群と部分群の基本性質

担当：大矢 浩徳 (OYA Hironori)

定義.

空でない集合 G が**群**であるとは，2 項演算 $G \times G \to G, (g_1, g_2) \mapsto g_1 \cdot g_2$ が定まっており，以下の 3 条件を満たすこと：

(I) 任意の $g_1, g_2, g_3 \in G$ に対して，$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ が成り立つ.

(II) ある $e \in G$ が存在して，任意の $g \in G$ に対し，$e \cdot g = g = g \cdot e$ が成り立つ.（この e を G の**単位元**と呼ぶ.）

(III) 任意の $g \in G$ に対して，ある $g' \in G$ が存在し，$g' \cdot g = e = g \cdot g'$ が成り立つ.（この g' を G における g **の逆元**と呼ぶ.）

群 G の**部分群**とは，群 G の空でない部分集合であって，G の 2 項演算によって群をなすものである.

以下は群の基本性質とその証明である.

命題 1.

群 G において，単位元 e はただ 1 つに定まる.

証明. $e, e' \in G$ が G の単位元だったとすると，

$$\begin{aligned} e &= e \cdot e' && (e'\text{は単位元なので}) \\ &= e' && (e\text{ は単位元なので}) \end{aligned}$$

である. □

命題 2.

任意の群 G の元 g に対し，G における g の逆元 g' はただ 1 つに定まる.

証明. $g', g'' \in G$ が G における g の逆元だったとすると，

$$\begin{aligned} g' &= g' \cdot e && (e\text{ は単位元なので}) \\ &= g' \cdot (g \cdot g'') && (g''\text{は } g \text{ の逆元なので}) \\ &= (g' \cdot g) \cdot g'' && (\text{結合法則}) \\ &= e \cdot g'' && (g'\text{は } g \text{ の逆元なので}) \\ &= g'' && (e\text{ は単位元なので}) \end{aligned}$$

である. □

命題 3.

G を群とし，H をその部分群とするとき，

(1) H の単位元は G の単位元に一致する.

(2) 任意の H の元 h に対し，H における h の逆元は G における h の逆元に一致する.

(1) の証明. H の単位元を e_H，G の単位元を e_G，G における e_H の逆元を $e_H^{-1,G}$ と書くと，

$$
\begin{aligned}
e_H &= e_G \cdot e_H && (e_G\text{は } G \text{ の単位元なので}) \\
&= (e_H^{-1,G} \cdot e_H) \cdot e_H && (e_H^{-1,G}\text{は } G \text{ における } e_H\text{の逆元なので}) \\
&= e_H^{-1,G} \cdot (e_H \cdot e_H) && (\text{結合法則}) \\
&= e_H^{-1,G} \cdot e_H && (e_H\text{は } H \text{ の単位元なので}) \\
&= e_G && (e_H^{-1,G}\text{は } G \text{ における } e_H\text{の逆元なので})
\end{aligned}
$$

である．特に，これは e_G が必ず部分群 H に含まれることも意味していることに注意する． □

(2) の証明. H における h の逆元を $h^{-1,H}$，G における h の逆元を $h^{-1,G}$ と書くと，

$$
\begin{aligned}
h^{-1,H} &= h^{-1,H} \cdot e && (e \text{ は } G \text{ の単位元なので}) \\
&= h^{-1,H} \cdot (h \cdot h^{-1,G}) && (h^{-1,G}\text{は } G \text{ における } h \text{ の逆元なので}) \\
&= (h^{-1,H} \cdot h) \cdot h^{-1,G} && (\text{結合法則}) \\
&= e \cdot h^{-1,G} && (h^{-1,H}\text{は } H \text{ における } h \text{ の逆元であり，(1) より } H \text{ の単位元も } e \text{ なので}) \\
&= h^{-1,G} && (e \text{ は } G \text{ の単位元なので})
\end{aligned}
$$

である． □

注意 (**群の定義補足 (興味のある方向け)**)．群の定義で (II) や (III) にある等式を『$g = g \cdot e$』のみ，『$g' \cdot g = e$』のみというようにさぼってはいけない．例えば，2×2 行列のなす集合

$$
G' := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a \in \mathbb{C}^\times, b \in \mathbb{C} \right\}
$$

を考える．すると，

$$
\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} a' & 0 \\ b' & 0 \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba' & 0 \end{pmatrix}
$$

より，G' には行列の積から定まる 2 項演算が定まっている (結合法則 (I) を満たす)．

さらに，$e := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G'$ と定めると，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，

$$
ge = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g
$$

が成立する．さらに，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，$g' = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \in G'$ とすると，

$$
g'g = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = e
$$

となる．これより，G' は群の性質のうち 2 項演算の存在，(I)，(II) の一部 (『$g = g \cdot e$』のみにしたもの)，(III) の一部 (『$g' \cdot g = e$』のみにしたもの) を満たすが，G' は群ではない．実際，G' が群であるなら任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，$e'g = g$ を満たす $e' = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \in G'$ が存在するはずである．しかし，

$$
e'g = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} e_1 a & 0 \\ e_2 a & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g
$$

なので，特に $e_2 a = b$ が任意の $a \in \mathbb{C}^\times$、$b \in \mathbb{C}$ に対して成り立つことになるが，そのような定数 e_2 は存在せず，矛盾する．