代数閉包の構成的な扱い

yotsunva

Mathematical Logic Advent Calendar 2026 (`https://adventar.org/calendars/12859`) の三日目の記事です。可換環を単に環と呼びます。代数閉包みたいなオカルト的対象は存在しないので、代数閉包を使う議論を使わない議論に書き換えます。代数閉包のことは [Coq00] にもっと色々書かれています。Entailment relation の応用について知りたい方は [SW21] とかが入門にちょうど良いと思います。（セクションのタイトルの元ネタ：[Ble21] のアブストラクト）

1 Without loss of generality, excluded middle holds

Entailment relation という論理結合子のない推論体系を導入し、排中律をタダで手に入れる。

定義 1. 集合 S の有限多重部分集合 U, V の間の関係 $\vdash$ が以下の条件をみたすとき、$\vdash$ を S 上の entailment relation と呼ぶ（多重部分集合では元の重複度を考慮する。最後の節で (r-ctr) をなくす話をするのでそうしている）：

(id) $a \vdash a$
(wkn) $U \vdash V$ ならば $U, U' \vdash V, V'$
(l-ctr) $U, a, a \vdash V$ ならば $U, a \vdash V$
(r-ctr) $U \vdash V, b, b$ ならば $U \vdash V, b$
(cut)「$U, a \vdash V$ かつ $U \vdash a, V$」ならば $U \vdash V$

注 2. Entailment relation は Paul Lorenzen によって導入された。その後 Dana Scott が同じ概念を独立に導入した。

S の元を命題だと思って、$a_0, \ldots, a_{m-1} \vdash b_0, \ldots, b_{n-1}$ を「$a_0, \ldots, a_{m-1}$ が全て成り立つならば $b_0 \vee \ldots \vee b_{n-1}$ のいずれかが成り立つ」と読むと、id, wkn, l-ctr, r-ctr, cut は正しそうなことを言っている。

定理 3. Entailment relation $\vdash$ が公理 $\{U_i \vdash V_i\}_{i \in I}$ で生成されているとする（つまり $\forall i. U_i \vdash V_i$ をみたす最小の entailment relation だとする）。S と S のコピーの disjoint union $S \sqcup \{\neg a : a \in S\}$ 上の entailment relation $\vdash_\neg$ を以下の公理で生成する：

- もとの $\vdash$ の公理たち $\{U_i \vdash_\neg V_i\}_{i \in I}$
- $a, \neg a \vdash_\neg$
- $\vdash_\neg a, \neg a$

このとき、有限部分集合 $U, V \subseteq S$ に対して $U \vdash V$ と $U \vdash_\neg V$ は同値。

証明. $U \vdash V$ の証明は $U \vdash_\neg V$ の証明にもなる。逆に $U \vdash_\neg V$ の証明があれば、その証明に現れる $\neg a$ の形の元を $\vdash_\neg$ の反対側に動かして $\neg$ を削除すれば $U \vdash V$ の証明が得られる。 □

つまり、$\vdash$ が公理で生成されていて $a_0, \ldots, a_{m-1} \vdash b_0, \ldots, b_{n-1}$ を示したいとき、勝手に否定命題を追加して排中律などを使っても良い。同様に $\wedge, \vee$ などの論理結合子も勝手に追加して良いことが示せる。排中律の有無で示せるかどうかが変わってしまうのは含意や否定のようなオカルトを使って書かれる主張であり、それらを使わないで書かれる本当の主張については何も変わらない。

2 Without loss of generality, any (reduced) ring is an integral domain

$b \in \sqrt{0}$ みたいな主張を示したいとき、A を整域だと思い込んでも良いことを示す。

定義 4 (A 上の整域の理論)**.** 環 A 上の entailment relation $\vdash_A$ を以下の公理から生成する：

$$\vdash_A 0$$
$$a, b \vdash_A a + b$$
$$a \vdash_A ax$$
$$ab \vdash_A a, b$$
$$1 \vdash_A$$

文脈から明らかなときは $\vdash_A$ を単に $\vdash$ と書く。

注 5. $a_0, \ldots, a_{m-1} \vdash_A b_0, \ldots, b_{n-1}$ は $a_0, \ldots, a_{m-1} \vdash_A b_0 \cdots b_{n-1}$ と同値になる。つまり $\vdash$ の右側を一つにまとめることができる。

$a_0, \ldots, a_{m-1} \vdash b_0, \ldots, b_{n-1}$ を「$(a_0 = 0) \wedge \cdots \wedge (a_{m-1} = 0)$ ならば $(b_0 = 0) \vee \ldots \vee (b_{n-1} = 0)$」と解釈すると、$\vdash_A$ 上で議論することは A を整域だと思い込んで議論することに相当する。A が実際に整域であれば、$\vdash_A$ で示せることは本当に成り立つ：

命題 6. A が整域で $a_0, \ldots, a_{m-1} \vdash b_0, \ldots, b_{n-1}$ だとする。このとき、$(a_0 = 0) \wedge \cdots \wedge (a_{m-1} = 0)$ ならば $(b_0 = 0) \vee \ldots \vee (b_{n-1} = 0)$ である。

証明. $a_0, \ldots, a_{m-1} \vdash b_0, \ldots, b_{n-1}$ の証明に関する帰納法。 □

A が整域でなくても、次のようなことが言える：

定理 7. 以下は同値：

1. $a_0, \ldots, a_{m-1} \vdash b_0, \ldots, b_{n-1}$
2. $b_0 \cdots b_{n-1} \in \sqrt{\langle a_0, \ldots, a_{n-1} \rangle_A}$（$\sqrt{\langle a_0, \ldots, a_{n-1} \rangle_A}$ は $a_0, \ldots, a_{n-1}$ が生成する A のイデアルの根基。）

証明. $1 \to 2$ は $a_0, \ldots, a_{m-1} \vdash b_0, \ldots b_{n-1}$ の証明の構造に関する帰納法で示せる。$2 \to 1$ はやるだけ。 □

上の定理によって、以降の話は entailment relation を使わずに根基の言葉で説明することも可能である。

系 8. 以下は同値：

1. $\vdash b$
2. $b \in \sqrt{0}$

つまり、A を整域だと思い込んで $b = 0$ が証明できたら、本当の世界では $b = 0$ は言えないが b が冪零になることが示せる（A が被約環なら $b = 0$ が示せる）。こういう議論は、古典的には「全ての素イデアルの共通部分は冪零根基である」という非構成的な結果を使って行われるが、上のように議論することで構成的に行うことができる。

3 Without loss of generality, any ring is a field

A を体だと思い込んでも良いことを示す。感覚的には $\vdash_A a, (\exists x. 1 - ax)$ みたいな公理を追加しても示せることは変わらないみたいなことが言いたい。

定理 9. $a \in A$, $U, V \subseteq A$ とする。以下は同値：

1. $U \vdash_A a, V$

2. $U, 1 - aX \vdash_{A[X]} V$

証明. $1 \to 2$ は $1-aX, a \vdash_{A[X]}$ と cut から示せる。逆を示す。V の元を全てかけたものを b とおく。$U, 1-aX \vdash_{A[X]} V$ より $b \in \sqrt{\langle 1-aX\rangle_{A[X]} + \langle U\rangle_{A[X]}}$ である。$b^m = (1-aX)f + g$ をみたす $m \geq 0$, $f \in A[X]$, $g \in \langle U\rangle_{A[X]}$ が存在する。$U \vdash_A a, b$ を示したいので、A が整域だと思い込んで「U の元が全て 0 ならば $(a=0) \vee (b=0)$」を示せばよい。排中律も使ってよい。

- U の元が全て 0 なので $g = 0$ で、$b^m = (1-aX)f$ である。$a \neq 0$ と仮定すると、両辺の最高次の係数が等しいことから $f = 0$ となり、$b = 0$ となる。

よって示せた。 □

系 10. $a \in A$, $U, V \subseteq A$ とする。以下は同値：

1. $U \vdash_A V$
2. $U, a \vdash_{A[X]} V$ かつ $U, 1 - aX \vdash_{A[X]} V$

上の議論を繰り返し使うことで、好きなだけ「$a = 0$ または a は逆元をもつ」という場合分けをしても良い。

4 Without loss of generality, any ring is an algebraically closed field

A を代数閉体だと思い込んでも良いことを示す。感覚的には $\vdash_A \exists x.\, x^n + a_{n-1}x^{n-1} + \cdots + a_0$ みたいな公理を追加しても示せることは変わらないみたいなことが言いたい。

定理 11. $n \geq 1$, $a_0, \ldots, a_{n-1} \in A$, $U, V \subseteq A$ とする。以下は同値：

1. $U \vdash_A V$
2. $U, X^n + a_{n-1}X^{n-1} + \cdots + a_0 \vdash_{A[X]} V$

証明. $1 \to 2$ は明らか。逆を示す。V の元を全てかけたものを b とおく。$U, X^n + a_{n-1}X^{n-1} + \cdots + a_0 \vdash_{A[X]} V$ より $b \in \sqrt{\langle X^n + a_{n-1}X^{n-1} + \cdots + a_0\rangle_{A[X]} + \langle U\rangle_{A[X]}}$ である。$b^m = (X^n + a_{n-1}X^{n-1} + \cdots + a_0)f + g$ をみたす $m \geq 0$, $f \in A[X]$, $g \in \langle U\rangle_{A[X]}$ が存在する。$U \vdash_A b$ を示したいので、A が整域だと思い込んで「U の元が全て 0 ならば $b = 0$」を示せばよい。

- U の元が全て 0 なので $g = 0$ で、$b^m = (X^n + a_{n-1}X^{n-1} + \cdots + a_0)f$ である。$n \geq 1$ なので最高次の係数の比較により $f = 0$ となり、$b = 0$ となる。

よって示せた。 □

例えば次のような場面で使える。

命題 12 (Cayley–Hamilton)**.** 正方行列 $M \in M_n(A)$ の固有多項式を f とすると、$f(M) = 0$ である。

証明. A が代数閉体なら M を三角化して示せる。その証明は $\vdash$ の言葉に翻訳できるので、A が被約環のときも示せる。特に generic matrix $(x_{i,j}) \in M_n(\mathbb{Z}[x_{i,j} : i, j \in \{0, \ldots, n-1\}])$ で成り立つので一般の環上の行列でも成り立つ。 □

$\mathbb{Z}[x_{i,j} : i, j \in \{0, \ldots, n-1\}]$ の商体の代数閉包をとっても同じ議論ができる（必要な分だけ拡大すれば代数閉包はいらないけど）。

5 古典的手法を超えて

非構成主義者から「古典的にできるのになぜこんな縛りプレイをするんですか？」という声が聞こえてきそうなので、非自明な話をする。まず次のような古典的定理がある：

命題 13. $f = a_m X^m + \cdots + a_0 \in A[X]$ が逆元 $g = b_n X^n + \cdots + b_0$ をもつなら、$a_m, \ldots, a_1$ は冪零である。

証明 (古典的証明)**.** $\sqrt{0} = \bigcap \mathfrak{p}$ なので、任意の素イデアル $\mathfrak{p} \subseteq A$ について $a_m, \ldots, a_1 \in \mathfrak{p}$ となることを示せば良い。$A/\mathfrak{p}$ は整域なので、$fg = 1$ の係数を比較すると $a_m, \ldots, a_1$ が $A/\mathfrak{p}$ 上 0 であることが順に分かる。例えば $a_m \neq_{A/\mathfrak{p}} 0$ と仮定すると、$a_m b_n =_{A/\mathfrak{p}} 0$ なので $b_n =_{A/\mathfrak{p}} 0$ となり、これを使うと $a_m b_{n-1} =_{A/\mathfrak{p}} a_m b_{n-1} + a_{m-1} b_n = 0$ なので再び $a_m \neq_{A/\mathfrak{p}} 0$ によって $b_{n-1} =_{A/\mathfrak{p}} 0$ となり、繰り返すと $b_0 =_{A/\mathfrak{p}} 0$ となり $0 =_{A/\mathfrak{p}} a_0 b_0 = 1$ となって矛盾する。 □

この証明は冪零であることを示しているが、例えば a_m を何乗すれば 0 になるのかはこの証明からは分からない。以下のような構成的証明をすれば、a_m を何乗すれば 0 になるのか計算するアルゴリズムが得られる：

証明 (構成的証明)**.** $i \in \{1, \ldots, m\}$ に対して $\vdash_A a_i$ を示せばよい。つまり A を整域だと思い込んで a_i が 0 になることを示せばよい。排中律を使っても良いので、古典的証明と同様にできる。例えば「$a_m \neq_{A/\mathfrak{p}} 0$ と仮定すると $b_n =_{A/\mathfrak{p}} 0$」の議論は $\neg a_m \vdash b_n$ の証明に書き換えられて、$\neg a_m \vdash b_{n-1}$, $\neg a_m \vdash b_{n-2}$,... と議論を進めると $\neg a_m \vdash$ が示せて、$\vdash a_m$ が言える。 □

しかし、この証明でも a_m を何乗すれば 0 になるのかはアルゴリズムに従って計算しないと分からないじゃないかと言う人もいると思うので、最後に contraction を制限して情報を取り出す方法について述べる。$\vdash_A$ の公理と id, wkn, l-ctr, cut と「$U \vdash a, b, V$ ならば $U \vdash ab, V$」をみたすように、r-ctr 以外をみたす entailment relation もどきを $\vdash'_A$ を生成する。このとき定理 7 と同様のことが言える：

定理 14. 以下は同値：

1. $a_0, \ldots, a_{m-1} \vdash' b_0, \ldots, b_{n-1}$
2. $b_0 \cdots b_{n-1} \in \langle a_0, \ldots, a_{n-1} \rangle_A$

定理 7 と比べると、こちらは根基がついていない。定理 3 と同様のことも言えるが、¬ がついた元には左コントラクション (l-ctr) が使えないことに注意する必要がある。命題 13 の古典的証明を $\vdash'$ での証明に翻訳してみると、例えば $a_m \neq_{A/\mathfrak{p}} 0$ を仮定して矛盾を示す部分では $a_m \neq_{A/\mathfrak{p}} 0$ という仮定を $n+1$ 回使っているので、$\underbrace{\neg a_m, \ldots, \neg a_m}_{n+1 \text{ 個}} \vdash'$ となり、$\vdash' \underbrace{a_m, \ldots, a_m}_{n+1 \text{ 個}}$ が示せる。よって、$a_m^{n+1} =_A 0$ だと分かる。a_{m-1} についても考えてみると、$a_m, \neg a_{m-1} \vdash' b_n$ が言えたり $a_m, \neg a_{m-1}, \neg a_{m-1} \vdash' b_{n-1}$ が言えたりして、最終的に $a_m, \underbrace{\neg a_{m-1}, \ldots, \neg a_{m-1}}_{n+1 \text{ 個}} \vdash'$ となるので、$\vdash' \underbrace{a_{m-1}, \ldots, a_{m-1}}_{(n+1)^2 \text{個}}$ が示せる。よって $a_{m-1}^{(n+1)^2} = 0$ が分かる（実際はもっと小さい指数で済むが、この古典的証明から取り出せるのはこれぐらいである）。このように、仮定を何回使っているか気にしていると良いことがあるかもしれない。

References

[Ble21] Ingo Blechschmidt. “Generalized Spaces for Constructive Algebra”. In: *Proof and Computation II*. Ed. by Helmut Schwichtenberg Klaus Mainzer Peter Schuster. World Scientific, 2021. Chap. 4, pp. 99–187. URL: https://doi.org/10.1142/9789811236488_0004.

[Coq00] T. Coquand. *Algebraic Closure*. 2000. URL: https://www.cse.chalmers.se/~coquand/closure.ps.

[SW21] Peter Schuster and Daniel Wessel. “Syntax for Semantics: Krull’s Maximal Ideal Theorem”. In: *Paul Lorenzen – Mathematician and Logician*. Ed. by Gereon Wolters Gerhard Heinzmann. Springer Verlag, 2021, pp. 77–102. URL: https://doi.org/10.1007/978-3-030-65824-3_6.