数学基礎論サマースクール2018
証明論，特に算術の無矛盾性証明

１．導入・三つの体系

2018年9月3日 神戸大学

菊池 誠（神戸大）

数学基礎論サマースクールの歴史

数学基礎論（数理論理学）

- 証明論（形式化された証明，理論計算機科学）
- 集合論（無限集合）
- 計算論（計算可能性，計算不可能性）
- モデル論（代数的構造，数学的構造の一般論）
- 非古典論理（部分構造論理，様相論理）

数学基礎論サマースクールの歴史

- 2019年：集合論
- 2018年：証明論（神戸）
- 2017年：計算理論
- 2016年：モデル理論
- 2015年：非古典論理（神戸）
- 2014年：集合論（神戸）
- 2013年：証明論
- 2012年：計算可能性とランダムネス
- 2011年：モデル理論（神戸）
- 2010年：超準解析
- 2009年：非古典論理
- 2008年：Asian Logic Conference（神戸）
- …

数学基礎論の歴史

19世紀後半

- 実数論の算術化（デデキント，カントール）
- 自然数全体集合の特徴づけ（デデキント）
- 素朴集合論の誕生（カントール）
- 証明の形式化（フレーゲ）
- 素朴集合論の逆理

1900年代から1920年代

- 形式主義 vs 直観主義
- ヒルベルトのプログラム
- 公理的集合論と1階述語論理の誕生
- ゲーデルの完全性定理

数学基礎論の歴史

1931年：ゲーデルの不完全性定理

Tを再帰的（何が公理か計算可能）で算術を含む公理系とする.

- T がω無矛盾ならば, T は不完全.
- T が無矛盾ならば, T の無矛盾性は T では証明できない.

1930年代〜40年代

- チューリング機械の誕生と計算論の発生
- ゲンツェンによる算術の無矛盾性の証明
- ゲーデルの構成可能集合の世界

1950年代〜60年代

- ヘンキンによる完全性定理の証明とモデル論の発生
- 竹内の基本予想（解析学の無矛盾性）
- コーエンの強制法（現代的な集合論の完成）

証明の形式化

論理的記号

- 命題結合子：$\neg$ 否定，$\wedge$ かつ，$\vee$ または，$\rightarrow$ ならば
- 量化子：$\forall$ 全て，$\exists$ 存在
- 等号：$=$，変数：x, y, z, …

非論理的記号

- 関数記号：f(x, y, …), g(x, y, …), …（項数あり）
- 定数記号：a, b, c, …
- 関係記号：P(x, y, …), Q(x, y, …), … （項数あり）

言語

- 非論理的記号の集合を言語という.
- 順序の言語 {<}，群論の言語 { · }，集合論の言語 {∈}，
  算術の言語 {+, · , 0, 1, <}

証明の形式化

項

- 命題変数および定数記号は項
- f が項数 n の関数記号で $t_1, \cdots, t_n$ が項のとき，
  $f(t_1, \cdots, t_n)$ は項

論理式

- P が項数 n の関数記号で $t_1, \cdots, t_n$ が項のとき，
  $P(t_1, \cdots, t_n)$ は論理式（原始的論理式という）
- A, B が論理式のとき，$\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$ は論理式
- A が論理式で x が変数のとき，$\forall x\, A$, $\exists x\, A$ は論理式

束縛変数と自由変数

- $\forall x A(x)$ の形で現れる $A(x)$ 中の変数 x を束縛変数という.
  束縛変数でない変数を自由変数という.
- 自由変数を持たない論理式を文という.

証明の形式化

証明

- 論理的公理と仮定から出発して，推論規則を用いて論理式を書き換えて得られる論理式の列.
- 証明の最後に現れる論理式が証明の結論または定理.

論理的公理

- 論理的記号の意味から正しさが明らかな論理式
  $A \to (A \vee B)$, $(A \wedge B) \to A$ など

推論規則

- 仮定から結論を導く規則

$$\text{MP}\quad \frac{A \quad A \to B}{B} \qquad\qquad \frac{A \quad B}{A \wedge B} \qquad \text{など}$$

- 横線の上が仮定，下が結論

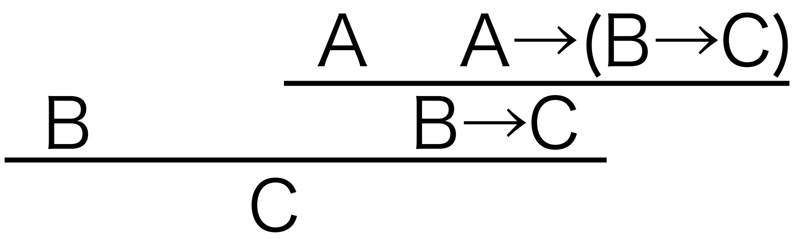
証明の形式化

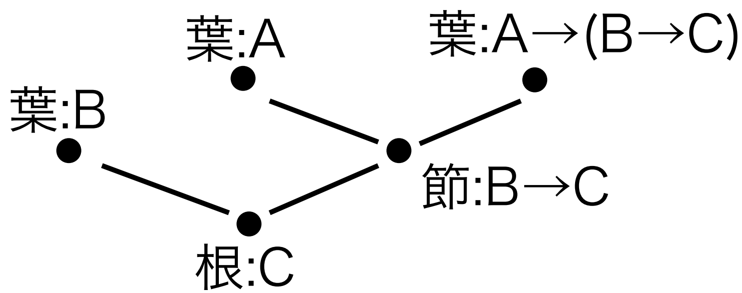
証明の例

- 以下の論理式の列は,　MP を推論規則,
  {A, B, A→(B→C)} を仮定の集合とする証明.

1. A→(B→C)　　(仮定)
2. A　　　　　(仮定)
3. B→C　　　　(MP, 1, 2)
4. B　　　　　(仮定)
5. C　　　　　(MP, 3, 4)

- 証明は木の構造を持つ．例えば：





証明の形式化

形式的体系

論理的公理と推論規則を定めると形式的体系が定まる.

- ヒルベルト流（フレーゲのものを改変）
- 自然演繹（ゲンツェン他．自然な形式化）
- シーケント計算 LK（ゲンツェン，綺麗な対称性）

理論と非論理的公理

- 非論理的公理：非論理的記号の意味を定める仮定
- 理論：非論理的公理の集合
  全順序の理論．群の理論，ZFC 集合論，ペアノ算術など

注意

- MP があれば非論理的推論規則はいらない.
- 等号の扱いは今回は省略.

ヒルベルト流の体系

論理的公理（有限個だが沢山）

- $\wedge$：$A \to (B \to A \wedge B)$, $A \wedge B \to A$, $A \wedge B \to B$
- $\vee$：$A \to A \vee B$, $B \to A \vee B$, $(A \to C) \to ((B \to C) \to (A \vee B \to C))$
- $\to$：$A \to (B \to A)$, $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- $\neg$：$(\neg A \to \neg B) \to (B \to A)$
- $\forall$：$\forall x A(x) \to A(t)$, $\forall x (A^* \to B(x)) \to (A^* \to \forall x B(X))$
- $\exists$：$\forall x (A \to B^*) \to (\exists x A(x) \to B^*)$, $A(t) \to \exists x A(x)$

ただし A^*, B^* に x は自由変数としては現れない.

推論規則（二つ）

（分離規則, MP） $$\frac{A \quad A \to B}{B}$$

（一般化） $$\frac{A(y)}{\forall x A(x)}$$

欠点：証明が著しく書きにくい.

ヒルベルト流の体系

証明可能性

T を理論，A を論理式とする．
仮定が T に含まれ結論が A である証明が存在するとき，
A は T の定理であるといい $T \vdash A$ と書く．($\vdash$：turnstyle)

演繹定理（証明を書きやすくする）

Tを理論，A を文，B を論理式とする．このとき，

$T \cup \{A\} \vdash B \Leftrightarrow T \vdash A \to B$

証明：$\Rightarrow$ は証明の長さに関する帰納法．
$\Leftarrow$ は MP を用いてすぐ．□

根本的な問題：論理的公理と推論規則は十分か？

ヒルベルト流の体系

意味論 (真理値/構造)

T：理論，A：論理式，M：構造とする．

- 定義：$M \models A$ ⇔ M 上で A が真
- 定義：$M \models T$ (M は T のモデル) ⇔ $B \in T$ ならば $M \models B$
- 定義：$T \models A$ ⇔ 全ての構造 M についてい $M \models T$ ならば $M \models A$

完全性定理（ゲーデル1930）

T を理論，A を論理式とする．このとき，$T \vdash A \Leftrightarrow T \models A$

根本的な問題に対する答：論理的公理と推論規則は十分．

他の体系

- 直観主義論理など
- 2階（高階）述語論理，ε 計算など

自然演繹 NK

NK の特徴

- 論理的公理なし．通常の推論に似て証明が書きやすい
- ヒルベルト流と同等（完全性定理が成立）
- λ計算と対応（Curry-Howard の isomorphism）
- （背理法）を取り除けば直観主義論理

推論規則

(∧導入) $$\frac{A \quad B}{A \wedge B}$$

(∧除去) $$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$

(∨導入) $$\frac{A}{A \vee B} \qquad \frac{B}{A \vee B}$$

(∨除去) $$\frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}$$

自然演繹 NK

⊥：矛盾を意味する記号.

¬A：A→⊥ の略記

推論規則（続き）

(⊥) $$\frac{\perp}{A}$$

(背理法) $$\frac{\begin{array}{c}[\neg A] \\ \vdots \\ \perp\end{array}}{A}$$

(→導入) $$\frac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \to B}$$

(演繹定理)

(→除去) $$\frac{A \qquad A \to B}{B}$$

(分離規則)

自然演繹 NK

推論規則（続き）

(∀導入) $$\frac{A(z)}{\forall x A(x)}$$

(∀除去) $$\frac{\forall x A(x)}{A(t)}$$

(∃導入) $$\frac{A(t)}{\exists x A(x)}$$

(∃除去) $$\frac{\exists x A(x) \qquad \begin{array}{c}[A(z)]\\ \vdots \\ B\end{array}}{B}$$

- (∀導入) において z は，∀xA(x) および A(z) に至る証明の仮定には自由変数として現れない.
- (∃除去) において z は，∃xA(x) および B に至る証明の仮定には自由変数として現れない.

シーケント計算 LK

シーケント

- $A_1, \cdots, A_n \vdash B$ の意味：$A_1 \wedge \cdots \wedge A_n$ ならば B
- $A_1, \cdots, A_n \vdash B_1, \cdots, B_m$：シーケント
- $\vdash$ の左右が対称になるように $\vdash$ を一般化
- 意味：$A_1 \wedge \cdots \wedge A_n$ ならば $B_1 \vee \cdots \vee B_m$

LK の特徴

- ヒルベルト流と同等（完全性定理が成立）
- 自然演繹の証明の構成は「仮定と結論の組み」の書き換え. そのプロセスを推論規則として記述.
- 対称性による優れた数学的性質
- $\Gamma \vdash B$ の形に制限すると直観主義論理

記法：$\Gamma, \Delta, \cdots$ は論理式の有限列

シーケント計算 LK

NK の規則をシーケントで表現

(∧導入)
$$\dfrac{\begin{matrix}\Gamma \\ \vdots \\ A\end{matrix} \qquad \begin{matrix}\Gamma \\ \vdots \\ B\end{matrix}}{A \wedge B} \quad \Rightarrow \quad \dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

(∧除去)
$$\dfrac{\begin{matrix}\Gamma \\ \vdots \\ A \wedge B\end{matrix}}{A} \quad \Rightarrow \quad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad \Rightarrow \quad \dfrac{\Gamma \vdash A \wedge B \qquad \dfrac{A \vdash A}{A \wedge B \vdash A}}{\Gamma \vdash A}$$

$\dfrac{A \wedge B}{B}$ も同様

シーケント計算 LK

NK の ∧ に関する規則を表現するのに必要な規則

(始式) $A \vdash A$

(∧左)
$$\frac{A,\ \Gamma \vdash \Delta}{A \wedge B,\ \Gamma \vdash \Delta} \qquad \frac{B,\ \Gamma \vdash \Delta}{A \wedge B,\ \Gamma \vdash \Delta}$$

(∧右)
$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}$$

(Cut)
$$\frac{\Gamma \vdash \Delta, A \qquad A, \Pi \vdash \Sigma}{\Gamma, \Pi \vdash \Delta, \Sigma}$$

- 同様の考え方で他の論理記号に関する規則も作る.

シーケント計算 LK

始式：$A \vdash A$

構造規則

Weakening (左) $$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}$$ (右) $$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}$$

Contraction (左) $$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}$$ (右) $$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

Exchange (左) $$\frac{\Gamma, A, B, \Pi \vdash \Delta}{\Gamma, B, A, \Pi \vdash \Delta}$$ (右) $$\frac{\Gamma \vdash \Delta, A, B, \Sigma}{\Gamma \vdash \Delta, B, A, \Sigma}$$

Cut $$\frac{\Gamma \vdash \Delta, A \qquad A, \Pi \vdash \Sigma}{\Gamma, \Pi \vdash \Delta, \Sigma}$$

シーケント計算 LK

論理規則

(∧左)

$$\frac{A,\ \Gamma \vdash \Delta}{A \wedge B,\ \Gamma \vdash \Delta} \qquad \frac{B,\ \Gamma \vdash \Delta}{A \wedge B,\ \Gamma \vdash \Delta}$$

(∧右)

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}$$

(∨左)

$$\frac{A,\ \Gamma \vdash \Delta \qquad B,\ \Gamma \vdash \Delta}{A \vee B,\ \Gamma \vdash \Delta}$$

(∧左)

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B}$$

シーケント計算 LK

論理規則（続き）

(¬左)
$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}$$

(¬右)
$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}$$

(→左)
$$\frac{\Gamma \vdash \Delta, A \qquad B, \Pi \vdash \Sigma}{A \to B, \Gamma, \Pi \vdash \Delta, \Sigma}$$

(→右)
$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}$$

(∀左)
$$\frac{A(t), \Gamma \vdash \Delta}{\forall x A(x), \Gamma \vdash \Delta}$$

(∀右)
$$\frac{\Gamma \vdash \Delta, A(z)}{\Gamma \vdash \Delta, \forall x A(x)}$$

(∃左)
$$\frac{A(z), \Gamma \vdash \Delta}{\exists x A(x), \Gamma \vdash \Delta}$$

(∃右)
$$\frac{\Gamma \vdash \Delta, A(t)}{\Gamma \vdash \Delta, \exists x A(x)}$$

- (∀右), (∃左) の下式に z は自由変数として現れない.

シーケント計算 LK

ゲンツェンの cut 消去定理

$\Gamma \vdash \Delta$ が LK で証明できるのならば,
$\Gamma \vdash \Delta$ は cut を用いずに LK で証明できる.

証明のアイディア

- cut を「前に」くりり出す.

$$\dfrac{\dfrac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B} \qquad \dfrac{A, \Pi \vdash \Sigma}{A \wedge B, \Pi \vdash \Sigma}}{\Gamma, \Pi \vdash \Delta, \Sigma} \ (A \wedge B \text{ を cut})$$

$$\Rightarrow \quad \dfrac{\Gamma \vdash \Delta, A \qquad A, \Pi \vdash \Sigma}{\Gamma, \Pi \vdash \Delta, \Sigma} \ (A \text{ を cut})$$

- より簡単な証明になる. これを繰り返す. □

シーケント計算 LK

<u>矛盾</u>

　LK が矛盾する

⇔ 全ての命題が LK で証明可能

⇔ $\vdash$ （空なシーケント）が LK で証明可能

<u>cut 消去定理の系</u>

　$\vdash$ は LK で証明可能でない．つまり，LK は無矛盾．

<u>証明のアイディア</u>

　cut がなければシーケント内の論理式は減らない．□

<u>注意</u>

　非論理的公理があると話は簡単でない．

告知

講義録

- 講義録は今年度中に出版予定.
 「算術の無矛盾性証明：証明論入門」
 原稿は大方完成．乞うご期待.

研究集会のお知らせ

- 竹内外史追悼シンポジウム
- 2018年9月18日（火）から20日（木）まで
- 神戸大学 瀧川記念学術交流会館
- 招待講演者：難波完爾，八杉満利子，小沢正直，
 J.Y.Girard，S.Buss, W.Sieg
- www2.kobe-u.ac.jp/~mkikuchi/saml2018/index.html