代数入門演習　NO. 1　　2014. 9.23

1　代数とは, 集合の基本事項 (復習)

代数入門および演習では主として足し算と掛け算のみを使って整数の性質を調べる. まず具体的な内容には触れず, 少し広い視点から代数という分野を説明する.

1.1　代数系 -環・体・群-

代数とは, 一言でいうと代数系の構造を研究する分野である [1]:

「代数系」=「和や積などができる集合」

例 1.1. すでによく知っている以下の集合は代数系の例である.

1. 整数全体の集合 $\mathbb{Z}$: 和が好きなようにできる. 積も割と好きなようにできる.
2. n 項列ベクトル空間 $\mathbb{C}^n$: 和とスカラー倍が好きなようにできる.
3. 有理数全体の集合 $\mathbb{Q}$: 和も積も好きなようにできる.
4. n 次行列全体の集合 $M_n(\mathbb{C})$: 和とスカラー倍は好きなように, 積は割と自由にできる.
5. n 次正則行列全体の集合 $GL_n(\mathbb{C})$: 積が好きなようにできる.

ここで, 「$\cdots$ が好きなようにできる」というのは, **考えている集合内でその逆の操作が常にできる**ことを, 「割と」は逆の操作は自由にできない, という意味である. 例えば, $\mathbb{Z}$ では和の逆の操作である「差」も自由にできる. しかし, 積の逆の操作である「商」は自由にはできない. (例えば $\mathbb{Z}$ の中で 2 による商を考えることは一般にはできない.) 一方, $\mathbb{Q}$ では 0 以外の全ての数に対して, 積の逆の操作である商が定義される.

上の例に出てきた「和」「積」「スカラー倍」は全て代数系の例を与えるが, その中でも「和」「積」は **2 項演算**と呼ばれるものの例である. ここで, ある集合 X 上の (2 項) 演算とは, X の 2 つの要素に対して, X の要素を対応させる写像 [2] のことである. 実際, 整数やベクトルの和や整数の積は次のように表すことができる.

$$m, n \in \mathbb{Z} \mapsto m + n \in \mathbb{Z}$$

$$\mathbf{a}, \mathbf{b} \in \mathbb{C}^n \mapsto \mathbf{a} + \mathbf{b} \in \mathbb{C}^n$$

$$m, n \in \mathbb{Z} \mapsto m \times n \in \mathbb{Z}$$

一方, ベクトルのスカラー倍は

$$c \in \mathbb{C}, \mathbf{a} \in \mathbb{C}^n \mapsto c\mathbf{a} \in \mathbb{C}^n$$

と表され, 定義域に異なる集合の要素があるため和や積とは違う形をしている. ともに 2 項演算であるという意味で, 和「+」と整数の積「×」は仲間である. 以下ある集合 X 上の 2 項演算を $\circ$ と表しておく. (とりあえず $\circ$ は $+$ や $\times$ を表すと思ってよい.) 2 項演算に関しては次が基本的な定義である.

[1] どういう代数系をどういう手法で研究するかでさらに細分化される.
[2] かっこよくいうと, X の直積集合を定義域とし, X を終域とする写像 $X \times X \to X$ のこと.

(結合律) 任意の $a,b,c \in X$ に対して $(a \circ b) \circ c = a \circ (b \circ c)$ が成立する.

(単位元) ある $e \in X$ が存在して任意の $a \in X$ に対して $a \circ e = e \circ a = a$ が成立する. この e を ($\circ$ に関する) 単位元という.

(逆元) $a \in X$ に対して $a \circ b = b \circ a = e$ となる $b \in X$ が存在する. この b を ($\circ$ に関する)a の逆元という.

(可換性) 任意の $a,b \in X$ に対して $a \circ b = b \circ a$ が成立する.

「結合律」は $a \circ b$ から計算しても $b \circ c$ から計算しても結果が同じになることを意味する. 当たり前の性質に見えるが下の例が示すようにそうではない. $X = \mathbb{Z}$ で $\circ = +$ の場合, $e = 0$ が単位元である. この場合 a の逆元 b とは要するに $-a$ のことである. ($\circ = \times$ の場合, 単位元 e や a の逆元は何か?) 「可換性」は $\circ = +$ では成立するが, 行列の $\times$ などでは成立しない.

例 1.2. $X = \mathbb{R}^3$ とし, 2 項演算 $\circ$ としてベクトルの外積 $\times$ を考える. つまり, $\mathbf{a} = {}^t\begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}, \mathbf{b} = {}^t\begin{pmatrix} b_1 & b_2 & b_3 \end{pmatrix} \in \mathbb{R}^3$ に対して

$$\mathbf{a} \circ \mathbf{b} := \mathbf{a} \times \mathbf{b} = \begin{pmatrix} a_2b_3 - b_2a_3 \\ a_3b_1 - b_3a_1 \\ a_1b_2 - b_1a_2 \end{pmatrix} \in \mathbb{R}^3$$

とする. この 2 項演算は結合律を満たさない. ($\mathbf{a} = \mathbf{b} = \mathbf{e}_1$, $\mathbf{c} = \mathbf{e}_2$ としてみよ.) また可換性も満たさず単位元も存在しない. (単位元がないので逆元を考えることもできない.) □

整数全体の集合 $\mathbb{Z}$ は 2 つの 2 項演算 $+$ と $\times$ をもっていて, それらはともに結合律と可換性をみたし, それぞれに対して単位元が存在する. また, 和に関しては逆元も必ず存在する. このような 2 種類の 2 項演算をもつ集合 R を **(可換) 環**という [3]. 他に大事な環の例として, 例えば $\mathbb{Z}$ 係数の多項式全体の集合 $\mathbb{Z}[x]$ がある. また n 次正方行列全体の集合 $M_n(\mathbb{C})$ は非可換な環の例である. **代数入門では, $\mathbb{Z}$ や $\mathbb{Z}[x]$ を通して可換環の基礎事項を学習する.** また, R が可換環であってさらに積に関しても (0 以外の任意の元の) 逆元が存在するとき, R は**体である,** という. 有理数全体の集合 $\mathbb{Q}$ や実数全体の集合 $\mathbb{R}$ は体の例である.

ちなみに, 結合律を満たし単位元と任意の元に対する逆元をもつような 2 項演算 $\circ$ がある集合は **($\circ$ に関して) 群である**, という. n 次正則行列全体の集合 $GL_n(\mathbb{C})$ は行列の積に関して群になる. また, n 文字の置換全体の集合 S_n も置換の合成に関して群になる.

1.2 集合の基本事項 (復習)

大文字 $(X, Y, A, B, A_i, B_j, \cdots)$ は集合を表すものとする. 次の基本事実 (鉄則) を使いこなせるようになるのがこのプリントの目標です.

1. 「$A \subset B$」は「$x \in A$ ならば $x \in B$」と同値.
2. 「$A = B$」は「$A \subset B$ かつ $A \supset B$」と同値.
3. 「$A \not\subset B$」は「$x \notin B$ をみたす $x \in A$ が存在する」と同値.
4. 「$x \in \bigcup_i A_i$」は「ある i に対して $x \in A_i$」と同値.
5. 「$x \in \bigcap_i A_i$」は「全ての i に対して $x \in A_i$」と同値.

[3] 正確には, 2 つの 2 項演算の間に「分配法則」が成り立つことも定義に入れる.

1.3 問題編

問題 1.1. A, B, C はどれも, ある集合 X の部分集合とする. 次を示せ.
(1) $A \subset B \iff A \cap B = A$.
(2) $A \subset B \Longrightarrow A \cap C \subset B \cap C$.
(3) $C \subset A$ かつ $C \subset B \Longrightarrow C \subset A \cap B$.

問題 1.2. A_i $(i \in \mathbb{N})$, A, B, C はどれも, ある集合 X の部分集合とする. 次の等式を示せ.
(1) $A \cap \left(\bigcup_{i \in \mathbb{N}} A_i \right) = \bigcup_{i \in \mathbb{N}} (A \cap A_i)$.
(2) $A \cup \left(\bigcap_{i \in \mathbb{N}} A_i \right) = \bigcap_{i \in \mathbb{N}} (A \cup A_i)$.
(3) $(A \cap B) - C = (A - C) \cap (B - C)$.
(4) $A - (B - C) = (A - B) \cup (A \cap C)$.

問題 1.3. 次の等式は正しいか? 正しければ証明を, 正しくなければ反例を与えよ.

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

問題 1.4. $\mathbb{R}^2$ の部分集合 A_n, B_n $(n \in \mathbb{N})$ を次で定義する.

$$A_n := \{(x, y) \in \mathbb{R}^2 \mid 0 \leq x \leq 2n,\ 0 \leq y \leq n\},$$
$$B_n := \{(x, y) \in \mathbb{R}^2 \mid 0 \leq x \leq 2n,\ 0 \leq y \leq 1/n\}.$$

(1) $\bigcup_{i \in \mathbb{N}} A_i$ を求めよ. (2) $\bigcap_{i \in \mathbb{N}} B_i$ を求めよ.

問題 1.5. $A := \{x \in \mathbb{R} \mid x = a + b\sqrt{2}\ (a, b \in \mathbb{Q})\}$ とする.
(1) $x \in A$, $y \in A \Rightarrow x + y \in A$, $x - y \in A$, $xy \in A$ を示せ.
(2) $x \in A - \{0\} \Rightarrow x^{-1} \in A$ を示せ.
(3) A の定義の「$a, b \in \mathbb{Q}$」を「$a, b \in \mathbb{Z}$」に変えた集合を A' とすると, A' について (1)(2) と同様のことは成立するか?