Computational content of the general Nullstellensatz for Jacobson rings

Ryota Kuroki

The University of Tokyo

Computer Algebra – Foundations and Applications
December 19, 2024

About me

Ryota Kuroki

A graduate student in mathematics at the University of Tokyo.

- My supervisor: Prof. Ryu Hasegawa
- Research interests: constructive algebra

I am interested in how much algebra can be done constructively.

What is constructive algebra?

Constructive algebra is algebra without nonconstructive principles (e.g., excluded middle, Zorn's lemma, ...).

Constructive proofs have computational content. They can be regarded as programs for proof assistants, such as Agda, Coq, and Lean.

1. Jacobson rings
2. Main result
3. Idea of the proof
4. Summary

Jacobson rings (non-constructive)

Definition 1

A Jacobson ring is a ring such that every prime ideal is an intersection of maximal ideals.

Example 1

All fields are Jacobson. The ring $\mathbb{Z}$ is Jacobson. The ring $\mathbb{Q}[[X]]$ is not Jacobson.

Proposition 1

A ring A is Jacobson if and only if

$$\bigcap_{I \subseteq \mathfrak{p} \subseteq A\colon \text{ prime}} \mathfrak{p} = \bigcap_{I \subseteq \mathfrak{m} \subseteq A\colon \text{ maximal}} \mathfrak{m}$$

holds for all ideals $I \subseteq A$.

The general Nullstellensatz (non-constructive)

Our main theorem provides a constructive version of the following theorem:

Theorem 2 ([Goldman 1951, Theorem 3], [Krull 1951, Satz 1])

If A is Jacobson, then so is $A[X]$.

Corollary 1

Let K be a field. For every ideal I of $A := K[X_1, \ldots, X_n]$,

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \subseteq A:\ \textit{prime}} \mathfrak{p} = \bigcap_{I \subseteq \mathfrak{m} \subseteq A:\ \textit{maximal}} \mathfrak{m}.$$

Classical proofs of the general Nullstellensatz use Zorn's lemma and the law of excluded middle.

Why do we need Zorn's lemma?

We use Zorn's lemma to prove that there are enough prime/maximal ideals (e.g., to prove $\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \subseteq A:\ \text{prime}} \mathfrak{p}$).

This is very useful. For example, we only have to prove that $\bar{x} =_{A/\mathfrak{p}} 0$ in domains $A/\mathfrak{p}$ to prove that $x \in A$ is nilpotent. Using this argument, it is easy to prove that if $a_n X^n + \ldots + a_0 \in A[X]$ is invertible, then $a_1, \ldots, a_n \in A$ are nilpotent.

However, this argument is not constructive. We often must avoid treating prime/maximal ideals directly in constructive algebra.

Definition without prime/maximal ideals (1/2)

Definition 3

Let $U \subseteq A$. We define ideals $\operatorname{Nil} U, \operatorname{Jac} U \subseteq A$ as follows:

$$\operatorname{Nil} U := \{a \in A : \exists n \geq 0.\ a^n \in \langle U \rangle\},$$
$$\operatorname{Jac} U := \{a \in A : \forall b \in A.\ 1 \in \langle U, 1 - ab \rangle\}.$$

Proposition 2 (non-constructive)

For every ideal $I \subseteq A$,

$$\operatorname{Nil} I = \bigcap_{I \subseteq \mathfrak{p} \subseteq A:\ \text{prime}} \mathfrak{p}, \quad \operatorname{Jac} I = \bigcap_{I \subseteq \mathfrak{m} \subseteq A:\ \text{maximal}} \mathfrak{m}.$$

Proposition 3 (non-constructive)

A is Jacobson if and only if $\operatorname{Jac} I \subseteq \operatorname{Nil} I$ holds for all ideals $I \subseteq A$. Note that the converse inclusion always holds.

Definition without prime/maximal ideals (2/2)

In constructive algebra, we use the following definition:

Definition 4 ([Wessel 2018, Section 2.4])

A ring A is called *Jacobson* if $\operatorname{Jac} I \subseteq \operatorname{Nil} I$ holds for all ideals $I \subseteq A$.

Example 2 (constructive)

All discrete fields are Jacobson. The ring $\mathbb{Z}$ is Jacobson. The latter is not trivial ([Kuroki 2024, Example 2.9]).

A constructive proof that a ring A is Jacobson works as an algorithm such that

- its input is an ideal I of A, an element a of A, and a function $f : A \to I \times A$ such that for any $b \in A$, if $(i, c) = f(b)$, then $1 = i + (1 - ab)c$, and
- its output is a natural number $n \geq 0$ such that $a^n \in I$.

Main result

Theorem 5 ([Kuroki 2024, Theorem 3.9])

In constructive mathematics, if A is Jacobson, then so is $A[X]$.

This theorem provides a solution to two questions on MathOverflow [Werner 2017; Arrow 2021] and two open problems [Lombardi 2023, 1.1, 1.2].

In constructive mathematics, although the definition of a Jacobson ring has been proposed in [Wessel 2018, Section 2.4], Jacobson rings are not well studied.

The main idea of the proof is to eliminate the use of prime/maximal ideals from a non-constructive proof in [Emerton 2010].

Dynamical method

We use a simple deductive system called the *entailment relation* to simulate an argument about prime ideals. For example, we use an entailment relation generated by the following axioms:

$$\vdash 0, \quad a, b \vdash a + b, \quad a \vdash ax, \quad ab \vdash a, b, \quad 1 \vdash .$$

The axiom $ab \vdash a, b$ corresponds to "a prime ideal containing ab contains a or b."

Suppose that we want to prove that $a \in \mathrm{Nil}\, I$. We can often translate a classical proof of $a \in \bigcap_{I \subseteq \mathfrak{p} \subseteq A:\ \text{prime}} \mathfrak{p}$ to a constructive proof of $U \vdash a$ for some finite subset $U \subseteq I$. Then we can use a constructive theorem $a \in \mathrm{Nil}\, U \iff U \vdash a$ instead of the non-constructive theorem $\mathrm{Nil}\, I = \bigcap_{I \subseteq \mathfrak{p} \subseteq A:\ \text{prime}} \mathfrak{p}$.

Generalizing Emerton's lemma

Let $A_a := A[1/a]$.

Lemma 1 (non-constructive, [Emerton 2010, Lemma 6])

If $A \to B$ is an injection of domains such that A is Jacobson, and for some $a \in A \setminus \{0\}$, the induced morphism $A_a \to B_a$ is integral, then $\bigcap_{\mathfrak{m} \subseteq B:\ \text{maximal}} \mathfrak{m} = 0$.

Lemma 2 (constructive, [Kuroki 2024, Lemma 3.6])

If $A \to B$ is a homomorphism of rings such that A is Jacobson, and for an element $a \in A$, the induced morphism $A_a \to B_a$ is integral, then $a \operatorname{Jac}_B J \subseteq \operatorname{Nil}_B J$ holds for all ideals $J \subseteq B$.

Summary and future work

Summary:

- The general Nullstellensatz has a constructive proof.
- Constructive proofs are programs.

Questions:

- Are there any applications of the general Nullstellensatz in constructive algebra?
- Can constructive algebra help computer algebra?

References

Arrow (2021). *Can you constructively prove a univariate polynomial algebra over a Jacobson ring is itself Jacobson?* MathOverflow. (version: 2021-11-06). URL: https://mathoverflow.net/q/405685.

Emerton, Matthew (2010). *Jacobson rings*. URL: https://www.math.uchicago.edu/~emerton/pdffiles/jacobson.pdf.

Goldman, Oscar (1951). "Hilbert rings and the Hilbert Nullstellensatz". In: *Math. Z.* 54, pp. 136–140. ISSN: 0025-5874, 1432-1823. DOI: 10.1007/BF01179855.

Krull, Wolfgang (1951). "Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie". In: *Math. Z.* 54, pp. 354–387. ISSN: 0025-5874, 1432-1823. DOI: 10.1007/BF01238035.

Kuroki, Ryota (2024). *A constructive proof of the general Nullstellensatz for Jacobson rings*. arXiv: 2406.06078v2 [math.AC].

Lombardi, Henri (2023). *Some classical results in Algebra needing one or several constructive versions*. URL: https://groups.google.com/g/constructivenews/c/Z6ZEmRdep8o/m/TNVpuihzAAAJ.

Werner, Jakob (2017). *Constructive treatment of Jacobson rings*. MathOverflow. (version: 2017-07-18). URL: https://mathoverflow.net/q/275737.

Wessel, Daniel (2018). "Choice, extension, conservation. From transfinite to finite proof methods in abstract algebra". PhD thesis. University of Trento, University of Verona. URL: http://eprints-phd.biblio.unitn.it/2759/.