A CONSTRUCTIVE PROOF OF THE GENERAL NULLSTELLENSATZ

Ryota Kuroki

Graduate School of Mathematical Sciences, The University of Tokyo, Japan

What is a constructive proof?

A proof is often called *constructive* if we can extract some algorithm from it. One typical way to make a proof constructive is to avoid non-constructive principles such as Zorn's lemma and the law of excluded middle.

Example 1. It is well known that there exist $a, b \in \mathbb{R} - \mathbb{Q}$ such that $a^b \in \mathbb{Q}$. A typical non-constructive proof says that $(a, b) = (\sqrt{2}, \sqrt{2})$ or $(a, b) = (\sqrt{2}^{\sqrt{2}}, \sqrt{2})$ satisfies the condition, but the proof by itself does not give an algorithm to determine which one satisfies the condition. On the other hand, it is easy to obtain a constructive proof that $(a, b) = (\sqrt{2}, 2\log_2 3)$ satisfies the condition.

Mathematics without non-constructive principles is often called *neutral mathematics*. Theorems in neutral mathematics hold in classical mathematics, and they also hold in anti-classical mathematics, such as Brouwer's intuitionistic mathematics and Russian constructive mathematics.

$$\cdots \leq \text{Neutral Math} \begin{matrix} \leq \text{Classical Math (Math in ZF(C))} \\ \leq \text{Anti-classical Math (not compatible with Excluded Middle)} \end{matrix}$$

Why constructive mathematics?

I'm doing constructive mathematics because it is more comfortable. There are some other reasons why people care about constructive mathematics:

1. A constructive proof works as an algorithm.
2. Constructive theorems hold in any toposes.

Constructive algebra

The main purpose of constructive algebra is to give a constructive proof of virtually any theorem in algebra.

Example 2. One of the most important results in constructive algebra is the elementary characterization of the Krull dimension of a commutative ring. Lombardi [5, Théorème 5] have proved that the following equivalences hold in ZFC:

$$\begin{aligned} \dim A < 1 &\iff \forall x \in A.\ \exists e \geq 0.\ x^e \in \langle x^{e+1} \rangle, \\ \dim A < 2 &\iff \forall x_1, x_2 \in A.\ \exists e_1, e_2 \geq 0.\ x_1^{e_1} x_2^{e_2} \in \langle x_1^{e_1+1}, x_1^{e_1} x_2^{e_2+1} \rangle, \\ \dim A < n &\iff \cdots . \end{aligned}$$

In constructive algebra, we use these as the definition of the Krull dimension. Classical theorems such as $\dim A < n \implies \dim A[X] < 2n$ can be proved constructively using this definition. See [7] for the constructive theory of the Krull dimension.

The general Nullstellensatz

Definition 1. Let A be a commutative ring and $U \subseteq A$. We define ideals $\operatorname{Nil} U, \operatorname{Jac} U \subseteq A$ as follows:

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

Proposition 1 (non-constructive)**.** For every subset $U \subseteq A$, the following equalities hold:

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

Goldman [1] and Krull [2] have independently introduced the notion of a Jacobson ring to generalize Hilbert's Nullstellensatz. In constructive algebra, the following definition has been proposed by Wessel [9].

Definition 2. A ring A is called *Jacobson* if $\operatorname{Jac} U \subseteq \operatorname{Nil} U$ holds for every subset U of A.

Example 3. All 0-dimensional rings are Jacobson. The ring $\mathbb{Z}$ is Jacobson. The ring $\mathbb{Q}[[X]]$ is not Jacobson.

Remark 1. It is easy to prove that $\mathbb{Z}$ is Jacobson in ZF, but finding a constructive proof is a non-trivial task. See [3, Example 2.9].

Theorem 1 (The general Nullstellensatz. [1, 2])**.** If A is Jacobson, then so is $A[X]$.

In [3], we have obtained a constructive proof of the general Nullstellensatz. Our result provides a solution to the first two problems of [6].

Why do we need Zorn's lemma in classical algebra?

We need Zorn's lemma to prove that there are enough prime/maximal ideals (e.g., to prove $\operatorname{Nil} U = \bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p}$). Some elementary theorems can be easily proved with enough prime/maximal ideals. 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.

How to convert a non-constructive proof into a constructive one?

We can often obtain a constructive proof by considering a syntactic counterpart of a classical proof.

nonconstructive proof		constructive proof
$\downarrow$		$\uparrow$
semantic argument involving prime/maximal ideals	$\rightarrow$	syntactic argument

We use a simple deductive system called the *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 $a \in \operatorname{Nil} U$. We can often translate a classical proof of $a \in \bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p}$ to a constructive proof of $U' \vdash a$ for some finite subset $U' \subseteq U$. Then we can use a constructive theorem "$a \in \operatorname{Nil} U' \iff U' \vdash a$" instead of the non-constructive theorem "$\operatorname{Nil} U = \bigcap_{U \subseteq \mathfrak{p} \subseteq A\text{: prime}} \mathfrak{p}$." See [8] for details.

Towards a quantitative general Nullstellensatz

For convenience, we use classical mathematics in this section.
The constructive proof ([3, Example 2.9]) that $\mathbb{Z}$ is Jacobson can be seen as a winning strategy of Prover for the games $J_2(\mathbb{Z}, x)$ ($x \in \mathbb{Z}$) defined as follows:

1. Let α be an ordinal, A be a ring, and $x \in A$. The game $J_\alpha(A, x)$ is played by two players called Prover and Delayer.
2. A possible position of the game is a pair (τ, U) of an ordinal $\tau \leq \alpha$ and a finite subset U of A.
3. The initial position of the game is $(\alpha, \emptyset)$.
4. Let (τ, U) be the current position.
   - If $\tau > 0$, then Prover declares a natural number $n \in \mathbb{N}$ and n elements $a_1, \ldots, a_n \in A$. Then Delayer declares n elements $b_1, \ldots, b_n \in A$. Then Prover declares an ordinal $\tau' < \tau$. The next position is (τ', U'), where $U' := U \cup \{1 - b_i(1 - a_i x) : i \in \{1, \ldots, n\}\}$.
   - If $\tau = 0$, then the game ends. Prover wins if $x \in \operatorname{Nil} U$. Delayer wins if $x \notin \operatorname{Nil} U$.

In the game $J_\alpha(A, x)$, Prover is trying to give an elementary proof that $(x \in \operatorname{Jac} U) \to (x \in \operatorname{Nil} U)$ holds for all U. A ring A is called α-*Jacobson* if Prover has a winning strategy for $J_\alpha(A, x)$ for all $x \in A$. The notion of α-Jacobson ring will be useful for studying the computational aspects of Jacobson rings. See [4] for details.

References

[1] Goldman, O. (1951). Hilbert rings and the Hilbert Nullstellensatz. *Math. Z.* 54:136–140.

[2] Krull, W. (1951). Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie. *Math. Z.* 54:354–387.

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

[4] Kuroki, R. (2025). *A quantitative general Nullstellensatz for Jacobson rings*, `arXiv:2502.11935v1 [math.AC]`.

[5] Lombardi, H. (2002). Dimension de Krull, Nullstellensätze et évaluation dynamique. *Math. Z.*, 242(1):23–46.

[6] Lombardi, H. (2023). *Some classical results in Algebra needing one or several constructive versions*. Available at: `https://groups.google.com/g/constructivenews/c/Z6ZEmRdep8o/m/TNVpuihzAAAJ`.

[7] Lombardi, H., Quitté, C. (2015). *Commutative algebra: constructive methods*. Algebra and Applications, Vol. 20. Springer, Dordrecht.

[8] Schuster, P., Wessel, D. (2021). Syntax for semantics: Krull's maximal ideal theorem. In: Heinzmann, G., Wolters, G., eds. *Paul Lörenzen – mathematician and logician*. Log. Epistemol. Unity Sci. Vol. 51. Springer, Cham, pp. 77–102.

[9] Wessel, D. (2018). *Choice, extension, conservation. From transfinite to finite proof methods in abstract algebra*. PhD thesis. University of Trento, University of Verona.

E-mail address: kuroki-ryota128 [at] g.ecc.u-tokyo.ac.jp