Title
Some results relevant to embeddability of rings (especially group algebras) in division rings

Author
Bergman, George M

Publication Date
2019-10-01

DOI
10.1016/j.jalgebra.2019.06.021

Peer reviewed

Comments, corrections, and related references welcomed, as always!
TEXed December 18, 2018

SOME RESULTS RELEVANT TO EMBEDDABILITY OF RINGS (ESPECIALLY GROUP ALGEBRAS) IN DIVISION RINGS

GEORGE M. BERGMAN

Abstract. P. M. Cohn showed in 1971 that given a ring R, to describe, up to isomorphism, a division ring D generated by a homomorphic image of R is equivalent to specifying the set of square matrices over R which map to singular matrices over D, and he determined precisely the conditions that such a set of matrices must satisfy. The present author later developed another version of this data, in terms of closure operators on free R-modules.

In this note, we examine the latter concept further, and show how an R-module M satisfying certain conditions can be made to induce such data. In an appendix we make some observations on Cohn's original construction, and note how the data it uses can similarly be induced by appropriate sorts of R-modules.

Our motivation is the longstanding question of whether, for G a right-orderable group and k a field, the group algebra kG must be embeddable in a division ring. Our hope is that the right kG-module $M = k((G))$ might induce a closure operator of the required sort. We re-prove a partial result in this direction due to N. I. Dubrovin, note a plausible generalization thereof which would give the desired embedding, and briefly sketch some thoughts on other ways of approaching the problem.

1. Background

A. I. Mal'cev [15] and, independently, B. H. Neumann [19] showed that if G is a group given with a 2-*sided-invariant* ordering, that is, a total ordering $\leq$ such that for all $e, f, g, h \in G$,

(1) $\qquad f \leq g \implies ef \leq eg \quad \text{and} \quad fh \leq gh,$

and if, for k a field, we let $k((G))$ denote the set of formal k-linear combinations $\sum_{g\in G} \alpha_g\, g$ of elements of G whose support,

(2) $\qquad \mathrm{supp}(\sum_{g\in G} \alpha_g\, g) \ = \ \{g \in G \mid \alpha_g \neq 0\},$

is well-ordered, then $k((G))$ can be made a ring in a natural way; in fact, a division ring. This division ring contains the group algebra kG, as the subalgebra of elements with finite support.

Now suppose G is merely given with a *right-invariant* ordering, that is, a total ordering satisfying

(3) $\qquad f \leq g \implies fh \leq gh,$

and again let $k((G))$ be the set of formal k-linear combinations of elements of G whose supports are well-ordered. This time we cannot extend the ring structure of kG to $k((G))$ in any evident way: if we try to take the formal product ab of elements $a, b \in k((G))$, the one-sided invariance of the ordering is not enough to guarantee that only finitely many occurrences of each $g \in G$ arise when we multiply ab out; and even when that is true, for instance, when a is a member of G, the support of the resulting formal sum ab may fail to be well-ordered.

However, by (3) we can make $k((G))$ a right kG-module; and this module has been shown to have a property that is very encouraging with respect to the possibility of embedding kG in a division ring: Dubrovin [10] shows that every nonzero element of kG acts invertibly on $k((G))$.

But it is not clear how to go further: if we form the ring of k-linear endomorphisms of $k((G))$ generated by the actions of the elements of kG and their inverses, there is no evident way to prove invertibility of all nonzero elements of this larger ring; so we are not in a position to iterate the adjunction of inverses. Indeed,

2010 *Mathematics Subject Classification.* Primary: 06F16, 16K40, 20C07. Secondary: 05B35, 06A05, 06A06, 43A17.

Key words and phrases. homomorphisms of rings to division rings; coherent matroidal structures on free modules; group algebras of right-ordered groups; prime matrix ideals.

Readable at `http://math.berkeley.edu/~gbergman/papers/` .

the question of whether group rings of all right-orderable groups are embeddable in division rings is listed in [18] as Problem 1.6, attributed to A. I. Mal'cev, and dating from the first (1965) edition of that collection of open problems in group theory. (The still more general question of whether group rings of all torsion-free groups embed in division rings also appears to be open [*ibid.*, Problems 1.3 and 1.5].)

P. M. Cohn [4]-[7] showed that a homomorphism from a noncommutative ring R into a division ring D can be studied in terms of the set of square matrices over R that become singular over D. He showed that this set of matrices determines the structure of the division subring of D generated by the image of R, and gave criteria for a set of matrices to arise in this way (recalled in §13 below); he named sets of matrices satisfying those criteria "prime matrix ideals". Subsequently, the present author showed in [2] that the same data can be described in terms of closure operators on free R-modules of finite rank (details recalled in §3 below).

Something I did not notice then is that a structure with *most* of the properties defining Cohn's prime matrix ideals, or my classes of closure operators, is determined by any right or left R-module M. In §5 we develop these observations for the closure operator construction, and describe the additional properties that M must have for the closure operator so induced to satisfy *all* the required conditions.

We then give, in §§6-8, a slightly modified proof of the result of Dubrovin cited above, and in §§9-10 look at a plausible strengthening of that result which would lead to the conclusion that $k((G))$ has the module-theoretic properties needed to induce, by the results of §5, an embedding in a division ring. In §11 and §12 we discuss some other ideas that might be of use in tackling this problem.

Finally, in an appendix, §13, we look at Cohn's concept of a prime matrix ideal. We note a discrepancy between the definition of that concept that he used in most of his works, and a weaker definition given in [6], and sketch an apparent difficulty with his reasoning about the latter version. But we record an argument supplied by Peter Malcolmson, which shows that adding a small additional condition to the weaker definition renders it equivalent to the other, and show that, so modified, it allows us to obtain prime matrix ideals from certain R-modules M in a way parallel to our results on closure operators induced by R-modules.

Let me remark, regarding the concepts of 2-sided and 1-sided orderability of groups, that though the former seems "intrinsically" more natural, the latter has considerable "extrinsic" naturality: A group is right orderable if and only if it can be embedded in the group of order-automorphisms of a totally ordered set, written as acting on the right [9, Proposition 29.5]. Here "only if" is clear, using the group's action on itself. To see "if" we need, for any totally ordered set A, a way of right-ordering $\mathrm{Aut}(A)$. To get this, index A as $\{a_i \mid i \in \kappa\}$ for some ordinal κ, and for $s \neq t \in \mathrm{Aut}(A)$, let $s \leq t$ if and only if for the *least* i such that $s_i \neq t_i$, we have $s_i < t_i$. (In this argument we could, in fact, merely let the a_i run over an order-dense subset of A. Since familiar totally ordered sets such as the real line tend to have explicit countable order-dense subsets, this construction can be performed for such groups without using the axiom of choice to get the desired indexing.)

Still another fascinating characterization of the one-sided orderable groups is that they are those groups embeddable in lattice-ordered groups (groups with a partial ordering, under which they are lattices, and which is 2-sided-invariant) [9, Corollary 29.8].

2. Conventions

Throughout this note, rings are associative with 1, ring homomorphisms respect 1, and modules are unital. If M is a right R-module and X a subset of M, then XR denotes the submodule of M generated by X, i.e., the set of finite sums $\sum x_i r_i$ with $x_i \in X$, $r_i \in R$. These include the empty sum, 0; hence if $X = \emptyset$, then XR is the zero submodule.

3. Closure structures on free modules

We review here the result of [2] relating homomorphisms of a ring R into division rings with certain closure operators on free R-modules of finite rank. Recall

Definition 1. *If X is a set, then a* closure operator *on X means a map* cl *from subsets of X to subsets of X, such that for all $S, T \subseteq X$,*

(4) $\qquad S \subseteq T \implies \mathrm{cl}(S) \subseteq \mathrm{cl}(T).$

(5) $\qquad \mathrm{cl}(S) \supseteq S.$

(6) $\quad \mathrm{cl}(\mathrm{cl}(S)) \ = \ \mathrm{cl}(S).$

A closure operator cl *will be called* finitary *if for all* $S \subseteq X$,

(7) $\quad \mathrm{cl}(S) \ = \ \bigcup_{\text{finite } S_0 \subseteq S} \ \mathrm{cl}(S_0).$

(The most common term for a closure operator satisfying (7) is "algebraic", because that condition is frequent in algebraic contexts. But "finitary" seems more to the point.)

Now suppose R is a ring, and $f: R \to D$ a homomorphism into a division ring. For every $n \geq 0$, let us define a closure operator cl_{R^n} on R^n by looking at the induced map $f: R^n \to D^n$, and sending each $S \subseteq R^n$ to the inverse image in R^n of the right span over D of the image of S in D^n. In writing this formally, it will be convenient to use the same letter f that denotes our homomorphism $R \to D$ for the induced homomorphisms of right R-modules, $R^n \to D^n$, for all $n \geq 0$. Then our definition says that for each $S \subseteq R^n$,

(8) $\quad \mathrm{cl}_{R^n}(S) \ = \ f^{-1}(f(S)D).$

It is not hard to verify that this construction satisfies the following five conditions for all $m, n \geq 0$.

(9) cl_{R^n} is a closure operator on the underlying set of the right R-module R^n, whose closed subsets are R-submodules.

(10) For all $n > 0$, $\mathrm{cl}_{R^n}(\emptyset)$ is a proper submodule of R^n.

(11) For every homomorphism of right R-modules $h: R^m \to R^n$ and every cl_{R^n}-closed submodule $A \subseteq R^n$, the submodule $h^{-1}(A) \subseteq R^m$ is cl_{R^m}-closed.

(12) The closure operator cl_{R^n} has the *exchange property*, namely, for $S \subseteq R^n$ and $t, u \in R^n$, if $u \notin \mathrm{cl}_{R^n}(S)$ but $u \in \mathrm{cl}_{R^n}(S \cup \{t\})$, then $t \in \mathrm{cl}_{R^n}(S \cup \{u\})$.

(13) The closure operator cl_{R^n} is finitary.

In [2], I named families of closure operations $(\mathrm{cl}_{R^n})_{n \geq 0}$ satisfying (9)-(13) "proper coherent matroidal structures on free R-modules" ("matroid" being the standard term for a set X given with a finitary closure operator cl having the exchange property of (12)), and it was shown that every such structure determines a homomorphism f of R into a division ring D which induces the given operators via (8), and which is, up to embeddings of division rings, the unique such homomorphism. By (8), the kernel of that homomorphism is $\mathrm{cl}_R(\emptyset)$.

Condition (11) above is stated in terms of inverse images of closed subsets. It is also equivalent (given (9)) to a statement about *closures of images* of subsets, namely:

(14) For every homomorphism of right R-modules $h: R^m \to R^n$ $(m, n \geq 0)$ and every subset $S \subseteq R^m$, the submodule $h(\mathrm{cl}_{R^m}(S))$ of R^n is contained in $\mathrm{cl}_{R^n}(h(S))$.

Indeed, consider an arbitrary subset $S \subseteq R^m$ and an arbitrary closed subset $A \subseteq R^n$. Then (11) is equivalent to the statement that for any such sets, if $S \subseteq h^{-1}(A)$ then $\mathrm{cl}_{R^m}(S) \subseteq h^{-1}(A)$, while (14) is equivalent to the statement that for any such sets, if $h(S) \subseteq A$ then $h(\mathrm{cl}_{R^m}(S)) \subseteq A$. These statements are clearly equivalent, so (11) and (14) are equivalent.

We remark that matroid theorists often require the underlying sets of matroids to be finite; for instance, this is assumed by Welsh [20], and only in his final chapter does he discuss ways the theory might be extended to infinite structures. But for most algebraic applications, including those of this note, the restriction to finite sets would be unnatural, and the appropriate version in the infinite case is clear: Regarding matroids as sets with closure operators (one of many equivalent formulations of the concept), one should simply require that these operators be finitary, i.e., one should impose condition (13). We shall call on many results from [20] in this note, tacitly understanding that the statements we quote go over to the infinite matroids we will be considering. The assumption that our closure operators are finitary makes it straightforward to deduce such statements from the corresponding facts about finite matroids.

(The term "matroid" is based on the motivating example of the linear dependence structure on the rows or columns of a matrix over a field K. From that point of view, the finiteness assumption is natural. But such systems of rows or columns are simply finite families of elements of a space K^n, and to the algebraist, linear dependence is most naturally viewed as structure on that generally infinite set.)

In the situations we shall be looking at, conditions (9)-(11) will generally be easy to establish. The next lemma restricts the instances one has to verify to show that (12) also holds, and shows that (13) is implied by (9) and (12).

Lemma 2. *Let R be a ring, n a nonnegative integer, and cl_{R^n} an operator on subsets of R^n satisfying* (9)*. Then*

(i) cl_{R^n} *satisfies the exchange property* (12) *if and only if it satisfies the restriction of that condition to sets $S \subseteq R^n$ of cardinality $< n$, i.e., the condition*

(15) *For every subset $S \subseteq R^n$ of cardinality $< n$, and every pair of elements $t, u \in R^n$, if $u \notin \mathrm{cl}_{R^n}(S)$ but $u \in \mathrm{cl}_{R^n}(S \cup \{t\})$, then $t \in \mathrm{cl}_{R^n}(S \cup \{u\})$.*

Moreover, if cl_{R^n} does satisfy (15)*, then*

(ii) *For all $S \subseteq R^n$, there exists $S_0 \subseteq S$ of cardinality $\leq n$ such that $\mathrm{cl}_{R^n}(S_0) = \mathrm{cl}_{R^n}(S)$, and*

(iii) *For $S \subseteq R^n$ whose closure is a proper subset of R^n, there exists S_0 as in* (ii) *of cardinality $< n$. Hence*

(iv) *If an operator cl_{R^n} satisfies* (9) *and* (12)*, it also satisfies* (13)*.*

Proof. Let us first show that (15) implies (ii) and (iii).

Since R^n is generated as an R-module by the standard basis $e_1, \dots, e_n$, and since by (9), closed subsets of R^n are submodules, we have $\mathrm{cl}_{R^n}(\{e_1, \dots, e_n\}) = R^n$.

Now the conclusion of (ii) that $\mathrm{cl}_{R^n}(S)$ is the closure of a $\leq n$-element subset of S is trivial if $S \subseteq \mathrm{cl}_{R^n}(\emptyset)$; in the contrary case, let $s_1 \in S - \mathrm{cl}_{R^n}(\emptyset)$, and choose a subset $\{e_{i_1}, \dots, e_{i_m}\}$ of $\{e_1, \dots, e_n\}$ minimal for having s_1 in its closure. Thus by (15) with $\{e_{i_1}, \dots, e_{i_{m-1}}\}$ in the role of S, we have $e_{i_m} \in \mathrm{cl}_{R^n}(\{e_{i_{m_1}}, \dots, e_{i_{m-1}}, s_1\})$; hence one can replace e_{i_m} by s_1 in the relation $\mathrm{cl}_{R^n}(\{e_1, \dots, e_n\}) = R^n$.

If $S \not\subseteq \mathrm{cl}_{R^n}(\{s_1\})$ (which by the above observation can only happen if $n > 1$), then taking $s_2 \in S - \mathrm{cl}_{R^n}(\{s_1\})$, the corresponding argument shows that we can replace another e_i by s_2; and so on. Since there are only n elements e_i to be replaced, this process must stop after $\leq n$ steps, giving a subset of $\leq n$ elements of S which (because the process has stopped) has S in its closure, hence has the same closure as S, proving (ii).

Further, if $\mathrm{cl}_{R^n}(S) \neq R^n$, this process can't terminate with all the e_i replaced by elements of S, since that would imply that S had closure R^n; so it must terminate with $< n$ elements so replaced. Again, the fact that the process has terminated means that the set of $< n$ elements by which we have replaced those elements has closure $\mathrm{cl}_{R^n}(S)$, establishing (iii).

Now to get (i), note that the exchange property of (12) for the closure operator cl_{R^n} clearly implies (15). To get the converse, assume (15) and suppose we are given $S \subseteq R^n$, and t and u satisfying $u \notin \mathrm{cl}_{R^n}(S)$ but $u \in \mathrm{cl}_{R^n}(S \cup \{t\})$. Thus $\mathrm{cl}_{R^n}(S) \neq R^n$, so since (15) implies (iii), there exists $S_0 \subseteq S$ of cardinality $< n$ such that $\mathrm{cl}_{R^n}(S_0) = \mathrm{cl}_{R^n}(S)$. Hence $u \notin \mathrm{cl}_{R^n}(S_0)$ and $u \in \mathrm{cl}_{R^n}(S_0 \cup \{t\})$; so (15) gives $t \in \mathrm{cl}_{R^n}(S_0 \cup \{u\})$, whence $t \in \mathrm{cl}_{R^n}(S \cup \{u\})$, establishing (12).

Clearly (ii) implies that cl_{R^n} is finitary, proving (iv). □

Statements (ii) and (iii) above are instances of well-known properties of matroids (X, cl) for which the whole set X is the closure of an n-element subset; cf. [20, Corollary to Theorem 1.5.1, p. 14]. The method of proof of statement (i) likewise yields a general result: if cl is a closure operator on a set X such that X is the closure under cl of an n-element subset, then (X, cl) is a matroid if and only if it satisfies the weakened version of the exchange property in which S is restricted to subsets of cardinality $< n$. I haven't seen this stated, but it is probably known.

Statement (iv) is [2, Lemma 2]. As noted in [2], I included finitariness in my list of conditions on the families of operators considered so that these would clearly be matroid structures; but that lemma showed the finitariness condition superfluous in the presence of the other conditions. So in the remainder of this note, the set of conditions on a family of closure operators that we shall understand need to be verified to get a homomorphism into a division ring will be (9)-(12).

4. Closure structures on restricted families of free modules

We shall consider in this section families $(\mathrm{cl}_{R^n})_{0 \leq n \leq N}$ of closure operators cl_{R^n} defined only for the finitely many values of n indicated in the subscript. The hope is that results on such families may prove useful in inductive proofs that certain infinite families $(\mathrm{cl}_{R^n})_{n\geq 0}$ satisfy (9)-(12) for all n. The results of this section will not be called on in later sections, so some readers may prefer to skip or skim this material.

Convention 3. *In this section, R will be a ring and N a fixed nonnegative integer, and for $0\leq n\leq N$, closure operators cl_{R^n} on R^n will be assumed given, which satisfy* (9)-(12) *for all $m,n\leq N$.*

It will be useful to regard elements of R^n as column vectors over R, and to treat finite families of such elements as matrices. Let us fix some conventions regarding these.

Given an $n\times m$ matrix H, we shall understand a *submatrix* of H to be specified by a (possibly empty) subset of the n row-indices and a (possibly empty) subset of the m column-indices. (Thus, submatrices determined by different pairs of subsets will be regarded as distinct, even if, when re-indexed using index-sets $1,\dots,n_0$ and $1,\dots,m_0$, they give equal matrices.) We shall regard the set of submatrices of H as ordered by inclusion (corresponding to inclusions among the sets of row-indices and column-indices involved), so that we can speak of submatrices maximal or minimal for a property. A submatrix of H will be called square if it has the same number of rows as of columns, even if these are not indexed by the same families of integers. Because the statements we will be considering will not be affected by re-indexing the rows and columns, we shall, however, for ease in visual presentation, often assume without loss of generality that submatrices we are interested in form contiguous blocks.

For R and $(\mathrm{cl}_{R^n})_{0\leq n\leq N}$ as in Convention 3, let us give names to the properties of matrices over R with $n\leq N$ rows which, in the special case where R is a division ring and $\mathrm{cl}_{R^n}(S)$ denotes the right subspace generated by S, describe right, left, and 2-sided invertibility of such matrices.

We remark that since conditions (9)-(12) are all stated in terms of *right* module structures, what we can say about these matrix conditions will not, in general, be symmetric with respect to rows and columns. Note also that an index m, n etc. may or may not be restricted to values $\leq N$, depending on whether it occurs in a context where it describes the heights of column vectors.

Definition 4. *An $n\times m$ matrix H over R with $n\leq N$ will be called* right strong *with respect to* cl_{R^n} *if the closure under that operation of its set of columns is all of R^n,* left strong *with respect to* cl_{R^n} *if no proper subfamily of its columns has closure equal to the closure of all the columns, and* strong *with respect to* cl_{R^n} *if both those conditions hold. When the closure operator in question is clear from context, we shall simply write "right strong", "left strong", and "strong".*

If operators cl_{R^n} are given for all $n\geq 0$ (and all cases of (9)-(12) are thus assumed), then the remaining results of this section are easy to prove using the homomorphism of R into a division ring D discussed following (9)-(12) above, together with basic linear algebra over division rings. But since here we are only assuming such operators given for $n\leq N$, we shall have to do things the hard way.

First, a few very basic facts, though some of them are lengthy to establish.

Lemma 5. (i) *For all $n\leq N$, the $n\times n$ identity matrix I_n is strong.*

(ii) *Among matrices over R with $\leq N$ rows, the class of right-strong matrices and the class of left-strong matrices are each closed under matrix multiplication* (*where defined*).

(iii) *The class of right-strong matrices is also closed under adjoining additional columns and under deleting rows, and the class of left-strong matrices under deleting columns and adjoining rows* (*so long as the number of rows remains $\leq N$*).

Proof. (i): The assertion that I_n is right strong says that $\mathrm{cl}_{R^n}(\{e_1,\dots,e_n\})=R^n$, which was noted in the second sentence of the proof of Lemma 2. The assertion that I_n is left strong says that none of these elements is in the closure of all the others. To see this, note that for each i, the inverse image of $\mathrm{cl}_R(\emptyset)$ under the i-th projection map $R^n\to R$ is closed by (11), and contains e_j for all $j\neq i$, but by (10) does not contain e_i.

To get the first assertion of (ii), suppose A and B are right-strong matrices, where A is $n\times n'$ and B is $n'\times n''$ with $n,\,n'\leq N$. Let $a: R^{n'}\to R^n$ and $b: R^{n''}\to R^{n'}$ be the linear maps on column vectors defined by left multiplication by these matrices. The image of a is the right R-submodule of R^n spanned by the columns of A, so the assumption that A is right strong implies (and, given (9), is equivalent to saying) that the closure of that image is all of R^n. Similarly, the assumption that B is right strong says that the closure of the image of b is all of $R^{n'}$. Now by (14), the closure of the image of ab contains the image under a of the closure of the image of b, in other words, $a(R^{n'})$, hence it contains $\mathrm{cl}_{R^n}(a(R^{n'}))$, which we have noted is R^n, proving that AB is right strong.

The proof of the statement about left-strong matrices is longer, and is most easily carried out with the help of some concepts and results from the theory of matroids. Let us call a family $(x_i)_{i\in I}$ of elements of R^m $(m \leq N)$ *independent* if the closure of $\{x_i \mid i \in I\}$, which for brevity we will call the closure of the I-tuple $(x_i)_{i\in I}$, is not the closure of any proper subfamily $(x_i)_{i\in J}$ $(J \subsetneq I)$; and let the *rank* of an arbitrary family $(x_i)_{i\in I}$ mean the cardinality of any independent subfamily $(x_i)_{i\in J}$ $(J \subseteq I)$ having the same closure as the whole family, that is, any subfamily minimal for having that closure. Such subfamilies exist by Lemma 2(ii), and by a standard result on matroids, based on an element-by-element replacement construction as in the proof of Lemma 2(ii), their cardinalities are all the same value $\leq m$ [20, Corollary to Theorem 1.5.1, p.14], justifying these definitions. That same replacement argument shows that every independent family of elements of R^m can be extended to an m-element independent family whose closure is all of R^m [20, Theorem 1.5.1].

Now suppose A is an $n \times n'$ left strong matrix (with $n \leq N$, and hence n' necessarily also $\leq N$ by the left-strong condition), let $a : R^{n'} \to R^n$ be the map it determines, and let $(x_i)_{i\in I}$ be any independent family of elements of $R^{n'}$. By the above observations, this can be extended to an n'-element independent family $(x_i)_{i\in J}$ $(J \supseteq I,\ \mathrm{card}(J) = n')$ with closure all of $R^{n'}$. Hence by (14),

$$\mathrm{cl}_{R^n}\{a(x_i) \mid i \in J\} = \mathrm{cl}_{R^n}(a(\mathrm{cl}_{R^{n'}}\{x_i \mid i \in J\})) = \mathrm{cl}_{R^n}(a(R^{n'})) = \mathrm{cl}_{R^n}\{a(e_i) \mid 1{\leq}i{\leq}n'\}, \tag{16}$$

where $\{e_1, \ldots, e_{n'}\}$ is the standard basis of $R^{n'}$. Now $\{a(e_i) \mid 1 \leq i \leq n'\}$ is independent because A is left strong. If $(a(x_i))_{i\in J}$ were dependent, then its closure would be the closure of an independent family of $< n'$ elements, so (16) would contradict the equal-cardinalities result cited in the next-to-last sentence of the preceding paragraph. So $(a(x_i))_{i\in J}$ is independent, so a fortiori, $(a(x_i))_{i\in I}$ is independent. Thus, a carries independent families to independent families.

But this is equivalent to the result we are trying to prove; for if B is an $n' \times n''$ left strong matrix and $b : R^{n''} \to R^{n'}$ its action, then the statement that B is left strong says that the family of its columns, $(b(e_i))_{1\leq i\leq n''}$, is independent, and the above result shows the same for $(ab(e_i))_{1\leq i\leq n''}$, the family of columns of AB. This completes the proof of (ii).

In (iii), the assertion that the class of right-strong matrices is closed under adjoining additional columns is clear from the definition of right strong.

That left strong matrices are closed under adjoining rows is most easily verified as the contrapositive statement, that the class of non-left-strong matrices is closed under dropping rows. This is equivalent to saying that a dependent family of column vectors remains dependent on dropping from each of its members a fixed subset of the entries. Such an entry-dropping operation corresponds to a homomorphism $R^m \to R^n$, and from (14) it is easy to see that the image of a dependent family under *any* homomorphism is dependent, giving the desired result.

In showing that dropping rows preserves the property of being right strong, and dropping columns that of being left strong, let our matrix be $n \times n'$, and assume without loss of generality that the rows or columns to be dropped are the last d rows or columns, for some d. Then the row-dropping operation is equivalent to left multiplication by the $n{-}d \times n$ matrix $(I_{n-d}\ \ 0)$, where I_{n-d} is the $n{-}d \times n{-}d$ identity matrix, and the column-dropping operation to right multiplication by the $n' \times n'{-}d$ matrix $\begin{pmatrix} I_{n'-d} \\ 0 \end{pmatrix}$. That these matrices are respectively right and left strong can be seen from the argument proving (i); the desired results then reduce to special cases of (ii). □

In some considerations, it is easy to deal with adding and deleting columns of a matrix, because these operations keep us within the same set R^n, but harder to handle adding and deleting rows. In such situations, the following observation will be helpful.

Lemma 6. *Let H be an $n \times n'$ matrix over R, with $0 \leq n \leq N$, and let us be given a list of indices $0 < i_1 < \cdots < i_d \leq n$. Let H' be the $n{-}d \times n'$ matrix formed by deleting from H the rows with indices $i_1, \ldots, i_d$, and H'' the $n \times n'{+}d$ matrix formed by adjoining to H the additional columns $e_{i_1}, \ldots, e_{i_d}$.*

Then H' is right strong, respectively, left strong, if and only if H'' is.

Sketch of proof. Let $f : R^n \to R^{n-d}$ be the map which drops the coordinates with indices $i_1, \ldots, i_d$, and $g : R^{n-d} \to R^n$ the right inverse to f which inserts 0's in these positions. We see that f^{-1} and g^{-1}, applied to submodules, give a bijection between all submodules of R^{n-d}, and those submodules of R^n

which contain $e_{i_1}, \dots, e_{i_d}$. By (11), f^{-1} and g^{-1} each carry closed submodules to closed submodules, hence by the preceding observation they induce a bijection between $(\mathrm{cl}_{R^{n-d}})$-closed submodules of R^{n-d}, and cl_{R^n}-closed submodules of R^n that contain $e_{i_1}, \dots, e_{i_d}$. It follows that if S is a subset and t an element of R^n, then $t \in \mathrm{cl}_{R^n}(S \cup \{e_{i_1}, \dots, e_{i_d}\})$ if and only if $f(t) \in \mathrm{cl}_{R^{n-d}}(f(S))$. The two conclusions of the lemma follow by combining these observations with the definitions of right and left strong. □

We can now generalize several facts about right and left invertible matrices over a division ring to right and left strong matrices with respect to the system $(\mathrm{cl}_{R^n})_{0 \le n \le N}$ of Convention 3.

Lemma 7. *Let H be an $n \times n'$ matrix over R, with $n \le N$. Then*

(i) *If H is right strong, then $n \le n'$, i.e., H has at least as many columns as rows.*

(ii) *If H is left strong, then $n \ge n'$, i.e., H has at least as many rows as columns.*

(iii) *Suppose H is right strong, and H' is a submatrix of H given by a subset of the columns of H. Then H' is minimal among such submatrices which are right strong if and only if it is maximal among such submatrices which are left strong. Hence if H' has either the above minimality property or the above maximality property, it is strong.*

(iv) *Suppose H is left strong, and H' is a submatrix of H given by a subset of the rows of H. Then H' is minimal among such submatrices which are left strong if and only if it is maximal among such submatrices which are right strong. Hence, again, if H' has either the above minimality property or the above maximality property, it is strong.*

(v) *If H is left or right strong, then it is strong if and only if $n = n'$, i.e., if and only if it is square.*

(vi) *If m is the common cardinality of all maximal independent sets of columns of H, equivalently, all sets of columns minimal for having the same closure as the set of all columns of H, then all maximal strong submatrices of H are $m \times m$.*

(vii) *If H is square, hence $n \times n$, and its upper left-hand $n{-}1 \times n{-}1$ block is strong, then H is strong if and only if its n-th column is not in the closure of its other $n{-}1$ columns.*

Proof. (i) says that any family of elements of R^n whose closure is R^n must have $\ge n$ elements, and (ii) that any independent family must have $\le n$ elements. Both of these facts follow easily from the results cited in the second paragraph of the proof of Lemma 5(ii).

Assertion (iii) is immediate: With the help of the exchange property, it is easy to check that the maximal independent subfamilies of the family of columns of H are the same as the minimal subfamilies having R^n as closure (an instance of a general property of matroids).

To get (iv), let H^* be the matrix $(H\ I_n)$ obtained by appending the columns $e_1, \dots, e_n$ to H. Clearly, H^* is right strong. Let us now consider submatrices of H^* which consist of all the columns of H, together with a subset of the columns of I_n, and apply (iii) to such submatrices. It is easy to see that a submatrix given by such a set of columns, which is minimal or maximal among such submatrices for one of the properties named in (iii), will in fact be minimal or maximal for the same property among *all* submatrices given by subsets of the columns of H^*. Applying (iii), and then Lemma 6, we get (iv).

In (v), the "only if" direction follows from (i) and (ii). To get "if", suppose that H is square and right strong. Statement (iii) tells us that by deleting some columns of H we can get a strong matrix H'; but if the set of columns so deleted were nonempty, then H' would not be square, contradicting the "only if" direction. So that set of columns is empty, so $H = H'$ is itself strong. In the case where H is left strong, one uses the same method, calling on (iv) in place of (iii).

The conclusion of (vi) is equivalent to saying that every strong submatrix of H is contained in an $m \times m$ strong submatrix; so let A be any strong submatrix of H, and assume without loss of generality (by permuting the rows and columns of H if necessary) that A is the upper left-hand $m' \times m'$ block of H for some $m' \le n$. Since A is strong it is left strong, hence by Lemma 5(iii), the submatrix H' of H given by the first m' columns of H is also left strong. Let us extend H' to a maximal left-strong submatrix H'' of H given by a subset of the columns; this will have m columns, which we can assume by a further rearrangement are the first m columns of H. Now the submatrix given by the first m' rows of H'' contains the columns of A, hence is right strong; let us adjoin further rows of H'' to get a maximal right strong submatrix A'' consisting of rows of H''. By (iv) (with H'' in the role of the H of that statement), A'' is strong, so it is the desired $m \times m$ strong submatrix of H containing A.

Finally, in the situation of (vii), note that the $n \times n{-}1$ submatrix given by the first $n-1$ columns of H is left strong, since it is obtained by adjoining a row to a left strong $n{-}1 \times n{-}1$ matrix. The matrix H

is obtained from that submatrix by bringing in a final column, so it will be left strong if and only if that column is not in the closure of the other columns. (The verification of the "if" direction uses the exchange property.) Since it is square, (v) tells us that that necessary and sufficient condition for it to be left strong is in fact necessary and sufficient for it to be strong. □

The above arguments were, as noted, row-column asymmetric because we were considering closure operators on column vectors, rather than on row vectors. Note, however, that the set of $m \times n$ matrices $(m, n \leq N)$ right strong with respect to $(\mathrm{cl}_{R^n})_{0 \leq n \leq N}$ is easily seen to determine $(\mathrm{cl}_{R^n})_{0 \leq n \leq N}$. It seems likely that one could find simple necessary and sufficient conditions for a set of matrices to be the right strong matrices with respect to such a family. If it should turn out that the left strong matrices satisfy the analogs of those conditions, it would follow that our family of closure operators on right modules is equivalent to a similar family on left modules. I have not investigated these ideas. (If one developed such results, one would want distinct notations for the sets of rows and columns of length n over R. Following Cohn, one might denote these R^n and ${}^nR$.)

Let us also note that the existence of just finitely many operators, cl_{R^n} for $0 \leq n \leq N$, as discussed in this section, cannot alone be sufficient for R to be embeddable in a division ring. For if R is any N*-fir*, the method of [2, §7] yields such closure operators for $0 \leq n \leq N$, but examples are known of N-firs whose free modules of larger finite ranks behave badly, e.g., satisfy $R^{N+1} \cong R^{N+2}$, making it impossible to embed such rings in division rings. Thus, if the results of this section are to be useful in proving results on embeddability in division rings, that use is likely to be, as suggested at the start of this section, as a tool in inductive developments. (Some details on the facts cited above: The concept of *fir*, i.e., free ideal ring, is recalled in [2, §7], and R is assumed to be a fir in most of the that section; but the final paragraphs of that section note how to generalize the arguments to the case of a *semifir*, and the same method, applied to N*-firs*, rings in which every right or left ideal generated by $\leq N$ elements is free of unique rank, gives the desired family $(\mathrm{cl}_{R^n})_{0 \leq n \leq N}$. For examples of N-firs whose free modules of ranks $> N$ behave badly, see the $V_{m,n}$ case of [1, Theorem 6.1].)

5. Systems of closure operators induced by R-modules

In §3 we saw how a homomorphism of a ring R into a division ring D induces, by (8), a system of closure operators satisfying (9)-(12). Suppose that instead of a homomorphism from R to a division ring, we are given a nonzero right R-module M. There is no obvious way to put M in place of D in (8) (even if we assume it a left rather than a right module); but we shall see below that there is a natural way to get from M a system of closure operators $(\mathrm{cl}_{R^n})_{0 \leq n}$ which, for $M = D_R$ (D regarded as a right R-module) agrees with that given by (8).

For each $n > 0$, let us write elements $a \in M^n$ as row vectors, and elements $x \in R^n$ as column vectors. Then for such a and x we can define $ax \in M$ in the obvious way; thus we can speak of elements of R^n annihilating elements of M^n. For $S \subseteq R^n$, let $\mathrm{cl}_{R^n}(S)$ be the set of elements of R^n that annihilate all elements of M^n annihilated by all elements of S. Writing $\mathrm{ann}_{M^n}(S)$ for $\{a \in M^n \mid (\forall\, s \in S)\ as = 0\}$, this becomes

$$(17) \qquad \mathrm{cl}_{R^n}(S) \ = \ \{x \in R^n \mid \mathrm{ann}_{M^n}(x) \supseteq \mathrm{ann}_{M^n}(S)\}.$$

We see that the closed subsets of R^n under (17) are precisely the annihilators of subsets of M^n.

It is not hard to check that given a homomorphism to a division ring, $f : R \to D$, as in §3, if we let $M = D_R$, then (17) describes the same closure operator as (8). (The key observation is that every subspace of the right D-vector space of height-n columns over D is the right annihilator of a set of length-n rows over D – since such row vectors correspond to the D-linear functionals on that space – so the right R-submodules of R^n that are inverse images under f of D-subspaces of D^n, regarded as sets of columns, are those that are annihilators of sets of elements of D^n regarded as rows.)

Returning to the case of a general right R-module M, let us, for any *matrix* A over R with n rows, write $\mathrm{ann}_{M^n}(A)$ for the subset of M^n annihilated by the right action of A, in other words, the annihilator in M^n of the set of columns of A.

Lemma 8. *Let R be a ring and M a nonzero right R-module, and for each $n \geq 0$ let cl_{R^n} be defined by* (17)*. Then this family of operators satisfies conditions* (9), (10) *and* (11)*. For each n, the condition that*

cl_{R^n} *also satisfy* (12) (*which, as we have seen, is equivalent to* (15)), *is equivalent to each of the following three statements.*

(18) *There do not exist a subset* $S \subseteq R^n$, *and elements* $u, t \in R^n$, *such that* $\mathrm{ann}_{M^n}(S) \supsetneqq \mathrm{ann}_{M^n}(S \cup \{u\}) \supsetneqq \mathrm{ann}_{M^n}(S \cup \{t\})$.

(19) *There do not exist an* $n \times n{-}1$ *matrix* A *over* R, *and* $n \times n$ *matrices* B, C *over* R, *each obtained by adding a single column to* A, *such that* $\mathrm{ann}_{M^n}(A) \supsetneqq \mathrm{ann}_{M^n}(B) \supsetneqq \mathrm{ann}_{M^n}(C)$.

(20) *There do not exist* $n \times n$ *matrices* A, B, C *over* R *which all agree except in one column, such that* $\mathrm{ann}_{M^n}(A) \supsetneqq \mathrm{ann}_{M^n}(B) \supsetneqq \mathrm{ann}_{M^n}(C)$.

Hence, if a ring R *has a* faithful *right module* M *which for all* $n \geq 0$ *satisfies* (18), *equivalently,* (19), *equivalently,* (20), *then* R *is embeddable in a division ring.*

Proof. That the operators defined by (17) satisfy (9) and (10) is straightforward, the key fact being that the annihilator in R^n of every element $a \in M^n$ is a right submodule of R^n, which is proper if $a \neq 0$.

(11) is also not difficult, but here are the details. Let $h : R^m \to R^n$ be represented by the $n \times m$ matrix H, acting on the left on columns of elements of R. The matrix H can also be applied on the right to rows of elements of M, so as to carry M^n to M^m, and if we also call this map h (and write it on the right), the associativity of formal matrix multiplication gives the law $(a\,h)\,x = a\,(h\,x)$. Thus, if $A \subseteq R^n$ is closed, i.e., is the annihilator of a subset $T \subseteq M^n$, and we write its inverse image $h^{-1}(A) \subseteq R^m$ as $\{x \in R^m \mid h\,x \in A\} = \{x \in R^m \mid (\forall\, t \in T)\ t\,(h\,x) = 0\} = \{x \in R^m \mid (\forall\, t \in T)\ (t\,h)\,x = 0\}$, we see that this is the annihilator of $T\,h \subseteq M^m$, hence also closed.

The equivalence of (12) with (18) is easy to see if we bear in mind that an inclusion between the annihilators in M^n of two subsets of R^n is equivalent to the *reverse* inclusion between the closures of those subsets of R^n, as defined by (17).

Condition (19) is a translation of (15), gotten by looking at the $< n$ elements of R^n in (15) as columns of a matrix (and if there are fewer than $n-1$ elements in the set, throwing in enough zero columns to bring the number of columns up to $n-1$), then applying the definition (17).

The difference between (19) and (20) is merely cosmetic. Indeed, if three $n \times n$ matrices with the properties referred to in (20) exist, then letting A' be the $n \times n{-}1$ matrix gotten by deleting the column in which those three differ, we get $\mathrm{ann}_{M^n}(A') \supseteq \mathrm{ann}_{M^n}(A) \supsetneqq \mathrm{ann}_{M^n}(B) \supsetneqq \mathrm{ann}_{M^n}(C)$, so A', B, C have the properties referred to in (19), while conversely, given A, B, C as in (19), if we expand A to an $n \times n$ matrix by adjoining a zero column, we get matrices with the properties of (20).

To see the final assertion of the lemma, note that applying (17) with $n = 1$ and $S = \emptyset$, we find that $\mathrm{cl}_R(\emptyset) \subseteq R$ is the annihilator of M. If M is faithful, this is the trivial ideal of R, so by [2, (21) and Theorem 22], the system of closure operators cl_{R^n} determines a homomorphism with zero kernel from R to a division ring. □

(So if, for every right ordered group G, we could prove that the right kG-module $k((G))$ satisfied (18), equivalently (19), equivalently (20), this would show kG embeddable in a division ring.)

Above, we have obtained a closure operator on free R-modules by comparing *kernels* of the maps $M^n \to M$ induced by elements of R^n. Can we get a similar construction using images rather than kernels?

Yes, but things have to be set up a bit differently. Note that in the key case where $M = D_R$ for D a division ring, images of maps $M^n \to M$ induced by elements of R^n aren't very diverse; so we should look instead at images of maps $M \to M^n$ induced by such elements. If we treat elements of R^n as row vectors, acting on a right R-module M, we find that the set of elements of R^n determining maps whose images lie in (say) the image of a given such map will not, in general, be a right R-submodule of R^n, but will be a left R-submodule. We could ask when the resulting left-R-submodule-valued closure operators satisfy the left-right duals of conditions (9)-(12), which, by symmetry, would also lead to homomorphisms into division rings; but let us, instead, stay in the context of (9)-(12) by starting with a *left* R-module L, and carrying out the left-right dual of the construction just sketched. Thus, given L, we again regard elements of R^n as column vectors, but now let them act on the left on L, mapping elements of L to column vectors over L. We now define closure operators cl_{R^n} $(n \geq 0)$ by specifying that for $S \subseteq R^n$,

(21) $\mathrm{cl}_{R^n}(S) \ = \ \{x \in R^n \mid x\,L \subseteq \sum_{s \in S} s\,L\}.$

We easily obtain the analog of Lemma 8:

Lemma 9. *Let R be a ring and L a nonzero left R-module, and for each $n \geq 0$ let cl_{R^n} be defined by* (21). *Then this family of operators satisfies conditions* (9), (10) *and* (11). *For each n, the condition that cl_{R^n} also satisfy the exchange property of* (12) (*which, as we have seen, is equivalent to* (15)) *is equivalent to each of the following three statements.*

(22) *There do not exist a subset $S \subseteq R^n$ and elements $u, t \in R^n$ such that* $\sum_{s\in S} sL \subsetneqq \sum_{s\in S\cup\{u\}} sL \subsetneqq \sum_{s\in S\cup\{t\}} sL.$

(23) *There do not exist an $n\times n{-}1$ matrix A and $n\times n$ matrices B and C, each obtained by adding a single column to A, such that* $AL^{n-1} \subsetneqq BL^n \subsetneqq CL^n.$

(24) *There do not exist $n\times n$ matrices A, B, C over R which all agree except in one column, such that* $AL^n \subsetneqq BL^n \subsetneqq CL^n.$

Hence, if a ring R has a faithful left module L which for all $n \geq 0$ satisfies (22), *equivalently,* (23), *equivalently,* (24), *then R is embeddable in a division ring.*

Sketch of proof. Again, the verifications of (9), (10) and (11) are straightforward, with that of (11) using associativity of matrix multiplication. The proofs that (22), (23), and (24) are all equivalent to (12) parallel the proofs for (18), (19), and (20). □

(Let us note examples showing that in the situations of the above two lemmas, condition (13) need not hold if (12) does not. Let k be a field, let $R \subseteq k^{\mathbb{N}}$ be the subring of all *eventually* constant sequences of elements of k, let $M = R$, and let $L = S =$ the ideal of eventually-zero sequences. It is not hard to verify that under the closure operator cl_R, defined either as in Lemma 8 using M or as in Lemma 9 using L, $\mathrm{cl}_R(S) = R$, while the closure of any finite subset of S is the ideal that it generates, hence does not contain $1 \in R$; so $\mathrm{cl}(S) \neq \bigcup_{\mathrm{finite}\, S_0\subseteq S} \mathrm{cl}(S_0)$.)

We remark that the description of matroids in terms of closure operators is only one of many surprisingly diverse, though ultimately equivalent, ways of developing that concept [20, Chapter 1]. Moreover, matroid structures on modules R^n, discussed above, and prime matrix ideals, considered in §13 below, are just two of several ways of describing the data that determine a homomorphism from R into a division ring; for others, see [17].

6. The idea of Dubrovin's result

Let us change gears, and in this and the next two sections develop the result:

(25) (After N. I. Dubrovin [10].) For G a right ordered group, the right action of every nonzero element of kG on $k((G))$ is invertible.

In this section we sketch what is involved; in §7 we look at an order-theoretic tool that can "organize" the proof, and in §8, we apply that tool to recover (25). In §§9-10 we shall return to the ideas of §5 above, and note a plausible generalization of (25) which, if true, would imply that the kG-module $k((G))$ satisfies (18).

Incidentally, Dubrovin [10] assumes G *left*-ordered and regards $k((G))$ as a left kG-module; but the results for left- and right-ordered groups are clearly equivalent. He also develops his result with k a general division ring, and with the multiplication of the group ring skewed by an action of G on k by automorphisms. In this note, I restrict attention to the case where k is a field and G centralizes k, simply because the added generality would be a distraction. But the generalizations mentioned seem to involve no fundamental complications, so if further positive results are eventually obtained for the case discussed here, the techniques are likely to go over to those more general cases.

(Dubrovin also proves in [11], [12] that group rings of certain particular classes of right-ordered groups are embeddable in division rings; but we are here concerned with what one can hope to prove for arbitrary right-ordered groups.)

So let G be a right ordered group and x an element of $kG - \{0\}$. The easy half of (25) result is that the action of x on $k((G))$ is one-to-one, i.e., that for any $a \in k((G)) - \{0\}$ we have $ax \neq 0$. To see this, let g_0 be the least element of the support of a. Then for each $h \in \mathrm{supp}(x)$, since right multiplication by h preserves the order of G, the least element of $\mathrm{supp}(a\,h)$ is $g_0\,h$. Since left multiplication by g_0 is one-to-one on G, the finitely many well-ordered sets $\mathrm{supp}(a\,h)$ $(h \in \mathrm{supp}(x))$ have distinct least elements $g_0\,h$; so the least of these least elements appears exactly once when we evaluate $a\,x$. Hence $a\,x \neq 0$.

Note, however, that we cannot say a priori which $h \in \mathrm{supp}(x)$ will make $g_0\,h$ the least element of the support of $a\,x$. It need not be the least element of $\mathrm{supp}(x)$, since *left* multiplication by g_0 does not, in general, preserve the ordering of G.

Nevertheless, given $x \in kG - \{0\}$, the function associating to each $g \in G$ the least product $g\,h$ for $h \in \mathrm{supp}(x)$ will be an order-preserving bijection $G \to G$. To see that it is order-preserving and one-to-one, let $g_0 < g_1 \in G$, and take an $a \in k((G))$ with $\mathrm{supp}(a) = \{g_0, g_1\}$. Then our observation that the least element of $\mathrm{supp}(a) \cdot \mathrm{supp}(x)$ has the form $g_0\,h$, and occurs just once, shows that $g_0\,h \in g_0\,\mathrm{supp}(x)$ must be distinct from the least element of $g_1\,\mathrm{supp}(x)$, and less than it, as asserted.

To see that the function $G \to G$ of the preceding paragraph is also surjective, take any $g \in G$, which we wish to show is in its range. Let h_0 be the member of $\mathrm{supp}(x)$ that *maximizes* $g\,h_0^{-1}$. Note that $g \in (g\,h_0^{-1})\,\mathrm{supp}(x)$; I claim g is the smallest element of that set. For taking any $h_1 \neq h_0$ in $\mathrm{supp}(x)$, by choice of h_0 we have $g\,h_1^{-1} < g\,h_0^{-1}$, hence, right multiplying by h_1, we get $g < (g\,h_0^{-1})\,h_1$, so g is indeed the least element of $(g\,h_0^{-1})\,\mathrm{supp}(x)$, as claimed.

Let us give the function we have defined a name.

(26) Suppose $x \in kG - \{0\}$. For each $g \in G$, we shall write $\rho_{\mathrm{supp}(x)}(g)$ for the least element of $g \cdot \mathrm{supp}(x)$. Thus, as shown above, $\rho_{\mathrm{supp}(x)}$ is an order-preserving bijection $G \to G$.

Here $\rho_{\mathrm{supp}(x)}$ is mnemonic for the fact that the operation involves *right* multiplication by $\mathrm{supp}(x)$.

We can now approach the task of showing that right multiplication by $x \in kG - \{0\}$ is surjective as a map $k((G)) \to k((G))$. Given $a \in k((G))$, we want to construct $b \in k((G))$ such that $b\,x = a$. If $a = 0$ there is no problem; if not, let g_0 be the least element of $\mathrm{supp}(a)$. From the above discussion, we see that the least element of $\mathrm{supp}(b)$ has to be $\rho^{-1}_{\mathrm{supp}(x)}(g_0)$. Attaching to this the appropriate coefficient in k, we get a first approximation to b; an element $b_0 \in k((G))$ whose product with x has the correct lowest term.

Now let $a_1 = a - b_0\,x$. If this is zero, we are again done; if not, we let g_1 be the least element of its support, and repeat the process.

But can we continue this process transfinitely? When we come to a limit ordinal α, will the expression b_α that the previously constructed expressions b_β $(\beta < \alpha)$ converge to have well-ordered support?

Dubrovin shows by a transfinite induction that this does indeed hold at every step. As a variant approach, we shall recall in the next section a general result on ordered sets, going back to G. Higman, using which we can obtain a well-ordered subset $Y \subseteq G$ such that the process sketched above keeps the supports of the b_α within Y. Indeed, what we have looked at as a process of successively modifying elements b_α becomes a transfinite coefficient-by-coefficient calculation of b, indexed by the well-ordered set Y.

The result on ordered sets is quite powerful, so we can hope that it will also be applicable to studying solutions to several linear equations in several unknown elements of $k((G))$, as might be needed to combine the idea of Dubrovin's result with the approach of §§3-5.

7. Generating well-ordered sets

What sort of order-theoretic result do we need? Given $a \in k((G))$ and $x \in kG$, we want to modify the former by subtracting off a multiple of the latter having the same least term, and iterate this process. At steps after the first, the least element in the support of our modified a might be one of the elements of the original support, or an element in the support of one of the terms we have subtracted off. What we can say is that it lies in the closure of $\mathrm{supp}(a)$ under adjoining, for every element g that at some stage is in our set, all the other elements of the unique left multiple of $\mathrm{supp}(x)$ having g for its least member. We want to know that this closure, like $\mathrm{supp}(a)$, is well-ordered.

If $\mathrm{supp}(x)$ has n elements, then the above construction can be thought of as closing $\mathrm{supp}(a)$ under $n(n-1)$ *partial* functions. Indeed, given $g \in G$, and distinct elements $h_0, h_1 \in \mathrm{supp}(x)$, we are interested in $g\,h_0^{-1}h_1$ *if* the left translate of $\mathrm{supp}(x)$ which has g as its least member is $g\,h_0^{-1}\mathrm{supp}(x)$, the translate in which h_0 is carried to g. So to each pair $h_0 \neq h_1$ of elements of $\mathrm{supp}(x)$, let us associate the partial function $G \to G$ which, if g is the least element of $(g\,h_0^{-1})\,\mathrm{supp}(x)$, takes g to $g\,h_0^{-1}\,h_1$, but is undefined otherwise.

These $n(n-1)$ partial functions are partial *unary* operations on G; but the order-theoretic arguments to be used can in fact handle partial operations of arbitrary finite arities. This suggest a general formulation that would start with a well-ordered set of constants, and a finite family of partial finitary operations. But a constant can be thought of as a zeroary operation; so if we allow our *finitely many* finitary operations to be replaced by *well-ordered families* of such operations – one such family for each of finitely many arities – then we can treat the constants as one of these families.

Finally, the assumption that the set on which we are operating (in our case, G) is given with a total ordering, and our families of operations are indexed by well-ordered sets, can be weakened to make the given set partially ordered, and the families of operations "well-partially-ordered", i.e., having descending chain condition and no infinite antichains. Indeed, in the case we are interested in, there is no natural order to put on the pairs (h_0, h_1) indexing our unary partial operations; and though G is totally ordered, if we hope to generalize our result from single relations $a\,x = b$ to families of relations on tuples $(a_1, \dots, a_n) \in k((G))^n$, then the elements $a_1, \dots, a_n$ will be multiplied by different elements of kG, so it would make most sense to regard their supports as belonging to a union of n copies of G, each ordered as G is, but with elements of the different copies incomparable.

A result of the sort suggested above was proved by G. Higman [13], except that he started with everywhere-defined functions. However, his proof goes over without modification to partial functions. We state the result, so generalized, and in modern language, below. (We drop a different sort of generality in the formulation of Higman's result. Namely, where we assume a partial ordering on X, he only assumed a preordering. But the hypotheses of his result imply that each of his operations, when applied to elements equivalent under the equivalence relation determined by the preordering (cf. [3, Proposition 5.2.2]), gives equivalent outputs. From this it can be deduced that his conclusion about the preordered set is equivalent to the corresponding statement about the partially ordered set gotten by dividing out by that equivalence relation.)

We shall denote the action of a partial function by "$\rightsquigarrow$".

Theorem 10 (after G. Higman [13, Theorem 1.1])**.** *Let X be any partially ordered set, let $I_0, \dots, I_{N-1}$ be well-partially-ordered sets for some $N \geq 0$, and suppose that for each $n \in \{0, \dots, N{-}1\}$ we are given a partial function $s_n : X^n \times I_n \rightsquigarrow X$. Suppose further that each s_n is, on the one hand,* isotone *(i.e., if $p, q \in X^n \times I_n$ lie in the domain of s_n, and $p \leq q$ under coordinatewise comparison, then $s_n(p) \leq s_n(q)$), and, on the other hand,* nondecreasing *in its arguments in X (i.e., if s_n is defined at $p = (x_0, \dots, x_{n-1}, i) \in X^n \times I_n$, then $s_n(p) \geq x_m$ for all $m < n$).*

Let Y be the subset of X generated by the above operations; that is, the least subset of X with the property that $s_n(x_0, \dots, x_{n-1}, i) \in Y$ whenever $0 \leq n < N$, $x_0, \dots, x_{n-1} \in Y$, $i \in I_n$, and s_n is defined on $(x_0, \dots, x_{n-1}, i)$. Then Y is well-partially-ordered.

(*Remark: if I_0 is empty, then Y is empty. It is the elements $s_0(i)$ $(i \in I_0)$ that "start" the process that generates Y.*)

Proof. As in [13]. $\square$

I recommend Higman's proof as a tour-de-force worth reading. (His Theorem 2.6, used in that proof, is a method of induction over the class of n-tuples of all well-partially-ordered sets.)

8. Recovering Dubrovin's bijectivity result

Let us now, with the help of the above result, prove the bijectivity of the right action on $k((G))$ of every nonzero element of kG.

Given

(27) $\quad a \in k((G)) \quad$ and $\quad x \in kG - \{0\},$

we wish to find $b \in k((G))$ such that $bx = a$. With this goal, we start by applying Theorem 10 with $N = 2$, and the following choices of X, I_n and s_n $(n < 2)$:

(28) $\quad X = G$, with its given right ordering.

(29) $\quad I_0 = \mathrm{supp}(a)$, and $s_0 : I_0 \to X$ is given by the restriction to I_0 of $\rho^{-1}_{\mathrm{supp}(x)}$ (defined in (26)). Thus, s_0 takes each $g \in \mathrm{supp}(a)$ to the $g' \in G$ such that g is the least element of $g'\,\mathrm{supp}(x)$.

(30) $I_1 =$ the finite set $\{(h_0, h_1) \in \mathrm{supp}(x)^2 \mid h_0 \neq h_1\}$, given with the antichain ordering (making distinct elements incomparable), and $s_1 : G \times I_1 \rightsquigarrow G$ is defined by $s_1(g,(h_0,h_1)) = g\, h_0^{-1} h_1$ if g is the least element of $g\, h_0^{-1}\,\mathrm{supp}(x)$ (equivalently, if $\rho^{-1}_{\mathrm{supp}(x)}(g) = g\, h_0^{-1}$), and is undefined otherwise.

Thus, s_1 encodes the $n(n-1)$ partial functions discussed in the second paragraph of the preceding section.

To see that the hypotheses of Theorem 10 are satisfied, note that I_0 and I_1 are well-partially-ordered, the former because, being the support of an element of $k((X))$, it is well-ordered, the latter because, though an antichain, it is finite. Since s_0 has no arguments in X, it only needs to be isotone in its argument in I_0, which it is, because $\rho^{-1}_{\mathrm{supp}(x)}$ is an order-automorphism of G. Since I_1 is an antichain, s_1 need only be isotone and non-decreasing in its argument in G. It is isotone in that argument because it is given, when defined, by *right* multiplication by the element $h_0^{-1} h_1$. By its definition, it is non-decreasing (in fact, increasing) in that argument when defined.

Thus, Theorem 10 yields a subset $Y \subseteq G$ closed under the above operations and well-partially-ordered; which, since G is totally ordered, means well-ordered. Closure under the operation of (29) means that $\rho^{-1}_{\mathrm{supp}(x)}(\mathrm{supp}(a)) \subseteq Y$, while closure under the operations of (30) says that for each $g \in Y$ we also have $\rho^{-1}_{\mathrm{supp}(x)}(g) \cdot \mathrm{supp}(x) \subseteq Y$. Note, finally, that the definition (26) of $\rho_{\mathrm{supp}(x)}$ shows that

(31) For every $b' \in k((G))$ having support in Y, we have $\mathrm{supp}(a - b'x) \subseteq \rho_{\mathrm{supp}(x)}(Y)$.

Let us now construct by recursion elements $\beta_g \in k$ for all $g \in Y$, such that $(\sum_{g \in Y} \beta_g\, g)\, x = a$. To do this, assume recursively that for some $g \in Y$ we have found $\beta_{g'}$ for all $g' < g$ in Y, such that for each $g_0 < g$,

(32) all elements of $\mathrm{supp}(a - (\sum_{g' \in Y,\, g' \leq g_0} \beta_{g'}\, g')\, x)$ are $> \rho_{\mathrm{supp}(x)}(g_0)$.

Then applying (32) to the greatest $g_0 < g$ in Y if there is one, or passing to the "limit" gotten by taking the union of the ranges of summation in (32) if there is not, we can say that

(33) all elements of $\mathrm{supp}(a - (\sum_{g' \in Y,\, g' < g} \beta_{g'}\, g')\, x)$ are $> \rho_{\mathrm{supp}(x)}(g_0)$ for all $g_0 < g$ in Y.

(The two changes from (32) are in the range of summation, and the final quantification of g_0.) Since $\rho_{\mathrm{supp}(x)}$ is an order automorphism of G, we see from (31) that the condition "$> \rho_{\mathrm{supp}(x)}(g_0)$ for all $g_0 < g$ in Y" is equivalent to "$\geq \rho_{\mathrm{supp}(x)}(g)$", so (33) says

(34) all elements of $\mathrm{supp}(a - (\sum_{g' \in Y,\, g' < g} \beta_{g'}\, g')\, x)$ are $\geq \rho_{\mathrm{supp}(x)}(g)$.

Given (34) for some $g \in Y$, let $\gamma \in k$ be the coefficient of $\rho_{\mathrm{supp}(x)}(g)$ in $a - (\sum_{g' \in Y,\, g' < g} \beta_{g'}\, g')\, x$, let $h = g^{-1}\rho_{\mathrm{supp}(x)}(g) \in \mathrm{supp}(x)$, and let δ be the coefficient of h in x. Then letting $\beta_g = \gamma\, \delta^{-1}$, we see that this is the unique choice of coefficient for g that will lead to (32) holding with g in place of g_0.

Constructing β_g in this way for each $g \in Y$, and taking $b = \sum_{g \in Y} \beta_g\, g$, we find that $bx = a$, as desired. From the way our recursive construction has forced a unique value for each β_g $(g \in Y)$, it is not hard to deduce that b is unique for that property (though this uniqueness is most easily seen as in §6). Thus we have

Theorem 11 (after N. I. Dubrovin [10])**.** *If G is a right-ordered group, and $x \in kG - \{0\}$, then the action of x on the right kG-module $k((G))$ is bijective.* □

9. What should we try to prove next?

In the context of Theorem 11, consider any column vector $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in (kG)^2$, and assume for simplicity that both x_1 and x_2 are nonzero. From that theorem it is not hard to deduce that the set K of row vectors $a = (a_1, a_2) \in k((G))^2$ right-annihilated by x has the property that the projection maps to first and second components each give a bijection $K \to k((G))$. We may ask

Question 12. *Given $x_1,\, x_2 \in kG - \{0\}$, let K be, as above, the kernel of the map $k((G))^2 \to k((G))$ induced by the column vector $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in (kG)^2$. Is it true that for each $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in (kG)^2$, the map $K \to k((G))$ induced by y, taking $(a_1, a_2) \in K$ to $a_1 y_1 + a_2 y_2$, is either zero or bijective?*

A positive answer seems intuitively plausible.

We shall see in the next section a sequence of conditions, indexed by an integer $n \geq 1$, on a right module M over a general ring R, such that for $R = kG$ and $M = k((G))$, the result of Theorem 11 is the $n = 1$ case, a positive answer to Question 12 would be the $n = 2$ case, and the full set of conditions would imply that R is embeddable in a division ring.

For the moment, let us restrict attention to Question 12. To see concretely what it asks, note that the kernel K can be described as the set of elements of $k((G))^2$ of the form $(a_1, -a_1 x_1 x_2^{-1})$ (where by x_2^{-1} I mean the inverse of the action of x_2 on $k((G))$). The image of such a member of K under y is $a_1 y_1 - a_1 x_1 x_2^{-1} y_2$; hence a positive answer to Question 12 would say that in the ring of endomaps of $k((G))$ generated by the actions of elements of kG and the inverses of those actions, every map of the form $y_1 - x_1 x_2^{-1} y_2$ is either zero or invertible. So this is, indeed, a "next step" after the invertibility of the actions of nonzero elements of kG itself.

If $y_2 \neq 0$, then right multiplying $y_1 - x_1 x_2^{-1} y_2$ by y_2^{-1}, we see that a positive answer to Question 12 is also equivalent to the statement that every nonzero map of the form $y_1 y_2^{-1} - x_1 x_2^{-1}$ is invertible. Alternatively, left multiplying by x_1^{-1} gives the corresponding condition on $x_1^{-1} y_1 - x_2^{-1} y_2$, while if we instead right multiply by y_1^{-1}, we get the same statement for $1 - x_1 x_2^{-1} y_2\, y_1^{-1}$. So we can restate Question 12 as

Question 13. *Is it true that for all $x_1, x_2, y_1, y_2 \in kG - \{0\}$, the endomap of $k((G))$ given by the* (*right*) *action of $y_1 y_2^{-1} - x_1 x_2^{-1}$ is either zero or invertible? Equivalently, is the same true of the endomaps given by the actions of $x_1^{-1} y_1 - x_2^{-1} y_2$, $y_1 - x_1 x_2^{-1} y_2$, $1 - x_1 x_2^{-1} y_2\, y_1^{-1}$?*

(The assumption that y_1 and y_2 are nonzero was not made in Question 12; but if either or both is zero, an affirmative answer to Question 12 is easily deduced from Theorem 11 and our description of K.)

The difficulty in approaching Question 13 is that we have no evident test for when a map such as $x_1^{-1} y_1 - x_2^{-1} y_2$ should be zero. Since each of x_1, x_2, y_1, y_2 is a finite k-linear combination of elements of G, we might hope that this could be answered by some finite computation; but the inverses appearing in each of the expressions in Question 13 represent operators on $k((G))$ that can behave differently on different "parts" of an element of that module.

A variant of this difficulty: Note that for every $r \in kG$, the expression $x_1^{-1} y_1 - x_2^{-1} y_2$ has the same action as $x_1^{-1}(y_1 + x_1 r) - x_2^{-1}(y_2 + x_2 r)$. This can allow one to transform an expression $a(x_1^{-1} y_1 - x_2^{-1} y_2)$ ($a \in k((G))$) such that the lowest elements of the supports of $a(x_1^{-1} y_1)$ and $a(x_2^{-1} y_2)$ cancel one another to an expression for the same element with higher lowest terms. But an r that has that effect for one $a \in k((G))$ might have the opposite effect for an a' with a different lowest term.

We remark, as an aside, that the statement that every map of the form $z_1^{-1} + z_2^{-1}$ ($z_1, z_2 \in kG - \{0\}$) is zero or invertible does not require an answer to Question 13; it follows from Theorem 11, by looking at $z_1^{-1} + z_2^{-1}$ as $z_1^{-1}(z_2 + z_1) z_2^{-1}$. (More generally, this holds for every map of the form $z_1^{-1} w_1 + w_2 z_2^{-1}$, since this can be rewritten $z_1^{-1}(w_1 z_2 + z_1 w_2) z_2^{-1}$.) The statement that every map of the form $z_1^{-1} + z_2^{-1} + z_3^{-1}$ is zero or invertible would, on the other hand, follow from a positive answer to Question 13, by writing that sum as $z_1^{-1}((z_2 + z_1) + z_1 z_3^{-1} z_2) z_2^{-1}$, and regarding the parenthesized factor as having the form $y_1 - x_1 x_2^{-1} y_2$.

10. A general condition

Let us now give the promised family of conditions generalizing both the result proved by Dubrovin and the extension of that result asked for in Question 13.

(Readers who have read §4 will notice similarities between the properties treated there and those considered below; for instance, between Lemma 7(vii) and Lemma 14. The material of §4 was, in fact, motivated by the idea of abstracting the results below to closure operators not necessarily arising from modules. But that turned out to require lengthier arguments, and I have not tried to carry it to completion.)

Given a ring R, a right R-module M, and any $n \geq 0$, let us refer to an $n \times n$ matrix over R as *M-invertible* if it induces an invertible map $M^n \to M^n$. The condition that we will be interested in for general $n \geq 1$ is

(35) For every $n \times n{-}1$ matrix X over R whose top $n{-}1 \times n{-}1$ block is M-invertible, and every column vector $y \in R^n$, the action of y either annihilates the kernel K of the additive group homomorphism $M^n \to M^{n-1}$ induced by X, or maps K bijectively onto M.

What does the $n=1$ case of (35) say? In that case the matrix X of (35) is $1\times 0,$ hence represents the unique map $M\to M^0=\{0\},$ which has kernel $M.$ Its upper 0×0 block, also an empty matrix, represents the unique endomorphism of $M^0=\{0\},$ which is clearly invertible; i.e., that block is M-invertible. Thus, that case of (35) says that every $y\in R$ not annihilating M maps M bijectively to itself. In particular, for $R=kG$ and $M=k((G)),$ this is the statement of Theorem 11; so for these R and $M,$ the $n=1$ case of (35) holds.

Given Theorem 11, we now see that Question 12 asks whether the $n=2$ case of (35) holds for this ring and module. (The one detail that has to be cleared up is that in formulating Question 12, I assumed for conceptual simplicity that $x_2\neq 0,$ which is not in the hypothesis of (35). But the hypothesis of (35) for $n=2$ does imply $x_1\neq 0,$ hence if $x_2=0,$ we get $K=\{0\}\times M,$ and the desired result holds by Theorem 11. So Question 12 asks for the part of the $n=2$ case of (35) which does not follow from this observation.)

In studying the general case of (35), the following observation will be useful.

Lemma 14. *Let R be a ring, M a right R-module, X an $n\times n{-}1$ matrix over R for some $n>0,$ and $y\in R^n$ a column vector. Then if the upper $n{-}1\times n{-}1$ block of X is M-invertible, and y maps $\mathrm{ann}_{M^n}(X)$ bijectively to $M,$ then the $n\times n$ matrix X' gotten by appending y to X as an n-th column is M-invertible.*

Proof. By assumption, y annihilates no member of $\mathrm{ann}_{M^n}(X)$; clearly this says that the matrix X' annihilates no member of $M^n.$

To see that X' is surjective, let $a\in M^n$ be an element we want to show is in its range. By the M-invertibility of the top $n{-}1\times n{-}1$ block of $X,$ we can find $b\in M^n$ with last term $0,$ and whose first $n-1$ terms form a vector carried by that subblock of X to the first $n-1$ terms of $a.$ Since the last term of b is 0, multiplying b by the whole matrix X still gives the first $n-1$ terms of $a.$ If we apply y to $b,$ we get an element $by\in M$ which may differ from the desired last term a_n of a; but since y carries the annihilator of X bijectively to $M,$ we can find an element b' in that annihilator which is carried by y to $a_n-by.$ We then get $(b+b')X'=a,$ proving surjectivity. $\square$

From this, we can prove, for any $N\geq 0,$

Lemma 15. *Suppose R and M are a ring and module satisfying* (35) *for all $0<n\leq N.$ Let H be an $n\times n'$ matrix over R with $n\leq N,$ and suppose* (*as we may, without loss of generality, by a permutation of the rows and columns*) *that $H=\begin{pmatrix}A&B\\C&D\end{pmatrix},$ where A is maximal among M-invertible square submatrices of $A.$ Say A is $m\times m.$* (*Here one or more of $m,$ $n-m,$ $n'-m$ may be zero, making some of the submatrices $A,$ $B,$ $C,$ D empty.*)

Then every column of $\begin{pmatrix}B\\D\end{pmatrix}$ annihilates $\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix})$; equivalently, $\mathrm{ann}_{M^n}(H)=\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix}).$

Proof. Let us write A^{-1} for the inverse of the action of A on M^m (though this action is not in general represented by a matrix over R). Then every element of $\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix})$ is uniquely determined by its final $n-m$ entries; namely, given $b\in M^{n-m},$ one sees that $(-b\,CA^{-1},b)$ is the unique member of M^n ending in b and annihilated by $\begin{pmatrix}A\\C\end{pmatrix}.$ Hence $\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix})$ is the direct sum over all i with $m<i\leq n$ of the additive subgroup of that annihilator consisting of elements whose only nonzero entry after the first m entries (if any) is in the i-th position.

Now suppose that for some $j>m,$ the j-th column of H did not annihilate $\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix}).$ By rearranging the columns of H after the m-th, we can assume without loss of generality that $j=m+1.$ Since the $m{+}1$-st column of H does not annihilate $\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix}),$ it will not annihilate all of the direct summands mentioned in the preceding paragraph, and by a rearrangement of the rows of $H,$ we can assume that a summand which it fails to annihilate consists of the members of $\mathrm{ann}_{M^n}(\begin{pmatrix}A\\C\end{pmatrix})$ whose only nonzero entry after the m-th (if any) is the $m{+}1$-st.

Let us now apply (35), putting in the role of X the $m+1 \times m$ matrix consisting of A and the top row of C, and in the role of y the column vector consisting of the first $m+1$ entries of the $m+1$-st column of H. By assumption, that column does not annihilate the annihilator of that matrix. By Lemma 14, that makes the upper left $m+1 \times m+1$ submatrix of H an M-invertible matrix, contradicting the maximality assumption on A. This contradiction shows that every column of $\begin{pmatrix} B \\ D \end{pmatrix}$ annihilates $\mathrm{ann}_{M^n}(\begin{pmatrix} A \\ C \end{pmatrix})$, as claimed. □

We can now prove

Proposition 16. *Let R and M be a ring and module satisfying* (35) *for $0 < n \leq N$. Then condition* (19) *holds for all $n \leq N$.*

Hence if (35) *holds for all $n > 0$, and the R-module M is faithful, then R admits an embedding in a division ring.*

Proof. Assume, by way of contradiction, that strict inclusions as in (19) hold; however, let us write H for the matrix there called A, and write the matrices there called B and C as (H, s) and (H, t), where $s, t \in R^n$ (freeing up the letters A through D for use as in Lemma 15).

Applying Lemma 15 to H, we get (after rearranging the rows and columns of H) an $n \times m$ submatrix $H' = \begin{pmatrix} A \\ C \end{pmatrix}$, where $m \leq n-1$, having the same left annihilator in M^n as H, and such that A is invertible. By hypothesis, the vectors s and t each act nontrivially on $\mathrm{ann}_{M^n}(H) = \mathrm{ann}_{M^n}(H')$, with s having strictly larger annihilator there than t does, so

$$(36) \qquad \mathrm{ann}_{M^n}(H', s) \supsetneqq \mathrm{ann}_{M^n}(H', t).$$

Now as in the proof of Lemma 15, we see that in $\mathrm{ann}_{M^n}(H')$, each element is determined uniquely by its final $n - m$ terms, and that since s acts nontrivially on that annihilator, it will act nontrivially on an element in which only one of those positions has a nonzero entry. By another rearrangement of rows we can assume that that position is the $m+1$-st. The annihilator of the action t on $\mathrm{ann}(H')$ was assumed to be contained in that of s, so t will also act nontrivially on that element.

Hence by Lemma 14, in each of the $n \times m+1$ matrices (H', s) and (H', t), the top $m+1 \times m+1$ block will be invertible. Hence in the annihilators of those matrices, every element will be determined uniquely by its last $n - m - 1$ terms. Clearly, if the functions determining such elements from their last $n - m - 1$ terms are the same for (H', s) and (H', t), then the annihilators of those matrices are the same, while if the functions are different, those annihilators are incomparable; so neither possibility is compatible with the assumed strict inclusion (36).

This contradiction completes the proof of (19). The final assertion of the proposition follows by Lemma 8. □

We remark that an R-module M satisfying (19) for all n, and hence leading to a homomorphism from R to a division ring D, need not, in general, itself be a vector space over a division ring. For example, if R is a commutative integral domain, one finds that the choice $M = R$ leads as in §5 to a closure operator that gives the field of fractions F of R. Indeed, the closure operator determined by M is the same as that determined by the R-module F, since the annihilator of any row vector over F is also the annihilator of a row vector over R, gotten by clearing denominators. On the other hand, I do not know whether a module satisfying the stronger condition (35) for all n must be a vector space over the division ring D that it determines. (This is indeed so in the case of commutative R, where the $n = 1$ case of (35) is the analog of Dubrovin's result: It says that every element of R that does not annihilate M acts invertibly on it.)

The $n = 2$ case of (35), discussed in the preceding section, should be a useful test case for ideas on how to try to prove that for $R = kG$ and $M = k((G))$, (35) holds for all n.

11. Sandwiching kG between a right and a left module

For R an algebra over a field k and M a right R-module, the dual k-vector space $M^* = \mathrm{Hom}_k(M, k)$ has a natural structure of *left* R-module. If we write the image of $a \in M$ under $b \in M^*$ as $\langle a, b \rangle \in k$, then the relation between these module structures is described by the rule

$$(37) \qquad \langle ar,\, b \rangle \;=\; \langle a,\, rb \rangle \quad \text{for} \quad a \in M,\ r \in R,\ b \in M^*.$$

I do not know whether M^* can somehow be used, together with M, in studying whether R is embeddable in a division ring. However, the above observation is really a lead-in to the observation that for $R = kG$ and $M = k((G))$, there is a left R-module that behaves much like the above M^*, but is not itself constructed from M, and hence has (conceivably) a better chance of bringing additional strength to our investigations.

Namely, given a group G with a right-invariant ordering $\leq$, let G^* be the same group under the corresponding *left*-invariant ordering, $\leq^*$, characterized by

$$(38) \qquad g \leq^* h \quad \Longleftrightarrow \quad g^{-1} \geq h^{-1}.$$

(A right- or left-invariant ordering $\leq$ on a group is determined by its *positive cone*, $\{g \in G \mid g \geq 1\}$. The ordering $\leq^*$ defined above is the left-invariant ordering having the same positive cone as the given right-invariant ordering $\leq$. Indeed, writing P for the positive cone of $\leq$, we have $g \leq h$ if and only if $h \in Pg$, so by (38), $g \leq^* h$ if and only if $g^{-1} \in Ph^{-1}$, which, left-multiplying by g and right-multiplying by h, comes to $h \in gP$.)

Let us write $k((G^*))$ for the space of formal k-linear combinations of elements of G having well-ordered supports under $\leq^*$; this clearly has a natural structure of *left* kG-module. I claim that we can define a k-bilinear map $\langle\,,\,\rangle : k((G)) \times k((G^*)) \to k$ by

$$(39) \qquad \langle \textstyle\sum \alpha_g g,\ \sum \beta_h h \rangle \;=\; \sum_{g\in G} \alpha_g \beta_{g^{-1}} \quad \text{for} \quad \sum \alpha_g g \in k((G)) \text{ and } \sum \beta_h h \in k((G^*)).$$

To see that the right-hand side of (39) makes sense, let A be the set of $g \in G$ such that both α_g and $\beta_{g^{-1}}$ are nonzero. The condition $\sum \alpha_g g \in k((G))$ shows that A is well-ordered under $\leq$. Similarly, since A is contained in the set of *inverses* of elements of the support of $\sum \beta_h h$, and the latter support is well-ordered under $\leq^*$, (38) shows that A is reverse-well-ordered under $\leq$. Being both well-ordered and reverse-well-ordered under $\leq$, A is finite; so the sum on the right-hand side of (39) is indeed defined.

The formula (39) looks as though it says, "Multiply the formal sums $\sum \alpha_g g$ and $\sum \beta_h h$ together, and take the coefficient of 1 in the result". But though the summation that would give that coefficient is, as we have just seen, defined, the same need not be true of the coefficients of other members of G. For instance, if G contains elements s, t, both > 1, such that $ts = st^{-1}$, then $\sum_{i\geq 0} t^i \in k((G))$ belongs to both $k((G))$ and $k((G^*))$; hence by left-invariance of the order on G^*, $\sum_{j\geq 0} st^j$ also belongs to $k((G^*))$. But the formal product of these two elements is $\sum_{i,j\geq 0} st^{j-i}$, in which the term s occurs infinitely many times. (More generally, in this summation, each term st^j occurs infinitely many times, while terms t^j, in particular, the term 1, never occurs; which is consistent with our observation that it can occur only finitely many times.)

Returning to the map (39), one finds that it satisfies the analog of (37):

$$(40) \qquad \langle a\,r,\, b\rangle = \langle a,\, r\,b\rangle \quad \text{for} \quad a \in k((G)),\ r \in kG,\ b \in k((G^*)).$$

This is intuitively clear from the "coefficient of 1" interpretation of $\langle\,,\,\rangle$. To verify it formally, one can first check it for $r \in G$, then take a general finite k-linear combination of the resulting formulas.

Let us write the common value of the two sides of (40) as $\langle a\,r\,b\rangle$. Thus, given $a \in k((G))$ and $b \in k((G^*))$, though one cannot associate to each $g \in G$ the "coefficient of g in their product", one can associate to each such g the value $\langle a\,g^{-1}\,b\rangle$. It is not hard to check that this is in fact the coefficient of g in the formal product ba; so the summations giving all coefficients of that product (unlike the summations that would give the coefficients in ab) do each involve only finitely many terms. Thus, the construction sending a pair (a,b) to the formal sum $\sum(\langle ag^{-1}b\rangle)\,g \in k^G$, equivalently, to the formal product ba, is a well-defined k-bilinear map $k((G)) \times k((G^*)) \to k^G$. However, the elements of the resulting subspace $k((G^*))\ k((G)) \subseteq k^G$ are not as "nice" as those of $k((G))$ and $k((G^*))$. For instance, for G having positive elements satisfying $ts = st^{-1}$ as above, $k((G))$ contains $(\sum_{i\geq 0} t^i)s = s(\sum_{i\geq 0} t^{-i})$, and $k((G^*))$, as we have noted, contains $s(\sum_{i>0} t^i)$; so $k((G^*))\ k((G))$ will contain $s(\sum_{i\geq 0} t^{-i}) \cdot 1 + 1 \cdot s(\sum_{i>0} t^i) = s(\sum_{-\infty}^{\infty} t^i)$. (If one wants to see that a product of a single element of $k((G^*))$ with a single element of $k((G))$ can misbehave in this way, note that in the product $(1 + s(\sum_{i\geq 0} t^{-i})) \cdot (1 + s(\sum_{i>0} t^i))$, the terms homogeneous of degree 1 in s give the expression just described.) However (again writing P for the positive cone of the right-ordered group G, equivalently of the left-ordered group G^*) we can at least say that each element of $k((G^*))\ k((G))$ has support which is contained in $u\,P\,v$ for some $u, v \in G$, equivalently, which is disjoint from $u\,(P - \{1\})^{-1}\,v$. Namely, given $\sum_{i=1}^{n} b_i a_i$ with each $b_i \in k((G^*))$ and each $a_i \in k((G))$, take u such that the supports of all the b_i are in uP, and v such that the supports of all the a_i are in Pv.

Suppose we now let S denote the set of pairs (s_1, s_2) such that s_1 is a k-vector-space endomorphism of $k((G))$ and s_2 a k-vector-space endomorphism of $k((G^*))$, written on the right and the left respectively, which satisfy

(41) $\quad \langle a\, s_1,\, b\rangle = \langle a,\, s_2\, b\rangle \quad$ for $\quad a \in k((G)),\ \ b \in k((G^*)).$

It is easy to see that in such a pair, s_1 and s_2 each determine the other. The set S forms a k-algebra under the obvious operations, and contains a copy of R, consisting of all pairs (r, r), where by abuse of notation we let the symbol for $r \in R$ denote both the right action of r on $k((G))$ and the left action of r on $k((G^*))$. For nonzero $r \in R$, we can see from Theorem 11 and its left-right dual that all such elements are invertible in S; so S contains all ring-theoretic expressions in "elements of R" and their inverses.

But if one has any hope that S might be a division ring (as I briefly did), that is quickly squelched. It contains, for instance, a copy of the direct product k-algebra k^G. Namely, if we let each $(c_g)_{g\in G}$ in that algebra act on $k((G))$ by $\sum \alpha_g g \mapsto \sum c_g \alpha_g g$ and on $k((G^*))$ by $\sum \beta_g g \mapsto \sum c_{g^{-1}} \beta_g g$, these actions are easily seen to satisfy (41), and to have the ring structure of the direct product of fields k^G.

In conclusion, I do not know whether the interaction of the right kG-module $k((G))$, the left kG-module $k((G^*))$, and the operator $\langle\, ,\, \rangle$ may, in some way, be useful in tackling the question of whether kG can be embedded in a division ring.

12. Further ideas – also having difficulties

12.1. **A different sort of kG-module?** We noted in the preceding section that a right ordered group G can have elements s and t satisfying $ts = st^{-1}$. Indeed, that relation gives a presentation of the simplest example of a group admitting a right invariant ordering but not a two-sided invariant ordering:

(42) $\quad G \ = \ \langle s, t \mid ts = st^{-1}\rangle.$

If we write elements of this group in the normal form $t^i s^j$ $(i, j \in \mathbb{Z})$, it is straightforward to verify that a right ordering is given by lexicographic ordering of the pairs (j, i) :

(43) $\quad t^i s^j \leq t^{i'} s^{j'} \quad \iff \quad j < j'$, or $j = j'$ and $i \leq i'$.

(Of course, elements of G also have the normal form $s^j t^i$; but if we used that, we would have to describe our right ordering as lexicographic ordering by the pairs $(j, (-1)^j i)$.) In fact, it is easy to check that (43), its conjugate by s, and their opposites, are the only right-invariant orderings on G.

Now consider the element $1 - t \in kG$. We know by Theorem 11 that it acts bijectively on the right on $k((G))$; let us write the inverse of this action on $k((G))$ as $(1-t)^{-1}$. Where does that operation send $1 \in k((G))$? Not surprisingly, to $1 + t + t^2 + \cdots + t^n + \cdots$. Where does it send s? We might expect that to go to $s + st + st^2 + \cdots + st^n + \cdots$; but rewriting the terms of this expression in our normal form, it becomes $s + t^{-1}s + t^{-2}s + \cdots + t^{-n}s + \cdots$, so under (43), these terms form a *descending* chain; so that expression does not describe a member of $k((G))$. Rather, we find that $(1-t)^{-1}$ sends s to the element $-st^{-1} - st^{-2} - \cdots - st^{-n} - \cdots = -ts - t^2 s - \cdots - t^n s - \cdots$. (This is an example of the phenomenon noted in §6, that given $x \in kG - \{0\}$, in this case $1 - t$, if we want to compute $g\,x^{-1}$ for some $g \in G$, the member of $\mathrm{supp}(x)$ which behaves like the "leading term" of x can depend on g.) So in its action on $1 \in k((G))$, the operator $(1-t)^{-1}$ "looks like" $\sum_{i\geq 0} t^i$, while in its action on s, it "looks like" $\sum_{i<0} -t^i$.

What if we ignore the ordering of G that has allowed us to define $k((G))$, and simply calculate in the right kG-module k^G? Then we find that right multiplication by $1-t$ takes both $\sum_{i\geq 0} t^i$ and $\sum_{i<0} -t^i$ to 1. That these both can be true follows from the fact that $1-t$ annihilates $(\sum_{i\geq 0} t^i) - (\sum_{i<0} -t^i) = \sum_{-\infty}^{\infty} t^i$.

This suggests that we look at a factor module of the kG-module k^G by a submodule containing $\sum_{-\infty}^{\infty} t^i$. Then the question "$\sum_{i\geq 0} t^i$ or $\sum_{i<0} -t^i$?" will disappear – these expressions represent the same element. So perhaps, for a general right ordered group G, we should, in place of $k((G))$, look at a module obtained by dividing k^G by some submodule of "degenerate" elements. But it is not clear how to find such a factor module with good properties; in particular, how the right orderability of G would be used.

12.2. **Partitioning G.** Suppose G is a right ordered group and S a finite subset of G. We have seen that for an element $g \in G$, the ordering on $gS \subseteq G$ need not be the one induced by the ordering of $S \subseteq G$; or to put it another way, the ordering $\leq_g$ on S defined by $s \leq_g t \iff gs \leq gt$ can depend on g. (We remark that since our ordering on G is right-invariant, the relation $gs \leq gt$ is equivalent to $gsg^{-1} \leq gtg^{-1}$, i.e., to the result of conjugating the given ordering on G by g.)

However, since S is finite, there are only finitely many orderings on S; so suppose we classify the elements $g \in G$ according to the restriction to S of the ordering $\leq_g$. If, for each total ordering $\preceq$ on S, we define the subset $G_\preceq = \{g \in G \mid (\leq_g|_S) = \preceq\}$, and write $k((G))$ as $\bigoplus_\preceq k((G_\preceq))$, i.e., as the direct sum of the subspaces of elements having supports in the various subsets $G_\preceq$, then we might expect multiplication by an element of kG with support in S to be "well-behaved" on each summand of this decomposition.

Unfortunately, some things we might hope for do not hold. For instance, the subset $G_\preceq$ of G containing 1, namely the one for which $\preceq$ is the ordering of S induced by its inclusion in G, need not be closed under multiplication.

To get an example of this, let us start with a free abelian group on two generators y and z, and formally write z as y^ω where ω denotes a primitive cube root of unity, so that we can write the general element $y^i z^j$ of this groups as $y^{i+\omega j}$ $(i, j \in \mathbb{Z})$. Now let G be the extension of that abelian group by an element x which acts by

$$(44) \qquad y^h x \ = \ x\, y^{\omega h} \qquad \text{for } h \in \mathbb{Z}[\omega]$$

(compare (42)). Since the group generated by the commuting elements y and y^ω is right orderable, as is the group generated by x, the same is true of the extension group G [8, statement 3.7]. (On the other hand, the fact that the group generated by y and y^ω has no ordering invariant under the action of x implies that G has no two-sided invariant ordering.) Let us fix a right-invariant ordering $\leq$ on G. Note that the three elements y, y^ω, y^{ω^2} of the orbit of y under conjugation by $\langle x \rangle$ have product 1. From the fact that the positive cone of $\leq$ is closed under multiplication, it follows that these three elements are not all on the same side of 1 with respect to $\leq$; so two of them must be on one side and the third on the other. Thus, one of these three elements must have the property that it stays on the same side of 1 under conjugation by x, but moves to the opposite side under conjugation by x^2. Calling the member of $\{y, y^\omega, y^{\omega^2}\}$ which has this property s, letting $S = \{1, s\}$, and letting $\preceq$ be the ordering on S induced by its inclusion in G, we see that $1, x \in G_\preceq$, but $x^2 \notin G_\preceq$.

So it does not look easy to put this decomposition of G to use.

Let us note a common generalization of the right-ordered groups described by (42) and (44). Let $\mathbb{Z}[c, c^{-1}]$ be the subring of the complex numbers generated by a fixed nonzero complex number and its inverse, and let us write the additive group of $\mathbb{Z}[c, c^{-1}]$ multiplicatively as $y^{\mathbb{Z}[c,c^{-1}]}$. Let G be the extension of this group by the infinite cyclic group generated by an elements x, with the action

$$(45) \qquad y^h x \ = \ x\, y^{ch} \quad \text{for } h \in \mathbb{Z}[c, c^{-1}].$$

We may order G by letting

$$(46) \qquad y^h x^n \ \geq \ y^{h'} x^{n'} \iff \begin{cases} \text{either} & n > n', \\ \quad \text{or} & n = n' \ \text{ and } \mathrm{Re}(h) > \mathrm{Re}(h'), \\ \quad \text{or} & n = n', \ \ \mathrm{Re}(h) = \mathrm{Re}(h'), \ \text{ and } \ \mathrm{Im}(h) \geq \mathrm{Im}(h')\,. \end{cases}$$

(Cf. (43).) In this situation, if c has the form $e^{\alpha\pi i}$ $(\alpha \in \mathbb{R})$, then for any S with more than one element, and any ordering $\preceq$ of S such that $G_\preceq$ is nonempty, it is not hard to show that $\{n \in \mathbb{Z} \mid x^n \in G_\preceq\}$ is periodic (invariant under some nonzero additive translation on $\mathbb{Z}$) if and only if α is rational. So in the irrational case, the sets $G_\preceq$ are particularly messy.

12.3. **One case that would imply the general result we want.** Yves de Cornulier (personal communication) has pointed out that to prove embeddability of kG in a division ring for every right-orderable group G, we 'merely' need to prove this for G the group of order-automorphisms of the ordered set of real numbers, or, alternatively, for G the order-automorphisms of the ordered set of rationals. For it is known [14, Proposition 2.5] that any *countable* right orderable group can be embedded in each of those groups; hence if one of those two group algebras were embeddable in a division ring, then for any right-orderable group G, all of its finitely generated subgroups G_0 would have group algebras kG_0 embeddable in division rings, and from this, a quick ultraproduct argument would give the embeddability of kG itself in a division ring.

12.4. **Can we use lattice-orderability?** Recall the fact mentioned at the end of §1, that the one-sided-orderable groups are the groups embeddable, group-theoretically, in lattice-ordered groups. So what we want is equivalent to saying that group algebra kG of every lattice-ordered group G is embeddable in a division ring. The partial ordering of a lattice-ordered group is required to be invariant under both right and left translations, and it is tempting to hope that we should be able to construct a division ring of formal infinite sums whose supports in G have some nice property with respect to such a lattice ordering.

However, note that any lattice-ordered group G can be embedded group-theoretically, by the diagonal map, in the lattice-ordered group $G \times G^{\mathrm{op}}$, where G^{op} is G with its order-relation reversed. Since the subgroup of $G \times G^{\mathrm{op}}$ given by the image of this embedding is an antichain, it is hard to see how the order structure can be used to pick out a class of infinite sums that would form a division ring and contain even that diagonal subring.

But one might be able to go somewhere with this idea – perhaps defining a permissible infinite sum not just in terms of order relations among the elements of its support, but also looking at properties of the sublattice generated by that support. (Incidentally, the lattice structure of a lattice-ordered group is always distributive [9, Corollary 3.17].)

13. Appendix on prime matrix ideals

Let us recall P. M. Cohn's approach to maps of rings into division rings, which we sketched in §1. It is based on

Definition 17 ([5], [6], [7])**.** *Let $f : R \to D$ be a homomorphism from a ring into a division ring. Then the* singular kernel *$\mathcal{P}$ of f is the set of square matrices over R whose images under f are singular matrices over D.*

Cohn shows that in the above situation, the structure of the division subring of D generated by $f(R)$ is determined by $\mathcal{P}$ ([5], [6], [7]; see also [16]), and he notes that $\mathcal{P}$ has properties (47)-(53) below.

Let me explain in advance the notation of (49) and (50). If A and B are square matrices of the same size, which agree except in their r-th row, or agree except in their r-th column, then $A \nabla B$ is defined to be the matrix which agrees with A and B in all rows or columns but the r-th, and has for r-th row or column the sum of those rows or columns of A and B. The specification of whether rows or columns are involved, and of the r in question, is understood to be determined by context. Cohn calls $A \nabla B$ the *determinantal sum* of A and B, in view of the expression, when R is commutative, for the determinant of that matrix.

Here are the properties of the singular kernel $\mathcal{P}$ of a homomorphism of R into a division ring used by Cohn:

(47) $\mathcal{P}$ contains every square $n \times n$ matrix that can be written as the product of an $n \times n{-}1$ matrix and an $n{-}1 \times n$ matrix over R. (Cohn calls such products *non-full* matrices.)

(48) If A is a matrix lying in $\mathcal{P}$, and B is *any* square matrix over R, then $\mathcal{P}$ contains the matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, denoted $A \oplus B$.

(49) If $\mathcal{P}$ contains square $n \times n$ matrices A and B which agree except in the r-th column for some r, then it contains their determinantal sum $A \nabla B$ with respect to that column.

(50) If $\mathcal{P}$ contains square $n \times n$ matrices A and B which agree except in the r-th row for some r, then it contains their determinantal sum $A \nabla B$ with respect to that row.

(51) If $\mathcal{P}$ contains a matrix of the form $A \oplus 1$, where 1 denotes the 1×1 matrix with entry 1, and $\oplus$ is defined as in (48), then $A \in \mathcal{P}$.

(52) The 1×1 matrix 1 is not in $\mathcal{P}$.

(53) If $A \oplus B \in \mathcal{P}$, then $A \in \mathcal{P}$ or $B \in \mathcal{P}$.

In [5], [7], and many other works, Cohn calls a set of square matrices over a ring R which satisfies (47)-(51) a *matrix ideal*, and calls a matrix ideal which also satisfies (52) and (53) *prime*. He proves that for every prime matrix ideal $\mathcal{P}$ of R, the ring gotten by universally adjoining to R inverses to all matrices not in $\mathcal{P}$ is a local ring, whose residue ring is a division ring D such that the singular kernel of the induced map

$R \to D$ is precisely $\mathcal{P}$ [7, Theorem 7.4.3]. Thus since, as mentioned, the singular kernel of a map $f : R \to D$ determines the division subring generated by the image of R, it follows that homomorphisms from R into division rings generated by the images of R are, up to isomorphisms making commuting triangles with those homomorphisms, in bijective correspondence with prime matrix ideals of R. We see from Definition 17 that the homomorphism $R \to D$ corresponding to $\mathcal{P}$ is one-to-one if and only if $\mathcal{P}$ contains no nonzero 1×1 matrix.

However, in [6, §4.4], Cohn defines matrix ideals by conditions (47)-(49) and (51), omitting (50), again calling such a matrix ideal prime if (52) and (53) hold. (He notes at [6, p. 164, two lines after display (30)] that one can similarly define determinantal sums with respect to rows, "but this will not be needed".) He claims to prove, under this definition, the same result cited above, that the prime matrix ideals are precisely the singular kernels of homomorphisms to division rings. This, together with the corresponding result proved using the stronger definition, would imply that the two definitions of prime matrix ideal are equivalent.

Now the shortened definition of prime matrix ideal would lend itself to an approach similar to the one we took in §5. Namely, given a right R-module M, we could for each $n \geq 0$ consider the $n \times n$ matrices over R which act non-injectively on M^n, verify that these together satisfy *most* of the conditions to form a prime matrix ideal (details below), and examine when they satisfy the remaining conditions. But this would be more difficult if we used the definition appearing in most of Cohn's work on this subject, containing condition (50).

Unfortunately, I have difficulty verifying one of the steps in the proof in [6] that prime matrix ideals, defined without condition (50), yield homomorphisms to division rings. Fortunately, Peter Malcolmson has been able to supply an argument, which with his permission I give below, showing that in the stronger definition of prime matrix ideal, condition (50) can be replaced by a condition that *is* easily verifiable for the set of matrices that act non-injectively on product modules M^n for a right R-module M.

Let me first sketch, for the reader with [6] in hand, my problem with the development given there. It concerns the assertion in the middle of p. 164 that the operation $\odot$ on square matrices introduced on that page respects equivalence classes under the equivalence relation $\sim$ defined on p. 163. That equivalence relation is generated by three sorts of operations on matrices: certain operations of left multiplication by elementary matrices, certain operations of right multiplication by elementary matrices, and certain operations of deleting rows and columns. If we have $a_1 \sim a_2$ via a left multiplication operation, or via the deletion operation, it is indeed straightforward that $a_1 \odot b \sim a_2 \odot b$ via the same operation; but if $a_1 \sim a_2$ via a right multiplication operation, I don't see why $a_1 \odot b \sim a_2 \odot b$ should hold. Similarly, if $b_1 \sim b_2$ via a right multiplication operation or a deletion operation, I have no problem, but if they are related via a left multiplication operation, I don't see that $a \odot b_1 \sim a \odot b_2$.

Here, however, is Malcolmson's result.

Lemma 18 (P. Malcolmson, personal communication)**.** *Let R be a ring, and $\mathcal{P}$ a set of square matrices over R satisfying* (47)-(49) *and* (51)*. Then $\mathcal{P}$ also satisfies* (50) *if and only if it satisfies*

(54) *For each $n > 0$, the set of $n \times n$ matrices in $\mathcal{P}$ is closed under left multiplication by matrices $I_n \pm e_{ij}$ $(i \neq j)$.*

Proof. "Only if" follows from [5, 2nd ed., point (f) on p. 398], which shows that a set $\mathcal{P}$ of square matrices satisfying conditions (47)-(51) (there called M.1-M.4, with M.3 being the conjunction of (49) and (50)) is closed under right and left multiplication by arbitrary square matrices. Below, we shall prove "if"; so assume (54) holds.

By a familiar calculation, the group generated by the elementary matrices $I + e_{ij}$ and their inverses $I - e_{ij}$ contains the matrices whose left actions transpose an arbitrary pair of rows, changing the sign of one of them. (The essence of that calculation is the 2×2 case, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.) This will be a key tool later on, but let us first use it in a trivial way: it allows us to reduce to the case where the row with respect to which we want to show closure under determinantal sums is the last row of our matrices. (That reduction also uses the observation that the operation of determinantal sum with respect to any row respects the operation of reversing the sign of a particular row in all matrices.)

Another fact we shall use is that if $\mathcal{P}$ is a set of square matrices satisfying (47) and (49), A an $n\times n$ matrix, B an $n'\times n'$ matrix, and C an $n'\times n$ matrix, then

(55) $\quad \mathcal{P}$ contains $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ if and only if it contains $\begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$.

This can be seen from point (e) on p. 397 of [5, 2nd edition]. (Although both (49) and (50) are assumed there, only the former is used in the calculation.)

Now to prove the "if" direction of our lemma, let H be an $n{-}1\times n$ matrix over R, and a, b length-n rows such that

(56) $\quad \begin{pmatrix} X \\ a \end{pmatrix},\ \begin{pmatrix} X \\ b \end{pmatrix} \in \mathcal{P}.$

Applying (48), we get $\begin{pmatrix} X & 0 \\ a & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} X & 0 \\ b & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{P}$. Applying (55) to these matrices, we get $\begin{pmatrix} X & 0 \\ a & 0 \\ b & 1 \end{pmatrix},\ \begin{pmatrix} X & 0 \\ b & 0 \\ -a-b & 1 \end{pmatrix} \in \mathcal{P}$. If we left-multiply the first of those two matrices by $I_n + e_{n-1,n}$, we get $\begin{pmatrix} X & 0 \\ a{+}b & 1 \\ b & 1 \end{pmatrix} \in \mathcal{P}$, while if we left multiply the second by a product of elementary matrices that transposes the last two rows and changes the sign of one of them, we get $\begin{pmatrix} X & 0 \\ a{+}b & -1 \\ b & 0 \end{pmatrix} \in \mathcal{P}$.

These two matrices differ only in their last column, and applying (49) to their determinantal sum with respect to that column gives $\begin{pmatrix} X & 0 \\ a{+}b & 0 \\ b & 1 \end{pmatrix} \in \mathcal{P}$. Applying (55) again, this gives $\begin{pmatrix} X & 0 \\ a{+}b & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{P}$, hence by (51), $\begin{pmatrix} X \\ a{+}b \end{pmatrix} \in \mathcal{P}$. Having gotten this from (56), we have proved the case of (50) where $r = n$, which we have seen is equivalent to the general case. $\square$

We can now obtain a result parallel to Lemma 8. As in the context of that lemma, elements of M^n will be regarded as row vectors, on which $n\times n'$ matrices over R act on the right. (Thus, the kernel K referred to in (58) below is not, in general, an R-submodule of M^n, but merely an additive subgroup.)

Lemma 19. *Let M be a nonzero right module over a ring R, and $\mathcal{P}$ the set of square matrices A over R such that, if A is $n\times n$, A gives a non-injective map $M^n \to M^n$. Then*

(i) *$\mathcal{P}$ satisfies* (48), (51), (52), (53), *and* (54).

(ii) *A necessary and sufficient condition for $\mathcal{P}$ to satisfy* (47) *is*

(57) *No $n\times n{-}1$ matrix over R induces an injection of abelian groups $M^n \to M^{n-1}$* $(n>0)$.

(iii) *A sufficient condition for $\mathcal{P}$ to satisfy* (49) (*and hence, by* (i) *and Lemma 18,* (50)) *is*

(58) *If $K \subseteq M^n$ is the kernel of the action on M^n of an $n\times n{-}1$ matrix over R, then either* (a) *every map $M^n \to M$ which is induced by a height-n column vector over R, and is nonzero on K, is one-to-one on K, or* (b) *no such map is one-to-one on K.*

Thus, if both (57) *and* (58) *hold, then $\mathcal{P}$ is a prime matrix ideal of R. Hence if, further, the right R-module M is faithful, then R is embeddable in a division ring.*

Proof. All parts of (i) are straightforward. (Condition (54) is a special case of the observation that $\mathcal{P}$ is closed under left and right multiplication by arbitrary invertible matrices.)

(ii) is also easy: Assume first that $\mathcal{P}$ satisfies (47). If A is an $n\times n{-}1$ matrix over R, then extending A by a zero column, we get an $n\times n$ matrix A' which is non-full in the sense stated in (47), hence by (47) lies in $\mathcal{P}$, hence, by our choice of $\mathcal{P}$, is not one-to-one on M^n. Hence A is not one-to-one there, proving (57).

Conversely, if A is a non-full $n \times n$ matrix, say $A = BC$ where B is $n \times n{-}1$ and C is $n{-}1 \times n$, then assuming (57), B acts on M^n with nonzero kernel, hence so does A, so $A \in \mathcal{P}$.

To prove (iii), let $A, B \in \mathcal{P}$ be as in (49), C the common $n \times n{-}1$ submatrix obtained by deleting the r-th columns from these, and K the kernel of the action of C on M^n. From the fact that $A, B \in \mathcal{P}$, we see that $K \neq \{0\}$. Now if, as in the first alternative of (58), every map $M^n \to M$ induced by a height-n column vector restricts to either the zero map or a one-to-one map on K, then for A and B to lie in $\mathcal{P}$, their r-th columns must both induce the zero map on K, hence so will the sum of those columns, showing (since $K \neq \{0\}$) that $A \nabla B$ lies in $\mathcal{P}$. On the other hand, if *no* height-n column vector induces a one-to-one map on K, then in particular, the r-th column of $A \nabla B$ does not, giving the same conclusion.

The first sentence of the last paragraph of the lemma is now clear. The final sentence follows by the results of [5] cited earlier. □

Remark: The converse of (iii) above is not true; i.e., $\mathcal{P}$ can satisfy (49) without satisfying (58). For example, suppose $R = \mathbb{Z}$ and M is the module $\mathbb{Z}/p^2\mathbb{Z}$ for some prime p. It is not hard to see that the $\mathcal{P}$ of Lemma 19 will consist of the square matrices over $\mathbb{Z}$ whose determinants are divisible by p. This is the prime matrix ideal corresponding to the homomorphism of $\mathbb{Z}$ into the field $\mathbb{Z}/p\mathbb{Z}$, so in particular, it satisfies (49). On the other hand, for any $n \geq 1$, the subgroup $K = \{0\}^{n-1} \times M \subseteq M^n$ is easily seen to be the kernel of the action of an $n \times n{-}1$ matrix; but if we take a height-n column vector with 1 in the n-th position, and another with p in that position, then both are nonzero on K, but the former is one-to-one while the latter is not; so (58) fails.

On a general note, the above approach to obtaining homomorphisms into division rings from modules may be thought of as less convenient than the one developed in §5, in that it leaves us the two conditions (59) and (60) to verify, in contrast to the one condition (18) (with equivalent forms (19), (20)). But it is, in another way, more robust, in that the concept of prime matrix ideal is left-right symmetric, and this allows us to produce a version of the same result based on surjectivity rather than injectivity *without* switching from right to left modules as we did in that section. Rather, the switch between injectivity and surjectivity can be made independently of whether we use right or left modules. The next lemma is the result based on right modules and surjectivity; the two left-module results are obtained from the two right-module results in the obvious way. We leave to the reader the proof of the lemma, which exactly parallels that of Lemma 19.

Lemma 20. *Let M be a nonzero right module over a ring R, and $\mathcal{P}$ the set of square matrices A over R such that, if A is $n \times n$, A gives a* non-surjective *map $M^n \to M^n$. Then*

(i) *$\mathcal{P}$ satisfies* (48), (51), (52), (53), *and the left-right dual of* (54) (*closure under* right *multiplication by matrices $I_n \pm e_{ij}$*).

(ii) *A necessary and sufficient condition for $\mathcal{P}$ to satisfy* (47) *is*

(59) *No $n{-}1 \times n$ matrix over R induces a surjection of abelian groups $M^{n-1} \to M^n$* $(n > 0)$.

(iii) *A sufficient condition for $\mathcal{P}$ to satisfy* (50) (*and hence, by* (i) *and the left-right dual of Lemma 18,* (49)) *is*

(60) *If $I \subseteq M^n$ is the image of M^{n-1} under the action of an $n{-}1 \times n$ matrix over R, then either* (a) *every map $M \to M^n$ which is determined by a length-n row vector and has image not contained in I has image which, with I, spans the additive group of M^n, or* (b) *no such map has image which, with I, spans that additive group.*

Thus, if both (59) *and* (60) *hold, then $\mathcal{P}$ is a prime matrix ideal of R. Hence if, further, every nonzero element of R carries M surjectively to itself, then R is embeddable in a division ring.* □

14. Acknowledgements

I am indebted to Pace Nielsen for many invaluable comments and corrections to earlier drafts of this note, to A. M. W. Glass for a helpful discussion of what is known about right-orderable groups, to Peter Malcolmson for showing the way to Lemma 18, and to Yves de Cornulier for the observation of §12.3.

References

[1] George M. Bergman, *Coproducts and some universal ring constructions*, Trans. A. M. S. **200** (1974) 33–88. MR0357503

[2] George M. Bergman, *Constructing division rings as module-theoretic direct limits*, Trans. A. M. S. **354** (2002) 2079–2114. MR1881031

[3] George M. Bergman, *An Invitation to General Algebra and Universal Constructions,* 2015, Springer Universitext, x+572 pp.. `http://dx.doi.org/10.1007/978-3-319-11478-1` . MR3309721

[4] Paul M. Cohn, *Un critère d'immersibilité d'un anneau dans un corps gauche,* C. R. Acad. Sci. Paris Sér. A-B **272** (1971) A1442–A1444. MR0279133

[5] P. M. Cohn, *Free rings and their relations,* London Mathematical Society Monographs, No. 2, xvi + 346 pp., 1971. MR0800091. Second ed.: same Monographs, No. 19, xxii + 588 pp., 1985. MR0371938

[6] P. M. Cohn, *Skew fields. Theory of general division rings.* Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge. xvi + 500 pp., 1995. MR1349108

[7] P. M. Cohn, *Free ideal rings and localization in general rings,* New Mathematical Monographs, 3. Cambridge University Press. xxii + 572 pp., 2006. MR2246388

[8] Paul Conrad, *Right-ordered groups,* Michigan Math. J. **6** (1959) 267–275. `http://projecteuclid.org/download/pdf_1/euclid.mmj/1028998233` MR0106954

[9] Michael R. Darnel, *Theory of lattice-ordered groups*, Monographs and Textbooks in Pure and Applied Mathematics, 187. Marcel Dekker, 1995. viii+539 pp. ISBN: 0-8247-9326-9. MR1304052

[10] N. I. Dubrovin, *Invertibility of the group ring of a right-ordered group over a division ring* (Russian), Mat. Zametki **42** (1987) 508–518, 622. `http://www.mathnet.ru/links/23b614b35d59ceea7b08b86289719949/mzm5014.pdf` . Transl. in Mathematical Notes of the Academy of Sciences of the USSR **42** (1987) 781–786. `http://link.springer.com/article/10.1007%2FBF01138310` . (That translation has many errors.) MR0917804

[11] N. I. Dubrovin, *Rational closures of group rings of left-ordered groups* (Russian), Mat. Sb. **184** (1993) 3–48. Transl. in Russian Acad. Sci. Sb. Math. **79** (1994) 231–263. `http://dx.doi.org/10.1070/SM1994v079n02ABEH003498` . MR1235288

[12] N. I. Dubrovin, *Rational operators of the space of formal series* (Russian), Fundam. Prikl. Mat. **12** (2006) 9–53. Transl. in J. Math. Sci. (N.Y.) **149** (2008) 1191–1223. `http://link.springer.com/article/10.1007%2Fs10958-008-0059-3` . MR2249705

[13] Graham Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc. (3) **2** (1952) 326–336. MR0049867

[14] Peter A. Linnell, *Left ordered amenable and locally indicable groups*, J. London Math. Soc. (2) **60** (1999) 133–142. MR1721820

[15] A. I. Mal'cev, *On the embedding of group algebras in division algebras* (Russian), Doklady Akad. Nauk SSSR (N.S.) **60** (1948) 1499–1501. MR0025457

[16] Peter Malcolmson, *A prime matrix ideal yields a skew field,* J. London Math. Soc. (2) **18** (1978) 221–233. `http://jlms.oxfordjournals.org/content/s2-18/2/221` . MR0509937

[17] Peter Malcolmson, *Determining homomorphisms to skew fields,* J. Algebra **64** (1980) 399–413. `http://dx.doi.org/10.1016/0021-8693(80)90153-2` . MR0579068

[18] V. D. Mazurov and E. I. Khukhro, ed.s, *The Kourovka notebook. Unsolved problems in group theory*, Seventeenth edition. Russian Academy of Sciences Siberian Division, Institute of Mathematics, Novosibirsk, 2010. 139 pp. MR3235009

[19] B. H. Neumann, *On ordered division rings*, Trans. Amer. Math. Soc. **66** (1949) 202–252. MR0032593

[20] D. J. A. Welsh, *Matroid Theory,* London Mathematical Society Monographs, No. 8, 1976. MR0427112

University of California, Berkeley, CA 94720-3840, USA

E-mail address: `gbergman@math.berkeley.edu`