




Advances in Arithmetic and Geometry over Division rings

Elad Paran*, , ¹

ABSTRACT

In recent years, there has been a flurry of activity surrounding non-commutative Nullstellensätze over the real quaternion algebra and over general division rings. From these results emerge rich arithmetic and geometry, which in many ways follow the classical themes and ideas of complex algebraic geometry, yet also exhibit new and interesting phenomena. In this survey, we review developments in this active research area and discuss emerging open questions.

ARTICLE HISTORY

Received: 2 October 2025

Revised: 5 November 2025

Accepted: 6 November 2025

Published: 10 December 2025

Communicated by

André Leroy

<https://doi.org/10.65908/gja.2025.24975>

KEYWORDS

Division rings;
noncommutative ring theory;
Nullstellensatz;
quaternions.

MSC

12E15;
16K20;
16K40;
16R20.

1 Introduction

Let K be a field and let $R = K[x_1, \dots, x_n]$ be the ring of polynomials in n variables over K . Given a set of points Z in the affine space K^n , let $\mathcal{I}(Z) \subseteq R$ be the ideal of polynomials vanishing at Z . Conversely, given an ideal J in R , we denote by $\mathcal{Z}(J)$ the set of common zeros of its polynomials. One then asks what happens when going back and forth between algebra and geometry. That is, what is $\mathcal{I}(\mathcal{Z}(J))$?

In the case where $K = \mathbb{C}$ is the field of complex numbers, the answer is given by Hilbert's Nullstellensatz: The ideal $\mathcal{I}(\mathcal{Z}(J))$ is the radical \sqrt{J} of J in R . This is a foundational result

*Corresponding author

1. Department of Mathematics and Computer Science, The Open University of Israel.

of classical algebraic geometry. An immediate consequence is the existence of a common zero for the elements of every proper ideal in $\mathbb{C}[x_1, \dots, x_n]$. This result is sometimes known as the “weak” Nullstellensatz, though it is in fact equivalent to the “strong” version via the famous Rabinowitsch trick. In the one variable case $n = 1$, a proper ideal in $\mathbb{C}[x]$ is generated by a single non-constant polynomial, and so in this case the statement of the Nullstellensatz is that every non-constant polynomial in $\mathbb{C}[x]$ has a zero – the Fundamental Theorem of Algebra. Thus one could think of the Nullstellensatz as a higher-dimensional generalization of Gauss’s celebrated theorem.

Suppose now that instead of a field, one considers a division ring, and let us first consider Hamilton’s ring of real quaternions \mathbb{H} . In 1941 Niven and Jacobson [49] proved a fundamental theorem of algebra for \mathbb{H} : Letting $\mathbb{H}[x]$ denote the ring of polynomials in a **central** variable x over \mathbb{H} , they showed that every non-constant polynomial $a_0 + a_1x + \dots + a_nx^n \in \mathbb{H}[x]$ admits a quaternionic zero.

The above discussion raises a question: If Hilbert’s Nullstellensatz is a higher-dimensional form of the fundamental theorem of algebra, and since the fundamental theorem holds over \mathbb{H} , do we also have a higher dimensional version of the latter? That is, is there a *quaternionic Nullstellensatz*?

While this question could have been asked in 1941, and while some related results have been published over the years (some of which will be discussed in this survey), the question itself was only recently fully addressed, in the 2020 paper [8] of Alon and the author.

Before stating the main results of [8], let us properly formulate the question in the non-commutative setting: Let D be a division ring, and let $D[x_1, \dots, x_n]$ be the ring of polynomials in n **central** variables over D . Substitution in such polynomials is generally well-defined only at points of D^n whose coordinates commute pairwise (see the discussion in §2 below). We denote the space of all such points by D_c^n and call it the **central affine space** over D . Given a set of points $Z \subseteq D_c^n$, let $\mathcal{I}(Z) \subseteq R$ be the set of polynomials vanishing at Z , which is generally only a **left** ideal in R . For this reason, in our non-commutative case, we must deal with one-sided ideals: Limiting ourselves to two-sided ideals would miss out on much of the geometry.

Conversely, given a left ideal J in $D[x_1, \dots, x_n]$, we associate to it the common set of zeros (in D_c^n) of its polynomials, and denote it by $\mathcal{Z}(J)$. As in the field case, we would like to know what happens when going back and forth between algebra and geometry – what is $\mathcal{I}(\mathcal{Z}(J))$?

One’s first guess might be that $\mathcal{I}(\mathcal{Z}(J))$ is the ideal of polynomials that admit a power in J , as in the commutative case. However, this turns out to be false, as is demonstrated in §3 below. The main result of [8] gives an **implicit** description of $\mathcal{I}(\mathcal{Z}(J))$ as the *radical* of J , defined as the intersection of all *completely prime* left ideals in R (see Definition 3.4). In the commutative case, the notion of a completely prime left ideal coincides with the usual notion of a prime ideal. Thus [8] yields a natural analogue of Hilbert “strong” Nullstellensatz, in its implicit form. We shall refer to this result as the *central quaternionic Nullstellensatz*. The second result of [8] is a “weak” quaternionic Nullstellensatz, describing the maximal left ideals in R : These are precisely those of the form $(x_1 - a_1, \dots, x_n - a_n)$, where (a_1, \dots, a_n) is a point in the central affine space \mathbb{H}_c^n . Thus here, as in the complex

case, we have a natural geometric correspondence between maximal (left) ideals and points in the relevant space. We note that unlike the commutative case, here there does not appear to be an immediate way to deduce the “strong” version from the “weak” one.

These initial results led to a flurry of activity and papers surrounding foundational questions of geometry and arithmetic over the quaternions and over general division rings: A Nullstellensatz for general quaternionic polynomial functions by Alon and the author in [7], and more generally for polynomial functions over division rings by Bao and Reichstein in [16]; Extension to rings of matrices by Cimprič in [18], [19] and [20]; A “Combinatorial” Nullstellensatz over division rings by the author in [51]; An explicit version of the central quaternionic Nullstellensatz by Aryapoor in [11]; A study of the geometry of the zero sets of quaternionic polynomials in two variables by Gori, Sarfatti and Vlacci in [29], extended to higher dimensions by Alon and the author in [10], by Alon, Chapman and the author in [2] and by Gori, Sarfatti and Vlacci in [30]; A generalization of the Ax-Grothendieck theorem to polynomials functions over centrally finite algebraically closed division rings by the author and Son in [54]; A study of contraction properties of maximal left ideals in polynomial rings over division rings by Chapman and the author in [22] which answered a question of Amitsur and Small from 1978, and additional extensions of these results by Chapman, Levin and Zaninelli in [21] and by Aryapoor in [12].

In this survey we shall review these works and discuss open questions and new research directions that arise from them.

2 Preliminaries

In this section we present basic material concerning polynomials in (one or several) central variables over non-commutative rings, that will be used throughout this survey. The familiar reader may wish to skip this section and refer to it as needed.

2.1 Polynomials over division rings in one central variable

Let R be any (associative, unital) ring, let $R[x]$ be the ring of polynomials over R , where the coefficients are written to the left of the monomials, and with the usual multiplication $(\sum a_i x^i) \cdot (\sum a_j x^j) = \sum_k (\sum_{i+j=k} a_i b_j) x^k$. Note that with this rule, we have $x \cdot a = ax$ for any $a \in R$, hence the variable x indeed belongs to the center of $R[x]$. If $f, g \in R[x]$ and g is monic, then we can follow Euclid’s algorithm to perform “right-hand division with remainder” and write $f = pg + r$ for some $p, r \in R[x]$ with $\deg(r) < \deg(g)$ (see [50, p. 483]). Similarly for “left-hand division with remainder”.

Let D be a division ring. The ring $D[x]$ was first systematically studied by Ore in his classical paper [50] (Ore studies, more generally, skew polynomials rings over division rings equipped with an endomorphism and a derivation, but in our context it suffices to consider the usual ring of polynomials $D[x]$). Ore showed that $D[x]$ is a left and right Euclidean domain; It is a left and right principal ideal domain, and satisfies a unique factorization theorem.

Given an element $c \in R$, we naturally have a substitution map $R[x] \rightarrow R$, mapping a polynomial $f(x) = a_0 + a_1x + \dots + a_nx^n$ to $f(c) = a_0 + a_1c + \dots + a_nc^n$. We say that c is a right zero of $f(x)$, if $f(c) = 0$. From now on we shall simply write “zero of a polynomial” instead of “right zero...”. Here one must note that substitution is generally not a homomorphism: If $f(c) = 0$ then $(gf)(c) = 0$ for all $g \in R[x]$, but $(fg)(c) = 0$ does not necessarily hold. Thus the kernel of such substitution maps is merely a left ideal. Nevertheless, we have the following product formula:

Lemma 2.1. *Let R be a ring. If $g(a)$ is invertible in R , then $(fg)(a) = f(a^{g(a)}) \cdot g(a)$, for any $f, g \in R[x]$, where $a^{g(a)}$ is the conjugation $g(a)ag(a)^{-1}$ of a by $g(a)$.*

Proof. See the proof of [37, Proposition 16.3, p. 263] (where R is assumed to be a division ring, but the proof holds for any ring provided that $g(a)$ is invertible). \square

Let D be a division ring. For two non-zero polynomials $f, g \in D[x]$ we will denote by $\text{lcm}(f, g)$ the monic **left-hand** common multiple of f and g of least degree. That is, $\text{lcm}(f, g)$ is the monic polynomial of minimal degree that is divisible from the **right** by both f and g . Such a polynomial always exists and is uniquely defined [50, p. 485]. If $f = x - a, g = x - b$ are monic linear polynomials, then $\text{lcm}(f, g)$ is the monic polynomial of smallest degree that vanishes at both a and b (since $p \in D[x]$ is divisible by $x - a$ from the right if and only if $p(a) = 0$). Note that in the commutative case, if $a \neq b$ then $\text{lcm}(x - a, x - b) = (x - a)(x - b)$, but for general division rings this is not always the case. For example, in $\mathbb{H}[x]$, one checks that $(x - i)(x - j)$ vanishes only at j , and $\text{lcm}(x - i, x - j) = x^2 + 1^*$.

More generally, for a set of polynomials $S \subseteq D[x]$, if there exists a non-zero polynomial that is right-hand divisible by all polynomials in S , then we will denote a monic such polynomial of minimal degree (which is always uniquely determined by S) by $\text{lcm}(p|p \in S)$.

Lemma 2.2. *Let $S \subseteq D[x]$, and suppose that $g = \text{lcm}(p|p \in S)$ exists. A polynomial $f \in D[x]$ is right-hand divisible by all polynomials in S if and only if f is right-hand divisible by g .*

Proof. By right-hand division with remainder we may write $f = qg + r$ with $\deg(r) < \deg(g)$. Then $r = f - qg$ is right-hand divisible by all polynomials in S , and by the minimality of the degree of g we must have $r = 0$. \square

A stark difference between the commutative and non-commutative case is that over division rings, polynomials may have more zeros than their degree. For example, the quadratic polynomial $x^2 + 1 \in \mathbb{H}[x]$ admits infinitely many zeros: It vanishes at every point of the form $ai + bj + ck$ with $a, b, c \in \mathbb{R}$ satisfying $a^2 + b^2 + c^2 = 1$. However, a remedy is given by a theorem of Gordon and Motzkin [26]: The zeros of a polynomial $f(x) \in D[x]$ of degree n represent at most n conjugacy classes of D . The algebraic theory of zeros of one variable

*

Throughout this survey, we shall denote the standard quaternionic generators by i, j, k , as opposed to the letters i, j, k which we reserve for indices.

polynomials over division rings was developed in a series of papers by Lam and Leroy [36], [42], [41], [40]. Following their work, we shall say that a set $A \subseteq D$ is *algebraic*, if there exists a monic polynomial $f \in D[x]$ which vanishes at every point in A . If A is algebraic, we denote by f_A the monic polynomial of minimal degree which vanishes at A (clearly, f_A is uniquely defined). The degree of f_A is called the (*algebraic*) *rank* of A , which we denote by $\text{rk}(A)$. The polynomial f_A is the least common left-hand multiple $\text{lcm}(x - a | a \in A)$ of the polynomials $x - a$, for $a \in A$. For example, if $D = \mathbb{H}$ is the real quaternion algebra, then the set

$$A = \{ai + bj + ck | a, b, c \in \mathbb{R}, a^2 + b^2 + c^2 = 1\}$$

is algebraic, with minimal polynomial $x^2 + 1$. Thus A is an algebraic set of rank 2. Clearly, if D is a field then a set A in D is algebraic if and only if it is finite, in which case $f_A = \prod_{a \in A} (x - a)$.

These notions lead to a non-trivial “one-dimensional” algebraic geometry over division rings, developed in the mentioned works of Lam and Leroy.

The following lemma will be useful for the proof of the Combinatorial Nullstellensatz in §5.

Lemma 2.3. *Let D be a division ring and let A be a non-empty algebraic subset of D . Let $a \in A$. The polynomial $(\text{lcm}(x - b^{b-a} | b \in A \setminus \{a\})) \cdot (x - a)$ is right-hand divisible in $D[x]$ by $\text{lcm}(x - b | b \in A)$.[†]*

Proof. Let

$$h = \text{lcm}(x - b^{b-a} | b \in A \setminus \{a\}).$$

By Lemma 2.2, we must show that $g = h \cdot (x - a)$ is right-hand divisible by $x - b$ for all $b \in A$. For $b = a$ this is clear. For any given $b \in A \setminus \{a\}$, since h is right-hand divisible by $x - b^{b-a}$, it follows that g is right-hand divisible by $p = (x - b^{b-a})(x - a)$. By Lemma 2.1 we have $p(b) = (b^{b-a} - b^{b-a})(b - a) = 0$, hence p is divisible by $x - b$, hence so is g . \square

Remark 2.4. *The ring $D[x]$ is a non-commutative polynomial ring; It is a special case of the more general skew polynomial ring $D[x, \sigma, \delta]$, where σ is an automorphism of D and δ is a σ -derivation of D . That is, a δ is an additive map on D satisfying the Leibnitz rule $\delta(ab) = a^\sigma \delta(b) + \delta(a)b$. These rings were introduced by Ore in his classical paper [50], and satisfy many elegant properties – for example they are left and right principal ideal and Euclidean domains. The evaluation of a skew polynomial in $p \in D[x, \sigma, \delta]$ at an element $a \in D$ is defined to be the unique element $p(a) \in D$ satisfying $p - p(a) \in D[x, \sigma, \delta]p$. The explicit calculation of $p(a)$ is technically a bit more complicated than for the usual ring $D[x]$, and the interested reader could find an detailed discussion of evaluation of one variable skew polynomials in the work [42, §2].*

†

Recall that b^{b-a} denotes the conjugation $(b - a)b(b - a)^{-1}$ of b by $b - a$.

2.2 Polynomials in several central variables

Again let R be any ring. In a similar fashion to the one variable case, we can define the ring $R[x_1, \dots, x_n]$ of polynomials in n central variables over R , where the coefficients are written to the left of the monomials. As in the commutative case, we may also view this ring as an iterated polynomial ring $R[x_1, \dots, x_{n-1}][x_n] = \dots = R[x_1][x_2] \dots [x_n]$. For any polynomial $p \in R[x_1, \dots, x_n]$, we denote by $\deg(p)$ the total degree of p – the maximum sum $k_1 + \dots + k_n$ for which there appears in p a monomial $\lambda x_1^{k_1} \dots x_n^{k_n}$ with $\lambda \neq 0$.

When considering zeros of polynomials in n central variables, an additional difficulty arises: Substitution is not generally well-defined at all points of R^n . Consider for example the quaternionic polynomial $p = xy \in \mathbb{H}[x, y]$. Since the variables are central, we have $xy = yx$. Substituting the point $(i, j) \in \mathbb{H}^2$ in p is not well-defined, since the order of substitution matters: We have $ij = k$ while $ji = -k$. If $a = (a_1, \dots, a_n) \in R^n$ is a point whose coordinates commute pairwise, then the order of substitution in monomials does not matter, and so we may evaluate any polynomial $f(x) \in R[x_1, \dots, x_n]$ at a and obtain a well-defined value $f(a)$. We say that a is a zero of $f(x)$, or that $f(x)$ vanishes at a , if $f(a) = 0$.

The above issue is formalized by the following lemma:

Lemma 2.5. *Let D be a division ring and let $a = (a_1, \dots, a_n) \in D^n$. Then the left ideal I_a in $D[x_1, \dots, x_n]$ generated by $x_1 - a_1, \dots, x_n - a_n$ is a proper left ideal if and only if $a_i a_j = a_j a_i$ for all i, j . If this condition holds, then I_a is a maximal left ideal. Moreover, a polynomial $f(x) \in D[x_1, \dots, x_n]$ vanishes at a if and only if $f(x) \in I_a$.*

Proof. See [8, §2] (where the claim is proven for $D = \mathbb{H}$, but the proof applies to a general division ring). \square

Let D be a division ring. In light of the above lemma, in our context the relevant space where substitution is well defined is the space D_c^n of all points whose coordinates commute pairwise. We shall call this space the *n -dimensional central affine space over D* , or simply the *central affine space* whenever D and n are fixed. In the case where $D = \mathbb{H}$, for example, every point $(a_1, \dots, a_n) \in \mathbb{H}_c^n$ which does not lie in \mathbb{R}^n induces an isomorphic copy $\mathbb{R}(a_1, \dots, a_n)$ of \mathbb{C} inside \mathbb{H} . Thus, intuitively, \mathbb{H}_c^n consists of $|\mathbb{C}|$ copies of \mathbb{C}^n , glued along the intersection \mathbb{R}^n .

Since we may view $D[x_1, \dots, x_n]$ as an iterated polynomial ring, for any point $a = (a_1, \dots, a_n) \in D_c^n$ the substitution $f \mapsto f(a)$ from $D[x_1, \dots, x_n] \rightarrow D$ is clearly the composition of the map $x_n \mapsto a_n$ from $D[x_1, \dots, x_n]$ to $D[x_1, \dots, x_{n-1}]$ and of the map $(x_1, \dots, x_{n-1}) \mapsto (a_1, \dots, a_{n-1})$ from $D[x_1, \dots, x_{n-1}]$ to D , just as in the commutative case.

Remark 2.6. *As noted in the concluding remark of the preceding section, the ring $D[x]$ is a special case of the skew polynomial ring $D[x, \sigma, \delta]$. Similarly, one can generalize the ring $D[x_1, \dots, x_n]$ and consider skew polynomial rings in several variables over D , where multiple derivations and automorphisms are involved. In this survey we shall limit our scope of discussion to the usual polynomial ring $D[x_1, \dots, x_n]$. For more information on*

multivariate skew polynomial rings and evaluation in these rings, we refer the reader to reader to the recent papers [44],[43].

3 The central quaternionic Nullstellensatz

The first result of [8] is the following:

Theorem 3.1 (Weak Central Quaternionic Nullstellensatz). *For every point $(a_1, \dots, a_n) \in \mathbb{H}_c^n$, the left ideal generated by $x_1 - a_1, \dots, x_n - a_n$ is a proper maximal left ideal in $\mathbb{H}[x_1, \dots, x_n]$. Moreover, every maximal left ideal in $\mathbb{H}[x_1, \dots, x_n]$ is of this form.*

To prove Theorem 3.1 we shall need a couple of lemmas. First, note that the real polynomial ring $R' = \mathbb{R}[x_1, \dots, x_n]$ is the center of $R = \mathbb{H}[x_1, \dots, x_n]$, by direct verification. We then have:

Lemma 3.2. *The extension R/R' is integral. That is, every element $f \in R$ satisfies an equality of the form $f^n + g_{n-1}f^{n-1} + \dots + g_1f + g_0 = 0$ with $g_0, \dots, g_{n-1} \in R'$.*

Proof. Since R' is commutative, R' is a finitely-accessible ring in the sense of [61, Definition 1.4], hence by a result of Sontag [61, Theorem 1.3], the extension R/R' is integral. \square

Using Lemma 3.2, the proof of the following “going-down” lemma is essentially the same as its commutative counterpart, which is well-known.

Lemma 3.3. *Let M be a maximal left ideal in R , and let $P = M \cap R'$. Then P is a maximal ideal in R' .*

Proof. Let $f \in R'$, $f \notin P$. Then $M + Rf = R$, hence there exist $m \in M, g \in R$ such that $gf + m = 1$. Since R/R' is integral, there exist polynomials $h_0, \dots, h_{n-1} \in R'$ such that $g^n + \sum_{i=0}^{n-1} h_i g^i = 0$. Since $f \in R'$ and R' is the center of R , we have $f^n g^n + \sum_{i=0}^{n-1} f^{n-i} h_i (fg)^i = 0$. That is, $(1 - m)^n + \sum_{i=0}^{n-1} f^{n-i} h_i (1 - m)^i = 0$, hence $1 + \sum_{i=0}^{n-1} f^{n-i} h_i \in M \cap R' = P$. But this implies that f is a unit modulo P . Thus R'/P is a field, hence P is maximal. \square

We can now prove Theorem 3.1:

Proof. Every ideal of the given form is maximal, by Lemma 2.5. For the converse, let M be a maximal left ideal in R and let $P = M \cap R'$. By the preceding lemma, P is a maximal ideal in R' , hence $F := R'/P$ is a finite field extension of \mathbb{R} , and P is the kernel of the projection $R' \rightarrow F$.

If $F \cong \mathbb{R}$, then P is generated by $x_1 - a_1, \dots, x_n - a_n$ for some $a_1, \dots, a_n \in \mathbb{R}$. In particular, $(a_1, \dots, a_n) \in \mathbb{H}_c^n$, hence by Lemma 2.5, the elements $x_1 - a_1, \dots, x_n - a_n \in P \subseteq M$ generate a maximal left ideal I in R , hence $M = I$.

Next, if $F \cong \mathbb{C}$, then P is the set of polynomials in R' which vanish at a complex point $(c_1 + d_1i, \dots, c_n + d_ni)$. By applying the real change[†] of variables $x_i \rightarrow x_i - c_i$ we may assume, without loss of generality, that $c_i = 0$ for all i . We may further replace x_i with $d_i^{-1}x_i$ whenever $d_i \neq 0$ to assume that $d_i = 1$ or $d_i = 0$ for all i . At least one of the d_i is 1, without loss of generality $d_1 = 1$. For any $i > 1$ with $d_i = 1$, we may replace x_i with $x_i - x_1$ to assume that $d_i = 0$.[§] Thus P is the set of polynomials vanishing at $(i, 0, \dots, 0)$, hence $P = \langle x_1^2 + 1, x_2, \dots, x_n \rangle$. Note that $x_1^2 + 1, x_2, \dots, x_n$ do not generate a maximal left ideal in R : Indeed, the left ideal generated by $x_1 + i, x_2, \dots, x_n$ is larger. Thus M must contain a non-zero element $h \in R$ which is not generated by $x_1^2 + 1, x_2, \dots, x_n$. By replacing in h every occurrence of x_2, \dots, x_n with 0 and every occurrence of x_1^2 with -1 , we may assume that $h = cx_1 - d$ for some $c, d \in \mathbb{H}$. Since M is a proper ideal we have $c \neq 0$. Multiplying h from the left by c^{-1} , we may assume that $c = 1$. Finally, by Lemma 2.5, the left ideal I generated by $x_1 - d, x_2, \dots, x_n$ is maximal in R , hence $M = I$. \square

Theorem 3.1 yields an algebro-geometric correspondence over the quaternion ring \mathbb{H} , similar to the one given by Hilbert's Nullstellensatz over \mathbb{C} .

Next, we turn to the Strong Central Nullstellensatz. To state it, we shall need the following definition:

Definition 3.4 (Reyes). *Let P be a left ideal in a ring R . We say that a P is a completely prime left ideal if whenever $a, b \in R$ satisfy $ab \in P$ and $Pb \subseteq P$ it follows that $a \in P$ or $b \in P$.*

The above definition was introduced by M. Reyes in [59], who showed that in certain non-commutative contexts, this notion serves as a “better” notion of a “one-sided prime ideal” than the more standard definition of a left prime ideal in non-commutative algebra: A left ideal P in a ring R is called *prime* if $RaRb \subseteq P$ implies $Ra \subseteq P$ or $Rb \subseteq P$, for all $a, b \in R$.

Using Definition 3.4, Reyes proves non-commutative analogues of theorems of Cohen and Kaplansky. Let us also note the following elegant fact: A non-zero ring is a division ring if and only if every proper left ideal in it is completely prime. For an additional application of this notion, see [9].

We shall now apply Reyes's notion to generalize the definition of the classical (commutative) notion of the radical of an ideal in a ring, as follows:

Definition 3.5. *Let J be a left ideal in a ring R . We define the radical \sqrt{J} of J as the intersection of all completely prime left ideals in R containing J .*

Using Definition 3.5, we can now state the main result of [8]:

†

That is, substituting $y_i = x_i - c_i$. Clearly, $\mathbb{H}_c[x_1, \dots, x_n] = \mathbb{H}_c[y_1, \dots, y_n]$.

§

Here we put $y_i = x_i - x_1$ or $y_i = x_i$ for each i , according to our construction. We have, as before, $\mathbb{H}_c[x_1, \dots, x_n] = \mathbb{H}_c[y_1, \dots, y_n]$, and any ideal of the form $\langle y_1 - b_1, \dots, y_n - b_n \rangle$ for some $(b_1, \dots, b_n) \in \mathbb{H}_c^n$ is also of the form $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ for some $(a_1, \dots, a_n) \in \mathbb{H}_c^n$.

Theorem 3.6 (Strong Central Quaternionic Nullstellensatz). *Let J be a left ideal in $\mathbb{H}[x_1, \dots, x_n]$. Then $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$.*

We note that in the commutative case, the radical as defined in Definition 3.5 coincides with the usual definition of the radical of an ideal in a commutative ring. However, in the non-commutative case, \sqrt{J} is not generally the same as $\{a \in R \mid a^k \in J \text{ for some } k \in \mathbb{N}\}$. Indeed, consider the single variable polynomial $f = (x - i)(x - j) \in \mathbb{H}[x]$. One checks that it admits a unique (!) zero j , thus $x - j \in \mathcal{I}(\mathcal{Z}(\mathbb{H}[x]f))$. However, no power of $x - j$ belongs to $\mathbb{H}[x]f$. Indeed, if $(x - j)^n \in \mathbb{H}[x]f$, then $(x - j)^{n-1} \in \mathbb{H}[x](x - i)$, hence $(x - j)^{n-1}(i) = 0$. However, by induction we have $(x - j)^{n-1}(i) = (-2j)^{n-2}(i - j) \neq 0$, a contradiction.

In the commutative case, the Strong Nullstellensatz can be easily deduced from the Weak Nullstellensatz via the Rabinowitsch trick. Let us briefly recall it (see [38, p. 380, proof of Theorem 1.5] for a more detailed exposition): Suppose J is an ideal in $\mathbb{C}[x_1, \dots, x_n]$ and $0 \neq f \in \mathcal{I}(\mathcal{Z}(J))$. Let us increase dimension by adding a variable y , and let $J' = \langle J, 1 - yf \rangle$ in $\mathbb{C}[x_1, \dots, x_n, y]$. Clearly, the elements of J have no common zero, hence by the Weak Nullstellensatz we have $J' = \mathbb{C}[x_1, \dots, x_n, y]$. Thus there are $g_0, \dots, g_r \in R', h_1, \dots, h_r \in J$ such that

$$g_0(1 - yf) + g_1h_1 + \dots + g_rh_r = 1.$$

Now, we translate the information given in this equation back to $\mathbb{C}[x_1, \dots, x_n]$ by applying the substitution \mathbb{C} -homomorphism from $\mathbb{C}[x_1, \dots, x_n, y]$ to $\mathbb{C}(x_1, \dots, x_n)$ given by $y \mapsto f^{-1}$:

$$g_1(x_1, \dots, x_n, f^{-1})h_1 + \dots + g_r(x_1, \dots, x_n, f^{-1})h_r = 1.$$

Multiplying this equation by a suitable power f^m we get:

$$\bar{g}_1h_1 + \dots + \bar{g}_rh_r = f^m$$

for suitable polynomials $\bar{g}_1, \dots, \bar{g}_r$. Thus $f \in \sqrt{J}$.

Trying to invoke this idea in the quaternionic case does not readily work, since substitution is not a homomorphism: We can carry out the first step – lifting the problem to a higher dimension, but cannot translate the information back down via substitution.

There are several other “quick” ways to prove the classical Nullstellensatz, that all fail in our case for essentially the same reason. In order to prove Theorem 3.6, we follow the more conceptual Jacobson approach. The proof requires a few lemmas, summarized in the following proposition:

Proposition 3.7. *Let R' denote the center $\mathbb{R}[x_1, \dots, x_n]$ of $R = \mathbb{H}[x_1, \dots, x_n]$. Then:*

1. *If M is a maximal left ideal in R , then the contraction $M \cap R'$ is a maximal ideal in R' .*
2. *The “going-up lemma”: If \mathfrak{m} is a maximal ideal in R' , then there is a maximal left ideal M in R with $\mathfrak{m} = M \cap R'$.*

3. The “incomparability lemma”: Let $P \subseteq Q$ be left ideals in R such that P is completely prime. If $P \cap R' = Q \cap R'$ then $P = Q$.

The proofs of the first two parts of the above lemma are technical, see [8, §3,§4]. The proof of the third part – the incomparability lemma – is trickier and more difficult than its commutative counterpart, and relies upon explicit quaternionic polynomial identities, see the proofs of [8, Proposition 4.1], [8, Lemma 4.2] and [8, Lemma 4.3]. This lemma is the heart of the proof of Theorem 3.6.

Using Proposition 3.7, we can show the proof of Theorem 3.6, which is conceptual and geometric in nature. We first have the following Jacobson-type property:

Proposition 3.8. *Let P be a completely prime left ideal in $R = \mathbb{H}[x_1, \dots, x_n]$. Then P is an intersection of maximal left ideals in R .*

Proof. The intersection $\mathfrak{p} = P \cap R'$ is a prime ideal in $R' = \mathbb{R}[x_1, \dots, x_n]$. The latter, as a polynomial ring over a field, is a Jacobson ring, hence $\mathfrak{p} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}$, where the intersection runs over all maximal ideals in R' containing \mathfrak{p} . By the going-up lemma (the second part of Proposition 3.7), for each such maximal ideal \mathfrak{m} there exists a maximal left ideal M in R with $M \cap R' = \mathfrak{m}$. Then the intersection $Q = \bigcap M$ of all these maximal left ideals is a left ideal in R with $P \subseteq Q$ and $Q \cap R' = P \cap R' = \mathfrak{p}$. Thus by the incomparability lemma, $P = Q$, hence P is an intersection of maximal left ideals. \square

Combining all of the above, we have:

Proof of Theorem 3.6. By the Weak Central Nullstellensatz, maximal left ideals in $R = \mathbb{H}[x_1, \dots, x_n]$ correspond to points in \mathbb{H}_c^n . Thus $\mathcal{I}(\mathcal{Z}(J))$ is the intersection of all maximal left ideals in R containing J . Every such ideal is, in particular, a completely prime left ideal, by the first part of Proposition 3.7. Conversely, every completely prime left ideal in R is an intersection of maximal left ideals, by the preceding proposition. Thus \sqrt{J} , which is the intersection of all completely prime left ideals in R containing J , coincides with the intersection of all maximal left ideals in R containing J . Thus $\sqrt{J} = \mathcal{I}(\mathcal{Z}(J))$. \square

The above proof raises a question for which the author do not know the answer: Does Proposition 3.8 hold if \mathbb{H} is replaced by an arbitrary division ring D ? If the answer is positive, this will yield a theorem which essentially generalizes the central quaternionic Nullstellensatz with the so-called “formal” Nullstellensatz over arbitrary fields (the fact that polynomial rings over fields are Jacobson rings).

One glaring issue with Theorem 3.6 is that it only yields an abstract, implicit description of $\mathcal{I}(\mathcal{Z}(J))$. An explicit description was given by Aryapoor in his 2024 paper [11]. He showed the following:

Theorem 3.9. *Let J be a left ideal in $\mathbb{H}[x_1, \dots, x_n]$. Then $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ is given by:*

$$\{f \mid \text{for all } a \in \mathbb{H} \text{ there exists } n \in \mathbb{N} \text{ s.t. } (af)^n \in J + J(af) + J(af)^2 + \dots + J(af)^n\}.$$

Aryapoor's proof of Theorem 3.9 relies upon Theorem 3.6 and a clever variation of the Rabinowitsch trick; As we remarked above, this technique does not apply directly as in the commutative case, since in our context substitution is not a homomorphism. Nevertheless, it is a “half-homomorphism”, satisfying the product formula given in 2.1. Aryapoor managed to exploit this formula (generalized to several variables) in order to adapt the Rabinowitsch trick to apply to the quaternionic case. The resulting claim is the more explicit version of the central quaternionic Nullstellensatz given by Theorem 3.9. Let us also note that in the special case where the ideal J happens to be a two-sided ideal, the description given by Theorem 3.9 is essentially the same as the usual explicit description of the radical in the commutative case. More precisely, if J is an ideal in $\mathbb{C}[x_1, \dots, x_n]$, then the condition that for any constant $a \in \mathbb{C}$ there exist $n \in \mathbb{N}$ such that $(af)^n \in J + J(af) + J(af)^2 + \dots + J(af)^n$ is the same as the condition that $f^n \in J$ for some $n \in \mathbb{N}$ (since $J + J(af) + J(af)^2 + \dots + J(af)^n = J$ and since non-zero constants may be divided out).

Let us also note that Aryapoor's description of the radical is specific to the quaternionic case. We do not yet have an explicit description of \sqrt{J} for a left ideal in $D[x_1, \dots, x_n]$, where D is an arbitrary division ring. This remains an open question.

Another interesting characterization of the radical was given in the recent work [20] of Cimpic. He proved the following:

Theorem 3.10 (Cimpic's characterization of the radical). *Let J be an ideal in $R = \mathbb{H}[x_1, \dots, x_n]$. Then \sqrt{J} is the intersection of all **prime** left ideals in R that contain J . Moreover, \sqrt{J} is the smallest **semi-prime** ideal in R that contains J .*

Here, a left ideal J in a ring R is called *semi-prime* if $aJa \subseteq R$ implies $a \in J$, for all $a \in R$.

Building upon Theorem 3.10 and following his earlier works [18] and [19], Cimpic studies prime, semi-prime, and completely prime left ideals in rings of matrices, as well as Nullstellensatz-type results for such rings, see [20, Theorem 1.3] and [20, Theorem 1.4]. This “matricial” line of study is beyond the scope of this survey.

Another open question that arises from Aryapoor's work is one of effectiveness: Can the integer n in Aryapoor's explicit Nullstellensatz be bounded, for all polynomials in the ideal J ? It should be noted that in the commutative case there have been numerous works studying effective versions of the Nullstellensatz, most notably the work [34] of Kollár, but in the non-commutative case such results have not yet been achieved.

3.1 The Amitsur-Small Nullstellensatz and the Amitsur-Small problem

As discussed above, in our non-commutative setup we must study left ideals in polynomial rings – limiting ourselves to two-sided ideals would simply miss out on much of the geometry. There have been some works studying limited variants of the Nullstellensatz for two-sided ideals, e.g. in [53], [14]. However, a work studying one-sided ideals in polynomial rings over division rings was conducted by Amitsur and Small in [13]. Their main result is the following:

Theorem 3.11 (Amitsur-Small Nullstellensatz). *Let D be a division ring, and let M be a maximal left ideal in $D[x_1, \dots, x_n]$. Then the quotient $D[x_1, \dots, x_n]/M$ is finite-dimensional as a left D -vector space.*

Amitsur and Small call this result a “Nullstellensatz over division rings”. However, this terminology is not quite fitting, in this author’s opinion, as the theorem is not directly concerned with zeros of polynomials: It is closer in nature to Zariski’s lemma or Noether’s normalization lemma. Granted, in the commutative case, Zariski’s lemma can be used to easily deduce the classical Nullstellensatz, but in the quaternionic case, this does not seem to follow in any immediate way. Nevertheless, [13] is an important and influential paper that led to several follow-up works. In particular, one problem that was raised in [13], and naturally arose from the proof of Theorem 3.11, is the following: Given a maximal left ideal M in $D[x_1, \dots, x_n]$, where D is a division ring, is the contraction $M \cap D[x_1]$ necessarily a maximal left ideal in $D[x_1]$? A critical lemma in the proof of Theorem 3.11 states that $M \cap D[x_1]$ is non-zero, which in the field case immediately implies that $M \cap D[x_1]$ is prime and hence maximal. However, in the case where D is an arbitrary division ring, Amitsur and Small write “We remark that we are unable to show that maximal left ideals in $D[x_1, \dots, x_n]$ intersect $D[x_1, \dots, x_k]$, $k < n$, in maximal or even semi-maximal left ideals” [13, p. 356] (a semi-maximal left ideal is the intersection of finitely many maximal left ideals). The second part of this problem was resolved by Small and Robson [31, Proposition 5.3]: They showed that if M is a semi-maximal left ideal in $D[x_1, \dots, x_n]$ then $M \cap D[x_1, \dots, x_k]$ is semi-maximal for any $1 \leq k \leq n$ (this also appears in [48, Theorem 6.8, p. 360]). The first part of the problem (whether maximal ideals contract to maximal ideals) remained unresolved by the mentioned works. Related results were given by Resco in [57], who noted that “It remains unknown, however, whether a maximal right ideal need contract to a maximal right ideal” [57, p. 70][¶]. Years later, in a paper of Rowen from 1995, he writes [39, p. 2272] that the solution to this question is negative “as shown recently by Amitsur and Small”. However, no reference is given by Rowen, and there does not seem to be a paper from that time presenting an answer. The author had written to Small, who does not recall that he or Amitsur had resolved this problem, and to Rowen, who also does not recall what the mentioned sentence in his work refers to.

The recent note [22] by Chapman and the author establishes a negative answer to the problem of Amitsur and Small, via Theorem 3.13 below (the paper [22] extends an unpublished note [52] by the author, which provided the first counter examples). However, it is also shown in [22] that for the quaternionic ring \mathbb{H} the answer to the Amitsur-Small problem is positive. This leads to the following definition:

Definition 3.12. *Let D be a division ring. We say that D is an Amitsur-Small ring if for all $n \in \mathbb{N}$ and $1 \leq k \leq n$, and for any maximal left ideal in $D[x_1, \dots, x_n]$, the contraction $M \cap D[x_1, \dots, x_k]$ is a maximal left ideal in $D[x_1, \dots, x_k]$.*

Examples of Amitsur-Small rings include all commutative fields [22, Proposition 3.3], and Hamilton’s real quaternion algebra \mathbb{H} [22, §4]. The main result of [22] is the following:

¶

Some of the mentioned papers work with left ideals, and some with right ideals, but of course, the two notions are interchangeable.

Theorem 3.13. *The only possible Amitsur-Small division algebras of degree 2 or 3 over their center are quaternions algebras $(-1, -1)_{2,F}$ over a Pythagorean field F .*

(Recall that a field F is called *Pythagorean* if every sum of squares in F is a square). From Theorem 3.13 it follows, for example, that the rational quaternion algebra $\mathbb{H}_{\mathbb{Q}} = (-1, -1)_{2,\mathbb{Q}}$ is not an Amitsur-Small ring, nor is the quaternion algebra $\mathbb{H}_{\mathbb{Q}_p} = (-1, -1)_{2,\mathbb{Q}_p}$ over any p -adic field, since \mathbb{Q} and \mathbb{Q}_p are not Pythagorean fields. An upcoming work of Chapman, Levin and Zaninelli [21] extends Theorem 3.13 further: By employing results of Lotscher, MacDonald, Meyer and Reichstein, they prove that every cyclic division algebra of prime order larger than 2 is not Amitsur-Small. An open question is whether every division ring of the form $(-1, -1)_{2,F}$ where F is a Pythagorean field necessarily an Amitsur-Small ring.

Remark 3.14. *Definition 3.12 is motivated, on the one hand, from the negative examples given by Theorem 3.13, and on the other hand, from the positive theorem of Small and Robson [31, Proposition 5.3], stating that if M is a semi-maximal left ideal in $D[x_1, \dots, x_n]$ then $M \cap D[x_1, \dots, x_k]$ is semi-maximal for any $1 \leq k \leq n$. In the examples of non Amitsur-Small division rings given in [22], the demonstration is with $n = 2, k = 1$. It is yet unknown to the author whether there exist non Amitsur-Small division rings where such examples are only possible with different values of n, k .*

There is an inherent connection between the Amitsur-Small problem, Amitsur-Small rings and the (weak) central quaternionic Nullstellensatz. In order to discuss this connection, let us introduce the following terminology:

Definition 3.15. *Let D be a division ring. We say that D is a Nullstellensatz ring, if for any $n \in \mathbb{N}$, the maximal left ideals in $D[x_1, \dots, x_n]$ are of the form $(x_1 - a_1, \dots, x_n - a_n)$, for some $(a_1, \dots, a_n) \in D_c^n$.*

In other words, a division ring is a Nullstellensatz ring if it satisfies the same algebro-geometric correspondence exhibited by the weak central Nullstellensatz for the quaternionic ring \mathbb{H} . Clearly, a Nullstellensatz ring D must be *algebraically closed*, in the sense that every non-constant polynomial in $D[x]$ must admit a zero in D . By a theorem of Baer in [49], a non-commutative centrally finite algebraically closed division ring is isomorphic to a quaternion ring over a real-closed field. However, there are examples of infinitely-dimensional algebraically closed division rings, the first constructed by Makar-Limanov in [46], and a variation of it in [33]. The rings in these examples satisfy an even stronger property – every *polynomial function* over them admits a zero (we shall discuss polynomial functions over division rings extensively in §6 below). We do not know whether every algebraically closed division ring is a Nullstellensatz ring – we only know this to hold for fields and for the real quaternion algebra \mathbb{H} (it should be noted that not every polynomial function over \mathbb{H} admits a zero, as will be discussed in §6). This problem is connected to the Amitsur-Small problem, via the following result [22, Theorem 4.2]:

Theorem 3.16. *Let D be an algebraically closed division ring. Then D is a Nullstellensatz ring if and only if D is an Amitsur-Small ring.*

Proof. Suppose that D is a Nullstellensatz ring, and let $M = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ be a maximal left ideal in $D[x_1, \dots, x_n]$, for a suitable point $(a_1, \dots, a_n) \in D_c^n$. Then for each $1 \leq k \leq n$, we have $x_1 - a_1, \dots, x_k - a_k \in M \cap D[x_1, \dots, x_k]$. But $\langle x_1 - a_1, \dots, x_k - a_k \rangle$ is a maximal left ideal in $D[x_1, \dots, x_k]$, by Lemma 2.5. Thus we must have an equality $M \cap D[x_1, \dots, x_k] = \langle x_1 - a_1, \dots, x_k - a_k \rangle$, hence $M \cap D[x_1, \dots, x_k]$ is maximal. Thus D is an Amitsur-Small ring.

Conversely, suppose that D is an Amitsur-Small ring, and let M be a maximal left ideal in $D[x_1, \dots, x_n]$. By [13, Lemma A], for each $1 \leq i \leq n$ we have $M \cap D[x_i] \neq 0$, and since $D[x_i]$ is a left principal ideal domain (see for example, [50]), we have $M \cap D[x_i] = D[x_i]p_i$ for a suitable monic polynomial p_i of minimal degree in x_i in M . By our assumptions, $D[x_i]p_i$ is a maximal left ideal in $D[x_i]$, hence p_i must be irreducible in $D[x_i]$. But since D is algebraically closed, p_i is right-hand divisible by $x_i - a_i$ for some $a_i \in D$, hence $p_i = x_i - a_i$, since p_i is monic. Thus M contains the left ideal $\langle x_1 - a_1, \dots, x_n - a_n \rangle$. If $(a_1, \dots, a_n) \notin D_c^n$ we get, by Lemma 2.5, that $M = D[x_1, \dots, x_n]$, a contradiction. Thus $(a_1, \dots, a_n) \in D_c^n$ and hence by Lemma 2.5 $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ is a maximal left ideal, hence $M = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Thus D is a Nullstellensatz ring. \square

A recent paper [12] of Aryapoor proves another equivalent criterion: An algebraically closed division ring is Amitsur-Small if and only if for every sequence a_1, \dots, a_k of pairwise commuting elements in D , the centralizer $C(a_1, \dots, a_k)$ is itself an algebraically closed division ring. Aryapoor calls rings satisfying this property *centrally algebraically closed*.

The above results raise the following question: Is every algebraically closed division ring a Nullstellensatz ring? (Equivalently, an Amitsur-Small ring?) Is the Makar-Limanov ring, in particular, a Nullstellensatz ring? The answer is yet unknown.

Finally, let us mention another recent result by the author and Thieu [56, Theorem 1.1] which is closely related to the Amitsur-Small Nullstellensatz of [13]:

Theorem 3.17 (Noether’s normalization for division rings). *Let D be a division ring, let I be a two-sided ideal in $D[x_1, \dots, x_n]$ and let $R = D[x_1, \dots, x_n]/I$. Then R is finite as a left module over a subring which is isomorphic to a polynomial ring in $k \leq n$ central variables over D .*

Let us emphasize that in the Nullstellensatz of Amitsur and Small, the ideal I is one-sided, but maximal, while in Theorem 3.17 the ideal I is an arbitrary two-sided ideal. Additional extensions of Noether’s normalization lemma to multivariate skew polynomial rings are studied in [56].

4 Quaternionic polynomials as slice regular functions

Let D be a division ring, and let $D[x_1, x_2, \dots, x_n]$ be the ring of polynomials in n central variables over D . As evident by Lemma 2.5, substitution in such polynomials is naturally well-defined only at points in the central affine space D_c^n . However, if one wants to “force the issue”, one can define substitution at any point in D^n by first fixing an ordering

of the variables, say the linear ordering, presenting each monomial with the order of multiplication determined by the fixed ordering, and then substituting along that order. For example, fixing $x_1 < x_2$, the evaluation of $x_1x_2 \in \mathbb{H}[x_1, x_2]$ at (i, j) would be determined to be $i \cdot j = k$.

While the choice of ordering is arbitrary, via this approach we may associate to each point $a \in \mathbb{H}^n$ a function $\varphi_a: \mathbb{H}^n \rightarrow \mathbb{H}$ which belongs to the class of *slice regular functions*. The theory of such functions, which is a quaternionic multi-variable extension of complex analysis, has been developed over the last 20 years, see for example [27], [28] and [58].

This extension of the substitution space from D_c^n to D^n comes at the price of losing some of the algebraic structure: The set of polynomials vanishing (as slice regular functions) at a set in D^n need not even be a left ideal. Nevertheless, given a left ideal J in R , we may denote by $\mathcal{V}(J)$ its set of zeros in D^n , and denote by $\mathcal{I}(\mathcal{V}(J))$ the set of polynomials in $D[x_1, x_2, \dots, x_n]$ which vanish (as slice regular functions) at $\mathcal{V}(J)$. Once again, the question arises – what happens when going back and forth between algebra and geometry? What is $\mathcal{I}(\mathcal{V}(J))$?

In [29], Gori, Sarfatti, and Vlacci prove the following remarkable result: If $n = 2$, then $\mathcal{I}(\mathcal{V}(J)) = \mathcal{I}(\mathcal{Z}(J))$! Equivalently, by the Central Quaternionic Nullstellensatz, $\mathcal{I}(\mathcal{V}(J)) = \sqrt{J}$. This theorem can be seen as a two-dimensional quaternionic Nullstellensatz for slice regular functions. Naturally, this raises the question of whether the same result holds in an arbitrary dimension. Gori, Sarfatti, and Vlacci conjectured in [29] that it does, which was confirmed by Alon and the author in [10], and independently proven by Gori, Sarfatti, and Vlacci in [30], with a different proof. Thus we have the following theorem:

Theorem 4.1 (Slice Regular Quaternionic Nullstellensatz). *Let J be a left ideal in $R = \mathbb{H}[x_1, \dots, x_n]$. Then $\mathcal{I}(\mathcal{V}(J))$ is the radical \sqrt{J} of J (as defined in Definition 3.5).*

Theorem 4.1 follows as an immediate consequence of the following result [10, Theorem 1.1]:

Theorem 4.2. *Let J be a left ideal in $R = \mathbb{H}[x_1, \dots, x_n]$. If a polynomial in R vanishes at $\mathcal{Z}(J)$, then as a slice regular function, it vanishes at $\mathcal{V}(J)$.*

The proof of Theorem 4.2 combines algebro-geometric and combinatorial ideas, which we shall not cover here, see [10, §3, §4] for details.

Theorem 4.2 and Theorem 4.1 reveal the non-obvious fact that interpreting polynomials in central variables as slice regular functions does not, in fact, yield a richer geometry than only considering them as polynomials in central variables in the sense discussed in the preceding sections. Nevertheless, these results and their proofs are of their own interest, and raise natural follow-up questions.

In particular, one could ask whether Theorem 4.2 holds when replacing the quaternion ring \mathbb{H} with an arbitrary division ring D . This was raised as an open question in [10], which was negatively resolved in a follow-up work by Alon, Chapman and the author [2], which provided a counter example. In that example, the division ring D is the symbol algebra $(\alpha, \beta)_F$, where F is a rational function field in three variables (α, β, γ) over \mathbb{R} ,

see [2, Proposition 6.1] for details. Describing the division rings for which the analogue of Theorem 4.2 holds is an open problem. In addition, [2] provides refined results concerning the geometry of zero sets of quaternionic polynomials. In particular, it provides a description of the “algebraic hull” of points in \mathbb{H}^n , proving that they are products of spheres, see the introduction of [2] for details.

5 The Combinatorial Nullstellensatz over division rings

Noga Alon’s celebrated Combinatorial Nullstellensatz is a central tool of modern algebraic combinatorics. The now classical theorem states the following:

Theorem 5.1. *Let K be a field and $p \in K[x_1, \dots, x_n]$ a polynomial of degree $\sum_{i=1}^n k_i$, where each k_i is a non-negative integer. Suppose that the coefficient of $x_1^{k_1} \cdots x_n^{k_n}$ in p is non-zero. If A_1, \dots, A_n are subsets of K with $|A_i| > k_i$ for $1 \leq i \leq n$, then there exists $a \in A_1 \times \cdots \times A_n$ such that $p(a) \neq 0$.*

Intuitively, the theorem states that any non-zero polynomial cannot vanish at a large enough “grid” in the affine space K . In the special case where $n = 1$, the theorem simply restates the rudimentary fact that a one-variable non-zero polynomial over a field cannot have more zeros than its degree. The theorem has numerous applications to various areas of combinatorics, including additive number theory, graph theory, and combinatorial geometry, see [4]. It is thus natural to ask whether the theorem can be extended from fields to division rings. Here one must note that already for one variable, the naive generalization of the theorem fails: As noted in §2, over division rings, one-variable polynomials may have more zeros than their degree.

In [51], the author generalized Alon’s theorem from fields to division rings. The key observation for this generalization, is that in the non-commutative case, the size of the sets A_1, \dots, A_n should not be measured by their cardinality, but rather by their algebraic rank (the same notion introduced by Lam and Leroy for other theoretical reasons, as discussed in §2). The statement of the generalized theorem is as follows:

Theorem 5.2 (Combinatorial Nullstellensatz over division rings). *Let D be a division ring and let $p \in D[x_1, \dots, x_n]$ be a polynomial of degree $\sum_{i=1}^n k_i$, in which the coefficient of $x_1^{k_1} \cdots x_n^{k_n}$ is non-zero. Let A_1, \dots, A_n be algebraic subsets of D with $A_1 \times \cdots \times A_n \subseteq D_c^n$ and $\text{rk}(A_i) > k_i$ for $i = 1, 2, \dots, n$. Then there exists $a \in A_1 \times \cdots \times A_n$ such that $p(a) \neq 0$.*

Proof. The proof here is inspired by Michalek’s proof of Alon’s Nullstellensatz, given in [47]. Suppose to the contrary that p vanishes at every point in $A_1 \times \cdots \times A_n$.

If $\deg(p) = 0$ then p is a non-zero constant in D and the assertion holds trivially. Suppose that $\deg(p) > 0$, that p vanishes on $A_1 \times \cdots \times A_n$, and that we have proven the theorem for all polynomials of degree smaller than $\deg(p)$. Without loss of generality, by permuting the labels of the variables, we may assume that $k_1 > 0$. Choose $a_1 \in A_1$ and apply right-hand division with remainder to write $p = q \cdot (x_1 - a_1) + r$ with $r \in D[x_2, \dots, x_n][x_1]$ of degree smaller than 1 in x_1 . That is, $r \in D[x_2, \dots, x_n]$. Since in p there appears a monomial of

the form $\lambda x_1^{k_1} \cdots x_n^{k_n}$, in q there appears a monomial of the form $\lambda x_1^{k_1-1} \cdots x_n^{k_n}$, and clearly $\deg(q) = \deg(p) - 1$.

Since $A_1 \times \cdots \times A_n \subseteq D_c^n$, given a point $a \in \{a_1\} \times A_2 \times \cdots \times A_n$, we may substitute it into the equation $p = q(x_1 - a_1) + r$ and get that $p(a) = r(a) = 0$. Since $r \in D[x_2, \dots, x_n]$, this means that r vanishes on the set $A_2 \times \cdots \times A_n$. In particular, for any point $b \in (A_1 \setminus \{a_1\}) \times A_2 \times \cdots \times A_n$ we have $r(b) = 0$, when viewing r as a polynomial in $D[x_1, \dots, x_n]$. Thus $(q(x_1 - a_1))(b) = p(b) - r(b) = 0$.

Consider the substitution map from $D[x_1, \dots, x_n] = D[x_2, \dots, x_n][x_1]$ to $D[x_2, \dots, x_n]$ given by $h(x_1, x_2, \dots, x_n) \mapsto h(b_1, x_2, \dots, x_n)$. By Lemma 2.1, applying this substitution to $q \cdot (x_1 - a_1)$ gives $q(b_1^{b_1-a_1}, x_2, \dots, x_n) \cdot (b_1 - a_1) \in D[x_2, \dots, x_n]$.

Next, applying the substitution $x_2 \mapsto a_2$ to this polynomial, we get the polynomial

$$q(b_1^{b_1-a_1}, a_2^{b_1-a_1}, x_3, \dots, x_n) \cdot (b_1 - a_1) \in D[x_3, \dots, x_n].$$

(Here we have used Lemma 2.1 in the special case where g is the constant $b_1 - a_1$.) But since the elements of A_1 commute with those of A_2 , we have $a_2^{b_1-a_1} = a_2$. Continuing to substitute all of the variables up to $x_n \mapsto a_n$, we get that

$$(q(x_1 - a_1))(b_1, a_2, \dots, a_n) = q(b_1^{b_1-a_1}, a_2, \dots, a_n) \cdot (b_1 - a_1).$$

Thus q vanishes at $(b_1^{b_1-a_1}, a_2, \dots, a_n)$. Note that this is indeed a point in D_c^n : For $i = 2, \dots, n$ we have:

$$b_1^{b_1-a_1} a_i = b_1^{b_1-a_1} a_i^{b_1-a_1} = (b_1 a_i)^{b_1-a_1} = (a_i b_1)^{b_1-a_1} = a_i^{b_1-a_1} b_1^{b_1-a_1} = a_i b_1^{b_1-a_1}$$

and $a_i a_j = a_j a_i$ for $1 < i < j \leq n$ since $(b_1, a_2, \dots, a_n) \in A_1 \times \cdots \times A_n \subseteq D_c^n$.

Put $B_1 = \{b_1^{b_1-a_1} | b_1 \in A_1 \setminus \{a_1\}\}$, and consider the polynomial

$$(\text{lcm}(x_1 - b_1^{b_1-a_1} | b_1 \in A_1 \setminus \{a_1\})) \cdot (x_1 - a_1) = (\text{lcm}(x_1 - c_1 | c_1 \in B_1)) \cdot (x_1 - a_1).$$

By Lemma 2.3, this polynomial is right-hand divisible in $D[x_1]$ by $\text{lcm}(x_1 - b_1 | b_1 \in A_1)$. By our assumptions, the degree $\text{rk}(A_1)$ of the latter polynomial is larger than k_1 , hence

$$\deg(\text{lcm}(x_1 - c_1 | c_1 \in B_1)) + 1 > k_1,$$

hence $\deg(\text{lcm}(x_1 - c_1 | c_1 \in B_1)) > k_1 - 1$.

We have shown that q vanishes on the set $B_1 \times A_2 \times \cdots \times A_n$. Since $\deg(q) = \deg(p) - 1$ and in q there appears the monomial $\lambda x_1^{k_1-1} \cdot x_2^{k_2} \cdots x_n^{k_n}$, this contradicts the induction hypothesis. \square

To show the value of the generalization from fields to division rings, below we demonstrate a couple of applications. Let us emphasize that the condition $A_1 \times \cdots \times A_n \subseteq D_c^n$ of the theorem only requires the elements of each set A_i to commute with those of A_j for $i \neq j$, while the elements of each set A_i need not commute with each other. This requirement is

natural in our context, since substitution is defined only at D_c^n . Moreover, as we will see, the necessity of this condition arises naturally in the applications below. This shows that here too, there is no inherent need to extend the space from D_c^n to D^n by interpreting polynomials as slice regular functions. Let us also remark that a generalization of Theorem 5.2 to multivariate skew polynomial rings is given in an upcoming work [1].

5.1 The Cauchy-Davenport theorem for division rings

Let G be a non-trivial abelian group. Let $\rho(G)$ denote the order of its smallest non-trivial subgroup (possibly $\rho(G) = \infty$). Let A, B be non-empty finite subsets of G , and let $A + B$ denote the *sumset* $\{a + b \mid a \in A, b \in B\}$. A combinatorial question is the following: How small can the set $A + B$ be. A theorem of Károlyi [32] asserts that if $|A + B| \leq \rho(G) + 1$, then $|A + B| \geq |A| + |B| - 1$. This result is known as the “Cauchy-Davenport theorem for abelian groups”. (In the special case where $G = \mathbb{Z}_p$ is the additive cyclic group of p elements, we obtain the classical Cauchy-Davenport theorem.)

This theorem applies to any non-trivial abelian group, and as such it applies to the additive group of any division ring D . However, this does not provide any meaningful information on the ring, since it ignores the multiplicative structure (for example, if $D = \mathbb{H}$, the statement is essentially a result for the group \mathbb{R}^4). In order to get a meaningful statement for division rings, we shall consider two algebraic sets A, B in D , and measure their size by their algebraic rank, instead of their cardinality. Then we can ask: How small can the **rank** of $A + B$ be? This is a question in which the multiplicative structure of the ring plays an inherent role via the minimal polynomials of the given sets. We have the following answer, given by the author in [51]:

Theorem 5.3. *Let D be a division ring. Let A, B be commuting^{||} algebraic sets in D . If $\text{rk}(A) + \text{rk}(B) - 1 \leq \rho(D)^{**}$, then $\text{rk}(A + B) \geq \text{rk}(A) + \text{rk}(B) - 1$.*

Proof. Suppose that $\text{rk}(A) + \text{rk}(B) - 1 \leq \rho(D)$ but $\text{rk}(A + B) \leq \text{rk}(A) + \text{rk}(B) - 2$. Let $r = \text{rk}(A) + \text{rk}(B) - \text{rk}(A + B) - 2$. By the Gordon-Motzkin theorem, we have

$$r + c(A + B) \leq r + \text{rk}(A + B) < \rho(D).$$

(here $c(A + B)$ denotes the number of conjugacy classes represented by elements of $A + B$). Let K denote the center of D . By definition, $\rho(D)$ is the cardinality of the prime field K_0 of K . Each element of K belongs to its own singleton conjugacy class, and in particular $A + B$ contains less than $\rho(D) - r$ elements of K_0 . Let us arbitrarily choose distinct elements $c_1, \dots, c_r \in K_0 \setminus (A + B)$, and let $C = (A + B) \cup \{c_1, \dots, c_r\}$.

Let $z = x + y$, and consider the subring $D[z]$ of $D[x, y]$. Since x, y are central, so is z , hence we may view $D[z]$ as an isomorphic copy of a polynomial ring in one central variable

||

By “commuting sets” here we mean that each element of A commutes with each element of B .

**

If D is of characteristic 0, then this condition is void.

over D . Let $p = \text{lcm}(z - c \mid c \in C) \in D[z]$ be the minimal polynomial of C . Since c_1, \dots, c_r all belong to singleton conjugacy classes, by a theorem of Lam [36, Theorem 22] we have

$$\text{rk}(C) = \text{rk}(A + B) + r = \text{rk}(A) + \text{rk}(B) - 2.$$

Let $k = \text{rk}(A) - 1, m = \text{rk}(B) - 1, n = \deg(p) = k + m$, and write $p = z^n + p_{n-1}z^{n-1} + \dots + p_0$. Recalling that $z = x + y$ and then expanding, let us present p as $(x + y)^n$ plus a sum of monomials of degree smaller than n . The polynomial $(x + y)^n$ belongs to the subring $K[x, y]$ of $D[x, y]$. Here we may apply the usual binomial formula, and so the coefficient of $x^k y^m$ in $(x + y)^n$, and hence in p , is $\binom{n}{k} = \binom{\text{rk}(A) + \text{rk}(B) - 2}{\text{rk}(A) - 1}$. This is a non-zero element in $K \subseteq D$, since $\text{rk}(A) + \text{rk}(B) - 2 < \rho(D)$.

By Theorem 5.2, there is a point $(a, b) \in A \times B$ with $p(a, b) \neq 0$ (viewing p as a polynomial in $D[x, y]$). But by our choice of p , we can write $p = q \cdot (x + y - (a + b))$ for some $q \in D[z] \subseteq D[x, y]$. Since $x + y - (a + b)$ vanishes at (a, b) we also have $p(a, b) = 0$, a contradiction. \square

Clearly, if D is a field, then the above theorem coincides with the theorem of Károlyi for the additive group of D , since in fields a set is algebraic if and only if it is finite, in which case we have $\text{rk}(A) = |A|, \text{rk}(B) = |B|$.

Remark 5.4. In the formulation of Theorem 5.3, the condition that A, B are commuting cannot be dropped. Indeed, take $D = \mathbb{H}$ to be the real quaternion algebra (where $\rho(D) = \infty$), and let $A = \{i, -i\}, B = \{j, -j\}$. Then $A + B = \{i + j, -i + j, i - j, -i - j\}$, and one directly verifies that A, B have the same minimal polynomial $x^2 + 1$, while the sumset $A + B$ has minimal polynomial $x^2 + 2$. Thus $\text{rk}(A) = \text{rk}(B) = \text{rk}(A + B) = 2$, so $\text{rk}(A + B) < \text{rk}(A) + \text{rk}(B) - 1 = 3$.

5.2 The Erdős-Heilbron Theorem for division rings

Given subsets A, B of an additive group, let $A \oplus B = \{a + b \mid a \in A, b \in B, a \neq b\}$. The following result was conjectured by Erdős and Heilbron in [25], and remained an open problem for many years, until finally proven by Dias da Silva and Hamidoune in [60].

Theorem 5.5. Let p be a prime and let A, B be non-empty subsets of \mathbb{Z}_p . Then $|A \oplus B| \geq \min\{p, |A| + |B| - 3\}$.

A very short proof of this theorem, based on the Combinatorial Nullstellensatz, was given by Alon-Nathanson-Rusza in [6]. They give a slightly more general version [6, Theorem 1], from which Theorem 5.5 follows as a special case (see [6, p. 253]). Let us prove here an analogue of their generalization of their theorem, for algebraic sets in division rings:

Theorem 5.6. Let D be a division ring, and let $A, B \subseteq D$ be commuting algebraic sets with $\text{rk}(A) \neq \text{rk}(B)$. If $\text{rk}(A) + \text{rk}(B) - 2 \leq \rho(D)$ then $\text{rk}(A \oplus B) \geq \text{rk}(A) + \text{rk}(B) - 2$.

Proof. Suppose that A, B satisfy $\text{rk}(A) + \text{rk}(B) - 2 \leq \rho(D)$ but $n \leq k + m - 3$, where $n = \text{rk}(A \oplus B), k = \text{rk}(A), m = \text{rk}(B)$.

Let $r = k + m - n - 3$. Let K be the center of D and let K_0 be the prime field of K . As in the proof of Theorem 5.3, let us arbitrarily choose elements $c_1, \dots, c_r \in K_0 \setminus (A \oplus B)$, and let $C = (A \oplus B) \cup \{c_1, \dots, c_r\}$. Again by [36, Theorem 22], we have $\text{rk}(C) = \text{rk}(A \oplus B) + r = k + m - 3$.

Put $z = x + y$ and let $f_C = \text{lcm}(z - c | c \in C)$ be a minimal polynomial for C in $D[z] \subseteq D[x, y]$. Let $g = (x - y) \cdot f_C$. This polynomial vanishes at $A \times B$. Multiplying it from the left by $(x + y)^r$ we get a polynomial h of degree $k + m - 2$ that vanishes at $A \times B$. As in the proof of Theorem 5.3, when expanding h there is no contribution from lower terms and we can compute the coefficient of $x^{k-1}y^{m-1}$ in h as in the commutative case. It is

$$\binom{k+m-3}{k-2} - \binom{k+m-3}{k-1} = \binom{(k-m)(k+m-3)!}{(k-1)!(m-1)!}$$

which is a non-zero element since $k + m - 3 < \rho(D)$ and $k \neq m$.

By Theorem 5.2, there is a point $(a, b) \in A \times B$ such that $h(a, b) \neq 0$. If $a + b \in C$, then we have $f_C = q \cdot (x + y - (a + b))$ for some $q \in D[z] \subseteq D[x, y]$. Since $x + y - (a + b)$ vanishes at (a, b) , so does h , a contradiction. Thus $a + b \notin C$, hence $a + b \notin A \oplus B$. Thus $a = b$. Finally, since $x - y$ is central, we have $g = f_C \cdot (x - y)$. But the polynomial $x - y$ vanishes at $(a, b) = (a, a)$, hence so does h , a contradiction. \square

We note that in the case where the ring D is a field of prime order, Theorem 5.6 specializes to Theorem 1 in [6] of Alon-Nathanson-Rusza. Indeed, in this case one can assume without loss of generality that $\text{rk}(A) + \text{rk}(B) - 2 = |A| + |B| - 2 \leq \rho(D)$, see the first lines of the proof of [6, Theorem 1].

Remark 5.7. Here too, the condition that A, B are commuting sets cannot be dropped. Indeed, let $D = \mathbb{H}$, and let $A = \{i, j\}$, $B = \{i, j, \frac{-1+\sqrt{3}}{2}(i+j)\}$. The minimal polynomial of A is $x^2 + 1$, while the minimal polynomial of B is $(x^2 + 1)(x - \frac{-1+\sqrt{3}}{2}(i+j))$, hence $\text{rk}(A) = 2, \text{rk}(B) = 3$. The minimal polynomial of

$$A \oplus B = \{i + j, \frac{1+\sqrt{3}}{2}i + \frac{-1+\sqrt{3}}{2}j, \frac{1+\sqrt{3}}{2}j + \frac{-1+\sqrt{3}}{2}i\}$$

is $x^2 + 2$, as one readily verifies. Thus $\text{rk}(A \oplus B) = 2$ is smaller than $\text{rk}(A) + \text{rk}(B) - 2 = 3$.

5.3 An application to combinatorial quaternionic geometry

Another variant of the Combinatorial Nullstellensatz, for rings of polynomial functions over division algebras, is given in [51, §5]. We shall not recount its exact formulation here, but only briefly mention a combinatorial application of a different flavor than those of the preceding subsections. Consider the following question: How many hyperplanes in \mathbb{R}^n are needed to cover all vertices of the unit cube except one? This question was asked by Komjath in 1992, and answered by Alon and Furedi in [3]: Precisely n hyperplanes are needed.

One can ask the same question for *quaternionic hyperplanes*, by which we mean the set of points in \mathbb{H}^n cut by an equation of the form

$$a_1 X_1 b_1 + \dots + a_n X_n b_n = c,$$

where $a_1, b_1, \dots, a_n, b_n, c$ are arbitrary quaternions. Using [51, Theorem 1.1], it is shown in [51, Theorem 5.2] that here too, precisely n such hyperplanes are needed to cover all vertices of the unit cube except one.

6 Zeros of polynomials functions over division rings

Up until this point, we have only considered zeros of polynomials in central variables over division rings. However, one may consider more general *polynomial functions* over division rings. Consider, for example, the quaternionic map $a \mapsto ai + ia$ from \mathbb{H} to \mathbb{H} . One easily checks that this map cannot be represented by substitution in any polynomial in a **central** variable over \mathbb{H} . Nevertheless, one may reasonably call this map a *polynomial function* – the function $Xi + iX$. When considering such functions, we shall denote our variables using capital letters, to add an additional visual distinction between them and the central variables considered above.

Given a division ring D , we shall denote by $D\{X_1, \dots, X_n\}$ the ring of all *polynomial functions* in n variables X_1, \dots, X_n over D . The elements of $D\{X_1, \dots, X_n\}$ are all functions from D^n to D that can be expressed using only sums and products of the variables and scalars from D .

Note that here, unlike the case of the ring of polynomials in central variables, substitution of any point $a = (a_1, \dots, a_n) \in D^n$ is always well-defined, and induces a homomorphism φ_a from $D\{X_1, \dots, X_n\}$ to D . Thus for any (two-sided!) ideal J in $D\{X_1, \dots, X_n\}$, we may associate the zero set $\mathcal{Z}(J)$ of all points in D^n at which all functions in J vanish. Conversely, given a set of points Z in D^n , we may associate the vanishing ideal $\mathcal{I}(Z)$, consisting of all functions in $D\{X_1, \dots, X_n\}$ which vanish at every point of D . Once again the question arises: What is $\mathcal{I}(\mathcal{Z}(J))$? It should be noted that here, for $D = \mathbb{H}$ the situation is very different than that of the central Nullstellensatz, already for $n = 1$. Indeed, here there exist one-variable polynomial functions that admit no quaternionic zeros, for example the function $Xi + iX + j$, as one easily verifies. (It should be noted that Eilenberg and Niven establish a class of polynomial functions over \mathbb{H} that all admit a zero, a class which is wider than just the “one-sided” non-constant polynomial functions, see [24, Theorem 1].)

The above question was answered in [7] for $D = \mathbb{H}$, establishing a Nullstellensatz for quaternionic polynomial functions. Before describing this result, let us describe the answer in the case where $D = \mathbb{R}$ is the usual field of real numbers. Here, by the *Real Nullstellensatz* (Krivine 1964, Dubois-Risler 1969), we have $\mathcal{I}(\mathcal{Z}(J))$ is the *real radical* $\sqrt[\mathbb{R}]{J}$ of J , defined as

$$\sqrt[\mathbb{R}]{J} = \{f \in \mathbb{R}[x_1, \dots, x_n] \mid f^{2d} + g_1^2 + \dots + g_s^2 \in J\}$$

for some $g_1, \dots, g_s \in \mathbb{R}[x_1, \dots, x_n], d \in \mathbb{N}$.

Equivalently, $\sqrt[\mathbb{R}]{J}$ is the intersection of all prime *real ideals* containing J : An ideal J (in an arbitrary ring) is called **real** if $g_1^2 + \dots + g_s^2 \in J$ implies $g_1, \dots, g_s \in J$, for all $g_1, \dots, g_s \in R$.

The formulation of the quaternionic analogue of this theorem is of a similar nature. First, one must note that given a function $f \in \mathbb{H}\{X_1, \dots, X_n\}$, the point-wise conjugate^{††} function \bar{f} also belongs to $\mathbb{H}\{X_1, \dots, X_n\}$. We call an ideal J in this ring *quaternionic*, if $\bar{g}_1 g_1 + \dots + \bar{g}_s g_s \in J$ implies $g_1, \dots, g_s \in J$. A two-sided ideal P in a ring R is called *prime* if $(a)(b) \subseteq P$ implies $(a) \subseteq P$ or $(b) \subseteq P$, for any $a, b \in R$ (this is the standard definition of a two-sided prime ideal in ring theory, due to Krull). We then have:

Theorem 6.1 (The Nullstellensatz for quaternionic polynomial functions). *For an ideal J in $R = \mathbb{H}\{X_1, \dots, X_n\}$, the ideal $\mathcal{I}(\mathcal{Z}(J))$ is the quaternionic radical of J , defined as:*

$$\sqrt[\mathbb{H}]{J} = \{f \in R \mid (\bar{f}f)^d + \bar{g}_1 g_1 + \dots + \bar{g}_s g_s \in J \text{ for some } g_1, \dots, g_s \in R, d \in \mathbb{N}\}.$$

Equivalently, $\sqrt[\mathbb{H}]{J}$ is the intersection of all quaternionic prime ideals in R containing J .

The key to the proof of Theorem 6.1 is an observation regarding the structure of the ring $\mathbb{H}\{X_1, \dots, X_n\}$: Generally, if D is a division ring of finite dimension d over its center K , then $D\{X_1, \dots, X_n\}$ is isomorphic to the ring of polynomials in nd central variables over D – a fact shown in [7, §3], where the structure of these rings is studied. Let us briefly describe this isomorphism: Fix a basis b_1, \dots, b_d for D over K . Given a function $f \in D\{X_1, \dots, X_n\}$, let us present it as $f = \sum_{l=1}^d b_l f_l$, where f_1, \dots, f_d are functions from D^n to K . We shall call f_1, \dots, f_d the **components** of f (these of course depend on our choice of basis). By [7, Corollary 4], f_1, \dots, f_n are themselves polynomial functions in $D\{X_1, \dots, X_n\}$! This follows from a theorem of Wilczynski from 2014, independently discovered in [7]: Let us introduce additional variables $Y_{ij}, 1 \leq i \leq n, 1 \leq j \leq d$, and consider the usual polynomial ring $K[Y_{ij} \mid 1 \leq i \leq n, 1 \leq j \leq d]$. We may view each f_l as an element of this ring, by [7, Theorem 5] or [62, Theorem 4.1]: Given a vector $y = (y_{ij})$, put $x_i = \sum b_j y_{ij}$ for each $1 \leq i \leq n$. Then $f_l(y) = f_l(x_1, \dots, x_n)$. For example, in the case where $D = \mathbb{H}$ and $n = 1$, we have, by direct verification (writing x instead of x_1):

$$\begin{aligned} 4y_1 &= x - \mathrm{i}x\mathrm{i} - \mathrm{j}x\mathrm{j} - \mathrm{k}x\mathrm{k} \\ 4y_2 &= \mathrm{j}x\mathrm{k} - x\mathrm{i} - \mathrm{i}x - \mathrm{k}x\mathrm{j} \\ 4y_3 &= \mathrm{k}x\mathrm{i} - x\mathrm{j} - \mathrm{j}x - \mathrm{i}x\mathrm{k} \\ 4y_4 &= \mathrm{i}x\mathrm{j} - x\mathrm{k} - \mathrm{k}x - \mathrm{j}x\mathrm{i}. \end{aligned}$$

Using this isomorphism, the proof of Theorem 6.1 is carried out by interpreting functions in $\mathbb{H}\{X_1, \dots, X_n\}$ as suitable vectors of real functions, which allows one to translate the problem into one for which the Real Nullstellensatz can be applied, and then translate the information back over \mathbb{H} and obtain the description given in Theorem 6.1. For the exact details of this translation technique, see [7, §2, §3, §4].

††

The conjugate of a quaternion $z = a + \mathrm{i}b + \mathrm{j}c + \mathrm{k}d$ is given by $\bar{z} = a - \mathrm{i}b - \mathrm{j}c - \mathrm{k}d$.

Next, let us consider the question of describing $\mathcal{I}(\mathcal{Z}(J))$ in the case of a general division ring D . Here, even if D is a field, an explicit description is unavailable – the problem is too dependent on the nature of the base field. However, one abstract yet meaningful description is available: The K -Nullstellensatz of Laksov [35]. To describe it, we shall introduce the following definition:

Definition 6.2. *Let K be a field and let $p \in K[x_1, \dots, x_m]$ be a homogeneous polynomial. We shall say that p is anisotropic, if $p(a_1, \dots, a_m) = 0$ implies $a_1 = \dots = a_m = 0$ for all $a_1, \dots, a_m \in K$. We shall say that p is quasi-anisotropic, if $p(a_1, \dots, a_m) = 0$ implies $a_m = 0$ for all $a_1, \dots, a_m \in K$. We denote by $Q_m(K)$ the set of all homogeneous quasi-anisotropic polynomials in $K[x_1, \dots, x_m]$.*

Using this terminology and notation, we now define:

Definition 6.3. *Let J be an ideal in $R = K[x_1, \dots, x_n]$. We define the K -radical of J as*

$$\begin{aligned} \sqrt[n]{J} = \{f \in R \mid \text{there exist } m \in \mathbb{N}, f_1, \dots, f_{m-1} \in K[x_1, \dots, x_n], P \in Q_m(K) \\ \text{such that } P(f_1, \dots, f_{m-1}, f) \in J\}. \end{aligned}$$

We then have:

Theorem 6.4 (Laksov's K -Nullstellensatz). *Let J be an ideal in $K[x_1, \dots, x_n]$. Then $\mathcal{I}(\mathcal{Z}(J)) = \sqrt[n]{J}$.*

Next, for a division ring D of finite dimension over its center K , we define for each $f \in D\{X_1, \dots, X_n\}$ the norm function $N(f)$, defined as the composition of f with the norm function $D \rightarrow K$. We then define:

Definition 6.5. *Let J be an ideal in $R = D\{X_1, \dots, X_n\}$. We define the D -radical of J as*

$$\begin{aligned} \sqrt[n]{J} = \{f \in R \mid \text{there exist } m \in \mathbb{N}, f_1, \dots, f_{m-1} \in R, P \in Q_m(K) \\ \text{such that } P(f_1, \dots, f_{m-1}, N(f)) \in J\}. \end{aligned}$$

We then have the following theorem of Bao and Reichstein [16]:

Theorem 6.6 (The general Nullstellensatz of Bao-Reichstein). *Let J be an ideal in $D\{X_1, \dots, X_n\}$. Then $\mathcal{I}(\mathcal{Z}(J)) = \sqrt[n]{J}$.*

The proof strategy for this theorem is similar to that of the proof of Theorem 6.1: Translating the information from D to K , applying the K -Nullstellensatz of Laksov (instead of the Real Nullstellensatz), and then translating the information back over D . The end result of this translation yields Theorem 6.6.

Let us note that Theorem 6.6 only applies in the case where D is of finite central dimension. We do not have a description of $\mathcal{I}(\mathcal{Z}(J))$ in the infinite-dimensional case. In particular, we do not have such a description in the case where D is the Makar-Limanov ring.

The observations made above concerning the structure of the ring $R = D\{X_1, \dots, X_n\}$ lead to several other results in recent papers, which we briefly recall here.

In [5], an application is given to non-commutative inverse Galois theory: The classical inverse Galois problem asks whether every finite group occurs as a Galois group of a field extension of \mathbb{Q} . This is a notoriously difficult problem, which was first asked by Hilbert in the late 19th century, and remains open to this day. However, over other fields the problem is known to have a positive solution, for example over the complex rational function field $\mathbb{C}(x)$, as a consequence of Riemann's Existence Theorem.

In [23], Deschamps and Legrand prove a quaternionic analogue of this result: Let $\mathbb{H}[x]$ be the ring of polynomials in a central variable over \mathbb{H} . The latter is an Ore domain, hence admits a division quotient ring $\mathbb{H}(x)$. The main result of [23] is that every finite group occurs as the Galois group of a division ring extension of $\mathbb{H}(x)$. More generally, Deschamps and Legrand establish connections between the inverse Galois problem over a centrally finite division ring and the inverse Galois problem over its center.

In [5], the main result of [23] is extended to the quotient division ring of $\mathbb{H}\{x\}$, proving that over this ring as well, every finite group occurs as a Galois group. The proof uses the structural observations made above to reduce the problem to the theorem of Deschamps and Legrand.

Regarding the division ring $\mathbb{H}(x)$, let us mention another thematically related recent result: The classical Lüroth's Theorem states that if K is a field and $K(x)$ is the field of rational functions over K , then any intermediate field $K \subset E \subseteq K(x)$ is itself a rational function field over K . A generalization to division rings is given in [45]: If D is a division ring, then any intermediate division ring $D \subset E \subseteq D(x)$ is itself isomorphic to $D(x)$.

Another application of the mentioned isomorphism is a generalization of the Ax-Grothendieck theorem for division rings, given by the author and Son in [54, Theorem 2.3]. The classical theorem states that if $f: C^n \rightarrow C^n$ is an n -dimensional injective polynomial map over an algebraically closed field C , then f is surjective. The generalization to division rings states:

Theorem 6.7 (The Ax-Grothendieck theorem for division rings). *Let D be a centrally finite algebraically closed division ring. Let $f_1, \dots, f_n \in D\{X_1, \dots, X_n\}$. If the map $f = (f_1, \dots, f_n): D^n \rightarrow D^n$ is injective, then f is surjective.*

Proof. If D is a field then the theorem follows by the usual Ax-Grothendieck theorem. Suppose that D is not a field. Then by a theorem of Baer given in [49], D is a quaternion algebra over a real-closed field R . Let us denote its standard basis by $(1, i, j, k)$. We then interpret f as a polynomial map from R^{4n} to R^{4n} , using the mentioned isomorphism above: We view f_1, \dots, f_n as functions from R^{4n} to R^4 by presenting each variable X_ℓ ($1 \leq \ell \leq n$) as $X_\ell = y_{\ell,1} + y_{\ell,2}i + y_{\ell,3}j + y_{\ell,4}k$, where $y_{\ell,1}, y_{\ell,2}, y_{\ell,3}, y_{\ell,4}$ represent variables taking values in R ; For any

$$((a_{11}, a_{12}, a_{13}, a_{14}), \dots, (a_{n1}, a_{n2}, a_{n3}, a_{n4})) \in R^{4n},$$

we write the value of

$$f_\ell(a_{11} + a_{12}i + a_{13}j + a_{14}k, \dots, a_{n1} + a_{n2}i + a_{n3}j + a_{n4}k)$$

as

$$\begin{aligned} & f_{\ell,1}((a_{11}, a_{12}, a_{13}, a_{14}), \dots, (a_{n1}, a_{n2}, a_{n3}, a_{n4})) \\ + & f_{\ell,2}((a_{11}, a_{12}, a_{13}, a_{14}), \dots, (a_{n1}, a_{n2}, a_{n3}, a_{n4}))\mathbf{i} \\ + & f_{\ell,3}((a_{11}, a_{12}, a_{13}, a_{14}), \dots, (a_{n1}, a_{n2}, a_{n3}, a_{n4}))\mathbf{j} \\ + & f_{\ell,4}((a_{11}, a_{12}, a_{13}, a_{14}), \dots, (a_{n1}, a_{n2}, a_{n3}, a_{n4}))\mathbf{k}, \end{aligned}$$

where $f_{\ell,1}, f_{\ell,2}, f_{\ell,3}, f_{\ell,4}$ are functions from R^{4n} to R . Thus the function

$$f: D^n \rightarrow D^n$$

is injective (resp. surjective) if and only if the function

$$f_R = ((f_{1,1}, f_{1,2}, f_{1,3}, f_{1,4}, \dots, f_{n,1}, f_{n,2}, f_{n,3}, f_{n,4}))$$

from R^{4n} to R^{4n} is injective (resp. surjective). Now, each of the functions $f_{\ell,1}, f_{\ell,2}, f_{\ell,3}, f_{\ell,4}$ is itself a **polynomial** in the ring

$$R[y_{1,1}, y_{2,2}, y_{3,3}, y_{4,4}, \dots, y_{n,1}, y_{n,2}, y_{n,3}, y_{n,4}],$$

by [62, Theorem 4.1] or [7, Corollary 4].

Finally, we apply a theorem of Bailynicki-Birula and Rosenlicht [17], which states that the Ax-Grothendieck theorem holds for polynomials over R (Bailynicki-Birula and Rosenlicht phrase their result in the case where R is the field of real numbers, but their theorem holds for any real-closed field, see [15, Theorem 11.4.2]). Thus, if f is injective, so is f_R , hence by the theorem of Bailynicki-Birula and Rosenlicht, f_R is surjective, hence so is f . \square

It is unknown to the author whether the above theorem holds for algebraically closed division rings of infinite central dimension. For additional thematically related results concerning the images of polynomial maps over division rings, see [54].

Another application of the isomorphism repeatedly used in this section applies to a non-commutative variant of Grothendieck's generic freeness lemma, see [55] for details.

7 Open questions for further study

In this section we provide a condensed list of all of the open questions and problems raised throughout this survey, as well as a few additional ones.

1. Is every division ring of the form $(-1, -1)_{2,F}$, where F is a Pythagorean field, necessarily an Amitsur-Small ring?
2. Is there a general characterization of the Amitsur-Small rings in terms of the arithmetic of the ring itself?

3. Are all algebraically closed division rings Amitsur-Small rings? (Equivalently, are all algebraically closed division rings Nullstellensatz rings?) In particular, is the Makar-Limanov ring a Nullstellensatz ring? Are all centrally algebraically closed division rings Amitsur-Small rings?
4. What can be said of the contraction of a completely prime, not necessarily maximal, left ideal in $D[x_1, \dots, x_n]$ to $D[x_1, \dots, x_k]$ with $k < n$? We note that such a contraction is not necessarily completely prime – this is another consequence of Theorem 3.13.
5. In the construction of Makar-Limanov in [46] of a division ring over which every non-constant polynomial function admits a zero, the constructed ring is of characteristic 0. A question raised in talks of Makar-Limanov is whether there exists a division ring of positive characteristic which satisfies this property. To the best of the author's knowledge, this problem is still unsolved.
6. For which division rings does the analogue of Theorem 4.2 apply?
7. Does Theorem 4.1 apply when replacing \mathbb{H} with algebraically closed division rings of infinite central dimension? In particular, does it hold for the Makar-Limanov ring? If it does not, that would mean that a richer geometry over such rings is accessible.
8. Does Aryapoor's description of the radical hold if one replaces \mathbb{H} with an arbitrary division ring D ? For any algebraically closed division ring? For the Makar-Limanov ring? For Amitsur-Small rings?
9. More generally, if J is a left ideal in an arbitrary ring R (not necessarily a polynomial ring), is there an explicit description of \sqrt{J} ?
10. Effectiveness of the Nullstellensatz: Can the integer n in Aryapoor's explicit Nullstellensatz be bounded, for all polynomials in the ideal J ?
11. Can the Nullstellensatz of Bao and Reichstein be extended in some form to division rings of infinite central dimension?
12. Does the Ax-Grothendieck theorem over division rings holds in the infinite central case? Does it hold for the Makar-Limanov ring?

Acknowledgment

The author wishes to express his sincere thanks to the anonymous reviewer for many valuable comments that improved the final version of this manuscript.

References

- [1] G. Alon, A. Behajaina, and E. Paron, *The Combinatorial Nullstellensatz, Chevalley-Waring Theorem and weak Finitesatz in skew polynomial rings*, preprint (2026).

- [2] G. Alon, A. Chapman, and E. Paran, *On the geometry of zero sets of central quaternionic polynomials II*, Israel J. Math. (2025).
- [3] N. Alon and Z. Füredi, *Coverings of the cube by affine hyperplanes*, European J. Combin. **14** (1993), no. 2, 79–83.
- [4] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.
- [5] G. Alon, F. Legrand, and E. Paran, *Galois groups over rational function fields over skew fields*, C. R. Math. Acad. Sci. Paris **358** (2020), no. 7, 785–790.
- [6] N. Alon, M. B. Nathanson, and I. Ruzsa, *Adding Distinct Congruence Classes Modulo a Prime*, Amer. Math. Monthly **102** (1995), no. 3, 250–255.
- [7] G. Alon and E. Paran, *A quaternionic Nullstellensatz*, J. Pure Appl. Algebra **225** (2021), no. 4.
- [8] G. Alon and E. Paran, *A central quaternionic Nullstellensatz*, J. Algebra **574** (2021), 252–261.
- [9] G. Alon and E. Paran, *Completely prime one-sided ideals in skew polynomial rings*, Glasgow Math. J. (2021).
- [10] G. Alon and E. Paran, *On the geometry of zero sets of central quaternionic polynomials*, J. Algebra **659** (2024), 780–788.
- [11] M. Aryapoor, *Explicit Hilbert’s Nullstellensatz over the division ring of quaternions*, J. Algebra **657** (2024), 26–36.
- [12] M. Aryapoor, *The Central Nullstellensatz over Centrally Algebraically Closed Division Rings*, J. Algebra (2026).
- [13] S. Amitsur and L. W. Small, *Polynomials over division rings*, Israel J. Math. **31** (1978), 353–358.
- [14] A. Kaučikas and R. Wisbauer, *Noncommutative Hilbert rings*, J. Algebra Appl. **3** (2004), no. 4, 437–443.
- [15] J. Bochnak, M. Coste, and M. F. Roy, *Real Algebraic Geometry*, Springer, 2013.
- [16] Z. Bao and Z. Reichstein, *A non-commutative Nullstellensatz*, J. Algebra Appl. **22** (2023), no. 4.
- [17] A. Bailynicki-Birula and M. Rosenlicht, *Injective morphisms of real algebraic varieties*, Proc. Amer. Math. Soc. **13** (1962), no. 2, 200–203.
- [18] J. Cimpic̆, *Matrix versions of Real and Quaternionic Nullstellensatze*, J. Algebra **610** (2022), 752–772.
- [19] J. Cimpic̆, *Prime and semiprime submodules of R^n and a related Nullstellensatz for $M_n(R)$* , J. Algebra Appl. **22** (2022), no. 11.

- [20] J. Cimpic̆, *Parallels between quaternionic and matrix Nullstellensätze*, J. Algebra **682** (2025), 92–108.
- [21] A. Chapman, I. Levin, and M. Zaninelli, *Cyclic Division Algebras of Odd Prime Degree are never Amitsur-Small*, preprint, <https://arxiv.org/abs/2508.07451> (2025).
- [22] A. Chapman and E. Paran, *Amitsur-Small rings*, J. Algebra **679** (2025), 86–95.
- [23] B. Deschamps and F. Legrand, *Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale*, J. Pure Appl. Algebra **224** (2020), no. 5.
- [24] I. Niven and S. Eilenberg, *The “fundamental theorem of algebra” for quaternions*, Bull. Amer. Math. Soc. **50** (1944), 246–248.
- [25] P. Erdős, *Some problems in number theory*, in: Computers in Number Theory, 1971, pp. 405–414.
- [26] B. Gordon and T. S. Motzkin, *On the Zeros of polynomials over division rings*, Trans. Amer. Math. Soc. **116** (1965), 218–226.
- [27] G. Gentili and C. Stoppato, *Zeros of regular functions and polynomials of a quaternionic variable*, Michigan Math. J. **56** (2008), no. 3, 655–667.
- [28] G. Gentili, C. Stoppato, and D. C. Struppa, *Regular functions of a quaternionic variable*, Springer, Heidelberg, 2013.
- [29] A. Gori, G. Sarfatti, and F. Vlacci, *Zero sets and Nullstellensatz type theorems for slice regular quaternionic polynomials*, Linear Algebra Appl. **685** (2024), 162–181.
- [30] A. Gori, G. Sarfatti, and F. Vlacci, *A strong version of the Hilbert Nullstellensatz for slice regular polynomials in several quaternionic variables*, J. Algebra (2025).
- [31] J. C. Robson and L. W. Small, *Liberal Extensions*, Proc. London Math. Soc. (3) **42** (1981), no. 1, 87–103.
- [32] G. Károlyi, *A compactness argument in the additive theory and the polynomial method*, Discrete Math. **302** (2005), no. 1–3, 124–144.
- [33] P. Kolesnikov, *The Makar-Limanov Algebraically Closed Skew Field*, Algebra Logic **39** (2000), no. 6, 378–395.
- [34] J. Kollár, *Sharp Effective Nullstellensatz*, J. Amer. Math. Soc. **1** (1988), no. 4, 963–975.
- [35] D. Laksov, *Radicals and Hilbert Nullstellensatz for not necessarily algebraically closed fields*, Enseign. Math. **33** (1987), no. 3–4, 323–338.
- [36] T. Y. Lam, *A general theory of Vandermonde matrices*, Exposition. Math. **4** (1986), no. 3, 193–215.
- [37] T. Y. Lam, *A first course in noncommutative rings*, Springer-Verlag, 1991.

- [38] S. Lang, *Algebra*, 3rd ed., Springer, 2005.
- [39] L. H. Rowen, *Left ideals of polynomial rings in several indeterminates*, Comm. Algebra **23** (1995), no. 6, 2263–2279.
- [40] T. Y. Lam, A. Leroy, and A. Ozturk, *Wedderburn polynomials over division rings. II*, in: Noncommutative rings, group rings, diagram algebras and their applications, Contemp. Math., vol. 456, Amer. Math. Soc., Providence, RI, 2008, pp. 73–98.
- [41] T. Y. Lam and A. Leroy, *Wedderburn polynomials over division rings. I*, J. Pure Appl. Algebra **186** (2004), no. 1, 43–76.
- [42] T. Y. Lam and A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), no. 2, 308–336.
- [43] A. Leroy and H. Merdach, *Polynomial evaluations in noncommutative settings, a survey*, J. Algebra Appl. (2026).
- [44] A. Leroy and M. Nasernejad, *Iterated Ore polynomial maps*, J. Algebra Appl. **24** (2025), no. 3.
- [45] F. Legrand and E. Paran, *Lüroth’s and Igusa’s theorems over division rings*, Osaka J. Math. **61** (2023), 261–274.
- [46] L. Makar-Limanov, *Algebraically closed skew fields*, J. Algebra **93** (1985), no. 1, 117–135.
- [47] M. Michalek, *A Short Proof of Combinatorial Nullstellensatz*, Amer. Math. Monthly **117** (2010), no. 9, 821–823.
- [48] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings*, Amer. Math. Soc., 2001.
- [49] I. Niven, *Equations in Quaternions*, Amer. Math. Monthly **48** (1941), 654–661.
- [50] O. Ore, *Theory of Non-Commutative Polynomials*, Ann. of Math. (2) **34** (1933), no. 3, 480–508.
- [51] E. Paran, *Combinatorial Nullstellensatz over division rings*, J. Algebraic Combin. **58** (2023), 895–911.
- [52] E. Paran, *On a problem of Amitsur and Small*, preprint, <https://arxiv.org/abs/2412.06230> (2024).
- [53] C. Procesi, *Non commutative Jacobson-rings*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **21** (1967), no. 2, 281–290.
- [54] E. Paran and T. N. Son, *Images of polynomial maps and the Ax-Grothendieck theorem over algebraically closed division rings*, preprint (2025).
- [55] E. Paran and T. N. Vo, *Generic freeness of modules over non-commutative domains*, J. Algebra **641** (2024), 735–753.

-
- [56] E. Paran and T. N. Vo, *Noether's Normalization in skew polynomial rings*, J. Pure Appl. Algebra (2025).
 - [57] R. Resco, *A Reduction Theorem for the Primitivity of Tensor Products*, Math. Z. **170** (1980), 1432–1823.
 - [58] G. Riccardo and A. Perotti, *Slice regular functions in several variables*, Math. Z. **302** (2022), no. 1, 295–351.
 - [59] M. L. Reyes, *A one-sided prime ideal principle for noncommutative rings*, J. Algebra Appl. **9** (2010), no. 6, 877–919.
 - [60] J. A. D. Silva and Y. O. Hamidoune, *Cyclic Spaces for Grassmann Derivatives and Additive Theory*, Bull. London Math. Soc. **26** (1994), no. 2, 140–146.
 - [61] E. D. Sontag, *On finitely accessible and finitely observable rings*, J. Pure Appl. Algebra **8** (1976), no. 1, 97–104.
 - [62] D. M. Wilczynski, *On the fundamental theorem of algebra for polynomial equations over real composition algebras*, J. Pure Appl. Algebra **218** (2014), no. 5, 1195–1205.