現代数学の流れ　第1回

この授業で学ぶもの

- 集合論の基礎 ← 現代数学の基礎
- 代数学の基礎（群，環，体）← 数理学科では3年次に学ぶ
- 暗号理論（代数学の応用）← オンラインショッピングなどで使われている
- 楕円曲線（数論幾何の導入）← 最先端の数学に触れる

集合論

… 現代数学の基礎

全ての数学は集合論を元に記述されている．

集合 … ものの集まり，数の集まり．

・集合の定義ははっきり定まっていないといけない．

集合 … 自然数全体の集合，整数全体の集合 ok
1以上の実数全体の集合

集合でない集まり … 髪の毛が黒い人の集合 ×
カッコイイ車の集合

集合 A を構成する一つ一つのものを元，または要素という．

a が A の元のとき，$a \in A$，$A \ni a$ と書く．

a が A の元でないとき，$a \notin A$ $A \not\ni a$ などと書く．

例

$\mathbb{N}$: 自然数全体の集合．

$\mathbb{Z}$: 整数全体の集合

$\mathbb{Q}$: 有理数全体の集合

$\mathbb{R}$: 実数全体の集合

$\mathbb{C}$: 複素数全体の集合

$3 \in \mathbb{N}$ $\quad 5 \in \mathbb{N}$ $\quad -1 \notin \mathbb{N}$ $\quad \frac{1}{2} \notin \mathbb{N}$

$-1 \in \mathbb{Z}$ $\quad -5 \in \mathbb{Z}$ $\quad \frac{1}{2} \notin \mathbb{Z}$ $\quad \frac{3}{2} \notin \mathbb{Z}$

$\frac{1}{2} \in \mathbb{Q}$ $\quad -\frac{3}{2} \in \mathbb{Q}$ $\quad \pi \notin \mathbb{Q}$ $\quad \sqrt{2} \notin \mathbb{Q}$

$\pi \in \mathbb{R}$ $\quad \sqrt{2} \in \mathbb{R}$ $\quad \sqrt{-1} \notin \mathbb{R}$ $\quad 1+2\sqrt{-1} \notin \mathbb{R}$

$\sqrt{-1} \in \mathbb{C}$ $\quad 1+2\sqrt{-1} \in \mathbb{C}$.

例 A: 素数全体の集合

$2, 3, 5, 7 \in A$ $\quad 4, 6, 8, 9 \notin A$.

2つの集合 A, B がまったく同じ要素からなるとき、

A と B は同じ集合であるとみなし、$A=B$ と書く。

$A=B$ でないとき、$A \neq B$ と書く。

例　A : $(x-1)(x-2)(x-3)=0$ の根全体の集合、

B : 1, 2, 3 からなる集合。

このとき、$A=B$ がいえる。

集合の表し方

a, b, c からなる集合を

$$\{a, b, c\} = \{b, a, c\} = \{c, b, a\}$$

などと書く。

例 $\{3, 5, 11\}$, $\{1, 4, 8, 100\}$

元の個数が多いとき、全ての元を書くことは不可能

そこで条件 P をみたす x の集合を

$$\{x \mid x \text{ は } P \text{ を満たす}\}$$

などと書く。

例 $\mathbb{N} = \{x \mid x \text{ は自然数}\}$

$\mathbb{Z} = \{x \mid x \text{ は整数}\}$

$\mathbb{Q} = \left\{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ かつ } q \neq 0\right\}$

$\mathbb{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}$

集合Aの中で条件Pをみたすxの集合を

$$\{x \in A \mid x\text{は}P\text{を満たす}\}$$

と書く。

例

$$A = \{x \in \mathbb{N} \mid x \leq 10000\}$$

$$B = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$$

このようにしたとき、集合

$$\{x \in \mathbb{R} \mid x^2 + 1 = 0\}$$

は元を持たない。そこで元を一つも持たない集合て
空集合と呼び、ϕと書く

つまり、$\{x \in \mathbb{R} \mid x^2+1 = 0\} = \phi$

がいえる。

元を有限個しか持たない集合を有限集合という.

例　$\{1, 2, 3, 4, 5\}$　　$\{x \in \mathbb{N} \mid x \leq 100\}$

$\{x \in \mathbb{Z} \mid -100 \leq x \leq 100\}$

無限個の元からなる集合を無限集合という.

例　$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

$$A = \{x \in \mathbb{R} \mid -1 \leq x \leq 2\}$$

2つの集合 A, B について 集合 A のどの元も B に含まれるとき.

つまり,　$x \in A \Rightarrow x \in B$

が成り立つとき. A は B に含まれる, または B は A を含む ~~という~~ という.

また A は B の部分集合であるという. $A \subset B$, $B \supset A$ と書く.

~~$A \not\subset B$~~　$A \subset B$ でないとき.　$A \not\subset B$ と書く.

$A\subset B$ かつ $A\neq B$ のとき，A は B の真部分集合といい，$A\subsetneq B$ と書く．

例　$\mathbb{N}\subsetneq\mathbb{Z}\subsetneq\mathbb{Q}\subsetneq\mathbb{R}\subsetneq\mathbb{C}$.

この記号を用いると，

$$A=B \iff A\subset B \text{ かつ } B\subset A$$

が言える．また，

$$A\subset B,\ B\subset C \Rightarrow A\subset C$$

もいえる．任意の集合 A について $\phi\subset A$ が言える．

集合 A の部分集合全体の集合

$$\{B \mid B\subset A\}$$

を $\mathfrak{P}(A)$ と表し，A のべき集合という．

例 $A = \{1, 2, 3\}$

$\mathcal{P}(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$

集合 A が n 個の元からなるとき、$\mathcal{P}(A)$は 2^n 個の元からなる。

どの元も集合であるような集合を集合族という

例 $a, b \in \mathbb{R}$ $(a < b)$

$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$

$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$

例 $\{[-n, n] \mid n \in \mathbb{N}\}$

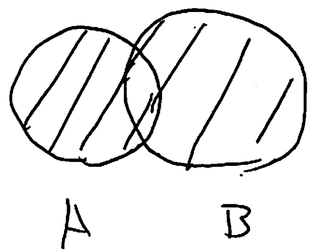
$\{[0, x) \mid x \in \mathbb{R},\ x > 0\}$

集合の演算

2つの集合A, Bの元全てを ~~集合~~ 集めてできた集合をAとBの和集合といい、

$A \cup B$ と表す。つまり、

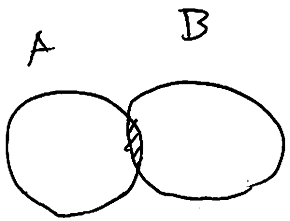
$$A \cup B = \{ x \mid x \in A \text{ または } x \in B \}$$



AとBの両方に含まれる元を集めた集合をAとBの共通部分といい、

$A \cap B$ と表す。つまり、

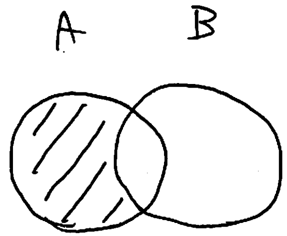
$$A \cap B = \{ x \mid x \in A \text{ かつ } x \in B \}$$



Aに含まれてBに含まれない元の集合をAとBの差集合といい、

A \ Bと表す。つまり

$$A \setminus B = \{x \mid x \in A \text{ かつ } x \notin B\}$$



AとBの共通部分が空でないとき、AとBは交わるという。

$A \cap B = \phi$ のとき、 $A \cup B$ を $A \sqcup B$ と表す。

AとBの非交和という。

例 $A = \{1, 2, 3, 4, 5, 6\}$ $B = \{4, 5, 6, 7, 8, 9\}$

$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$A \cap B = \{4, 5, 6\}$

$A \setminus B = \{1, 2, 3\}$

$B \setminus A = \{7, 8, 9\}$

命題1 集合 A, B について以下が成り立つ.

(1) $A \subset A \cup B$ (2) $B \subset A \cup B$ (3) $A \cup B = B \cup A$

(4) $A \cap B \subset A$ (5) $A \cap B \subset B$ (6) $A \cap B = B \cap A$

(証) (1) $x \in A$ とする.

このとき $x \in A$ が成り立つので, $x \in A$ または $x \in B$ も成り立つ.

$\therefore x \in A \cup B$.

(3) $x \in A \cup B \Rightarrow x \in A$ または $x \in B$

$\Rightarrow x \in B$ または $x \in A$

$\Rightarrow x \in B \cup A$.

$\therefore \quad A \cup B \subset B \cup A$

$B \cup A \subset A \cup B$ も同様

$\therefore \quad A \cup B = B \cup A$ //

命題2　集合 A, B, C, D について

(1) $A \subset C$ かつ $B \subset C \Rightarrow A \cup B \subset C$

(2) $D \subset A$ かつ $D \subset B \Rightarrow D \subset A \cap B$

 (1) $x \in A \cup B \Rightarrow x \in A$ または $x \in C$

$x \in A$ のとき $A \subset C$ より $x \in C$

$x \in B$ のとき $B \subset C$ より $x \in C$

$\therefore \quad x \in A$ または $x \in B \Rightarrow x \in C \quad \therefore A \cup B \subset C$

(2) $x \in D$ のとき.

$D \subset A$ より, $x \in A$

$D \subset B$ より, $x \in B$

$x \in D \Rightarrow x \in A$ かつ $x \in B$

$\Rightarrow x \in A \cap B$

$\therefore D \subset A \cap B$. //

2つの ~~定理~~ 命題 より. $A \cup B$ は A と B を含む集合のうち最小.

$A \cap B$ は A と B に含まれる集合のうち最大

命題3 (結合法則)

(1) $(A \cup B) \cup C = A \cup (B \cup C)$

(2) $(A \cap B) \cap C = A \cap (B \cap C)$

(二) 省略

命題3より、 $(A \cup B) \cup C$ などを $A \cup B \cup C$ と書いて良い

$A \cap (B \cap C)$ などを $A \cap B \cap C$ と書く。

このように:

$$A \cup B \cup C = B \cup C \cup A = A \cup C \cup B$$

$$A \cap B \cap C = A \cap C \cap B = B \cap A \cap C$$

命題4 (分配法則)

集合 A、B、C について

(1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(1) $x \in A \cup (B \cap C)$

$\Rightarrow x \in A$ または $(x \in B \cap C)$

$x \in A$ のとき、 $x \in A \cup B$ かつ $x \in A \cup C$ が成り立つ.

$\therefore \quad x \in (A \cup B) \cap (A \cup C)$

$x \in B \cap C$ のとき、 $x \in B$ かつ $x \in C$ が成り立つ.

$\therefore \quad x \in A \cup B$ かつ $x \in A \cup C$ が成り立つ.

よって $x \in (A \cup B) \cap (A \cup C)$

以上より、 $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$.

次に $x \in (A \cup B) \cap (A \cup C)$ を仮定する。

このとき、$x \in A \cup B$ かつ $x \in A \cup C$

がいえる。$x \in A$ ならば、$x \in A \cup (B \cap C)$ である。

そこで、$x \notin A$ とすると、$x \in A \cup B$ より、$x \in B$ がいえる。

同様に、$x \in A \cup C$ かつ $x \notin A$ より、$x \in C$ がいえる。

$\therefore$ $x \in B$ かつ $x \in C$ がいえ、$x \in B \cap C$

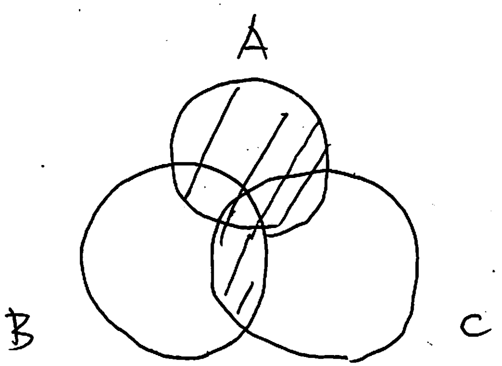
すなわち、$x \in A \cup (B \cap C)$ がいえる。

以上より、$(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$ がいえる。

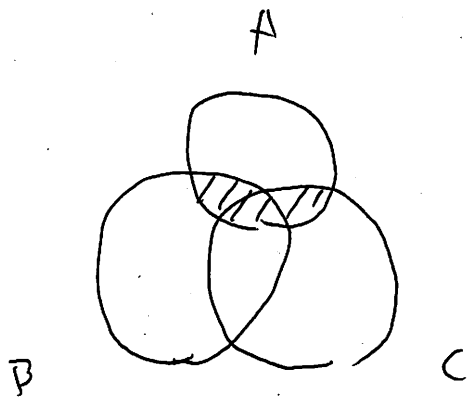
$$\therefore A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

が従う。

(2) 省略



$$A \cup (B \cap C)$$
$$\parallel$$
$$(A \cup B) \cap (A \cup C)$$



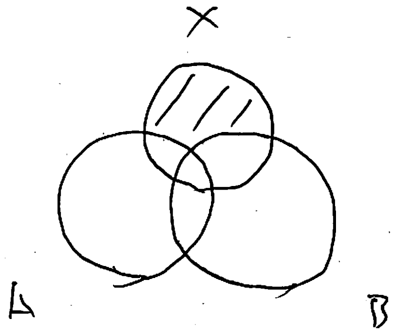
$$A \cap (B \cup C)$$
$$\parallel$$
$$(A \cap B) \cup (A \cap C)$$

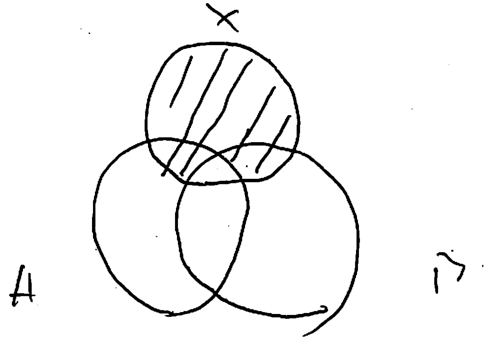
ド・モルガンの法則

定理5　X, A, B: 集合

(1) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$

(2) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$





$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ $\qquad$ $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

∵ (1) $x \in X \setminus (A \cup B)$

$\Leftrightarrow$ $x \in X$ かつ $x \notin A \cup B$

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

$\Leftrightarrow$ $x \in X$ かつ ($x \notin A$ かつ $x \notin B$)

$\Leftrightarrow$ $x \in X$ かつ $x \notin A$ かつ $x \in X$ かつ $x \notin B$

$\Leftrightarrow$ $x \in X \setminus A$ かつ $x \in X \setminus B$

$\Leftrightarrow$ $x \in (X \setminus A) \cap (X \setminus B)$

(2) 省略。

//