情報数理 I 要綱 #2

2003–11–6　河野

1　群の定義と基礎概念

イントロで述べた様な対称性に関する議論をもう少しきちんとするためにこの節では群を定義し，その性質に関して議論する。

定義 1.1 G を空ではない集合とする。G 上の 2 項演算 $\circ$ が定義されていて次を満たすとき $(G, \circ)$ を**群** (*group*) と呼ぶ。

(1) 結合法則を満たす ; 任意の $g, g', g'' \in G$ に対し $(g \circ g') \circ g'' = g \circ (g' \circ g'')$

(2) 単位元の存在 ; G には e(単位元と呼ばれる) という元が存在して，任意の $g \in G$ に対し $g \circ e = e \circ g = g$ が成立する。

(3) 逆元の存在 : 任意の $g \in G$ に対し，$g \circ g' = g' \circ g = e$ を満たす元 $g' \in G$ が存在する。この元 g' を g の逆元と呼び $g' = g^{-1}$ と書く。

命題 1.2 群 $(G, \circ)$ に対しその単位元は唯 1 つ存在する。任意の元 g に対しその逆元 g^{-1} も唯 1 つ存在する。

命題が意味していることは，定義の (2) の性質を持つ元が 2 つあり，それを e, e' とするとき $e = e'$ という事である。また g に対し (3) を満たす元が 2 つあり，それを g', g'' とするとき $g' = g''$ である。

証明　$e \circ e'$ を考える。e が (2) の性質を持つので $e \circ e' = e'$ となる。また e' も (2) の性質を持つので $e \circ e' = e$ となる。よって $e = e'$ である。

結合法則より $g' \circ (g \circ g'') = (g' \circ g) \circ g''$ である。g'' は (3) の性質を持つので $g \circ g'' = e$，よって $g' \circ (g \circ g'') = g' \circ e = g'$ である。また g' も (3) の性質を持つので $g' \circ g = e$，よって $(g' \circ g) \circ g'' = e \circ g'' = g''$ となる。よって $g' = g''$ である。 ∎

例 1.3　(1) $\boldsymbol{Z}$ を整数全体が作る集合とする。$+$ を通常の加法とすると $(\boldsymbol{Z}, +)$ は群になる。$\boldsymbol{Z}$ は空集合ではなく，$+$ は $\boldsymbol{Z}$ 上の 2 項演算になっているので定義 1.1 の条件 (1)–(3) をチェックすればよい。

$\boldsymbol{Z}$ には積 $\times$ も定義されている。$(\boldsymbol{Z}, \times)$ は定義 1.1 の条件 (1)–(2) を満たすが，(3) を満たさないので群ではない。

(2) $\boldsymbol{Q}$ を有理数全体が作る集合とする。$(\boldsymbol{Q}, +)$ は (1) と同様に群であることが分かる。$(\boldsymbol{Q}, \times)$ は群ではない (どの性質が成り立たないか確認せよ)。

0 以外の有理数全体からなる集合を $\boldsymbol{Q}^*$ と表す。$(\boldsymbol{Q}^*, \times)$ は群になる。

正の有理数全体からなる集合を $\boldsymbol{Q}^+$ と表す。$(\boldsymbol{Q}^+, \times)$ は群になる。

(3) $\boldsymbol{R}$ を実数全体が作る集合とする。$(\boldsymbol{R}, +)$ は群である。$(\boldsymbol{R}, \times)$ は群ではない。

0 以外の実数全体からなる集合を $\boldsymbol{R}^*$ と表す。$(\boldsymbol{R}^*, \times)$ は群になる。

正の実数全体からなる集合を $\boldsymbol{R}^+$ と表す。$(\boldsymbol{R}^+, \times)$ は群になる。

(4) $\boldsymbol{C}$ を複素数全体が作る集合とする。$(\boldsymbol{C}, +)$ は群である。$(\boldsymbol{C}, \times)$ は群ではない。

0 以外の複素数全体からなる集合を $\boldsymbol{C}^*$ と表す。$(\boldsymbol{C}^*, \times)$ は群になる。

絶対値が 1 である複素数全体からなる集合を ${\boldsymbol{C}^*}_1$ と表す (この記号は一般的ではない)。$({\boldsymbol{C}^*}_1, \times)$ は群になる。

(5) $M = \left\{ f \,\middle|\, f \text{ は} \boldsymbol{R}^2 \text{から} \boldsymbol{R}^2 \text{への写像で長さを保つ} \right\}$ とする。演算は写像の合成とすると，M は群になる。$A(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ とし，$\boldsymbol{b}$ を $\boldsymbol{R}^2$ の任意のベクトルとする。$f : \boldsymbol{R}^2 \to \boldsymbol{R}^2$ を $f(\boldsymbol{x}) = A(\theta)\boldsymbol{x} + \boldsymbol{b}$ で定義すると $f \in M$ が分かる。$B(\theta) = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$ とし，$\boldsymbol{b}$ を $\boldsymbol{R}^2$ の任意のベクトルとする。$g : \boldsymbol{R}^2 \to \boldsymbol{R}^2$ を $g(\boldsymbol{x}) = B(\theta)\boldsymbol{x} + \boldsymbol{b}$ で定義すると $g \in M$ が分かる。

逆に M の元は上で述べた f, g のタイプに限る事が分かる (この事実は後の節で証明する)。

$M(3) = \left\{ f \,\middle|\, f \text{ は} \boldsymbol{R}^3 \text{から} \boldsymbol{R}^3 \text{への写像で長さを保つ} \right\}$ とする。演算は写像の合成とすると，$M(3)$ は群になる。$M(3)$ の元がどのように表されるかはもう少し後で考えよう。n 次元空間 $\boldsymbol{R}^n$ のベクトル $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ に対し長さを $\|\boldsymbol{x}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$ で定義する。

$M(n) = \{ f \,|\, f \text{ は} \boldsymbol{R}^n \text{から} \boldsymbol{R}^n \text{への写像で長さを保つ} \}$ とする。演算は写像の合成とすると，$M(n)$ は群になる。

(6) $N(n) = \{1, 2, \ldots, n\}$ とする。$N(n)$ から $N(n)$ の上への一対一写像全体の作る集合を S_n と書き，演算を写像の合成で定義すると群になる。これを n 次の**対称群** (*symmetric group*) という。S_n の元を σ とする。σ を表現するのに $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ という表記をする事がある。σ を**置換** (または n–置換) という事もある。$n = 3$ の場合を考えよう。このとき 3–置換は 6 個あり，それらを $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$,
$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ と書く。σ_1 が単位元で，$\sigma_3\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma_2$ 等が成立する。

交代群 (*alternating group*)A_n というものを定義したい。一般的に議論しても分かりにくいので $n = 3$ のときを考える。x_1, x_2, x_2 を変数とし，x_1, x_2, x_3 に関する多項式 $F(x_1, x_2, x_3)$ を $F(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ とする。S_3 の元 σ に対し $F^\sigma(x_1, x_2, x_3) = (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)})$ と定義する。例えば σ_4 は $\sigma_4(1) = 2, \sigma_4(2) = 3, \sigma_4(3) = 1$ なので $F^{\sigma_4} = (x_2 - x_1)(x_2 - x_3)(x_3 - x_1) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = F$ となる。σ_2 は $\sigma_2(1) = 1, \sigma_2(2) = 3, \sigma_2(3) = 2$ なので $F^{\sigma_2} = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) = -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = -F$ となる。S_n の任意の元 σ に対し $F^\sigma = \pm F$ となる。そ

こで $F^\sigma = \mathrm{sgn}(\sigma)F$ と定義する。$\mathrm{sgn}(\sigma)=1$ となる置換を**偶置換**，$\mathrm{sgn}(\sigma)=-1$ となる置換を**奇置換**と呼ぶ。$\mathrm{sgn}(\sigma\tau)=\mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ が成立するので偶置換の積は偶置換になる。そこで $A_3=\{\sigma\in S_3 \mid \sigma \text{は偶置換}\}$ と定義すると A_3 は群になる。この定義は一般の n でできる。

(7) 正則な実 2 次行列全体の作る集合を $GL(2,\boldsymbol{R})$ とすると，行列の積に関して群をなす。正則な複素 2 次行列全体の作る集合を $GL(2,\boldsymbol{C})$ とすると，行列の積に関して群をなす。これらを**一般線型群** (*general linear group*) と呼ぶ。行列式が 1 の実 2 次行列全体の作る集合を $SL(2,\boldsymbol{R})$ とすると，行列の積に関して群をなす。行列式が 1 の複素 2 次行列全体の作る集合を $SL(2,\boldsymbol{C})$ とすると，行列の積に関して群をなす。これらを**特殊線型群** (*special linear group*) と呼ぶ。
一般の n に対しても同様に $GL(n,\boldsymbol{R}), GL(n,\boldsymbol{C}), SL(n,\boldsymbol{R}), SL(n,\boldsymbol{C})$ が定義できる。

群 $(G,\circ)$ は演算付きなので集合 G だけで決まるわけではなく，演算 $\circ$ も指定する必要がある。しかしその演算が明確な場合群 G という言い方をする場合もある。演算 $\circ$ を省略して $g\circ g'$ を gg' と書く場合も多い。以下演算が明確な場合，そうする事とする。

定義 1.4 G, G' を群とする。G から G' への写像 f が次の条件を満たすとき**準同型写像** (*homomorphism*) という；任意の $g, g\in G$ に対し $f(gg')=f(g)f(g')$ が成立する。
G から G' への準同型写像 f が上への一対一写像のとき f を**同型写像** (*isomorphism*) と呼ぶ。このとき G と G' は**同型** (*isomorphic*) であるといい，$G\cong G'$ と書く。

命題 1.5 f を G から G' への準同型写像とする。e, e' を G, G' の単位元とすると，$f(e)=e'$ となる。また任意の $g\in G$ に対し $f(g^{-1})=f(g)^{-1}$ となる。

例 1.6 (1) 行列に対しその行列式を対応させる写像を det と書く。det は $GL(n,\boldsymbol{R})$ から $(\boldsymbol{R}^*,\times)$ への準同型写像である。また $GL(n,\boldsymbol{C})$ から $(\boldsymbol{C}^*,\times)$ への準同型写像も与える。

(2) $(\boldsymbol{R},+)$ と $(\boldsymbol{R}^+,\times)$ は同型である。指数関数 $f(x)=e^x$ が同型写像を与える。一方 $(\boldsymbol{Q},+)$ と $(\boldsymbol{Q}^+,\times)$ の間に同型写像は存在しない。

(3) $f:(\boldsymbol{R},+)\to({\boldsymbol{C}^*}_1,\times)$ を $f(x)=e^{ix}$ で定義すると f は準同形写像である。

(4) $(\boldsymbol{C}^*,\times)$ から $(\boldsymbol{R}^+,\times)$ への写像 f を $f(z)=|z|$ で定めると，f は準同型写像である。

(5) $\{1,-1\}$ は積に関して群をなす。S_n から $\{1,-1\}$ への写像 sgn は準同型写像である。

定義 1.7 群 G の部分集合 H が群 G の演算に関し群をなすとき，H を G の**部分群** (*subgroup*) といい，$H\leqq G$ と表す。$H\leqq G$ かつ $H\neq G$ のとき**真部分群** (*proper subgroup*) といい，$H<G$ と表す。

命題 1.8 群 G の空でない部分集合 H が G の部分群である必要十分条件は次の 2 つが成立する事である。
(1) 任意の $h, h'\in H$ に対し $hh'\in H$ が成立する。
(2) 任意の $h\in H$ に対し $h^{-1}\in H$

命題 1.9 G, G' を群とし $f: G\to G'$ を準同型写像とする。このとき $\mathrm{Ker}(f)=\{g\in G \mid f(g)=e'\}$ (ここで e' は G' の単位元) 及び $\mathrm{Im}(f)=\{g'\in G' \mid \text{ある } g\in G \text{ が存在して } g'=f(g)\}$ とおくと，$\mathrm{Ker}(f)\leqq G$, $\mathrm{Im}(f)\leqq G'$ である。
$H\leqq G$ に対し $f(H)=\{g'\in G' \mid \text{ある } h\in H \text{ が存在して } g'=f(h)\}$ と定義する。また $H'\leqq G'$ に対し $f^{-1}(H')=\{g\in G \mid f(g)\in H'\}$ と定義する。このとき $f^{-1}(H')\leqq G$, $f(H)\leqq G'$ が成立する。

例 1.10

(1) $(\boldsymbol{Z},+)<(\boldsymbol{Q},+)<(\boldsymbol{R},+)<(\boldsymbol{C},+)$ である。また $(\boldsymbol{Q}^+,\times)<(\boldsymbol{Q}^*,\times)<(\boldsymbol{R}^*,\times)<(\boldsymbol{C}^*,\times)$ である。また $(\boldsymbol{Q}^+,\times)<(\boldsymbol{R}^+,\times)<(\boldsymbol{R}^*,\times)$ である。

(2) X を平面内の図形とする。$M(X)=\{\,f\in M\mid\ f(X)=X\,\}$ とおくと $M(X)\leqq M$ となる。$X=\boldsymbol{R}^2$ の場合のみ $M(X)=M$ となり，それ以外の場合 $M(X)<M$ となる。

(3) 準同型写像 $\mathrm{sgn}:S_n\to\{1,-1\}$ に対し $\mathrm{Ker}(\mathrm{sgn})=A_n$ が成立する。

(4) 例 1.6 の (2) の準同型写像 $f:(\boldsymbol{C}^*,\times)\to(\boldsymbol{R}^+,\times)$ に対し $\mathrm{Ker}(f)=({\boldsymbol{C}^*}_1,\times)$ が成立する。

(5) 例 1.6 の (3) の準同型写像 $f:(\boldsymbol{R},+)\to({\boldsymbol{C}^*}_1,\times)$ に対し $\mathrm{Ker}(f)=\boldsymbol{Z}$ が成立する。

(6) 準同型写像 $\det:GL(n,\boldsymbol{R})\to(\boldsymbol{R}^*,\times)$ に対し $\mathrm{Ker}(\det)=SL(n,\boldsymbol{R})$ である。
$O(n)=\{\,A\in GL(n,\boldsymbol{R})\mid\ AA^t=E\,\}$ を**直交群** (*orthogonal group*) と呼ぶ。また
$SO(n)=\{\,A\in O(n)\mid\ \det(A)=1\,\}$ を**特殊直交群** (*special orthogonal group*) と呼ぶ。
$SO(n)<O(n)<GL(n,\boldsymbol{R})$ である。対称性の議論でこれらの群は重要な役割を果たす。