離散数学 第 4 回
集合と論理 (4)：論理を使った証明 (第 2 ステップ)

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2013 年 5 月 14 日

最終更新：2013 年 5 月 15 日　13:11

今日の概要

今日の目標
- 人間の読める証明が書けるようになる
  - 定義に基づいて書き直すこと
  - 推論に基づいて書き下すこと
- 全称命題の証明ができるようになる

なぜ証明を勉強するのか？
- 証明は論理的思考の根幹 $\leadsto$ 論理的思考の訓練
- 証明は文章 (主張) $\leadsto$ 文章構造と論理構造の対応に注目

これを通して，文章を論理的に読み書きできるようになる

目次

とりあえず，証明を見てみる

証明してみること (1)
集合 A, B に対して，
$$A \cap B \subseteq A$$
が成立する．

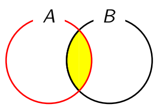
証明：
- x を任意に選び，$x \in A \cap B$ であると仮定する．
- 共通部分の定義より，$x \in A$ かつ $x \in B$．
- よって，$x \in A$ が成り立つ．
- したがって，$A \cap B \subseteq A$ が成り立つ．□

疑問？
これは何？

オイラー図の与える直観

証明してみること (1)
集合 A, B に対して，
$$A \cap B \subseteq A$$
が成立する．

オイラー図を描いてみる



これは直観を与えるだけで，証明は論理に基づいて行う

証明とは？

証明とは？ (常識に基づく定義)
定義と前提に基づき，推論を重ねて，結論を導くこと

「結論を導く」とは？
「『前提』ならば『結論』」という命題が恒真命題であることを示すこと

証明してみること (1)
集合 A, B に対して，
$$A \cap B \subseteq A$$
が成立する．

これはどういう命題なのか？ 定義に戻って書き直す
- $\cap$ (共通部分) の定義に戻る
- $\subseteq$ (部分集合) の定義に戻る

証明の作り方：定義に基づいて書き直す

証明したいこと
$$A \cap B \subseteq A$$

それを $\subseteq$ の定義に基づいて書き直したもの
任意の x に対して ($x \in A \cap B$ ならば $x \in A$)

それを $\cap$ の定義に基づいて書き直したもの
任意の x に対して (($x \in A$ かつ $x \in B$) ならば $x \in A$)

証明の作り方：定義に基づいて書き直す (続)

書き直してできたもの (再掲)
任意の x に対して (($x \in A$ かつ $x \in B$) ならば $x \in A$)

ここで，命題関数 $P(x)$ と $Q(x)$ を次のように置く
- $P(x) =$ 「$x \in A$」
- $Q(x) =$ 「$x \in B$」

「書き直してできたもの」を $P(x)$ と $Q(x)$ によって書き直したもの
$$\forall x\, ((P(x) \land Q(x)) \to P(x))$$

この論理式が恒真式であることを示せばよい

はじめの「そっけない証明」をもう一度見てみる

証明したいこと

$$A \cap B \subseteq A$$

証明：
- x を任意に選び，$x \in A \cap B$ であると仮定する．
- 共通部分の定義より，$x \in A$ かつ $x \in B$．
- よって，$x \in A$ が成り立つ．
- したがって，$A \cap B \subseteq A$ が成り立つ． □

ポイント
- 「定義に基づいて書き直す」ことを確かに行っている
  - しかし，どこで行っているのかは分かりにくい

まず，「定義に基づいて書き直す」ことに主眼を置く

とりあえず，証明を見てみる：パート 2

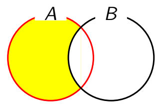
証明してみること (2)

集合 A, B に対して，

$$(A \cup B) - B \subseteq A$$

が成立する．

オイラー図から直観を得る



「証明してみること」を定義に基づいて書き直す

定義に基づいて書き直す

証明したいこと

$$(A \cup B) - B \subseteq A$$

それを $\subseteq$ の定義に基づいて書き直したもの

任意の x に対して ($x \in (A \cup B) - B$ ならば $x \in A$)

定義に基づいて書き直す (続)

「$x \in (A \cup B) - B$」を $-$ の定義に基づいて書き直したもの

$x \in A \cup B$ かつ $x \notin B$

それを $\cup$ の定義に基づいて書き直したもの

($x \in A$ または $x \in B$) かつ $x \notin B$

それを $\notin$ の定義に基づいて書き直したもの

($x \in A$ または $x \in B$) かつ ($x \in B$ ではない)

定義に基づいて書き直す (続 2)

証明したいことを $\subseteq$，$-$，$\cup$，$\notin$ の定義に基づいて書き直したもの

任意の x に対して

((($x \in A$ または $x \in B$) かつ ($x \in B$ ではない)) ならば $x \in A$)

ここで，命題関数 $P(x)$ と $Q(x)$ を次のように置く
- $P(x) =$ 「$x \in A$」
- $Q(x) =$ 「$x \in B$」

「書き直したもの」を $P(x)$ と $Q(x)$ によって書き直したもの

$$\forall x\ (((P(x) \lor Q(x)) \land \neg Q(x)) \rightarrow P(x))$$

目次

とりあえず，証明を見てみる (再掲)

証明してみること (1)

集合 A, B に対して，

$$A \cap B \subseteq A$$

が成立する．

証明：
- x を任意に選び，$x \in A \cap B$ であると仮定する．
- 共通部分の定義より，$x \in A$ かつ $x \in B$．
- よって，$x \in A$ が成り立つ．
- したがって，$A \cap B \subseteq A$ が成り立つ． □

今からやること

定義に基づいて書き下したものから，証明の構造を考える

格言

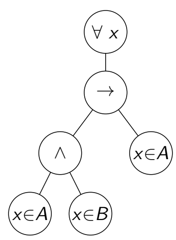
証明は文章 (文章の構造をしっかりと捉える)

定義に基づいて書き下す (1)

定義に基づいて書き下したもの (再掲)

任意の x に対して (($x \in A$ かつ $x \in B$) ならば $x \in A$)

構造



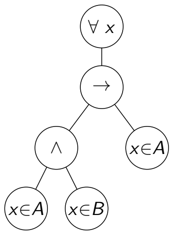
証明を書き進めるときのポイント

構造によって類型化され，
次の 2 つを組にして考える
- 証明の文章構造
- 論理操作 (同値変形，推論)

構造による類型化：全称命題

証明する目標が「$\forall x \in D$ (〇〇)」の場合

- 文章構造：「$x \in D$ を任意に選ぶ」として，〇〇を証明する
- 論理操作：「$x \in D$」であることを仮定して，〇〇を証明する



全称命題の証明：文章構造

部分集合の定義より，「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．
〈 ここに「$x \in A \cap B$ ならば $x \in A$」の証明を書く 〉
したがって，$A \cap B \subseteq A$ が成立する． □

全称命題の証明：論理操作

操作前

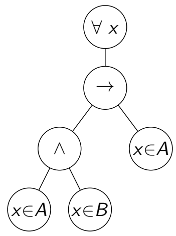
使える性質 (仮定)	導く性質 (目標)
	任意の x に対して $x \in A \cap B$ ならば $x \in A$

操作後

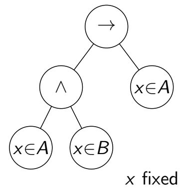
使える性質 (仮定)	導く性質 (目標)
	$x \in A \cap B$ ならば $x \in A$

全称命題の証明：目標の構造も変化

操作前の目標



操作後の目標



↑ x は固定済み

全称命題の証明：一般論

操作前の目標

$\forall x\, (P(x) \to Q(x))$ が正しい (恒真である) ことの証明

操作後の目標

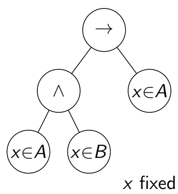
$P(x) \to Q(x)$ がすべての x に対して正しい (恒真である) ことの証明

この 2 つが同じ結論を導くことは，$\forall$ の定義から分かる
(同値変形を記号ではなく，文章で行ったにすぎない)

構造による類型化：含意

証明する目標が「〇〇 → △△」の場合

- 文章構造：「〇〇を仮定する」として，△△を証明する
- 論理操作：〇〇であることを仮定して，△△を証明する



含意の証明：文章構造

部分集合の定義より，「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．
$x \in A \cap B$ であると仮定する．
〈 ここに「$x \in A$」の証明を書く 〉
したがって，$A \cap B \subseteq A$ が成立する． □

含意の証明：論理操作

操作前

使える性質 (仮定)	導く性質 (目標)
	$x \in A \cap B$ ならば $x \in A$

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in A \cap B$	$x \in A$

含意の証明：一般論

操作前の目標
$P \to Q$ が正しいことの証明

操作後の目標
P が正しいときに，Q が正しいことの証明

この 2 つが同じ結論を導くことは，$\to$ の定義から分かる
(同値変形を記号ではなく，文章で行ったにすぎない)

証明の続き (1)：文章構造

部分集合の定義より,「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．
$x \in A \cap B$ であると仮定する．
⟨ ここに「$x \in A$」の証明を書く ⟩
したがって，$A \cap B \subseteq A$ が成立する． □

証明の続き (2)：文章構造

部分集合の定義より,「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．
$x \in A \cap B$ であると仮定する．
$x \in A \cap B$ より，$x \in A$ かつ $x \in B$ が成り立つ．
よって，$x \in A$ が成り立つ．
したがって，$A \cap B \subseteq A$ が成立する． □

証明終了：文章構造

部分集合の定義より,「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．
$x \in A \cap B$ であると仮定する．
$x \in A \cap B$ より，$x \in A$ かつ $x \in B$ が成り立つ．
よって，$x \in A$ が成り立つ．
したがって，$A \cap B \subseteq A$ が成立する． □

証明終了：清書

- 部分集合の定義より,「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．
- x を任意に選ぶ．
- $x \in A \cap B$ であると仮定する．
- $x \in A \cap B$ より，$x \in A$ かつ $x \in B$ が成り立つ．
- よって，$x \in A$ が成り立つ．
- したがって，$A \cap B \subseteq A$ が成立する． □

格言 (再掲)
証明は文章 (文章の構造をしっかりと捉える)

最後に行った論理操作は何なのか？

推論に基づく証明

推論とは？ (常識に基づいた定義)
「$P \Rightarrow Q$」であるとき，
使える性質 (仮定) の中の P を Q で置き換えること

注意：「導く性質 (目標) の P」を Q で置き換えてはいけない

重要な性質
操作後の目標が証明できると，操作前の目標も証明できたことになる

推論 (1)：論理操作

操作前

使える性質 (仮定)	導く性質 (目標)
$x \in A \cap B$	$x \in A$

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in A \cap B$	$x \in A$
$x \in A$ かつ $x \in B$	

推論に用いた事実：$x \in A \cap B \Leftrightarrow x \in A$ かつ $x \in B$ ($\cap$ の定義)

推論 (2)：論理操作

操作前

使える性質 (仮定)	導く性質 (目標)
$x \in A \cap B$	$x \in A$
$x \in A$ かつ $x \in B$	

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in A \cap B$	$x \in A$
$x \in A$ かつ $x \in B$	
$x \in A$	

推論に用いた事実：$P \wedge Q \Rightarrow P$ (恒真式)

もう一度証明を見てみる

部分集合の定義より，「任意の x に対して，$x \in A \cap B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．

$x \in A \cap B$ であると仮定する．

$x \in A \cap B$ より，$x \in A$ かつ $x \in B$ が成り立つ．
よって，$x \in A$ が成り立つ．

したがって，$A \cap B \subseteq A$ が成立する． □

推論に基づく証明：一般論

操作前の目標

$P \to R$ が正しいことの証明

ここで「$P \Rightarrow Q$」が成り立つとする

操作後の目標

$P \wedge Q \to R$ が正しいことの証明

操作後の目標が達成できれば，操作前の目標も達成できる

- なぜか？
- $((P \to Q) \wedge ((P \wedge Q) \to R)) \Rightarrow (P \to R)$ が成り立つから (演習問題)

ポイント

推論により，証明において使える性質が増えていき，
証明がしやすくなっていく

目次

とりあえず，証明を見てみる：パート 2

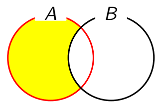
証明してみること (2)

集合 A, B に対して，

$$(A \cup B) - B \subseteq A$$

が成立する．

オイラー図から直観を得る

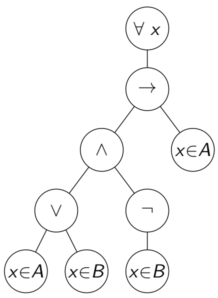


定義に基づいて書き直したもの

任意の x に対して

$(((x \in A$ または $x \in B)$ かつ $(x \in B$ ではない$))$ ならば $x \in A)$

証明することの構造



全称命題の証明：文章構造

部分集合の定義より，「任意の x に対して，$x \in (A \cup B) - B$ ならば $x \in A$」を証明すればよい．

x を任意に選ぶ．

〈 ここに「$x \in (A \cup B) - B$ ならば $x \in A$」の証明を書く 〉

したがって，$(A \cup B) - B \subseteq A$ が成立する． □

全称命題の証明：論理操作

操作前

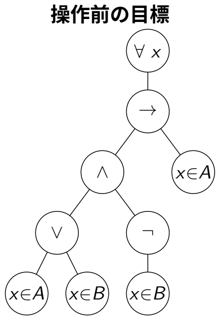
使える性質 (仮定)	導く性質 (目標)
	任意の x に対して $x \in (A \cup B) - B$ ならば $x \in A$

操作後

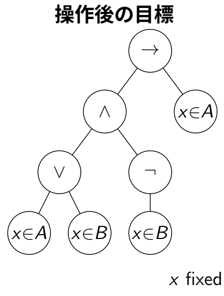
使える性質 (仮定)	導く性質 (目標)
	$x \in (A \cup B) - B$ ならば $x \in A$

全称命題の証明：目標の構造も変化

操作前の目標



操作後の目標



↑ x は固定済み

含意の証明：論理操作

操作前

使える性質 (仮定)	導く性質 (目標)
	$x \in (A \cup B) - B$ ならば $x \in A$

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in (A \cup B) - B$	$x \in A$

含意の証明：文章構造

部分集合の定義より,「任意の x に対して，$x \in (A \cup B) - B$ ならば $x \in A$」を証明すればよい.

x を任意に選ぶ.

$x \in (A \cup B) - B$ であると仮定する.

〈 ここに「$x \in A$」の証明を書く 〉

したがって，$(A \cup B) - B \subseteq A$ が成立する. □

同値変形 (1)：論理操作

操作前

使える性質 (仮定)	導く性質 (目標)
$x \in (A \cup B) - B$	$x \in A$

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in (A \cup B) - B$ $x \in A \cup B$ $x \notin B$	$x \in A$

推論に用いた事実：$x \in (A \cup B) - B \Leftrightarrow x \in A \cup B$ かつ $x \notin B$

同値変形 (2)：論理操作

操作前

使える性質 (仮定)	導く性質 (目標)
$x \in (A \cup B) - B$	$x \in A$

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in (A \cup B) - B$ $x \in A \cup B$ $x \notin B$ $x \in A$ または $x \in B$	$x \in A$

推論に用いた事実：$x \in A \cup B \Leftrightarrow x \in A$ または $x \in B$

同値変形：文章構造

部分集合の定義より,「任意の x に対して，$x \in (A \cup B) - B$ ならば $x \in A$」を証明すればよい.

x を任意に選ぶ.

$x \in (A \cup B) - B$ であると仮定する.

$x \in (A \cup B) - B$ より，$x \in A \cup B$ かつ $x \notin B$ である.
$x \in A \cup B$ より，$x \in A$ または $x \in B$ である.
...

したがって，$(A \cup B) - B \subseteq A$ が成立する. □

推論：論理操作

操作後

使える性質 (仮定)	導く性質 (目標)
$x \in (A \cup B) - B$ $x \in A \cup B$ $x \notin B$ $x \in A$ または $x \in B$ $x \in A$	$x \in A$

推論に用いた事実：$\neg Q \land (P \lor Q) \Rightarrow P$
(選言三段論法と呼ばれることがある)

推論：文章構造

部分集合の定義より,「任意の x に対して，$x \in (A \cup B) - B$ ならば $x \in A$」を証明すればよい.

x を任意に選ぶ.

$x \in (A \cup B) - B$ であると仮定する.

$x \in (A \cup B) - B$ より，$x \in A \cup B$ かつ $x \notin B$ である.
$x \in A \cup B$ より，$x \in A$ または $x \in B$ である.
しかし，$x \notin B$ であるため，$x \in A$ となる.

したがって，$(A \cup B) - B \subseteq A$ が成立する. □

証明完了：清書

- 部分集合の定義より,「任意の x に対して，$x \in (A \cup B) - B$ ならば $x \in A$」を証明すればよい.
- x を任意に選ぶ.
- $x \in (A \cup B) - B$ であると仮定する.
- $x \in (A \cup B) - B$ より，$x \in A \cup B$ かつ $x \notin B$ である.
- $x \in A \cup B$ より，$x \in A$ または $x \in B$ である.
- しかし，$x \notin B$ であるため，$x \in A$ となる.
- したがって，$(A \cup B) - B \subseteq A$ が成立する. □

有用な推論

三段論法（前回）

$(P \to Q) \land (Q \to R) \Rightarrow P \to R$

選言三段論法（今回）

$(P \lor Q) \land \neg P \Rightarrow Q$

モードゥス・ポネンス（前回）

$P \land (P \to Q) \Rightarrow Q$

$\land$ の除去（今回）

$P \land Q \Rightarrow P$

他のものは出て来たときに説明

目次

今日のまとめ

今日の目標

- 人間の読める証明が書けるようになる
  - 定義に基づいて書き直すこと
  - 推論に基づいて書き下すこと
- 全称命題の証明ができるようになる

なぜ証明を勉強するのか？

- 証明は論理的思考の根幹 $\rightsquigarrow$ 論理的思考の訓練
- 証明は文章（主張）$\rightsquigarrow$ 文章構造と論理構造の対応に注目

これを通して，文章を論理的に読み書きできるようになる

コミュニケーションとしての証明：補足

$(A \cup B) - B \subseteq A$ を証明するとき

例えば，次の証明は正しいか？

- x を任意に選び，$x \in (A \cup B) - B$ と仮定する．
- このとき，$x \in A$ である． $\square$

問題点

- 1 行目と 2 行目の間に，本来あるべきステップがない
- しかし，それがあれば正しい
- 「本来あるべきステップ」は書くほどのものでもない？

格言

証明は「正しく」かつ「伝わるように」書くことが重要

- 証明は書き手の主張を読み手に伝えるもの
- 「伝え方」は誰が書き手であるかによって変わる
- 「伝わり方」は誰が読み手であるかによって変わる