition 3.1.

EXAMPLE 3.2. For an arbitrary ring R, consider $M_3(R)$. Then $\mathcal{B}$ consists of:

$$v_{11} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad v_{12} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad v_{13} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$v_{21} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad v_{22} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad v_{23} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$v_{31} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad v_{32} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad v_{33} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and $\mathcal{B}^{-1}$ consists of:

$$v_{11}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad v_{12}^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad v_{13}^{-1} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$v_{21}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad v_{22}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{bmatrix} \quad v_{23}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$v_{31}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \quad v_{32}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} \quad v_{33}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

PROPOSITION 3.3. *Let T be invertible over S and S invertible over R. Then T is invertible over R. If furthermore S invertible-2 (respectively, invertible-3 or invertible-4) over R and,in addition, T has an invertible-2 (respectively, invertible-3 or invertible-4) basis $\mathcal{A}$ such that S commutes with $\mathcal{A}$ then T is invertible-2 (respectively, invertible-3 or invertible-4) over R.*

PROOF. Let $\mathcal{A} = \{a_i | i \in I\}$ be an invertible basis for S over R and $\mathcal{B} = \{b_j | j \in J\}$ be an invertible basis for T over S. We claim $\mathcal{C} = \{a_i b_j | i \in I, j \in J\}$ is an invertible basis for T over R. Let $\sum_{i,j} \alpha_{ij} a_i b_j = 0$. Then $\sum_j (\sum_i \alpha_{ij} a_i) b_j = 0$. Then for all j we must have $\sum_i \alpha_{ij} a_i = 0$ since $\mathcal{B}$ is linearly independent over S. Then we must have $\alpha_{ij} = 0$ for all i and j since $\mathcal{A}$ is linearly independent over R. Therefore, $\mathcal{C}$ is a linearly independent set over R. Now let $x \in T$. Then $x = \sum_j \beta_j b_j$ where $\beta_j \in S$ and $b_j \in T$. Further, for each j we may write $\beta_j = \sum_i \alpha_{ij} a_{ij}$ where $\alpha_{ij} \in R$ and $a_{ij} \in S$. Then

$$x = \sum_j \beta_j b_j = \sum_j (\sum_i \alpha_{ij} a_{ij}) b_j = \sum_{i,j} \alpha_{ij} (a_{ij} b_j).$$

Therefore, $\mathcal{C}$ is a generating set. Since $\mathcal{C}$ consists of invertible elements, $\mathcal{C}$ is an invertible basis for T over R.

Assume now that the bases $\mathcal{A}$ and $\mathcal{B}$ above are in fact both invertible-2 and that S commutes with $\mathcal{A}$. Then, $\mathcal{A}^{-1}$ and $\mathcal{B}^{-1}$ are also bases. Furthermore, the basis obtained from them in the way $\mathcal{C}$ was obtained from $\mathcal{A}$ and $\mathcal{B}$ coincides with $\mathcal{C}^{-1}$ by virtue of the fact that the elements of $\mathcal{B}^{-1} \subset S$ commute with those in $\mathcal{A}$ and, consequently, with those in $\mathcal{A}^{-1}$. Therefore, $\mathcal{C}^{-1}$ is a also basis and therefore $\mathcal{C}$ is invertible-2.

The corresponding implications for the cases invertible-3 and invertible-4 follow similar reasonings.

□

PROPOSITION 3.4. *A simple finite dimensional algebra A over a field F has an invertible-2 basis.*

PROOF. Since A is simple and finite dimensional, there exists a finite dimensional division ring extension K of the field F and $A \cong M_n(K)$. Now apply Proposition 2.4 and Propositions 3.1 and 3.3. □

PROPOSITION 3.5. *Let A and B be finite dimensional invertible (invertible-2) algebras over a ring R such that there exists $x \in R$ such that x is invertible and $1-x$ is invertible. Then $C = A \oplus B$ is a finite dimensional invertible (invertible-2) algebra.*

PROOF. Let $\mathcal{A}$ and $\mathcal{B}$ be invertible bases for A and B respectively. Let

$$\mathcal{C} = (\mathcal{A}, b_1) \cup (a_1, \mathcal{B} \setminus \{b_1\}) \cup \{(a_1, xb_1)\}$$

for $a_1 \in \mathcal{A}$, $b_1 \in \mathcal{B}$ and $x \in R$ such that x is invertible and $1 - x$ is invertible. Clearly $\mathcal{C} \subset U(C)$. Consider

$$0 = \sum_{a \in \mathcal{A}} \alpha_a (a, b_1) + \sum_{b \in \mathcal{B} \setminus \{b_1\}} \beta_b (a_1, b) + \gamma (a_1, xb_1)$$

for $\alpha_a, \beta_b, \gamma \in R$. So,

$$(\sum_{a \in \mathcal{A}} \alpha_a + \gamma x) b_1 + \sum_{b \in \mathcal{B} \setminus \{b_1\}} \beta_b b = 0$$

and

$$(\alpha_{a_1} + \sum_{b \in \mathcal{B} \setminus \{b_1\}} \beta_b + \gamma) a_1 + \sum_{a \in \mathcal{A} \setminus \{a_1\}} \alpha_a a = 0.$$

By linear independence we have that for $a \in \mathcal{A} \setminus \{a_1\}$, $\alpha_a = 0$ and for $b \in \mathcal{B} \setminus \{b_1\}$, $\beta_b = 0$. Then

$$(\alpha_{a_1} + \gamma x) b_1 = 0$$

and

$$(\alpha_{a_1} + \gamma) a_1 = 0.$$

This implies $\alpha_{a_1} = \gamma = 0$ which shows $\mathcal{C}$ is a linearly independent set. Now we have

$$(\mathcal{A}, b_1) - [(1-x)^{-1}(a_1, b_1) - (1-x)^{-1}(a_1, xb_1)] = (\mathcal{A}, 0).$$

Therefore, we can generate anything of the form $(\mathcal{A}, 0)$ and thus generate $(0, \mathcal{B})$. Following the same argument above it can be shown that if A and B are invertible-2 then $\mathcal{C}$ is an invertible-2 basis. Therefore, $A \oplus B$ is invertible-2. □

Rings in which the identity is the sum of two units have appeared earlier in the literature. In particular, in [2], right self-injective rings in which the identity is the sum of two units are characterized as being precisely those right self-injective rings that do not have any quotient ring isomorphic to F_2.

PROPOSITION 3.6. *A finite direct sum of invertible algebras over a right self-injective ring R which does not have a factor ring isomorphic to F_2 is also an invertible algebra over R.*

Using Proposition 3.5, it can be shown that any finite direct sum of of algebras with a finite invertible basis will have a finite invertible basis. This leads to the following interesting Corollary.

COROLLARY 3.7. *Any finite dimensional semisimple algebra over a field $F \neq F_2$ is invertible.*

PROOF. A consequence of Lemma 3.4 and Proposition 3.5. □

REMARK 3.8. $F_2 \oplus F_2$ is a finite dimensional semisimple non-invertible algebra over F_2, showing that Corollary 3.7 cannot be extended further.

DEFINITION 3.9. An invertible F_2-algebra is *nice* if there exists an invertible basis containing a subset of an even number of elements whose sum is invertible.

LEMMA 3.10. *Let A be an invertible algebra over F_2. If there exists an invertible element $a \in A$ such that it is the sum of an even number of invertible elements from A then A does not have a factor ring isomorphic to F_2. In particular, nice invertible algebras do not have a factor ring isomorphic to F_2.*

PROOF. Assume A has an ideal I such that $\bar{A} = \frac{A}{I} \cong F_2$. Let $a \in A$ be invertible. Assume $a = a_1 + \cdots + a_n$ such that $a_1, \ldots, a_n \in A$ are invertible where n is even. Since $\bar{A} \cong F_2$, $\bar{a_1} = \cdots = \bar{a_n} = \bar{a} \neq 0$. So, $a_i = e + b_i$ for some $e \in A$ invertible and $b_i \in I$. Then $a = ne + b_1 + \cdots + b_n = b_1 + \cdots + b_n \in I$. This is a contradiction since $a \notin I$. □

Since $F_2 \oplus F_2$ is not an invertible algebra we must address the question of when the direct sum of F_2-invertible algebras is invertible. That is the subject of the following three propositions.

PROPOSITION 3.11. *Let A and B be finite dimensional invertible algebras over F_2. Assume A is nice. Then $C = A \oplus B$ is invertible.*

PROOF. Let $\mathcal{A}$ and $\mathcal{B}$ be invertible bases for A and B respectively. Let $a \in A$ such that it is the sum of an even number of elements from $\mathcal{A}$. Let

$$\mathcal{C} = (\mathcal{A}, b_1) \cup (a_1, \mathcal{B} \setminus \{b_1\}) \cup \{(a, b_1)\}$$

for $a_1 \in \mathcal{A}$ and $b_1 \in \mathcal{B}$. Similarly as in Proposition 3.5, it can be shown that $\mathcal{C}$ is an invertible basis for C. □

PROPOSITION 3.12. *Any factor ring of an invertible algebra over a field F is also invertible.*

PROOF. Let A be a finite dimensional invertible algebra over a field F and $I \lhd A$. Let B be an invertible basis for C and define $\bar{A} = \frac{A}{I}$. Since B consists of invertible elements it is clear that $\bar{B} = \{v + I | v \in B\}$ is a spanning set of invertible elements for $\bar{A}$. So, there is a subset of $\bar{B}$ that is a basis for $\bar{A}$. □

PROPOSITION 3.13. *An invertible algebra over F_2 that is a direct sum of invertible algebras has at most one direct summand isomorphic to F_2.*

PROOF. Let A be a finite dimensional invertible algebra over F_2. Assume A has multiple copies of F_2 as direct summands. Let $I, J \lhd A$ such that $A = I \oplus J$ and $I \cong F_2 \oplus F_2$. By Proposition 3.12, I is also an invertible algebra. Example ?? shows $F_2 \oplus F_2$ is not invertible. Therefore, this is a contradiction and A cannot have multiple copies of F_2 as direct summands. □

We will consider next the invertibility of factor rings of polynomial rings over a field in one variable. We will give a complete characterization on which ones have an invertible basis.

PROPOSITION 3.14. *Let $F \neq F_2$ be a field. Then $\frac{F[x]}{\langle f(x)\rangle}$ is invertible-2 for all $f(x)$.*

PROOF. Let $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ with $\alpha_0 \neq 0$. Since $\alpha_0 \neq 0$ we have $x(\alpha_n x^{n-1} + \alpha_{n-1}x^{n-2} + \cdots + \alpha_2 x + \alpha_1) = -\alpha_0$. Therefore, x is invertible and so $\mathcal{B} = \{1, x, x^2, \ldots, x^{n-1}\}$ is an invertible basis. We will show this basis is actually invertible-2. Let $\sum_{i=0}^{n-1} \alpha_i x^{-i} = 0$. Then multiply through by x^{n-1} and we obtain $\sum_{i=0}^{n-1} \alpha_i x^{(n-1)-i} = 0$. But since $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis, we must have $\alpha_i = 0$ for $i = 0, \ldots, n-1$. Thus $\mathcal{B}^{-1} = \{1, x^{-1}, x^{-2}, \ldots, x^{-(n-1)}\}$ is a basis for $\frac{F[x]}{\langle f(x)\rangle}$.

Now in the factor ring $\frac{F[x]}{\langle x^m\rangle}$, $\{x^j | j = 1, 2, \ldots, m-1\}$ consists of nilpotent elements. Therefore, for every j, $1 + x^j$ is invertible. So $\mathcal{A} = \{1\} \cup \{1 + x^j | j = 1, \ldots, m-1\}$. Let $v_0 = 1$, and $v_i = 1 + x^i$. Then $v_0^{-1} = 1$ and $v_i^{-1} = \sum_{j=0}^{m-1} (-1)^j x^{ij}$. Let $\sum_{i=0}^{m-1} \alpha_i v_i^{-1} = 0$. As $\alpha_1 v_1^{-1}$ is the only term including x, $\alpha_1 = 0$. So $\sum_{i\neq 1} \alpha_i v_i^{-1} = 0$ and $\alpha_2 v_2^{-1}$ is the only term including x^2. Then $\alpha_2 = 0$. Continuing this way we obtain that $\alpha_i = 0$ for $i = 1, \ldots, m-1$. It then follows that α_0 is also zero. Therefore, $\mathcal{A}^{-1}$, having the same number of elements as $\mathcal{A}$, is a basis.

It only rests to consider the case $f(x) \in F[x]$ with $f(0) = 0$ but $f(x)$ not a power of x. Under that assumption, by the Chinese remainder theorem, $\frac{F[x]}{\langle f(x)\rangle} \cong \frac{F[x]}{\langle x^m\rangle} \oplus \frac{F[x]}{g(x)}$ for some positive integer m and $g(x)$ such that $g(x) \neq 0$. The result then follows from the first two cases and Proposition 3.5. □

PROPOSITION 3.15. *Let $F = F_2$. Then the factor rings $A_1 = \frac{F[x]}{\langle (x+1)^n\rangle}$ and $A_2 = \frac{F[x]}{\langle x^n\rangle}$ are both invertible but neither is nice.*

PROOF. The proof of the above proposition requires the hypothesis that F be other than F_2 only when it comes to applying Proposition 3.5 for the third case. So, the same arguments as above show that A_1 and A_2 are invertible. The fact that they are not nice is a consequence of Lemma 3.10. □

PROPOSITION 3.16. *Let $F = F_2$ and $f(x) \in F[x]$ then $A = \frac{F[x]}{\langle f(x)\rangle}$ is invertible if and only if $x(x+1)$ does not divide $f(x)$.*

PROOF. Let $F = F_2$ and $A = \frac{F[x]}{\langle f(x)\rangle}$. Write $f(x) = x^m(x+1)^n g(x)$ where x and $(x+1)$ do not divide $g(x)$. We show that A is invertible if and only if $n \cdot m = 0$. Suppose $A = \frac{F[x]}{\langle f(x)\rangle}$ is invertible. Observe $\frac{F[x]}{\langle x^m\rangle}$ and $\frac{F[x]}{\langle (x+1)^n\rangle}$ both have factor rings isomorphic to F_2. Then by Proposition 3.13 we can only have one direct summand isomorphic to F_2. Therefore, either n or m must be 0.

Now suppose $n \cdot m = 0$. Then either n or m is 0 then we have at most one direct summand isomorphic to F_2 and by Proposition 3.13 we are done. □

References

[1] Xiang-dong Hou, Sergio R. López-Permouth, and Benigno Parra-Avila. Rational power series, sequential codes and periodicity of sequences. *J. Pure Appl. Algebra*, 213:1157–1169, 2009.

[2] Dinesh Khurana and Ashish K. Srivastava. Right self-injective rings in which every element is a sum of two units. *J. Algebra Appl.*, 6(2):281–286, 2007.

[3] Marek Kuczma. *An introduction to the theory of functional equations and inequalities.* Prace naukowe Uniwersytetu Slaskiego w Katowicach. University of Silesia, Warzawa, 1985. Panstwowe Wydawnictwo Naukowe.

[4] Richard D. Mabry. No nontrivial Hamel basis is closed under multiplication. *Aequationes Math.*, 71(3):294–299, 2006.
[5] Donald S. Passman. *The algebraic structure of group rings.* Robert E. Krieger Publishing Co. Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
[6] César Polcino Milies and Sudarshan K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications.* Kluwer Academic Publishers, Dordrecht, 2002.
[7] R. Raphael. Rings which are generated by their units. *J. Algebra*, 28:199–205, 1974.