

# 不変式の話

—対称式と方程式から第14問題の反例へ—

向井 茂

- I. 初日は不変式の最も基本となる対称式から話を始める.
- II. 群の不変式はここからすぐそこにある. また, Hilbert の第 14 問題もすぐに定式化できる.
- III. 直接の関係はないが不変式の個数を数える定量的な話で不変式に親しもう. 第 3 日は方程式の不変式へと進む.
- IV. 最終日は頑張って第 14 問題に対する永田の反例に挑戦しよう. 近年その理解が進み紹介が容易になっている.

## §1 対称式

$x_1, \dots, x_n$  の多項式  $f(x_1, \dots, x_n)$  は変数の置換<sup>1</sup>に対して不変, すなわち,

$$f(\sigma(x_1), \dots, \sigma(x_n)) = f(x_1, \dots, x_n)$$

がすべての置換  $\sigma \in \mathfrak{S}_n$  に対して成立するとき, 対称式という. たとえば,  $x^3 + y^3 + z^3$  や  $xyz - 3$  などは  $x, y, z$  の対称式である.

例 1. 3 変数  $x, y, z$  の 2 次対称式は, 4 個の定数  $a, b, c, d$  でもって

$$a(x^2 + y^2 + z^2) + b(xy + xz + yz) + c(x + y + z) + d$$

と表される.

例 2. 3 変数  $x, y, z$  の 4 次斉次<sup>2</sup>対称式は, 4 個の定数  $a, b, c, d$  でもって

$$a(x^4 + y^4 + z^4) + b(x^3y + xy^3 + x^3z + xz^3 + y^3z + yz^3) + c(x^2y^2 + x^2z^2 + y^2z^2)$$

<sup>1</sup>集合  $\{x_1, x_2, \dots, x_n\}$  から自分自身への全単射. 添字の集合  $\{1, 2, \dots, n\}$  の置換と同一視する. また, これらの全体 ( $n!$  個ある) をドイツ文字  $\mathfrak{S}_n$  で表す.

$$+d(x^2yz + xy^2z + xyz^2)$$

と表される .

対称式にはいろいろと特別なものが知られているが , 次は最も基本的である . それは積

$$\prod_1^n (t + x_i) = (t + x_1)(t + x_2) \cdots (t + x_n)$$

を  $t$  に関して展開したときの係数

$$\begin{cases} s_1 = x_1 + x_2 + \cdots + x_n \\ s_2 = \sum_{i < j} x_i x_j \\ s_3 = \sum_{i < j < k} x_i x_j x_k \\ \cdots \\ s_n = x_1 x_2 \cdots x_n \end{cases}$$

で ,  $x_1, x_2, \dots, x_n$  の基本対称式と呼ばれる .  $s_r = s_r(x_1, x_2, \dots, x_n)$  は  $x_1, x_2, \dots, x_n$  から  $r$  個をとった  $\binom{n}{r}$  個の積の和である .

定理 1 (対称式の基本定理).  $x_1, x_2, \dots, x_n$  の対称式は基本対称式  $s_1, s_2, \dots, s_n$  の多項式として表される .

いろんな証明が知られている . よくあるのは単項式に辞書式順序を入れる方法である . 時間がありそうなら講義で証明するが , 各自で適当な代数学の本で勉強しておいて下さい .

演習問題  $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$  は  $x_1, x_2, x_3, x_4$  の対称式か ? もしそうなら , 基本対称式 of 多項式で表せ .

## §2 交代式

多項式  $f(x_1, \dots, x_n)$  は変数の互換でもって符号をかえる , すなわち ,

$$f(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -f(x_1, \dots, \overset{i}{x}_j, \dots, \overset{j}{x}_i, \dots, x_n), \quad 1 \leq i < j \leq n$$

---

<sup>2</sup>同次多項式ともいう . それに含まれる単項式  $x^p y^q z^r$  の総次数  $p + q + r$  が一定値である多項式のこと .

がみたまされるとき, 交代式と呼ばれる. たとえば,  $x_1^2 - x_2^2$  は  $x_1, x_2$  の交代式であり, 差積

$$\begin{aligned} \prod_{i < j} (x_i - x_j) &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \cdots (x_1 - x_n) \\ &\quad \times (x_2 - x_3)(x_2 - x_4) \cdots (x_2 - x_n) \\ &\quad \times (x_3 - x_4) \cdots (x_3 - x_n) \\ &\quad \vdots \\ &\quad \times (x_{n-1} - x_n) \end{aligned}$$

は  $x_1, x_2, \dots, x_n$  の交代式である. 以下, これを  $\Delta(x_1, x_2, \dots, x_n)$  で表す.

命題 2. 交代式はいつも差積  $\Delta(x)$  と対称式の積である.

例 3.  $x^3(y-z) + y^3(z-x) + z^3(x-y)$  は  $x, y, z$  の交代式である. これは  $(x-y)(x-z)(y-z)(x+y+z)$  と因数分解される.

二つの交代式の積は対称式である. とくに, 差積の平方  $\Delta(x)^2$  が対称式であることが重要である. 線形代数で習うように差積は行列式で表される (Vandermonde). 例えば,

$$\Delta(x, y, z) = \begin{vmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{vmatrix}$$

である. これをまねて沢山の交代式を構成することができる. 差積で割って沢山の対称式が得られる.

例 4. 非負整数  $p, q, r$  に対して, 行列式

$$\begin{vmatrix} x^p & y^p & z^p \\ x^q & y^q & z^q \\ x^r & y^r & z^r \end{vmatrix}$$

は  $x, y, z$  の交代式である. これを差積で割ってえられる対称式を Schur 関数という. 例えば,  $(p, q, r) = (0, 2, 3)$  のとき, それは 2 次基本対称式である.

$$\begin{vmatrix} 1 & 1 & 1 \\ x^2 & y^2 & z^2 \\ x^3 & y^3 & z^3 \end{vmatrix} = -(x-y)(x-z)(y-z)(xy+xz+yz)$$

よりみち すべての対称式は Schur 関数の (定数係数) 線形結合で表される. また, Schur 関数を具体的に基本対称式で表すことができる (Jacobi-Trudi の行列式). これらを使って定理 1 の別証ができる.

### §3 置換による不変式

よく知られているように, 置換には偶奇の2種類がある. 差積に変数変換したときは符号を除いて差積自身と一致する:

$$\Delta(\sigma(x_1), \dots, \sigma(x_n)) = \pm \Delta(x_1, x_2, \dots, x_n).$$

ここにおける符号が $+$ ,  $-$ に従って $\sigma$ を偶置換, 奇置換とよぶ. 偶置換全体の集合は通常 $\mathfrak{A}_n$ で表される. これは結合でもって閉じている.

定義 1. 多項式  $f(x_1, \dots, x_n)$  は変数の偶置換に対して不変, すなわち,

$$f(\sigma(x_1), \dots, \sigma(x_n)) = f(x_1, \dots, x_n)$$

がすべての偶置換  $\sigma \in \mathfrak{A}_n$  に対して成立するとき, 半対称式<sup>3</sup>という.

対称式や交代式, そしてそれらの和は半対称式であるが, これは逆も成立する.

補題 3. 半対称式は対称式と交代式の和に表される.

この補題と命題 2 より次をえる.

命題 4. 半対称式は二つの対称式  $f(x), g(x)$  でもって,  $f(x) + \Delta(x)g(x)$  として表される.

定理 1 と合わせて次をえる.

定理 5. 半対称式は基本対称式  $s_1, s_2, \dots, s_n$  と差積  $\Delta(x)$  の多項式として表される.

対称式や半対称式は置換の集合  $S \subset \mathfrak{S}_n$  に一般化される.

定義 2. 多項式  $f(x_1, \dots, x_n)$  は

$$f(\sigma(x_1), \dots, \sigma(x_n)) = f(x_1, \dots, x_n)$$

がすべての置換  $\sigma \in S$  に対して成立するとき,  $S$  不変式という.

$S$  が  $\mathfrak{S}_n$  全体するとき  $S$  不変式は対称式に他ならない.  $S$  として偶置換の全体  $\mathfrak{A}_n$  をとった場合が半対称式である.

<sup>3</sup>まだここだけの仮の用語なので公共の場で使うときには注意して下さい.

## §4 不変式

置換の全体  $\mathfrak{S}_n$  から  $n$  次正則行列の全体  $GL(n)$  に考察を拡張しよう. 正則行列  $A = (a_{ij})_{1 \leq i, j \leq n}$  とその定める変数変換を

$$x_i \mapsto Ax_i := \sum_{j=1}^n a_{ij}x_j, \quad 1 \leq i \leq n$$

を同一視する. 多項式  $f(x_1, \dots, x_n)$  は

$$f(Ax_1, \dots, Ax_n) = f(x_1, \dots, x_n)$$

をみたすとき,  $A$  不変という. また, 正則行列の集合  $S \subset GL(n)$  に関する不変性も置換のときと同様に定義する.

例 5. 2 変数多項式  $f(x, y)$  が  $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  で不変とは  $f(x, y) = f(x, -y)$  をみたすことである. そのような多項式はそれに含まれる各項の  $y$  のべき指数が偶数であるものに他ならない. よって,  $A$  不変な多項式は  $x$  と  $y^2$  の多項式である.

例 6.  $f(x, y)$  が  $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$  で不変とは  $f(x, y) = f(-x, -y)$  をみたすことで, それに含まれる各項の総次数が偶数ということである. よって,  $A$  不変な多項式は  $x^2, xy$  と  $y^2$  の多項式で表される.

置換による不変式は特別な線形変換 (置換行列) による不変式である. こう見る方が自由度が増えて考えやすい.

例 7. 4 変数  $x_1, x_2, x_3, x_4$  の 3 つの置換<sup>4</sup>(12)(34), (13)(24), (14)(23) による不変式

$$f(x_1, x_2, x_3, x_4) = f(x_2, x_1, x_4, x_3) = f(x_3, x_4, x_1, x_2) = f(x_4, x_3, x_2, x_1)$$

を考えよう. 新しい変数として,

$$\begin{cases} y_1 = x_1 + x_2 + x_3 + x_4 \\ y_2 = x_1 + x_2 - x_3 - x_4 \\ y_3 = x_1 - x_2 + x_3 - x_4 \\ y_4 = x_1 - x_2 - x_3 + x_4 \end{cases}$$

<sup>4</sup>恒等置換と合わせて Klein の 4 元群と呼ばれる群になる.

をとってくる．このとき，3つの置換は  $y_1$  を保つ．また， $y_2, y_3, y_4$  のうち一つは固定して他の二つの符号を入れ替える．言い換えると， $y_1, y_2, y_3, y_4$  という新変数に関して3つの線形変換

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix}$$

で不変な多項式と同値である．よって，不変式は  $y_1$  と  $y_2^2, y_3^2, y_4^2$  と  $y_2y_3y_4$  の多項式で表される（3次式  $y_2y_3y_4$  に関しては §1 末の演習問題を考えてみよ．）

## §5 Hilbert の第 14 問題

今まで多項式の係数の範囲をはっきりさせなかったが，有理数の全体  $\mathbb{Q}$ ，実数の全体  $\mathbb{R}$ ，複素数の全体  $\mathbb{C}$  のどれかで考えている．このような数の体系<sup>5</sup>の一つを以下では  $K$  で表す． $K$  の元を係数とする多項式  $f(x_1, \dots, x_n)$  の全体の集合を  $K[x_1, \dots, x_n]$  で表す．これは専門用語で「環」と呼ばれるものの一つの典型例である．<sup>6</sup>その意味するところは

「多項式どうしでもって足し算と引き算ができ，かけ算もでき，結合律や分配律等が成立している」

である． $K$  の元を成分とする  $n$  次正則行列の集合  $S \subset GL(n, K)$  に関して不変な多項式

$$f(Ax_1, \dots, Ax_n) = f(x_1, \dots, x_n), \quad \forall A \in S$$

全体のなす集合を  $K[x_1, \dots, x_n]^S$  で表す．

「 $S$  不変式同士でもって足し算と引き算したものやかけ算した結果はまた  $S$  不変式である」

が，このことを専門用語では

$K[x_1, \dots, x_n]^S$  は  $K[x_1, \dots, x_n]$  の部分環になっている

という．

<sup>5</sup>専門用語では体という．

<sup>6</sup>もう一つの典型例として整数全体のなす環  $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$  がある．

定義 3. すべての  $S$  不変式が  $f_1(x), \dots, f_N(x) \in K[x_1, \dots, x_n]^S$  の ( $N$  変数)  $K$  係数多項式で表されるとき,  $K[x_1, \dots, x_n]^S$  は ( $K$  上)  $f_1(x), \dots, f_N(x)$  で生成されるという.  $\{f_1(x), \dots, f_N(x)\}$  が  $S$  不変式の基本生成系であるともいう.

次はこれに関する基本的な問題である. 歴史的な背景はいろいろとあるが (§8), 問題を述べることは容易である.

Hilbert の第 14 問題  $S$  不変式環  $K[x_1, \dots, x_n]^S$  は有限個の不変式で生成されるか?<sup>7</sup>

有限変数の多項式環の部分環でも有限個の多項式で生成されない場合があることに注意しよう.

例 8. 2 変数多項式環  $K[x, y]$  の中で  $y = 0$  を代入して定数になる多項式  $a + yg(x, y)$  ( $a \in K$ ) の全体を  $R$  とする.  $R$  は無限個の単項式  $x^n y, n \geq 0$ , で生成されるが, 有限個の生成系はもたない.

最も簡単な肯定的結果は次である.

命題 6. 置換の集合  $S$  に対して  $S$  不変式環  $K[x_1, \dots, x_n]^S$  は有限個の不変式で生成される.

正則行列  $A$  に関しても  $B$  に関しても不変なら, 行列の合成  $AB$  に関しても不変である. また, 逆行列  $A^{-1}$  に関しても不変である.  $S \subset GL(n, K)$  が与えられたとき,  $S$  の元とそれらの合成や逆行列の操作の繰り返しでもって得られる行列すべてよりなる部分集合を  $G(S)$  とする. このとき,  $G(S) \subset GL(n, K)$  は合成と逆行列に関して閉じている. 専門用語では

$G(S)$  は  $GL(n, K)$  (正則行列全体のなす群) の部分群になっている

という.

このとき, 多項式  $f(x_1, \dots, x_n)$  が  $S$  で不変であるということと  $G(S)$  で不変であることは同値である. よって,  $S$  から  $G = G(S)$  に移行することにより, 最初から部分群  $G \subset GL(n, K)$  に限って  $G$  不変式を考えても一般性を失わない. ただし,  $S$  が有限集合であっても  $G(S)$  はそうとは限らないことに注意しよう.  $G(S)$  が有限というのは強い制約条件である.

命題 7. 線形変換の有限部分群  $G \subset GL(n, K)$  に対して  $G$  不変式環  $K[x_1, \dots, x_n]^G$  は有限個の不変式<sup>8</sup>で生成される.

<sup>7</sup>いくつかの version がある. その中でこれは線形作用版というべきものである.

<sup>8</sup>生成系の不変式はその次数をすべて  $|G|$  の元の個数 (位数) 以下にすることができる (Noether の定理).

## §6 Molien の公式

有限群の不変式環の構造を決めるのに有用な公式を紹介しよう． $K[x_1, \dots, x_n]$  内の  $d$  次単項式の個数は  $\binom{n+d-1}{d}$  である．これらは  $d$  次斉次多項式全体のなす  $K$  ベクトル空間  $K[x_1, \dots, x_n]_d$  の基底をなしている． $S$  不変な  $d$  次斉次多項式全体  $K[x_1, \dots, x_n]_d^S$  はこれの部分空間になっている．この次元を係数とする級数

$$\sum_{d=0}^{\infty} (\dim_K K[x_1, \dots, x_n]_d^S) t^d$$

を  $S$  不変式環の Hilbert 級数<sup>9</sup> という．

例 9.  $S = \emptyset$  のとき,  $K[x_1, \dots, x_n]^S = K[x_1, \dots, x_n]$  で, Hilbert 級数は  $(1-t)^{-n}$  に等しい．

例 10. 対称式全体のなす環  $K[s_1, \dots, s_n]$  と半対称式の環の Hilbert 級数はそれぞれ

$$\frac{1}{(1-t)(1-t^2)\cdots(1-t^n)}, \quad \frac{1+t^{n(n-1)/2}}{(1-t)(1-t^2)\cdots(1-t^n)}$$

に等しい．

これらの例は(不変式)環の構造が解っているから Hilbert 級数がわかるという場合であるが, そうではなく前もって Hilbert 級数を計算しておいてそれを道標にして環構造を決めてゆくという場合が多い．

$n$  次正方行列  $A$  に対して, 行列式  $\det(tI_n - A)$  で定義される  $n$  次多項式を  $A$  の固有多項式という．行列式  $\det(I_n - tA)$  は係数をひっくり返したもので反転固有多項式と呼ばれる．

定理 8. 有限群  $G \subset GL(n)$  の不変式環の Hilbert 級数は,  $A$  が  $G$  を動くときの,  $A$  の反転固有多項式の逆平均

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - tA)}$$

に等しい．

次の応用例が有名である．

<sup>9</sup>Poincaré 級数とも呼ばれる．母関数 (generating function) と呼ばれるものの一種である．



計算例 (拡大正 20 面体群)  $\varepsilon$  は 1 の原始 5 乗根として 3 つの 2 次正則行列

$$S := \begin{pmatrix} \varepsilon^3 & \\ & \varepsilon^2 \end{pmatrix}, \quad T := \frac{1}{\varepsilon^2 - \varepsilon^3} \begin{pmatrix} \varepsilon + \varepsilon^4 & 1 \\ 1 & -\varepsilon - \varepsilon^4 \end{pmatrix}, \quad U := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

を考えよう. これらはすべて行列式が 1 である.  $S$  は 5 乗して初めて単位行列  $I_2$  になる. すなわち, 位数 5 である.  $T$  と  $U$  は対角成分の和 (trace) が 0 なので, 位数は 4 である. 簡単ではないが, これらは正則行列全体  $GL(2, \mathbb{C})$  の中で<sup>10</sup>位数 120 の部分群を生成することが確かめられる ([K1, 第 1 部]). この群  $G_{icosa}$  に属する行列の位数の分布は次の通りである.

位数	1	2	3	4	5	6	10
個数	1	1	20	30	24	20	24
trace	2	-2	-1	0	$\cos 2\pi/5, \cos 4\pi/5$	1	$-\cos 2\pi/5, -\cos 4\pi/5$

よって, Hilbert 級数の 120 倍は

$$\begin{aligned} & \frac{1}{(1-t)^2} + \frac{1}{(1+t)^2} + \frac{20}{1+t+t^2} + \frac{30}{1+t^2} + \frac{24(1+\frac{t}{2}+t^2)}{1+t+t^2+t^3+t^4} \\ & + \frac{20}{1-t+t^2} + \frac{24(1-\frac{t}{2}+t^2)}{1-t+t^2-t^3+t^4} \end{aligned}$$

に等しい. 計算より, Hilbert 級数は

$$\frac{1+t^{30}}{(1-t^{12})(1-t^{20})} = \frac{1-t^{60}}{(1-t^{12})(1-t^{20})(1-t^{30})} \quad (1)$$

である.

これを展開することにより, 次数 12, 20, 30 の不変式が (定数倍を除いて) ひとつづつあることがわかる. 計算よりそれらを直接求めることもできるが, ここでは正 20 面体を用いて答えだけを述べよう. 正 20 面体を球面  $S$  に内接させたとき,  $S$  上には 12 個の頂点がのっている. この球面  $S$  を Riemann 球  $\mathbb{C}P^1 = \mathbb{C} \cup \{\infty\}$  と思って, 12 個の頂点の座標を  $\alpha_1, \dots, \alpha_{12} \in \mathbb{C}$  とする. このとき,

$$f(x, y) = \prod_{i=1}^{12} (x - \alpha_i y)$$

は  $G_{icosa}$  の 12 次不変式である. 座標系を上手に選ぶことにより,

$$f(x, y) = xy(x^{10} + 11x^5y^5 - y^{10})$$

<sup>10</sup>行列式 1 のもの全体  $SL(2, \mathbb{C})$  にも入っている. より精密にいうと, 特殊ユニタリ群  $SU(2)$  に入っている.

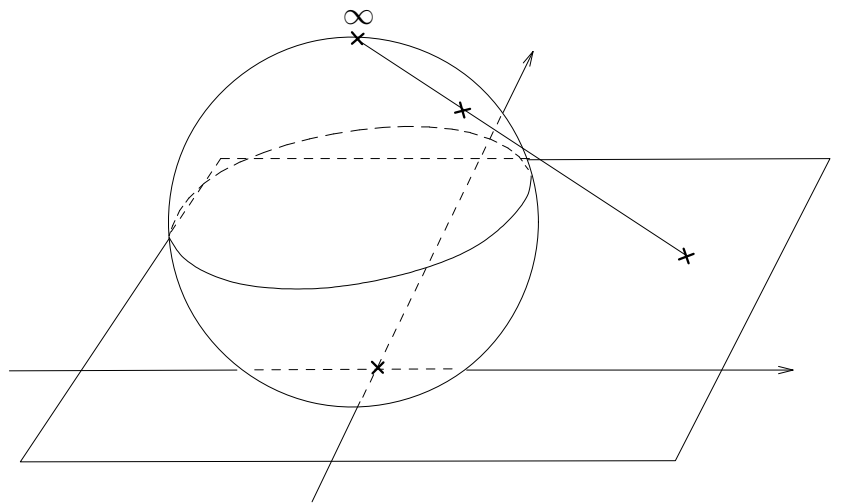
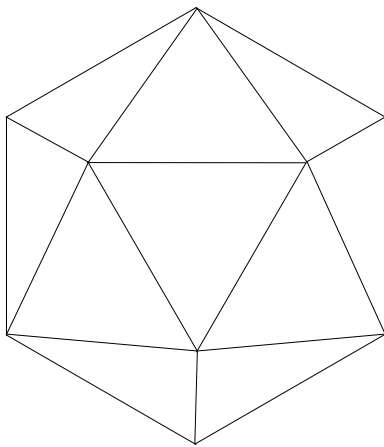
となる．この Hesse 行列式

$$H = \frac{1}{11^2} \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix} = -x^{20} + 228x^{15}y^5 - 494x^{10}y^{10} - 228x^5y^{15} - y^{20}$$

は次数 20 の不変式である．また,  $f$  と  $H$  の Jacobi 行列式

$$J = \frac{1}{20} \begin{vmatrix} f_x & f_y \\ H_x & H_y \end{vmatrix}$$

は次数 30 の不変式である．



### 正 20 面体と Riemann 球

(1) より, 次数 60 の不変式で線形独立なものは 2 個しかない．よって,  $f^5, H^3, J^2$  は線形従属である．実際

$$J^2 = 1728f^5 - H^3$$

の関係がある． $f, H$  は代数的に独立なので (1) より, 不変式環  $\mathbb{C}[x, y]^{G_{icosa}}$  は  $f, H, J$  で生成される．

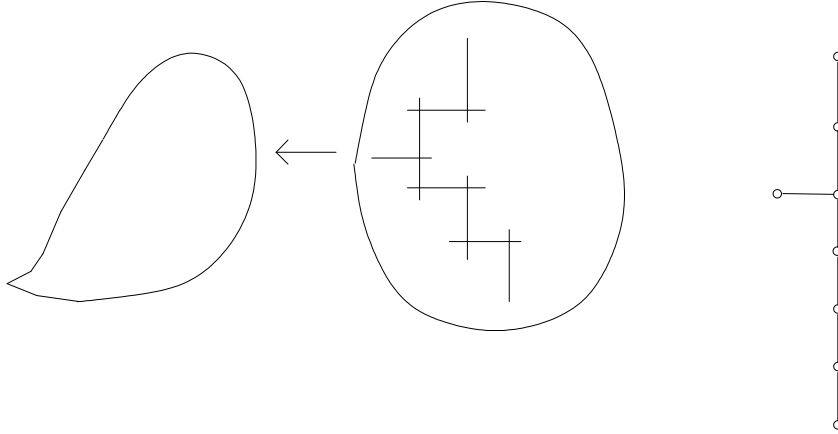
よりみち 高級なので解らなくても差し支えないが, 上の事実は代数幾何学の言葉では

アフィン平面  $A^2$  の拡大正 20 面体群による商多様体  $A^2/G_{icosa}$  は 3 次元アフィン空間  $A^3$  の中の曲面

$$w^2 = 1728u^5 - v^3$$

と同型である

と翻訳される．この曲面  $A^2/G_{icosa}$  は原点で特異であるが，これは  $E_8$  型の有理2重点と呼ばれるものである．この特異点の極小解消の例外集合には8本の射影直線が次のように交わって現われる．



$E_8$  型特異点の極小特異点解消と射影直線配置の双対グラフ

## §7 方程式の不変式

これから説明するのが数学史的な意味での「不変式」である．名著 [Be] の第 21 章 (不変の双子, Sylvester(1814–1897) と Cayley(1821–1895)) から引用しよう．

「不変式概念の多様な拡張は，代数的不変式の理論から自然に導きだされるものであるが，その代数的不変式論は，きわめて単純な観察から生み出された．Boole<sup>11</sup> についての章でも指摘するが，その考えの例は Lagrange<sup>12</sup> の業績のなかに見いだされる．そして Lagrange から Gauss<sup>13</sup> の整数論上の業績へと通じている．しかし，これら二人の学者は，この単純であるが代数的に注目し得る現象を，自分たちの眼前にしなから，それがより遠大な理論への芽を有しているということには気づかなかつたのである．Boole にしても，Lagrange の業績を研究しつづけ，大幅に拡張してゆく途上でそれを発見したのだが，そのことの意義を完全には理解していなかったように思われる．一度ささいな口論があったとき以外は，Sylvester 発見の優先権の問題について，Boole に対して公平で寛大な態度をとった．もちろん，Cayley もその点について，公平であった。」

「上述の単純な観察というのは，2 次方程式を解いてみたことのある人ならだれでも理解することができる．それはただつぎのようなことにすぎないのである．方程式  $ax^2 + 2bx + c = 0$  は重根をもつための必要にして十分な条件は， $b^2 - ac = 0$  が成り

<sup>11</sup>1815–1864

<sup>12</sup>1736–1813

<sup>13</sup>1777–1855

立つことである．ここで変数を1次(分数)変換  $y = (px + q)/(rx + s)$  によって新変数  $y$  に置き換えてみよう．そうすると,  $x$  は上式を  $x$  について解いた結果, つまり  $x = (q - sy)/(ry - p)$  によって置き換えられる．これによって与えられた方程式は  $y$  に関する別の方程式へと変換される．この新しい方程式が  $Ax^2 + 2Bx + C = 0$  になったとしよう．簡単な代数的計算によって, 新しい係数  $A, B, C$  は, 前の係数  $a, b, c$  によって次のように表される．

$$\begin{aligned} A &= as^2 - 2bsr + cr^2 \\ B &= -aqs + b(qr + sp) - cpr \\ C &= aq^2 - 2bpq + cp^2 \end{aligned}$$

この式からつぎのことが容易に導かれる(実際に  $A, B, C$  を計算しないでも, この結果を論理的に導き出す簡単な方法もあるが, もし必要なら, 別に小細工をほどこさない強引な計算によってこの結果を導くことができる)．

すなわち

$$B^2 - AC = (ps - qr)^2(b^2 - ac).$$

この  $b^2 - ac$  は  $x$  に関する2次方程式の判別式(discriminant)と呼ばれる．したがって,  $y$  に関する2次方程式の判別式は,  $B^2 - AC$  である．そしてつぎのことが示されたのである．すなわち, 変換後の方程式の判別式は, もとの方程式の判別式に, 因数  $(ps - qr)^2$  をかけたものに等しい．このかけられる因数は, 変数  $x$  を新変数  $y$  に変える1次変換  $y = (px + q)/(rx + s)$  の係数  $p, q, r, s$  にしか関係しない．

「このささいな事実のなかに, 注目すべき何物かがあることに最初に気づいたのは Boole であった(1841年)．すべての代数方程式は, 判別式をもっている．それは, 方程式の係数から作られる一定の形の式(例えば2次方程式に対しては,  $b^2 - ac$ )であって, 方程式の二つまたはそれ以上の根が等しい場合に, またそのときにかぎって0となる．Boole は, はじめにつぎのような疑問をもった．どんな方程式においても,  $x$  を, 前述の2次方程式の場合と同じような関係にある新変数  $y$  でおきかえる場合, 変数の際に用いられた係数だけからなる因数を除外すれば, 判別式に変化がないのではないだろうか, と．かれは, 実際にそれが変化しないことを発見した．つぎにかれは, こういう疑問をもった．すなわち, 係数からできている式で, 1次変換のもとで不変という特性をもっているものが, 判別式以外にはないものだろうか, と．かれは, 一般4次方程式に対して, そのような式が二つあることを見いだした(以下略)」

いくつか補足しよう．上で根と言ってるのは方程式の解のことである． $n$ 次方程式  $a_0x^n + \dots = 0$  の解を  $\alpha_1, \dots, \alpha_n$  とするとき, それらの差積の平方  $\Delta(\alpha_1, \dots, \alpha_n)^2$  は解の対称式である．よって, 解と係数の関係と定理1より,  $a_0$  以外の係数  $a_1, \dots, a_n$  を  $a_0$  で割ったものの多項式で表される．これに  $a_0^{2n-2}$  をかけたもの  $a_0^{2n-2}\Delta(\alpha_1, \dots, \alpha_n)^2$  は係数  $a_0, a_1, \dots, a_n$  の多項式である．これが, 上で判別式と呼んでいるものである．3















