Dimension theory of rings in constructive algebra

Ryota Kuroki

The University of Tokyo

数学基礎論若手の会
October 13, 2024

What is constructive algebra?

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

We can extract computational content from a constructive proof. One way of doing this is to use type theories with canonicity (e.g. Martin-Löf type theory (using setoids), cubical type theory, ...).

How to constructivize?

$$
\begin{tikzcd}
\text{nonconstructive proof} \arrow[d] & \text{constructive proof} \\
\begin{array}{c}\text{semantic argument}\\ \text{involving ideal objects}\\ \text{(models, points, ...)}\end{array} \arrow[r] & \begin{array}{c}\text{syntactic argument}\\ \text{(point-free)}\end{array} \arrow[u]
\end{tikzcd}
$$

Entailment relations

Definition 1

A binary relation $\vdash$ on the set of finite multisubsets of S is called an entailment relation on S if $\vdash$ satisfies the following conditions:

(id) $a \vdash a$.

(wkn, ctr) $(U \subseteq U',\ V \subseteq V',\ U \vdash V) \implies U' \vdash V'$.

(cut) $(U \vdash V, a,\ U, a \vdash V) \implies U \vdash V$.

Here, $U \subseteq U'$ denotes the subset inclusion (we do not care about the multiplicity).

Entailment relations are closely related to distributive lattices ([Cederquist and Coquand 2000], [Lombardi 2020]).

Completeness theorems (nonconstructive)

Definition 2

$\nu : S \to 2$ is called a model of $\vdash$ if ν satisfies the following condition: $U \vdash V \implies ((\forall u \in U.\ \nu u = 1) \to (\exists v \in V.\ \nu v = 1))$.

Theorem 3 ([Scott 1974, Proposition 1.3])

The following are equivalent:

1. $U \vdash V$.
2. *For all models* ν *of* $\vdash$, $(\forall u \in U.\ \nu u = 1) \to (\exists v \in V.\ \nu v = 1)$.

Theory of prime ideals

We generate an entailment relation on a ring A by the following constructors (axioms):

$$\begin{aligned} &\vdash 0, \\ a, b &\vdash a + b, \\ a &\vdash ax, \\ ab &\vdash a, b, \\ 1 &\vdash . \end{aligned}$$

The models of $\vdash$ correspond to prime ideals of A, so $U \vdash a \iff a \in \bigcap_{\mathfrak{p} \supseteq U:\ \text{prime}} \mathfrak{p}$ by the completeness theorem (nonconstructively).
The purely syntactic statement "$U \vdash a \iff a \in \sqrt{\langle U \rangle}$" is constructively provable. This constructivizes the classical theorem "$\bigcap_{\mathfrak{p} \supseteq U:\ \text{prime}} \mathfrak{p} = \sqrt{\langle U \rangle}$".

A useful lemma

When we want to prove that "$U \vdash V$ implies something", the following lemma is useful.

Lemma 4 ([Wessel 2018, Lemma 4.34])

Let $\vdash$ be an entailment relation on S generated by constructors (axioms) of the form $U \vdash V$. Let Φ be a predicate on $\mathrm{Pow}_{\mathrm{fin}}(S)$ satisfying the following conditions:

- $U \subseteq U' \implies \Phi(U) \to \Phi(U')$.
- *For all constructors of the form $U \vdash V$, the following holds:* $[\forall U'. \, (\forall v \in V. \, \Phi(U', v)) \implies \Phi(U', U)]$ *($\Phi(U', v)$ means $\Phi(U' \cup \{v\})$).*

Then $U \vdash V$ implies $[\forall U'. \, (\forall v \in V. \, \Phi(U', v)) \implies \Phi(U', U)]$.

Theory of chains of prime ideals

We generate an entailment relation on $A \times \{0, \dots, n\}$ by the following constructors (axioms):

$$
\begin{aligned}
&\vdash (0, k), \\
(a, k), (b, k) &\vdash (a + b, k), \\
(a, k) &\vdash (ax, k), \\
(ab, k) &\vdash (a, k), (b, k), \\
(1, k) &\vdash , \\
(a, k) &\vdash (a, k + 1).
\end{aligned}
$$

The models of $\vdash$ correspond to the chains of prime ideals $P_0 \subseteq \cdots \subseteq P_n$ of A.

Definition of the Krull dimension

Classically, we have

$$
\begin{aligned}
& \forall a_1, \dots, a_n \in A.\ (a_1, 1), \dots, (a_n, n) \vdash (a_1, 0), \dots, (a_n, n-1) \\
\iff & \neg(\exists a_1, \dots, a_n \in A.\ (\text{there exists a chain of prime ideals} \\
& \quad P_0 \subseteq \cdots \subseteq P_n \text{ such that } a_k \in P_k - P_{k-1} \text{ for all } k)) \\
\iff & \neg(\text{there exists a strictly increasing chain of prime ideals} \\
& \quad P_0 \subsetneq \cdots \subsetneq P_n) \\
\iff & \operatorname{Kdim} A < n
\end{aligned}
$$

An elementary characterization of $\vdash$

Theorem 5 ([Coquand and Lombardi 2003, Theorem 3.5])

The following are equivalent:

1. $(U_0, 0), \dots (U_n, n) \vdash (V_0, 0), \dots, (V_n, n)$.
2. $\exists \mathbf{e}_k \in \mathbb{N}^{|V_k|}.\ V_0^{\mathbf{e}_0} \cdots V_n^{\mathbf{e}_n} \in \langle U_0, U_1 V_0^{\mathbf{e}_0}, \dots, U_n V_0^{\mathbf{e}_0} \cdots V_{n-1}^{\mathbf{e}_{n-1}} \rangle$.

Here, $(U_k, k) := \{(u, k) : u \in U_k\}$, $\{v_1, \dots, v_{|V_k|}\}^{\mathbf{e}_k} := \prod_i v_i^{\mathbf{e}_{k,i}}$, and $Uv := \{uv : u \in U\}$.

Using lemma 4, we can prove this directly (Let $\Phi((W_0, 0), \dots (W_n, n))$ be the proposition $\exists \mathbf{e}_k.\ V_0^{\mathbf{e}_0} \cdots V_n^{\mathbf{e}_n} \in \langle W_0, W_1 V_0^{\mathbf{e}_0}, \dots, W_n V_0^{\mathbf{e}_0} \cdots V_{n-1}^{\mathbf{e}_{n-1}} \rangle$).

An elementary characterization of the Krull dimension

Corollary 6 ([Coquand and Lombardi 2003, Corollary 3.6])

The following are equivalent:

1. Kdim $A < n$.
2. $\forall a_1, \ldots, a_n \in A.\ \exists e_1, \ldots, e_n \geq 0.\ a_1^{e_1} \cdots a_n^{e_n} \in \langle a_1^{e_1+1}, a_1^{e_1} a_2^{e_2+1}, \ldots, a_1^{e_1} \cdots a_n^{e_n+1} \rangle$.
3. *For all $a_1, \ldots, a_n \in A$, there exists a polynomial $P \in A[X_1, \ldots, X_n]$ such that the coefficient of its lowest degree term (with respect to the lexicographic order) is 1 and $P(a_1, \ldots, a_n) = 0$.*

The relation between (Krull/valuative) dimension and monomial orders has been studied in [Kemper and Viet Trung 2014; Kemper and Yengui 2020]. These results are purely new (not known even classically).

Constructive results

The following results are constructively provable (see [Lombardi and Quitté 2015]):

- $\operatorname{Kdim} \mathbb{Z} < 2$.
- If $\operatorname{Kdim} A < n$ and $a \in A$ is regular, then $\operatorname{Kdim} A/\langle a \rangle < n-1$ $(n \geq 1)$.
- If $\operatorname{Kdim} A < n$, then $\operatorname{Kdim} A[X_1, \ldots, X_m] < (m+1)n$.

It is not known if the following classical result is constructively provable:

- If A is Noetherian and $\operatorname{Kdim} A < n$, then $\operatorname{Vdim} A < n$.

The following result cannot be proved constructively:

- $\operatorname{Kdim} \mathbb{Q}[[X]] < 2$ (since this implies the limited principle of omniscience. Let $a_1 := X$, $a_2 := X^n$ $(n \in \mathbb{N}_\infty)$ to see this).

The dimension of Rees algebras (1/3)

For an ideal $I \subseteq A$, let $A[It] := \bigoplus_{k \geq 0} I^k t^k \subseteq A[t]$.
(I don't know if the following theorem is already known (even classically). Can we generalize this result?)

Theorem 7

If Kdim $A < 1$, *then* Kdim $A[It] < 2$.

A nonconstructive proof (1/3).

Let $P_0 \subsetneq P_1 \subsetneq P_2$ be prime ideals of $A[It]$,
$f = a_m t^m + \cdots + a_0 \in P_1 - P_0$ and $g = b_n t^n + \cdots + b_0 \in P_2 - P_1$.
Note that $P_0 \cap A = P_1 \cap A = P_2 \cap A$. We will derive a contradiction by induction on $m + n$.

- If $m = 0$ or $n = 0$, then $f \in P_1 \cap A \subseteq P_0$ or $g \in P_2 \cap A \subseteq P_1$. This is a contradiction.

The dimension of Rees algebras (2/3)

A nonconstructive proof (2/3).

- If $n \geq m \geq 1$, then there exists $h \in A[It]$ such that $\deg(a_m^{n-m+1}g - hf) < m$. We have $a_m^{n-m+1}g - hf \in P_2$. So $a_m^{n-m+1}g - hf \in P_1$ must hold by the inductive hypothesis (with $(f,g) := (f, a_m^{n-m+1}g - hf)$). So $a_m^{n-m+1}g - hf \in P_0$ by the inductive hypothesis (with $(f,g) := (a_m^{n-m+1}g - hf, g)$). So $a_m^{n-m+1}g \in P_1$. So $a_m \in P_1 \cap A \subseteq P_0$. Since Kdim $A \leq 0$, there exist $k \geq 0$ and $x \in A$ such that $a_m^k = x a_m^{k+1}$. So $(a_m t^m)^k = x a_m (a_m t^m)^k \in P_0$. So $f - a_m t^m \in P_1 - P_0$. This is a contradiction by the inductive hypothesis with $(f,g) := (f - a_m t^m, g)$.

The dimension of Rees algebras (3/3)

A nonconstructive proof (3/3).

- If $m \geq n \geq 1$, then there exists $h \in A[It]$ such that $\deg(b_n^{m-n+1}f - hg) < n$ and $\deg h < m$. We have $b_n^{m-n+1}f - hg \in P_2$. So $b_n^{m-n+1}f - hg \in P_1$ by the inductive hypothesis with $(f, g) := (f, b_n^{m-n+1}f - hg)$. So $b_n^{m-n+1}f - hg \in P_0$ by the inductive hypothesis with $(f, g) := (b_n^{m-n+1}f - hg, g)$. So $hg \in P_1$. So $h \in P_1$. So $h \in P_0$ by the inductive hypothesis with $(f, g) := (h, g)$. So $b_n^{m-n+1}f \in P_0$. So $b_n \in P_0$. Since Kdim $A \leq 0$, there exist $k \geq 0$ and $x \in A$ such that $b_n^k = xb_n^{k+1}$. So $(b_n t^n)^k = xb_n(b_n t^n)^k \in P_0$. So $g - b_n t^n \in P_2 - P_1$. This is a contradiction by the inductive hypothesis with $(f, g) := (f, g - b_n t^n)$. $\square$

A conservative extension

We can conservatively extend $\vdash$ by adding negative propositions $\neg(a, k)$ and the following axioms:

$$\begin{aligned} (a, k), \neg(a, k) &\vdash, \\ &\vdash (a, k), \neg(a, k). \end{aligned}$$

Using this extension, we can argue like "[Assume $(f, 1)$, $\neg(f, 0)$, $(g, 2)$, and $\neg(g, 1)$. Then we get a contradiction.] So $(f, 1), \neg(f, 0), (g, 2), \neg(g, 1) \vdash$. So $(f, 1), (g, 2) \vdash (f, 0), (g, 1)$."

References I

Cederquist, Jan and Thierry Coquand (2000). "Entailment relations and distributive lattices". In: Logic Colloquium '98 (Prague). Vol. 13. Lect. Notes Log. Assoc. Symbol. Logic, Urbana, IL, pp. 127–139. ISBN: 1-56881-113-6. DOI: 10.1017/9781316756140.011.

Coquand, Thierry and Henri Lombardi (2003). "Hidden constructions in abstract algebra: Krull dimension of distributive lattices and commutative rings". In: Commutative ring theory and applications (Fez, 2001). Vol. 231. Lecture Notes in Pure and Appl. Math. Dekker, New York, pp. 477–499. ISBN: 0-8247-0855-5. URL: https://arxiv.org/abs/1801.00097.

Kemper, Gregor and Ngo Viet Trung (2014). "Krull dimension and monomial orders". In: J. Algebra 399, pp. 782–800. ISSN: 0021-8693,1090-266X. DOI: 10.1016/j.jalgebra.2013.10.005. URL: https://arxiv.org/abs/1303.3937.

Kemper, Gregor and Ihsen Yengui (2020). "Valuative dimension and monomial orders". In: J. Algebra 557, pp. 278–288. ISSN: 0021-8693,1090-266X. DOI: 10.1016/j.jalgebra.2020.04.017. URL: https://arxiv.org/abs/1906.12067.

Lombardi, Henri (2020). "Spectral spaces versus distributive lattices: a dictionary". In: Advances in rings, modules and factorizations. Vol. 321. Springer Proc. Math. Stat. Springer, Cham, pp. 223–245. ISBN: 978-3-030-43416-8. DOI: 10.1007/978-3-030-43416-8_13.

References II

Lombardi, Henri and Claude Quitté (2015). Commutative algebra: constructive methods. revised. Vol. 20. Algebra and Applications. Finite projective modules, Translated from the French by Tania K. Roblot. Springer, Dordrecht, pp. xlix+996. ISBN: 978-94-017-9944-7. DOI: 10.1007/978-94-017-9944-7. URL: https://arxiv.org/abs/1605.04832.

Scott, Dana (1974). "Completeness and axiomatizability in many-valued logic". In: Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. Calif Vol. Vol. XXV. Proc. Sympos. Pure Math. Published for the Association for Symbolic Logic by the American Mathematical Society, Providence, RI, pp. 411–435.

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/.