現代数学への流れ　第6回

復習　群

定義1　G：集合

$$\cdot : G \times G \to G \qquad G\text{上の演算}$$
$$(g_1, g_2) \mapsto g_1 \cdot g_2$$

$(G, \cdot)$ が群であるとは以下の3つの条件が成り立つことをいう．

(i)（結合法則）　任意の $g_1, g_2, g_3 \in G$ に対して
$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$$
が成立する．

(ii)（単位元の存在）　ある $e \in G$ が存在して任意の $g \in G$ に対して
$$g \cdot e = e \cdot g = g$$
が成立する．

(iii)（逆元の存在）　任意の $g \in G$ に対して $g^{-1} \in G$ が存在して
$$g \cdot g^{-1} = g^{-1} \cdot g = e$$
が成立する．

部分群

定義2 G: 群　　$H \subset G$: 部分集合

H が G の部分群であるとは、H が G の演算に関して群になることをいう。

補題2 G: 群　　$H \subset G$: 部分集合

H が部分群になるための必要十分条件は以下が成立することである。

(i) $e_G \in H$

(ii) 任意の $h_1, h_2 \in H$ について、$h_1 \cdot h_2 \in H$

(H は積で閉じている。)

(iii) 任意の $h \in H$ について　　$h^{-1} \in H$ がいえる。

(H は逆元で閉じている。)

(:) H が部分群であるとする.

このとき Hには 演算が 定義できていないといけないので.

$$h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$$

が成り立つ. ∴ (ii) が成う.

また Hは 単位元 $e_H \in H$ を持つが

$$e_H \cdot e_H = e_H$$

が成り立つ. 左から e_H^{-1} をかけて.

$$e_H = e_G$$

が成り立つ. ∴ (i) が成う.

よって $h \in H$ に対して $h \cdot h' = h' \cdot h = e_G$ を満たす $h' \in H$ が 存在するが

これは $h^{-1} \in G$ の 他ならない. ∴ $h^{-1} \in H$.

次に (i) (ii) (iii) が 成り立つとする.

(ii) より. 演算

$$\begin{array}{ccc} H \times H & \longrightarrow & H \\ \cup & & \cup \\ (h_1, h_2) & \longmapsto & h_1 \cdot h_2 \end{array}$$

が定まる. このとき. この演算が結合法則をみたすのは ok.

さらに (i) より 単位元の存在がいえる.

(iii) より 逆元の存在もいえる.

$\therefore$ H は G の部分群. //

例 G : 群

このとき. $\{e\}$, G と G は 部分群

これらを 自明な群 と呼ぶ.

例　$n \in \mathbb{Z}$

$\mathbb{Z} \supset n\mathbb{Z} = \{ nx \mid x \in \mathbb{Z} \}$ は $\mathbb{Z}$ の部分群

(一言)

(i)　$0 = n \cdot 0 \in n\mathbb{Z}$

(ii)　$nx + ny = n(x+y) \in n\mathbb{Z}$

(iii)　$-(nx) = n(-x) \in n\mathbb{Z}$.　//

例　$G = \mathbb{R}^\times = \mathbb{R} - \{0\}$

$(G, \cdot)$ は アーベル群.

つぎに.　$\{\pm 1\} \subset \mathbb{R}^\times$ は 部分群

(一言)

(i)　$1 \in \{\pm 1\}$

(ii)　$1 \cdot 1 = 1 \in \{\pm 1\}$　　$(-1) \cdot 1 = (-1) \in \{\pm 1\}$

$1 \cdot (-1) = -1 \in \{\pm 1\}$　　$(-1) \cdot (-1) = 1 \in \{\pm 1\}$

(iii)　$1^{-1} = 1 \in \{\pm 1\}$　　$(-1)^{-1} = (-1) \in \{\pm 1\}$

//

例 $SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid \det(A) = 1 \}$

は $GL_n(\mathbb{R})$ の部分群.

(i) $\det(E_n) = 1$ より. $E_n \in SL_n(\mathbb{R})$

(ii) $A, B \in SL_n(\mathbb{R})$ について

$$\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$$

より, $AB \in SL_n(\mathbb{R})$.

(iii) $A \in SL_n(\mathbb{R})$ について

$$\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$$

より. $A^{-1} \in SL_n(\mathbb{R})$ //

$SL_n(\mathbb{R})$ を 特殊線形群 という.

例1

$$O(n) = \{ A \in GL_n(\mathbb{R}) \mid {}^tA \cdot A = E_n \}$$

は $GL_n(\mathbb{R})$ の部分群.

(i) ${}^tE_n \cdot E_n = E_n$ より, $E_n \in O(n)$

(ii) $A, B \in O(n)$

$\longrightarrow$ ${}^t(AB)\,AB = {}^tB\,{}^tA\,A\,B$

$= {}^tB\,B = E_n$

より, $AB \in O(n)$.

(iii) $A \in O(n)$ について ${}^tA \cdot A = E_n$ より, ${}^tA = A^{-1}$ がいえる.

$\therefore {}^t(A^{-1}) \cdot A^{-1} = ({}^tA)^{-1} A^{-1} = ({}^tA)^{-1}\,{}^tA = E_n$

より, $A^{-1} \in O(n)$.

//

$O(n)$ は 直交群 という.

例 G: 群 $H_1, H_2 \subset G$: 部分群

このとき. $H_1 \cap H_2$ も 部分群

☺ (i) $e \in H_1$ $e \in H_2$ より $e \in H_1 \cap H_2$

(ii) $h_1, h_2 \in H_1 \cap H_2$ $\Rightarrow$ $h_1, h_2 \in H_1$ $h_1, h_2 \in H_2$

$\Rightarrow$ $h_1 \cdot h_2 \in H_1$ $h_1 \cdot h_2 \in H_2$

$\Rightarrow$ $h_1 \cdot h_2 \in H_1 \cap H_2$

(iii) $h \in H_1 \cap H_2$ $\Rightarrow$ $h \in H_1$ $h \in H_2$

$\Rightarrow$ $h^{-1} \in H_1$ $h^{-1} \in H_2$

$\Rightarrow$ $h^{-1} \in H_1 \cap H_2$

//

例 $SO(n) = O(n) \cap SL_n(\mathbb{R})$ も部分群

例 $A_n = \{ \sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1 \} \subset S_n$ は S_n の部分群

(i) $\mathrm{sgn}(e) = 1$ より $e \in A_n$

(ii) $\sigma, \tau \in A_n \Rightarrow \mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau) = 1 \cdot 1 = 1$

より $\sigma\tau \in A_n$

(iii) $\sigma \in A_n \Rightarrow \mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1} = \mathrm{sgn}(\sigma) = 1$ より

$\sigma^{-1} \in A_n$. //

A_n を交代群という.

例1 $i=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & \sqrt{-1}\end{pmatrix}$ $j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ $k=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}$

$H=\{\pm E_2, \pm i, \pm j, \pm k\} \subset G=GL_2(\mathbb{C})$

このとき $i^2=j^2=k^2=-E_2$

$ij=k=-ji$ $ik=-ki=j$

$ki=-ik=j$

が成立する. このとき H は部分群.

例2 $G=GL_n(\mathbb{R})$

$H=GL_n(\mathbb{Z})=\{A\in G \mid A$ の成分は整数 $\Rightarrow \det(A)=\pm 1\}$

このとき. H は G の部分群.

(i) $E_n \in GL_n(\mathbb{Z})$ は ok.

(ii) $A, B \in GL_n(\mathbb{Z})$

⇒ AB の成分は整数で

$\det(AB) = \det(A) \cdot \det(B) = (\pm 1)\cdot(\pm 1) = \pm 1$

$\therefore \quad AB \in GL_n(\mathbb{Z})$

(iii) $A \in GL_n(\mathbb{Z})$ とする.

余因子行列 A^* は整数~~係数~~成分を持つ.

ここで. $A^{-1} = \det(A)^{-1} A^T$

$= \pm A^*$

また. $\det(A^{-1}) = \det(A)^{-1} = (\pm 1)^{-1} = \pm 1$

$\therefore \quad A^{-1} \in GL_n(\mathbb{Z})$.

例1　G: 群　$g \in G$

$$\langle g \rangle = \{ g^n \in G \mid n \in \mathbb{Z} \}$$

すると $\langle g \rangle$ は G の部分群で可換群になる.

これを g によって生成される部分群という.

(∵)

(i) $e = g^0 \in \langle g \rangle$

(ii) $g^n, g^m \in \langle g \rangle \Rightarrow g^n \cdot g^m = g^{n+m} \in \langle g \rangle$

(iii) $g^n \in \langle g \rangle \Rightarrow (g^n)^{-1} = g^{-n} \in \langle g \rangle$

さらに可換群であるには

$$g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n$$

より分かる. //

定義4 G: 群

G が巡回群であるとは、ある $g \in G$ が存在し

$G = \langle g \rangle$ が成り立つことをいう。

例1 $G = \mathbb{Z}$ $\mathbb{Z} = \langle 1 \rangle$

例2 $n \in \mathbb{N}$ $G = \mathbb{Z}/n\mathbb{Z}$ $G = \langle \overline{1} \rangle$

元の位数

定義5 G: 群 $g \in G$

$g^n = e$ となる $n \in \mathbb{N}$ が存在するとき、

そのような n の最小の値を g の位数という。

$g^n = e$ となる $n \in \mathbb{N}$ が存在しないとき、g の位数は ∞ とする。

例 G: 群

e は G の位数は 1 (∵ $e^1 = e$)

逆に $g \in G$ の位数が 1 ならば $g = g^1 = e$ より $g = e$ がいえる.

∴ e は G の中で, 位数 1 の元.

例 $n < 0$ において $g^n = e$ のとき.

$g^{-n} = e$ となるので g の位数は有限.

例 $G = \mathbb{Z}$ $n \neq 0 \in \mathbb{Z}$

のとき. 任意の $m \in \mathbb{H}$ について $m \cdot n \neq 0$

より n の位数は ∞.

例 $n \in \mathbb{N}$ $G = \mathbb{Z}/n\mathbb{Z}$

このとき. $\overline{1}$ の位数は n

一般に $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ の位数は $\dfrac{n}{\gcd(m,n)}$ である.

例 $G = S_3$ (123) の位数は 3

(12) の位数は 2

例 G: 群 $g \in G$ について

$g^n = e \iff g^{-n} = e \iff (g^{-1})^n = e$

より g の位数 $= g^{-1}$ の位数

命題6　G: 有限群　すなわち　$|G| < \infty$

$g \in G$ について　g の位数は有限

(証)　G は有限集合なので

$\{g^i \mid i \in \mathbb{N}\}$ は有限集合.

∴ ある $i < j$ が存在して　$g^i = g^j$

$\Rightarrow$　$g^{j-i} = e$　//

よって　ok.