5　代数系の基礎（２）–群–

• 5-1 ： 群の定義

科学的な現象には, なにかしらの「対称性」が現れることがある. この対称性を数学的に記述する道具が「群」である. 群の定義は, その抽象度が高い故に物理, 情報工学, 化学など様々なものに応用される. 数学では, 2 次方程式などの代数方程式の根がもつ対称性に着目して群を考えることで「5 次以上の代数方程式には代数的な解の公式が存在しない」といったアーベルの定理が証明されたのは有名な事実である. また, 情報工学では, ある数 p が素数であるか否かを判定するプログラムが多項式時間で検証できるという結果にはやはり群はその背景にある. このように, 科学における様々な事象で「群」という数学的構造が潜んでいる.

空でない集合 G に対して, 写像 $*: G \times G \longrightarrow G$ を G の **二項演算** という. $(a, b) \in G \times G$ のこの写像による像を $a * b$, あるいは単に ab とかく. このとき, 集合 G に 1 つの二項演算が与えられているといい, $(G, *)$ で表す.

例 5-1　(1) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ は二項演算の例である. また, 積に関して $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ も二項演算の例である.

(2) k を $\mathbb{R}$ または $\mathbb{C}$ とする. $\mathsf{Mat}_n(\mathsf{k})$ を成分が k の要素であるような n 次正方行列全体とする. このとき, 行列の和と積に関して $(\mathsf{Mat}_n(\mathsf{k}), +)$, $(\mathsf{Mat}_n(\mathsf{k}), \cdot)$ は二項演算である.

(3) m を 1 より大きい整数とする. このとき, 2 章で導入した演算 $+, \cdot$ についてこのとき, $(\mathbb{Z}/m\mathbb{Z}, +)$ と $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ は二項演算である.

(4) $I \subset \mathbb{R}$ を区間とする. このとき, I 上の C^∞ 級関数全体を $C^\infty(I)$ とおく. このとき, $f, g \in C^\infty(I)$ に対して,

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x)g(x), \quad x \in I$$

と定めると, $(C^\infty(I), +)$, $(C^\infty(I), \cdot)$ は二項演算である.

(5) X を空でない集合とする. $\mathsf{Map}(X, X)$ で X から X 自身への写像全体とする. このとき, 合成 $\circ$ に関して $(\mathsf{Map}(X), \circ)$ は二項演算である.

命題 3.5 の状況の骨組みを抜き出して公理化したものが「群」である.

定義 5.1. 空でない集合 G に 1 つの二項演算 $*$ が与えられていて, 次の条件を満たすとき, G は演算 $*$ に関して **群** であるという.

(G1) 二項演算 $*$ は **結合法則** を満たす. すなわち, 任意の $x, y, z \in G$ に対して,

$$(x * y) * y = x * (y * z)$$

を満たす.

(G2) G の特別な元 $e \in G$ が存在して, 任意の $x \in G$ に対して $e * x = x = x * e$ を満たす. このような e を G の **単位元** という.

(G3) 任意の $x \in G$ に対して, ある $y \in G$ が存在して $x * y = e = y * x$ をいたす. このような y を x の **逆元** という.

以降, 単に G が群である, という場合には G 上のある二項演算 $*$ で群であるときをいい, この演算を G の **積** と呼ぶ. 群 G の要素の数を $|G|$ と表し, これを G の **位数** という. ここで, $|G| = \infty$ もあり得る.

担当：茨城大学 情報科学領域　宮本 賢伍

例 5-2　(1) 通常の和に関して, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は群をなす. ただし, $\mathbb{N}$ は和に関して群をなさない. 実際, $2 \in \mathbb{N}$ の逆元は自然数ではないからである. また, 通常の積に関しては $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ のいずれも群をなさない. なぜならば, 単位元は 1 であるが, 0 に逆元が存在しないからである.

一方, $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ はいずれも積に関して群となる. この $\mathbb{C}^*$ は **トーラス** とも呼ばれる.

(2) k を $\mathbb{R}$ または $\mathbb{C}$ とする. $\mathsf{Mat}_n(\mathsf{k})$ を成分が k の要素であるような n 次正方行列全体とする. このとき, 行列の和に関して $\mathsf{Mat}_n(\mathsf{k})$ は群をなす. 実際, 行列の和は結合法則を満たすので, (G1) を満たす. 単位元は零行列 O をとればよいので (G2) を満たす. 任意の $X \in \mathsf{Mat}_n(\mathsf{k})$ に対して, X は逆元 $-X$ をもつ. これは, 行列の積に関しては群をなさない.

(3) k を $\mathbb{R}$ または $\mathbb{C}$ とする. n 次正則行列全体をなす集合を $\mathsf{GL}_n(\mathsf{k})$ とおく. これは行列の積に関して群をなす. 実際, 行列の積は結合法則を満たすので, (G1) を満たす. 単位元は単位行列 E_n をとればよいので (G2) を満たす. 任意の $X \in \mathsf{GL}_n(\mathsf{k})$ に対して, X は正則なので逆行列 X^{-1} が存在するが, これが X の逆元である. $\mathsf{GL}_n(\mathsf{k})$ は **一般線形群** と呼ばれる. これは, 行列の和に関しては群をなさない. 実際, 行列の和は $\mathsf{GL}_n(\mathsf{k})$ 上の二項演算ではない.

(4) m を 1 より大きい整数とする. このとき, 3 章で導入した和 $+$ について, **命題 3.5** より $\mathbb{Z}/m\mathbb{Z}$ は群をなす.

上の一般線形群の例に挙げられるように, 群 G の積 $*$ は, いつでも任意の $a, b \in G$ に対して $a * b = b * a$ を満たす必要はない. 実際, $\mathsf{GL}(\mathsf{k})$ には行列の積に関して群をなすが, 行列の積はいつでも $XY = YX$ を満たすとは限らない.

レポート 5-1　集合 Z を絶対値が 1 となる複素数全体, すなわち

$$Z = \{z \in \mathbb{C} \mid |z| = 1\}$$

とする. Z は複素数の積に関して群をなすことを示せ.

命題 5.2. 集合 G が群であるとする. このとき, G の単位元 e はただ一つに定まる. また, x の逆元 y は x に対してただ一つに定まる.

証明. 単位元の一意性を示す. $e, e' \in G$ を共に G の単位元であるとすると, e' は単位元であるから $e = e * e'$ である, 一方, e も単位元なので $e * e' = e'$. 従って $e = e'$ となる. よって単位元の一意性が示された.

任意に $x \in G$ をとり, $y, y' \in G$ が共に x の逆元であるとする. このとき, y が x に逆元なので $x * y = e$ である. これの両辺に左から y' をかけると, y' も x の逆元であるから

$$y' * x * y = y * e \quad \Longleftrightarrow \quad y' = y$$

である. よって x の逆元は一意的である. □

レポート 5-2　G を群とする. このとき, 任意の $a, b \in G$ に対して

$$(ab)^{-1} = b^{-1}a^{-1}$$

であることを示せ.

• 5-2 : 対称群

自然数 n に対して, $X_n = \{1, 2, \ldots, n\}$ とおく. X_n から X_n への全単射写像 $\rho : X_n \to X_n$ の全体の集合を S_n で表す. $\rho \in S_n$ によって $i \in X_n$ が $\rho(i) \in X_n$ にうつるとき, これを

$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix}$$

という記号で表す. $\rho \in S_n$ をひとつ決めれば, ρ は全単射なので $(1, 2, \ldots, n)$ の順列がただ一つ定まるので $|S_n| = n!$ である.

例 5-3　(1) $n = 2$ のとき, S_2 は次の 2 つの元からなる集合である.

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

(2) $n = 3$ のとき, S_3 は次の 6 つの元からなる集合である.

$$e := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\tau_1 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau_3 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

さて, 集合 S_n 上の二項演算を写像の合成で定める. つまり, $\sigma, \tau \in S_n$ に対して,

$$\sigma\tau := \sigma \circ \tau$$

で定める. つまり,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}$$

と定義する.

例 5-4　S_3 において, σ_1 と τ_1 の積を計算してみよう.

$$\sigma_1\tau_1(1) = \sigma_1(1) = 2, \quad \sigma_1\tau_1(2) = \sigma_1(3) = 1, \quad \sigma_1\tau_1(3) = \sigma_1(2) = 3$$

だから

$$\sigma_1\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_3$$

である. また,

$$\tau_1\sigma_1(1) = \tau_1(2) = 3, \quad \tau_1\sigma_1(2) = \tau_1(3) = 2, \quad \tau_1\sigma_1(3) = \tau_1(1) = 1$$

だから

$$\tau_1\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2$$

である. 特に, $\sigma_1\tau_1 \neq \tau_1\sigma_1$ である.

補題 5.3. 写像 $f : X \to Y$, $g : Y \to Z$, $h : Z \to W$ に対して,

$$(h \circ g) \circ f = h \circ (g \circ f)$$

が成り立つ. すなわち, 写像の合成は結合法則を満たす.

証明. 任意の $x \in X$ に対して,

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))), \quad h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$$

だから $(h \circ g) \circ f(x) = h \circ (g \circ f)(x)$ が示された. $x \in X$ は任意だったので, 写像として $(h \circ g) \circ f = h \circ (g \circ f)$ である. □

定理 5.4. S_n は写像の合成に関して群をなす. このようにして群とみなした S_n を n **次対称群** と呼ぶ.

証明. S_n における写像の合成が (G1), (G2), (G3) を満たすことを示せば良い.

(G1)：**補題 5.3** より, 写像の合成は結合法則を満たすので, 任意の $\sigma, \tau, \rho \in S_n$ に対して $(\sigma\tau)\rho = \sigma(\tau\rho)$ である.

(G2)：$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ をとれば, 任意の $\rho \in S_n$ に対して,

$$\rho e = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} = \rho$$
$$e\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} = \rho$$

である. 従って単位元 e が存在する.

(G3)：任意に $\rho \in S_n$ をとれば, ρ: $X_n \to X_n$ は全単射なので, 逆写像 ρ^{-1} が存在する. このとき,

$$\rho\rho^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho \circ \rho^{-1}(1) & \rho \circ \rho^{-1}(2) & \cdots & \rho \circ \rho^{-1}(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = e$$
$$\rho^{-1}\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho^{-1} \circ \rho(1) & \rho^{-1} \circ \rho(2) & \cdots & \rho^{-1} \circ \rho(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = e$$

となる. 従って, ρ の逆元は ρ^{-1} である.

以上で S_n は写像の合成に関して群をなす. □

レポート 5-3　3 次対称群 S_3 において, 演算表を作成しなさい. また, それぞれの元に対する逆元を求めよ.

担当：茨城大学 情報科学領域　宮本 賢伍