

低次の多項式に対し、

具体的に、その **Galois** 群を計算してみよう

- 既約性判定
(**Gauss** の補題・**Eisenstein** の判定法など)
- 有限群・置換群の知識
(置換群のリスト・**Sylow** の定理
・有限群の表現論など)
- 「根の間の関係式」の候補
(**判別式**・**分解式** (**解核多項式**) など)

分解式・解核多項式 (resolvent)

$R := K[\mathbf{X}] = K[X_1, \dots, X_n]$: n 変数多項式環

$\mathfrak{S}_n \curvearrowright R$: 変数の置換で作用 ($\sigma(X_i) = X_{\sigma(i)}$)

$P(\mathbf{X}) \in R$ に対し、

$${}^\sigma P(\mathbf{X}) = \sigma(P)(\mathbf{X}) := P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

$G_P := \{\sigma \in \mathfrak{S}_n \mid {}^\sigma P = P\}$: P の固定群

$S_P := \text{Ord}_{\mathfrak{S}_n}(P) = \{{}^\sigma P \mid \sigma \in \mathfrak{S}_n\}$: P の \mathfrak{S}_n -軌道

分解式・解核多項式 (resolvent)

$$G_P = \{\sigma \in \mathfrak{S}_n \mid \sigma P = P\}$$

$$S_P = \text{Ord}_{\mathfrak{S}_n}(P) = \{\sigma P \mid \sigma \in \mathfrak{S}_n\}$$

$$\begin{array}{ccc} S_P & \simeq & \mathfrak{S}_n / G_P \\ \sigma P & \longleftrightarrow & \sigma G_P \end{array}$$

(G-集合の準同型定理)

従って

$$\#S_P = \frac{n!}{\#G_P}$$

(Lagrange の定理!!)

分解式・解核多項式 (resolvent)

$f(X) \in K[X]$: 分離的, $\deg f = n$

$W = \{w_1, \dots, w_n\}$: f の根全体

$L := K(W) = \text{Spl}(f/K)$

: f の K 上の (最小) 分解体

$\varphi : R \longrightarrow L$: 全射環準同型

$h \longmapsto h(w_1, \dots, w_n)$

$I = I(f/K) := \text{Ker} \varphi$ とすると、

$$\text{Gal}(f/K) = \{\sigma \in \mathfrak{S}_n \mid \sigma(I) \subset I\}$$

分解式・解核多項式 (resolvent)

$P(\mathbf{X}) \in R$ に対し、

$$\begin{aligned} R(P; f)(T) &:= \prod_{Q \in S_P} (T - Q(w_1, \dots, w_n)) \\ &= \prod_{\sigma \in \mathfrak{S}_n / G_P} (T - {}^\sigma P(w_1, \dots, w_n)) \\ &\in K[T] \end{aligned}$$

: P に関する f の**分解式 (resolvent)**

$R(P; f)(T)$ の K 上の既約分解の様式で
 $\text{Gal}(f/K)$ を識別する

分解式・解核多項式 (resolvent)

$R(P; f)(T)$ の K 上の既約分解の様式

$$\updownarrow \quad 1:1$$

$\text{Gal}(f/K) \backslash \mathfrak{S}_n / G_P$ (両側剰余類分解)

実際には、

G_P が程々の大きさになる P を巧く取って、
 $\text{Gal}(f/K)$ を選り分けていく

例: 判別式 (discriminant)

$$\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j) \in R: \text{差積}$$

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (w_i - w_j)$$

$$D(f) = \Delta(f)^2 : f \text{ の判別式} \in K$$

$$G_\Delta = \mathfrak{A}_n, \quad S(\Delta) = \{\Delta, -\Delta\}$$

$$R(\Delta; f)(T) = T^2 - D(f) \in K[T]$$

$$R(\Delta; f)(T) : K \text{ 上可約} \iff \text{Gal}(f/K) \subset \mathfrak{A}_n$$

例: $n = 3$

$f \in K[X] : K$ 上既約、 $\deg f = 3$ のとき、

$\text{Gal}(f/K)$ は $D(f)$ で識別可能

	位数	偶奇 : $R(\Delta; f)(T)$ の分解
$\mathfrak{A}_3 = C_3$	3	+ : (1次) \times (1次)
$\mathfrak{S}_3 = D_3$	6	- : 2次既約

例: $n = 4$

$f \in K[X] : K$ 上既約、 $\deg f = 4$

$P(\mathbf{X}) := X_1X_3 + X_2X_4 \in R$

$G_P = \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle \simeq D_4$

$S_P =$
 $\{X_1X_2 + X_3X_4, X_1X_3 + X_2X_4, X_1X_4 + X_2X_3\}$

$R_3(f)(T) := R(P; f)(T) \in K[T]$

: **Cardano-Ferrari** の分解式

例: $n = 4$

	位数	偶奇	$R_3(f)$ の分解
C_4	4	-	(1次) \times (2次)
V_4	4	+	(1次) \times (1次) \times (1次)
D_4	8	-	(1次) \times (2次)
\mathfrak{A}_4	12	+	3次既約
\mathfrak{S}_4	24	-	3次既約

C_4 or D_4 を除いて、

$D(f)$ と $R_3(f)$ とで識別可能

実は、 $D(f) = D(R_3(f))$ なので、

$\text{Gal}(f/K) = C_4, D_4$

$$\implies \text{Spl}(R_3(f)/K) = K(\sqrt{D(f)})$$

例: $n = 4$

$f(X) = X^4 + pX^2 + qX + r$ のとき、

$$R_3(f)(T) = T^3 - pT^2 - 4rT - (q^2 - 4pr)$$

(Cardano-Ferrari の分解式)

特に、 $q = 0$ (複二次式) のときは、

$$\begin{aligned} R_3(f)(T) &= T^3 - pT^2 - 4rT + 4pr \\ &= (T - p)(T^2 - 4r) \end{aligned}$$

$$\longrightarrow \text{Gal}(f/K) \subset D_4$$

例: $n = 5$

\mathfrak{S}_5 の可移部分群のリスト

	位数	偶奇	構造
C_5	5	+	$\simeq \mathbf{Z}/5\mathbf{Z}$
D_5	10	+	$\simeq \{\pm 1\} \times \mathbf{Z}/5\mathbf{Z}$
$F_{5,4}$	20	-	$\simeq (\mathbf{Z}/5\mathbf{Z})^\times \times \mathbf{Z}/5\mathbf{Z}$
\mathfrak{A}_5	60	+	非可解 (単純群)
\mathfrak{S}_5	120	-	非可解

(共役を除いて5種)

例: $n = 5$

$f \in K[X] : K$ 上既約、 $\deg f = 5$

$P(\mathbf{X})$

$$\begin{aligned} &:= (X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1) \\ &\quad - (X_1X_3 + X_2X_4 + X_3X_5 + X_4X_1 + X_5X_2) \end{aligned}$$

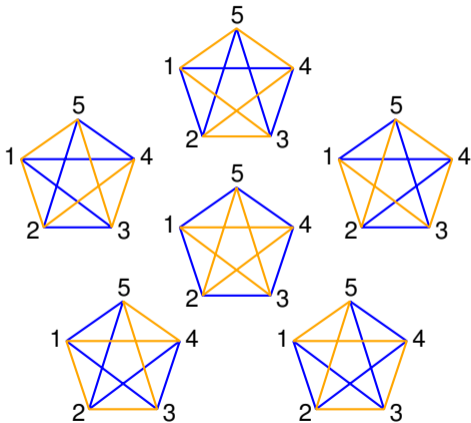
$$G_P = \langle (1\ 2\ 3\ 4\ 5), (1\ 4)(2\ 3) \rangle \simeq D_5$$

$$G_{P^2} = \langle (1\ 2\ 3\ 4\ 5), (1\ 2\ 4\ 3) \rangle \simeq F_{5,4}$$

$$R_6(f)(T) := R(P^2; f)(T) \in K[T]$$

: Cayley-Weber の分解式

例: $n = 5$



例: $n = 5$

	位数	偶奇	$R_6(f)$ の分解
C_5	5	+	(1次) \times (5次)
D_5	10	+	(1次) \times (5次)
$F_{5,4}$	20	-	(1次) \times (5次)
\mathfrak{A}_5	60	+	6次既約
\mathfrak{S}_5	120	-	6次既約

C_5 or D_5 を除いて、

$D(f)$ と $R_6(f)$ とで識別可能

特に、 $R_6(f)$ が K 内に根を持つ

$\iff \text{Gal}(f/K)$: 可解

Galois の逆問題 (構成問題)

K : 体と G : 可移部分群 $\subset \mathfrak{S}_n$ に対し、

$\text{Gal}(f/K) = G$ となるような $f(X) \in K[X]$ は

- 存在するか
- 存在するなら
 - ★ 具体的に構成せよ
 - ★ 沢山 (無限個・パラメタ付きで) 作れ
 - ★ 全部作れ

パラメタ付きの多項式

k : 体

$f(t; X) \in k(t)[X]$

: 係数にパラメタ t が入った多項式

- 有理関数体 $K := k(t)$ 上の多項式と見る
- $t = a \in \tilde{k} \supset k$ を代入する度に、
 $f_a(X) = f(a; X) \in \tilde{k}[X]$ を
 \tilde{k} 上の多項式と見る

多項式をパラメタ付きで作る

- 有理関数体上での構成
... 解析・幾何の援用

- パラメタに値を代入 (特殊化) する毎に
異なる多項式が得られる
→ G -拡大の無限族が得られることがある

多項式をパラメタ付きで作る

$C(t)$ 上での構成 ← 被覆・基本群

↓ **Weil descent** (定義体の降下)

$\overline{Q}(t)$ 上に落ちる

↓ ここは難しい (出来ない時もある?)

$Q(t)$ 上に落とす

↓ **Hilbert** の既約性定理

Q 上での **Galois** 群の構成