数学展望 I **第 14 回：ガロアの理論**

4 次方程式の解法 (フェラーリの解法) を紹介し, ガロア理論の基本に触れる.

12.1　4 次方程式の解法

実数係数の 4 次方程式 $X^4 + aX^3 + bX^2 + cX + d = 0$ の解法 (**フェラーリの解法**) について述べる．3 次方程式の場合と同様に, X^3 の係数が 0 になるように変形して,

$$X^4 + pX^2 + qX + r = 0 \cdots\cdots (1)$$

を考えよう．$q = 0$ の場合は X^2 を 1 つの変数と思えば 2 次方程式の場合に帰着されるから, 以下では, $q \neq 0$ と仮定してよい．このとき, (1) を次の様に変形する:

$$\left(X^2 + \frac{y}{2}\right)^2 = (y - p)X^2 - qX + \left(\frac{y^2}{4} - r\right)$$

そこで, 右辺が $(\alpha X + \beta)^2$ の形になるように y を選んだとすると, その判別式を考えて,
y についての 3 次方程式 (もとの **4 次方程式の分解式**と言われる)

$$D = q^2 - (y - p)(y^2 - 4r) = 0, \quad \text{すなわち,} \quad y^3 - py^2 - 4ry - (q^2 - 4pr) = 0$$

が得られる．この 3 次方程式の根の 1 つを y_0 とすると, ($q \neq 0$ のとき, $y_0 \neq p$ に注意すれば) もとの 4 次方程式の根は 2 つの 2 次方程式

$$X^2 + \frac{y_0}{2} = \pm\sqrt{y_0 - p}\left(X - \frac{q}{2(y_0 - p)}\right)$$

を解いて得られる.

4 次方程式 $X^4 + pX^2 + qX + r = 0$ の根を x_1, x_2, x_3, x_4 とすると,

$$\begin{aligned} 0 &= x_1 + x_2 + x_3 + x_4 \\ p &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ -q &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ r &= x_1x_2x_3x_4 \end{aligned}$$

が成り立つ．右辺に現れた i 次式を x_1, x_2, x_3, x_4 に関する i 次の**基本対称式**と言う．一般に, 多項式 $F = F(x_1, x_2, x_3, x_4)$ において, どの 2 つの変数を入れ換えても同じ式が得られるとき, F を**対称式**と言う．符号だけ入れ替わる式を**交代式**と言う．例えば, 根の差積

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

は交代式であり, 判別式 $D = \Delta^2$ は対称式である.

定理 12.1. $x_1, \ldots, x_n$ についてのどんな対称式も基本対称式の整式 (整数係数の多項式) の形に書くことができる.　　例: $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2$.

今, $y = x_1x_2 + x_3x_4$, $y_2 = x_1x_3 + x_2x_4$, $y_3 = x_1x_4 + x_2x_3$ とおくと,

$$(y - y_1)(y - y_2)(y - y_3) = y^3 + c_1y^2 + c_2y + c_3$$

の各係数 c_1, c_2, c_3 は y_1, y_2, y_3 に対する基本対称式であるが, これらは x_1, x_2, x_3, x_4 に関する対称式でもある. したがって, それらは p, q, r の整式の形に書けるはずである.

問 1. 先に見た 4 次方程式の分解式は y_1, y_2, y_3 を 3 根にもつことを示せ.

12.2　ガロア対応

$\mathbb{C}$ の空でない部分集合 K が加減乗除で閉じているとき, K は**体** (正確には $\mathbb{C}$ の**部分体**) であると言う.

問 2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a,\, b \in \mathbb{Q}\}$ は $\mathbb{C}$ の部分体であることを示せ.
(注) $\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ と $\sqrt{2}$ を含む最小の体である.

$\mathbb{Q}$ 係数の n 次多項式 $f(X) = X^n + c_1X^{n-1} + \cdots + c_n$ の n 個の根を $\alpha_1, \ldots, \alpha_n$ とする. $\mathbb{Q}$ と $\alpha_1, \ldots, \alpha_n$ を含む最小の体を $f(X)$ の $\mathbb{Q}$ 上の**最小分解体**と呼び, $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ と表す.
$f(X) = X^3 - 2$ の 3 根は $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ だから, その最小分解体は,

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

である. (注) これは $(X^2 + X + 1)(X^3 - 2)$ の最小分解体に等しい.

$f(X) = 0$ の**ガロア群** G_f は n 次対称群 S_n の部分群である. G_f の元は n **根の置換**に少し肉付けしたものである[1]. 例えば, $X^4 - 2$ のガロア群は正 2 面体群 $D_{2\cdot 4}$ であり, $(X^2 - 2)(X^3 - 2)$ のガロア群は位数が 4 の**アーベル群** ($ab = ba$ が成り立つ群) である.

方程式の根がどのようにして得られるか, どんな根であるかなどを調べるには, $f(X) = 0$ の最小分解体の $\mathbb{Q}$ 上の拡大の様子 (部分体の有無など) を調べればよい. **ガロア理論の基本定理**によれば, **体の拡大の様子がガロア群の部分群の様子として記述される.**

群 G が可解群であるとは, "良い部分群[2]の列" の存在を意味する. そして, 方程式がべき根によって解けるのは, ガロア群が可解群になるときに限られる. しかるに, **5 次交代群** A_5 は可解群ではないから, それを含む群は可解群にはならない.

定理 12.2 (ルフィニ・アーベル). 一般に 5 次方程式は必ずしもべき根によって解くことができない.
例えば, $f(X) = X^5 - 4X + 2 = 0$ のガロア群は S_5 であり, この方程式はべき根によって解くことはできない.

[1] $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ の $\mathbb{Q}$ 自己同型群として得られる.
[2] N が G の正規部分群で, 剰余群がアーベル群である.