An introduction to constructive algebra

Ryota Kuroki

The University of Tokyo

Logic Winter School III
February 20, 2025

About me

Ryota Kuroki

I am a first-year 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 non-constructive principles (e.g., excluded middle ($P \vee \neg P$), Zorn's lemma, ...).

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

Myth

Myth: Algebra is constructive.

Non-constructive proofs in algebra (1/2)

Let A be a ring. For a subset $U \subseteq A$, let

$$\operatorname{Nil} U := \{x \in A : \exists e \geq 0.\ x^e \in \langle U \rangle\},$$

where $\langle U \rangle$ denotes the ideal generated by U.

Theorem 1 (non-constructive)

$$\bigcap_{U \subseteq \mathfrak{p} \subseteq A:\ \textit{prime}} \mathfrak{p} = \operatorname{Nil} U.$$

We need enough prime ideals to prove this theorem.

Non-constructive proofs in algebra (2/2)

An elementary application:

Theorem 2

If $(a_m X^m + \cdots + a_0)(b_n X^n + \cdots + b_0) =_{A[X]} 1$, *then* $a_1, \ldots, a_m \in \operatorname{Nil} 0$.

Proof.

Let $\mathfrak{p} \subseteq A$ be a prime ideal. Since

$$(a_m X^m + \cdots + a_0)(b_n X^n + \cdots + b_0) =_{(A/\mathfrak{p})[X]} 1,$$

the elements $a_1, \ldots, a_m$ are zero in $A/\mathfrak{p}$. Hence

$$a_1, \ldots, a_m \in \bigcap_{\mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p} = \operatorname{Nil} 0. \qquad \square$$

Can you extract an $e \geq 0$ such that $a_i^e = 0$ from this proof?

How to constructivize?

The trick we have seen:

1. Proceed as if A were an integral domain. Deduce $a = 0$ (in an elementary way).
2. Then you have $a \in \mathrm{Nil}_A\, 0$.

Is this trick *legitimate* in constructive algebra?

Let's see item 1 in detail.

What are we doing? (1/4)

Let A be an integral domain.
How does $(a_2X^2+a_1X+a_0)(b_2X^2+b_1X+b_0)=1$ imply $a_1=0$?

Naive proof.

We have $a_2b_2=0$.

- If $a_2=0$, then $a_1b_2=0$.
  - If $a_1=0$, then it's ok.
  - If $b_2=0$, then $a_1b_1=0$...
- If $b_2=0$, then $a_2b_1=0$.
  - If $a_2=0$, then $a_1b_1=0$...
  - If $b_1=0$, then $a_2b_0=0$.
    - If $a_2=0$, then...
    - If $b_0=0$, then $0=_A 1$. Hence $a_1=0$. □

What are we doing? (2/4)

$$(a_2X^2 + a_1X + a_0)(b_2X^2 + b_1X + b_0) = 1$$

is equivalent to

$$\begin{aligned}&(a_2b_2 = 0) \wedge (a_2b_1 + a_1b_2 = 0)\\ &\wedge (a_2b_0 + a_1b_1 + a_0b_2 = 0)\\ &\wedge (a_1b_0 + a_0b_1 = 0) \wedge (a_0b_0 - 1 = 0)\end{aligned}$$

What are we doing? (3/4)

$$S := \{a_2b_2, a_2b_1 + a_1b_2, a_2b_0 + a_1b_1 + a_0b_2, a_1b_0 + a_0b_1, a_0b_0 - 1\}.$$

Regard an element $a \in A$ as the proposition "a is zero."

$$\dfrac{\dfrac{\dfrac{a_2b_2 \vdash a_2b_2}{S \vdash a_2b_2} \quad a_2b_2 \vdash a_2, b_2}{S \vdash a_2, b_2}\,(*) \quad \dfrac{\dfrac{\vdots}{S, a_2 \vdash a_1b_2} \quad a_1b_2 \vdash a_1, b_2}{S, a_2 \vdash a_1, b_2}\,(*)}{S \vdash a_1, b_2}\,(*)$$

$$\dfrac{\vdots}{S \vdash a_1}$$

$(*)$: cut

What are we doing? (4/4)

We are proving $S \vdash a_1$ in the following deductive system:

Rules:

$$\frac{}{a \vdash a}\ ,\quad \frac{U \vdash V}{U, U' \vdash V, V'}\ ,\quad \frac{U \vdash V, a \qquad U', a \vdash V'}{U, U' \vdash V, V'}\ (,\ \text{Exc},\ \text{Ctr}).$$

Axioms:

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

Theorem 3 ([Johnstone 1982, Section V.3.2], [Schuster and Wessel 2021], constructive)

$a_1, \ldots, a_m \vdash b_1 \ldots b_n$ is derivable iff $b_1 \cdots b_n \in \operatorname{Nil}\{a_1, \ldots, a_m\}$.

Hence $S \subseteq \{0\}$ and $S \vdash a_1$ together implies $a_1 \in \operatorname{Nil} 0$. The trick has been justified constructively.

The completeness theorem

In the constructive justification of the trick, we have used

$$U \vdash a \iff a \in \operatorname{Nil} U.$$

In the non-constructive justification, we have used

$$\bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p} \subseteq \operatorname{Nil} U,$$

which says that

$$\forall \mathfrak{p} \supseteq U.\ a \in \mathfrak{p} \iff a \in \operatorname{Nil} U.$$

They are the same thing by the completeness theorem.

(Axioms: $\vdash 0$, $\quad a, b \vdash a + b$, $\quad a \vdash ax$, $\quad ab \vdash a, b$, $\quad 1 \vdash$.)

Jacobson rings, non-constructively

Definition 4

A ring A is called *Jacobson* if

$$\bigcap_{U \subseteq \mathfrak{m} \subseteq A\text{: maximal}} \mathfrak{m} \subseteq \bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p}$$

holds for all $U \subseteq A$.

Example 1

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

Theorem 5 (the general Nullstellensatz, [Goldman 1951, Theorem 3], [Krull 1951, Satz 1])

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

Jacobson rings, constructively (1/2)

$$\operatorname{Nil} U := \{x \in A : \exists e \geq 0.\ x^e \in \langle U \rangle\},$$
$$\operatorname{Jac} U := \{x \in A : \forall a \in A.\ \exists b \in A.\ 1 - b(1 - ax) \in \langle U \rangle\}.$$

Proposition 1 (non-constructive)

$$\bigcap_{U \subseteq \mathfrak{p} \subseteq A:\ \textit{prime}} \mathfrak{p} = \operatorname{Nil} U, \qquad \bigcap_{U \subseteq \mathfrak{m} \subseteq A:\ \textit{maximal}} \mathfrak{m} = \operatorname{Jac} U.$$

Jacobson rings, constructively (2/2)

Definition 6 ([Wessel 2018, Section 2.4])

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

Example 2 (constructive)

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

Theorem 7 ([Kuroki 2024, Theorem 3.9])

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

We have extracted the constructive proof from a classical proof [Emerton 2010, Theorem 8]. This result solves problems on MathOverflow [Werner 2017; Arrow 2021] and problems in Lombardi's list [Lombardi 2023, 1.1, 1.2].

$\mathbb{Z}$ is Jacobson, non-constructively

Maximal ideals of $\mathbb{Z}$ are $\langle 2\rangle, \langle 3\rangle, \langle 5\rangle, \langle 7\rangle, \ldots$
Prime ideals of $\mathbb{Z}$ are $\langle 0\rangle, \langle 2\rangle, \langle 3\rangle, \langle 5\rangle, \langle 7\rangle, \ldots$

- If $U \subseteq \{0\}$, then

$$\bigcap_{U \subseteq \mathfrak{m} \subseteq A\text{: maximal}} \mathfrak{m} = 0 = \bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p}.$$

- If $U \not\subseteq \{0\}$, then

$$\bigcap_{U \subseteq \mathfrak{m} \subseteq A\text{: maximal}} \mathfrak{m} = \bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p}.$$

$\mathbb{Z}$ is Jacobson, constructively

$$\operatorname{Nil} U := \{x \in \mathbb{Z} : \exists e \geq 0.\ x^e \in \langle U \rangle\},$$
$$\operatorname{Jac} U := \{x \in \mathbb{Z} : \forall a \in \mathbb{Z}.\ \exists b \in \mathbb{Z}.\ 1 - b(1 - ax) \in \langle U \rangle\}.$$

We have to prove $\forall U.\ (x \in \operatorname{Jac} U) \to (x \in \operatorname{Nil} U)$ for all x.
Let $x := 6$.

Prover	Give me a $b \in \mathbb{Z}$ s.t. $1 - b(1 - 1 \cdot 6) \in \langle U \rangle$.
Delayer	$b = 4$. So you have $21 \in \langle U \rangle$.
Prover	Give me a $b \in \mathbb{Z}$ s.t. $1 - b(1 - (-1) \cdot 6) \in \langle U \rangle$.
Delayer	$b = 2$. So you have $15 \in \langle U \rangle$.
Prover	$6 = 21 - 15 \in \langle U \rangle$. So $6 \in \operatorname{Nil} U$. I win.

n-Jacobson rings

When $A = \mathbb{Z}$, Prover has a winning strategy for this game. It's enough to make two queries, but the second depends on the answer to the first.

Additional rules:

- We allow Prover to make finitely many queries at once.
- Prover can make queries at most n times.

A ring A is called n-Jacobson if Prover has a winning strategy for the game.

Example 3

The ring $\mathbb{Z}$ is 2-Jacobson but not 1-Jacobson. All fields are 1-Jacobson but not 0-Jacobson.

Every n-Jacobson ring is Jacobson.

A quantitative general Nullstellensatz

Theorem 8 ([Kuroki 2025, Corollary 25])

If A is n-Jacobson, then $A[X]$ is $(n+1)$-Jacobson.

Example 4

$\mathbb{Z}[X_1, \ldots, X_n]$ is $(2+n)$-Jacobson.

I think it's difficult to prove this theorem without knowing the constructive proof of the general Nullstellensatz.
Constructive methods may be useful even for non-constructivists.

Summary

Algebra *is* constructive.

References I

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.

Johnstone, Peter T. (1982). *Stone Spaces*. Cambridge University Press.

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

References II

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

— (2025). *A quantitative general Nullstellensatz for Jacobson rings*. arXiv: 2502.11935 [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.

Schuster, Peter and Daniel Wessel (2021). "Syntax for semantics: Krull's maximal ideal theorem". In: *Paul Lorenzen—mathematician and logician*. Vol. 51. Log. Epistemol. Unity Sci. Springer, Cham, pp. 77–102. ISBN: 978-3-030-65824-3. DOI: 10.1007/978-3-030-65824-3_6.

References III

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/.