現代数学への流れ　第9回

部分群による商集合

G：群　　$H \subset G$：部分群

G 上に次の関係を導入する：

$g_1, g_2 \in G$ に対して

$$g_1 \sim g_2 \iff g_1 g_2^{-1} \in H$$

このとき $\sim$ は同値関係になる。

∵　(i)　$g_1 g_1^{-1} = e \in H$ より

$$g_1 \sim g_1$$

(ii)　$g_1 \sim g_2 \Rightarrow g_1 g_2^{-1} \in H \Rightarrow (g_1 g_2^{-1})^{-1} \in H$

$$\Rightarrow (g_2^{-1})^{-1} g_1^{-1} \in H \Rightarrow g_2 g_1^{-1} \in H \Rightarrow g_2 \sim g_1$$

(iii) $g_1 \sim g_2,\ g_2 \sim g_3 \Rightarrow g_1 g_2^{-1} \in H$ かつ $g_2 g_3^{-1} \in H$

$\Rightarrow g_1 g_2^{-1} \cdot g_2 \cdot g_3^{-1} \in H \Rightarrow g_1 g_3^{-1} \in H$

$\Rightarrow g_1 g_3^{-1} \in H$.

//

例 $G = \mathbb{Z}$, $n \in \mathbb{Z}$ $H = n\mathbb{Z}$

このとき. $x, y \in \mathbb{Z}$ に対して

$x \sim y \iff x - y \in n\mathbb{Z} \iff n \mid x - y$.

例 V: $\mathbb{C}$ 上 の ベクトル空間

$W \subset V$: 部分空間

$v, w \in V$ に対して

~~v~~ $v \sim w \iff$ ~~~~ $v - w \in W$

G, H について　$g \in G$ の剰余類

$$C(g) = \{ g' \in G \mid g \sim g' \}$$

を考える．このとき．

$$
\begin{aligned}
C(g) &= \{ g' \in G \mid g \sim g' \} \\
&= \{ g' \in G \mid g g'^{-1} \in H \} \\
&= \{ g' \in G \mid g' g^{-1} \in H \} \\
&= \{ g' \in G \mid \text{ある } h \in H \text{ が存在して } g' g^{-1} = h \} \\
&= \{ g' \in G \mid \text{ある } h \in H \text{ が存在して } g' = h g \} \\
&= \{ h g \in G \mid h \in H \} \\
&= H g
\end{aligned}
$$

となる．

$$\therefore \quad G/\sim \; = \{ C(g) \mid g \in G \}$$

$$= \{ Hg \mid g \in G \}$$

とでき、これを $H \backslash G$ と書く。

このとき、

$$\begin{array}{ccc} G & \to & H\backslash G \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ g & \mapsto & Hg \end{array}$$ が定まる。

同様にして G, H, $g_1, g_2 \in G$ に対して

$$g_1 \sim g_2 \iff g_1^{-1} g_2 \in H$$

と関係を導入すれば、これも同値関係になる（∵ 略）

このとき、 $C(g) = \{ g' \in G \mid g \sim g' \}$

$= \{ g' \in G \mid g^{-1} g' \in H \}$

$= \{ g' \in G \mid$ ある $h \in H$ が存在して $g^{-1} g' = h \}$

$= \{ g' \in G \mid$ ある $h \in H$ が存在して $g' = gh \}$

$= \{ gh \in G \mid h \in H \}$

$= gH$

となり、 $G/_{\sim} = \{ C(g) \mid g \in G \}$

$= \{ gH \mid g \in G \}$

となる。この集合を G/H と書く。

命題 1　G：群　$H \subset G$：部分群

このとき、以下がいえる。

(1) $\left| G/H \right| = \left| H \backslash G \right|$

(2) $\left| gH \right| = \left| Hg \right| = \left| H \right|$

(証) $\Phi : G/H \to H \backslash G$

$gH \mapsto Hg^{-1}$

と定めると、これは well-defined.

(証) $g' \in gH \Rightarrow g' = gh \quad (h \in H)$

このとき、$Hg'^{-1} = H(gh)^{-1} = Hh^{-1}g^{-1}$

このとき、 $Hh^{-1} = \{h'h^{-1} \mid h' \in H\} \subset H$

および $Hh \subset H \Rightarrow H \subset Hh^{-1}$ より $H = Hh^{-1}$ がいえる。

$\therefore \; Hh^{-1}g = Hg$.

同様に

$$\begin{array}{rccc} \Psi : & H \backslash G & \to & G/H \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & Hg & \mapsto & g^{-1}H \end{array}$$

も well-defined.

また、 $\Phi \circ \Psi = id$ 　 $\Psi \circ \Phi = id$ なので、

$\therefore$ Φ は全単射.

(2) $l_g : H \to gH$ これは全単射.

$h \mapsto gh$

全射は ok

$gh = gh' \Rightarrow h = h'$

より単射もいえる. //

$\therefore \ |H| = |gH|$

$|Hg| = |H|$ も同様. //

<u>定義2</u> $|G/H| = |H\backslash G| = [G:H]$ と書き.

Hの指数と呼ぶ.

定理3 (ラグランジュの定理)

G: 群 $H \subset G$: 部分群

このとき

$$|H|\,[G:H] = |G|$$

が成立.

∵ $R \subset G$ を G/H の完全代表系とすると.

$$G = \coprod_{g \in R} gH$$

$$\therefore\ |G| = \sum_{g\in R} |gH| = \sum_{g \in R} |H|$$

$$= |R| \cdot |H| = [G:H]\,|H|$$

//

系4 G: 有限群　$H \subset G$: 部分群

(1) $|H|$ は $|G|$ の約数

(2) 任意の $g \in G$ の位数は $|G|$ の約数.

(∵) (1) 定理3 より従う.

(2) $H = \langle g \rangle$ とおくと. $|H| = g$ の位数 なので, (1) より従う. //

命題5 p: 素数　G: 群

$|G| = p \Rightarrow G$ は巡回群

(∵) $g \in G$ を一つとる. $H = \langle g \rangle$ とおくと, $|H| \mid p$ だが
$\neq e$

$g \neq e$ より $|H| \geq 2$ $\therefore$ $|H| = p$ つまり, $G = \langle g \rangle$ がいえる. //

定理6 (Fermat の小定理)

p: 素数 $x \in \mathbb{Z}$ について

$$p \nmid x \Rightarrow x^{p-1} \equiv 1 \mod p$$

$p \nmid x$ より $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ がいえる。

$|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ より、$\bar{x}$ の位数は $p-1$ の約数。

$\therefore$ $\bar{x}^{p-1} \equiv 1 \mod p$ がいえる。 //

系7 $\forall x \in \mathbb{Z}$

$$x^p \equiv x \mod p$$

$p \mid x$ のとき $x^p \equiv 0 \equiv x \mod p$ より ok.

$p \nmid x$ のとき $x^{p-1} \equiv 1 \mod p$ より

両辺に x をかけて $x^p \equiv x \mod p$ がいえる。 //

例（S_3 の部分群）

S_3　$\langle (12) \rangle$, $\langle (23) \rangle$, $\langle (13) \rangle$

$\langle (123) \rangle$ 〜