計算代数統計

中村 文士

October 9, 2024

目次

目次

進め方

- 計算代数統計の本を読む形で進めていって、不明点があれば、この資料の中で導出していきます。
- この本は、線形代数や微積の知識すらなくとも理解できるように書かれていると思うので、他の知識の前提がなく理解できるかと思います。
- 一通り本の導出部分も追ったつもりですが、証明は説明できるほど理解できていないと思うので、適宜ご指摘頂ければと思います。
- コメントの枠で書かれている部分はこの資料の作成者の感想を書いているだけなので正しいか怪しいです。

グレブナー基底でできる事の理解

今回読む本や論文、雑誌などを見て、どういった応用があるか列挙しています。

- 多項式の連立方程式 (線形でなく、x^n などの項も含む) を簡単にする時に使える
- 実験計画法の考えるべき入力の組み合わせを列挙できる
- 制御の問題で複数の多項式制約が与えられたとき、それを簡単にする時に使える
- 整数格子状の三角形分割で使える (数理科学)
- マルコフ基底というものを考える時に使う?(数理科学, Algebraic Statistics)
- transfomer を使ったある問題で使える, IBIS2023 の発表にあった

目次

目次

線形な連立方程式

以下の問題をまず考える

$$\begin{cases} x + 2y - z = 2 \\ x + y - 4z = 3 \\ x + 3y + 3z = 0 \end{cases} \tag{1}$$

これは、連立 1 次方程式なので、線形代数で学ぶ手法を使えば良い

次に、以下の問題も考えてみる

$$\begin{cases} x^2 + y^2 + 4z^2 = 81 \\ x - y + z^2 = 13 \\ xz - 2y = 18 \end{cases} \tag{2}$$

これは、第 2 式の 2 倍を第 3 式から引いて y を消去し、$xz - 2x - 2z^2 = -8$ を得て、この因数分解 $(z-2)(x-2z-4) = 0$ を行うことで、計算ができる。

次の問題は少し難しい

$$\begin{cases} x^2 + y^2 + 4z^2 = 90 \\ x - y + z = 12 \\ xz - 3y = 28 \end{cases} \tag{3}$$

これは、同じような因数分解ができない。グレブナー基底の計算のような方法で解いてみようと思ったが、教科書と同じ式導出になりそうなので、教科書で説明

注意点

- 先ほどの手順はグレブナー基底の計算アルゴリズムになっていることが、後の章で分かる。
- グレブナー基底は、各単項式 (定義はいずれ出てくる) の順序を与えると得られるもので、今回の手順は、$x \succ y \succ z$ で純辞書式順序という順序を用いた場合の結果になっている
- 最終的に得られた連立方程式の形式は z だけの式だった。これは偶然ではなく、消去定理の結果から、純辞書式順序を用いると、連立方程式のうちの一つが一つの変数の方程式になるためである (これはすごいと思った)。

実演

ここまでの式のグレブナー基底を Python 求めてみる:
Python でグレブナー基底を使う方法に例えば sympy があるので、それを簡単に紹介する

目次

いくつかの概念の定義

いくつかの概念を定義する

- 単項式: $\prod_{i=1}^{n} x_i^{a_i} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, 各 a_i は非負整数
- 単項式の次数: $\sum_{i=1}^{n} a_i$
- 多項式: 変数 $x_1, \ldots, x_n$ の有限個の項の和
- 多項式の次数: 多項式の単項式 f の次数の中で最大のもの. $deg(f)$ と表記する

※ 負の整数も含んだ多項式はローラン多項式という。この本では取り扱わないが、発展的な話題として存在しているようです。

定義したものの例

$$f = -5x_1^2x_2x_3^2 + \frac{2}{3}x_2x_4^3x_5^2 - x_3^3 - 7$$

を考える。この場合、単項式は

- $-5x_1^2x_2x_3^2$
- $\frac{2}{3}x_2x_4^3x_5^2$
- $-x_3^3$
- -7

であり、$deg(f) = 6$ である。
-7 は、係数が -7 で 1 の単項式であり、各変数の次数が 0 なので次数 0 の単項式を表す。

多項式環

K を $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ として用いる.
→ 有理数, 複素数, 実数は零割り以外の四則演算ができて、そういった集合を体と呼ぶ.
K のいずれかを係数とした $x_1, \ldots, x_n$ の多項式の集合を $K[x_1, \ldots, x_n]$ で定義する.

コメント

本を読んだとき $x_1, \ldots, x_n$ が何の集合か不明に感じましたが、不定元と呼ばれるもので、K 上の元の代入はできるが、K 上の元である必要はないもののようです。

$K[x_1, \ldots, x_n]$ の 2 つの元 f, g に対して加減算 $f + g$, $f - g$、積 fg は $K[x_1, \ldots, x_n]$ の元であるが、商 f/g は多項式とは限らないため、$K[x_1, \ldots, x_n]$ の元とはいえない。このように加減算と積について閉じている集合を環という。
$K[x_1, \ldots, x_n]$ は多項式の環なので、多項式環と呼ぶ。

アフィン多様体

イデアルを考える動機付けを行うため、まずアフィン多様体を定義する:
$K[x_1, \ldots, x_n]$ の r 個の元による連立方程式を考える;

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \cdots \\ f_r(x_1, \ldots, x_n) = 0 \end{cases} \tag{4}$$

$K^n := \{(a_1, \ldots, a_n) | a_1, \ldots, a_n \in K\}$ と定義する。
この時、多項式 $f(x_1, \ldots, x_n)$ の零点とは K^n の元 $(a_1, \ldots, a_n)$ で

$$f(a_1, \ldots, a_n) = 0$$

を満たすものをいう (各 x_i に a_i を代入している)。アフィン多様体は、連立方程式全ての零点を与える集合 (つまり、連立方程式の解) であり、数式で書くと、以下のようになる:

$$V(f_1, \ldots, f_r) = \{(a_1, \ldots, a_n) | f_i(a_1, \ldots, a_n) = 0, i = 1, \ldots, r\}. \tag{5}$$

アフィン多様体の具体例

前節の難しかった連立方程式
$f_1 = x^2 + y^2 + 4z^2 - 90(= 0), f_2 = x - y + z - 12(= 0), f_3 = xz - 3y - 28(= 0)$ を解くことは、アフィン多様体を求めることであり、したがって f_1, f_2, f_3 のアフィン多様体は

$$V(f_1, f_2, f_3) = \left\{ \left(\frac{7 \pm \sqrt{3}}{2}, \frac{-13 \pm 3\sqrt{3}}{2}, 2 \pm \sqrt{3} \right), \left(4 \pm \sqrt{6}, \frac{-26 \pm 6\sqrt{6}}{5}, \frac{14 \pm \sqrt{6}}{5} \right) \right\}$$

である。これを解く過程を見ることで、連立方程式を解くうえで、どういった演算ができる必要があるかを確認していく。

まず、$f_2 = 0$ を x について解いて $(x = y - z + 12)$、$f_3 = xz - 3y - 28$ にそれを代入するということを行っていた:

$$\begin{cases} f_1 = x^2 + y^2 + 4z^2 - 90 = 0 \\ f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \end{cases}$$

これは

$$\begin{aligned} f_4 &= (y - z + 12)z - 3y - 28 = (y - z + 12)z - xz + xz - 3y - 28 \\ &= (y - z + 12 - x)z + xz - 3y - 28 = -zf_2 + f_3 \end{aligned}$$

となっていることから、$f_4 = f_3 - zf_2$ であることが分かる。
これがもとの連立方程式と同値なことは、$f_2 = f_3 = 0 \Rightarrow f_2 = f_4 = 0,\ f_2 = f_4 = 0 \Rightarrow f_3 = zf_2 + f_4 = 0, f_2 = 0$ であることより従う。

コメント

少し後に書いてあるが、代入操作というものは、f_3 の x を $f_2 - y + z - 12$ で置き換えて余りを f_4 としていることに他ならない。

次に $f_2 = 0$ を x について解いて $(x = y - z + 12)$、$f_1 = x^2 + y^2 + 4z^2 - 90$ に代入して、$f_4 = 0$ を yz について解いたものを代入することで、

$$\begin{cases} f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \\ f_5 = 2y^2 + 18y + 3z^2 - 2 = 0 \end{cases}$$

を導いた。この f_5 を導くための演算は

$$f_1 - (x + y - z + 12)f_2 + 2f_4 = f_5$$

となっていた。

さらにここから、f_4 の yz と f_5 の $2y^2$ を打ち消すため、$2yf_4 - zf_5$ を作って、$f_4 = 0$ を yz について解いた式と $f_5 = 0$ を y^2 について解いた式を代入し、最後に全体を -1 倍することで、

$$f_6 = 2y + 5z^3 - 33z^2 + 54z + 6 = 0$$

を得た。この f_6 の求めるための演算を整理すれば、

$$\begin{aligned} f_6 &= -1 \times (2yf_4 - zf_5 + 3f_5 + (2z - 6)f_4 + 6f_4) \\ &= (-2y - 2z)f_4 + (z - 3)f_5 \end{aligned}$$

となる。f_5 が不要かどうか自明でないため、ここでは一旦残しておいて、連立方程式を

$$\begin{cases} f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \\ f_5 = 2y^2 + 18y + 3z^2 - 2 = 0 \\ f_6 = 2y + 5z^3 - 33z^2 + 54z + 6 = 0 \end{cases}$$

とする。

最後に

$$f_7 = -2f_4 + (z-3)f_6 = 5z^4 - 48z^3 + 155z^2 - 180z + 38$$
$$f_8 = 2f_2 + f_6 = 2x + 5z^3 - 33z^2 + 56z - 18$$

として最終的な連立方程式を得ていた (前節で解いたときは f_5 は消えていた)。

イデアル

この連立方程式を求めるうえで、行った操作を振り返ると、代入やある項を打ち消す演算というのは、元々の多項式の多項式倍と、その足し合わせで定義されることが確認できた。そこで、もとの連立方程式を定義する多項式 $f_1, \ldots, f_r$ から、多項式倍の足し合わせにより得られるすべての多項式の集合に着目する:

$$\{h_1 f_1 + \ldots + h_r f_r | h_1, \ldots, h_r \in K[x_1, \ldots, x_n]\} := \langle f_1, \ldots, f_r \rangle \tag{6}$$

これまで求めた f_4, f_5, f_6, f_7 は $\langle f_1, f_2, f_3 \rangle$ の元であることは確認出来て、例えば f_7 は

$$
\begin{aligned}
f_7 &= -2f_4 + (z-3)f_6 = -2f_4 + (z-3)((-2y-2z)f_4 + (z-3)f_5) \\
&= (-2-(z-3)(2y+2z))f_4 + (z-3)^2 f_5 \\
&= (-2-(z-3)(2y+2z))f_4 + (z-3)^2(f_1 - (x+y-z+12)f_2 + 2f_4) \\
&= (-2+(z-3)(-2y-6))f_4 + (z-3)^2 f_1 - (z-3)^2(x+y-z+12)f_2 \\
&= (z-3)^2 f_1 + (2yz^2 - 6yz + 6z^2 - 16z - (z-3)^2(x+y-12))f_2 + (-2yz+6y-6z+16) \\
&\in \langle f_1, f_2, f_3 \rangle
\end{aligned}
$$

である (途中の式展開はちょっと怪しい。ただ、f_1, f_2, f_3 の多項式倍の和であることは分かるかと思います)。

多項式の集合 $\langle f_1, \ldots, f_r \rangle$ は連立方程式 $f_1 = \cdots = f_r = 0$ を解くときの多項式倍と足し合わせの式変形により現れうる全ての多項式からなる集合である。
$\langle f_1, \ldots, f_r \rangle$ は無限個の多項式を含むことがあるが、これが元の連立方程と同じ点を解の集合 (アフィン多様体) を持つことを確認する:
$\langle f_1, \ldots, f_r \rangle$ のアフィン多様体を $V(\langle f_1, \ldots, f_r \rangle)$ と書くことにする。この時
$V(f_1, \ldots, f_r) = V(\langle f_1, \ldots, f_r \rangle)$ であることを示す。

証明.

$V(\langle f_1, \ldots, f_r \rangle) \subset V(f_1, \ldots, f_r)$ を示す。
$a \in V(\langle f_1, \ldots, f_r \rangle)$ ならば $\sum_r h_r(a) f_r(a) = 0$ が任意の $h_r \in K[x_1, \ldots, x_n]$ で成り立つ必要があるため、$f_1(a) = \cdots = f_r(a) = 0$ であることが分かる。
次に $V(f_1, \ldots, f_r) \subset V(\langle f_1, \ldots, f_r \rangle)$ を示す。
$a \in V(f_1, \ldots, f_r)$ ならば $f_1(a) = \cdots = f_r(a) = 0$ なので、$h_1(a) f_1(a) + \cdots + h_r(a) f_r(a) = 0$ が成り立つ。
これは $a \in V\langle f_1, \ldots, f_r \rangle$ であることを示しているため、$V(f_1, \ldots, f_r) = V(\langle f_1, \ldots, f_r \rangle)$ であることが示された。 □

前ページの結果から、$\langle f_1, \ldots, f_r \rangle$ のアフィン多様体を求めることで、元の連立方程式のアフィン多様体 (連立方程式の解) が求まることが分かった。
$\langle f_1, \ldots, f_r \rangle$ は以下で定義する多項式環のイデアルの一つであり、連立方程式を求めるため、イデアルの性質を使うことができるため、$\langle f_1, \ldots, f_r \rangle$ を主に考えていく:

定義 1 (イデアル)

多項式環の空でない部分集合 $I \subset K[x_1, \ldots, x_n]$ がイデアルとは、以下の 2 つの条件を満たすことである。

1. $f, g \in I \to f + g \in I$ (和について I の中で閉じている)
2. $f \in I, h \in K[x_1, \ldots, x_n] \to hf \in I$ (多項式倍について I の中で閉じている)

コメント

$f, g \in I$ に対して、$-1 \in K[x_1, \ldots, x_n]$ から $-1 \times g \in I$ で、$f + (-g) = f - g \in I$ である (差についても閉じていて、そういう前提で説明していく)

また、この定義は厳密には左イデアルと言う気がするがこの教科書ではイデアルと呼ぶ。

イデアルの例

$I = \langle f_1, \ldots, f_r \rangle \subset K[x_1, \ldots, x_n]$ がイデアルであることを、定義に従って確認する。
$f, g \in \langle f_1, \ldots, f_r \rangle$ とする。$f = \sum_{i=1}^{r} h_i f_i, g = \sum_{i=1}^{r} h'_i f_i$ とすると、$f + g = \sum_{i=1}^{r} (h_i + h'_i) f_i$ となり $f + g \in I$ である。
$f = \sum_{i=1}^{r} h_i f_i \in \langle f_1, \ldots, f_r \rangle, h \in K[x_1, \ldots, x_n]$ とすると、$hf = \sum_{i=1}^{r} (h_i h) f_i$ となり $hf \in I$ である。
したがって、I はイデアルである。

有限生成なイデアル

イデアル $\langle f_1, \ldots, f_r \rangle$ は、有限個の多項式 $\{f_1, \ldots, f_r\}$ から定義される自然なイデアルであるが、任意のイデアルがこのように書けるかは自明でないため、それが可能か考えていく。
それを考えるため $K[x_1, \ldots, x_n]$ の空でない部分集合 $\{f_\lambda | \lambda \in \Lambda\}$ に対する有限和

$$\sum_{\lambda \in \Lambda} h_\lambda f_\lambda, h_\lambda \in K[x_1, \ldots, x_n]$$

の全体からなる集合を考える。ここで、Λ は添字集合 (有限でも、加算でも、非加算でも良い) であり、$\{h_\lambda | \lambda \in \Lambda\}$ は有限個を除いて 0 である多項式の集合である。
この集合は和、多項式倍について閉じていることは自明なのでイデアルである。
このイデアルを $\{f_\lambda | \lambda \in \Lambda\}$ が生成するイデアルと呼び

$$\langle \{f_\lambda | \lambda \in \Lambda\} \rangle$$

と書く。

逆に、任意のイデアル $I \subset K[x_1, \ldots, x_n]$ に対して、例えば、その部分集合の元そのものを使って、$I = \langle \{f_\lambda | \lambda \in \Lambda\} \rangle$ となるような $K[x_1, \ldots, x_n]$ の部分集合 $\{f_\lambda | \lambda \in \Lambda\}$ を作ることができる。この $\{f_\lambda | \lambda \in \Lambda\}$ を I の生成元と呼ぶ。
添字集合は無限の場合も考えられるが、$\langle f_1, \ldots, f_r \rangle$ は有限個の多項式から生成されていて、そういったイデアルを有限生成なイデアルと呼ぶ。

コメント

この資料を準備した当初有限個を除いて 0 である多項式の集合は有限な生成系のように感じていましたが、後の証明を考える過程で

$$\sum_{\lambda \in \Lambda} h_\lambda f_\lambda, h_\lambda \in K[x_1, \ldots, x_n]$$

の $h_\lambda \neq 0$ が有限個というのは、各元で 0 になる h_λ は異なるので有限な生成系にはならないものだと理解しました。

イデアルに関する諸問題

イデアルに関する内容について、ここまでの話をまとめる。
まず、多項式の連立方程式のアフィン多様体 (連立方程式の解) は、有限生成なイデアルのアフィン多様体で与えられることを学んだ。
そのため、イデアルについて考えていくことは重要である。
また、連立方程式の解を求める以外にもイデアルの応用はあり、そういった応用を考えるうえで以下の問題を考えていく。

考える問題

- イデアル記述問題: 任意に与えられたイデアル $I \subset K[x_1, \ldots, x_n]$ が、$\langle f_1, \ldots, f_r \rangle$ といった形で書けるかどうかを判定する問題
- イデアル所属問題: イデアル I と多項式 f が与えられたとき、$f \in I$ かどうかを判定する問題

イデアル記述問題, イデアル所属問題は、連立方程式の解を求める問題には不要であるが、2章の実験計画法を考える上で必要になる。

コメント

これらを解決するうえで、グレブナー基底という概念が重要である。グレブナー基底を求めることによって、消去定理が得られて、1.1 節で計算していた連立方程式の簡約化ができるため、これらの解決を目指していくことになる。

1 変数の記述問題・所属問題

まず、1 変数の多項式環 $K[x]$ について、イデアル記述問題とイデアル所属問題がどうなるかを考える。
鍵となるのは、多項式の割り算であり、例題を使って考えていく。高校の時に習った一変数の筆算を思い出すと、$f(x)$ を $g(x)$ で割ったとき、商を $q(x)$, 余りを $r(x)$ とすると、

$$f(x) = q(x)g(x) + r(x)$$

とかけて、$r(x)$ の次数は $g(x)$ より小さく、$q(x)$ と $r(x)$ は一意に定まっていた。
具体例として以下の問題を解いてみる。

問題 1.4

$f(x) = x^4 + 2x^3 - x^2 + 4x - 1$ を $g(x) = x^2 - 3x + 1$ で割った商とあまりを求めよ

これは筆算を用いるなどすれば、$f(x) = (x^2 + 5x + 13)g(x) + 38x - 14$ となる。

先ほどの計算を $g(x)$ で次数が一番大きい項である x^2 を $g(x)+3x-1$ に置き換えていると思って、$f(x)$ 上の $g(x)$ を置き換えられなくなるまで (置き換えていない項の次数が $g(x)$ の次数より小さくなるまで) 置き換えると次のようになる:

$$\begin{aligned} f(x) &= x^2(g(x)+3x-1)+(2x^3-x^2+4x-1) \\ &= x^2g(x)+5x^3-2x^2+4x-1 \\ &= x^2g(x)+5x(g(x)+3x-1)-2x^2+4x-1 \\ &= (x^2+5x)g(x)+13x^2-x-1 \\ &= (x^2+5x)g(x)+13(g(x)+3x-1)-x-1 \\ &= (x^2+5x+13)g(x)+38x-14 \end{aligned}$$

単項イデアル

先ほどの 1 変数の多項式の割り算をもとに、1 変数の多項式環のイデアルについて考えてみる。
1 変数の単項式間 $K[x]$ のイデアルを $I \in K[x]$ とする。この I の元のうち、次数が最小のものに注目し、そのうちの一つを $g \in I$ とする。この時、$f \in I$ ならば、$f = qg + r$ とかけるが、g の次数は r よりも小さいため、$r = 0$ である。
したがって、1 変数の多項式環のイデアルは、次数が最小の元で生成されるということがわかる:

$$I = \{qg | q \in K[x]\} = \langle g \rangle$$

これが、1 変数の多項式環のイデアル記述問題の解であり、このように一つの多項式からなる生成系を持つイデアル、単項イデアルとよぶ。

次にイデアル所属問題について考えてみる。
これは $\forall f \in K[x], f \in I = \langle g \rangle$ かどうかを判定する問題である。
これは、f が g の多項式倍になっているかどうかを確認すればよくて、

$$f \in \langle g \rangle \Leftrightarrow \exists q \in K[x], f = qg \tag{7}$$

を確認すればよい。
さらに、次数が最小の I の元 g は、定数倍を除いて一意的に定まることも示すことができる:

証明.

一意に定まらないとすると、次数が最小の 2 つの元 f, g に対してその定数倍の集合 $A_g = \{cg | c \in K, g \in K[x]\}$,$A_f = \{cf | c \in K, f \in K[x]\}$ があり、これらは $A_g \neq A_f$ である.
一方、任意の $f' \in A_f, g' \in A_g$ に対して、$f' - g' \in I$ だが、これらの最大の項の係数が同じとき、$f' - g'$ の次数は f', g' の次数よりも小さい。これは f, g が次数が最小であることに反する。したがって、$A_g = A_f$ となる。 □

目次

単項式イデアル

前節で、1 変数の多項式環におけるイデアル記述問題とイデアル所属問題について考えた。次に多変数の多項式環について考えたいが、任意のイデアルを考えることは難しいので、単項式から生成されるイデアルである単項式イデアルについてまず考える。

定義 2

単項式イデアル単項式からなる生成系を持つイデアルのことを、単項式イデアルと呼ぶ。

例えば、$\langle x, xy, x^2 \rangle \subset K[x, y]$ は単項式イデアルである。また、単項式イデアルの生成系は、必ず単項式の集合になるわけではなく、$\langle x_1^2, x_2^3 \rangle = \langle x_1^2, x_1^2 + x_2^3 \rangle$ などと表すことができる。

単項式を考えるので、単項式の集合を定義しておく。変数 $x_1, \ldots, x_n$ の単項式全体の集合を

$$M_n := \{\prod_{i=1}^{n} x_i^{a_i} | a_i \in \mathbb{Z}_{\geq 0}\}$$

と表す。このとき、単項式イデアルは、M_n の必ずしも有限でない部分集合 $M \subset M_n$ をもとに、$I = \langle \{u | u \in M\} \rangle$ と書くことができる。

単項式イデアルの元となる単項式

有限生成な単項式イデアルの一例として、$I = \langle x_1x_2^5, x_1^4x_2^3, x_1^6 \rangle \subset K[x_1, x_2]$ を考える。これは、M_2 の有限な部分集合 $\{x_1x_2^5, x_1^4x_2^3, x_1^6\}$ が I の生成系となっていることが分かる。また、生成系の定義から、このイデアルに属する多項式 f は、

$$f = h_1x_1x_2^5 + h_2x_1^4x_2^3 + h_3x_1^6, h_1, h_2, h_3 in K[x_1, x_2]$$

と書くことができるし、このように書ける元を集めたものが I でもある。
I の特徴づけをする。生成系の元の単項式のいずれかで割り切れる単項式は、全て I の元であることがわかる。

例

$x_1x_2^7 = x_2^2(x_1x_2^5) \in I$, であり $x_1x_2^5$ で割り切れる。

逆に、ある単項式 $u \in M_2$ があって、これが I の元であるとする。このとき

$$u = h_1 x_1 x_2^5 + h_2 x_1^4 x_2^3 + h_3 x_1^6, h_1, h_2, h_3 \in K[x_1, x_2]$$

と表せるが、左辺は単項式なので、右辺は $\{x_1 x_2^5, x_1^4 x_2^3, x_1^6\}$ のいずれかで割り切れる。

コメント

今回の例では、u は 3 つの単項式のいずれかで割り切れるが、h_i は任意の多項式なので、基本的に項の数は 3 つ以上ある。ただ、それらの項は 3 つの単項式のいずれかで括れる (=割り切れる) ということを述べている。

以上の議論を、必ずしも有限とは限らない単項式の集合 $\{u_\lambda | \lambda \in \Lambda\} \subset M_n$ で生成される一般の単項式イデアルに拡張する。単項式イデアル $\langle \{u_\lambda | \lambda \in \Lambda\} \rangle$ の元である単項式 u は

$$u = \sum_{\lambda \in \Lambda} g_\lambda u_\lambda, g_\lambda \in K[x_1, \ldots, x_n]$$

と表すことができ、この右辺を展開して得られる項のうち係数が 0 でないものはただ一つであり、その項は $\{u_\lambda | \lambda \in \Lambda\}$ のいずれかの元で割り切れる。これを補題としてまとめると、以下の通りになる。

補題 3

$I = \langle \{u | u \in M\} \rangle$ を $K[x_1, \ldots, x_n]$ の単項式イデアルとすると、単項式 $v \in M_n$ が I の元であるための必要十分条件は、ある単項式 $u \in M$ が v を割り切ることである。

ここで単項式 $u = x_1^{a_1} \cdots x_n^{a_n}$ が単項式 $v = x_1^{b_1} \cdots x_n^{b_n}$ を割り切るとは、$a_i \leq b_i$ が全ての i に対して成り立つことをいう。

なお、2 変数の単項式イデアルと、それに属する単項式かどうかは $x^a y^b$ を二次元平面上の点 (a, b) と対応させることで確認できる (教科書の図 1.1 参照)。
図 1.1 の各点は単項式イデアル $I = \langle xy^5, x^4y^3, x^6 \rangle$ に含まれる多項式を表しているが、$(1, 5), (4, 3), (6, 0)$ を左下の点として、幅、高さが無限の四角形の和集合が I に含まれる単項式であることを表している (単項式の次数は非負整数なので、非負整数上のみ考える)。

単項式イデアルの元となる多項式

次に単項式イデアル $I = \langle \{u_\lambda | \lambda \in \Lambda\} \rangle$ の元となる多項式 $f \in I$ を特徴づける。
f を

$$f = \sum_{\lambda \in \Lambda} g_\lambda u_\lambda, g_\lambda \in K[x_1, \ldots, x_n]$$

と表し、右辺に含まれる単項式を考える。それらはすべて、いずれかの u_λ で割り切れて、I の元の単項式であることがわかる。
逆に、単項式イデアル I の元である単項式を任意に選び、それらの線形結合として、多項式 f を作ればイデアルの性質から $f \in I$ である。

これらをまとめて、補題にすると以下のようになる。

補題 4

I を $K[x_1, \ldots, x_n]$ の単項式イデアルとし、$f \in K[x_1, \ldots, x_n]$ とする。
このとき、次の *3* つは互いに同値である。

1. $f \in I$
2. f の全ての項は I に属する
3. f は I の元である単項式の線形結合として表せる *(*単項式のイデアルの定義から成り立つような*...)*

単項式イデアルのイデアル所属問題

補題 3, 補題 4 から、単項式イデアルのイデアル所属問題 (ある多項式がイデアルの所属するか) の解を考える。
$f \in K[x_1, \ldots, x_n]$ が単項式イデアル $I = \langle \{u | u \in M_n\} \rangle$ に含まれるかどうかは、f の全ての単項式が I に含まれるかどうかを調べればよい (補題 4 の条件 2 より)。
f の各単項式が M_n のいずれかの元で割り切れれば、補題 3 からその単項式は I に含まれるので f も I に含まれる。以上をまとめると、

単項式イデアルの所属問題

f に含まれるすべての単項式が、それぞれいずれかの $u \in M_n$ で割り切れることが、f が I の元であるための必要十分条件である。

単項式イデアルの記述問題

単項式イデアルの記述問題 (単項式イデアルが与えられたとき、それを有限生成なイデアルで記述できるかどうか) を考える。
任意の単項式イデアル I は補題 4 の条件 3 から、I の単項式の線形結合で表せる (でもこれは、単項式イデアルの定義のような気もする)。
したがって、$I = \langle \{u | u \in M \subset M_n\} \rangle$ と書けるが、$\{u | u \in M \subset M_n\}$ は有限集合とは限らないので、生成系として不要な元を取り除くこと (かつ同じものを生成するイデアル) を考える。

不要な元の例

不要な元の例として、以下のようなものが考えられる:

- $I =< xy, xy^2 >$ を考えると、xy^2 は、$y \times (xy)$ なので不要。こういった不要な元を取り除くことを考えていく。
- ある単項式 $u \in I$ は、それを割り切る単項式 $v \in I$ があれば、生成系には不要な元になる (補題 3。

極小元による生成系

取り除けない元を極小元として次に定義する。

定義 5

極小元単項式の集合 M_n の空でない部分集合 M に対して、$u \in M$ が M の極小元であるとは、任意の $v \in M$ について、条件「v が u を割り切るならば $v = u$ である」が成立することをいう。

極小元の例

- $M = \{xy, xy^2, xy^3\}$ の時、$u = xy$ は、$v = xy^2, xy^3$ に割り切られないが、$v = xy$ に割り切られていて、$v = u$ が成り立っているので、$u = xy$ は M の極小元
- $M = \{x^2y^2, x^5, x^10y^10, x^4y^4\}$ の時、$u = x^5$ は、他の元に割り切られていないので、極小元である。$u = x^2y^2$ も他に割り切られてないので、極小元である。

コメント

この資料を準備していて、単項式の集合 M における極小元というのは、M における素数のようなもの (単位元がないので違うが) だと感じた。

不要な元を削っていった結果、極小元が得られるが、それによって元の単項式イデアルを表現できることを次の補題で示す。

補題 6

単項式イデアル $I = \langle \{u | u \in M \subset M_n\} \rangle$ について、M のすべての極小元からなる集合は I の生成系となる

証明は次ページで行うが、この補題によって極小元によって単項イデアルは表現できる事がわかる (ただし、極小元の数は有限かどうかはこの補題では分からない)。

証明.

M の全ての極小元からなる集合を $\tilde{M}$ とおき、$I_0 = \langle \{u | u \in \tilde{M}\} \rangle$ とおく。このとき、$\tilde{M} \subset M$ より、$I_0 \subset I$ は自明である。
$I \subset I_0$ を示すため、$f \in I$ が I_0 に含まれることを示す。生成系の定義より、

$$f = \sum_{u \in M} g_u u, g_u \in K[x_1, \ldots, x_n]$$

と書ける。g_u は有限個を除いて 0。$g_u \neq 0$ となる u について、u を割り切る単項式を $\tilde{M}$ から選ぶことができるので、これを v_u とする。$h_u = g_u u / v_u$ とすると、これは $K[x_1, \ldots, x_n]$ の元であり、

$$f = \sum_{u \in M} h_u v_u$$

と書くことができる。 証明続き] $v_u \in \tilde{M}$ についてまとめたもの (同じ v_u を与える h_u は和をとる) で改めて書き直すと、

証明.

[証明続き] $v_u \in \tilde{M}$ についてまとめたもの (同じ v_u を与える h_u は和をとる) で改めて書き直すと、

$$f = \sum_{v \in \tilde{M}} h_v^* v$$

$\{h_v^* | v \in M\}$ も有限個を除いて 0 なので、$f \in I_0$ である。 □

極小元の生成系の例

単項式イデアル $I = \langle xy^5, x^4y3, x^6 \rangle$ は極小元は、$\{xy^5, x^4y^3, x^6\}$ である。この極小元に対して、冗長な元を適当に追加すると、例えば

$$xy^5, xy^6, x^2y^6,$$
$$x^5y^5, x^6, x^6y^3,$$
$$x^7y^4, x^7y^5, x^9$$

を考えて、これらの生成系を作ることもできるが、この生成系は、極小元による生成系によって表現することができて、証明と同じように極小元にまとめる処理を行うと、

$$f = h_1xy^5 + h_2xy^6 + h_3x^2y^6 + h_4x^5y^5 + h_5x^6 + h_6x^6y^3 + h_7x^7y^4 + h_8x^7y^5 + h_9x^9$$
$$= (h_1 + yh_2 + xyh_3 + x^4h_4)xy^5 + (h_5 + x^3h_9)x^6 + (x^2h_6 + x^3yh_7 + x^3y^2h_8)x^4y^3$$

となる。なお、表し方は一意でなくて、後述の順序関係を与えれば、一意な構成方法を与えることは可能になる (はず)。

Dickson の補題

ここまでで、単項式イデアルのイデアル記述問題 (イデアルが有限生成である) は、単項式の任意の集合の極小元が高々有限個であることを示せれば良い事がわかった。これは次の Dickson の補題によって保証される:

定理 7 (Dickson の補題)

空でない単項式の任意の集合 $M \subset M_n$ の極小元は高々有限個である。