

論理学

第4回「証明」

萩野 達也

hagino@sfc.keio.ac.jp

lecture URL

<https://vu5.sfc.keio.ac.jp/slide/>

前回まで

- 命題

- 真偽が決まっている文
- 命題変数
- 論理結合子 ($\wedge$, $\vee$, $\rightarrow$, $\neg$)
- 論理式
- 真理値表
- トートロジー

- 標準形

- 論理和標準形
- 論理積標準形
- 論理結合子の制限

推論

- 真理値表を用いた命題の**正しさ**の定義
 - 基本的な命題(命題変数)の真偽値から, 命題の真偽を計算する.
- **推論**
 - すでに正しいと分かっている命題から, 別の正しい命題を導く
 - 推論規則を繰り返し用いて, 前提となる命題から, 命題導く
 - 「前提 $B_1, \dots, B_n$ から A が推論される」
- **推論規則**(inference rule)
 - 正しい命題から正しい命題を導く規則
- 例
 - A と $A \rightarrow B$ から B を導く
 - **モーダスポネンス**(modus ponens)
 - **三段論法**(syllogism)とも呼ばれる
 - 「人間は死すべきもの」であり「ソクラテスは人間である」, ゆえに「ソクラテスは死すべきもの」である.

公理と定理

- **公理** (axiom)
 - 正しいと考える前提
 - 「異なった2点を通る直線はただ一つ存在する」
 - 「平行線は交わらない」
- **定理** (theorem)
 - 公理から推論規則を使って得られた命題
 - 定理を導く推論の過程を**証明** (proof) という
 - 「3 角形の内角の和は180 度である」
 - 「ピタゴラスの定理」

形式論理体系

- 扱っている論理学を形式的に扱う**体系**
 - 論理式の構文や操作に関する体系
 - 公理と推論規則からなる
- 古典命題論理 (classical propositional logic) の形式体系
 - ヒルベルト (Hilbert) の体系
 - 公理中心で推論規則はモーダスポネンスだけ
 - ゲンツェン (Gentzen) の **自然演繹** (natural deduction) の体系
 - 日常の推論に近いもの
 - **NK体系**
 - ゲンツェンの **sequent計算** の体系
 - 形式的な表現にすぐれている
 - **LK体系**

LKの式

- LK 体系では次の**式** (sequent) を用いる

$$A_1, \dots, A_m \vdash B_1, \dots, B_n$$

- 意味
 - 「 A_1 から A_m を**すべて** 仮定すると, B_1 から B_n の**どれか** が導かれる」
- 「**⊢**」の読み方
 - ターンスタイル (turnstile, 回転扉)
 - ティー (tee)
- $A_1, \dots, A_m \vdash B_1, \dots, B_n$
 - 「 $A_1, \dots, A_m$ 」 **前件** (antecedent)
 - 「 $B_1, \dots, B_n$ 」 **後件** (succedent)
 - 「前件から後件が導かれる」

式の特別な場合

$$A_1, \dots, A_m \vdash B_1, \dots, B_n$$

- m や n は0でもかまわない
 - $\vdash B_1, \dots, B_n$
 - 仮定は必要なく「 B_1 から B_n のどれかである」
 - $\vdash B$
 - 「 B である」
 - $A_1, \dots, A_m \vdash$
 - 導かれるものがないので、「 A_1 から A_m をすべて仮定すると矛盾する」
 - 「 A_1 から A_m のすべてを仮定してはいけない」
 - 「 A_1 から A_m のどれかではない」
 - $A \vdash$
 - 「 A から導かれるものはない」
 - 「 A ではない」
 - $\vdash$
 - 仮定は必要がないのに、導くものがない
 - 「矛盾している」

LKの推論規則

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ (CL)}$$

前提の式

推論規則の名前

結論の式

- **前提** (premise) の式から, **結論** (conclusion) の式を得る

- A は論理式
- Γ, Δ は論理式の列
 - 空でも構わない

- 例

$$\frac{A, A, B, C \vdash D}{A, B, C \vdash D} \text{ (CL)} \quad \frac{A, A \vdash A \wedge B}{A \vdash A \wedge B} \text{ (CL)} \quad \frac{A \vee B, A \vee B \vdash A \wedge B}{A \vee B \vdash A \wedge B} \text{ (CL)}$$

$$\frac{p \rightarrow q \vee r, p \rightarrow q \vee r, p \wedge s \vdash s \rightarrow t}{p \rightarrow q \vee r, p \wedge s \vdash s \rightarrow t} \text{ (CL)}$$

LKの公理と推論規則

- 公理: **始式** (initial sequent) と定数

$$\frac{}{A \vdash A} \text{ (I)}$$

$$\frac{}{\vdash \top} \text{ (T)}$$

$$\frac{}{\perp \vdash} \text{ (}\perp\text{)}$$

- 構造に関する **推論規則**: weakening, contraction, exchange, cut

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ (WL)}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \text{ (WR)}$$

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ (CL)}$$

$$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A} \text{ (CR)}$$

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta} \text{ (EL)}$$

$$\frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2} \text{ (ER)}$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \text{ (Cut)}$$

(ここで Γ, Δ は論理式の列)

推論規則(つづき)

- 論理結合子に関する推論規則

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} (\wedge L_1)$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} (\vee R_1)$$

$$\frac{B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} (\wedge L_2)$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B} (\vee R_2)$$

$$\frac{A, \Gamma_1 \vdash \Delta_1 \quad B, \Gamma_2 \vdash \Delta_2}{A \vee B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} (\vee L)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \wedge B} (\wedge R)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \rightarrow B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} (\rightarrow L)$$

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \rightarrow B} (\rightarrow R)$$

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

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

LKの公理

$$\frac{}{A \vdash A} \text{ (I)}$$

- 意味

- 「 A から A を導くことができる」

- LKでは公理は実質一つだけ

- A は任意の論理式なので、実際には無数にある
- A が任意なので、 A を実際の論理式に当てはめる必要がある

- 例

$$\frac{}{p \vdash p} \text{ (I)}$$

$$\frac{}{p \wedge q \vdash p \wedge q} \text{ (I)}$$

$$\frac{}{p \rightarrow q \vee r \vdash p \rightarrow q \vee r} \text{ (I)}$$

$$\frac{}{A \vee B \vdash A \vee B} \text{ (I)}$$

LKの定数に関する公理

$$\frac{}{\vdash \top} (\top) \qquad \frac{}{\perp \vdash} (\perp)$$

- 意味
 - 「真を導くことができる」
 - 「偽からは何も導くことはできない」

Weakening, Contraction, Exchange推論規則

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ (WL)}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \text{ (WR)}$$

- weakening

- 前件や後件に任意の論理式を付け加えても構わない

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ (CL)}$$

$$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A} \text{ (CR)}$$

- contraction

- 同じ論理式は1つに縮約することができる

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta} \text{ (EL)}$$

$$\frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2} \text{ (ER)}$$

- exchange

- 前件内あるいは後件内の論理式の順序を入れ替えても構わない

Cut推論規則

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \text{ (Cut)}$$

- **cut**
 - A を**後件**に持つ式と, A を**前件**に持つ式から, A を**切り離した**式を推論する
 - $\Gamma_2 \vdash \Delta_2$ を直接示すことが難しい
 - A を別を示しておいて
 - $A, \Gamma_2 \vdash \Delta_2$ を推論する

左と右の推論規則

- 規則の**結論部分**に論理結合子がある

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} (\wedge L_1)$$

$$\frac{B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} (\wedge L_2)$$

$$\frac{A, \Gamma_1 \vdash \Delta_1 \quad B, \Gamma_2 \vdash \Delta_2}{A \vee B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} (\vee L)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \rightarrow B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} (\rightarrow L)$$

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

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} (\vee R_1)$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B} (\vee R_2)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \wedge B} (\wedge R)$$

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \rightarrow B} (\rightarrow R)$$

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

左: 前件に論理結合子

右: 後件に論理結合子

「 $\wedge$ 」の推論規則

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} (\wedge L_1)$$

$$\frac{B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} (\wedge L_2)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \wedge B} (\wedge R)$$

- 2つの左の規則 ($\wedge L_1, \wedge L_2$)
 - 前件に「 $\wedge$ 」を追加する
 - 「 A を $A \wedge B$ にする」
 - 「 B を $A \wedge B$ にする」
- 1つの右の規則 ($\wedge R$)
 - 後件に「 $\wedge$ 」を追加する
 - 「 A と B をあわせて $A \wedge B$ にする」
 - 前提の2つの式から結論の式を推論する

「 $\vee$ 」の推論規則

$$\frac{A, \Gamma_1 \vdash \Delta_1 \quad B, \Gamma_2 \vdash \Delta_2}{A \vee B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \quad (\vee L)$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \quad (\vee R_1)$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B} \quad (\vee R_2)$$

- 1つの左の規則 ($\vee L$)
 - 前件に「 $\vee$ 」を追加する
 - 「 A と B をあわせて $A \vee B$ にする」
 - 前提の2つの式から結論の式を推論する
- 2つの右の規則 ($\vee R_1, \vee R_2$)
 - 後件に「 $\vee$ 」を追加する
 - 「 A を $A \vee B$ にする」
 - 「 B を $A \vee B$ にする」

「 $\rightarrow$ 」の推論規則

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \rightarrow B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} (\rightarrow L)$$

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \rightarrow B} (\rightarrow R)$$

- 1つの左の規則 ($\rightarrow L$)
 - 前件に「 $\rightarrow$ 」を追加する
 - 「後件の A と, 前件の B をあわせて $A \rightarrow B$ にする」
 - 前提の2つの式から結論の式を推論する
- 1つの右の規則 ($\rightarrow R$)
 - 後件に「 $\rightarrow$ 」を追加する
 - 「前件の A と, 後件の B をあわせて $A \rightarrow B$ にする」

「 $\neg$ 」の推論規則

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

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

- 1つの左の規則 ($\neg L$)
 - 前件に「 $\neg$ 」を追加する
 - 「後件の A を前件の $\neg A$ にする」
- 1つの右の規則 ($\neg R$)
 - 後件に「 $\neg$ 」を追加する
 - 「前件の A を後件の $\neg A$ にする」

LKの証明図

- LK の証明図 (proof figure)
 - 始式(あるいは定数)から出発し, 推論規則を次々に適用していく過程を記述したもの
 - 証明図の一番下にある式を, その証明図の終式 (end sequent) という.
- 例: 証明図

$$\begin{array}{c}
 \frac{}{A \vdash A} \text{ (I)} \\
 \frac{}{\vdash A, \neg A} \text{ (}\neg\text{R)} \\
 \frac{}{\vdash A, A \vee \neg A} \text{ (}\vee\text{R}_2\text{)} \\
 \frac{}{\vdash A \vee \neg A, A} \text{ (ER)} \\
 \frac{}{\vdash A \vee \neg A, A \vee \neg A} \text{ (}\vee\text{R}_1\text{)} \\
 \frac{}{\vdash A \vee \neg A} \text{ (CR)}
 \end{array}$$

← 終式

- S を終式とする証明図が存在する時, S はLKで証明可能である (provable) という.

練習問題

- 次の命題を証明しなさい.
 - $\vdash A \rightarrow \neg\neg A$
 - $\vdash \neg\neg A \rightarrow A$
 - $\vdash A \wedge B \rightarrow B \wedge A$
 - $\vdash A \vee B \rightarrow B \vee A$
 - $\vdash \neg(A \wedge \neg B) \rightarrow (A \rightarrow B)$
 - $\vdash (A \rightarrow B) \rightarrow \neg(A \wedge \neg B)$

宿題(証明)

- 問題

- 次の論理式を証明しなさい.

$$\vdash \neg(A \wedge B) \rightarrow (\neg A \vee \neg B)$$

- 提出

- 提出先: SOL
- 期限: 今週土曜日
- 形式: Powerpointなどで作成しPDFにしてください
- 注意:
 - 証明図を書きなさい
 - どの推論規則を使ったかが分かるようにしなさい
 - 始式から始めて終式が上記の論理式になるようにしなさい

まとめ

- 推論
 - 公理
 - 定理
- LK体系
 - 始式
 - LK推論規則
- 証明
 - 証明図