離散数学 University of Electro-Communications

7. ― 8.　証明法(1)-(2)

植野真臣

本授業の構成

---

1. 本日の目標

① 全称命題の証明
② 存在命題の証明
③ 背理法による証明
④ 含意「ならば」型命題の証明
⑤ 場合分けによる証明
⑥ 含意命題の否定の証明
⑦ 集合包含関係の証明
⑧ 複数量化子の命題の証明

---

1. 証明とは？

「証明」は、真理(Truth)を立証するための手法である。

証明の方法は分野によって異なる。

- 法的真理は、法廷で示される証拠と法律、陪審員、裁判官によって決定される。
- 科学的真理は、実験によって確認される。
- 哲学的真理は、厳密な論証の積み重ねによって導かれる。
- 宗教的真理は、歴史的な宗教のコミュニティにより決定される。
- 組織的真理は、権威により決定づけられる。

数学での証明の定義

定義
「証明」とは　基礎的公理(Axiom)集合から命題(Proposition)を導く論理的推論（Logical Deduction)の連鎖である。

←―
The Smartest Proof（最も　賢い証明）

再掲 ：証明の定義

Def

「証明」とは 基礎的公理(Axiom)集合から命題(proposition)を導く論理的推論（Logical Deduction)の連鎖である。

再掲：公理

Def 公理とは証明された真の命題のこと

公理の種類

1. 定理 (Theorem) 非常に重要な命題
2. 補題(Lemma) 重要な命題を証明するために必要な公理の証明
3. 系(corollary) すでに証明されている定理から容易に証明できる命題

2. 証明法

① 全称命題の証明
② 存在命題の証明
③ 背理法による証明
④ 含意「ならば」型命題の証明
⑤ 場合分けによる証明
⑥ 含意命題の否定の証明
⑦ 集合包含関係の証明
⑧ 複数量化子の命題の証明

3. 全称命題$\forall x P(x)$の証明

$\forall x \in \boldsymbol{U}[P(x)]$の証明の手順

(1) Uの不特定の要素が与えられたとする。その要素をxで表す。（数学の慣例で，全称命題の束縛変数を不特定の要素としてそのまま使う。）

(2) $P(x)$が真であることを示す。

例題

$\forall x \in \mathbb{R}[x^2 + 2x + 4 > 0]$を証明せよ。

例題

$\forall x \in \mathbb{R}[x^2 + 2x + 4 > 0]$を証明せよ。

証明

①$x \in \mathbb{R}$とする

「 $\mathbb{R}$ の不特定の要素が与えられたとし，それをxと表す」 という意味。数学では上の表現でOK。

この時点で値が入力され，自由変数でなくなっていることが重要。自由変数はまだ値が得られていないことを示すのでそのままでは述語は命題にはなっていない。

例題

$\forall x \in \mathbb{R}[x^2 + 2x + 4 > 0]$を証明せよ。
証明
①$x \in \mathbb{R}$とする.
②$x^2 + 2x + 4 = x^2 + 2x + 1 + 3$
$= (x+1)^2 + 3$
$x \in \mathbb{R}$より,
$(x+1)^2 \geq 0$
従って, $x^2 + 2x + 4 \geq 3 > 0$
以上より, $\forall x \in \mathbb{R}[x^2 + 2x + 4 > 0]$ ■

数学的帰納法

$\forall n \in \mathbb{N}$に関する全称命題の証明法。

(1) $P(1)$ は真である
(2) $\forall n \in \mathbb{N}[P(n) \rightarrow P(n+1)]$が真である。
の両方が成り立っていれば
$\forall n \in \mathbb{N}[P(n)]$が真である。

数学的帰納法については、「証明法」の最後で詳しく学ぶ。

4. 存在命題$\exists x P(x)$の証明

$\exists x \in \boldsymbol{U}[P(x)]$の証明の手順

(1) 条件$P(x)$を満たすUの要素aを見つける。
(2) $P(a)$が真であることを示す。

例題1

$\exists x \in \mathbb{R}[x^2 - 4x + 1 < 0]$を証明せよ。

例題1

$\exists x \in \mathbb{R}[x^2 - 4x + 1 < 0]$を証明せよ。
証明
$\mathbb{R}$の要素1について, $1^2 - 4 \times 1 + 1 = -2 < 0$
である。従って、
$\exists x \in \mathbb{R}[x^2 - 4x + 1 < 0]$ ■

例題1

$\exists x \in \mathbb{R}[x^2 - 4x + 1 < 0]$を証明せよ。
証明
$\mathbb{R}$の要素1について, $1^2 - 4 \times 1 + 1 = -2 < 0$
である。従って、
$\exists x \in \mathbb{R}[x^2 - 4x + 1 < 0]$ ■

注）$x = 1$はどこから出てきたのかをいちいち説明する必要はない。

例題2

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$を証明せよ。

例題2

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$を証明せよ。

証明

$x^2 - 5x + 6 = (x-2)(x-3)$なので$2 < x < 3$を満たす$\mathbb{R}$の要素は$x^2 - 5x + 6 < 0$を満たす。従って，

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$ ■

例題2

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$を証明せよ。

証明

$x^2 - 5x + 6 = (x-2)(x-3)$なので$2 < x < 3$を満たす$\mathbb{R}$の要素は$x^2 - 5x + 6 < 0$を満たす。従って，

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$ ■

注）「$\mathbb{R}$の要素が$2 < x < 3$を満たせば$x^2 - 5x + 6 < 0$を満たす」ことを述べているだけで，そのような$\mathbb{R}$の要素が存在するかどうかについては何も示していない。

例題2

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$を証明せよ。

証明

$x^2 - 5x + 6 = (x-2)(x-3)$なので$2 < x < 3$を満たす$\mathbb{R}$の要素は$x^2 - 5x + 6 < 0$を満たす。従って，

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$ ■

誤り証明のわかりやすい補足のための変形問題

$\exists x \in \mathbb{N}[x^2 - 5x + 6 < 0]$を証明せよ。

証明

$x^2 - 5x + 6 = (x-2)(x-3)$なので$2 < x < 3$を満たす$\mathbb{N}$の要素は$x^2 - 5x + 6 < 0$を満たす。従って，$\exists x \in \mathbb{N}[x^2 - 5x + 6 < 0]$ ■

注）「$\mathbb{N}$の要素が$2 < x < 3$を満たせば$x^2 - 5x + 6 < 0$を満たす」ことを述べているだけで，そのような$\mathbb{N}$の要素が存在するかどうかについては何も示していない。そのため、実際に存在もしないのに誤った結果を導いている。

例題2

$\exists x \in \mathbb{R}[x^2 - 5x + 6 < 0]$を証明せよ。

証明

$x^2 - 5x + 6 = (x-2)(x-3)$だから，$2 < x < 3$のとき，$x^2 - 5x + 6 < 0$が成り立つ．このとき，実数$\frac{5}{2}$は$x$についての条件$2 < x < 3$を満たす．よって，

$x^2 - 5x + 6 \geq 0$ を満たさない実数$\frac{5}{2}$が存在する．

したがって，「すべての実数xについて$x^2 - 5x + 6 \geq 0$」は偽である． ■

($\frac{5}{2}$がどこから出てきたかを説明する必要はない)

離散数学 University of Electro-Communications

5. 背理法

存在命題$\exists x[P(x)]$で「 $P(x)$ を満たすx を見つける」ことは正攻法である。しかし、そのようなxを見つけるのが難しい場合がある。そのような場合は背理法を用いる。

25

離散数学 University of Electro-Communications

背理法の手順

（1） 「 $P(x)$を背理法で証明する」と書く。
（2） 「 $\neg P(x)$ を仮定する」と書く。
（3） その結果、矛盾があることを導く。
（4） 「これは矛盾である。ゆえに， $P(x)$ が証明された。」と書く。

26

離散数学 University of Electro-Communications

例題1

素数が無限にあることを証明せよ。

27

離散数学 University of Electro-Communications

例題1

素数が無限にあることを背理法で証明せよ。

証明

背理法で証明する。素数が有限個しかないと仮定する。
その個数をn個とし，すべての素数を小さい順にならべ，
それらを $p_1, p_2, \cdots, p_n$とする。このとき、p_nは最大の素数である。… ①
このとき， $Q = p_1 \times p_2 \times \cdots \times p_n$+1という数$Q$を考える。
すると，Qの形より，どの素数$(p_1, p_2, \cdots, p_n)$でわっても
1あまるからQは素数である。
また，①より，最大の素数より大きいからQは素数ではない。
これは矛盾である。ゆえに，素数が無限にあるが証明された。

■ 28

離散数学 University of Electro-Communications

例題2

$\sqrt{2}$が無理数であることを証明せよ。

Def.

有理数の定義：有理数は，

$$\frac{n}{m}$$

と書ける数。ただし，互いに素な $n \in \mathbb{Z}, m(\neq 0) \in \mathbb{Z}$.

29

離散数学 University of Electro-Communications

例題2 $\sqrt{2}$が無理数であることを証明せよ。

[証明]

背理法で証明する。$\sqrt{2}$が有理数であると仮定する。

$$\sqrt{2} = \frac{n}{m} \quad \cdots ①$$

と書ける。ただし，$\sqrt{2} > 0$より、n、mは互いに素な1以上の自然数。①の両辺を二乗すると，

$2 = \frac{n^2}{m^2}$ より， $2m^2 = n^2 \cdots$ ②

これより、nは偶数。$n = 2k, k \in \mathbb{N}$とかける 。
②に代入すると ，$2m^2$=$4k^2$ よりm^2=$2k^2$ … ③
これより，mは偶数。n、mはともに偶数であり，互いに素な自然数の仮定に矛盾する。ゆえに， $\sqrt{2}$は 無理数である。

■ 30

6. 含意型命題$\forall x \in \boldsymbol{U}\ [P(x) \to Q(x)]$ の証明

含意型命題証明の手順
これは全称命題の一つであるので
（1） Uの要素xが$P(x)$を満たすと仮定する。
(2) $Q(x)$が真であることを示す。

例題1

$\forall x \in \mathbb{R}\ [x > 4 \to x^2 > 3]$を証明せよ。

例題1

$\forall x \in \mathbb{R}\ [x > 4 \to x^2 > 3]$を証明せよ。
[証明]
①実数xが$x > 4$を満たすと仮定する。
②$4 > 0$および実数の法則より，$x^2 > 16$である。
$16 > 3$より，$x^2 > 3$である。
従って，
$\forall x \in \mathbb{R}\ [x > 4 \to x^2 > 3]$ ■

例題2

$\forall x \in \mathbb{R}\ [x^2 - 5x + 6 = 0 \to x = 2 \lor x = 3]$を証明せよ。

例題2

$\forall x \in \mathbb{R}\ [x^2 - 5x + 6 = 0 \to x = 2 \lor x = 3]$を証明せよ。
[証明]
①実数xが$x^2 - 5x + 6 = 0$を満たすと仮定する。
②$x^2 - 5x + 6 = (x-2)(x-3) = 0$
xは実数なので， $x - 2 = 0$または$x - 3 = 0$となる。
従って， $x = 2$または$x = 3$となる。
$\forall x \in \mathbb{R}\ [x^2 - 5x + 6 = 0 \to x = 2 \lor x = 3]$ ■

7． $\forall x \in \boldsymbol{U}[\neg P(x) \lor Q(x)]$の証明と場合分け

$\forall x\ [P(x) \to Q(x)]$は$\forall x\ [\neg P(x) \lor Q(x)]$と同値であるので，その証明を考える。
$\forall x \in \boldsymbol{U}[\neg P(x) \lor Q(x)]$の手順
（1） Uの要素xが$P(x)$を満たす場合と満たさない場合に分ける。
(2) それぞれの場合で$\neg P(x) \lor Q(x)$が真であることを示す。

例題

$\forall x \in \mathbb{R}\,[\neg\{x|x>3\} \vee \{x|x^2>3\}]$を証明せよ。

例題

$\forall x \in \mathbb{R}\,[\neg\{x|x>3\} \vee \{x|x^2>3\}]$を証明せよ。

証明

(1)　$x \leq 3$のとき

$\neg\{x|x>3\}$は真となり，$\neg\{x|x>3\} \vee \{x|x^2>3\}$は真。

(2)　$x>3$のとき

$3>0$および実数の法則より，$x^2>9$である。

$9>3$より，$x^2>3$である。

$\{x|x^2>3\}$は真となり，$\neg\{x|x>3\} \vee \{x|x^2>3\}$は真。

以上より、$\forall x \in \mathbb{R}\,[\neg\{x|x>3\} \vee \{x|x^2>3\}]$　■

問

$\forall x\,[P(x) \to Q(x)]$と$\forall x\,[\neg P(x) \vee Q(x)]$

は同じことを証明している。

どちらの証明がよいか？

$\forall x\,[P(x) \to Q(x)]$と$\forall x\,[\neg P(x) \vee Q(x)]$の証明の違い

4．3　含意型命題$\forall x\,[P(x) \to Q(x)]$

では、(2)　$x>2$のとき、すなわち、$P(x)$が真のときのみを証明。

場合分けで$P(x)$が偽のとき、$\neg P(x)$は真になるので$\neg P(x) \vee Q(x)$は必ず真になる。

なので、その証明を省略して、$P(x)$が真のときのみを扱っているのが含意型命題$\forall x\,[P(x) \to Q(x)]$。

基本的に同値関係。

注意

ただし、含意型の否定の場合には

$\forall x\,[\neg P(x) \vee Q(x)]$　が使える。

8．含意型命題$\forall x \in \boldsymbol{U}[P(x) \to Q(x)]$の否定

$\neg[\forall x \in \boldsymbol{U}[P(x) \to Q(x)]] \Leftrightarrow$

$\neg[\forall x \in \boldsymbol{U}[\neg P(x) \vee Q(x)]] \Leftrightarrow$

$[\exists x \in \boldsymbol{U}[P(x) \wedge \neg Q(x)]]$

「$P(x)$を満たし、かつ$Q(x)$を満たさない$x \in \boldsymbol{U}$が存在すること」を証明すればよい。結局，存在命題の証明に帰着する。

$\forall x \in \boldsymbol{U}[P(x) \to Q(x)]$の否定の証明の手順

(1)　$P(x)$を満たし、かつ$Q(x)$を満たさない$\boldsymbol{U}$の要素xを見つける。

(2)　$P(x) \wedge \neg Q(x)$　が真であることを証明する。

例

$\neg[\forall x \in \mathbb{R}\ [x^2 > 9 \rightarrow x > 3]]$を証明せよ。

例

$\neg[\forall x \in \mathbb{R}\ [x^2 > 9 \rightarrow x > 3]]$を証明せよ。
証明
（まず$x^2 > 9 \wedge x < 3$となるxを見つける:-4）
$\mathbb{R}$の要素-4は，$x^2 = 16 > 9$であるが，-4> 3でない。
従って，$\forall x \in \mathbb{R}\ [x^2 > 9 \rightarrow x > 3]$は偽で
$\neg[\forall x \in \mathbb{R}\ [x^2 > 9 \rightarrow x > 3]]$が成り立つ。 ■

9. 対偶命題の証明

含意型命題$\forall x\ [P(x) \rightarrow Q(x)]$
はその対偶　$\forall x\ [\neg Q(x) \rightarrow \neg P(x)]$
と同値である。
ときには，含意型命題$\forall x\ [P(x) \rightarrow Q(x)]$
の証明よりも
その対偶命題
$$\forall x\ [\neg Q(x) \rightarrow \neg P(x)]$$
の証明が簡単な場合がある。

対偶命題$\forall x \in \boldsymbol{U}\ [\neg Q(x) \rightarrow \neg P(x)]$の証明手順

(1)「対偶を証明する」と書き，命題の対偶を書く。
(2) 4.3.含意型命題証明の手順
　(2.1) Uの要素xが$\neg Q(x)$を満たすと仮定する。
　(2.2) $\neg P(x)$が真であることを示す。

例題

$\forall r \in \mathbb{R}^+\ [r \notin \mathbb{Q} \rightarrow \sqrt{r} \notin \mathbb{Q}]$を証明せよ。

例題

$\forall r \in \mathbb{R}^+[r \notin \mathbb{Q} \rightarrow \sqrt{r} \notin \mathbb{Q}]$を証明せよ。
証明
対偶$\forall r \in \mathbb{R}^+[\sqrt{r} \in \mathbb{Q} \rightarrow r \in \mathbb{Q}]$を証明する。
$\sqrt{r} \in \mathbb{Q}$が存在すると仮定する。このとき，
$$\sqrt{r} = \frac{a}{b}$$
を満たす$a \in \mathbb{N}$，0でない$b \in \mathbb{N}$が存在する。
両辺を二乗すると　$r = \frac{a^2}{b^2}$
このとき，$a^2 \in \mathbb{N}, b^2 \in \mathbb{N}$となり，$r \in \mathbb{Q}$である。
従って，$\forall r \in \mathbb{R}\ [r \notin \mathbb{Q} \rightarrow \sqrt{r} \notin \mathbb{Q}]$ ■

10. 集合包含関係$A \subset B$の証明

$A \subset B$は

$$\forall x \in U\ [x \in A \to x \in B]$$

と同値。
従って，含意型命題と同じ手順により証明する。
証明の手順
(1) Uの要素xが$x \in A$を満たすと仮定する。
(2) $x \in B$が真であることを示す。

例題1.

$S = \{x \in \mathbb{R} | x > 2\}, T = \{x \in \mathbb{R} | x^2 > 2\}$とする。
$S \subset T$を証明せよ。

例題1.

$S = \{x \in \mathbb{R} | x > 2\}, T = \{x \in \mathbb{R} | x^2 > 2\}$とする。
$S \subset T$を証明せよ。
証明
$x \in \mathbb{R}$が$x > 2$を満たすと仮定する。
xは正の実数であるので，
両辺を二乗して$x^2 > 4$を満たす。$4 > 2$より，$x^2 > 2$となり，$x \in T$。
従って，$\forall x \in R\ [x \in S \to x \in T]$，$S \subset T$が証明される。

■

例題2

$\mathbb{N}$の要素$\mathrm{n} \geq 1$に対し，集合A_nを$A_n = \left\{x \in \mathbb{R} | x + 1 < \frac{1}{n}\right\}$ とし，集合系$\langle A_n | n \in \mathbb{N} \rangle$を考える。
このとき，

$$\bigcup_{n=1}^{\infty} A_n = \{x | \exists n (x + 1 < \frac{1}{n})\} = \{x | x < 0\}$$

を証明せよ。

例題2

$\mathbb{N}$の要素$\mathrm{n} \geq 1$に対し，集合A_nを$A_n = \left\{x \in \mathbb{R} | x + 1 < \frac{1}{n}\right\}$ とし，集合系$\langle A_n | n \in \mathbb{N} \rangle$を考える。
このとき，

$$\bigcup_{n=1}^{\infty} A_n = \{x | \exists n (x + 1 < \frac{1}{n})\} = \{x | x < 0\}$$

を証明せよ。
[証明]
$x \in \mathbb{Z}$が$x \in \bigcup_{n=1}^{\infty} A_n$を満たすと仮定する。
$\bigcup_{n=1}^{\infty} A_n = \left\{x \middle| \exists n \left(x + 1 < \frac{1}{1}\right)\right\} = \left\{x \middle| x < \frac{1}{1} - 1\right\}$=$\{x | x < 0\}$.

■

例題2

$\mathbb{N}$の要素$\mathrm{n} \geq 1$に対し，集合A_nを$A_n = \left\{x \in \mathbb{Z} | -5 < x + 1 < \frac{1}{n}\right\}$ とし，集合系$\langle A_n | n \in \mathbb{N} \rangle$を考える。このとき， $\bigcup_{n=1}^{\infty} A_n = \{x | \exists n (-5 < x + 1 < \frac{1}{n})\} = \{x | -5, -4, -3, -2, -1\}$ を証明せよ。
証明の方針::集合の相等の定義に戻れ。$A = B \Leftrightarrow A \subset B \land B \subset A$

離散数学 University of Electro-Communications

例題2

$\mathbb{N}$の要素$n \geq 1$に対し，集合A_nを$A_n = \left\{x \in \mathbb{Z} | -5 < x + 1 < \frac{1}{n}\right\}$ とし，集合系$\langle A_n | n \in \mathbb{N} \rangle$を考える。このとき， $\bigcup_{n=1}^{\infty} A_n = \{x | \exists n(-5 < x + 1 < \frac{1}{n})\} = \{x | -5, -4, -3, -2, -1\}$ を証明せよ。

証明の方針::集合の相等の定義に戻れ。$A = B \Leftrightarrow A \subset B \land B \subset A$

[証明]

(1) $x \in \mathbb{Z}$が$x \in \bigcup_{n=1}^{\infty} A_n$を満たすと仮定する。

$\bigcup_{n=1}^{\infty} A_n = \left\{x \middle| \exists n \left(-5 < x + 1 < \frac{1}{n}\right)\right\} = \left\{x \middle| -5 - 1 < x < \frac{1}{1} - 1\right\}.$

従って$\bigcup_{n=1}^{\infty} A_n \subset \{x | -5, -4, -3, -2, -1\}.$

(2) $x \in \mathbb{Z}$が$x \in \{x | -5, -4, -3, -2, -1\}$を満たすと仮定する。

$-5, -4, -3, -2, -1$は,すべて$\bigcup_{n=1}^{\infty} A_n = \left\{x \middle| \exists n \left(-5 < x + 1 < \frac{1}{n}\right)\right\}$の要素を満たす。従って$\bigcup_{n=1}^{\infty} A_n \supset \{x | -5, -4, -3, -2, -1\}.$

(1)(2)より $\bigcup_{n=1}^{\infty} A_n = \{x | -5, -4, -3, -2, -1\}$ ■

55

離散数学 University of Electro-Communications

例題3

$S = \{x \in \mathbb{R} | x > 3\}, T = \{x \in \mathbb{R} | x^2 > 3\}$とする。
$T \not\subset S$を証明せよ。

56

離散数学 University of Electro-Communications

例題3

$S = \{x \in \mathbb{R} | x > 3\}, T = \{x \in \mathbb{R} | x^2 > 3\}$とする。
$T \not\subset S$を証明せよ。

定義に戻れ

$T \subset S \Leftrightarrow [\forall x[x \in T \rightarrow x \in S]]$

$T \not\subset S \Leftrightarrow \neg[\forall x[x \in T \rightarrow x \in S]]$

57

離散数学 University of Electro-Communications

例題3

$S = \{x \in \mathbb{R} | x > 3\}, T = \{x \in \mathbb{R} | x^2 > 3\}$とする。
$T \not\subset S$を証明せよ。

[証明]

$T \not\subset S \Leftrightarrow \neg[\forall x[x \in T \rightarrow x \in S]] \Leftrightarrow$
$\neg[\forall x[x \in T \rightarrow x \in S]]$の証明なので
$\exists x[x \in T \land x \notin S]$を証明すればよい。
$\mathbb{R}$の要素$x = -2$は，$(-2)^2 = 4 > 3$なので
$x \in T$。しかし，$-2<3$なので$x \notin S$。
従って，$\exists x[x \in T \land x \notin S]$となり，$T \not\subset S$ ■

58

離散数学 University of Electro-Communications

11. 2変数以上の述語と入れ子になった量化子

$(x, y) \in U \times V$のとき，$P(x, y)$の真理集合は
$\{(x, y) | P(x, y)\}$
で$U \times V$の部分集合になる。

まず，2変数以上の演算に慣れよう！！

59

離散数学 University of Electro-Communications

例題1

自由変数$x, y \in \mathbb{N}$についての述語「$x + y < 5$」を$P(x, y)$で表す。$P(x, y)$の真理集合$\{(x, y) | P(x, y)\}$を求めよ。

60

例題1

自由変数$x, y \in \mathbb{N}$についての述語「$x + y < 5$」を$P(x, y)$で表す。$P(x, y)$の真理集合$\{(x, y) | P(x, y)\}$を求めよ。

$P(x, y)$の真理集合
$\{(x, y) | P(x, y)\}$は$\mathbb{N}^2$の部分集合で,
$\{(x, y) | P(x, y)\} = \{(x, y) | x + y < 5\}$
$= \{(0,1), (0,2), (0,3), (0,4), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (3,0), (3,1), (4,0)\}$

例題2

$x, y, t \in \mathbb{R}$, 自由変数x, yについての述語「$2x - y = 0$」を$Q(x, y)$で表す。$Q(x, y)$の真理集合$\{(x, y) | Q(x, y)\}$を求めよ。

例題2

$x, y, t \in \mathbb{R}$, 自由変数x, yについての述語「$2x - y = 0$」を$Q(x, y)$で表す。$Q(x, y)$の真理集合$\{(x, y) | Q(x, y)\}$を求めよ。

[解答]

$Q(x, y)$の真理集合
$\{(x, y) | Q(x, y)\}$は$\mathbb{R}^2$の部分ベクトル空間で,
$\{(x, y) | Q(x, y)\}$
$= \{(x, y) | \exists t \in \mathbb{R} [(x, y) = t(1,2)]\}$
$= \{t(1,2) | \ t \in \mathbb{R}\}$

例題3

$x, y \ \in \mathbb{R}$, 自由変数x, yについての述語「$x + y - 1 = 0$」を$P(x, y)$, 「$x^2 + y^2 - 1 = 0$」を$Q(x, y)$で表す。$P(x, y) \land Q(x, y)$の真理集合$\{(x, y) | P(x, y) \land Q(x, y)\}$を求めよ。

例題3

$x, y \ \in \mathbb{R}$, 自由変数x, yについての述語「$x + y - 1 = 0$」を$P(x, y)$, 「$x^2 + y^2 - 1 = 0$」を$Q(x, y)$で表す。$P(x, y) \land Q(x, y)$の真理集合$\{(x, y) | P(x, y) \land Q(x, y)\}$を求めよ。

[解答]

$P(x, y) \land Q(x, y)$の真理集合
$\{(x, y) | P(x, y) \land Q(x, y)\}$は$\mathbb{R}^2$の部分集合で,
$P(x, y)$と$Q(x, y)$のx, yについての連立方程式である。$2x^2 - 2x = 0$より, $x = 0,1$, 従って、
$\{(x, y) | P(x, y) \land Q(x, y)\} = \{(1,0), (0,1)\}$

同じ量化子が続けて出てくる場合は順序は気にする必要はない！！

例1　以下の命題は互いに同値。

(1) $\forall x \in U, \forall y \in V \ [P(x, y)]$
(2) $\forall y \in V, \forall x \in U \ [P(x, y)]$
(3) $\forall (x, y) \in U \times V \ [P(x, y)]$

例2　以下の命題は互いに同値。

(1) $\exists x \in U, \exists y \in V \ [P(x, y)]$
(2) $\exists y \in V, \exists x \in U \ [P(x, y)]$
(3) $\exists (x, y) \in U \times V \ [P(x, y)]$

全称量化子と存在量化子が入れ子の場合は順序で意味が変わるので注意すべし！！

問題

$x, y \in \mathbb{R}$, 自由変数x, yについての述語「 $x \le y$」を$P(x, y)$で表す。このとき，以下の命題は真か？

(1)　$\forall x\ \exists y P(x, y)$

(2)　$\exists y \forall x P(x, y)$

全称量化子と存在量化子が入れ子の場合は順序で意味が変わるので注意すべし！！

問題

$x, y \in \mathbb{R}$, 自由変数x, yについての述語「$x \le y$」を$P(x, y)$で表す。このとき，以下の命題は真か？

(1)　$\forall x\ \exists y P(x, y)$：すべての$x$について「ある$y$について$x \le y$」。「ある$y$について$x \le y$」の真理集合は$\mathbb{R}$なので，$\forall x\ \exists y P(x, y)$ は真。

(2)　$\exists y \forall x P(x, y)$:あるyについて「すべてのxについて$x \le y$」。「すべてのxについて$x \le y$」の真理集合は$\emptyset$なので，$\forall x\ \exists y P(x, y)$ は偽。

問題

$x, y \in \mathbb{R}$, 自由変数x, yについての述語「$x \le y$」を$P(x, y)$で表す。このとき，以下の命題は真か？

[証明]

(1)　$\forall x\ \exists y P(x, y)$：

$x \in \mathbb{R}$について，$\exists y[x \le y]$を証明すればよい．$y = x + 1$とすると，$x \le y$を満たす。従って，$\forall x\ \exists y P(x, y)$　■

(2) $\exists y \forall x P(x, y)$:$\forall x[x \le y]$となるy　は存在しない。$\forall x\ \exists y P(x, y)$ は偽。　→命題の否定へ　■

12．量化子が入れ子になった命題の証明

証明の手順

- 命題を構成している最も先頭の量化子に注目する。このあとは全称命題、存在命題の証明法に従う。
- 最も先頭の量化子が全称量化子であれば、束縛変数に不特定の与えられた値(xなど）が得られたとして，内側の述語にすすむ。
- 最も先頭の量化子が存在量化子であれば、存在するとされる値を見つけ出して、束縛変数にその値を代入してから内側にすすむ。

注意）次の段階に移るときには、最も先頭の量化子が外れていて、最も先頭の量化子の対象となっていた束縛変数には値が代入されている状態であること。

例題1

自由変数$x, y \in \mathbb{R}$についての述語「 $x^2 + 2x + 1 \ge y$」を$P(x, y)$で表す。このとき，$\forall x\ \exists y P(x, y)$を証明せよ。

例題1

自由変数$x, y \in \mathbb{R}$についての述語「 $x^2 + 2x + 1 \ge y$」を$P(x, y)$で表す。このとき，$\forall x\ \exists y P(x, y)$を証明せよ。

[証明]

$x \in \mathbb{R}$とする。$x^2 + 2x + 1 \ge y$となるyを見つける。

$y = 0$とすると，$x^2 + 2x + 1 = (x + 1)^2 \ge 0$より，

$x^2 + 2x + 1 \ge y$.

すなわち，$\forall x\ \exists y P(x, y)$は真となる。　■

例題2

自由変数$x, y \in \mathbb{R}$についての述語「$x^2 + 2x + 1 \leq y$」を$P(x, y)$で表す。このとき，$\forall x\ \exists y P(x, y)$を証明せよ。

例題2

自由変数$x, y \in \mathbb{R}$についての述語「$x^2 + 2x + 1 \leq y$」を$P(x, y)$で表す。このとき，$\forall x\ \exists y P(x, y)$を証明せよ。

[証明]

$x \in \mathbb{R}$とする。さらに，$y = x^2 + 2x + 1 + 1$とする。($\exists y$は$x^2 + 2x + 1 \leq y$となるyを見つける)(この問題はyを数値で求められないので yをxの関数で求める。実はこのような方法が数学ではよく用いられる。)

このとき，$x^2 + 2x + 1 < x^2 + 2x + 1 + 1$より，$x^2 + 2x + 1 \leq y$，すなわち，$\forall x\ \exists y P(x, y)$は真となる。 ■

例題3

自由変数$x, y \in \mathbb{R}$についての述語「$y \leq x^2 + 2x + 1$」を$Q(x, y)$で表す。このとき，$\exists y \forall x Q(x, y)$を証明せよ。

例題3

自由変数$x, y \in \mathbb{R}$についての述語「$y \leq x^2 + 2x + 1$」を$Q(x, y)$で表す。このとき，$\exists y \forall x Q(x, y)$を証明せよ。

証明

$y = -1$とする。(注)このとき，なぜ-1かは説明する必要はない。)

$x \in \mathbb{R}$とする。$x^2 + 2x + 1 = (x + 1)^2 \geq 0$より，$y \leq x^2 + 2x + 1$.

すなわち，$\exists y \forall x Q(x, y)$は真となる。 ■

13. 量化子が入れ子になった述語の否定

手順

(1) 全体の外側に¬をつける。

(2) ¬を量化子の内側にいれていく。

このとき、存在量化子を全称量化子に、全称量化子を存在量化子に変えていく。

例

$\neg(\forall x\ \exists y P(x, y))$

量化子が入れ子になった述語の否定

手順

(1) 全体の外側に¬をつける。

(2) ¬を量化子の内側にいれていく。

このとき、存在量化子を全称量化子に、全称量化子を存在量化子に変えていく。

例 $\neg(\forall x\ \exists y P(x, y)) \equiv$
$\exists x \neg(\exists y P(x, y)) \equiv \exists x\ \forall y \neg P(x, y)$

例題

自由変数$x, y \in \mathbb{R}$についての述語「$y > x^2 + 2x + 1$」を$Q(x, y)$で表す。このとき，$\neg(\forall y \exists x Q(x, y))$を証明せよ。

例題

自由変数$x, y \in \mathbb{R}$についての述語「$y > x^2 + 2x + 1$」を$Q(x, y)$で表す。このとき，$\neg(\forall y \exists x Q(x, y))$を証明せよ。

[証明]

$$\neg\big(\forall y \exists x Q(x, y)\big) = \exists y \forall x [\neg Q(x, y)]$$
$$= \exists y \forall x (y \leq x^2 + 2x + 1).$$

$y = -1$とする。

$x \in \mathbb{R}$とする。$x^2 + 2x + 1 = (x+1)^2 \geq 0$より，$y \leq x^2 + 2x + 1$. すなわち，$\neg(\forall y \exists x Q(x, y))$は真となる。 ■

14. イプシロンデルタ

関数の極限
関数の連続
数列の極限
など

14. イプシロン―デルタ(関数の極限値）

Def 1

$$\lim_{x \to a} f(x) = A \Leftrightarrow$$

$\forall \varepsilon > 0, \exists \delta > 0, \forall x$

$[|x - a| < \delta \to |f(x) - A| < \varepsilon]$

14. イプシロン―デルタ(関数の極限値）

Def 1

$$\lim_{x \to a} f(x) = A \Leftrightarrow$$

$\forall \varepsilon > 0, \exists \delta > 0, \forall x$

$[|x - a| < \delta \to |f(x) - A| < \varepsilon]$

注）$\forall \varepsilon > 0, \exists \delta$, の順序は変えられない。変えれば矛盾命題になってしまう！！

証明「$\forall \varepsilon$についてδが存在する」とは、条件にあうδをεで示せばよい。そのようなδを見つける問題。

イプシロン―デルタ(関数の極限値）

1. $\forall \varepsilon > 0, \exists \delta > 0, \forall x$
$[|x - a| < \delta \to |f(x) - A| < \varepsilon]$
を証明すればよい．」と書く.

2. $\forall \varepsilon > 0$ について$|x - a| < \delta \to |f(x) - A| < \varepsilon$となる$\delta$を見つける。
このとき、$\delta < 1$という条件を入れる．十分、小さいということであり、証明に必要なテクニック。

3. $\forall \varepsilon > 0, \exists \delta > 0, \forall x$
$[|x - a| < \delta \to |f(x) - A| < \varepsilon]$ ■
と書く。

例題

数列$\lim_{x \to 1} x^2 = 1$を証明せよ。

例題

数列$\lim_{x \to 1} x^2 = 1$を証明せよ。

[証明]

$\forall \varepsilon > 0,\ \exists \delta > 0, \forall x[|x-1| < \delta \to\ |x^2-1| < \varepsilon]$を証明すればよい.

$|x-1| < \delta \Leftrightarrow 1-\delta < x < 1+\delta \Leftrightarrow (1-\delta)^2 < x^2 < (1+\delta)^2$

一方、

$|x^2-1| < \varepsilon \Leftrightarrow 1-\varepsilon < x^2 < 1+\varepsilon$ ($\varepsilon > 0$の条件を考え、条件にあうδを見つける。) より $1-\varepsilon < (1-\delta)^2, (1+\delta)^2 < 1+\varepsilon \Leftrightarrow$ $2\delta \pm \delta^2 < \varepsilon$ となるδをとればよい。$\delta < 1$とすると(パターン)

$2\delta \pm \delta^2 \leq 2\delta + \delta^2 < 2\delta + \delta = 3\delta < \varepsilon$ より$\delta = \frac{\varepsilon}{4}$とすればよい。

$\forall \varepsilon > 0, \delta = \frac{\varepsilon}{4}, |x-1| < \delta \to \forall \varepsilon > 0\ |x^2-1| < \varepsilon.$

$\lim_{x \to 1} x^2 = 1$ ■

この証明は正解 しかし、

わかりやすいかもしれないが、いつも解けるとは限らない。

なぜそのようにδを決めたかは書かない。

次ページの別解が 模範解答。

例題 模範解答

数列$\lim_{x \to 1} x^2 = 1$を証明せよ。

別解 [証明]

$\forall \varepsilon > 0,\ \exists \delta > 0, \forall x[|x-1| < \delta \to\ |x^2-1| < \varepsilon]$を証明すればよい.

$\delta = \min(\frac{\varepsilon}{3}, 1)$ とすると,（注 $\frac{\varepsilon}{3}$は本当は下の計算で求めておく, 1は1以下という条件）

$|x^2-1| = |x-1||x+1| \leq |x-1|(|x-1|+2) < \frac{\varepsilon}{3}(1+2) = \varepsilon$

従って

$\forall \varepsilon > 0, \delta = \frac{\varepsilon}{4}, |x-1| < \delta \to \forall \varepsilon > 0\ |x^2-1| < \varepsilon.$

$\lim_{x \to 1} x^2 = 1$ ■

注意：先と異なる$\frac{\varepsilon}{3}$を設定したことに注意。

なぜイプシロンーデルタが難しいか？

証明の例では、なぜ、そのδを選んだかがか書かれていない。εの条件からδを見つけるのだが、δの決め方はいろいろあってよい。∃の問題はそもそもそのような問題であった。

「δはすごく小さくて1以下という仮定」が説明なく用いられていることが多く、$\min(\frac{\varepsilon}{3}, 1)$ などと条件に書かれると意味がまったく分からなくなってしまう。

15. 良い証明のためのTips

1. 最初に証明の仕方を宣言する。Ex. ①...を証明するために背理法を用いる。②. ...を証明するために以下の場合に分ける。③ ...を証明するために数学的帰納法を用いる。
2. 独立の数式や理由をバラバラにつなぎ合わせているような証明はよくない。順序だてて、次の式や文をステップごとに導いているように構成しなければならない。
3. 多くの初心者が説明を少なくし、計算結果を長く書く。証明とは文章である。読者の立場に立ち、計算は結果のみでよく、その理由やあらすじを文章で書け。
4. よく推敲（読み直し）、なるべくシンプルに書け。
5. 長い証明は 構造化せよ。 定理 (Theorem) 、補題(Lemma) 、系 (corollary)に分解するのもよい。
6. 「～は明らか」はよく用いられる。しかし、読者にとって本当に「～は明らか」なのかを考えよ。
7. わからないのは読者のせいではない。どのようにすればわかりやすい証明になるか、読者が「確かに！」と納得してくれるかを考えよ。
8. 読者は上のような作法になれている読者であると考えて書け。

まとめ

① 全称命題の証明
② 存在命題の証明
③ 背理法による証明
④ 含意「ならば」型命題の証明
⑤ 場合分けによる証明
⑥ 含意命題の否定の証明
⑦ 集合包含関係の証明
⑧ 複数量化子の命題の証明
⑨ 証明の考え方！！

演習問題

問題1．変数$x \in \mathbb{R}$についての以下の述語が真であればそれを証明し，偽であれば否定を証明せよ。

1. $\forall x \in \mathbb{R}(x^2 - 5x + 6 = 0)$
2. $\forall x \in \mathbb{R}(x^2 - 2x + 1 > 0)$
3. $\forall x \in \mathbb{R}(x^2 - 6x + 12 > 0)$
4. $\forall x \in \mathbb{R}(x \le 1 \lor x \ge 2)$
5. $\forall x \in \mathbb{R}(x \le 1 \lor x > 1)$
6. $\exists x \in \mathbb{R}(x^2 - 5x + 6 = 0)$
7. $\exists x \in \mathbb{R}(x^2 - 2x + 1 > 0)$
8. $\exists x \in \mathbb{R}(x \ne 0 \land x^2 = 0)$

問題2　以下の述語が真であればそれを証明し，偽であれば否定を証明せよ。

1. $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}[xy = 0]$
2. $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}[xy = 1]$
3. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}[xy = 1]$
4. $\forall a, \forall b \in \mathbb{Z}, \exists c, \exists d \in \mathbb{Z}[a^2 - b^2 = cd]$
5. $\exists c, \exists d \in \mathbb{Z}, \forall a, \forall b \in \mathbb{Z}[a^2 - b^2 = cd]$
6. $\forall x \in \mathbb{R}[x^2 > 9 \to x > 3]$

問題3　次の命題を証明せよ。

1. $\forall x \in \mathbb{R}[x > 4 \to x^2 > 16]$
2. $\forall x \in \mathbb{R}[x^2 - 3x + 2 = 0 \to x = 1 \lor x = 2]$
3. $\forall x, \forall y \in \mathbb{R}[xy = 1 \leftrightarrow \exists t \in \mathbb{R}(x = t \land y = \frac{1}{t} \land t \ne 0)]$
4. $\forall a, \forall b, \forall \varepsilon (> 0) \in \mathbb{R}[a < b + \varepsilon \to a \le b]$
(ヒント：対偶を用いよ)
5. $\forall a, \forall b, \forall \varepsilon (> 0) \in \mathbb{R}[a \le b \to a < b + \varepsilon]$
(ヒント：背理法を用いよ)

問題 4 以下を証明せよ

1. 任意の集合A,Bに対して $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$
2. 任意の集合A,B,Cに対して $(A \cup B) \times C = (A \times C) \cup (B \times C)$
3. 任意の集合A,Bに対して$A \cup (B - A) = A \cup B$
4. 任意の集合A,B,Cに対して $A - (B \cup C) = (A - B) \cap (A - C)$
5. 任意の集合A,B,Cに対して $\left(A \cap (C - B)\right) \times \left(B \cap (C - A)\right) = (A \times B) \cap ((C - B) \times (C - A))$

問題5. 変数$x, y \in \mathbb{R}$について「$x \leq y$」を$P(x, y)$, 「$x^2 - y = 0$」を$Q(x, y)$とかく。以下が真であればそれを証明し，偽であれば否定を証明せよ。

(1) $P(1, y)$, (2) $P(x, 3)$, (3) $Q(-2,4)$, (4) $Q(x, 2)$,
(5) $\exists x Q(x, y)$, (6)$\exists y Q(x, y)$, (7)$\forall x P(x, y)$,
(8) $\exists x P(x, y)$, (9) $\forall y \exists x Q(x, y)$, (10) $\forall x \exists y Q(x, y)$,
(11) $\exists y \forall x P(x, y)$, (12) $\forall y \exists x P(x, y)$

問題6. 次の述語を証明せよ

(1) $\forall y \exists x [x^3 = y]$
(2) $\exists y \forall x [x^2 \neq y]$
(3) $x \neq y \rightarrow x^3 \neq y^3$
(4) $\forall z \ \exists y [x \geq y \rightarrow \sqrt[3]{x} > z]$
(5) $\forall z \forall y \exists x [(x > y) \wedge (x \sin x > z)]$
(6) $y > 0 \rightarrow \exists x [(x < y) \wedge (2x > y)]$

問題7

$\sqrt{2}$が無理数であることを使って，$\sqrt{2} + 3$が無理数であることを証明せよ。

問題8 以下の命題を証明せよ。

(1) $ax^2 + bx + c = 0$, かつ　$a \neq 0$ならば、

$$x = \left(-b \pm \sqrt{b^2 - 4ac}\right)/2a$$

(2) nが2以上の奇数ならば、nは二つの素数の和で示される
(3) $0 \leq x \leq 2$ならば、$-x^3 + 4\mathrm{x} + 1 > 0$

問題9

$\mathbb{C}$を普遍集合とする。$S = \{z | z^7 - 1 = 0\}, T = \{z | z^8 - Z = 0\}$とおく。
(1) $S \subset T$を証明せよ。
(2) $T \not\subset S$を証明せよ。

問題10

Def「 $x \in A \rightarrow x \leq r$ 」が成り立つとき，rはAの上界である。
を用いて以下の命題を証明せよ。

$$B = \{x | x \in \mathbb{R}, x < 2\}$$

「3はB の上界である」。
注1）Bは最大値を持っていない。しかし、上界を持つ。
注2）Aが上界を持つとき,「 A は上に有界である」という。

問題11

Def　集合Aと$r \in \mathbb{R}$について,「 r がAの上界であり, かつ「 y がAの上界ならば$y \geq r$である」とき, rはAの上限である」という。注: r がAの最小の上界であるとき, rはAの上限である。

問い: $B = \{x | x \in \mathbb{R}, x < 2\}$

のとき､「2はB の上限である」｡を証明せよ。

ヒント　対偶: 「$\mathrm{y} < 2$ならばyはBの上界でない」--→ $\mathrm{y} < 2 \rightarrow \exists x[x \in B \wedge x > y]$」を用いよ。

-→ $\mathrm{y} < 2$を仮定し, $x = \frac{y+2}{y}$とおけ。

問題12

$\mathbb{R}$の部分集合Dを$D = \{x | 1 \leq x \wedge x < 2\}$とする。2は$D$の上限であることを証明せよ。

問題13

Def

$\forall r \in \mathbb{R}, \exists n \in \mathbb{N}[m > n \rightarrow f(m) > r]$ が成り立つとき,「 $\mathbb{N} \rightarrow \mathbb{R}$の関数$f$は正の無限大に発散する」という。

問

$$f: \mathbb{N} \rightarrow \mathbb{R}, f(n) = \sqrt{n}$$
$$g: \mathbb{N} \rightarrow \mathbb{R}, g(n) = (-1)^n \sqrt{n}$$

(a)関数 f は正の無限大に発散することを証明せよ。

(b)関数gは正の無限大に発散しないことを証明せよ。