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)

$R := K[\mathbf{X}] = K[X_1, \ldots, X_n]$：$n$ 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、
$${}^{\sigma}P(\mathbf{X}) = \sigma(P)(\mathbf{X}) := P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

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

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

分解式・解核多項式 (resolvent)

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

$S_P = \mathrm{Ord}_{\mathfrak{S}_n}(P) = \{{}^\sigma P | \sigma \in \mathfrak{S}_n\}$

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

(G-集合の準同型定理)

従って

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

(Lagrange の定理!!)

Lagrange の定理(の元々の形)

n 次多項式の根から作った有理式 u に対し、

全ての根の置換 $n!$ 個のうち
u を不変にする置換が m 個ならば、

$$m \mid n!$$

であり、u は根の置換により
$d := \dfrac{n!}{m}$ 個の異なる値を取る。

更にこのとき、
u は係数から作られる d 次多項式の根である。

分解式・解核多項式 (resolvent)

$f(X) \in K[X]$: **分離的**, $\deg f = n$

$W = \{w_1, \ldots, w_n\}$: f **の根全体**

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

: f **の** K **上の (最小) 分解体**

$$\begin{aligned} \varphi : R &\longrightarrow L \\ h &\longmapsto h(w_1, \ldots, w_n) \end{aligned}$$: **全射環準同型**

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

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

分解式・解核多項式 (resolvent)

$P(X) \in R$ に対し、

$$\varphi(P) = P(w_1, \dots, w_n) \in L$$

$\varphi(P) \in L$ の K 上の共役は次の形:

$\sigma \in \mathrm{Gal}(L/K) = \mathrm{Gal}(f/K)$ に対し、

$$\begin{aligned}\sigma(\varphi(P)) &= P(\sigma(w_1), \dots, \sigma(w_n)) \\ &= P(w_{\sigma(1)}, \dots, w_{\sigma(n)}) \\ &= {}^{\sigma}P(w_1, \dots, w_n) = \varphi({}^{\sigma}P)\end{aligned}$$

しかし、この $\mathrm{Gal}(f/K)$ が判らない

分解式・解核多項式 (resolvent)

とにかく、$\mathrm{Gal}(f/K) \in \mathfrak{S}_n$ **なので、**

次の形ではある:

$\sigma \in \mathfrak{S}_n$ **に対し、**

$$\varphi({}^{\sigma}P) = {}^{\sigma}P(w_1, \ldots, w_n) = P(w_{\sigma(1)}, \ldots, w_{\sigma(n)})$$

(見た目上 $\#S_P$ **個)**

このうちのどれだけが実際の K **上の共役か？**

分解式・解核多項式 (resolvent)

$P(X) \in R$ に対し、

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

: 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 $\mathrm{Gal}(f/K)$ 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

$$\updownarrow \quad 1:1$$

$\mathrm{Gal}(f/K)\backslash\mathfrak{S}_n/G_P$ (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、
$\mathrm{Gal}(f/K)$ を選り分けていく

分解式・解核多項式 (resolvent)

自明な場合:

- $P = X_1$
  $G_P = \mathfrak{S}_{n-1}, \; S_P = \{X_1, \ldots, X_n\}$
  $$R(P; f)(T) = \prod_{i=1}^{n}(T - w_i) = f(T)$$
- P**: 対称式**
  $G_P = \mathfrak{S}_n, \; S_P = \{P\}$
  $R(P; f)(T) = T - P(w_1, \ldots, w_n) \in K[T]$

$\longrightarrow$ **これでは役に立たない**

例: 判別式 (discriminant)

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

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

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

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

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

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

例: $n = 3$

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

$\mathrm{Gal}(f/K)$ **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、**$\deg f = 4$

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

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

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

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

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**

判別式・分解式の具体的な計算

根の対称式

$\longrightarrow$ **基本対称式 (**$=\ \mathrm{f}$ **の係数) で書ける**

$\longrightarrow$ **実演へ**

4 次方程式の Ferrari の解法(回想)

$$f(X) = X^4 + pX^2 + qX + r = 0$$

補助変数 t を導入して、

$$(X^2 + t)^2 = (2t - p)X^2 - qX + (t^2 - r)$$

の右辺が完全平方になる

$$\Updownarrow$$

$$q^2 - 4(2t - p)(t^2 - r) = 0$$

これは t の 3 次方程式

$\longrightarrow$ **この t を用いて解く**

4 次方程式の Ferrari の解法(回想)

$$g(t) = q^2 - 4(2t - p)(t^2 - r)$$

: 3 次**分解式** (**解核多項式**,**resolvent**)

$T := 2t$ とおいて、

$$R(T) := -g\left(\frac{T}{2}\right)$$
$$= T^3 - pT^2 - 4rT - (q^2 - 4pr)$$

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**

	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、**

$\mathrm{Gal}(f/K) = C_4, D_4$ **のとき**

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

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、**

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

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

例: $n = 5$

$f \in K[X]$ **:** K **上既約、**$\deg f = 5$

$$P(\mathbf{X}) := (X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1) \\ -(X_1X_3 + X_2X_4 + X_3X_5 + X_4X_1 + X_5X_2)$$

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

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

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

: Cayley-Weber の分解式