2　群の定義と具体例

ここでは群の定義と具体例について思い出しておこう.

• 2-1 : 群の公理

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 2-1　(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.

定義 2.1. 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. G が有限集合であるとき, G は **有限群** と呼ばれる. また, 群 G の積について, 任意の $x,y \in G$ に対して

$$x*y = y*x$$

を満たすとき, G は **アーベル群** であるいう.

• 2-2 : 群の具体例

例 2-2　(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. 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.

レポート 2-1　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のはなぜか説明せよ.

(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) n を 2 以上の自然数とする. n 文字の **置換** とは, $X = \{1, 2, \ldots, n\}$ からそれ自身への全単射 $\sigma : X \to X$ のことをいう. 置換 σ は

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

のように表す. X の中の相異なる $i_1, i_2, \ldots, i_p$ に対して, 置換 σ が

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots, \quad \sigma(i_{p-1}) = i_p, \quad \sigma(i_p) = i_1$$

と写して, $j \neq i_1, \ldots, i_p$ に対しては $\sigma(j) = j$ によって定義されるとき, σ を **長さ p の巡回置換** といい, $(i_1, i_2, \ldots, i_p)$ で表す. $p = 2$ のとき, **互換** という. n 文字の置換全体からなる集合を $\mathfrak{S}_n$ で表し, 写像の合成を積として群をなす. これを**n 次対称群** と呼ぶ.

$n = 2$ のときは,

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

であり, $n = 3$ のときは,

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

である.

レポート 2-2　$n = 4$ のとき, $\mathfrak{S}_4$ の元をリストアップせよ.

レポート 2-3　$\mathfrak{S}_n$ で表し, 写像の合成を積として群をなすことを示せ.

補題 2.2. 任意の $\sigma \in \mathfrak{S}_n$ は互換の積で書くことができる. (ただし, 表し方は一意的ではない.)

証明. n に関する帰納法で証明する. $n = 2$ のとき, $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ は自身が互換 $(1, 2)$ であり,

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1, 2)(1, 2)$$

である. よって $n=2$ のとき, 主張は正しい.

$(n-1)$ 次対称群まで主張が正しいとしよう. 置換 σ は

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

であると表しておく. $\sigma(n)=n$ なら, σ は $n-1$ 個の文字の置換であるから帰納法の仮定より σ を互換の積で表すことができる. $\sigma(n)=k\neq n$ であるとする. $\tau=(k,n)$ とおくと, $\tau\sigma$ は n を固定するから, $\tau\sigma$ は $n-1$ 個の文字の置換である. よって帰納法の仮定より $\tau\sigma$ を互換の積で表すことができる. これを

$$\tau\sigma = \rho_1 \cdots \rho_\ell$$

で表しておくと, $\sigma = \tau\rho_1\cdots\rho_\ell$ である. 以上で σ を互換の積で表すことができた. □

レポート 2-4　任意の置換が互換の積でかけることの証明を上のやり方とは別に与えよ.

$\sigma \in \mathfrak{S}_n$ に対して, σ の **符号** を

$$\mathsf{sgn}(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$$

で定義する.

補題 2.3. 互換 σ に対して, $\mathsf{sgn}(\sigma) = -1$ である.

証明. $\sigma=(k,l)$ とおく. 自然数 N を $i<j$ だが $\sigma(i)>\sigma(j)$ を満たす組 $\{i,j\}$ の組の個数とおけば

$$\mathsf{sgn}(\sigma) = (-1)^N$$

とかけるので, あとは N が奇数であることを示せば良い. 自然数 L に対して, 列 $\sigma(1),\ldots,\sigma(n)$ を考えたとき L の左側にあるが L よりも大きい数字の個数を n_L とおくと

$$N = n_1 + n_2 + \cdots + n_n$$

である. ここで, 数え上げにより $n_{k+1}=n_{k+2}=\cdots=n_{l-1}=1$, $n_k = l-k$, それ以外の n_i は 0 だから, 結局 $N=2(l-k)-1$ となり証明が完了した. □

補題 2.4. 置換 σ,τ に対して, $\mathsf{sgn}(\sigma\tau) = \mathsf{sgn}(\sigma)\mathsf{sgn}(\tau)$ である.

証明. 符号の定義により

$$\mathsf{sgn}(\sigma\tau) = \prod \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} = \prod \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \prod \frac{\tau(j)-\tau(i)}{j-i} = \mathsf{sgn}(\sigma)\mathsf{sgn}(\tau)$$

となり, 欲しい式が得られる. □

以上によって, 置換を互換の積でかいたとき, その表示の仕方は一意的ではないが, その個数の偶奇は一定であることが証明される.

定理 2.5. 置換 σ を互換の積で表したとき, 用いる互換の数の偶奇はその表し方に依らずに一定である.

証明. 任意に置換をとれば, **補題 2.2** から, これは互換の積で表される. σ を 2 通りに互換の積で表しておこう:

$$\rho_1\rho_2\cdots\rho_m = \tau_1\tau_2\cdots\tau_n$$

このとき, 両辺の符号をとれば**補題 2.3, 2.4** より $(-1)^m=(-1)^n$ である. よって, m と n の偶奇は一致する. □

置換 $\sigma\in\mathfrak{S}_n$ を互換の積で書いたとき, 偶数個の互換の積でかけるような置換を **偶置換**, 奇数個の互換の積でかけるような置換を **奇置換** という.

担当：茨城大学 情報科学領域　宮本 賢伍

- **1-3 : 3 次方程式の解の公式**

3 次方程式 $x^3+ax^2+bx+c=0$ を考える. $a\neq 0$ であれば,

$$x^3+ax^2+bx+c=\left(x+\frac{a}{3}\right)^3+\left(b-\frac{a^2}{3}\right)x+c-\frac{a^3}{27}$$

なので, $y=x+\frac{a}{3}$ とおくことで結局 $y^3+py+q=0$ の形に変形できる. 従って, 改めて $x^3+px+q=0$ の形の解放を与えれば, 任意の 3 次方程式が解けるようになる. ω を 1 の原始 3 乗根のひとつとする. このとき, **定理??**から

$$C(x,-u,-v)=(x-u-v)(x-\omega u-\omega^2 v)(x-\omega^2 u-\omega v)$$

が成立する. 一方, $C(x,-u,-v)=x^3-3uvx-u^3-v^3$ だから係数比較をすると

$$p=-3uv,\quad q=-u^3-v^3$$

となる. これを満たす u,v が求まったとすれば,

$$x=u+v,\quad x=\omega u+\omega^2 v,\quad x=\omega^2 u+\omega v$$

として 3 つの解が得られたことになる. $p=-3uv$ より, $u^3v^3=-\frac{p^3}{27}$ であり, $q=-u^3-v^3$ と同時に満たすものを考えればよい. 解と係数の関係より, u^3, v^3 は 2 次方程式

$$X^2+qX-\frac{p^3}{27}=0$$

の解である. こうして u^3, v^3 の 3 乗根のうち, $p=-3uv$ を満たすものが $x^3+px+q=0$ の解である.

担当：茨城大学 情報科学領域　宮本 賢伍