mon

NO. 1

「理論的な観点からの導入」

DATE 09 · 9 · 14

グレブナー基底入門

K：体

$S = K[x_1, \cdots, x_n]$

$Mon(S) = \{ x_1^{a_1} \cdots x_n^{a_n} \mid a_i \in \mathbb{Z}_{\geq 0} \}$

特に $1 = x_1^0 \cdots x_n^0 \in Mon(S)$

・$x^a = x_1^{a_1} \cdots x_n^{a_n}$, $x^b = x_1^{b_1} \cdots x_n^{b_n}$ のとき、

$x^a \mid x^b$ （x^a が x^b を割り切る） $\underset{def}{\iff}$ $a_i \leq b_i \ \forall i$

・$\phi \neq M \subset Mon(S)$

$x^a \in M$ が極小元 $\underset{def}{\iff}$ $x^b \in M$ $x^b \mid x^a$ なら $x^b = x^a$

M^{min}：M の極小元全体の集合

定理1（Dicksonの補題）

M^{min} は有限集合である

・S 上の単項式順序とは、$Mon(S)$ 上の全順序であって

i) $1 < u$ $\forall u \in Mon(S) \setminus \{1\}$

ii) $u < v \Rightarrow wu < wv$ $\forall u, v, w \in Mon(S)$

例1

$a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$ とするとき、

・辞書式順序

$x^a <_{lex} x^b \underset{def}{\iff}$ (i) $\sum a_i < \sum b_i$

(ii) $\sum a_i = \sum b_i$ かつ $a-b$ の成分で最も左にある0でないものは負

・逆辞書式順序

$x^a <_{rev} x^b \underset{def}{\iff}$ (i) 〃

(ii) 〃 右 〃

〃 正

練習3 各自試みる。

補題4

$u, v \in Mon(S)$, $u \neq v$ とする. このとき.

$$u \mid v \Rightarrow u < v$$

証明:

$v = wu$, $w \neq 1$ となる単項式 w がある.

$w \neq 1$ より $1 < w$

すると. $1 \cdot u < w \cdot u$ $\therefore$ $u < v$ □

- $0 \neq f = \sum_{u \in Mon(S)} a_u u \in S$ $(a_u \in K)$ ← 有限和

$supp(f) := \{u \mid a_u \neq 0\}$

$in_<(f)$: $supp(f)$ に含まれる $<$ に関して最大の単項式, initial monomial と呼ぶ

- $I \subset S$ イデアル

$\{f_\lambda\}_{\lambda \in \Lambda}$ が I の生成系 $\overset{def}{\Leftrightarrow}$ $I = \{\sum_{\text{有限和}} h_\lambda f_\lambda \mid h_\lambda \in S\}$

このとき. $I = (\{f_\lambda\}_{\lambda \in \Lambda})$ と書く.

特に生成系が有限集合のときは, $I = (f_1, \cdots, f_s)$ と表し.
I は有限生成であると言う.

- 単項式から成る生成系を持つイデアルを単項式イデアルと呼ぶ. すると

単項式イデアル I は有限生成である

実際. $(I \cap Mon(S))^{min}$ は I の生成系であり. Dickson の補題より有限集合である.

- $0 \neq I \subset S$: イデアル

$in_<(I) := (\{in_<(f) \mid 0 \neq f \in I\})$ I の initial ideal

定義5

有限集合 $\{g_1, \cdots, g_s\} \subset I$ が I のグレブナー基底とは

$$in_<(I) = (in_<(g_1), \cdots, in_<(g_s))$$

なるときいう.

例6 (例16を参照)

補題7
単項式の無限減少列
$u = u_0 > u_1 > u_2 > \cdots$
は存在しない
証明: Dicksonの補題 + 補題4 □

定理8
Iのグレブナー基底はIの生成系である
証明:
$\{g_1, \cdots, g_s\}$ をIのGBとする. $0 \neq f \in I$ があれば.
$in_<(f) \in in_<(I) = (in_<(g_1), \cdots, in_<(g_s))$
$\exists w \in Mon(S) \quad \exists i \quad in_<(f) = w\, in_<(g_i)$
$f = c_0 in_<(f) + \cdots$, $g_i = c_i in_<(g_i) + \cdots$ とすると,
$h := f - c_0 c_i^{-1} g_i$ とすると $h \in I$ であって $h \neq 0$ ならば $in_<(h) < in_<(f)$
である. この操作は補題7まり有限回で終了し、$f \in (g_1, \cdots, g_s)$ を得る □

系9
多項式環Sのイデアルは有限生成である. (Hilbertの基底定理)

例10 (大杉の3大反例の一つ)

定理11 (割り算アルゴリズム) (fの$g_1, \cdots, g_s$に関する標準表示)
$g_1, \cdots, g_s$: 0でない多項式
任意の $0 \neq f \in S$ について、次の表示が存在する.
$f = f_1 g_1 + \cdots + f_s g_s + f'$ $(f_1, \cdots, f_s, f' \in S)$.
但し ① $f' \neq 0$ なら $\forall u \in supp(f')$ と $\forall i$ について $in_<(g_i) \nmid u$
② $f_i \neq 0$ なら $in_<(f_i g_i) \leqq in(f)$
f' を f の $g_1, \cdots, g_s$ に関する余りという

例12
$S = K[x, y, z]$ $<_{lex}$
$g_1 = x^3 - z$, $g_2 = xy - 1$, $f = x^3 - x^2 y - x^2 - 1$

f = $x^3 - x^2 y - x^2 - 1$
(g_1で割る) = $x(g_1 + z) - x^2 y - x^2 - 1$
= $x g_1 + xz - x^2 y - x^2 - 1$

$xz - x^2 y$ は g_1 で割る, $-x^2 - x^2$ は g_2 で割る

g_1で割る $= x_1 g_1 + xz - (g_1 + z)y - x^2 - 1$
$= (x-y)g_1 + xz - yz - x^2 - 1$
$= (x-y)g_1 + xz - yz - (g_1 + z) - 1$
$= (x-y-1)g_1 + (xz - yz - z - 1)$
余り

g_2で割る $= x g_1 + xz - x(g_2 + 1) - x^2 - 1$
$= x g_1 - x g_2 + xz - x^2 - x - 1$
$= x g_1 - x g_2 + xz - (g_1 + z) - x - 1$
$= (x-1)g_1 - x g_2 + (xz - x - z - 1)$
余り

? 余りは一意的でない

補題13.
$\{g_1, \cdots, g_s\}$ が $I = (g_1, \cdots, g_s)$ のGBならば、任意の $0 \neq f \in S$ の $g_1, \cdots, g_s$ に関する余りは一意的である

証明:
f' と f'' が f の余りで $f' \neq f''$ とせよ. すると $f - f' \in I$, $f - f'' \in I$
だから $0 \neq f' - f'' \in I$. すると、$in_<(f' - f'') \in in_<(I) = (in_<(g_1), \cdots, in_<(g_s))$
$\exists i \quad in_<(g_i) \mid in_<(f' - f'')$
他方. $in_<(f' - f'') \in supp(f') \cup supp(f'')$ だから
$\forall i \quad in_<(g_i) \nmid in_<(f' - f'')$ 矛盾 ☒

・$S = k[x_1, \cdots, x_n]$
$<$: 単項式順序

$(0 \neq) f, g \in S$ に対し
$lcm(in_<(f), in_<(g))$: $in_<(f)$ と $in_<(g)$ の最小公倍元
c_f : f における $in_<(f)$ の係数
c_g : g 〃 $in_<(g)$ 〃

$$S(f,g) := \frac{lcm(in_<(f), in_<(g))}{c_f\, in_<(f)} f - \frac{lcm(in_<(f), in_<(g))}{c_g\, in_<(g)} g$$

f と g の S-多項式

(例) $f = x_1x_4 - x_2x_3$, $in_{<_{lex}}(f)$
$g = 2x_4x_7 - x_5x_6$, $in_{<_{lex}}g$
$<_{lex}$: $x_1 > x_2 > \cdots > x_7$
このとき、

$$S(f,g) = \frac{x_1x_4x_7}{1\cdot x_1x_4} f - \frac{x_1x_4x_7}{2\cdot x_4x_7} g$$
$$= \frac{x_1x_4x_7}{x_1x_4}(x_1x_4 - x_2x_3) - \frac{x_1x_4x_7}{2x_4x_7}(2x_4x_7 - x_5x_6)$$
$$= -x_2x_3x_7 + \frac{1}{2}x_1x_5x_6$$

先頭項が打ち消し合う

$f, g_1, g_2, \cdots, g_s \in S$
f が $g_1, \cdots, g_s$ に関して余り0 $\overset{def}{\Longleftrightarrow}$ 割算アルゴリズムにおいて
$f = f_1g_1 + \cdots + f_sg_s + 0$
という標準表示が存在する

補題14
$(0 \neq) f, g \in S$ に対して、
$lcm(in_<(f), in_<(g)) = in_<(f)\, in_<(g)$
$\Rightarrow S(f,g)$ は f, g に関して余り0

証明:
簡単のため $c_f = c_g = 1$ とする
$f = in_<(f) + f_1$
$g = in_<(g) + g_1$ とおく

$$S(f,g) = \frac{in_<(f)\, in_<(g)}{in_<(f)} f - \frac{in_<(f)\, in_<(g)}{in_<(g)} g$$
$$= in_<(g) f - in_<(f) g$$
$$= (g - g_1) f - (f - f_1) g$$
$$= f_1 g - g_1 f$$ ← これが標準表示であることをいう

つまり、$in_<(f_1g), in_<(g_1f) \leq in_<(S(f,g))$ を示せばよい。

$in_<(f,g) \neq in_<(g,f)$ を示す.

$\| \qquad \|$

$in_<(f_1)\,in_<(g) \qquad in_<(g_1)\,in_<(f)$

$in_<(f_1)\,in_<(g) = in_<(g_1)\,in_<(f)$ と仮定すると, $in_<(f)$ と $in_<(g)$ は互いに素だから
$in_<(f_1)$ は $in_<(f)$ で割り切れる. $\therefore in_<(f_1) > in_<(f)$ これは矛盾 //

定理15 (Buchberger判定法)

$0 \neq I = (g_1, \cdots, g_s) \subset S$

このとき

$G = \{g_1, \cdots, g_s\}$ が I のグレブナー基底

$\Leftrightarrow$ 任意の $i \neq j$ に対して $S(g_i, g_j)$ は $g_1, \cdots, g_s$ に関して余り0

Buchbergerアルゴリズム

Input : $\{g_1, \cdots, g_s\} \subset S$

$<$: 単項式順序

Output : $I = (g_1, \cdots, g_s)$ の $<$ に関するGB

① $G = \{g_1, \cdots, g_s\}$

② $G' = G$ とおく

各 $f_1, f_2 \in G'$ $(f_1 \neq f_2)$ に対して, $S(f_1, f_2)$ の G' に関する余りを r が 0 でないならば $G = G \cup \{r\}$ とおく.

③ $G = G'$ ならば G を出力

$G \neq G'$ なら ② に戻る.

* アルゴリズムは必ず停止する!

(∵) ② において $r \neq 0$ のとき, r は"余り"だから $in_<(r)$ を割り切るような $in_<(g)$ $(g \in G')$ は存在しない.

$\therefore in_<(r) \notin (in_<(g) \mid g \in G')$

$\therefore (in_<(g) \mid g \in G') \subsetneq (in_<(g) \mid g \in G' \cup \{r\})$

もし停止しないとすると,

$(in_<(g_1), \cdots, in_<(g_s))$

$\subsetneq (in_<(g_1), \cdots, in_<(g_s), in_<(g_{s+1}))$

$\subsetneq (in_<(g_1), \cdots, in_<(g_s), in_<(g_{s+1}), in_<(g_{s+2}))$

$\vdots$

と無限列が構成される. これは Dicksonの補題に矛盾

(Hilbertの基底定理) //

Example 16

$S = K[x_1, \cdots, x_7]$

$<_{lex} : x_1 > \cdots > x_7$

$f = x_1x_4 - x_2x_3$

$g = x_4x_7 - x_5x_6$

$I = (f, g)$

このグレブナー基底を求める

$G = \{f, g\}$

$S(f,g) = x_7 f - x_1 g$
$= \boxed{x_1 x_5 x_6 - x_2 x_3 x_7} = h$
↑余り

$G = \{f, g, h\}$
$S(f,g)$ (済)
$S(g,h)$ $x_4 x_7$ と $x_1 x_5 x_6$ は互いに素
$S(f,h) = x_2 x_3 g$ ← f, g, h に関して余り0
∴ $\{f, g, h\}$ は I のグレブナー基底

定理17 (消去定理)
$S = k[x_1, \cdots, x_n]$
$S' = k[x_{i_1}, \cdots, x_{i_m}]$ $(1 \le i_1 < \cdots < i_m \le n)$
$<$: 単項式順序 on S 「on S'」
g : イデアル $0 \neq I \subset S$ の $<$ に関するGB
$<$ が条件
「$g \in G$, $in_<(g) \in S' \Rightarrow g \in S'$」
を満たすならば
$G \cap S$ は $I \cap S'$ の $<$ に関するグレブナー基底である

Example 18 purely lex-order $x_1 > x_2 > \cdots > x_n$
$x^a <_{plex} x^b \overset{def}{\Leftrightarrow}$ $a-b$ の最も左にあるゼロでない成分が負
(成分で)
$S' = k[x_m, x_{m+1}, \cdots, x_n]$
どんな I に関しても消去定理が使える。

Example 19

$$\begin{cases} f_1 = x^2 + y + z - 1 = 0 \\ f_2 = x + y^2 + z - 1 = 0 \\ f_3 = x + y + z^2 - 1 = 0 \end{cases}$$

$I = (f_1, f_2, f_3)$
$<_{plex} : x > y > z$

$$\begin{cases} g_1 := x + y + z^2 - 1 \\ g_2 := y^2 - y - z^2 + z \\ g_3 := 2yz^2 + z^4 - z^2 \\ g_4 := z^6 - 4z^4 + 4z^3 - z^2 \end{cases}$$

g_1 ← x, y, z
g_2, g_3 ← y, z のみ
g_4 ← z のみ
は GB

$I = (g_1, \cdots, g_4)$
$I \cap \mathbb{C}[z] = (g_4)$

対応表

午前	午後
lex	全次数特異式
reverse lex	全次数逆特異式
purely lex	特異式