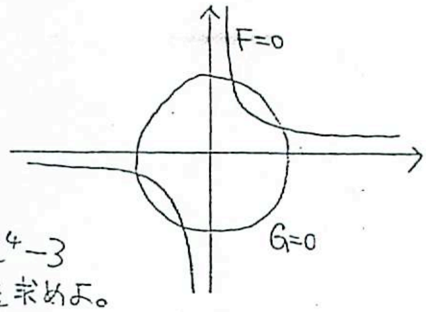
第1部: Gröbner 基底入門 (チュートリアル)

$$\begin{cases} F = xy - 1 \\ G = x^2 + y^2 - 4 \end{cases}$$ とおく。



問1. $F = G = 0$ の解をすべて求めよ。

問2. $PF + QG = -x^3y + 4xy - 3x^2 + x^4 - 3$ の解 (P, Q) $P, Q \in \mathbb{C}[x, y]$ を求めよ。

問3. F, G で生成される $\mathbb{C}[x, y]$ のイデアルを J と書く。
$-x^3y + 4xy - 3x^2 + x^4 - 3 \in J$ か?
(問. イデアルの定義をのべよ。F, G で生成されるイデアルとは何か? 定義をのべよ。)

問4.* $f \in \mathbb{C}[x, y]$ が $f \in J$ かどうか判定するアルゴリズムはないか。

⊙ Gröbner 基底の概念, Buchberger アルゴリズムはこれらの問に対してシステマティックかつ一般的に答えている。

問1. を高校数学風に解くと、

$$\begin{cases} F = xy - 1 & \text{——— ①} \\ G = x^2 + y^2 - 4 & \text{——— ②} \end{cases}$$

①より、$y = \frac{1}{x}$ ——— ③

②に代入して、 $x^2 + \frac{1}{x^2} - 4 = 0$

$x^4 - 4x^2 + 1 = 0$ ——— ④

$x^2 = 2 \pm \sqrt{3}$

$x = \pm\sqrt{2 \pm \sqrt{3}}$, y は③より求まる。

①② $\Longrightarrow$ ④ 消去法

別の見方をすると、F と G を y の多項式として見た時の終結式が④である。

⊙ この消去法をシステマテックにおこなうのが Buchberger アルゴリズムである。ここでは

Order

の概念が重要な役割をはたす。

⊙ 以下、はんざつにしないため、2変数多項式環で説明するが、n 変数, 微分作用素環, Lie 環の universal enveloping algebra, これらの上の自由加群などに一般化可能である。

§§1. Gröbner基底

$$\mathbb{N}_0 = \{0,1,2,\cdots\}$$

Order on $\mathbb{N}_0^2 \ni (k_0, k_1)$

Def 0 ←(zeroである。ファイでない。)

(ア) lexicographic order : $(k_0, k_1) \succ (\tilde{k}_0, \tilde{k}_1)$

$\Leftrightarrow$ (① $k_1 > \tilde{k}_1$) or (② $k_1 = \tilde{k}_1$ and $k_0 > \tilde{k}_0$)

(イ) total degree order : $(k_0, k_1) \succ (\tilde{k}_0, \tilde{k}_1)$

$\Leftrightarrow$ (① $k_0 + k_1 > \tilde{k}_0 + \tilde{k}_1$) or (② $k_0 + k_1 = \tilde{k}_0 + \tilde{k}_1$ and $k_0 > \tilde{k}_0$)

つまり、lexicographic orderでは、

$$\begin{aligned} \perp &\prec (0,0) \prec (1,0) \prec (2,0) \prec \cdots \\ &\prec (0,1) \prec (1,1) \prec (2,1) \prec \cdots \\ &\prec (0,2) \prec (1,2) \prec \cdots \\ &\quad \vdots \end{aligned}$$

$\perp$はただの記号で 最小元を表わす。あとで ○に特定させる。

total degree orderでは、

$$\begin{aligned} \perp \prec (0,0) \prec (0,1) &\prec (1,0) \\ &\prec (0,2) \prec (1,1) \prec (2,0) \\ &\prec (0,3) \prec (1,2) \prec (2,1) \prec (3,0) \\ &\prec \cdots \end{aligned}$$

これらのorderは well-founded, i.e., 無限減少列がない, i.e.,

(※) $a_k \in \mathbb{N}_0^2 \quad k = 1, 2, \cdots$

$a_k \succeq a_{k+1}$ とするとき、$\exists k_0, \ a_k = a_{k_0} \quad k \geq k_0$

となる。上のlexicographic orderの例でもわかるように、たとえば、lexicographic orderで、(1,2)より小さい元は無限個あるから、上の性質はあたりまえではない。total degree orderでは、ある元 (a, b) より小さい元は有限個しかないから上の性質は明らかである。

問5* 上の(※)を証明せよ。

- Well-foundedの概念は"プログラムの検証"の分野でよく用いられる。

→ Z. Manna: プログラムの理論 第三章 (日本コンピュータ協会)

以下、order < を lexicographic order に fix する。

注. 実際の計算をおこなう時は、lexicographic order を用いるのは、時間と空間のむだとなる。total degree で求めてから連立方程式を解いて lexicographic order の basis を求める。これについては後述する。

$$A = K[x, y] \qquad K \text{は} \mathbb{Q} \text{とか} \mathbb{C} \text{とか 体}$$
$$\cup\!\!\!\!\!\! \shortmid \qquad\qquad\qquad \mathbb{Z} \text{はダメ.}$$
$$f = \sum_{k \in S} a_k x^{k_0} y^{k_1}, \quad k = (k_0, k_1)$$

Def1.

$$\deg : A \longrightarrow \mathbb{N}_0^2 \cup \{\perp\} \quad \text{を、}$$

$$\deg(0) = \perp$$
$$\deg(f) = \max_{k \in S} k$$
ここで $f = \sum_{k \in S} a_k x^{k_0} y^{k_1}$

deg を Exp. と書くこともある。

例. $\deg(a_{00} + a_{51} x^5 y + a_{12} x y^2) = (1, 2)$ ← lexicographic order より.

Def2. $f = \sum_{k \in S} a_k x^{k_0} y^{k_1}$, $\deg(f) = p$ とするとき、

$$\mathrm{head}(f) = a_p x^{p_0} y^{p_1}$$

つまり、head(f) とは、f を構成しているモノミアルの中で、order > で最大のものである。

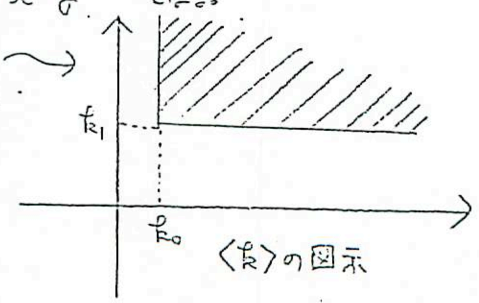
例. $\mathrm{head}(a_{00} + a_{51} x^5 y + a_{12} x y^2) = a_{12} x y^2$ (lexicographic order で)

total degree order では,
$\mathrm{head}(a_{00} + a_{51} x^5 y + a_{12} x y^2) = a_{51} x^5 y$ となる。

Def3. $k \in \mathbb{N}_0^2$ とする。

$$\langle k \rangle = \langle (k_0, k_1) \rangle := (k_0, k_1) + \mathbb{N}_0^2$$

この図は とてもべんり. →



$\langle k \rangle$ の図示

Prop1. $\langle k \rangle \underset{\nwarrow \text{as set}}{\supseteq} \langle j \rangle$ $\qquad k, j \in \mathbb{N}_0^2$

$\Rightarrow k \leq j$

問. (ア) Prop1を証明せよ。
(イ) 逆が成立しない例をつくれ。
(ウ) jより order $\leq$ で小さい部分を図示せよ。

Prop2. $F, G \in A$, $F \neq 0$ とする。

$\langle \deg(G) \rangle \subseteq \langle \deg(F) \rangle$

$\Rightarrow \exists h \in A$, s.t. $\deg(G - hF) < \deg(G)$

$\because$ $G = ax^{j_0}y^{j_1}$ + lower terms ← lexicographic order or total degree order での lower term の意。

$F = bx^{k_0}y^{k_1} + \cdots$

$l_0 = j_0 - k_0$, $l_1 = j_1 - k_1$ とおく。

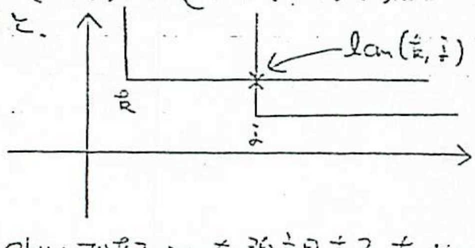
$h = \frac{a}{b} x^{l_0} y^{l_1}$ とおけばよい。//

例. $F = \underbrace{xy}_{\text{head}} - 1$, $G = \underbrace{x^2y}_{\text{head}} + xy - 4$ のとき、$h = x$ とおけばよい。

Def4. $k, j \in \mathbb{N}_0^2$

$\mathrm{lcm}(k, j) := (\max(k_0, j_0), \max(k_1, j_1))$

図示すると、



注. 数ベクトルであることを強調するため k を $\vec{k}$ と書くときがある。

例. $\mathrm{lcm}((0,5), (1,1)) = (1,5)$

注. $k = \deg(cF) = \deg(dG)$ $\qquad c, d, F, G \in A$, $c, d \neq 0$

$\Rightarrow \langle k \rangle \subseteq \langle \mathrm{lcm}(\deg(F), \deg(G)) \rangle$

問7. 上を証明せよ。

Def 5. $F, G \in A$ とする。

$F = b\,x^{k_0}y^{k_1} + \text{lower term.}$

$G = a\,x^{j_0}y^{j_1} + \cdots$

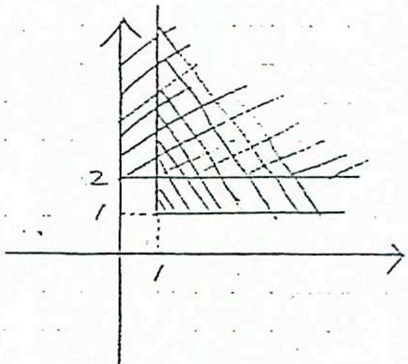
$l := \mathrm{lcm}(k, j)$, $c := \frac{1}{b}x^{l_0-k_0}y^{l_1-k_1}$, $h := \frac{1}{a}x^{l_0-j_0}y^{l_1-j_1}$

$sp(F,G) := cF - hG$

と定義する。 $sp(F,G)$ を F と G の S-polynomial という。

注. $\deg(sp(F,G)) < \mathrm{lcm}(\deg(F), \deg(G))$

問8. 上を証明せよ。



例. $sp(\underset{\nwarrow\text{head}}{xy}+1,\ x^2-\underset{\nwarrow\text{head}}{y^2})$

$c = \frac{1}{-1}x^0y^1 = -y$, $h = x^1y^0 = x$

$= -y(xy+1) - x(x^2-y^2) = \underset{\nwarrow\text{head}}{-y} - x^3$

発見的考察. S-polynomial をどんどん付け加えていって、イデアルの generator を太らせていくと よい generator に達するのではないか。

実験. order $x<y$ (lexicographic order) でやる。

$F = \underset{\nwarrow\text{head}}{xy} - 1$, $G = x^2 + \underset{\nwarrow\text{head}}{y^2} - 4$

$sp(F,G) = yF - xG = -y - x^3 + 4x =: H$

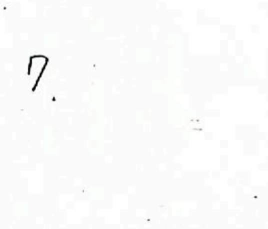
$sp(F,H) = -F - xH = -xy + 1 + xy + x^4 - 4x^2 = x^4 - 4x^2 + 1 =: J$.

J は x のみの式, H は y の1次式 + x のみの式　　(実は、$\{H, J\}$ が Gröbner 基底)

と、とてもよい形をしている。 また、

F と G

F と G と H



F, G, H, J

実は これ以上 S-polynomial をとっても これ以上 よいもの はでない。

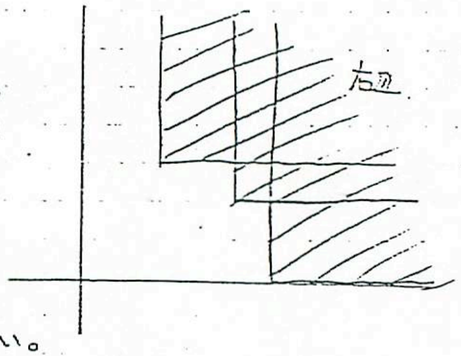
$$
\begin{aligned}
Sp(H,G) = G + yH &= x^2+y^2-4-y^2-x^3y+4xy \\
&= \underline{\underline{-x^3y}}+4xy+x^2-4 \\
&\xrightarrow[\text{by } H]{} x^3(x^3-4x)+\underline{\underline{4xy}}+x^2-4 \\
&\xrightarrow[\text{by } H]{} x^3(x^3-4x)+4x(-x^3+4x)+x^2-4 \\
&= \underline{\underline{x^6}}-8x^4+17x^2-4 \\
&\xrightarrow[\text{by } J]{} 4x^4-x^2-x^4+17x^2-4 \\
&= -4x^4+16x^2-4 \\
&\xrightarrow[\text{by } J]{} 0.
\end{aligned}
$$

(← これは.後述の reduction)

Def 6. $F, G_1, \cdots, G_m \in A$.

Fが reducible by $\mathcal{G} = \{G_1, \cdots, G_m\}$

$\Leftrightarrow \deg(F) \in \bigcup_{i=1}^{m} \langle \deg(G_i) \rangle$



例. $\underline{\underline{xy}}-1$ は $\{x^2+\underline{\underline{y^4}}-4\}$ で reducible でない。

Fが $\mathcal{G}$で irreducible $\Leftrightarrow$ Fが $\mathcal{G}$ で reducible でない。

Def 7. (Fの$\mathcal{G}$による reduction)

Fが $\mathcal{G}$で reducible とする。このとき、

$\exists G_{i_1} \in \mathcal{G}$, $\exists h_1 \in A$ s.t. $\deg(\underbrace{F-h_1G_{i_1}}_{=F_1}) < \deg(F)$

とできる。

FをF_1に書き換える操作を reduction といい

$$F \longrightarrow F_1 \quad \text{by } \mathcal{G}$$

と書く。(by $\mathcal{G}$ は $\mathcal{G}$が明らかな時は省略)

$$F \to F_1 \to F_2 \to \cdots \to \tilde{F}$$

をreductionの列とする。$\tilde{F}$がirreducibleのとき、この列を、

$$F \xrightarrow{\;*\;} \tilde{F}$$

と書く。

例. 前ページの計算をみよ。$\mathcal{G}=\{H, J\}$ とおくと、

$$sp(H, G) \xrightarrow{\;*\;} 0 \quad by \quad \mathcal{G}$$

である。

注意. $\tilde{F}$はFによって一意的にはきまらない。

例. $\mathcal{G}=\{\overset{G_1}{\overset{\shortparallel}{\underset{\text{head}}{xy^2}-1}},\ \overset{G_2}{\overset{\shortparallel}{x^2+\underset{\text{head}}{y^2}-4}}\}$ とおく。

$$xy^2 \xrightarrow{by\ G_1} y$$

$$xy^2 \xrightarrow{by\ G_2} 4x-x^3$$

よって、

$$xy^2 \xrightarrow{\;*\;} y$$

$$xy^2 \xrightarrow{\;*\;} 4x-x^3$$

と$\tilde{F}$は2とおりある。

例. $\mathcal{G}=\{J=x^4-4x^2+1,\ H=-y-x^2+4x\}$

$$xy^2 \xrightarrow{by\ H} -x^4y+4x^2y$$

$$-x^4y+4x^2y \xrightarrow{by\ J} -4x^2y+y+4x^2y = y$$

$$y \xrightarrow{by\ H} = -x^3+4x$$

$$-x^4y+4x^2y \xrightarrow{by\ H} x^7-4x^5+4x^2y$$

$$\xrightarrow{by\ H} x^7-4x^5-4x^5+16x^3 = x^7-8x^5+16x^3$$

$$\xrightarrow{by\ J} 4x^5-x^3-8x^5+16x^3 = -4x^5+15x^3$$

$$\xrightarrow{by\ J} -16x^3+4x+15x^3 = -x^3+4x$$

このときは、どんな順番でreduction ⟹ しても $\xrightarrow{*}$ の値は一意的。

問9. $\mathcal{G}=\{H,J\}$, $H=-y-x^3+4x$, $J=x^4-4x^2+1$ とする。

$\mathcal{G}$で x^2+y^4-4 をreductionせよ。

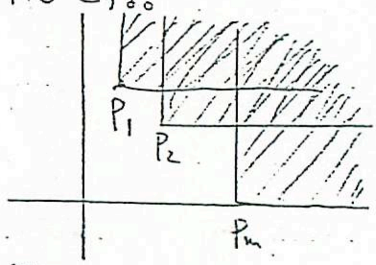
問10. $\mathcal{G}=\{G_1,\cdots,G_m\}$ とする $\mathcal{G}$によるreductionが必ず停止することを(irreducibleな元まで書き換わることを)、$>$ が well-founded であることを用いて証明せよ。

参考. モノイデアル.

def. $I\subseteq \mathbb{N}_0^2$ がモノイデアル $\Leftrightarrow$ $I+\mathbb{N}_0^2\subseteq I$.

Th3. (ア) I_k $(k=0,1,2,\cdots)$ を$\mathbb{N}_0^2$のモノイデアルとする。
$I_k\subseteq I_{k+1}$

$\Rightarrow$ $\exists k_0$, $I_k=I_{k_0}$ $(k\geq k_0)$



(イ) I を$\mathbb{N}_0^2$のモノイデアルとする。

$\Rightarrow$ Iは有限生成.
i.e. $\exists P_1,\cdots,P_m\in\mathbb{N}_0^2$ s.t. $I=\bigcup_{k=1}^{m}\langle P_k\rangle=\bigcup_{k=1}^{m}(P_k+\mathbb{N}_0^2)$

問11. 上のThを証明せよ。

Def8. $\mathcal{J}$をAのイデアルとする。

$\mathcal{G}=\{G_1,\cdots,G_m\}$ が$\mathcal{J}$のGröbner基底である。

$\Leftrightarrow$ $\bigcup_{F\in\mathcal{J}}\langle\deg(F)\rangle=\bigcup_{G_i\in\mathcal{G}}\langle\deg(G_i)\rangle$ かつ $\forall i$, $G_i\in\mathcal{J}$.

<u>Th4.</u> Aのイデアル$\mathcal{J}$に対して必ずGröbner基底

$$\mathcal{G}=\{G_1,\cdots,G_m\}$$

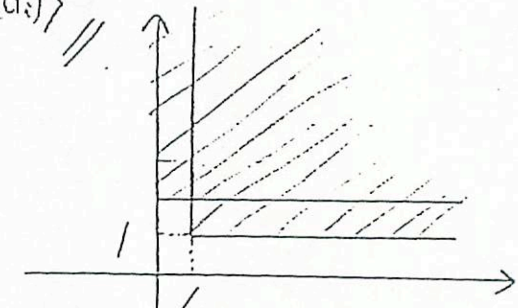
が存在する。(一意的ではない.)

☺ $\bigcup_{F\in\mathcal{J}}\langle\deg(F)\rangle$ は$\mathbb{N}_0^2$のモノイデアルである。

Th3より、このモノイデアルは有限生成。

$\therefore\ \exists G_1, \cdots, G_m \in J$

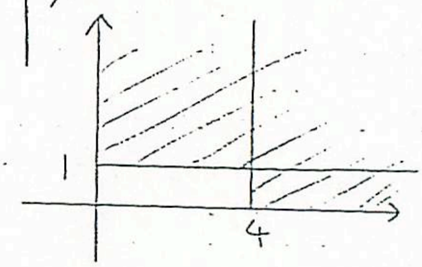
s.t. $\displaystyle\bigcup_{F \in J} \langle \deg(F) \rangle = \bigcup_{i=1}^{m} \langle \deg(G_i) \rangle$



例. $J = (xy-1,\ x^2+y^2-4)$

・$\{xy-1,\ x^2+y^2-4\}$ は、Gröbner 基底でない。

・$\{x^4-4x^2+1,\ -y-x^3+4x\}$ は Gröbner 基底



次の定理が基本定理であり、またGröbner基底の構成アルゴリズムを与えている。

<u>Th5</u> $\mathcal{G} = \{G_1, \cdots, G_m\}$ がイデアル J の Gröbner 基底

$\Leftrightarrow\ \forall i, j \quad sp(G_i, G_j) \xrightarrow{\ *\ } 0 \quad \text{by } \mathcal{G}$

かつ $\mathcal{G}$ がイデアル J を生成する。

問に. $\mathcal{G} = \{G_1, G_2\}$ $\begin{cases} G_1 = x^4-4x^2+1 \\ G_2 = -y-x^3+4x \end{cases}$ のときに、

$\forall i, j \quad sp(G_i, G_j) \xrightarrow{\ *\ } 0 \quad \text{by } \mathcal{G}$

をたしかめよ。

上のTh5を証明するために2つlemmaを用意する。

lemma6.

$$sp(G_i, G_j) \xrightarrow{\ *\ } 0 \quad \text{by } \mathcal{G}$$

とする。このとき、 $\exists S_k^{(ij)} \in A$ s.t.

(ア) $sp(G_i, G_j) = \sum_{k=1}^{m} S_k^{(ij)} G_k$

(イ) $\forall k,\ \deg(S_k^{(ij)} G_k) \preceq \deg(sp(G_i, G_j))$

(∵) 仮定より、

$$F_{i_0}:=sp(G_i,G_j)\longrightarrow F_{i_0}-{}^{\exists}g_{i_1}G_{i_1}=:F_{i_1}$$

$$F_{i_1}\longrightarrow F_{i_1}-{}^{\exists}g_{i_2}G_{i_2}=:F_{i_2}$$

$$\vdots$$

$$F_{i_q}\longrightarrow F_{i_q}-{}^{\exists}g_{i_{q+1}}G_{i_{q+1}}=0$$

$F_{i_1},\cdots,F_{i_q}$ を消去して (ア)を得る。

各 stepで、

$$\deg(F_{i_\ell}-g_{i_{\ell+1}}G_{i_{\ell+1}})<\deg(F_{i_\ell})$$

$$\deg(F_{i_\ell})=\deg(g_{i_{\ell+1}}G_{i_{\ell+1}})$$

より (イ)を得る。//

lemma 7.

$\vec{h}=(h_1,\cdots,h_m)\in A^m$ に対して、($h_1\in A$, $h_m\in A$)

$$\deg(\vec{h}):=\max_{i=1,\cdots,m}\{\deg(h_iG_i)\}$$

$$M(\vec{h}):=\#\{h_i\mid \deg(h_iG_i)=\deg(\vec{h})\}$$ とおく。

($\#$: 個数)

$\mathcal{G}=\{G_1,\cdots,G_m\}$

$\forall i,j\quad sp(G_i,G_j)\xrightarrow{*}0$ by $\mathcal{G}$ と仮定

$D=\sum_{i=1}^m h_iG_i$ かつ $\deg(\vec{h})>\deg(D)$

$\Rightarrow\ \exists\vec{j}\in A^m$ s.t.

$$\left.\begin{array}{l} D=\sum_{i=1}^m j_iG_i \\ \text{かつ}\ (\deg(\vec{j})<\deg(\vec{h})\ \text{ or }\ M(\vec{j})<M(\vec{h})) \end{array}\right\}\text{―①}$$

$$\deg(\vec{h}) > \deg(D) \text{ より } \quad M(\vec{h}) \geq 2.$$

番号をつけかえて、

$$\deg(\vec{h}) = \deg(h_1 G_1) = \deg(h_2 G_2)$$

としてよい。

$$sp(G_1, G_2) = {}^{\exists}c_1 G_1 - {}^{\exists}c_2 G_2, \quad \deg(c_1 G_1) = \deg(c_2 G_2)$$

$${}^{\exists}q \in A, \quad \deg(h_1 G_1 - q c_1 G_1) < \deg(h_1 G_1)$$

とできる。

$$\begin{aligned} D &= h_1 G_1 + \sum_{l \neq 1} h_l G_l \\ &= h_1 G_1 - q c_1 G_1 + \underbrace{q c_1 G_1}_{= q\, sp(G_1, G_2) + q c_2 G_2} + \sum_{l \neq 1} h_l G_l \\ &= (h_1 - q c_1) G_1 + q \sum_{i=1}^{m} S_i^{(12)} G_i + q c_2 G_2 + \sum_{l \neq 1} h_l G_l \end{aligned}$$

$$j_1 := h_1 - q c_1 + q S_1^{(12)}$$

$$j_2 := q S_2^{(12)} + q c_2 + h_2$$

$$j_l := h_l \qquad l \neq 1, 2$$

とおくと、結論①の条件をみたす。//

Th5の証明.

$${}^{\forall}i, j \quad sp(G_i, G_j) \xrightarrow{*} 0 \ \text{by} \ \mathcal{G}, \quad \mathcal{G} \text{ が } J \text{ を生成}$$

$$\Rightarrow \underbrace{\boxed{\bigcup_{F \in J} \langle \deg(F) \rangle}}_{(ア)} = \underbrace{\boxed{\bigcup_{G_i \in \mathcal{G}} \langle \deg(G_i) \rangle}}_{(イ)}$$

(ア) ⊇ (イ) は $\mathcal{G} \subset J$ より o.k.

(ア) ⊆ (イ) を示す。

$D \in \mathcal{I}$ とする。

$\mathcal{G}$ は $\mathcal{I}$ の generator だから、 $\exists h_i \in A$ $\quad D=\sum_{i=1}^{m} h_i G_i$

と書ける。

$$\deg(\vec{h})=\max\{\deg(h_i G_i)\} \leq \deg(D)$$

なら、 $\deg(D) \in (\mathcal{K})$ となる。

$\deg(\vec{h}) > \deg(D)$ と仮定しよう。

lemma 7を有限回適用することにより、 $\exists \vec{j} \in A^m$

$$D=\sum_{i=1}^{m} j_i G_i$$

$$\deg(D)=\deg(\vec{j})$$

とすることができる。

$\therefore \deg(D) \in (\mathcal{K})$

$\therefore (\mathcal{D})=(\mathcal{K})$ //

Th5の証明,つづき

⇐ 仮定より.

$F\in J$ なら $\deg(F)\in\bigcup_{i=1}^{m}\langle\deg(G_i)\rangle$ だから.

Fは$\mathcal{G}$で reducible である。よって、$F \xrightarrow{*} 0$ by $\mathcal{G}$.

とくに. $sp(G_i,G_j)\in J$ だから. $sp(G_i,G_j)\xrightarrow{*}0$ //

定理. (大切)

$\mathcal{G}$がJのGröbner basisなら, $F\in J$ のとき. どんな(順番で)reductionをしても.

$$F\xrightarrow{*}0 \quad \text{by } \mathcal{G}$$

となる。

例. $\mathcal{G}$がGröbner basisでないとこのようなことは成立しない。

$\mathcal{G}=\{xy-1,\ y^2-x\}$ とせよ。 $F=xy^2-y$ とする。orderはlexicographic.

$$\begin{tikzcd} & F \arrow[dl, "\text{by } xy-1"'] \arrow[dr, "\text{by } y^2-x"] & \\ 0 & & x^2-y \arrow[ll] \end{tikzcd}$$

共に$\mathcal{G}$でirreducibleである。

例. $\{xy-1,\ y^2-x\}$ より出発して. Gröbner基底を計算してみよう。(total degree orderで)

$sp(xy-1,\ y^2-x)=y(xy-1)-x(y^2-x)=\cancel{xy^2}-y-\cancel{xy^2}+x^2=x^2-y$ ← 新しいs-poly

$sp(xy-1,\ x^2-y)=x(xy-1)-y(x^2-y)=-x+y^2\longrightarrow 0$ by y^2-x

$sp(y^2-x,\ x^2-y)=x^2(y^2-x)-y^2(x^2-y)=-x^3+y^3$

$-x^3+y^2\longrightarrow -x^3+y^2+x(x^2-y)=y^2-xy$ by x^2-y

$y^2-xy\longrightarrow y^2-xy+xy-1=y^2-1$ by $xy-1$

$y^2-1\longrightarrow y^2-1-(y^2-x)=x-1$ by y^2-x ← 新しいs-poly

$\{xy-1,\ y^2-x,\ x^2-y,\ x-1\}$ において、$x-1$を用いて他の要素を簡約すると、→ cf. アルゴリズム11.

$\{x-1,\ y-1\}$ となる。

$sp(x-1,\ y-1)=y(x-1)-x(y-1)=-y+x\longrightarrow 0$ by $\{x-1,\ y-1\}$ より、

$\{x-1,\ y-1\}$ が basis.

問13.(ア) 上の定理を用いて、問3を解け。

(イ) $x^4y+x^2\in J$ か判定せよ。

問14. total degree order を用いて、

$$J=\{xy-1,\ x^2+y^2-4\}$$

のGröbner基底を求めよ。この基底を用いて問13を解け。

定義. $\dim_K A/J < +\infty$ ← K上のlinear spaceとしての次元.

なるイデアルJを0次元イデアルという。

Th8. $>$ をlexicographic order とする。

Jが0次元イデアル $\Rightarrow$ $\exists f \in K[x]$ s.t. $f \in J$の$>$についてのGröbner基底

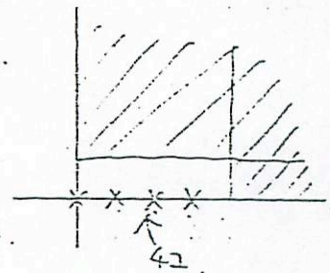
例. $J=(xy-1,\ x^2+y^2-4)$の$>$についてのGröbner基底は、

$$x^4-4x^2+1 \in K[x]$$ を含む。

☺ このような元fがないとするとTh5より、(lexicographic orderだから Gの元のheadは必ずyを含む!) $x^p-x^q \notin J$ $(p \neq q)$

よって、$A/J \ni 1, x, x^2, \cdots$ 異なる。これは、$\dim_K A/J < +\infty$ にむじゅん//

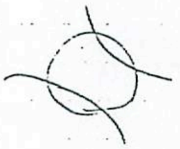
例. $J=(xy-1,\ x^2+y^2-4)=(x^4-4x^2+1,\ -y-x^3+4x)$ のとき。



右図から分かるように、

$$\dim_K A/J = 4.$$

である。この4という数は、



4点で交じわる。

ことと無関係でない。

問. 曲線のintersection numberをGröbner basisを用いて計算する方法を考えなさい。

Th9. $\dim_K A/J = \#S$. ここで $S=\mathbb{N}_0^2 \setminus \bigcup_{G_i \in G} \deg(G_i)$, GはJのGröbner基底.

問. 上を証明せよ。

§2. アルゴリズム.

Th5より、Gröbner基底を構成するアルゴリズムは次のとおり。

アルゴリズム10. (Buchberger アルゴリズム)

入力: $L^{(1)}, \cdots, L^{(p)}$ ($L^{(i)} \in A$, イデアルの generator)

出力: $\mathcal{G}$ (Gröbner 基底)

| $\mathcal{G}$:= 空集合 ; $S := \{L^{(1)}, \cdots, L^{(p)}\}$;
| while $S \neq$ 空集合 do
| | $\mathcal{G} := \mathcal{G} \cup S$; $S :=$ 空集合;
| | $\mathcal{G}$の簡約 (やらなくてもよい)
| | $P, Q \in \mathcal{G}$ のすべてのくみあわせ (P, Q) について以下をおこなう
う → | | | $T := sp(P, Q)$;
| | | $T \xrightarrow{*} T_0$ by $\mathcal{G}$;
| | | if $T_0 \neq 0$ then $S := S \cup \{T_0\}$;

アルゴリズム11. $\mathcal{G}$の簡約 ($\mathcal{G}$より余計なものを除く.)

While $\mathcal{G}$中に, $\mathcal{G} \setminus \{L_0\}$でreducibleな元$L_0$がある do
| $\mathcal{G} := \mathcal{G} \setminus \{L_0\}$
| $L_0 \xrightarrow{*} L$ by $\mathcal{G}$
| if $L \neq 0$ then $\mathcal{G} := \mathcal{G} \cup \{L\}$

問15. $L^{(1)} = xy - 1$, $L^{(2)} = x^2 + y^2 - 4$ を入力として. Buchberger アルゴリズムを lexicographic order で実行してみなさい。 (答えは、$\{x^4 - 4x^2 + 1, -y - x^3 + 4x\}$)

問16. $\mathcal{G} = \{xy - 1, -y - x^3 + 4x, x^4 - 4x^2 + 1\}$ とおく。アルゴリズム11を適用すると. $\mathcal{G} = \{-y - x^3 + 4x, x^4 - 4x^2 + 1\}$ となることをたしかめよ。

問15の答え。 $y \rhd x$. (プログラムのトレース.)

$\mathcal{G}=\phi$; $S=\{xy-1,\ x^2+y^2-4\}$;

・$S \neq \phi$ なので.

$\mathcal{G}=\{xy-1, x^2+y^2-4\}$; $S=\phi$;

$xy-1$ は x^2+y^2-4 で irreducible.
x^2+y^2-4 は $xy-1$ で 〃 .
} $\mathcal{G}$ の簡約

$T=sp(xy-1, x^2+y^2-4)$;

$=y(xy-1)-x(y^2+x^2-4)$

$=-y-x^3+4x$.

T は $\mathcal{G}$ で irreducible. よって、

$S=\{-y-x^3+4x\}$

$S \neq \phi$ なので.

$\mathcal{G}=\{xy-1, y^2+x^2-4, -y-x^3+4x\}$; $S=\phi$;

$xy-1$ は $\{y^2+x^2-4, -y-x^3+4x\}$ で reducible.

$xy-1+x(-y-x^3+4x)$

$=-1-x^4+4x^2$

$\mathcal{G}=\{-x^4+4x^2-1, y^2+x^2-4, -y-x^3+4x\}$

y^2+x^2-4 は $\{-x^4+4x^2-1, -y-x^3+4x\}$ で reducible.

$y^2+x^2-4+y(-y-x^3+4x)$

$=x^2-4-yx^3+4xy$

$-yx^3+x^2+4xy-4-x^3(-y-x^3+4x)$

$=x^2+4xy-4+x^6-4x^4$

⋮

M.a.

問17. (ア) $L^{(1)} = xy - 1$, $L^{(2)} = y^2 - x$ を入力として Gröbner 基底を求めよ。

(イ) $J = (xy-1, y^2-x)$, $K = \mathbb{Q}$ のとき、$\dim_K A/J$ を求めよ。

(ウ) $xy^2 - y$ を上の Gröbner 基底で reduction せよ。ルールの適用順序をかえても、最終結果は同じとなることをたしかめよ。

定理12. (ア) Buchberger アルゴリズムは必らず停止する。

(イ) Buchberger アルゴリズムの出力は Gröbner 基底である。

☺ (ア) プログラムの切点 ⓑ で考える。ⓑ において、任意の S の元は、$\mathcal{G}$ で irreducible である。したがって、

$$\forall f \in S, \quad \deg(f) \notin \bigcup_{G \in \mathcal{G}} \langle \deg(G) \rangle$$

よって $S =$ 空集合なら、$\displaystyle\bigcup_{f \in \mathcal{G} \cup S} \langle \deg(f) \rangle \supsetneq \bigcup_{G \in \mathcal{G}} \langle \deg(G) \rangle$ —— (エ)

プログラムが停止しない $\Leftrightarrow$ 切点 ⓑ を無限回とおる、かつ 切点 ⓑ で $S \neq$ 空集合。

よってプログラムが停止しないとすると (エ) より、モノイデアルの真の増大列が存在することになる。これは Th3 にむじゅん。//

(イ) 切点 ⓑ で考える。プログラムが停止 $\Rightarrow$ $S =$ 空集合。

これは、$\forall G, \tilde{G} \in \mathcal{G}$, $sp(G, \tilde{G}) \xrightarrow{*} 0$ by $\mathcal{G}$

を意味する。Th5 より、$\mathcal{G}$ は Gröbner 基底。//

注. Gröbner 基底の概念は、多項式環だけでなく、微分作用素環、Lie 環の universal enveloping algebra などでも、定義できる。証明法は、今説明した方法とすべて同じである。(gr. を使ってもよい。)

§§3. R^m の Gröbner 基底, Free resolution, Hilbert 関数.

$R=K[x_1,\cdots,x_n]$ とか $K\langle x_1,\cdots,x_n,\partial_1,\cdots,\partial_n\rangle$ としよう。

R^m に Gröbner 基底を定義することができる。

$\triangleleft$ を R の元の間に定義された lexicographic または total degree order とする。 R^m の元 $\vec{f},\vec{g}$ の元の間に次のように order を定義する。

<u>Def.</u> $\vec{f}=(f_1,\cdots,f_m)$, $\vec{g}=(g_1,\cdots,g_m)$ とおく。

$\mathrm{topIndex}(\vec{f})=k$ (ここで、k は、$f_k\neq 0$, $f_i=0$ $i>k$ となる数である。)

$\mathrm{topIndex}(\vec{g})=l$ (〃 l 〃 $g_l\neq 0$, $g_i=0$ $i>l$ 〃)

$\vec{f}>\vec{g} \Longleftrightarrow \mathrm{topIndex}(\vec{f})>\mathrm{topIndex}(\vec{g})$

or $(\mathrm{topIndex}(\vec{f})=\mathrm{topIndex}(\vec{g})=k$ かつ $f_k \triangleright g_k)$

<u>Def.</u> $\vec{f}$ が $\vec{g}$ で reducible.

$\Longleftrightarrow \mathrm{topIndex}(\vec{f})=\mathrm{topIndex}(\vec{g})=k$ かつ f_k が g_k で reducible.

<u>Def.</u> $\vec{f}\longrightarrow\vec{h}$ by $\vec{g}$, $\vec{f}$ が $\vec{g}$ で reducible かつ.

$\vec{h}=\vec{f}-a\vec{g}$, ここで $f_k\to h_k$ by g_k

$h_k=f_k-a\,g_k$

$k=\mathrm{topIndex}(\vec{f})$

<u>Def.</u> $sp(\vec{f},\vec{g})=\begin{cases}0, & \mathrm{topIndex}(\vec{f})\neq\mathrm{topIndex}(\vec{g})\\ a\vec{f}-b\vec{g}, & \mathrm{topIndex}(\vec{f})=\mathrm{topIndex}(\vec{g})=k\end{cases}$

ここで $sp(f_k,g_k)=af_k-bg_k$

<u>Def.</u> $G=\{\vec{g}_1,\cdots,\vec{g}_p\}$ が R^m の部分加群 M の Gröbner 基底 $\Longleftrightarrow$

$\forall i,j$ $sp(\vec{g}_i,\vec{g}_j)\xrightarrow{*}0$ by G かつ G が M を生成。

定理13 (ア) R^m の部分加群 M は Gröbner 基底 G をもつ。

(イ) $\vec{h}\in M \Rightarrow \vec{h}\xrightarrow{*}0$ by G。

R^m における不定方程式

(3.1) $\sum_{i=1}^{m} h_i \vec{g}_i = 0$

の解空間 $\{(h_1, \cdots, h_m)\} =: \mathcal{H}$ は左R加群となる。Gröbner基底を用いると、$\mathcal{H}$ の generator を求めることができる。$\{\vec{g}_i\}$ をGröbner基底であるとしよう。このとき、

$$sp(\vec{g}_i, \vec{g}_j) \xrightarrow{\ *\ } 0 \quad \text{by } \{\vec{g}_i\}$$

だから、

$$sp(\vec{g}_i, \vec{g}_j) = \sum_{k=1}^{m} {}^{\exists} s_k^{(ij)} \vec{g}_k \ , \quad \deg(s_k^{(ij)} \vec{g}_k) \preceq \deg(sp(\vec{g}_i, \vec{g}_j))$$

となる。$sp(\vec{g}_i, \vec{g}_j) = u_i^{(ij)} \vec{g}_i - u_j^{(ij)} \vec{g}_j$ とおくと、

$$\sum_{k=1}^{m} \tilde{s}_k^{(ij)} \vec{g}_k = 0, \quad \tilde{s}_i^{(ij)} = s_i^{(ij)} - u_i^{(ij)}, \ \tilde{s}_j = s_j^{(ij)} + u_j^{(ij)} \vec{g}_j,$$
$$\tilde{s}_k^{(ij)} = s_k^{(ij)} \quad (k \neq i, j)$$

である。

定理14 $\{\vec{g}_i\}$ がGröbner基底であるとする。このとき、(3.1)の解空間 $\mathcal{H}$ は、

$$\vec{s}^{(ij)} = (\tilde{s}_1^{(ij)}, \cdots, \tilde{s}_m^{(ij)}) \quad , \quad i, j = 1, \cdots, m$$

で生成される。

証明. 証明は定理5と同様である。つまり、

$$\vec{h} = (h_1, \cdots, h_m), \ \deg(\vec{h}) := \max_{i=1,\cdots,m} \deg(h_i \vec{g}_i), \ M(\vec{h}) := \#\{h_i \mid \deg(h_i \vec{g}_i) = \deg(\vec{h})\}$$

とおく。たして0だから、$M(\vec{h}) \geq 2$ である。添字の順番をかえて

$\deg(\vec{h}) = \deg(h_1 \vec{g}_1) = \deg(h_2 \vec{g}_2)$

とする。

$\exists q \in R,\ \deg(h_1\vec{g}_1 - q u_1^{(12)}\vec{g}_1) < \deg(h_1\vec{g}_1)$ とできる。

$$0 = \sum_{i=1}^{m} h_i \vec{g}_i + q \sum_{k=1}^{m} \tilde{S}_k^{(12)} \vec{g}_k \quad \text{———} \ (*)$$

$$= (h_1 - q u_1^{(12)})\vec{g}_1 + q\sum_{k=1}^{m} S_k^{(12)} \vec{g}_k + q u_2^{(12)} \vec{g}_2 + \sum_{i\geq 2} h_i \vec{g}_i$$

$= \quad j_1 := h_1 - q u_1^{(12)} + q S_1^{(12)}$

$\quad j_2 := q S_2^{(12)} + q u_2^{(12)} + h_2$

$\quad j_i := h_i + q S_i^{(12)}, \ (i \neq 1,2)$ とおくと.

$= \sum j_k \vec{h}_k$

$\therefore \deg(j_1\vec{g}_1) < \deg(\vec{h}),\quad \deg(j_k \vec{g}_k) \leq \deg(h_k \vec{g}_k)\ (k \geq 2)$

よって、$M(\vec{h})$ か $\deg(\vec{h})$ が減少する。したがって $(*)$ の操作をくりかえせば（h_i を j_i とおく）、最後には $h_i = 0$ が となる。//

定理4. を用いることにより、Free resolution を計算できる。

$$\begin{array}{ccc} R^m & \xrightarrow{A} & R^n \\ \cup & & \cup \\ \vec{x} & & \vec{y} \end{array}, \quad \vec{y} = \vec{x}A.$$

のとき、$\mathrm{Ker}\,A = \{\vec{x} \mid \vec{x}A = \vec{0}\} = \{(x_1, \cdots, x_m) \mid \sum_{i=1}^{m} x_i \vec{A}_i = 0\}$,

ここで、$A = \begin{pmatrix} \vec{A}_1 \\ \vdots \\ \vec{A}_m \end{pmatrix}$ $\vec{A}_k$ は横ベクトル である。

$\{\vec{A}_k\}$ の Gröbner basis を $\{\vec{g}_k\}$ とする。

$$\vec{g}_k = \sum_j c_{kj} \vec{A}_j, \quad c_{kj} \in R$$

と書ける。

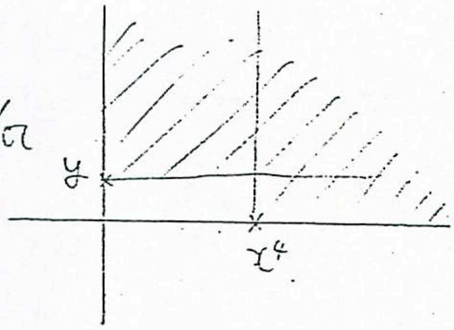
$$\sum_{k=1}^{p} y_k \vec{g}_k = 0 \quad \text{とするとき.}$$

$$\sum_{k=1}^{p} y_k \sum_{j=1}^{m} c_{kj} \vec{A}_j = \sum_{j=1}^{m} \left(\sum_{k=1}^{p} y_k c_{kj} \right) \vec{A}_j = 0$$

∴ Ker A は. $\left(\sum_{k=1}^{p} \tilde{S}^{(ij)}_k c_{k1}, \cdots, \sum_{k=1}^{p} \tilde{S}^{(ij)}_k c_{km} \right)$, $i, j = 1, \cdots, p$

でR上生成される。

例. $R = K[x, y]$, $\mathfrak{a} = (x^4, y)$, $M = R/\mathfrak{a}$ とする.



$$\begin{array}{ccccc} R & \longrightarrow & M & \longrightarrow & 0 \\ \Psi & & \Psi & & \\ f & \longmapsto & [f] & & \end{array}$$

$$\begin{array}{ccccccc} R^2 & \longrightarrow & R & \longrightarrow & M & \longrightarrow & 0. \\ \Psi & & \Psi & & & & \\ (f, g) & \longmapsto & fx^4 + gy & & & & \end{array} \qquad \text{(exact)}$$

$Sp(x^4, y) = y \cdot x^4 - x^4 \cdot y = 0$ より, $\{x^4, y\}$ は Gröbner basis. よって.

$fx^4 + gy = 0$ の解空間 (f, g) は, $(y, -x^4)$ でR上生成される。

∴

$$\begin{array}{ccccccccccc} 0 & \to & R & \longrightarrow & R^2 & \longrightarrow & R & \to & M & \longrightarrow & 0 \\ & & \Psi & & \Psi & & & & & & \\ & & h & \longmapsto & h(y, -x^4) & & & & & & \end{array} \qquad \text{(exact)}$$

例. $R = K[x, y, z]$, $\mathfrak{a} = (x^2, y, z)$, $M = R/\mathfrak{a}$ とする。

$$\begin{array}{ccccccc} R^3 & \longrightarrow & R & \longrightarrow & M & \longrightarrow & 0 \\ \Psi & & \Psi & & & & \\ (f, g, h) & \longmapsto & fx^2 + gy + hz & & & & \end{array} \qquad \text{(exact)}$$

$Sp(x^2, y) = y\cdot x^2 - x^2\cdot y = 0$, $Sp(y, z) = z\cdot y - y\cdot z = 0$, $Sp(z, x^2) = x^2\cdot z - z x^2 = 0$

より、 $f x^2 + g y + h z = 0$ の解は、

$\vec{v_1} = (y, -x^2, 0)$, $\vec{v_2} = (0, z, -y)$, $\vec{v_3} = (-z, 0, x^2)$

で生成される。 ※※ R^3 での lexicographic order で、

$Sp(\vec{v_1}, \vec{v_2}) = 0$, $Sp(\vec{v_2}, \vec{v_3}) = x^2 \vec{v_2} + y \vec{v_3} = (-yz, x^2 z, 0)$

$(-yz, x^2 z, 0) + z\vec{v_1} = (0,0,0)$ $\therefore Sp(\vec{v_2}, \vec{v_3}) \xrightarrow{*} 0$ by $\{\vec{v_1}, \vec{v_2}, \vec{v_3}\}$

$Sp(\vec{v_3}, \vec{v_1}) = 0$。

よって、$\{\vec{v_1}, \vec{v_2}, \vec{v_3}\}$ は Gröbner basis である。 ※※※

※※ までより、

$$\begin{array}{ccccccccc} R^3 & \longrightarrow & R^3 & \longrightarrow & R & \longrightarrow & M & \longrightarrow & 0 \quad (\text{exact}) \\ \cup & & \cup & & & & & & \\ (f,g,h) & \longmapsto & f\vec{v_1} + g\vec{v_2} + h\vec{v_3} & & & & & & \end{array}$$

※※※ より、

$$f\vec{v_1} + g\vec{v_2} + h\vec{v_3} = 0$$

の解空間は、 (z, x^2, y) で R 上生成される。

$\therefore$

$$\begin{array}{ccccccccccc} 0 \to R & \longrightarrow & R^3 & \longrightarrow & R^3 & \longrightarrow & R & \longrightarrow & M & \longrightarrow & 0 \quad (\text{exact}) \\ \cup & & \cup & & & & & & & & \\ f & \longmapsto & f(z, x^2, y) & & & & & & & & \end{array}$$

Hilbert 関数の計算法

$\mathcal{F}_k = \left\{ \sum_{|\alpha|+|\beta|\leq k} a x^\alpha y^\beta \;\middle|\; a \in K \right\}$ とおく。$\mathfrak{a}$ を $R=K[x,y]$ のイデアルとするとき、

$$h(k) = \dim_K \mathcal{F}_k / \mathcal{F}_k \cap \mathfrak{a}$$

を加群 $R/\mathfrak{a}$ の Hilbert 関数とよぶ。

さて、$G = \{g_1, \cdots, g_m\}$ を $\mathfrak{a}$ の Gröbner 基底としよう。

$\mathrm{head}(g) = a x^\alpha y^\beta$ のとき、

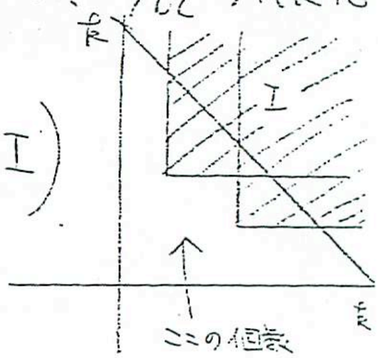
$\mathrm{Exp}(g) = (\alpha, \beta)$ と書くことにする。

$I = \bigcup_{i=1}^{m} \left(\mathrm{Exp}(g_i) + \mathbb{N}_0^2 \right)$ とおく。I は $\mathbb{N}_0^2$ のモノイデアルである。

定理5 より、$\{ x^\alpha y^\beta \mid (\alpha, \beta) \in \mathbb{N}_0^2 \setminus I \}$ が、$R/\mathfrak{a}$ の代表元である。したがって、$k \gg 0$ のとき、

$$h(k) = \#\left(\{ (\alpha,\beta) \in \mathbb{N}_0^2 \mid |\alpha|+|\beta| \leq k \} \setminus I \right)$$

となる。



$G(I)$ で I の generator をあらわすと上の場合、

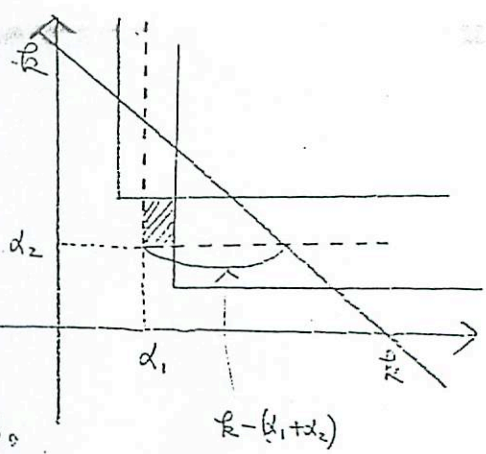
$G(I) = \{ \mathrm{Exp}(g_1), \cdots, \mathrm{Exp}(g_m) \}$ である。

I を $\mathbb{N}_0^n$ のモノイデアルとする。

$$\#\left(\{ \alpha \in \mathbb{N}_0^n \mid |\alpha| \leq k \} \setminus I \right)$$

を求める公式を作ろう。$G(I)$ の個数についての再帰的な公式で上の個数はあらわせる。

$\#G(I)=p$ の時の公式がわかっているとする。$p+1$ 個目のgeneratorを新しくもってくる。このgeneratorを α とすれば、右図 //// の個数を p の時の公式から引けばよい。しかしながら、//// の個数は、α を原点と考えれば p 以下の時の公式を用いて書ける。以上をまとめよう。



$\alpha^i=(\alpha^i_1,\cdots,\alpha^i_n)\in\mathbb{N}_0^n$, $i=1,\cdots,p$ が与えられているとする。

$$H(k;p;\alpha^1,\cdots,\alpha^p)=\#\left(\{\alpha\in\mathbb{N}_0^n \mid |\alpha|\le k\}\setminus\bigcup_{i=1}^{p}(\alpha^i+\mathbb{N}_0^n)\right)$$ とおく。

このとき、

公式 $H(k;p;\alpha^1,\cdots,\alpha^p)$

$=$ if $p=1$ then

$K:=k-|\alpha^1|$

return$\left[\binom{n+k}{n}-\binom{n+K}{n}\right]$

else

$\tilde{\alpha}^i:=\mathrm{lcm}(\alpha^i,\alpha^p)-\alpha^p$ をすべての i に対してやる。

return$\left[H(k,p-1;\alpha^1,\cdots,\alpha^{p-1})-H(\underbrace{\ }_{k-|\alpha^p|},p-1;\tilde{\alpha}^1,\cdots,\tilde{\alpha}^{p-1})\right]$

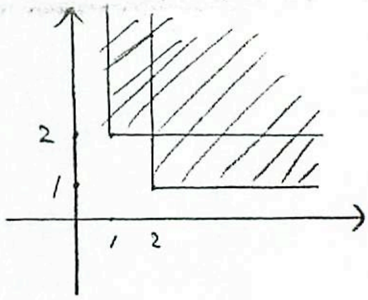
endif

さて、

$h(k)=H(k;p;\mathrm{Exp}(g_1),\cdots,\mathrm{Exp}(g_m))$ である。

例. $\alpha^1=(2,1)$, $\alpha^2=(1,2)$

$n=2$.



$H(k;2;\alpha^1,\alpha^2)$

$$= H(k;1;\alpha^1) - H(k-3;1;(1,0))$$

$$= \binom{2+k}{2} - \binom{2+(k-3)}{2} - \binom{2+k-3}{2} + \binom{2+k-3-1}{2}$$

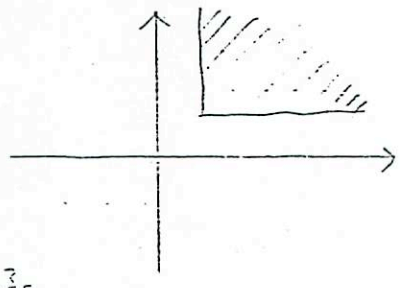
$$= \binom{2+k}{2} - \binom{k-1}{2} - \binom{k-1}{2} + \binom{k-2}{2}$$

以上より、次のよく知られた定理を得ることができる。

定理 15.　Hilbert 関数 $h(k)$ は k の多項式である。さらにくわしく、$h(k)$ は 2 項係数の和で書ける。

例.

$\mathfrak{a} = (xy - 1)$, $R = K[x, y]$　order は total degree order



$\mathrm{Head}(xy-1) = xy$

$\mathrm{Exp}(x, y) = (1, 1)$ より.

$$h(k) = \binom{2+k}{2} - \binom{n+k-2}{n} = C(k)$$ となる。

以上のチュートリアルの原論文をあげておく。

Gröbner 基底は、[Buch0], [Buch2] など

R^m の Gröbner 基底, Free resolution, ヒルベルト関数については [FSK], [MM] など

書きまちがいがないよう注意したが、あったらごめんなさい。