A central quaternionic Nullstellensatz

Gil Alon and Elad Paran

November 23, 2020

Abstract

Let $I$ be a proper left ideal in the ring $\mathbb{H}[x_1, \ldots, x_n]$ of polynomials in $n$ central variables over the quaternion algebra $\mathbb{H}$. Then there exists a point $a = (a_1, \ldots, a_n) \in \mathbb{H}^n$ with $a_i a_j = a_j a_i$ for all $i, j$, such that every polynomial in $I$ vanishes at $a$. This generalizes a theorem of Jacobson, who proved the case $n = 1$. Moreover, a polynomial $f \in \mathbb{H}[x_1, \ldots, x_n]$ vanishes at all common zeroes of polynomials in $I$ if and only if $f$ belongs to the intersection of all completely prime left ideals that contain $I$ – a notion introduced by Reyes in 2010.

1 Introduction

Let $R = \mathbb{C}[x_1, \ldots, x_n]$ be the ring of complex polynomials in $n$ variables, and let $I$ be a proper ideal in $R$. By Hilbert’s Nullstellensatz, there exists a point $a = (a_1, \ldots, a_n) \in \mathbb{C}^n$ such that all elements of $I$ vanish at $a$.\footnote{This is the Bezout form of the Nullstellensatz, also known as the “weak” Nullstellensatz. We discuss the “strong” Nullstellensatz below.} In the case $n = 1$, this reduces to the statement that every non-constant polynomial in one variable over $\mathbb{C}$ admits a zero – the fundamental theorem of algebra. Thus the Nullstellensatz may be regarded as a higher dimensional generalization of Gauss’s celebrated theorem.

Consider now the ring $\mathbb{H}[x]$ of polynomials over Hamilton’s quaternion algebra$^2$ $\mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R}$, in a central$^3$ variable $x$. In [Niv41], Niven gives a quaternionic “fundamental theorem of algebra”: Every non-constant polynomial in $\mathbb{H}[x]$ admits a zero. Niven attributes this result to Jacobson.

$^*$Corresponding Author.

$^2$We denote the standard generators of $\mathbb{H}$ by $i, j, k$, as opposed to the letters $i, j, k$ which we use for indices.

$^3$That is, where the variable $x$ commutes with the coefficients.
It is natural to ask whether Jacobson’s theorem extends to higher dimension – is there a “quaternionic Nullstellensatz”? In this work we prove such a theorem. Let $R = \mathbb{H}[x_1, \ldots, x_n]$ be the ring of polynomials in $n$ central variables over $\mathbb{H}$, and let $\mathbb{H}_c^n$ denote the set of points $(a_1, \ldots, a_n) \in \mathbb{H}^n$ satisfying $a_ia_j = a_ja_i$ for all $i \neq j$. We observe (see Proposition 2.2 below) that every point $a \in \mathbb{H}_c^n$ yields a well-defined substitution map $p \mapsto p(a)$ from $R$ to $\mathbb{H}$. We show that the maximal left ideals in $R$ are precisely those generated by $x_1 - a_1, \ldots, x_n - a_n$ for some $a = (a_1, \ldots, a_n) \in \mathbb{H}_c^n$ – i.e. the ideal of polynomials in $R$ which vanish at $a$. As a consequence, we obtain the following “weak Nullstellensatz” for $\mathbb{H}$:

**Theorem 1.1** (Weak Nullstellensatz). Let $I$ be a proper left ideal in $R$. Then there exists a point $a = (a_1, \ldots, a_n) \in \mathbb{H}_c^n$ such that all polynomials in $I$ vanish at $a$.

The ring $\mathbb{H}[x]$ is a left principal ideal domain [Ore33, p. 483]. In particular, the set of polynomials vanishing at a point $a \in \mathbb{H}$ is a left ideal in $\mathbb{H}[x]$. Thus the case $n = 1$ in Theorem 1.1 above is Jacobson’s theorem in [Niv41].

Let $I$ be a proper ideal in $\mathbb{C}[x_1, \ldots, x_n]$. The “strong” Nullstellensatz asserts that a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes at all common zeroes of $I$ if and only if $f$ belongs the radical $\sqrt{I}$ of $I$ – the intersection of all prime ideals that contain $I$. We prove an analogous result for $\mathbb{H}[x_1, \ldots, x_n]$:

**Theorem 1.2** (Strong Nullstellensatz). Let $I$ be a proper left ideal in $R$. A polynomial $f \in R$ vanishes at all common zeroes of polynomials in $I$ in $\mathbb{H}_c^n$ if and only if $f$ belongs to the intersection of all completely prime left ideals that contain $I$.

Here a left ideal $I$ in a ring $R$ is called **completely prime** if given $a, b \in R$ with $ab \in I$ and $ib \subseteq I$, it follows that $a \in I$ or $b \in I$. This notion was introduced by Reyes in 2010, who demonstrated in [Rey10] and [Rey12] that, from certain aspects, completely prime one-sided ideals in noncommutative rings are a good analogue of prime ideals in commutative rings. Theorem 1.2 above gives further evidence of that.

Finally, we note that one may ask for a Nullstellensatz for quaternionic polynomials in **non-central** variables, but here already in dimension 1 the “fundamental theorem” fails – for example the polynomial function $X \mapsto Xi + iX + j$ admits no zeros in $\mathbb{H}$. Nevertheless, there is a form of Nullstellensatz for such quaternionic polynomial functions, closer in nature to the Real Nullstellensatz, see [AP21].

---

4 In commutative rings, this definition obviously coincides with the usual definition of a prime ideal.
Thus we express $M \rightarrow p$ tuples in $HR$. Let $a = (a_1, a_2, \ldots, a_n) \in \mathbb{H}^n$, and suppose that $a_ia_j \neq a_ja_i$ for some $1 \leq i, j \leq n$. Then $I_a = R$.

Proof. One directly verifies that

$$(x_i - a_i)(x_j - a_j) - (x_j - a_j)(x_i - a_i) = a_i a_j - a_j a_i$$

hence $a_i a_j - a_j a_i$ is a non-zero element of $H$ in $I_a$, therefore $I_a = R$.

Let $\mathbb{H}_c^n$ denote the set of points $(a_1, \ldots, a_n) \in \mathbb{H}^n$ satisfying the condition $a_ia_j = a_ja_i$ for all $i \neq j$. For a point $a = (a_1, \ldots, a_n) \in \mathbb{H}_c^n$ and a monomial $M = bx_1^{k_1} \cdots x_n^{k_n}$ with $b \in H$, we define the substitution of $a$ in $M$ as $M(a) = ba_1^{k_1} \cdots a_n^{k_n}$. We additively expand this to a substitution map $p \mapsto p(a)$ from $R$ to $\mathbb{H}$. We say that $p \in R$ vanishes at $a \in \mathbb{H}^n$ if $p(a) = 0$. We note that the substitution map is generally not a homomorphism.

Proposition 2.2. Let $a = (a_1, \ldots, a_n) \in \mathbb{H}_c^n$. Then $I_a$ is a proper left ideal in $R$, and a polynomial $p \in R$ vanishes at $a$ if and only if $p \in I$. Moreover, $I_a$ is a maximal left ideal in $R$.

Proof. One directly checks that for any monomial $M = bx_1^{k_1} \cdots x_n^{k_n}$, the polynomial $M(x_i - a_i)$ vanishes at $a$ for any $i$. It follows that any polynomial in $I_a$ vanishes at $a$. In particular, $1 \notin I_a$.

Given a polynomial $p \in R$, we may perform “division with remainder”: Repeatedly rewrite each occurrence of $x_i$ as $(x_i - a_i) + a_i$ and open brackets, to express $p$ in the form $q + b$ with $q \in I_a$ and $b \in \mathbb{H}$. Then $b = p(a) - q(a) = p(a)$. Thus $p(a) = 0$ if and only if $p \in I_a$.

We note that any point $(a_1, \ldots, a_n) \in \mathbb{H}_c^n$ lying outside of $\mathbb{R}^n$ generates a field $\mathbb{R}(a_1, \ldots, a_n)$ which is necessarily isomorphic to $\mathbb{C}$. Thus the space $\mathbb{H}_c^n$ is formed by “patching” uncountably many copies of $\mathbb{C}^n$, intersecting at $\mathbb{R}^n$. Note also that in light of Lemma 2.1, one cannot define substitution at tuples in $\mathbb{H}^n$ lying outside of $\mathbb{H}_c^n$ in any meaningful way.

Let $R' = \mathbb{R}[x_1, \ldots, x_n]$ be the center of $R$.

---

5The choice to express monomials with $x_1$ to the left and $x_n$ to the right is arbitrary, but since the $a_i$ commute, this choice does not matter for substitution.

6We note that for $n = 1$, substitution satisfies the following product formula: $(fg)(a) = f(g(a)ag(a)^{-1})(g(a))$ whenever $g(a) \neq 0$, see [LL88, S2].
Lemma 2.3. The extension $R/R'$ is integral. That is, every $f \in R$ satisfies an equality of the form $f^n + g_{n-1}f^{n-1} + \ldots + g_1f + g_0 = 0$ with $g_0, \ldots, g_{n-1} \in R'$.

Proof. Since $R'$ is commutative, $R'$ is a finitely-accessible ring [Son76, Definition 1.4], hence by [Son76, Theorem 1.3], the extension $R/R'$ is integral. \(\square\)

The proof of the following “going-down” lemma is essentially the same as for finite extensions of commutative domains.

Lemma 2.4. Let $B/A$ be an integral extension of rings, where $A$ is a domain contained in the center of $B$. If $M$ is a maximal left ideal in $B$, then $M \cap A$ is a maximal ideal in $A$.

Proof. Since $M$ is maximal, for any $a \in A \setminus (M \cap A)$ we have $M + Ba = B$, so there exist $m \in M, b \in B$ such that $ab + m = 1$. Since $B/A$ is integral, there exist elements $h_0, \ldots, h_{n-1} \in A$ such that $b^n + \sum_{i=0}^{n-1} h_i b^i = 0$. Since $a \in A$, this implies that $(ab)^n + \sum_{i=0}^{n-1} a^{n-i} h_i(ab)^i = 0$. That is, $(1 - m)^n + \sum_{i=0}^{n-1} a^{n-i} h_i(1 - m)^i = 0$, which implies that $1 + \sum_{i=0}^{n-1} a^{n-i} h_i \in M \cap A$. But this implies that $a$ is invertible modulo $M \cap A$. Thus $A/(M \cap A)$ is a field. \(\square\)

Lemma 2.5. The left ideal $I$ generated by $x_1^2 + 1, x_2, \ldots, x_n$ in $R$ does not contain $x_1 + i$.

Proof. Let $\varphi : R \rightarrow \mathbb{H}[x_1]$ be the $\mathbb{H}[x_1]$-preserving epimorphism given by $\varphi(x_2) = \varphi(x_3) = \ldots = \varphi(x_n) = 0$. Suppose $x_1 + i \in I$, and write $x_1 + i = p(x_1^2 + 1) + p_2 x_2 + \ldots + p_n x_n$. Then $x_1 + i = \varphi(x_1 + i) = \varphi(p)(x_1^2 + 1) = \varphi(p)(x_1 + i)(x_1 + i)$, hence $1 = \varphi(p)(x_1 + i)$. Thus $x_1 + i$ is invertible in $\mathbb{H}[x_1]$, a contradiction. \(\square\)

Proposition 2.6. The maximal left ideals in $R$ are those of the form $I_a$ for $a \in \mathbb{H}^n_c$.

Proof. One direction of the claim is given by Proposition 2.2. For the converse, let $M$ be a maximal left ideal in $R$ and let $P = M \cap R'$. The extension $R/R'$ is integral by Lemma 2.3, hence by Lemma 2.4, $P$ is a maximal ideal in $R'$. Thus $F := R'/P$ is a finite field extension of $\mathbb{R}$, and $P$ is the kernel of the projection homomorphism $R' \rightarrow F$.

If $F \cong \mathbb{R}$, then $P$ is generated by $x_1 - a_1, \ldots, x_n - a_n$ for some $a_1, \ldots, a_n \in \mathbb{R}$. Then $(a_1, \ldots, a_n) \in \mathbb{H}^n_c$, thus by Proposition 2.2, the elements $x_1 - a_1, \ldots, x_n - a_n \in P \subseteq M$ generate a maximal left ideal $I$ in $R$, hence $M = I$.

If $F \cong \mathbb{C}$, then $P$ is the set of polynomials in $R'$ vanishing at a complex point $(c_1 + d_1 i, \ldots, c_n + d_n i)$. We may make the real change\(^7\) of variables

\(^7\)That is, we put $y_i = x_i - c_i$. Clearly, $\mathbb{H}[x_1, \ldots, x_n] = \mathbb{H}[y_1, \ldots, y_n]$. 

4
$x_i \rightarrow x_i - c_i$ to 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, so we assume, without loss of generality that $d_1 = 1$. Finally, for any $i > 1$ with $d_i = 1$, replace $x_i$ with $x_i - x_1$ to assume that $d_i = 0$. Thus $P$ is the set of polynomials vanishing at $(i, 0, \ldots, 0)$, hence $P = \langle x_i^2 + 1, x_2, \ldots, x_n \rangle$. By Lemma 2.5, $x_i^2 + 1, x_2, \ldots, x_n$ do not generate a maximal left ideal in $R$: Indeed, the left ideal generated by $x_1 + i, x_2, \ldots, x_n$ is larger. Thus $M$ must contain a non-zero element $h \in R$ which is not generated by $x_1^2 + 1, x_2, \ldots, x_n$. By replacing in $h$ every occurrence of $x_2, \ldots, x_n$ 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 $c = 1$. By Proposition 2.2, the left ideal $I$ generated by $x_1 - d, x_2, \ldots, x_n$ is maximal in $R$, hence $M = I$. \hfill \Box

Theorem 1.1 is now an immediate consequence of Proposition 2.6.

We note that if one initially defines “right substitution” by $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} b \mapsto x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} b$, then one obtains symmetric results to those given here, where left ideals are replaced by right ideals.

One may ask if Theorem 1.1 generalizes to other division algebras. However, $\mathbb{H}$ is essentially the only noncommutative division algebra for which Jacobson’s theorem in [Niv41] holds: A theorem of Baer asserts that if $D$ is a noncommutative division algebra with center $C$, such that every polynomial in $D[x]$ admits a root in $D$, then $C$ is a real-closed field and $D$ is the quaternion algebra over $C$ (see the introduction of [Niv41]).

# 3 A going-up theorem

For this section, let $B$ be a right Ore domain. That is, for each nonzero $x, y \in B$ there exist $r, s \in B$ such that $xr = ys \neq 0$. Then [GW04, Theorem 6.8] $B$ admits a classical (skew) field of fractions, whose elements are of the form $ab^{-1}$ with $a, b \in B, b \neq 0$. Let $A$ be a subring of the center of $B$. Suppose $B/A$ is an integral extension: Every element $0 \neq b \in B$ satisfies an equation of the form $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$ with $a_0, \ldots, a_{n-1} \in A$.

In this section we prove a “going-up” theorem for the extension $B/A$, connecting completely prime ideals in $B$ and prime ideals in $A$.

---

8Here we put $y_i = x_i - x_1$ or $y_i = x_i$ for each $i$, according to our construction. We have, as before, $\mathbb{H}[x_1, \ldots, x_n] = \mathbb{H}[y_1, \ldots, y_n]$, and any ideal of the form $\langle y_1 - b_1, \ldots, y_n - b_n \rangle$ for some $(b_1, \ldots, b_n) \in \mathbb{H}_C^n$ is also of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $(a_1, \ldots, a_n) \in \mathbb{H}_C^n$.  

5
Given a multiplicative subgroup $S$ of $A$, the localization $B_S = \{bs^{-1}|b \in B, s \in S\}$ is clearly a subring of the fraction field of $B$.

**Lemma 3.1.** Let $S$ be a multiplicative subgroup of $A$ and $P$ a completely prime left ideal in $B_S$. Then $P \cap B$ is a completely prime left ideal in $B$.

**Proof.** Let $a, b \in B$ be such that $ab \in P \cap B$, $(P \cap B)b \subseteq (P \cap B)$. Let us prove that $Pb \subseteq P$: Given an element $ps^{-1} \in P$ with $p \in B, s \in S$, we have $s(ps^{-1}) = p \in P \cap B$, hence $pb \in P \cap B$, therefore $(ps^{-1})b = s^{-1}pb \in P$. Thus $Pb \subseteq P$, hence $a \in P \cap B$ or $b \in P \cap B$. $\square$

For a left ideal $I \subseteq B$, we denote by $I_c$ the contraction $I \cap A$ of $I$ in $A$. We have the following “going-up” theorem:

**Theorem 3.2.** Let $Q$ be a completely prime left ideal in $B$, let $q = Q_c = A \cap Q$ and let $p$ be a prime ideal in $A$ with $q \subseteq p$. Then there exists a completely prime left ideal $P$ in $B$ such that $P_c = p$ and $Q \subseteq P$.

**Proof.** Put $S = A \setminus p$. Then $S$ is a multiplicative subset of $A$, and $A_S = A_p$ is a local ring, which we view as a subring of $B_S$. We have $S \cap Q = \emptyset$ hence $Q_S$ is a proper ideal of $B_S$. Let $M$ be a maximal left ideal in $B_S$ containing $Q_S$. Since $B/A$ is integral, it is straightforward to check that $B_S/A_S$ is also integral. By Lemma 2.4 (with $(A_S, B_S)$ instead of $(A, B)$) we get that $M \cap A_S$ is a maximal ideal in $A_S$, hence $M \cap A_S$ is the unique maximal ideal $p_S$ of $A_S$. By [Rey10, Corollary 2.10], $M$ is a completely prime left ideal, hence by Lemma 3.1, $P = M \cap B$ is a completely prime left ideal in $B$, and we have $P_c = P \cap A \subseteq M \cap A \subseteq (M \cap A_S) \cap A = p_S \cap A = p$. On the other hand, $p \subseteq p_S \subseteq M$ and $p \subseteq A \subseteq B$, hence $p \subseteq M \cap B = P$. Thus $P_c = p$, and since $Q \subseteq M$ we have $Q \subseteq P$. $\square$
4 Strong Nullstellensatz

Let \( R = \mathbb{H}[x_1, \ldots, x_n] \) and \( R' = \mathbb{R}[x_1, \ldots, x_n] \). For a quaternion \( z = a + ib + jc + kd \) with \( a, b, c, d \in \mathbb{R} \), let \( \overline{z} = a - ib - jc - kd \) denote its quaternion conjugate. Then \( \overline{z} + z, z\overline{z} = \overline{zz} \in \mathbb{R} \) for all \( z \in \mathbb{H} \). For any \( f \in R \), let \( \overline{f} \) be the polynomial obtained from \( f \) by conjugating all its coefficients. Then \( f + \overline{f}, f\overline{f} = \overline{ff} \in R' \) for all \( f \in R \).

**Proposition 4.1.** The ring \( R \) is a left and right Ore domain. That is, for each \( a, b \in R \) with \( a, b \neq 0 \) there exists a non-zero element in \( R \) which is divisible from the right by both \( a \) and \( b \), and a non-zero element which is divisible from the left by \( a \) and \( b \).

**Proof.** We have \( a\overline{a} = bb\overline{a} \).

Proposition 4.1 will allow us to apply Theorem 3.2 in the proof of Proposition 4.4 below.

**Lemma 4.2.** Let \( P \) be a two-sided ideal \( P \) of \( R \), and let \( p = P \cap R' \). Then the ideal \( \mathbb{H}p = \mathbb{H}P = p + pi + pj + pk \) is \( P \).

**Proof.** The inclusion \( \mathbb{H}p \subseteq P \) is clear. For the opposite inclusion, let \( u = a + ib + jc + kd \in P \), with \( a, b, c, d \in R' \). Direct computation gives:

\[
\begin{align*}
a &= \frac{1}{4}(u - iui - juj - kuk) \\
b &= \frac{1}{4}(juk - ui - iu - kuj) \\
c &= \frac{1}{4}(ku - uj - ju - iuk) \\
d &= \frac{1}{4}(iu - jk - ku - jui)
\end{align*}
\]

hence \( a, b, c, d \in p \) and \( u \in \mathbb{H}p = \mathbb{H}P \).

The following “incomparability lemma” is key to the proof of Theorem 1.2.

**Lemma 4.3.** If \( P \subseteq Q \) are left ideals in \( R \) such that \( P \) is completely prime and \( Q \cap R' = P \cap R' \), then \( Q = P \).

**Proof.** Let \( p = P \cap R' \). For any \( a \in Q \) we have \( a\overline{a} = \overline{aa} \in Q \cap R' = p \subseteq P \).

Thus, for any \( a \in Q \) and \( b \in P \), we have

\[
\overline{ab} + \overline{ba} = (\overline{a} + \overline{b})(a + b) - \overline{aa} - \overline{bb} \in P
\]
Since $P$ is a left ideal, we conclude that $\bar{ba} \in P$, so $\bar{P}Q \subseteq P$. Conjugating, we get $\bar{QP} \subseteq \bar{P}$. Since $\bar{P}$ is evidently a right ideal in $R$, we have $\bar{QP}R \subseteq \bar{P}$, where $PR$ is the right $R$-ideal generated by $P$. Note that $PR$ is a two-sided ideal. By Lemma 4.2, we have $PR = \mathbb{H}p'$ for some ideal $p' \supseteq p$ of $R'$. In particular, we have $Qp' \subseteq \bar{P}$. Conjugating again, keeping in mind that $p'$ is invariant under conjugation, we get that $p'Q \subseteq P$. We now consider two cases:

- **Case 1:** $p' = p$. Let $a \in p' \setminus p$. For any $q \in Q$, we have $aq = qa \in P$, and $Pa = aP \subseteq P$, since $a$ is in the center $R'$ of $R$. Since $P$ is completely prime, we have $a \in P$ or $q \in P$, but per our choice, $a \notin P$, so $q \in P$. Thus $Q \subseteq P$.

- **Case 2:** $p' = p$. Then $PR = \mathbb{H}p \subseteq P$, so $P$ is a two-sided ideal. Let $a \in Q$, then as before, $\bar{a}a \in P$. We have $Pa \subseteq P$, and since $P$ is completely prime, we have $a \in P$ or $\bar{a} \in P$. If $\bar{a} \in P$ then $\bar{a} \in Q$, so $a + \bar{a} \in Q \cap R' = p$, and in particular, $a + \bar{a} \in P$, hence $a \in P$. So either way, we have $a \in P$. Thus $Q \subseteq P$.

We can now show that $R$ satisfies the following “Jacobson property”:

**Proposition 4.4.** Let $P$ be a completely prime left ideal. Then $P$ is an intersection of maximal left ideals in $R$.

**Proof.** Put $p = P \cap R'$. Since $P$ is completely prime, $p$ is clearly a prime ideal in $R'$. Since $R'$ is a Jacobson ring [Eis04, Theorem 4.19], we have $p = \bigcap_{m \subseteq \mathfrak{m}} m$, where the intersection is taken over all maximal ideals in $R'$ that contain $p$. By Theorem 3.2 (with $B = R, A = R'$), for each such $\mathfrak{m}$ there exists a maximal left ideal $M$ in $R$ such that $P \subseteq M$ and $M \cap R' = \mathfrak{m}$. Let $Q$ be the intersection of all such $M$. Then $Q$ is a left ideal in $B$ with $Q \cap R' = P \cap R' = p$, hence by Lemma 4.3 we have $P = Q$.

**Definition 4.5.** Let $A$ be an associative ring with unity. For a left ideal $I$ in $A$, we define the left radical $\sqrt{I}$ of $I$ as the intersection of all completely prime left ideals that contain $I$.

Clearly, if $A$ is a commutative ring and $I$ is an ideal in $A$, then the left radical of $I$ is the classical radical of $I$.

Given a left ideal $I$ in $R$, let $Z(I)$ be the set of points in $\mathbb{H}^n$ at which all polynomials in $I$ vanish. Given a set of points $Z \subseteq \mathbb{H}^n$, let $I(Z)$ be the left ideal of polynomials that vanish at every point of $Z$. We can now prove the strong Nullstellensatz:
Theorem 4.6. Let $I$ be a left ideal in $R$. Then $I(Z(I)) = \sqrt{I}$.

Proof. By Proposition 2.6, the maximal left ideals that contain $I$ are those of the form $I_a$, with every $f \in I$ vanishing at $a = (a_1, \ldots, a_n) \in \mathbb{H}^n$. Thus $I(Z(I))$ is the intersection of all maximal left ideals that contain $I$, and every such maximal ideal is completely prime, by [Rey10, Corollary 2.10]. By Proposition 4.4, every completely prime left ideal that contains $I$ is an intersection of maximal left ideals that contain $I$. Thus $I(Z(I)) = \sqrt{I}$. \qed

We note that the classical strong Nullstellensatz for $\mathbb{C}[x_1, \ldots, x_n]$ can be easily deduced as an immediate consequence of the weak Nullstellensatz, using the famous Rabinowitsch trick (see [Lan05, p. 380, proof of Theorem 1.5]). Such a proof does not seem possible for $\mathbb{H}[x_1, \ldots, x_n]$, since substitution is not a homomorphism. Therefore we took a longer route of proof, as presented above.

The definition of the left radical $\sqrt{I}$ given here is an abstract one, a generalization of the abstract definition of the classical radical. One may ask if the left radical $\sqrt{I}$ of an ideal $I$ in $\mathbb{H}[x_1, \ldots, x_n]$ can also be described explicitly as the set of roots of elements of $I$, as in the commutative case. Below we give an example showing that this is not the case. We shall first need the following lemma:

Lemma 4.7. Let $R = \mathbb{H}[x]$ and let $p \in R$ be a monic polynomial. The ideal $Rp$ is completely prime if and only if $p = x - a$ for some $a \in \mathbb{H}$.

Proof. First suppose that $p = x - a$ for $a \in \mathbb{H}$, and that $f, g \in R$ satisfy $fg \in Rp$ and $Rpg \subseteq Rp$. Then $(fg)(a) = 0$ and $(pg)(a) = 0$. If $g \notin Rp$, then $g(a) \neq 0$ and by [LL88, Theorem 2.8] we have $f(a^g) = 0$ and $p(a^g) = 0$, where $a^g = g(a)g(a)^{-1}$. The equality $p(a^g) = 0$ thus implies $a^g = a$, hence we have $f(a) = 0$, hence $f \in Rp$. Thus $R(x - a)$ is completely prime.

Conversely, suppose $Rp$ is completely prime, but $p$ is composite. By Jacobson’s theorem in [Niv41], every polynomial in $\mathbb{H}[x]$ factors into a product of linear terms. Thus we may write $p = (x - a)f$ with $f$ monic of positive degree. Put $g = (x - \bar{a})(x - a) = (x - a)(x - \bar{a}) \in \mathbb{R}[x]$. Then $(x - a)p = gf \in Rp$, and $Rpg \subseteq Rp$ since $g$ belongs to the center $\mathbb{R}[x]$ of $\mathbb{H}[x]$. Since $Rp$ is completely prime, we have $f \in Rp$ or $g \in Rp$. The first option cannot hold since $\deg(f) < \deg(p)$, and the second option implies that $\deg(p) = \deg(g) = 2$ and $f = x - \bar{a}$. We have $(x - a)(x - \bar{a})(x - a) = (x - a)(x - \bar{a})(x - \bar{a})(x - \bar{a}) = (x - \bar{a})p$, hence $Rp(x - \bar{a}) \subseteq Rp$. Since $p = (x - a)(x - \bar{a}) \in Rp$ and $Rp$ is completely prime, we have $x - a \in Rp$ or $x - \bar{a} \in Rp$, a contradiction. \qed
Example 1. Let $f = (x - i)(x - j)$ in $R = \mathbb{H}[x]$, and let $I = Rf$. Then $j$ is the only zero of $f$ (see [GS08, Example 4.4]). Thus by Lemma 4.7 we have $\sqrt{I} = R(x - j)$. However, if $(x - j)^n \in Rf$ for some $n > 1$, then $(x - j)^{n-1}$ vanishes at $i$, a contradiction. (Indeed, using [LL88, Theorem 2.8], one proves inductively that $(x - j)^m(i) = (-2j)^{m-1}(i - j)$ for all $m \in \mathbb{N}$.)

Bibliography


\footnote{We note that in [GS08], substitution is done “from the left” instead of “from the right” as we do here. Thus the root $i$ in [GS08, Example 4.4] is replaced with the root $j$ here.}