グレブナ基底と代数多様体入門 (Ideals, Varieties, and Algorithms)

ashiato45 のメモ，著者は D.Cox, J.Little, D.O'Shea

2015 年 6 月 29 日

1　幾何，代数，アルゴリズム

2　グレブナ基底

3　消去理論

4　代数と幾何の対応

5　多様体上の多項式関数と有理関数

6　ロボティクスの幾何の定理の自動証明

7　有限群の不変式論

7.1　対称多項式

定理 3(対称式の基本定理): $k[x_1, \ldots, x_n]$ の任意の対称多項式は、基本対称式 $\sigma_1, \ldots, \sigma_n$ の多項式として一意に表すことができる。

証明

1. $x_1 > x_2 > \cdots > x_n$ という順序を使う。
2. $\forall f$: $f \in k[x_1, \ldots, x_n]$ を $f \neq 0$ とする。
3. a, α: $\mathrm{LT}(f) = ax^\alpha$
4. $\alpha_\bullet$: $\alpha = (\alpha_1, \ldots, \alpha_n)$
5. $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$?
   (a) $\exists i$: $\alpha_i < \alpha_{i+1}$ と仮定する。
   (b) β: $\beta = (\ldots, \alpha_{i+1}, \alpha_i, \ldots)$
   (c) 3 より、ax^α は f の項。
   (d) f は対称式なので、ax^β も f の項。
   (e) $\beta > \alpha$ なので、上は 3 の LT であることに矛盾。
   (f) $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$
6. h: $h = \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \ldots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$ とする。

7. 5 より、

$$\begin{aligned}\mathrm{LT}(h) &= \mathrm{LT}(\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\dots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}) &(1)\\ &= \mathrm{LT}(\sigma_1)^{\alpha_1-\alpha_2}\mathrm{LT}(\sigma_2)^{\alpha_2-\alpha_3}\dots\mathrm{LT}(\sigma_n)^{\alpha_n} &(2)\\ &= x_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3}\dots(x_1\dots x_n)^{\alpha_n} &(3)\\ &= x_1^{\alpha_1}\dots x^{\alpha_n}. &(4)\end{aligned}$$

8. 上より、$\mathrm{LT}(f) = \mathrm{LT}(ah)$ となる。
9. $f - ah \neq 0$ のときは、$f_1 = f - ah$ とする。
10. $\exists t$: 5-9 までの操作を繰替えすと、

$$\mathrm{multideg}(f) > \mathrm{multideg}(f_1) > \mathrm{multideg}(f_2) > \dots \tag{5}$$

をみたす列が得られる。これは停止するので、$f_{t+1} = 0$ となる t がある。
11. $f = ah + a_1h_1 + \dots + a_th_t$ となる。存在は示された。
12. g_1, g_2: $f = g_1(\sigma_1, \dots, \sigma_n) = g_2(\sigma_1, \dots, \sigma_n)$ とする。$g_1, g_2 \in k[y_1, \dots, y_n]$ とする。$g_1 = g_2$ を示したい。
13. g: $g = g_1 - g_2$
14. $g(\sigma_1, \dots, \sigma_n) = 0$
15. $g = 0$ を示したい。$g \neq 0$ と仮定する (背理法)。
16. $a_\bullet$: $g = \sum_\beta a_\beta y^\beta$ とする。
17. $g_\bullet$: $g_\beta = a_\beta\sigma_1^{\beta_1}\dots\sigma_n^{\beta_n}$ とする。$g_\beta \in k[x_1, \dots, x_n]$ になっている。
18. $g(\sigma_1, \dots, \sigma_n)$ は g_β たちの和である。$g(\sigma_1, \dots, \sigma_n) = \sum_\beta a_\beta g_\beta$ である。
19. 計算すると、

$$\mathrm{LT}(g_\beta) = a_\beta x_1^{\beta_1+\dots+\beta_n}x_2^{\beta_2+\dots+\beta_n}\dots x_n^{\beta_n} \tag{6}$$

20.

$$(\beta_1, \dots, \beta_n) \mapsto (\beta_1 + \dots + \beta_n, \beta_2 + \dots + \beta_n, \dots, \beta_n) \tag{7}$$

は単射である (尻尾から決めればいい。)。
21. 上と 19 より、g_β たちはそれぞれ異なる先頭項を持つ。
22. $\mathrm{LT}(g_\beta)$ が最高になるものを選べるが、上よりそのようなものは 1 つしかない。それを β にする。
23. $\gamma \neq \beta$ なら、$\mathrm{LT}(g_\beta)$ は g_γ のすべての項よりおおきい。

$$\mathrm{LT}(g_\beta) > \mathrm{LT}(g_\gamma) \geq (\forall g_\gamma\text{の項}) \tag{8}$$

24. $g(\sigma_1, \dots, \sigma_n)$ は $k[x_1, \dots, _n]$ で零でない[*1]。これは 14 に矛盾。

(証終)

命題 4: 環 $k[x_1, \dots, x_n, y_1, \dots, y_n]$ において、$x_1, \dots, x_n$ のうち 1 つでも含む単項式は、$k[y_1, \dots, y_n]$ のすべての単項式より大きくなるような単項式順序を 1 つ固定する。G をイデアル

$$\langle\sigma_1 - y_1, \dots, \sigma_n - y_n\rangle \subset k[x_1, \dots, x_n, y_1, \dots, y_n] \tag{9}$$

のグレブナ基底とする。このとき、次のことが成り立つ。

(i) f が対称であることと、$g \in k[y_1, \dots, y_n]$ は同値である。
(ii) f が対称ならば、$f = g(\sigma_1, \dots, \sigma_n)$ は、f の基本対称式 $\sigma_1, \dots, \sigma_n$ の多項式としての一意的な表示である。

[*1] g が $k[y_1, \dots, y_n]$ のなかで零であることを示したかった。そのこととは違う。

証明

1. $g_\bullet$: $G = \{g_1, \ldots, g_t\}$ とする。
2. $f, A_\bullet, g$: f を G で割る。

$$f = A_1 g_1 + \cdots + A_t g_t + g. \tag{10}$$

3. $\Leftarrow$ を示す。$g \in k[y_1, \ldots, y_n]$ とする。
   (a) 仮定の $f \in k[x_1, \ldots, x_n]$、$y_\bullet$ がないことより、$f(x_1, \ldots, x_n, \sigma_1, \ldots, \sigma_n) = f$ である。
   (b) $y_\bullet \Leftarrow \sigma_\bullet$ という代入操作を行うと、$\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$ の元はすべて 0 になる。
   (c) 上のことより $y_\bullet \Leftarrow \sigma_\bullet$ によって $g_1, \ldots, g_t \in \langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$ は 0 になる。
   (d) 2 に $y_\bullet \Leftarrow \sigma_\bullet$ すると、(a)-(c) より、

$$f = g(\sigma_1, \ldots, \sigma_n) \tag{11}$$

   である。
   (e) f は対称である。
4. $\Rightarrow$ を示す。$f \in k[x_1, \ldots, x_n]$ が対称であるとする。
   (a) g'[*2]: $f = g'(\sigma_1, \ldots, \sigma_n)$ となるような $g' \in k[y_1, \ldots, y_n]$ が存在する。
   (b) (f を G でわったあまりが g'?)
   (c) $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_{\geq 0}$ とすると、$B_1, \ldots, B_n \in k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ を用いて、

$$\begin{aligned} \sigma_1^{\alpha_1} \ldots \sigma_n^{\alpha_n} &= (y_1 + (\sigma_1 - y_1))^{\alpha_1} \ldots (y_n + (\sigma_n - y_n))^{\alpha_n} && (12) \\ &= y_1^{\alpha_1} \ldots y_n^{\alpha_n} + B_1 \cdot (\sigma_1 - y_1) + \cdots + B_n \cdot (\sigma_n - y_n). && (13) \end{aligned}$$

   とかける。
   (d) 上より、g' の $y_\bullet$ たちでできた単項式について上を適用し足し合わせて、

$$g'(\sigma_1, \ldots, \sigma_n) = g'(y_1, \ldots, y_n) + C_1 \cdot (\sigma_1 - y_1) + \cdots + C_n \cdot (\sigma_n - y_n). \tag{14}$$

   となる $C_1, \ldots, C_n \in k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ である。
   (e) (a) と上より、

$$f = C_1 \cdot (\sigma_1 - y_1) + \cdots + C_n \cdot (\sigma_n - y_n) + g'(y_1, \ldots, y_n). \tag{15}$$

   (f) (g' は f を G でわった余り？)
   (g) g' のどの項も、$\mathrm{LT}(G)$ の項でも割りきれない？
      i. g' のある項が $\mathrm{LT}(G)$ のある項で割り切れるとする。
      ii. $\exists i$: $\mathrm{LT}(g_i)$ が g' を割り切るような $g_i \in G$ がある。
      iii. $g' \in k[y_1, \ldots, y_n]$ より、$\mathrm{LT}(g_i)$ は $y_1, \ldots, y_n$ だけを含む。
      iv. 上と、順序付の仮定[*3]より $g_i \in k[y_1, \ldots, y_n]$ となる。
      v. $g_i \in \langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$ なので、$g_i(\sigma_1, \ldots, \sigma_n) = 0$ となる。
      vi. 上より、g_i は $k[x_1, \ldots, x_n]$ として対称多項式である。
      vii. 上と定理 3、それに v より、$g_i \in k[y_1, \ldots, y_n]$ は $k[y_1, \ldots, y_n]$ の元として 0 である。
      viii. 上は、g_i がグレブナ基底の一個であり、非零であることに矛盾する。
      g' のどの項も、$\mathrm{LT}(G)$ のどの項を使っても割り切ることはできない。
   (h) (e),(g) と、G がグレブナ基底であることより、f を G で割ったあまりは g' である。
   (i) 上より、$g = g' \in k[y_1, \ldots, y_n]$ となり、$g \in k[y_1, \ldots, y_n]$ である。

後半の (ii) は、$f = g(\sigma_1, \ldots, \sigma_n)$ となっていることは上の考察から従う。それが一意であることは定理 3 から従う。

[*2] 本だと字がぶつかっていてやばい。
[*3] $x_\bullet$ を含んだら $y_\bullet$ だけの単項式より大きい

(証終)

命題 5: $k[x_1,\dots,x_n,y_1,\dots,y_n]$ 上の $x_1>\cdots>x_n>y_1>\dots y_n$ で決まる lex 順序を固定する。このとき、$k=1,\dots,n$ に対して、多項式

$$g_k = h_k(x_k,\dots,x_n)+\sum_{i=1}^{k}(-1)^i h_{k-i}(x_k,\dots,x_n)y_i \tag{16}$$

は、イデアル $\langle\sigma_1-y_1,\dots,\sigma_n-y_n\rangle$ のグレブナ基底をなす。

証明
演習問題 10 をとく。h_k は、次数 k の単項式すべての和である。x^α は k 次の単項式であり、x^α にあらわれる変数の個数を a とする。

(a)「x^α が $h_{k-i}\sigma_i$ のなかに現れるならば、$i\le a$ を示せ。」
x^α も $h_{k-i}\sigma_i$ のすべての項も次数 k なので次数の心配はいらない。仮に $i>a$ とする。σ_i にはちょうど i 個の変数があらわれるので、$h_{k-i}\sigma_i$ のすべての項には i 個以上の変数があらわれ、つまり a よりも真に大きい個数の変数があらわれる。このとき、x^α の変数の個数は a なのだから、$h_{k-i}\sigma_i$ の項たちにあらわれることができない。対偶が示された。

> $i\le a$ ならば、σ_i のなかのちょうど $\binom{a}{i}$ 個の項が、x^α にあらわれる変数だけを含んでいる。

(b) あきらか。

> $i\le a$ ならば、x^α は係数 $\binom{a}{i}$ を持つ $h_{k-i}\sigma_i$ の項であることを示せ。

(c) σ_i のなかから x^α に含まれている変数だけを持っているものを選び、それに対して適当な h_{k-i} の項を選んでかければ (これは h_{k-i} の定義より可能である。) 多重次数は α に一致する。また、x^α に含まれていない変数を選んでものそのようなことはできない。よって、x^α の $h_{k-i}\sigma_i$ での係数は、σ_i での x^α に含まれる係数だけを持つもの全体の個数と一致する。よって、それは上の問題より $\binom{a}{i}$ である。

> $\sum_{i=0}^{k}(-1)^i h_{k-i}{\sigma_i}^{*4}$における x^α の係数は $\sum_{i=0}^{\alpha}(-1)^i\binom{a}{i}$ であることを結論せよ。それから 2 項定理を使って x^α の係数が 0 であることを示せ。

(d) 係数は上よりあきらか。係数も、これは $(1-1)^a$ なので簡単。
(e) 以上で、

$$0=\sum_{i=0}^{k}(-1)^i h_{k-i}h_i(x_1,\dots,x_n)\sigma_i(x_1,\dots,x_n). \tag{17}$$

次に、問題 11 をとく。$S\subset\{1,\dots,k-1\}$ のとき、x^S で変数の積をあらわす。

(a)「

$$\sigma_i(x_1,\ldots,x_n)=\sum_{S\subset\{1,\ldots,k-1\}} x^S\sigma_{i-|S|}(x_k,\ldots,x_n) \tag{18}$$

ここで、$j<0$ のとき $\sigma_j=0$。」左と右の項を考えれば。

$$\sum_{i=0}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_i(x_1,\ldots,x_n)=\sum_{S\subset\{1,\ldots,k-1\}} x^S(\sum_{i=|S|}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_{i-|S|}(x_k,\ldots,x_n)). \tag{19}$$

(b) (a) の式に $(-1)^i h_{k-i}$ をかけて $\sum_{i=0}^{k}$ をとる。$\sigma_{\text{負の数}}=0$ に注意して、

$$\sum_{i=0}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_i(x_1,\ldots,x_n)=\sum_{S\subset\{1,\ldots,k-1\}} x^S(\sum_{i=0}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_{i-|S|}(x_k,\ldots,x_n)) \tag{20}$$

$$=\sum_{S\subset\{1,\ldots,k-1\}} x^S(\sum_{i=|S|}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_{i-|S|}(x_k,\ldots,x_n)). \tag{21}$$

$$\sum_{i=|S|}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_{i-|S|}(x_k,\ldots,x_n)=0 \tag{22}$$

(c)

$$\sum_{i=|S|}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)\sigma_{i-|S|}(x_k,\ldots,x_n)=\sum_{j=0}^{k-|S|}(-1)^{j+|S|}h_{k-j-|S|}(x_k,\ldots,x_n)\sigma_j(x_k,\ldots,x_n) \tag{23}$$

$$=(-1)^{|S|}\sum_{j=0}^{k-|S|}(-1)^j h_{(k-|S|)-j}(x_k,\ldots,x_n)\sigma_j(x_k,\ldots,x_n) \tag{24}$$

$$\overset{\boxed{\text{問題 10}}}{=}0. \tag{25}$$

次に演習 12 をとく。

$$g_k=h_k(x_k,\ldots,x_n)+\sum_{i=1}^{k}(-1)^i h_{k-i}(x_k,\ldots,x_n)y_i \tag{26}$$

としてある。

$$g_k=(-1)^k(y_k-\sigma_k)+\sum_{i=1}^{k-1}(-1)^i h_{k-i}(x_k,\ldots,x_n)(y_i-\sigma_i) \tag{27}$$

は既知。

(a)「

$$\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle \subset \langle g_1, \ldots, g_n \rangle \tag{28}$$

」$\sigma_1 - y_1 = g_1$ なので、$\sigma_1 - y_1 \in$ (右) となる。$(-1)^2\sigma_2 - y_2 = g_2 - g_1 \in$ (右) となる。以降おなじ。

(b) $\mathrm{LT}(g_k) = x_k^k$ であること。定義の式からあきらか y_i を含まないほうしか見るものがない。

(c) $g_1, \ldots, g_k$ がグレブナ基底？ (b) より、$i \neq j$ のとき、$\mathrm{LT}(g_i)$ と $\mathrm{LT}(g_j)$ は互いに素になっている。よって、命題 9-4 より、$S(g_i, g_j) \to_G 0$ になる。よって、命題 9-3 より、$\{g_1, \ldots, g_n\}$ はグレブナ基底になっている。

証明する。

1. 演習 10 と 11 より、

$$0 = h_k(x_k, \ldots, x_n) + \sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \ldots, x_n)\sigma_i. \tag{29}$$

2. $g_1, \ldots, g_n$ は $\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$ の基底？
   (a) g_k の定義

$$g_k = h_k(x_k, \ldots, x_n) + \sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \ldots, x_n)y_i \tag{30}$$

   から 1 の式を引いて、

$$g_k = \sum_{i=1}^{k} (-1)^i h_{k-i}(x_k, \ldots, x_n)(y_i - \sigma_i). \tag{31}$$

   (b) よって、$\langle g_1, \ldots, g_n \rangle \subset \langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle$
   (c) (a) から、

$$g_k = (-1)^k(y_k - \sigma_k) + \sum_{i=1}^{k-1} (-1)^i h_{k-i}(x_k, \ldots, x_n)(y_i - \sigma_i). \tag{32}$$

   (d) 上と演習 12 より、$\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle \subset \langle g_1, \ldots, g_n \rangle$。
   (e) (b)(d) より、$\langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle = \langle g_1, \ldots, g_n \rangle$ となる。
3. 演習問題 12 で $\mathrm{LT}(g_k) = x_k^k$ を示して、さらにグレブナ基底であることを示す。おわり。

(証終)

命題 7:多項式 $f \in k[x_1, \ldots, x_n]$ が対称であることと、f のすべての斉次成分が対称であることは同値である。

証明
$\Rightarrow$ を示せばよい。f が対称であるとする。

1. $\forall i_1, \ldots, i_n$: $x_{i_1}, \ldots, x_{i_n}$ を $x_1, \ldots, x_n$ の置換とする。
2. 置換しても、次数はかわらない。
3. $f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)$
4. 上 2 つより、全次数が k の斉次も対称。

(証終)

定理 8: k が有理数体 $\mathbb{Q}$ を含む体ならば、$k[x_1, \ldots, x_n]$ の任意の対称多項式はベキ和 $s_1, \ldots, s_n$ の多項式として表せる。

証明
演習 14 をやる。ニュートン恒等式は

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0 \quad (1 \le k \le n), \tag{33}$$
$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0 \quad (k > n) \tag{34}$$

である。

1. 「$\sigma_0 = 1$ と $i < 0, i > n$ のときに $\sigma_i = 0$ としておく。このとき、

$$^\forall k \ge 1\text{: } s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0 \tag{35}$$

と同値？」$k \le n$ と $k > n$ とで分ける。
2. 「上の恒等式を変数の数 n に関する帰納法で示せ。ただし、n 変数の σ_i を σ_i^n、s_k を s_k^n とする。」$n = 1$ のとき: $1 \le k \le n$ のとき、すなわち $k = 1$ のときを考える。

$$\underbrace{s_k^1 - \sigma_1^1 s_{k-1}^1 \cdots + (-1)^{k-1}\sigma_{k-1}^1 s_1^1}_{k\text{コ}} + (-1)^k k\sigma_k^1 = s_1^1 + (-1)^1 \cdot 1 \cdot \sigma_1^1 = x_1 - x_1 = 0. \tag{36}$$

$k > n$ のとき、すなわち $k > 1$ のときを考える。このときは、σ_0, σ_1 だけが非零になる。

$$\underbrace{s_k^1 - \sigma_1^1 s_{k-1}^1 \cdots + (-1)^{k-1}\sigma_{k-1}^1 s_1^1}_{k\text{コ}} + (-1)^k k\sigma_k^1 = s_1^1 + \sigma_1^1 s_0^1 + (-1)^1 \cdot 1 \cdot \sigma_1 \tag{37}$$
$$= x_1 + x_1 \cdot 0 - x_1 \tag{38}$$
$$= 0. \tag{39}$$

$n - 1$ 変数でうまく行っているとする。???

(証終)

7.2 有限行列群と不変式環

$\mathbb{Q} \subset k$ とする。

定義 1: 体 k の元を成分に持つ可逆な $n \times n$ 行列全体の集合を $GL(n, k)$ であらわす。

定義 2: 有限部分集合 $G \subset GL(n, k)$ が有限行列群であるとは、空でなく、行列のかけ算で閉じていることをいう。G の元の個数を、G の位数とよび、$|G|$ であらわす。

$G \subset GL(n, k)$ を有限行列群とする。

(i) $I_n \in G$。
(ii) $A \in G$ ならば、ある正の整数 m があって、$A^m = I_n$ となる。
(iii) $A \in G$ ならば、$A^{-1}G$ である。

証明

- (ii):
  1. $A \in G$ とする。
  2. G が積で閉じているので、$\{A, A^2, A^3, \dots\} \subset G$ である。

3. i, j: G は有限なので、$A^i = A^j$ となる $i, j \in \mathbb{N}$ がある。$i > j$ とする。
4. $m = i - j$ とする。
5. 3 より、$A^m = A^{i-j} = A^i A^{-j} = E$ となる。m が条件をみたしたことになる。

- (iii):
  1. $I_n = A^{m-1} \cdot A$ となる。m は上のもの。
  2. G は積で閉じているので、$A^{m-1} \in G$ となる。
  3. $A^{-1} = A^{m-1} \in G$ となる。
- (i): $I_n = A^m \in G$ となる。

(証終)

定義 7: $G \subset GL(n,k)$ を有限行列群とする。多項式 $f(\mathbb{x}) \in k[x_1, \ldots, x_n]$ が、すべての $A \in G$ に対して、$f(\mathbb{x}) = f(A \cdot \mathbb{x})$ をみたすとき、G で不変であるという。G で不変な多項式全体の集合を $k[x_1, \ldots, x_n]^G$ であらわす。

例 8:

$$k[x_1, \ldots, x_n]^{S_n} = \{k[x_1, \ldots, x_n]\text{内のすべての対称多項式}\} \tag{40}$$

命題 9: $G \subset GL(n,k)$ を有限行列群をする。このとき、集合 $k[x_1, \ldots, x_n]^G$ は和と積で閉じており、すべての定数多項式を含む。

証明
演習 10。

- 和:$f(\mathbb{x}), g(\mathbb{x}) \in k[x_1, \ldots, x_n]^G$ とする。

$$(f+g)(A\mathbb{x}) = f(A\mathbb{x}) + g(A\mathbb{x}) = f(\mathbb{x}) + g(\mathbb{x}) = (f+g)(\mathbb{x}). \tag{41}$$

- 積:f, g は同様。

$$(fg)(A\mathbb{x}) = f(A\mathbb{x})g(A\mathbb{x}) = f(\mathbb{x})g(\mathbb{x}) = (fg)(\mathbb{x}). \tag{42}$$

- 定数を含む:$c \in k$ とする。

$$c(A\mathbb{x}) = c = c(\mathbb{x}). \tag{43}$$

$c \in k[x_1, \ldots, x_n]^G$ である。

(証終)

命題 10: $G \subset GL(n,k)$ を有限行列群とする。このとき、多項式 $f \in k[x_1, \ldots, x_n]$ が G で不変であることと、その斉次成分がすべて G で不変であることとは同値である。

証明
$\mathbb{x} \mapsto A\mathbb{x}$ は次数を変えないので、A によって単項式はその次数を変えない。よって、$f(\mathbb{x})$ の次数 N のものは $f(A\mathbb{x})$ の次数 N のものに移ることになる。

$F: \{f(\mathbb{x})\text{の項}\} \to \{f(A\mathbb{x})\text{の項}\}$ f が不変なので、F は可逆写像になっている。$N \in \mathbb{Z}_{\geq 0}$ とする。$F|_{\{\text{次数}N\text{の項}\}}: \{f(\mathbb{x})\text{の}N\text{次の項}\} \to \{f(A\mathbb{x})\text{の項}\}$ だが、先の考察より $\mathbb{x} \mapsto A\mathbb{x}$ は次数を変えないので、

$F|_{\{\text{次数}N\text{の項}\}}: \{f(\mathbb{x})\text{の}N\text{次の項}\} \to \{f(A\mathbb{x})\text{の}N\text{次の項}\}$ になっている。F が単射だったので、$F|_{\{\text{次数}N\text{の項}\}}$ も単射になっている。よって、$\#\{f(\mathbb{x})\text{の}N\text{次の項}\} \leq \#\{f(A\mathbb{x})\text{の}N\text{次の項}\}$ となる。さらに、F が有限集合同士の可逆写像なので、

$$\#\{f(\mathbb{x})\text{の項}\} = \#\{f(A\mathbb{x})\text{の項}\} = \sum_N \#\{f(A\mathbb{x})\text{の}N\text{次の項}\} \geq \sum_N \#\{f(\mathbb{x})\text{の}N\text{次の項}\} = \#\{f(\mathbb{x})\text{の項}\} \quad (44)$$

なので、各 N について、$\#\{f(\mathbb{x})\text{の}N\text{次の項}\} = \#\{f(A\mathbb{x})\text{の}N\text{次の項}\}$ となり、$F|_{\{\text{次数}N\text{の項}\}}$ は同型になる。これは、斉次成分が G で不変であることを意味する。

(証終)

補題 11: $G \in GL(n,k)$ を有限行列群とし、$A_1, \ldots, A_m \in G$ が存在して、任意の $A \in G$ を次の形で表すことができる。

$$A = B_1 B_2 \ldots B_t. \quad (45)$$

ここで、各 i に対して $B_i \in \{A_1, \ldots, A_m\}$ である。(このとき $A_1, \ldots, A_m$ は群 G を生成するという。) このとき、$f \in k[x_1, \ldots, x_n]$ が $k[x_1, \ldots, x_n]^G$ の元であることと、

$$f(\mathbb{x}) = f(A_1\mathbb{x}) = \cdots = f(A_m\mathbb{x}) \quad (46)$$

が成り立つことは同値である。

証明

1. f が行列 $B_1, \ldots, B_t$ すべての作用で不変であるとする。このとき積 $B_1 \ldots B_t$ でも f は不変？
   (a) $t = 1$ のときはあきらか。$t-1$ のとき成立すると仮定する。t で示す。
   (b)

$$f((B_1 \ldots B_t)\mathbb{x}) = f((B_1 \ldots B_{t-1}) \cdot B_t \cdot \mathbb{x}) \quad (47)$$
$$= f(B_t \cdot \mathbb{x}) \quad (\text{帰納法の仮定}) \quad (48)$$
$$= f(\mathbb{x}). \quad (49)$$

2. $\Leftarrow$ を示す。f は $A_1, \ldots, A_m$ で不変であるとする。
   (a) $\forall A$: $A \in G$ とする。
   (b) $\exists t, B_\bullet$: 仮定より、$A = B_1 \ldots B_t$ となる $B_\bullet \in \{A_1, \ldots, A_m\}$ が存在する。
   (c) 1 より、f は A で不変である。
3. $\Rightarrow$ はあきらか。

(証終)

7.3 不変式環の生成元

定義 1: $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ に対して、$f_1, \ldots, f_m$ の k 係数の多項式全体で表される元全体からなる $k[x_1, \ldots, x_n]$ の部分集合を $k[f_1, \ldots, f_m]$ で表す。
$\langle f_1, \ldots, f_m \rangle$ とは違う。

定義 2: 有限行列群 $G \subset GL(n,k)$ に対し、次のように定義される写像 $R_G: k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ を G

のレイノルズ作用素という。すなわち、$f(\mathbb{x}) \in k[x_1, \ldots, x_n]$ に対し、

$$R_G(f)(\mathbb{x}) = \frac{1}{|G|} \sum_{A \in G} f(A\mathbb{x}). \tag{50}$$

命題 3: 有限行列群 G のレイノルズ作用素 R_G に対し、次が成り立つ。

(i) R_G は k 線型写像である。
(ii) $f \in k[x_1, \ldots, x_n]$ ならば $R_G(f) \in k[x_1, \ldots, x_n]^G$。
(iii) $f \in k[x_1, \ldots, x_n]^G$ ならば $R_G(f) = f$。

証明
(i) を示す。

$$\begin{aligned} R_G(af + bg)(\mathbb{x}) &= \frac{1}{|G|} \sum_{A \in G} (af + bg)(A\mathbb{x}) && (51)\\ &= \frac{a}{|G|} \sum_{A \in G} (f)(A\mathbb{x}) + \frac{b}{|G|} \sum_{A \in G} (g)(A\mathbb{x}) && (52)\\ &= aR_G(f)(\mathbb{x}) + bR_G(g)(\mathbb{x}) && (53)\\ &= (aR_G(f) + bR_G(f))(\mathbb{x}). && (54) \end{aligned}$$

(ii) を示す。

1. $\forall B$: $B \in G$
2. $$\begin{aligned} R_G(f)(B\mathbb{x}) &= \frac{1}{|G|} \sum_{A \in G} f(A \cdot B\mathbb{x}) && (55)\\ &= \frac{1}{|G|} \sum_{A \in G} (AB \cdot \mathbb{x}). && (56) \end{aligned}$$
3. $\exists A_\bullet$: $G = \left\{A_1, \ldots, A_{|G|}\right\}$ とする。重複のないようにしておく。
4. $i \neq j$ のとき、$A_iB \neq A_jB$ になる。
5. 上より、$\left\{A_1B, \ldots, A_{|G|}B\right\}$ はそれぞれ異なる $|G|$ 個の元である。
6. また、$\left\{A_1B, \ldots, A_{|G|}B\right\}$ は 1 の $B \in G$ より、$\subset G$ である。
7. 3,5,6 より、
$$G = \left\{A_1, \ldots, A_{|G|}\right\} = \left\{A_1B, \ldots, A_{|G|}B\right\} = \{AB; A \in G\}. \tag{57}$$
8. $$\frac{1}{|G|} \sum_{A \in G} f(AB \cdot \mathbb{x}) \overset{\boxed{7}}{=} \frac{1}{|G|} \sum_{A \in G} f(A \cdot \mathbb{x}) = R_G(f)(\mathbb{x}). \tag{58}$$
9. 1 おわり:
$$^\forall B \in G\text{: } R_G(f)(B \cdot \mathbb{x}) = R_G(f)(\mathbb{x}). \tag{59}$$
10. 上より、$R_G(f) \in k[x_1, \ldots, x_n]^G$ となる。

(iii) を示す。$f \in k[x_1, \ldots, x_n]^G$ とする。f は不変式なので、

$$R_G(f)(\mathbb{x}) = \frac{1}{|G|} \sum_{A \in G} f(A\mathbb{x}) = \frac{1}{|G|} \sum_{A \in G} f(\mathbb{x}) = f(\mathbb{x}). \tag{60}$$

(証終)

定理 5: 有限行列群 $G \subset GL(n, k)$ に対し、

$$k[x_1, \ldots, x_n]^G = k[R_G(x^\beta); |\beta| \leq |G|] \tag{61}$$

が成り立つ。特に、$k[x_1, \ldots, x_n]^G$ は有限個の斉次不変式で生成される。

証明
$\subset$ を示す。

1. $\forall f$: $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]^G$ とする。
2. 命題 3 より、

$$f = R_G(f) = R_G(\sum_\alpha c_\alpha x^\alpha) = \sum_\alpha c_\alpha R_G(x^\alpha). \tag{62}$$

3. 1 おわり: すべての不変式は $R_G(x^\alpha)$ の k 上の線形結合である。
4. すべての α について、$R_G(x^\alpha)$ が $|\beta| \leq |G|$ をみたす $R_G(x^\beta)$ に関する多項式？
   (a) $\forall k$: $k \in \mathbb{Z}_{\geq 0}$ とする。
   (b) a:

$$(x_1 + \cdots + x_n)^k = \sum_{|\alpha|=k} a_\alpha x^\alpha \tag{63}$$

   (c) a_α が正整数であることを示す。演習 4。$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ とし、$|\alpha| = k$ とする。

$$\binom{k}{\alpha} = \frac{k!}{\alpha_1! \ldots \alpha_n!}. \tag{64}$$

   i. 「$\binom{k}{\alpha}$ は正整数？」2 項係数が整数になることは既知とする[*5]。$n = 2$ のときは成立している。n のとき成立していると仮定する。

$$\begin{aligned}
\binom{k}{(\alpha_1, \ldots, \alpha_{n+1})} &= \frac{k!}{\alpha_1 \ldots \alpha_{n+1}} && (65)\\
&= \frac{(\alpha_1 + \cdots + \alpha_n)!}{\alpha_1! \ldots \alpha_n!} \cdot \frac{k \cdot \ldots \cdot (k - (\alpha_1 + \cdots + \alpha_n) + 1)}{\alpha_{n+1}!} && (66)\\
&= \binom{\alpha_1 + \cdots + \alpha_n}{(\alpha_1, \ldots, \alpha_n)} \cdot \frac{(\alpha_{n+1} + (\alpha_n + \cdots + \alpha_1)) \cdot \ldots \cdot (\alpha_{n+1} + 1)}{\alpha_{n+1}!} && (67)\\
&= \binom{\alpha_1 + \cdots + \alpha_n}{(\alpha_1, \ldots, \alpha_n)} \cdot \frac{(\alpha_{n+1} + (\alpha_n + \cdots + \alpha_1))!}{\alpha_{n+1}! (\alpha_n + \cdots + \alpha_1)!} && (68)\\
&= \binom{\alpha_1 + \cdots + \alpha_n}{(\alpha_1, \ldots, \alpha_n)} \cdot \binom{\alpha_{n+1} + \cdots + \alpha_1}{(\alpha_n + \cdots + \alpha_1, \alpha_{n+1})}. && (69)
\end{aligned}$$

   ii. 「

$$(x_1 + \cdots + x_n)^k = \sum_{|\alpha|=k} \binom{k}{\alpha} x^\alpha. \tag{70}$$

   」あきらか。

[*5] パスカルの三角形の漸化式で多分行ける。

(d) 記号を整備する。

$$(Ax)^{\alpha} = (A_1x)^{\alpha_1} \cdot (A_nx)^{\alpha_n} \tag{71}$$

と $\square^{\alpha}: k^n \to k$ を定める。

(e)

$$R_G(x^{\alpha}) = \frac{1}{|G|} \sum_{A \in G} (Ax)^{\alpha}. \tag{72}$$

(f) $u_1, \ldots, u_n$: 不定元 $u_1, \ldots, u_n$ を用意して、(b) に $x_1 \Leftarrow u_i A_i x$ を代入すると、

$$(u_1A_1x + \cdots + u_nA_nx)^k = \sum_{|\alpha|=k} a_{\alpha}(Ax)^{\alpha}u^{\alpha}. \tag{73}$$

(g) $b_{\bullet}$: 上で $A \in G$ にわたる和をとり S_k とする。

$$S_k = \sum_{A \in G} (u_1A_1x + + u_nA_nx)^k \tag{74}$$

$$= \sum_{|\alpha|=k} a_{\alpha} (\sum_{A \in G} (Ax)^{\alpha}) u^{\alpha} \tag{75}$$

$$= \sum_{|\alpha|=k} \underbrace{b_{\alpha}}_{\exists} R_G(x^{\alpha})u^{\alpha}. \tag{76}$$

ここで、$b_{\alpha} = |G|\, a_{\alpha}$ とした。

(h) $U_{\bullet}$: $A \in G$ をインデックスとして、

$$U_A = u_1A_1x + \cdots + u_nA_nx \tag{77}$$

とする。

(i) $S_k(\square)$: $S_k = S_k(U_A : A \in G) = \sum_{A \in G} U_A^k$。$S_k$ は $U_1, \ldots, U_A$ の「k 乗のベキ和」になっている。

(j) 上と定理 1-7-8[*6]より、$\{U_A; A \in G\}$ の対称式は $S_1, \ldots, S_{|G|}$ のの多項式である。

(k) $\exists F$: S_k は $\{U_A; A \in G\}$ の対称式なので、上より

$$S_k = F(S_1, \ldots, S_{|G|}) \tag{78}$$

となる k 係数 n 変数多項式 F が存在する。なお、これは $k > |G|$ でもよい！！ 1

(l) 上 (k) に (g) を代入 $S_k \Leftarrow \sum_{|\alpha|=k} b_{\alpha} R_G(x^{\alpha})u^{\alpha}$ する。

$$\sum_{|\alpha|=k} b_{\alpha}R_G(x^{\alpha})u^{\alpha} = F(\sum_{|\beta|=1} b_{\beta}R_G(x^{\beta})u^{\beta}, \ldots, \sum_{|\beta|=|G|} b_{\beta}R_G(x^{\beta})u^{\beta}) \tag{79}$$

(m) $\forall \alpha$: $|\alpha| = k$ とする。

(n) (l) の両辺の多重次数 α の項を取り出して係数比較すると、

$$b_{\alpha}R_G(x^{\alpha}) = (|\beta| \le |G| \text{ となる} \beta \text{についての} R_G(x^{\beta}) \text{の多項式}). \tag{80}$$

(o) (g) で $b_{\alpha} = |G|\, a_{\alpha}$ と、4 の $a_{\alpha} > 0$ と体 k の標数が 0 であることより、$b_{\alpha} \neq 0$ である。

(p) (n)(o) より、

$$R_G(x^{\alpha}) = (|\beta| \le |G| \text{ となる} \beta \text{についての} R_G(x^{\beta}) \text{の多項式}). \tag{81}$$

よって、すべての α について、$R_G(x^{\alpha})$ が $|\beta| \le |G|$ をみたす $R_G(x^{\beta})$ に関する多項式。

[*6] 対称式はベキ和で表せる

(証終)

よって、全次数が $|G|$ 以下である全ての単項式についてレイノルズ作用素を計算すれば G の不変式環の生成元全体を求めることができる。

多項式 $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ が与えらえれたとする。ここで、$k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ の単項式順序を、変数 $x_1, \ldots, x_n$ のうち 1 つでも含む多項式は $k[y_1, \ldots, y_m]$ のすべての単項式より大きくなるように定める。イデアル $\langle f_1 - y_1, \ldots, f_m - y_m \rangle \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ のグレブナ基底を G とする。与えられた $f \in k[x_1, \ldots, x_n]$ に対し、$g = \overline{f}^G$ を f の G による割り算の余りとする。このとき次が成り立つ。

(i) $f \in k[f_1, \ldots, f_m]$ と $g \in k[y_1, \ldots, y_m]$ は同値。
(ii) $f \in k[f_1, \ldots, f_m]$ ならば、$f = g(f_1, \ldots, f_m)$ となり、これは f の $f_1, \ldots, f_m$ の多項式としての表示を与える。

証明

(i) を示す。

1. G: $G = \{g_1, \ldots, g_t\}$ とし、重複、0 はないものとする。
2. $A_\bullet$: f を G で割って、

$$f = A_1 g_1 + \cdots + A_t g_t + g. \tag{82}$$

$A_1, \ldots, A_t \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ を得る。

3. $\Leftarrow$ を示す。$g \in k[y_1, \ldots, y_m]$ とする。
   (a) 2 に $y_\bullet \Leftarrow f_\bullet$ を代入する。$g_\bullet \in \langle f_1 - y_1, \ldots, f_m - y_m \rangle$ なので、$g_\bullet(x_1, \ldots, x_n, f_1, \ldots, f_m) = 0$ となり、$f \in k[x_1, \ldots, x_n]$ なのんで代入するとそのまま f である。

$$f = \widetilde{g}(f_1, \ldots, f_m). \tag{83}$$

   (b) 上より、$f \in k[f_1, \ldots, f_m]$ となる。
4. $\Rightarrow$ を示す。$f \in k[f_1, \ldots, f_m]$ とする。
   (a) $\exists \widetilde{g}$: $\widetilde{g} \in k[y_1, \ldots, y_m]$ があって、$f = \widetilde{g}(f_1, \ldots, f_m)$ とかける。
   (b)

$$f = C_1 \cdot (f_1 - y_1) + \cdots + C_m \cdot (f_m - y_m) + \widetilde{g}(y_1, \ldots, y_m). \tag{84}$$

   i. $k[f_1, \ldots, f_m]$ の α 次の単項式は、

$$f_1^{\alpha_1} \ldots f_m^{\alpha_m} = (y_1 + (f_1 - y_1))^{\alpha_1} \ldots (y_m + (f_m - y_m))^{\alpha_m} \tag{85}$$
$$= y_1^{\alpha_1} \ldots y_m^{\alpha_m} + B_1 \cdot (f_1 - y_1) + \cdots + B_m \cdot (f_m - y_m). \tag{86}$$

   と、$B_1, \ldots, B_m \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ を使ってかける。
   ii. 上を係数をかけて足せば、

$$\widetilde{g}(f_1, \ldots, f_m) = C_1 \cdot (f_1 - y_1) + \cdots + C_m \cdot (f_m - y_m) + \widetilde{g}(y_1, \ldots, y_m) \tag{87}$$

   と、$C_1, \ldots, C_m \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ を使ってかける。
   iii. (a) と上より、

$$f = C_1 \cdot (f_1 - y_1) + \cdots + C_m \cdot (f_m - y_m) + \widetilde{g}(y_1, \ldots, y_m). \tag{88}$$

   (c) G': $G' = G \cap k[y_1, \ldots, y_m]$ とする。さらに、$G' = \{g_1, \ldots, g_s\}$ としてよい。

(d) $B_1, \ldots, B_s, g'$: $\widetilde{g}$ を G' で割る。

$$\widetilde{g} = B_1 g_1 + \cdots + B_s g_s + g' \tag{89}$$

となる $B_1, \ldots, B_s, g' \in k[y_1, \ldots, y_m]$ が得られる。

(e) $C'_1, \ldots, C'_m$: (b),(d),$g_\bullet \in \langle f_1 - y_1, \ldots, f_m - y_m \rangle$ より、

$$f = C'_1 \cdot (f_1 - y_1) + \cdots + C'_m \cdot (f_m - y_m) + g'(y_1, \ldots, y_m) \tag{90}$$

となる $C'_1, \ldots, C'_m \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ が得られる。

(f) g' は f の割り算の余り？ つまり、g' のどの項も $\mathrm{LT}(G)$ の元で割り切れない？

i. g' のある項が $\mathrm{LT}(G)$ のある元で割り切れると仮定する (背理法)。

ii. $\exists i$: $\mathrm{LT}(g_i)$ は g' のある項を割り切る、となるような $g_i \in G$ が存在する。

iii. $g' \in k[y_1, \ldots, y_m]$ なので、$\mathrm{LT}(g_i)$ は $y_1, \ldots, y_m$ のみを含む。

iv. 上と、順序付より $g_i \in k[y_1, \ldots, y_m]$ となる。

v. 上と、$g_i \in G$ より、$g_i \in G'$ となる。(G' は 4-(c))。

vi. g' は G' による割り算の余りなので (d)、$\mathrm{LT}(g_i)$ は g' のどの項も割り切らない。

vii. 上は、i に矛盾する。

よって、g' は f の割り算の余り。$g = g' \in k[y_1, \ldots, y_m]$ となる。

(ii) を示す。$f \in k[f_1, \ldots, f_m]$ なら、上の証明の後半の (4-e) と (4-f) より、

$$f = C'_1 \cdot (f_1 - y_1) + \cdots + C'_m \cdot (f_m - y_m) + g(y_1, \ldots, y_m) \tag{91}$$

となっている。ここで、$y_\bullet \Leftarrow f_\bullet$ とすることで、

$$f = g(f_1, \ldots, f_m). \tag{92}$$

(証終)