`Comments, corrections, and related references welcomed, as always!`

TEXed September 2, 2009

THE CONDITION $(\exists\, x_1,\dots,x_n)\ A = x_1A+\dots+x_nA$ IN NONASSOCIATIVE ALGEBRAS, AND BASE-CHANGE

GEORGE M. BERGMAN

ABSTRACT. To any not-necessarily-associative finite-dimensional algebra A over a field k such that $AA = A$, i.e., such that every element may be written as a sum of products, we can associate the least integer n such that A can be written $x_1A+\dots+x_nA$ for $x_1,\dots,x_n \in A$. If k is infinite, this invariant is unchanged under extension of base field. There are counterexamples if k is finite, or A infinite-dimensional.

The results in this write-up are "orphans". Originally, this was to be part of a note with N. Nahlus in which, using the structure theory of finite-dimensional simple Lie algebras L over an algebraically closed field of characteristic 0, it would be shown that every such L contains elements x_1 and x_2 such that

(1) $\quad L \;=\; [x_1, L] \;+\; [x_2, L],$

and it would then be deduced, with the help of the proposition in §1 below, that the same is true of finite-dimensional simple Lie algebras over *any* field of characteristic 0. The consequence that every element of such a Lie algebra is a sum of two brackets was to be used in [1] and [2] in proving a result on homomorphic images of infinite direct products of such Lie algebras.

Subsequently, we learned of the result of [3], that every finite-dimensional simple Lie algebra over an algebraically closed field of characteristic not 2 or 3 is generated as an algebra by two elements. By a method having some features in common with that of §1 below, we were able to show from this that ([1, Theorem 26]) every finite-dimensional simple Lie algebra L over any infinite field of characteristic not 2 or 3 can be written as in (1) (though not every such algebra is generated by two elements ([1, Lemma 38])).

Despite this change of plans, the results of §1 below, simpler than the arguments we now use to prove [1, Theorem 26], seem worth recording, along with counterexamples to some modified statements. Hence this note. At present, I have no plans of submitting it for publication.

Results by Nahlus on particular elements x_1 and x_2 satisfying (1) in a finite-dimensional split simple Lie algebra over a field of characteristic 0, and related matters, are similarly recorded in [4].

The idea of §1 below is well-known in the study of Lie algebras: one proves that the set of elements, or tuples of elements, of a finite-dimensional Lie algebra, that have some property is Zariski open; one shows that the set of points with that property having coordinates in the algebraic closure of the base field is nonempty; and one concludes that the set of points with that property over the original base field is also nonempty. What is not necessarily easy to guess is *which* properties it will be possible to treat in this way. For instance, in a general nonassociative algebra, the property that every element can be written as a sum of n products does not carry over from an extension field to a smaller field; nor vice versa. (For counterexamples see [1, §12.5].) But we shall see below that the property that there exist n elements $x_1,\dots,x_n$ such that $A = x_1A+\dots+x_nA$ does.

For the reader already familiar with the general technique, the interesting material here may be the examples in §2.2 and §2.3.

1. Linear maps and base change.

I will not assume familiarity with the Zariski topology; we will obtain our results from first principles, starting with

---

2000 *Mathematics Subject Classification.* Primary: 17A01.

Key words and phrases. idempotent nonassociative algebra; least number of x_i needed to write $A = \sum x_iA.$.

This preprint accessible online at the four URLs http://math.berkeley.edu/~ gbergman/papers/x1Adots.{tex,dvi,ps,pdf} .

Lemma 1. *Let k be an infinite field, p, q and r natural numbers, and*

(2) $$f:\ k^p \times k^q \ \to\ k^r$$

a map which is polynomial as a function of the arguments in k^p, and linear in the arguments in k^q. Let K be any extension field of k, and let

(3) $$f_K:\ K^p \times K^q \ \to\ K^r$$

be the extension of f given by the same polynomial expressions.

If there exists an $x \in K^p$ such that the induced linear map $f_K(x,-): K^q \to K^r$ is surjective, then there also exists $x' \in k^p$ such that the linear map $f(x',-): k^q \to k^r$ is surjective. (*The converse is also true, even without the condition that k be infinite.*)

Proof. Since f is linear in the arguments in k^q, we can get from f a matrix-valued function

(4) $$F:\ k^p \ \to\ M_{r\times q}(k),$$

such that for $a \in k^p$, $b \in k^q$,

(5) $$F(a)\, b \ =\ f(a,b).$$

Since f is polynomial in the argument from k^p, (4) will also be a polynomial map.

For $x \in k^p$, $f(x,-)$ is surjective if and only if $F(x)$ is a matrix of rank r, i.e., if and only if one of its $r \times r$ minors is nonzero. Such a minor is given by a polynomial in the coordinates of x, so since k is an infinite field, the condition that there exist an x for which that minor has nonzero value is equivalent to the condition that the expression for that minor be a nonzero polynomial in the entries of x.

Now f_K is given by the same polynomials as f, so it determines the same system of determinantal-minor polynomials. This immediately yields our main assertion, and the converse of that result. To see that that converse holds without the assumption that k be infinite, note that a point of k^p where a polynomial is nonzero is also a point of K^p where that polynomial is nonzero. □

In the above lemma, we allowed f to be polynomial in k^p rather than specifying that it be linear, because the proof worked as well under that general hypothesis. In the next two results, for simplicity of statement, we forgo that extra generality; but at the end of this section we will comment briefly on consequences we can get using the greater generality of Lemma 1.

Corollary 2. *Let k be an infinite field, let A, B and C be finite-dimensional k-vector-spaces, and let*

(6) $$m:\ A \times B \ \to\ C$$

be a bilinear map. Let K be any extension field of k, let $A_K = A \otimes_k K$, $B_K = B \otimes_k K$, $C_K = C \otimes_k K$, and let

(7) $$m_K:\ A_K \times B_K \ \to\ C_K$$

be the map arising from (6) *by extension of scalars.*

Then if, for a given natural number n, there exist $a_1,\dots,a_n \in A_K$ such that

(8) $$m_K(a_1,\, B_K) + \dots + m_K(a_n,\, B_K) \ =\ C_K,$$

then there also exist $a'_1,\dots,a'_n \in A$ such that

(9) $$m(a'_1, B) + \dots + m(a'_n, B) \ =\ C.$$

(*The converse is true without the condition that k be infinite.*)

Proof. Given n, let

(10) $$f:\ A^n \times B^n \ \to\ C$$

be defined by

(11) $$f(a_1,\dots,a_n;\, b_1,\dots,b_n) \ =\ m(a_1,b_1) + \dots + m(a_n,b_n).$$

This will be linear (hence polynomial) in the argument from A^n, and also linear in the argument from B^n. If we choose coordinates using any k-bases of A^n, B^n and C, the preceding lemma immediately gives the asserted result. □

In particular, we have

Proposition 3. *Let k be an infinite field, A a finite-dimensional not-necessarily-associative k-algebra (a finite-dimensional k-vector-space given with a bilinear map $A \times A \to A$), and n a natural number.*

Then for any extension field K of k, writing A_K for the algebra $A \otimes_k K$, if there exist $x_1, \dots, x_n \in A_K$ such that

$$x_1 A_K + \cdots + x_n A_K \;=\; A_K, \tag{12}$$

then there also exist $x'_1, \dots, x'_n \in A$ such that

$$x'_1 A + \cdots + x'_n A \;=\; A. \tag{13}$$

(*The converse is true without the condition that k be infinite.*)

In other words, if $A = AA$, then the least n for which A has such an n-tuple of elements is invariant under base-change. □

Lemma 1 can actually be used to get invariance statements for a much wider variety of conditions on a finite-dimensional algebra A than the existence of $x_1, \dots, x_n$ satisfying $A = x_1 A + \cdots + x_n A$. For a few random examples, we get the corresponding results for conditions such as

(14) There exist $x_i,\, y_i,\, z_i$ $(i = 1, \dots, n)$ such that $A = (x_1A)(y_1z_1) + \cdots + (x_nA)(y_nz_n)$.

(15) There exist x_i $(i = 1, \dots, n)$ such that $A = (x_1A)(x_1x_1) + \cdots + (x_nA)(x_nx_n)$.

(16) There exist $x_i,\, y_i$ $(i = 1, \dots, n)$ such that, writing $\{a, x, y\}$ for $a(xy) - (ax)y$, one has $A = \{A, x_1, y_1\} + \cdots + \{A, x_n, y_n\}$.

(17) There exists $x \in A$ such that $A = Ax + (Ax)x + ((Ax)x)x + \cdots + ((\dots(Ax)\dots)x)x$ (n terms).

The key point is that in each of these formulas, once the x_m etc. are fixed, the expression is linear in the remaining A-valued variables. Proposition 3 is likely to be the most useful case, and I felt it would be most transparent to formulate that case explicitly, then note that cases like (14)-(17) can be gotten from Lemma 1 if needed. One can likewise get the generalization of Proposition 3, applicable to not necessarily idempotent algebras A, in which the right-hand sides of (12) and (13) are replaced by $A_K A_K$ and $A\,A$ respectively; and similarly generalize the results based on (14)-(17).

2. Some counterexamples.

2.1. **Left versus right.** The statement of Proposition 3 is asymmetric, in that the fixed elements x_i appear to the left of the A's. Of course, by an obvious symmetry argument, that result implies its left-right dual. Let us give a quick example showing that for an algebra A, the number of summands needed on the right can be very different from the number needed on the left; then a variant example, showing that both these numbers can be equal, but be much larger than the least n such that every element of A is a sum of n products (called in [1] the "idempotence rank" of A).

Let k be a field, n a natural number, and A the (associative, nonunital) subalgebra of the $n \times n$ matrix algebra $M_n(k)$ spanned by $e_{11}, e_{21}, \dots, e_{n1}$. Thus, the multiplication of A is given by

$$e_{i1}\, e_{j1} \;=\; \begin{cases} e_{i1} & \text{if } j = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

We see that for each $x \in A$,

$$x\,A \;=\; x\,(ke_{11}) \;=\; k\,x. \tag{19}$$

Hence, if we wish to span A using summands xA, we need $\dim_k(A) = n$ of these. On the other hand, e_{11} is a right unit for A, so the one term $A\,e_{11}$ gives all of A.

In this example, every element can be written as a single product. If we take the direct product of this algebra and its opposite, we see that that is still the case, but that to get all of A as a sum of terms $x\,A$, or $A\,x$, or even a mixture of both, n summands are still needed.

2.2. **The need for k to be infinite.** I do not know any Lie or associative examples showing the need for k to be infinite in Proposition 3; but here is a class of non-Lie, nonassociative examples.

Let k be any field, d a positive integer, and

(20) $\quad A \;=\;$ the k-vector-space of matrices with zero main diagonal $\subseteq\; M_d(k)$.

Let $f: A \to M_d(k)$ be a map which takes each matrix $x \in A$ to a *diagonal* matrix $f(x)$, by assigning to each position on the diagonal the entry found in some fixed corresponding position in x, with no position used more than once, and with all the diagonal positions in x considered "the same position" (since they all have the same value, 0. Thus, these are not used more than once, if at all.) For instance, we might take

(21) $\quad f(a) \;=\; \sum_{i=1}^{d} e_{i1}\, a\, e_{ii}$, which moves the entries in the first row of a onto the diagonal, and ignores all other entries,

or

(22) $\quad f(a) = \sum_{i=1}^{d} e_{ii}\, a\, e_{i+1,i}$, which moves each $a_{i,i+1}$ to the (i,i) position. Here we take arithmetic of subscripts to be modulo d, so that for $i = d$, the symbol $e_{i+1,i}$ means e_{1d}.

Given any such f, we may define an algebra structure on A by letting

(23) $\quad a * b \;=\; f(a)\, b - b\, f(a)$.

By the familiar description of the commutator of a diagonal matrix and an arbitrary matrix, the (i,j) entry of $a*b$ arises by multiplying the (i,j) entry of b by the difference between the i-th and j-th diagonal entries of $f(a)$. (In particular, $a*b$ is indeed A-valued.)

Now if $\mathrm{card}(k) \geq d$, we can choose an $x \in A$ such that the entries of x at the d positions used by the function f are distinct. For such an x, $f(x)$ has distinct diagonal entries, so the linear map $x * - : A \to A$ is bijective, giving $A = x * A$. Conversely, if $\mathrm{card}(k) < d$, then for any $x \in A$, $f(x)$ must have at least two equal diagonal entries, say the i-th and the j-th $(i \neq j)$, whence $x * A$ will contain no elements with nonzero (i,j) entry. Thus, if $k \subseteq K$ are fields with $\mathrm{card}(k) < d \leq \mathrm{card}(k)$, the algebra A constructed as above from K satisfies the condition of Proposition 3 with $n = 1$, but the algebra constructed from k does not.

More generally, given $n \geq 1$, it is not hard to verify that the necessary and sufficient condition for there to exist $x_1, \dots, x_n$ with $A = x_1 * A + \dots + x_n * A$ is

(24) $\quad \mathrm{card}(k)^n \;\geq\; d$.

So by taking d sufficiently large compared with $\mathrm{card}(k)$, one can make the smallest acceptable n arbitrarily large; and then, by passing to a large enough extension field K, bring that number down to 1.

2.3. **The need for A to be finite-dimensional.** In §1 we assumed our vector spaces and algebras finite-dimensional so that we could argue using determinants. Let us show that the results of that section fail without that assumption.

Our constructions will use properties of Dedekind domains; but we will accompany them by a particular example for which we will verify the properties used; so familiarity with the definition and theory of Dedekind domains, though helpful, will not be needed.

Here are the general data we will use to build our examples:

(25) Let k be an infinite field, and D a k-algebra which is a Dedekind domain but not a principal ideal domain, but which becomes a principal ideal domain D_K on extension of scalars to some overfield K of k. Let I be a nonprincipal ideal of D, and x a generator of the induced ideal $I_K = D_K I$ of the principal ideal domain D_K.

For an explicit example, let $k = \mathbb{R}$, let D be the ring $\mathbb{R}[\sin t, \cos t]$ of trigonometric polynomials, and let $I \subseteq D$ be the ideal of elements vanishing at $t = 0$. To see that I is not principal, note that if a trigonometric polynomial $f(t)$ has a simple zero at $t = 0$, then it changes sign there; hence by periodicity, it has opposite signs at 0^+ and $2\pi^-$, hence it must have a zero at some θ in the open interval $(0, 2\pi)$. Thus, the ideal generated by $f(t)$ cannot contain elements of I with no zero at θ (such as $1 - \cos t$). On the other hand, if $f(t)$ has a multiple zero at $t = 0$, the ideal it generates cannot contain elements of I with a simple zero there (such as $\sin t$). So no single element generates I.

However, when we extend scalars to $\mathbb{C}$, we see that

(26) $\quad D_{\mathbb{C}} \;=\; \mathbb{C}[\sin t,\, \cos t] \;=\; \mathbb{C}[e^{it},\, e^{-it}] \;\cong\; \mathbb{C}[z,\, z^{-1}]$

is generated over $\mathbb{C}$ by a transcendental element and its inverse. It is thus a localization of the principal ideal domain $\mathbb{C}[z]$, and so is itself a principal ideal domain.

Thus, the extension $I_{\mathbb{C}} \subseteq D_{\mathbb{C}}$ of the above nonprincipal ideal I must be principal; let us find a generator for it. We know that a nonzero ideal of $\mathbb{C}[z]$ is determined by the locations and multiplicities of the common zeroes in $\mathbb{C}$ of its elements; hence the same will be true of a nonzero ideal of $\mathbb{C}[z, z^{-1}]$, with the stipulation that the locations be at nonzero values of z. Elements of I have zeroes at $t = 0$, hence at $e^{it} = 1$, i.e., $z = 1$, and some elements of I (such as $\sin t$) have simple zeroes there, while others (such as $1 - \cos t$) have no zeroes anywhere else. Hence $I_{\mathbb{C}}$ must consist of all elements of $\mathbb{C}[z, z^{-1}]$ having a zero of multiplicity ≥ 1 at $z = 1$; so we can take $1 - z$ for the generator x in (25). It is easily deduced that I itself is generated over D by the real and imaginary parts of $1 - z = 1 - e^{it}$, namely $1 - \cos t$ and $-\sin t$.

In the general situation of (25), let us now take for the k-bilinear map (6) the multiplication of D, restricted to give a map

(27) $\quad I \times D \to I.$

We see that this will be surjective, and that for $x_1, \dots, x_n \in I$, we will have $m(x_1, D) + \cdots + m(x_n, D) = I$ if and only if $x_1, \dots, x_n$ generate I as an ideal of D. It is known that any ideal of a Dedekind domain can be generated by two elements (e.g., for the I of our above example, $1 - \cos t$ and $\sin t$). So the least integer n as in (9) is 2, while the least value as in (8) is 1. This gives the desired contradiction to the analog of Corollary 2.

Can we get an algebra out of the above?

A quick-and-dirty way to do so is to note that D and I have the same dimension over k, hence there exists a k-vector-space isomorphism $g : D \cong I$. We can thus turn (27) into a multiplication $* : I \times I \to I$ by defining

(28) $\quad a * b \;=\; a\, g(b).$

It is immediate that this multiplication and its extension to K give a counterexample to the conclusion of Proposition 3. But if we want to do any explicit computations, e.g., test this algebra for one or another identity, we cannot do so without a formula for g.

A more complicated, but more concrete construction uses the fact that any nonzero ideal I of a Dedekind domain has an inverse as a fractional ideal; that is, there is a (unique) finitely generated D-submodule I^{-1} of the field of fractions of D such that

(29) $\quad I\, I^{-1} \;=\; D.$

In the trigonometric polynomial case, this consists of the *rational* functions in $\sin t$ and $\cos t$ having at most a simple *pole* at 0, and no poles on the complex plane other than at 0 and its translates by multiple of 2π. Another way to get this object is to first verify that within D, the product ideal $I\,I$ is principal:

(30) $\quad I\, I \;=\; (1 - \cos t)\, D.$

Hence, defining $I^{-1} = (1 - \cos t)^{-1} I$, one has (29). One finds that I^{-1} is generated as a D-module by the elements $(\sin t)/(1 - \cos t) = \cot(t/2)$ and $(1 - \cos t)/(1 - \cos t) = 1$. (In the language of Dedekind domains, (30) shows that I yields an element of order 2 in the ideal class group of D.)

Now back to the general situation of (25). Let

(31) $\quad A \;=\; I^{-1} \times D \times I,$

and define a multiplication $A \times A \to A$ by

(32) $\quad (x^{(-1)}, x^{(0)}, x^{(1)})\,(y^{(-1)}, y^{(0)}, y^{(1)}) \;=\; (x^{(-1)} y^{(0)},\ x^{(1)} y^{(-1)},\ x^{(0)} y^{(1)}).$

It is easy to see that under this multiplication, $AA = A$. (E.g., to verify that one gets every element of I^{-1} in the first position as a sum of products, one uses the fact that $I^{-1} D = I^{-1}$; and similarly for the other positions.) One sees that necessary and sufficient conditions for an element $a = (a^{(-1)}, a^{(0)}, a^{(1)})$ to satisfy $a\,A = A$ are that $a^{(-1)}$ be a generator of I^{-1}, $a^{(0)}$ a generator of D, and $a^{(1)}$ a generator of I, as D-modules. Thus, after extension of scalars to K, there will exist such a generator; but in A itself, there will not.

(I do not know any important identities satisfied by the above algebra A; it is not associative or Lie. It is a D-algebra in an obvious way, and is an order in the 3-dimensional algebra A_L over the field of fractions L of D, which can be described as L^3 with multiplication again given by (32). Because A_L is 3-dimensional, it has the property that if we let $\langle a_1, a_2, a_3, a_4\rangle$ denote any bracketing of the formal product $a_1\,a_2\,a_3\,a_4$, A_L satisfies the identity $\sum_{\pi\in S_4}(-1)^\pi\,\langle a_{\pi(1)}, a_{\pi(2)}, a_{\pi(3)}, a_{\pi(4)}\rangle = 0$. One also sees that the decomposition of A into summands $A^{(-1)} = I^{-1}$, $A^{(0)} = D$, $A^{(1)} = I$ is a $\mathbb{Z}$-grading.)

3. Questions.

The examples constructed in §2.2 and §2.3 above were neither Lie nor associative, suggesting part (a) of the question below.

Question. (a) *Can one find* Lie *or* associative *algebras showing the properties of the examples in* §2.2 *or* §2.3*? I.e., are there Lie or* (*nonunital*) *associative algebras which are either finite-dimensional over a finite field, or infinite-dimensional over an infinite field* (*or, if neither is possible, which are infinite-dimensional over a finite field*)*, such that the number of fixed elements* $x_1,\dots,x_n$ *needed to write the whole algebra as* $x_1A+\dots+x_nA$ *changes under extension of base field?* (*Cf.* [1, Question 45(a)].)

(b) *Do there exist infinite-dimensional idempotent algebras* A *over infinite fields such that the above number changes by more than* 1 *under some extension of base field?* (*Cf. the example of* §2.3 *above, and also* [1, §12.5 and Question 45(b)].)

As noted, any associative algebra as in part (a) above must be nonunital, since in a unital algebra, every element is a single product. In the infinite-dimensional case of (a), and in (b), "the number of fixed elements needed" could be infinite, but in that case, it is not hard to show that it is unaffected by base change, so the real question is for the case where (as in our Dedekind-domain-based example) it is finite.

We would have the example asked for in (b) if we could find an algebra, perhaps commutative, over a field k, with an ideal I that required >2 generators, but became principal on extension of scalars to an overfield K of k.

References

[1] George M. Bergman and Nazih Nahlus, *Homomorphisms on infinite direct product algebras, especially Lie algebras*, preprint, 32 pp., August 2009, readable at http://math.berkeley.edu/~gbergman/papers .

[2] —, *Linear maps on* k^I, *and homomorphic images of infinite direct product algebras*, preprint, 12pp., August 2009, readable at http://math.berkeley.edu/~gbergman/papers .

[3] Jean-Marie Bois, *Generators of simple Lie algebras in arbitrary characteristics*, Mathematische Zeitschrift **262** (2009) 715-741. http://arxiv.org/pdf/0708.1711.

[4] Nazih Nahlus, *On* $L=[L,a]+[L,b]$ *and* $x=[a,b]$ *in split simple Lie algebras*, to be written, title tentative.

(G. Bergman) University of California, Berkeley, CA 94720-3840, USA
E-mail address: gbergman@math.berkeley.edu