A Universal Noncommutative Splitting Algebra for Polynomials

GPT-5.5, edited by Darij Grinberg

July 12, 2026

Abstract

Abstract. Let R be a commutative ring. We show that every homogeneous polynomial $f \in R[x_1, \ldots, x_m]$ of degree n splits into a product of n homogeneous linear forms over a suitable noncommutative ring extension S of R (that is, over a noncommutative R-algebra S whose structure morphism $R \to S$ is injective). The algebra S is universal for such factorizations and is free as an R-module.

The proof uses Bergman's Diamond Lemma: we define S by generators and relations, and the relations form a terminating reduction system that has no ambiguities and thus is confluent.

An analogous result is also shown for inhomogeneous polynomials (with inhomogeneous factors). This easily follows from the homogeneous case by homogenizing and then setting the homogenizing variable equal to 1.

Manifest. This note was written by GPT-5.5 in response to my prompting it with MathOverflow question #27675. There is nothing deep or difficult here; GPT's main contribution was abstracting away from the unnecessary specifics of the question. – DG[1]

1 Introduction

If $f(t) \in R[t]$ is a univariate polynomial over a commutative ring R, then one can construct a commutative R-algebra S whose structure map $R \to S$ is injective (i.e., the ring R canonically embeds into S) and such that $f(t)$ splits into linear factors in $S[t]$. This fact is well-known when $f(t)$ is monic (in which case we can obtain S by successively adjoining roots of $f(t)$ one by one using the classical $R[t]/(f(t))$ construction), and has been proved in [2, Theorem 2.1] in the general case. This can be viewed as an analogue of splitting fields for arbitrary commutative rings (even though this construction does not always produce a field S when R is a field).

This fact cannot be extended to arbitrary multivariate polynomials $f(x_1, x_2, \ldots, x_m)$ while keeping S commutative. The reason is that a multivariate form which is a product

[1] This work is in the public domain.

of linear forms satisfies polynomial equations in its coefficients. Already for quadratic forms, a product of two linear forms (over a ring in which 2 is invertible) has a vanishing catalecticant[2], while a generic quadratic form does not. Thus a general quadratic form cannot be made into a product of linear forms merely by enlarging the commutative coefficient ring.

In the present note, we show that by allowing S to be noncommutative, we can remove all such obstructions and recover a multivariate version of the splitting algebra S. The construction of this algebra S is the usual "make a wish" universal construction: The variables x_i remain central, but the coefficients of the desired linear factors need not commute with each other. When f is homogeneous of degree n, we introduce independent coefficients

$$a_i^{(k)} \qquad (1 \le i \le m,\ 1 \le k \le n)$$

for the k-th linear factor and impose the coefficient identities forced by

$$f = \prod_{k=1}^{n} \left(\sum_{i=1}^{m} x_i a_i^{(k)} \right).$$

This gives a universal noncommutative coefficient algebra. We show that this algebra is free as an R-module; hence the map from R into it is injective.

The freeness proof is the most nontrivial step, but even that is straightforward from the right viewpoint. We regard the defining relations as a reduction system in the sense of Bergman's Diamond Lemma [1]. For each coefficient relation, we choose a monic leading word. Every leading word has the same superscript pattern $1, 2, \ldots, n$. Consequently, a proper suffix of one leading word cannot be a proper prefix of another, and one leading word cannot properly contain another. Thus there are no overlap ambiguities and no inclusion ambiguities, in Bergman's terminology. The irreducible words therefore form an R-basis.

After proving these results, we derive an inhomogeneous version, in which f is no longer required to be homogeneous (and its factors now are allowed to have constant terms). This follows easily from the homogeneous case: homogenize f by adding a new variable x_0, apply the homogeneous theorem, and then set $x_0 = 1$. The final section records the generic determinant as a special case, answering MathOverflow question #27675.

[2]Explicitly: If a quadratic form $ax^2 + by^2 + cz^2 + 2dyz + 2ezx + 2fxy \in R[x, y, z]$ factors as a product $(\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z)$ over a commutative ring, then $\det \begin{pmatrix} a & f & e \\ f & b & d \\ e & d & c \end{pmatrix} = 0$.

2 The homogeneous construction

Let R be a commutative ring, and let $m, n \in \mathbb{N}$, where $\mathbb{N}$ is the set of all nonnegative integers. Assume that n is positive. Let

$$f \in R[x_1, x_2, \ldots, x_m]$$

be a homogeneous polynomial of degree n. Write f as

$$f = \sum_{\substack{\alpha \in \mathbb{N}^m; \\ |\alpha| = n}} c_\alpha x^\alpha,$$

where for each m-tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{N}^m$ we set

$$|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_m, \qquad x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m},$$

and where $c_\alpha = [x^\alpha] f \in R$ are the coefficients of f.

Let

$$F = R\left\langle a_i^{(k)} \mid 1 \leq i \leq m,\ 1 \leq k \leq n \right\rangle$$

be the free associative unital R-algebra on the mn generators $a_i^{(k)}$ with $1 \leq i \leq m$ and $1 \leq k \leq n$. As an R-module, F is free, with a basis consisting of all *words* (i.e., noncommutative monomials) in these mn generators.

We shall construct a quotient R-algebra of F over which the polynomial f factors as $\prod_{k=1}^{n} \left(\sum_{i=1}^{m} x_i a_i^{(k)} \right)$. (So the parenthesized superscripts (k) in $a_i^{(k)}$ distinguish the factors of this factorization.)

For an n-tuple

$$\mathbf{i} = (i_1, i_2, \ldots, i_n) \in \{1, 2, \ldots, m\}^n,$$

define its *content* $\operatorname{cont}(\mathbf{i}) \in \mathbb{N}^m$ to be the m-tuple whose j-th entry (for each $1 \leq j \leq m$) is

$$\operatorname{cont}(\mathbf{i})_j = \#\{k \mid i_k = j\}$$

(so that $x^{\operatorname{cont}(\mathbf{i})} = x_{i_1} x_{i_2} \cdots x_{i_n}$), and we define the *layered word*

$$w(\mathbf{i}) = a_{i_1}^{(1)} a_{i_2}^{(2)} \cdots a_{i_n}^{(n)} \qquad \text{(a word in } F\text{)}.$$

For instance, if $m = 3$ and $n = 4$ and $\mathbf{i} = (1, 3, 2, 3)$, then $\operatorname{cont}(\mathbf{i}) = (1, 1, 2)$ and $w(\mathbf{i}) = a_1^{(1)} a_3^{(2)} a_2^{(3)} a_3^{(4)}$.

For each $\alpha \in \mathbb{N}^m$ with $|\alpha| = n$, set

$$r_\alpha = \sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \operatorname{cont}(\mathbf{i}) = \alpha}} w(\mathbf{i}) - c_\alpha. \tag{1}$$

For example, if $m = 3$ and $n = 3$, then

$$\begin{aligned} r_{(2,0,1)} &= w\left((1,1,3)\right) + w\left((1,3,1)\right) + w\left((3,1,1)\right) - c_{(2,0,1)} \\ &= a_1^{(1)} a_1^{(2)} a_3^{(3)} + a_1^{(1)} a_3^{(2)} a_1^{(3)} + a_3^{(1)} a_1^{(2)} a_1^{(3)} - c_{(2,0,1)}. \end{aligned}$$

Finally define the quotient R-algebra

$$S_f = F / \underbrace{\left(r_\alpha \mid \alpha \in \mathbb{N}^m,\ |\alpha| = n\right)}_{\text{ideal of } F \text{ generated by all these } r_\alpha} \qquad \text{of } F.$$

Consider the polynomial ring $S_f[x_1, x_2, \ldots, x_m]$ in m indeterminates $x_1, x_2, \ldots, x_m$ over S_f. (These indeterminates are supposed to commute with everything, even though S_f is not commutative.) Then, by construction, in $S_f[x_1, x_2, \ldots, x_m]$ we have[3]

$$f = \prod_{k=1}^{n} \left(\sum_{i=1}^{m} x_i a_i^{(k)} \right). \tag{2}$$

Indeed, the right hand side of this equality rewrites as follows:

$$\begin{aligned} \prod_{k=1}^{n} \left(\sum_{i=1}^{m} x_i a_i^{(k)} \right) &= \sum_{\mathbf{i}=(i_1,i_2,\ldots,i_n) \in \{1,2,\ldots,m\}^n} \underbrace{x_{i_1} x_{i_2} \cdots x_{i_n}}_{=x^{\mathrm{cont}(\mathbf{i})}} \underbrace{a_{i_1}^{(1)} a_{i_2}^{(2)} \cdots a_{i_n}^{(n)}}_{=w(\mathbf{i})} \\ &= \sum_{\mathbf{i} \in \{1,2,\ldots,m\}^n} x^{\mathrm{cont}(\mathbf{i})} w\left(\mathbf{i}\right) = \sum_{\substack{\alpha \in \mathbb{N}^m; \\ |\alpha| = n}} x^\alpha \underbrace{\sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \mathrm{cont}(\mathbf{i}) = \alpha}} w(\mathbf{i})}_{\substack{=r_\alpha + c_\alpha \\ \text{(by (1))}}} \\ &= \sum_{\substack{\alpha \in \mathbb{N}^m; \\ |\alpha| = n}} x^\alpha \underbrace{\left(r_\alpha + c_\alpha\right)}_{\substack{=c_\alpha \text{ in } S_f \\ \text{(since we factored out } r_\alpha \text{ to get } S_f\text{)}}} = \sum_{\substack{\alpha \in \mathbb{N}^m; \\ |\alpha| = n}} x^\alpha c_\alpha = \sum_{\substack{\alpha \in \mathbb{N}^m; \\ |\alpha| = n}} c_\alpha x^\alpha = f. \end{aligned}$$

The construction of S_f is universal in the evident sense:

Proposition 1 (Universal property of S_f)**.** *Let T be any associative unital R-algebra with elements $b_i^{(k)} \in T$ satisfying*

$$f = \prod_{k=1}^{n} \left(\sum_{i=1}^{m} x_i b_i^{(k)} \right) \quad \text{in } T[x_1, x_2, \ldots, x_m]. \tag{3}$$

Then there is a unique R-algebra homomorphism $S_f \to T$ sending $a_i^{(k)}$ to $b_i^{(k)}$.

[3]Noncommutative products of the form $\prod_{k=1}^{n} u_k$ are always understood to mean $u_1 u_2 \cdots u_n$.

Proof. By running the above proof of (2) in reverse, we can see that the equality (3) is equivalent to having all the coefficientwise equalities

$$\sum_{\substack{\mathbf{i}\in\{1,2,\ldots,m\}^n;\\ \operatorname{cont}(\mathbf{i})=\alpha}} w_T(\mathbf{i}) = c_\alpha \qquad \text{for all } \alpha \in \mathbb{N}^m \text{ satisfying } |\alpha| = n$$

hold in T, where $w_T(\mathbf{i}) = b_{i_1}^{(1)} b_{i_2}^{(2)} \cdots b_{i_n}^{(n)}$ for any n-tuple $\mathbf{i} = (i_1, i_2, \ldots, i_n) \in \{1, 2, \ldots, m\}^n$. But the latter coefficientwise equalities are simply saying that the R-algebra morphism $F \to T$ that sends each $a_i^{(k)}$ to $b_i^{(k)}$ annihilates all the $r_\alpha \in F$. And this, in turn, means that the morphism $F \to T$ factors through the quotient algebra $F/\left(r_\alpha \mid \alpha \in \mathbb{N}^m,\ |\alpha| = n\right) = S_f$. □

3 The reduction system

Our goal in this little note is to prove that the structure map of the R-algebra S_f (that is, the R-algebra morphism $R \to S_f,\ r \mapsto r \cdot 1$) is injective. This will allow us to view S_f as a ring extension of R (that is, as a ring that contains R as a subring).

We shall use Bergman's terminology for reduction systems in free associative algebras [1, Section 1]. Thus a *reduction system* is a set of pairs (W, g), where W is a word and g is a linear combination of smaller words (with respect to some order that we shall specify below). Each of these pairs (W, g) is called a *reduction rule*[4], and is written as $W \longrightarrow g$; we refer to W as its *leading word* and to g as its *tail*. The possible conflicts between two such rules are the *overlap ambiguities* and *inclusion ambiguities* defined in [1, Section 1]; they happen when the leading words W and W' of two distinct reduction rules (W, g) and (W', g') have a prefix-suffix collision (i.e., a nonempty proper suffix of W equals a nonempty proper prefix of W') or when one of them is a contiguous subword of the other. Given a reduction system in a free algebra, the *difference ideal* of this system means the ideal generated by the $W - g$ for all reduction rules (W, g), and the *difference quotient* of this system means the quotient of the free algebra by this ideal. A word w is said to be *irreducible* with respect to the reduction system if none of the leading words of the system appears as a contiguous subword of w. The crux of [1, §1] is a sufficient criterion ([1, Theorem 1.2 (a) $\Longrightarrow$ (c)]) for when the irreducible words (or, more precisely, their canonical projections) form a basis of the difference quotient. Namely, this happens whenever

1. there is a *semigroup partial ordering* consistent with the reduction system and satisfying the descending chain condition, and

2. all ambiguities of the reduction system are *resolvable*.

[4]Bergman does not use this terminology; instead he writes S for the set of all these pairs (W, g). (Of course, this is not our S.)

We refer to [1, §1] for the meanings of these concepts. Note that if no ambiguities exist, then all ambiguities are resolvable (for vacuous reasons); such situations are particularly simple (and we are lucky enough that we will end up in precisely such a situation).

Let us apply this in our free algebra F. Our alphabet $\mathfrak{A}$ consists of all the mn symbols $a_i^{(k)}$ with $1 \leq i \leq m$ and $1 \leq k \leq n$. We order words over this alphabet by degree-lexicographic order (i.e., shorter words are always smaller than longer ones, but words of equal length are compared lexicographically), where the lexicographic order is such that

$$\begin{aligned} & a_1^{(1)} < a_1^{(2)} < \cdots < a_1^{(n)} \\ < & \, a_2^{(1)} < a_2^{(2)} < \cdots < a_2^{(n)} \\ < & \, \cdots \\ < & \, a_m^{(1)} < a_m^{(2)} < \cdots < a_m^{(n)}. \end{aligned}$$

[5] This total order on words is a semigroup partial ordering (i.e., if $w \leq w'$, then $uwv \leq uwv'$ for any words w, w', u, v), and satisfies the descending chain condition. Thus, Bergman's [1, Theorem 1.2 (a) $\Longrightarrow$ (c)] applies to any reduction system that is consistent with it and has only resolvable ambiguities.

For each m-tuple $\alpha \in \mathbb{N}^m$ with $|\alpha| = n$, let

$$\mathbf{i}^\alpha = (i_1^\alpha, i_2^\alpha, \ldots, i_n^\alpha)$$

be the lexicographically largest of all n-tuples $\mathbf{i} \in \{1, 2, \ldots, m\}^n$ satisfying $\operatorname{cont}(\mathbf{i}) = \alpha$. Equivalently, the sequence $i_1^\alpha, i_2^\alpha, \ldots, i_n^\alpha$ is weakly decreasing with respect to our chosen order and satisfies $\operatorname{cont}(\mathbf{i}^\alpha) = \alpha$. (This is equivalent because the n-tuples $\mathbf{i} \in \{1, 2, \ldots, m\}^n$ satisfying $\operatorname{cont}(\mathbf{i}) = \alpha$ form an orbit under the permutation action of the symmetric group S_n, and the lexicographically largest among them is the one whose entries weakly decrease.) Define the word

$$W_\alpha = w(\mathbf{i}^\alpha) = a_{i_1^\alpha}^{(1)} a_{i_2^\alpha}^{(2)} \cdots a_{i_n^\alpha}^{(n)}.$$

Then,

$$r_\alpha = \sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \operatorname{cont}(\mathbf{i}) = \alpha}} w(\mathbf{i}) - c_\alpha = W_\alpha + \sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \operatorname{cont}(\mathbf{i}) = \alpha; \\ \mathbf{i} \neq \mathbf{i}^\alpha}} w(\mathbf{i}) - c_\alpha$$

(here, we have split off the addend $w(\mathbf{i}^\alpha) = W_\alpha$ from the sum). Thus, the relation $r_\alpha = 0$ gives the reduction rule

$$W_\alpha \longrightarrow c_\alpha - \sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \operatorname{cont}(\mathbf{i}) = \alpha; \\ \mathbf{i} \neq \mathbf{i}^\alpha}} w(\mathbf{i}).$$

[5] Actually, many other choices of order on the indeterminates would work equally well; all we need is that the order relation between two indeterminates $a_i^{(k)}$ and $a_j^{(\ell)}$ with $i \neq j$ depends only on i and j and not on k and ℓ. We chose the above ordering merely for its familiarity.

This is a reduction rule over R. Its leading word is W_α, whereas its tail is an R-linear combination of words that are strictly smaller than W_α in the chosen order (indeed, each $w(\mathbf{i})$ is lexicographically smaller than W_α while having the same length as W_α, whereas the constant term c_α is smaller by degree[6]). Thus, if we consider the reduction system that consists of all these reduction rules (for all $\alpha \in \mathbb{N}^m$ satisfying $|\alpha| = n$), then our chosen order on words is consistent with this reduction system.

The difference ideal of this reduction system is the ideal generated by all the differences

$$W_\alpha - \left(c_\alpha - \sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \operatorname{cont}(\mathbf{i}) = \alpha; \\ \mathbf{i} \neq \mathbf{i}^\alpha}} w(\mathbf{i}) \right) = W_\alpha + \sum_{\substack{\mathbf{i} \in \{1,2,\ldots,m\}^n; \\ \operatorname{cont}(\mathbf{i}) = \alpha; \\ \mathbf{i} \neq \mathbf{i}^\alpha}} w(\mathbf{i}) - c_\alpha = r_\alpha.$$

Hence, the difference quotient is precisely $F/\left(r_\alpha \mid \alpha \in \mathbb{N}^m,\ |\alpha| = n\right) = S_f$. Crucially, our reduction system has the following nice property, which will allow us to obtain an R-module basis for S_f from it using [1, Theorem 1.2 (a) $\Longrightarrow$ (c)]:

Lemma 2. *Our reduction system has no ambiguities.*

Proof. Each leading word W_α has superscript pattern $1, 2, \ldots, n$ (meaning that it has the form $a_{i_1}^{(1)} a_{i_2}^{(2)} \cdots a_{i_n}^{(n)}$ for some $i_1, i_2, \ldots, i_n$).

An overlap ambiguity would require a nonempty proper suffix of a leading word W_α to equal a nonempty proper prefix of a leading word W_β. But such an equality is impossible, since the former suffix would begin with a letter with superscript $r \geq 2$ (where r is the position of W_α at which it starts), while the latter prefix would begin with a letter with superscript 1 (the first letter of W_β). Thus, there are no overlap ambiguities.

Inclusion ambiguities don't exist either. Indeed, an inclusion ambiguity would require one of our leading words W_α to be a contiguous subword of another. Since all our leading words have the same length, this could only happen if the leading words were equal; but this cannot happen (because $W_\alpha = W_\beta$ is easily seen to imply $\alpha = \beta$).

Thus, our reduction system has no ambiguities. □

Lemma 2 shows that all ambiguities of our reduction system are resolvable (since there are none). Hence, Bergman's Diamond Lemma [1, Theorem 1.2 (c)] applies to it, and shows that the irreducible words (i.e. the words containing no W_α as a contiguous subword) form an R-basis of the quotient R-module S_f. We summarize:

Theorem 3. *The algebra S_f is a free R-module. More precisely, an R-basis of S_f is given by the images of all words in the alphabet $a_i^{(k)}$ which do not contain any of the leading words W_α as a (contiguous) subword.*

[6] NB: Here we are using $n > 0$.

As a consequence:

Theorem 4. *The natural map $R \to S_f$ is injective. Consequently, the natural map*

$$R[x_1, x_2, \ldots, x_m] \longrightarrow S_f[x_1, x_2, \ldots, x_m] \tag{4}$$

is injective, where the variables x_i are central over S_f.

Proof. The empty word is irreducible, and hence its image is one of the basis vectors of the R-module basis of S_f found in Theorem 3. Thus no nonzero element of R can vanish in S_f. Moreover, the basis of S_f found in Theorem 3 gives an R-linear projection $S_f \to R$ sending the empty word to 1 and all other irreducible words to 0. Extending this projection coefficientwise to polynomials gives an $R[x_1, x_2, \ldots, x_m]$-linear projection $S_f[x_1, x_2, \ldots, x_m] \to R[x_1, x_2, \ldots, x_m]$ that splits the map (4). Hence the latter map is injective. □

Thus every homogeneous degree-n polynomial over R splits into n homogeneous linear factors after an injective extension of the coefficient ring to a noncommutative R-algebra.

4 The inhomogeneous case

Now we turn to a slightly more general situation. Let

$$f \in R[x_1, x_2, \ldots, x_m]$$

be any polynomial of degree at most n (not necessarily homogeneous). Write it in the form

$$f = \sum_{\substack{\beta \in \mathbb{N}^m; \\ |\beta| \leq n}} c_\beta x^\beta.$$

Define the degree-n homogenization of f to be the polynomial

$$F(x_0, x_1, \ldots, x_m) := \sum_{\substack{\beta \in \mathbb{N}^m; \\ |\beta| \leq n}} c_\beta x_0^{n-|\beta|} x^\beta \in R[x_0, x_1, \ldots, x_m].$$

This is homogeneous of degree n. Applying the homogeneous construction to F, we obtain a noncommutative R-algebra S_F, free as an R-module, and a factorization

$$F(x_0, x_1, \ldots, x_m) = \prod_{k=1}^{n} \left(\sum_{i=0}^{m} x_i a_i^{(k)} \right) \tag{5}$$

in $S_F[x_0, x_1, \ldots, x_m]$, where the variables $x_0, x_1, \ldots, x_m$ are central.

Now set $x_0 = 1$ (that is, apply the canonical left-S_F-linear R-algebra morphism $S_F[x_0, x_1, \ldots, x_m] \to S_F[x_1, x_2, \ldots, x_m]$ that sends each monomial $x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m}$ to $x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$) to (5). Thus, (5) transforms into

$$f(x_1, x_2, \ldots, x_m) = \prod_{k=1}^{n} \left(a_0^{(k)} + \sum_{i=1}^{m} x_i a_i^{(k)} \right) \tag{6}$$

in $S_F[x_1, x_2, \ldots, x_m]$. This shows that the polynomial f splits into n affine-linear factors over the ring S_F, which is an injective noncommutative ring extension of R. So we have shown the following:

Theorem 5. *Let R be a commutative ring and let $f \in R[x_1, x_2, \ldots, x_m]$ be a polynomial of degree at most n, where n is a positive integer. Then there exists an associative unital R-algebra S, free as an R-module, such that*

$$R[x_1, x_2, \ldots, x_m] \hookrightarrow S[x_1, x_2, \ldots, x_m]$$

injectively and such that f splits in $S[x_1, x_2, \ldots, x_m]$ as a product of n affine-linear factors.

Proof. Take $S = S_F$, where F is the degree-n homogenization of f. Then, (6) gives the factorization. Since S_F is free as an R-module (by Theorem 3), the same irreducible-word projection used in Theorem 4 shows that $R[x_1, x_2, \ldots, x_m] \to S_F[x_1, x_2, \ldots, x_m]$ is injective. □

Remark 6. *If $f \neq 0$, one may take $n = \deg f$ in Theorem 5. If $f = 0$, then any positive n may be chosen.*

Theorem 4 can be recovered from Theorem 5 by comparing the degree-n components of both sides. (Per se, Theorem 5 only gives a factorization into affine-linear factors; but projecting down to the n-th degree component will make all the constant terms go away.)

5 The determinant as a special case

Applying Theorem 4 to $R = \mathbb{Z}$, $m = n^2$, and $f = \det((x_{ij})_{1 \leq i,j \leq n})$, we obtain a universal splitting algebra for the generic determinant polynomial $\det((x_{ij})_{1 \leq i,j \leq n})$. The variables are indexed by the matrix positions (i, j), and the coefficients c_α are $0, 1, -1$: they are nonzero precisely when α is the characteristic function of the graph of a permutation $\sigma \in S_n$, in which case $c_\alpha = \operatorname{sgn}(\sigma)$.

The proof above shows that the corresponding algebra $S_f = S_{\det}$ is a free $\mathbb{Z}$-module, and hence that

$$\mathbb{Z}[x_{ij} \mid 1 \leq i, j \leq n] \hookrightarrow S_{\det}[x_{ij} \mid 1 \leq i, j \leq n]$$

is injective. This answers MathOverflow question #27675 in the positive.

References

[1] George M. Bergman, *The Diamond Lemma for Ring Theory*, Advances in Mathematics **29** (1978), 178–218.
See `https://math.berkeley.edu/~gbergman/papers/updates/diamond.html` for errata.

[2] GPT-5.5 with prompting by Darij Grinberg, *Splitting a univariate polynomial over a commutative extension of the coefficient ring*, 4 July 2026, `https://www.cip.ifi.lmu.de/~grinberg/algebra/factorpoly-gpt.pdf`.