2025(令和7)年度特別研究

対称式の基本定理

(指導教員　平野 幹)

1320077C 小松 純平
2320221U 森山 貴文
2320237Z 上野 広夢
2320134K 武田 大輝

次の式

$$x^2 + 2xy + y^2$$

は x と y を入れ替えても同じ式となる :

$$y^2 + 2yx + x^2 = x^2 + 2xy + y^2$$

このように, 文字を入れ替えても変わらない式を対称式という. また, この式は

$$x^2 + 2xy + y^2 = (x + y)^2$$

と表すことで x と y について対称であることがよりよく分かる.

以上は 2 変数の場合であるが, 一般に変数が 2 個以上の場合についても対称式というものを考えることができる. 以下, n 変数の場合を考える.

一般に対称式とは, 変数をどのように入れ替えても変わらない式のことをいう.

Ex 1. $k \in \mathbb{Z}_{\geq 0}$ に対し,

$$p_k = x_1^k + \cdots + x_n^k$$

は対称式であり, これをニュートン多項式という.

次に, 基本対称式について定義する.

Def 1. $i = 1, \ldots, n$ に対し,

$$\sigma_i \overset{\text{def}}{=} \sum_{1 \leq n_1 < \cdots < n_i \leq n} x_{n_1} \cdots x_{n_i}$$

これを $x_1, \ldots, x_n$ に関する基本対称式という.

Ex 2. 基本対称式について,

$$\begin{aligned}
&\sigma_1 = x_1 + \cdots + x_n \\
&\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\
&\sigma_n = x_1 \cdots x_n \\
&(X - x_1) \cdots (X - x_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n \qquad (1)
\end{aligned}$$

が成り立つ.

上で定義した基本対称式とニュートン多項式の間には関係があることが知られている.

Thm 1 (ニュートンの公式)**.** $k \in \mathbb{Z}_{\geq 1}$ に対し,

$$p_k - p_{k-1}\sigma_1 + p_{k-2}\sigma_2 - \cdots + (-1)^{m-1}p_{k-m+1}\sigma_{m-1} + (-1)^m \frac{m}{n} p_{k-m}\sigma_m = 0$$

が成り立つ. ただし, $m = \min\{n, k\}$.

(proof) まず $k \geq n$ のとき, Ex 2(1) の両辺に X^{k-n} をかけると,

$$(X - x_1) \cdots (X - x_n)X^{k-n} = X^k - \sigma_1 X^{k-1} + \cdots + (-1)^{n-1}\sigma_{n-1}X^{k-n+1} + (-1)^n\sigma_n X^{k-n}$$

この式の X に x_1 から x_n までをそれぞれ代入して,

$$\begin{cases}
x_1^k - \sigma x_1^{k-1} + \cdots + (-1)^{n-1}\sigma_{n-1}x_1^{k-n+1} + (-1)^n\sigma_n x_1^{k-n} = 0 \\
\qquad\qquad\qquad\qquad \vdots \\
x_n^k - \sigma x_n^{k-1} + \cdots + (-1)^{n-1}\sigma_{n-1}x_n^{k-n+1} + (-1)^n\sigma_n x_n^{k-n} = 0
\end{cases}$$

辺々足すと,

$$p_k - p_{k-1}\sigma_1 + \cdots + (-1)^{n-1}p_{k-n+1}\sigma_{n-1} + (-1)^n p_{k-n}\sigma_n = 0$$

となり, $m = n$ のときの式が得られる.

次に $k < n$ のとき, 式

$$p_k - p_{k-1}\sigma_1 + \cdots + (-1)^{k-1}p_1\sigma_{k-1} + (-1)^k k\sigma_k \tag{2}$$

は $x_1, \ldots, x_n$ に関して k 次の斉次式だから (2) の全ての項は

$$x_{i_1}^{\nu_1} \cdots x_{i_k}^{\nu_k} \ (1 \leq i_1 < \cdots < i_k \leq n,\ \nu_i \geq 0,\ \nu_1 + \cdots + \nu_k = k) \tag{3}$$

の定数倍として表すことができる. そこで, 項 $x_{i_1}^{\nu_1} \cdots x_{i_k}^{\nu_k}$ を 1 つ取ってその係数を考える.

(2) の x_j $(j \neq i_1, \ldots, i_k)$ に 0 を代入して得られる式の, (3) の係数は元の式のものと等しい.

一方, x_j $(j \neq i_1, \ldots, i_k)$ に 0 を代入して得られる式は $k = n$ のときのニュートンの公式と等しいから, 恒等式の性質より (3) の係数は 0.

よって (2) の全ての項の係数は 0 であり, $m = k$ のときのニュートンの公式

$$p_k - p_{k-1}\sigma_1 + \cdots + (-1)^{k-1}p_1\sigma_{k-1} + (-1)^k k\sigma_k = 0$$

が得られた. □

Ex 3. $n = 2,\ k = 2$ のときのニュートンの公式は,

$$p_2 - p_1\sigma_1 + p_0\sigma_2 = 0$$

実際,

$$(x_1^2 + x_2^2) - (x_1 + x_2)(x_1 + x_2) + 2x_1x_2 = 0$$

が成り立つ.

また, ニュートンの公式を用いて次の公式が得られる.

Thm 2 (ウェアリングの公式)**.** $k \in \mathbb{Z}_{\geq 1}$ に対し,

$$p_k = \sum_{i_1 + 2i_2 + \cdots + ni_n = k} (-1)^{i_2 + i_4 + \cdots} \frac{(i_1 + i_2 + \cdots + i_n - 1)!k}{i_1!\, i_2! \cdots i_n!} \sigma_1^{i_1}\sigma_2^{i_2} \cdots \sigma_n^{i_n}$$

が成り立つ. ただしこの和は, $i_1 + 2i_2 + \cdots + ni_n = k$ を満たす全ての非負整数 $i_1, \ldots, i_n$ にわたる和である.

(proof) k に関する帰納法で示す.

$k = 1$ のとき, $p_1 = \sigma_1$ より成り立つ.

次に, ある k 以下でウェアリングの公式が成り立つとし, $k + 1$ のときを考える. ニュートンの公式より,

$$\begin{aligned} p_{k+1} &= p_k\sigma_1 - p_{k-1}\sigma_2 + \cdots \\ &\qquad + (-1)^{m-2}p_{k-m+2}\sigma_{m-1} + (-1)^{m-1}\frac{m}{n}p_{k-m+1}\sigma_m \quad (m = \min\{n, k+1\}) \\ &= \sum_{j=1}^{m-1}(-1)^{j-1}p_{k-j+1}\sigma_j + (-1)^m\frac{m}{n}p_{k-m+1}\sigma_m \end{aligned}$$

$k+1 \leq n$ のとき, すなわち $m = k+1$ のとき,

$$\begin{aligned} p_{k+1} &= \sum_{j=1}^{k} (-1)^{j-1} p_{k-j+1}\sigma_j + (-1)^{k+1}(k+1)\sigma_{k+1} \\ &= \sum_{j=1}^{k} (-1)^{j-1} \sum_{i_1+2i_2+\cdots+ni_n=k-j+1} (-1)^{i_2+\cdots} \frac{(i_1+\cdots+i_n-1)!(k-j+1)}{i_1!\cdots i_n!} \sigma_1^{i_1}\cdots\sigma_j^{i_j+1}\cdots\sigma_n^{i_n} \\ &\qquad + (-1)^{k+1}(k+1)\sigma_{k+1} \\ &\qquad (\because \text{帰納法の仮定より}) \end{aligned}$$

ここで, $i_1+2i_2+\cdots+ni_n = k+1$ を満たす $i_1,\ldots,i_n \in \mathbb{Z}_{\geq 0}$ に対し, $\sigma_1^{i_1}\cdots\sigma_n^{i_n}$ の係数を考える.
$i_{k+1} = 0$ のとき, 係数は

$$\sum_{i_j\neq 0} (-1)^{i_2+\cdots} \frac{(i_1+\cdots+i_n-2)!(k-j+1)}{i_1!\cdots(i_j-1)!\cdots i_n!} = (-1)^{i_2+\cdots}\frac{(i_1+\cdots+i_n-2)!}{i_1!\cdots i_n!} \sum_{i_j\neq 0}(k-j+1)i_j \tag{4}$$

ここで,

$$\begin{aligned} \sum_{i_j\neq 0}(k-j+1)i_j &= (k+1)\sum_{i_j\neq 0} i_j - \sum_{i_j\neq 0} j i_j = (k+1)(i_1+\cdots+i_n) - (k+1) \\ &= (k+1)(i_1+\cdots+i_n-1) \\ \therefore (4) &= (-1)^{i_2+\cdots}\frac{(i_1+\cdots+i_n-1)!(k+1)}{i_1!\cdots i_n!} \end{aligned}$$

これは, $k+1$ のときのウェアリングの公式の係数と等しい.
$i_{k+1} = 1$ のとき $i_j = 0$ $(j \neq k+1)$ であり, 係数は

$$(-1)^{k+1}(k+1) = (-1)^{i_2+\cdots}\frac{(i_1+\cdots+i_n-1)!(k+1)}{i_1!\cdots i_n!}$$

したがって, $k+1$ $(\leq n)$ のときもウェアリングの公式が成り立つ.

また, $k+1 > n$ のとき, すなわち $m = n$ のとき,

$$p_{k+1} = \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1+2i_2+\cdots+ni_n=k-j+1} (-1)^{i_2+\cdots} \frac{(i_1+\cdots+i_n-1)!(k-j+1)}{i_1!\cdots i_n!} \sigma_1^{i_1}\cdots\sigma_j^{i_j+1}\cdots\sigma_n^{i_n}$$

$k+1 \leq n$ のときと同様に, $\sigma_1^{i_1}\cdots\sigma_n^{i_n}$ $(i_1+2i_2+\cdots+ni_n = k+1)$ の係数は

$$(-1)^{i_2+\cdots}\frac{(i_1+\cdots+i_n-1)!(k+1)}{i_1!\cdots i_n!}$$

となる. □

Ex 4. $n = 2,\ k = 5$ のときのウェアリングの公式を考える. $i_1+2i_2 = 5$ を満たす i_1, i_2 の組は,

$$(i_1, i_2) = (5,0), (3,1), (1,2)$$

の 3 通り. よって,

$$p_5 = (-1)^0\frac{(5+0-1)!\ 5}{5!\ 0!}\sigma_1^5\sigma_2^0 + (-1)^1\frac{(3+1-1)!\ 5}{3!\ 1!}\sigma_1^3\sigma_2^1 + (-1)^2\frac{(1+2-1)!\ 5}{1!\ 2!}\sigma_1^1\sigma_2^2$$

$$= \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2$$

実際,

$$x_1^5 + x_2^5 = (x_1 + x_2)^5 - 5(x_1 + x_2)^3 x_1 x_2 + 5(x_1 + x_2)(x_1 x_2)^2$$

が成り立つ.

ウェアリングの公式より, ニュートン多項式は基本対称式の多項式として表されることが分かった. 実は一般に, すべての対称式は基本対称式の多項式として表されることが知られている (対称式の基本定理). 次に, この証明をガロア理論を用いて行う.

ガロア理論について紹介するために, まずは体の拡大について確認する.

以下, K を体とする.

Def 2. L, F : 体とする. このとき,

(1) L が K の拡大体 (L/K と表す) $\overset{\text{def}}{\iff}$ L は K を部分体としてもつ

(2) F が L/K の中間体 $\overset{\text{def}}{\iff}$ L/F かつ F/K

(3) L を K 上のベクトル空間としてみたときの次元 ($\dim_K L$) が有限のとき, L/K を有限次拡大といい,

$$[L : K] \overset{\text{def}}{=} \dim_K L$$

とする. これを L/K の拡大次数という.

拡大次数について, 以下の命題が知られている.

Prop 1. L/K : 有限次拡大, $F : L/K$ の中間体とする. このとき,

$$[L : K] = [L : F][F : K]$$

が成り立つ. また, $\{u_1, \ldots, u_n\}$ を L/F の基底, $\{v_1, \ldots, v_m\}$ を F/K の基底とすると,

$$\{u_i v_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$$

は L/K の基底である.

Def 3. $L/K,\ \Omega$: 体とする. このとき,

(1) L/K が代数拡大 $\overset{\text{def}}{\iff}$ $\forall \alpha \in L,\ \exists f \in K[X]$ s.t. $f(\alpha) = 0$

(2) Ω が代数的閉体
$\overset{\text{def}}{\iff}$ $\forall f \in \Omega[X]\ (\deg f = n),\ \exists c, \alpha_1, \ldots, \alpha_n \in \Omega$ s.t. $f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$

(3) Ω が K の代数的閉包 $\overset{\text{def}}{\iff}$ Ω : 代数的閉体かつ K の代数的拡大体

代数的閉包に関して, 次の定理が知られている.

Thm 3. K は同型を除いてただ 1 つ代数的閉包をもつ.

以下, L/K: 有限次代数拡大とし, K の代数的閉包 Ω を 1 つとって固定する.

Def 4. $\alpha \in L$ に対し, $I = \{f \in K[X] \mid f(\alpha) = 0\}$ は $K[X]$ のイデアルであるから,

$$\exists! f_\alpha \in K[X] : \text{モニック s.t. } I = (f_\alpha) \quad (\because K[X] : \text{PID}, \alpha : K \text{ 上代数的})$$

この f_α を α の最小多項式という.

最小多項式と拡大次数について, 次の命題が知られている.

Prop 2. $\alpha \in \Omega$ に対し,

$$[K(\alpha) : K] = \deg f_\alpha$$

また, $\deg f_\alpha = n$ とすると, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ は $K(\alpha)/K$ の基底である.

次に, ガロア理論について紹介する.

Def 5. (1) $f \in K[X]$ が分離的 $\overset{\text{def}}{\iff}$ f は Ω 内で重根を持たない

(2) L/K がガロア拡大 $\overset{\text{def}}{\iff}$ $\exists f \in K[X] : \text{分離的}$ s.t. $f = (X - \alpha_1) \cdots (X - \alpha_n)$
$(n = \deg f, \alpha_1, \ldots, \alpha_n \in \Omega)$ としたとき,

$$L = K(\alpha_1, \ldots, \alpha_n)$$

また, L/K がガロア拡大のとき,

$$G(L/K) \overset{\text{def}}{=} \{\sigma : L \to L \mid \sigma : \text{環同型}, \ \sigma a = a \ (\forall a \in K)\}$$

とおき, これを L/K のガロア群という.

Rem. (1) ガロア群は写像の合成を演算として群をなす.
(2) $[L : K] = \#G(L/K)$ が成り立つ.

ガロア拡大について, 次の定理が知られている.

Thm 4 (ガロア理論の基本定理)**.** L/K : ガロア拡大 とし,

$$\mathscr{F} = \{F \mid F : L/K \text{ の中間体 }\}$$
$$\mathscr{G} = \{G \mid G : G(L/K) \text{ の部分群 }\}$$

とする. このとき, 写像

$$\mathscr{F} \to \mathscr{G}; F \mapsto G(L/F) = \{\sigma \in G(L/K) \mid \sigma a = a \ (\forall a \in F)\}$$

は全単射で, その逆写像は

$$\mathscr{G} \to \mathscr{F}; G \mapsto L^G = \{a \in L \mid \sigma a = a \ (\forall \sigma \in G)\}$$

対称式に関する議論をガロア理論を用いてするために, ここで改めて対称式について定義する.

Def 6. S_n を n 次対称群とする.
(1) S_n から L への作用を以下で定義する.

$$\sigma f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \quad (\sigma \in S_n, \ f \in L)$$

(2) $f \in L$ が対称有理式 $\overset{\text{def}}{\iff}$ $\sigma f = f \ (\forall \sigma \in S_n)$
特に f が多項式のとき, f を対称多項式という.

Thm 5. $M = K(\sigma_1, \ldots, \sigma_n)$ とする. このとき,

$$M = L^{S_n}$$

すなわち, すべての対称有理式は基本対称式の有理式として表される.

(proof) $f(X) = (X - x_1) \cdots (X - x_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n \in M[X]$ とおく. このとき, $x_1, \ldots, x_n$ は $f(X)$ の全ての根であり相異なる. よって f は分離的であり,

$$L = M(x_1, \ldots, x_n) \quad (\because L = K(x_1, \ldots, x_n) \text{ で, } M \text{ は } L/K \text{ の中間体})$$

が成り立つ. よって, L/M はガロア拡大.

ここで, $\sigma \in S_n$ は $L \to L$ の同型写像である. また, $\sigma \in S_n$ は M の元を動かさないから,

$$\begin{aligned} S_n &\subset G(L/M) \\ \therefore \#S_n &\leq \#G(L/M) \end{aligned} \tag{5}$$

一方, $\forall \tau \in G(L/M),\ \forall i \in \{1, \ldots, n\}$ に対し,

$$\begin{aligned} f(x_i) = 0 \iff \tau(f(x_i)) = 0 &\iff f(\tau x_i) = 0 \quad (\because f \in M[X] \text{ かつ } \tau a = a\ (\forall a \in M)) \\ &\iff \tau x_i = x_j\ (\exists j \in \{1, \ldots, n\}) \end{aligned}$$

よって, $x_i \mapsto \tau x_i = x_j$ を $i \mapsto j$ と同一視すると, τ: 単射より写像 $\varphi : G(L/M) \to S_n$ が与えられる. ここで, $L = M(x_1, \ldots, x_n)$ より,

$$\tau x_i = \rho x_i\ (\tau, \rho \in G(L/M),\ \forall i \in \{1, \ldots, n\}) \Longrightarrow \tau a = \rho a\ (\forall a \in L) \Longrightarrow \tau = \rho$$

よって, φ は単射である.

$$\begin{aligned} &\therefore \#G(L/M) \leq \#S_n \\ &\therefore \#G(L/M) = \#S_n \\ &\therefore G(L/M) = S_n \quad ((5) \text{ より}) \end{aligned}$$

したがって, ガロア理論の基本定理より

$$M = L^{S_n}$$

□

Thm 5 より, 以下の定理が示される.

Thm 6 (対称式の基本定理)**.**

$$K[x_1, \ldots, x_n] \cap M = K[\sigma_1, \ldots, \sigma_n]$$

すなわち, すべての対称多項式は基本対称式の多項式として表される.

(proof) $i \in \{1, \ldots, n\}$ に対し,

$$M_{i-1} = M(x_i, \ldots, x_n)$$

$$F_i(X) = (X - x_1)\cdots(X - x_i) = \frac{X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n}{(X - x_{i+1})\cdots(X - x_n)} \tag{6}$$

とおく. また, $M_n = M$ とおく. (6) の右辺の分数を実際に計算すると, 係数が $\sigma_1, \ldots, \sigma_n, x_{i+1}, \ldots, x_n$ の多項式となることが分かる. すなわち, $F_i \in M_i[X]$ である.

ここで, $M_{i-1} = M_i(x_i)$, $F_i(x_i) = 0$, $F_i \in M_i[X]$ より,

$$[M_{i-1} : M_i] = [M_i(x_i) : M_i] \leq \deg F_i = i$$

が分かる. 一方,

$$[M_0 : M_1][M_1 : M_2]\cdots[M_{n-1} : M_n] = [M_0 : M_n] = [L : M] = \#G(L/M) = \#S_n = n!$$

より, $[M_{i-1} : M_i] = i$ であることが分かる.

よって, M_{i-1}/M_i の基底の 1 つとして, $\{1, x_i, x_i^2, \ldots, x_i^{i-1}\}$ がとれる. したがって,

$$\{x_1^{\nu_1} \cdots x_n^{\nu_n} \mid 0 \leq \nu_i \leq i - 1\}$$

は L/M の基底である. よって, $\forall g \in L$ は

$$g = \sum_{0 \leq \nu_i \leq i-1} c_{\nu_1 \cdots \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n} \quad (c_{\nu_1 \cdots \nu_n} \in M) \tag{7}$$

の形に一意的に表せる.

ここで, $g \in K[x_1, \ldots, x_n]$ とする. $F_i(x_i) = 0$, $\deg F_i = i$, F_i : モニック, $F_i \in M_i[X]$ より, x_i^i は $\sigma_1, \ldots, \sigma_n, x_i, \ldots, x_n$ の多項式 (x_i の次数は $i - 1$ 以下) で表せる.

$$\begin{pmatrix} \text{例えば, } x_1 = \sigma_1 - x_2 - \cdots - x_n, \\ \qquad x_2^2 = (\sigma_1 - x_3 - \cdots - x_n)(x_2 + \cdots + x_n) - (\sigma_2 - x_3x_4 - x_3x_5 - \cdots - x_{n-1}x_n) \end{pmatrix}$$

これを $i = 1, \ldots, n$ と順次 g に代入すると, g は $\sigma_1, \ldots, \sigma_n, x_1, \ldots, x_n$ の多項式 (x_i の次数は $i - 1$ 以下) で表せる. これは (7) の表示となっているから,

$$g \in K[x_1, \ldots, x_n] \Longrightarrow c_{\nu_1 \cdots \nu_n} \in K[\sigma_1, \ldots, \sigma_n]$$

が従う. よって,

$$g \in K[x_1, \ldots, x_n] \cap M \Longrightarrow g = c_{0\cdots 0} \in K[\sigma_1, \ldots, \sigma_n]$$

$g \in K[\sigma_1, \ldots, \sigma_n] \Longrightarrow g \in K[x_1, \ldots, x_n] \cap M$ は明らかだから,

$$K[x_1, \ldots, x_n] \cap M = K[\sigma_1, \ldots, \sigma_n]$$

□

最後に, 対称式の基本定理をニュートン多項式でない対称式で確かめる.

Ex 5. 次の式

$$(x - y)^{10} + (y - z)^{10} + (z - x)^{10} \tag{8}$$

は x, y, z に関する対称式である. 対称式の基本定理より, (8) は $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$, $\sigma_3 = xyz$ の多項式として表されるが, これを実際に計算する.

$X = x - y$, $Y = y - z$, $Z = z - x$ とおき, X, Y, Z に関する基本対称式を $\sigma_1', \sigma_2', \sigma_3'$ とすると,

$$\begin{aligned}
\sigma_1' &= X + Y + Z = 0 \\
\sigma_2' &= XY + YZ + ZX = -x^2 - y^2 - z^2 + xy + yz + zx = -\sigma_1^2 + 3\sigma_2 \\
\sigma_3' &= XYZ = -x^2y - y^2z - z^2x + xy^2 + yz^2 + zx^2
\end{aligned}$$

ここで σ_3' は対称式でないが, $(\sigma_3')^2$ は対称式で,

$$(\sigma_3')^2 = -4\sigma_1^3\sigma_3 + \sigma_1^2\sigma_2^2 + 18\sigma_1\sigma_2\sigma_3 - 4\sigma_2^3 - 27\sigma_3^2$$

と表せる. また, ウェアリングの公式より,

$$(8) = X^{10} + Y^{10} + Z^{10} = \sum_{i+2j+3k=10} (-1)^j \frac{(i+j+k-1)!10}{i!\,j!\,k!} (\sigma_1')^i (\sigma_2')^j (\sigma_3')^k$$

$i + 2j + 3k = 10$ を満たす i, j, k の組は,

$$\begin{aligned}
(i,j,k) = {} & (10,0,0), (8,1,0), (7,0,1), (6,2,0), (5,1,1), (4,3,0), (4,0,2), \\
& (3,2,1), (2,4,0), (2,1,2), (1,3,1), (1,0,3), (0,5,0), (0,2,2)
\end{aligned} \tag{9}$$

の 14 通りあるが, $\sigma_1' = 0$ より $i > 0$ の項は 0 となる. よって,

$$\begin{aligned}
(8) = & -2(\sigma_2')^5 + 15(\sigma_2')^2(\sigma_3')^2 \\
= & -2(-\sigma_1^2 + 3\sigma_2)^5 + 15(-\sigma_1^2 + 3\sigma_2)^2(-4\sigma_1^3\sigma_3 + \sigma_1^2\sigma_2^2 + 18\sigma_1\sigma_2\sigma_3 - 4\sigma_2^3 - 27\sigma_3^2) \\
= & 2\sigma_1^{10} - 30\sigma_1^8\sigma_2 - 60\sigma_1^7\sigma_3 + 195\sigma_1^6\sigma_2^2 + 630\sigma_1^5\sigma_2\sigma_3 - 690\sigma_1^4\sigma_2^3 - 405\sigma_1^4\sigma_3^2 \\
& - 2160\sigma_1^3\sigma_2^2\sigma_3 + 1305\sigma_1^2\sigma_2^4 + 2430\sigma_1^2\sigma_2\sigma_3^2 + 2430\sigma_1\sigma_2^3\sigma_3 - 1026\sigma_2^5 - 3645\sigma_2^2\sigma_3^2
\end{aligned}$$

と基本対称式の多項式として表せた.

ところで, (9) が 14 通りなのに対し, この式は 13 項しかない. 具体的には, $(1, 0, 3)$ に対応する $\sigma_1\sigma_3^3$ という項がない. これは,

$$(x-y)^{10} + (y-z)^{10} + (z-x)^{10} = -2(\sigma_2')^5 + 15(\sigma_2')^2(\sigma_3')^2$$

において, σ_2' は 2 次式だから, ここに σ_3 は現れない. よって, σ_3 のパターンを決定しているのは $(\sigma_3')^2$ のところだけである. しかしこれは 6 次式だから, ここに σ_3^3 は現れない. よって, $\sigma_1\sigma_3^3$ という項が (8) に出てこないことが分かる.

参考文献

[1] 足立恒雄, ガロア理論講義 [増補版], 日本評論社, 2003.

[2] Lidl, R., Niederreiter, H., Finite fields, Second edition, Encyclopedia Math. Appl., 20, Cambridge University Press, Cambridge, 1997.