2019 年度 前期 代数学特論 III

更新日時 2019-05-21 20:55:59　担当 和地 輝仁

目次

1　シラバス抜粋

授業概要　多項式の割り算やグレブナ基底の理論とその応用について学ぶ授業です。

到達目標

1. グレブナ基底の性質を知り、多項式の除算に利用できる。
2. グレブナ基底の理論を連立方程式の求解などに応用できる。

授業計画　順序を交換する場合もあるので注意すること。

1. 多項式環
2. 多項式環のイデアル
3. 項順序
4. 割り算アルゴリズム
5. ディクソンの補題
6. イニシャルイデアル
7. グレブナ基底
8. ヒルベルトの基底定理
9. ブッフベルガーの判定条件
10. ブッフベルガーのアルゴリズム
11. 簡約グレブナ基底
12. 消去定理
13. 拡張定理
14. 計算機への応用
15. まとめと期末試験

成績評価　期末試験 (80%) と、毎回課す演習問題の状況 (20%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

2 授業のノート

§1 多項式環

(1.1) **定義 (環、可換環)** 2 種類の演算、和と積が定義された集合 R が**環**であるとは、次の条件 (R1) から (R7) を満たすときを言う。

(R1) 和が結合法則を満たす
(R2) 和が交換法則を満たす
(R3) 和の単位元 0 が存在する $(a + 0 = 0 + a = a)$
(R4) 和の逆元が存在する $(a + (-a) = 0$ なる $-a$ の存在$)$
(R5) 積が結合法則を満たす
(R6) 0 とは異なる積の単位元 1 が存在する $(a \cdot 1 = 1 \cdot a = a)$
(R7) 分配法則が成立する $(a(b + c) = ab + ac, (a + b)c = ac + bc)$

さらに、

(R8) 積が交換法則を満たす

も成立しているとき、R を **可換環**と呼ぶ。

可換環ではない環にも、$n \times n$ 行列全体のなす環 n **次全行列環**など重要なものがあるが、この講義では可換環のみを学ぶ。

(1.2) **例 (数のなす環)** 環の定義は条件が多く思えるかも知れないが、数の集合であれば、単に **1 と 0 を含み、和、差、積で閉じている集合**は環である、ということである。

(1) まず、複素数全体の集合 $\mathbb{C}$、実数全体の集合 $\mathbb{R}$、有理数全体の集合 $\mathbb{Q}$、整数全体の集合 $\mathbb{Z}$ はすべて環である。
(2) 偶数全体の集合 $2\mathbb{Z}$ は、1 を含まないので環ではない。ただし、それ以

外の条件は満たしている。
(3) $\{a + b\sqrt{2}\ ;\ a,b$ は整数 $\}$ は環である。
(4) m を法とした $\mathbb{Z}$ の剰余環 $\mathbb{Z}/(m)$ は (その名どおり) 環である。

(1.3) **定義 (1 変数多項式環)** 環 R の元を係数に持つような x の多項式全体の集合を

$$R[x] = \left\{ a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \;\middle|\; \begin{array}{l} n \geq 0, \\ a_0, \ldots, a_n \in R \end{array} \right\}$$

で表し、R 上の **1 変数多項式環**と呼ぶ。また、$f \in R[x]$ の**次数**を $\mathbf{deg}\,\boldsymbol{f}$ で表す。可換環上の多項式環は明らかに可換環である。

(1.4) **定義 (多変数多項式環)** R を環とする。x, y を変数とする、R 上の 2 変数多項式環 $R[x, y]$ を、

$$R[x, y] = (R[x])[y] \quad (y \text{ を変数とする、} R[x] \text{ 上の 1 変数多項式環})$$

で定める。以下、帰納的に n **変数多項式環** $R[x_1, x_2, \ldots, x_n]$ も定める。

§2 多項式環のイデアル

(2.1) **イデアル** 環 R の部分集合 $I \subset R$ が次の条件を満たすとき、I を R の**イデアル**と呼ぶ。

(I1) $0 \in I$
(I2) $f, g \in I$ ならば $f + g \in I$
(I3) $a \in R,\ f \in I$ ならば $af \in I$

以下しばらく R を環とする。

(2.2) **例** イデアルの例をいくつかあげる。

(1) $R = \mathbb{Z}$ のとき、$I = \{$ 偶数全体 $\}$ は R のイデアルである。
(2) $R = \mathbb{R}[x]$ のとき、$I = \{$ 定数項のない多項式全体 $\}$ は R のイデアルである。

(2.3) **補題 (単項イデアル)** $f \in R$ のとき、

$$\langle f \rangle = Rf = \{af \mid a \in R\}$$

と定めると、$\langle f \rangle$ は R のイデアルになる。$\langle f \rangle$ を f で**生成される単項イデアル**と呼び、f を $\langle f \rangle$ の**生成元**と呼ぶ。

(2.4) **補題 (イデアルの演算)** $I, J \subset R$ をイデアルとするとき、

$$I + J = \{f + g \mid f \in I, g \in J\},$$
$$IJ = \{\sum_{\text{有限和}} f_i g_i \mid f_i \in I, g_i \in J\}$$

と定めると、$I + J$, $I \cap J$, IJ はすべて R のイデアルである。

(2.5) **補題** $f_1, \ldots, f_s \in R$ のとき、

$$\langle f_1, \ldots, f_s \rangle = \{a_1 f_1 + \cdots + a_s f_s \mid a_j \in R\}$$

と定めると $\langle f_1, \ldots, f_s \rangle$ は R のイデアルである。これを、$f_1, \ldots, f_s$ で**生成されるイデアル**と呼び、$f_1, \ldots, f_s$ を $\langle f_1, \ldots, f_s \rangle$ の**生成元** (**生成系**) と呼ぶ。

(2.6) **補題** K を $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ のいずれかとすると、1 変数多項式環 $K[x]$ のイデアルはすべて単項イデアルである。また、$\mathbb{Z}$ のイデアルもすべて単項イデアルである。

(2.7) **例** $\langle x^2-1, x^2-x\rangle \subset K[x]$ に x^3+1 が属するかどうか調べよ。
(解) $I = \langle x^2-1, x^2-x\rangle$ とする。I は単項イデアルだから、その生成元を求める。まず、$x-1 = (x^2-1)-(x^2-x) \in I$ なので、$\langle x-1\rangle \subset I$ である。次に、$x^2-1 = x(x-1)$ かつ $x^2-x = x(x-1)$ だから $x^2-1, x^2-x \in \langle x-1\rangle$ である。よって、$I \subset \langle x-1\rangle$ なので $I = \langle x-1\rangle$ である。すると x^3+1 は ($K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ いずれでも) $x-1$ の倍元ではないので、x^3+1 は I に属さない。

(2.8) **命題** $f_1, \ldots, f_s \in K[x]$ のとき、$f_1, \ldots, f_s$ の最大公約元を f とすると、$\langle f_1, \ldots, f_s\rangle = \langle f\rangle$ である。ただし、最大公約元とは公約元のうち最大次数のものを言う。

Proof. $I \subset \langle f\rangle$ は容易。逆に $f = \sum_i a_i f_i$ と書けることは、互除法を使って帰納的に言える。 □

(2.9) **問題** 次のイデアル I に、与えられた多項式 f が属するかどうか言え。

(1) $I = \langle x^2-1, x^3-1\rangle \subset K[x]$, $f = x^3+1$.
(2) $I = \langle x^2-1, x^2+1\rangle \subset K[x]$, $f = x^3+1$.

(2.10) 例 (多変数多項式環でのイデアル所属問題) 2 変数以上の多項式環のイデアルは単項とは限らない。このため、多項式がイデアルに属するかどうかの判定は難しくなる。

例として、$K[x,y]$ のイデアル $I = \langle x+y, x^2+y^2 \rangle$ に y^3 は属するか調べる。素朴な方針としては、まず y^3 を $x+y$ で「割り算」し、

$$y^3 = p(x+y) + q$$

として、余りの q を x^2+y^2 で「割り算」して、

$$q = r(x^2+y^2)$$

と割り切れたら

$$y^3 = p(x+y) + r(x^2+y^2) \in I$$

と判定する方法がある。しかし、実際にやってみると「割り切れ」ない。

ところが、$f_1 = x+y$, $f_2 = x^2+y^2$ とおくと、$y^3 = -y((x-y)f_1 - f_2)/2 \in I$ であるから、上の判定方法は機能していない。

同様に、下の 2 例でも、f が I に属するかどうか一見わからないが、実際には属している。

(1) $I = \langle x^2+xy+y^2, x^3+y^3 \rangle \subset K[x,y]$, $f = (x+y)^3$

(2) $I = \langle x^2+y, x+y^2 \rangle \subset K[x,y]$, $f = x(x^3+1)$

(2.11) 今後の目的 $R = \mathbb{Q}[x_1, \dots, x_n]$ のとき、

(1) 任意のイデアルの「よい」生成元を求められるか (現時点で $n=1$ なら yes)。

(2) $I \subset R$ と $f \in R$ に対し $f \in I$ かどうか判定できるか (現時点で $n=1$ な

ら yes)。
(3) $f_1, \ldots, f_s \in R$ のとき、連立方程式 $f_1 = 0, \ldots, f_s = 0$ が解けるか (現時点で $s = 1$ なら 4 次方程式までは yes)。

§3　項順序

以下しばらく、K は $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ のいずれか、$R = K[x_1, \ldots, x_n]$ とする。

(3.1)　**多重指数**　n 変数多項式環 R の単項式 $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $(\alpha_j \in \mathbb{Z}_{\geq 0})$ を x^α $(\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n)$ と表す。$\alpha \in (\mathbb{Z}_{\geq 0})^n$ を**多重指数**と呼ぶ。

(3.2)　**項順序**　n 変数多項式環 R の単項式の単項式 x^α $(\alpha \in (\mathbb{Z}_{\geq 0})^n)$ 全体の集合上の順序 $\geq$ が**項順序**であるとは、次の条件 (T1) から (T3) を満たすことを言う。また、単項式全体の集合は $(\mathbb{Z}_{\geq 0})^n$ と同一視できるから、$(\mathbb{Z}_{\geq 0})^n$ 上の順序として条件を書く。

(T1)　$\geq$ は $(\mathbb{Z}_{\geq 0})^n$ 上の**全順序**である。
(T2)　$\alpha \geq \beta$ ならば $\alpha + \gamma \geq \beta + \gamma$.
(T3)　$\geq$ は **整列順序**である。

ここに、全順序とは、どの $\alpha, \beta \in (\mathbb{Z}_{\geq 0})^n$ に対しても、$\alpha \geq \beta$ か $\alpha \leq \beta$ のいずれかが成立し、両方とも成立するのは $\alpha = \beta$ の場合に限り、加えて推移律を満たすことを言う。また、整列順序とは、任意の部分集合に最小元が存在するような (全) 順序のことである。

$\alpha \geq \beta$ かつ $\alpha \neq \beta$ のとき $\alpha > \beta$ と書き、$\geq$ が項順序であると言う代わりに $>$ が項順序であるとも言う。

(3.3) **補題** $>$ を項順序とするとき、$(\mathbb{Z}_{\geq 0})^n$ 内の減少列 $\alpha_1 > \alpha_2 > \cdots > \alpha_k > \cdots$ は有限で止まる。

Proof. (T3) の単なる言い換え。 □

(3.4) **例 (辞書式順序)** $(\mathbb{Z}_{\geq 0})^n$ 上の項順序 $>_{\mathrm{lex}}$ を次で定める: $\alpha, \beta \in (\mathbb{Z}_{\geq 0})^n$ に対して、$\alpha >_{\mathrm{lex}} \beta$ であるとは、α と β の成分を左から比較していくと j 番目で初めて異なるとしたとき、$\alpha_j > \beta_j$ となっていることと定める。

言い換えると、$\alpha - \beta$ の成分を左から見ていき、初めての 0 でない成分が正であるとき $\alpha >_{\mathrm{lex}} \beta$ と定めると言ってもよい。

(3.5) **例 (次数付き辞書式順序)** $(\mathbb{Z}_{\geq 0})^n$ 上の項順序 $>_{\mathrm{glex}}$ を次で定める: $\alpha, \beta \in (\mathbb{Z}_{\geq 0})^n$ に対して、$\alpha >_{\mathrm{glex}} \beta$ であるとは、α の成分の和 $|\alpha|$ が β の成分の和 $|\beta|$ より大きいか、または、$|\alpha| = |\beta|$ かつ $\alpha >_{\mathrm{lex}} \beta$ となっていることと定める。

(3.6) **例 (次数付き逆辞書式順序)** $(\mathbb{Z}_{\geq 0})^n$ 上の項順序 $>_{\mathrm{revlex}}$ を次で定める: $\alpha, \beta \in (\mathbb{Z}_{\geq 0})^n$ に対して、$\alpha >_{\mathrm{revlex}} \beta$ であるとは、$|\alpha| > |\beta|$、または、$|\alpha| = |\beta|$ かつ $\alpha - \beta$ の成分を右から順に見て初めての 0 でない成分が負であることと定める。

以上 3 つの項順序はどれも、1 次式に対して、$x_1 > x_2 > \cdots > x_n$ を満たしている。また、$K[x_1, x_2, x_3]$ の高々 2 次の単項式を、3 つの項順序で大き

い順に並べると次のようになる。$x = x_1, y = x_2, z = x_3$ とおいた。

$>_{\mathrm{lex}}$	x^2	xy	xz	x	y^2	yz	y	z^2	z	1
$>_{\mathrm{glex}}$	x^2	xy	xz	y^2	yz	z^2	x	y	z	1
$>_{\mathrm{revlex}}$	x^2	xy	y^2	xz	yz	z^2	x	y	z	1

(3.7)　**定義 (先頭項、先頭単項式、先頭係数、多重次数)**　$f = \sum_\alpha a_\alpha x^\alpha \in R$ を 0 ではない多項式とし、$>$ を R 上の項順序とする。

(1) $a_\alpha \neq 0$ なる α のうち $>$ に関して最大のものを $\mathrm{multideg}(f) \in (\mathbb{Z}_{\geq 0})^n$ とおき、f の $>$ に関する**多重次数**と呼ぶ。

以下では f の多重次数を β と置く。

(2) $\mathrm{LM}(f) = x^\beta$ と置き、f の $>$ に関する**先頭単項式**と呼ぶ。

(3) $\mathrm{LC}(f) = a_\beta$ と置き、f の $>$ に関する**先頭係数**と呼ぶ。

(4) $\mathrm{LT}(f) = a_\beta x^\beta$ と置き、f の $>$ に関する**先頭項**と呼ぶ。

(3.8)　**問題**　$K[x_1, x_2, x_3]$ に属する次の多項式を、上で定めた 3 つの項順序に関して、それぞれ、項の大きい順に整理せよ。ただし、$x = x_1, y = x_2, z = x_3$ とおいた。

(1) $2x - xy + 3xz - 4y^2$　　(2) $x^2 + xyz + x^2z + y^3 + xy^2$

§4　割り算アルゴリズム

(4.1)　**割り算アルゴリズム (割る式が 1 つ)**　$f \in R$ を $g \in R$ で割り算するとは、次の手順を行うことである。

(1) $\mathrm{LT}(f)$ が $\mathrm{LT}(g)$ で割り切れるならば、商として $\mathrm{LT}(f)/\mathrm{LT}(g)$ を立てて割り算を 1 段階実行し、$f - g\,\mathrm{LT}(f)/\mathrm{LT}(g)$ を新たな f として割り算

を続行する。

(2) $\mathrm{LT}(f)$ が $\mathrm{LT}(g)$ で割り切れないならば、$\mathrm{LT}(f)$ は余りに加算し、f から $\mathrm{LT}(f)$ を除いたものを新たな f として割り算を続行する。

(3) f が 0 になるまで繰り返す。

(4.2) **例** 辞書式順序を用いて、$(x^2y^3+x^2)\div(xy+y^3)$ を計算する。

$$
\begin{array}{r|ll}
 & xy^2 \qquad -y^4 & \\ \hline
xy+y^3 & x^2y^3+x^2 & \\
 & x^2y^3+xy^5 & \\ \cline{2-2}
 & -xy^5+x^2 & \to x^2 \\ \cline{2-2}
 & -xy^5 & \\
 & -xy^5-y^7 & \\ \cline{2-2}
 & y^7 & \to y^7 \\ \cline{2-2}
 & 0 &
\end{array}
$$

以上より、商が xy^2-y^4 で、余りが x^2+y^7 である。

(4.3) **注意** $f\in R$ を $g\in R$ で割ったとき $f=ag+r$ とすると、$\mathrm{multideg}(f)\geq\mathrm{multideg}(ag)$ である。また、余り r のどの項も、$\mathrm{LT}(g)$ で割り切れない。

(4.4) **例** (4.2) を、次数付き辞書式順序で計算してみると、以下のように商と余りが変わる。

$$
\begin{array}{r|ll}
 & x^2 & \\ \hline
xy+y^3 & x^2y^3+x^2 & \\
 & x^2y^3+x^3y & \\ \cline{2-2}
 & -x^3y+x^2 & \to -x^3y+x^2 \\ \cline{2-2}
 & 0 &
\end{array}
$$

(4.5) 割り算アルゴリズム (割る式が複数) $f \in R$ を $g_1, \ldots, g_s \in R$ で割り算するとは、次の手順を行うことである。

(1) $\mathrm{LT}(f)$ が $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$ で割り切れるか順に試し、最初に割り切れたものを $\mathrm{LT}(g_i)$ とすると、商として $\mathrm{LT}(f)/\mathrm{LT}(g_i)$ を立てて割り算を 1 段階実行し、$f - g_i \,\mathrm{LT}(f)/\mathrm{LT}(g_i)$ を新たな f として割り算を続行する。
(2) $\mathrm{LT}(f)$ がどの $\mathrm{LT}(g_i)$ で割り切れないならば、$\mathrm{LT}(f)$ は余りに加算し、f から $\mathrm{LT}(f)$ を除いたものを新たな f として割り算を続行する。
(3) f が 0 になるまで繰り返す。

(4.6) 例 次の例はともに辞書式順序で割り算しているが、割る式の並べる順序を変えただけで結果が異なっている。

$$
\begin{array}{ll}
 & 1:\quad y^3 \\
 & 2:\qquad\quad 1 \\
\hline
\left.\begin{array}{l} x^2+y \\ xy^2+y \end{array}\right) & x^2y^3 + xy^2 \\
 & \underline{y^4 + x^2y^3} \\
 & xy^2 - y^4 \\
 & \underline{xy^2 + y} \\
 & \underline{-y^4 - y} \quad \to -y^4 - y \\
 & 0
\end{array}
$$

$$
\begin{array}{ll}
 & 1:\quad xy \\
 & 2: \\
\hline
\left.\begin{array}{l} xy^2+y \\ x^2+y \end{array}\right) & x^2y^3 + xy^2 \\
 & \underline{xy^2 + x^2y^3} \\
 & 0
\end{array}
$$

(4.7)　**割り算の恒等式**　$f \in R$ を $g_1, \ldots, g_s \in R$ で割ったとき、余りを $r \in R$、g_i に対応する商を $a_i \in R$ とすると次の式が成り立つ。

$$f = a_1 g_1 + \cdots + a_s g_s + r$$
$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i g_i) \qquad (1 \leq i \leq s)$$

また、r のすべての項は、どの $\mathrm{LT}(g_i)$ でも割り切れない。

(4.8)　**命題**　$f \in R$ を $g_1, \ldots, g_s \in R$ で割ったとき、余りがゼロならば $f \in \langle g_1, \ldots, g_s \rangle$ である。ただし、逆は一般には成り立たない。

(4.9)　**問題**　辞書式順序、次数付き辞書式順序、次数付き逆辞書式順序で、次の f を g_1, g_2 で割り算せよ。
(1) $f = x^2y^2z + x^2z^2$, $g_1 = xz + y^2$, $g_2 = z^2 - x$
(2) $f = x^2y^2z - y^5$, $g_1 = xyz - y^3$, $g_2 = xy - z^3$

§5　ディクソンの補題

以下でもしばらく $R = K[x_1, \ldots, x_n]$ と置く。

(5.1)　**定義（単項式イデアル）**　イデアル $I \subset R$ が**単項式イデアル**であるとは、(必ずしも有限個とは限らない) 単項式で I が生成されるときを言う。

(5.2) 補題 A を多重指数の集合とし、$I = \langle x^\alpha \mid \alpha \in A \rangle$ を R の単項式イデアルとすると、$x^\beta \in I$ であることとある $\alpha \in A$ に対して x^α が x^β を割り切ることは同値である。

Proof. 一方は容易 (だが宿題か)。
$x^\beta \in I$ のとき、$x^\beta = \sum h_\alpha x^\alpha$ と書けるが、右辺に現れる単項式はすべて、ある x^α の倍元だから右辺もそうであり OK. □

(5.3) 補題 (1) $I \subset R$ を単項式イデアルとする。$f \in I$ であるための必要十分条件は、f に現れる単項式はすべて I に属することである。
(2) $I, J \subset R$ を 2 つの単項式イデアルとする。I の元に現れる単項式全体の集合が、J の元に現れる単項式全体の集合と一致するならば、$I = J$ である。

Proof. (1) 十分性は自明、必要性は上の補題の証明と同様 (宿題)。
(2) (1) を用いよ。 □

(5.4) 定理 (ディクソンの補題) A を多重指数の集合とし、$I = \langle x^\alpha \mid \alpha \in A \rangle$ を R の単項式イデアルとすると、この生成元のある有限部分集合で I は生成される。つまり、A の有限部分集合 A' があって、I は有限個の単項式 x^α $(\alpha \in A')$ で生成される。

Proof. n の帰納法。$n = 1$ ではよいから、n まで OK と仮定する。$R_{n+1} = K[x_1, \ldots, x_n, y]$ とし、単項式を $x^\alpha y^m$ と表し、$I = \langle x^\alpha y^m \mid (\alpha, m) \in A \rangle$ と書く。

まず、R のイデアル J を次のように構成し、帰納法の仮定より有限個の生成元をとる:

$$J := \langle x^\alpha \mid (\alpha, m) \in A \rangle = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle.$$

各 i に対し、$(\alpha(i), m_i) \in A$ だが、M を m_i の最大値とする。次に $0 \leq k \leq M-1$ に対し、R のイデアル J_k を次のように構成し、帰納法の仮定より有限個の生成元をとる:

$$J_k := \langle x^\alpha \mid (\alpha, k) \in A \rangle = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle.$$

このとき I は次の I に属する単項式

$$x^{\alpha(i)} y^M \quad (1 \leq i \leq s), \qquad x^{\alpha_k(i)} y^k \quad (0 \leq k \leq M-1,\ 1 \leq i \leq s_k).$$

で生成される。なぜなら、I の単項式 $x^\alpha y^p$ があったとき、$p \geq M$ ならば J の構成より、ある $x^{\alpha(i)} y^M$ で割り切れ、$p < M$ ならば J_k の構成より、ある $x^{\alpha_q(i)} y^q$ $(q \leq p)$ で割り切れる。

さらに、上の各生成元たちは I に属するから、ある $x^\alpha y^m$ $((\alpha, m) \in A)$ で割り切れる。その生成元をこの $x^\alpha y^m$ に交換しても、生成するイデアルは小さくならないから、やはり I に等しい。こうして得られた生成元の集合は A の有限部分集合である。

□

(5.5) **命題** $(\mathbb{Z}_{\geq 0})^n$ 上の順序 $>$ が、(3.2) の (T1) と (T2) を満たすとする。このとき、$>$ が整列順序であることと、すべての $\alpha \in (\mathbb{Z}_{\geq 0})^n$ が $\alpha \geq 0$ であることは同値である。

Proof. 整列の時 $(\mathbb{Z}_{\geq 0})^n$ の最小元が $\alpha < 0$ ならば、$2\alpha < \alpha$ と、α の最小性に反する。

逆。$A \subset (\mathbb{Z}_{\geq 0})^n$ とし、$\langle A \rangle$ の有限生成系の最小元を α とする。$\alpha = \beta + \gamma$ のとき、$\gamma \geq 0$ より、$\alpha \geq \beta$ なので、α が A の最小元だとわかる。 $\square$

(5.6) **問題** R のイデアル I が次の性質を満たすならば、I は単項式イデアルであることを証明せよ: 「$f \in I$ ならば f に現れる単項式はすべて I に属する」

(5.7) **問題** R の単項式イデアル $I = \langle x^\alpha \mid \alpha \in A \rangle$ があり、$S \subset (\mathbb{Z}_{\geq 0})^n$ を、I の元に現れる単項式の多重指数すべての集合とする。このとき、すべての項順序 $>$ に対して、$>$ に関する S の最小元は A に属することを証明せよ。

(5.8) **命題** I を R の単項式イデアルとすると、ディクソンの補題より有限個の単項式で生成されるが、**極小**の生成系が唯一存在する。ただし、生成系が極小であるとは、生成系のどの 2 つの単項式 x^α, x^β の間にも割り切る関係がないことを言う。

Proof. 割り切られるのを省いていけば極小生成系の存在は OK. $\{x^\alpha\}$ も $\{x^\beta\}$ も極小とすると、どの x^α もある x^β で割り切れ、それはある $x^{\alpha'}$ で割り切れるが、極小性から $\alpha = \alpha'$、よって $\alpha = \beta$ だから一意。 $\square$

§6 先頭項イデアル

以下でもしばらく $R = K[x_1, \ldots, x_n]$ と置く。

(6.1) 定義 (先頭項イデアル) R 上の項順序をひとつ決めておく。I を R の 0 ではない (単項式イデアルとは限らない) イデアルとするとき、単項式の集合 $\mathrm{LT}(I)$ と単項式イデアル $\langle \mathrm{LT}(I) \rangle$ を

$$\mathrm{LT}(I) = \{f \text{ の先頭項} \mid f \in I,\ f \neq 0\},$$
$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(I) \text{ で生成される単項式イデアル } \rangle$$

で定める。$\langle \mathrm{LT}(I) \rangle$ を I の**先頭項イデアル**と呼ぶ。

(6.2) 注意 $I = \langle f_1, \ldots, f_s \rangle$ のとき、常に $\langle \mathrm{LT}(I) \rangle \supset \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ ではあるが、等号は必ずしも成立しない。

例えば、辞書式順序を考えたとき、$I = \langle x + y, x^2 + y^2 \rangle \subset K[x, y]$ の各生成元の先頭項で生成されるイデアルは、$\langle x, x^2 \rangle = \langle x \rangle$ である。ところが、(2.10) により $y^3 \in I$ であったから、$\langle \mathrm{LT}(I) \rangle \supsetneq (x)$ である。

しかし、I が単項式イデアルならば、$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ である。

§7 グレブナ基底

(7.1) 定義 (グレブナ基底) I を R の 0 ではない (単項式イデアルとは限らない) イデアルとし、項順序を固定する。I の有限部分集合 $G = \{g_1, \ldots, g_s\}$ が I の**グレブナ基底**であるとは、$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$ であるときを言う。

ひとつグレブナ基底があれば、それに I の元を有限個追加してもグレブナ基底である。特に、グレブナ基底は一意的ではない。

(7.2) 例 (1) 単項式イデアルは、ディクソンの補題により有限の生成系を持つが、それはグレブナ基底である。

(2) 単項イデアルはその唯一の生成元がグレブナ基底をなす。

(7.3) 命題 R 上の項順序を固定する。I を R のイデアルとすると、I のグレブナ基底は存在する。

Proof. $\langle \mathrm{LT}(I) \rangle$ は $\mathrm{LT}(I)$ で生成される単項式イデアルだから、生成系から有限個を選べる。 □

(7.4) 定理 R 上の項順序を固定する。I を R のイデアルとし、G を I のグレブナ基底とする。このとき、G は I の生成系である。

Proof. $I \supset \langle G \rangle$ は OK. $f \in I$ を G で割り、$\sum_i a_i g_i + r$ と書く。$r \neq 0$ なら各項はどの $\mathrm{LT}(g_i)$ でも割れないが、$r \in I$ だからある $\mathrm{LT}(g_i)$ で割れる。よって $r = 0$. □

(7.5) 命題 (割り算の余りの一意性) R 上の項順序を固定する。I を R の 0 ではないイデアルとし、$G = \{g_1, \ldots, g_s\}$ を I のグレブナ基底とする。このとき次が成立する。

(1) $f \in R$ に対して、次の 2 条件を見たす $r \in R$ がただ 1 つ存在する。

(i) r のすべての項は、どの $\mathrm{LT}(g_i)$ $(i = 1, \ldots, s)$ でも割り切れない。

(ii) $f = g + r$ となる $g \in I$ が存在する。

(2) グレブナ基底 G による割り算の余りは、G の元の順番や、グレブナ基底のとり方によらない。

Proof. (1) 存在は割り算の余り。一意性は、$g+r=h+q$ ならば、$r-q$ の各項がどの $\mathrm{LT}(g_i)$ でも割れないのに、$\mathrm{LT}(r-q)=\mathrm{LT}(h-g)\in(\mathrm{LT}(I))=(\mathrm{LT}(G))$ は、ある $\mathrm{LT}(g_i)$ でも割れるので $r-q=0$.
(2) (i) は、r のすべての項が $\mathrm{LT}(I)$ に属さない、と書き換わり、G に依存しない。 □

(7.6) **定理 (イデアル所属問題)** R 上の項順序を固定し、I を R の 0 ではないイデアルとする。$f\in I$ であるための必要十分条件は、I のあるグレブナ基底 G で f を割った余りが 0 となることである。

Proof. $f\in I$ のとき、$f=f+0$ が条件を満たすので、一意な余りは 0。 □

§8 ヒルベルトの基底定理

以下でもしばらく $R=K[x_1,\dots,x_n]$ と置く。次の定理は、(7.3) と (7.4) から明らかである。

(8.1) **定理 (ヒルベルトの基底定理)** I を R のイデアルとしたとき、I の生成系として I の有限部分集合がとれる。

(8.2) **命題 (昇鎖条件)** R の中のイデアルの列

$$I_1\subset I_2\subset I_3\subset\cdots$$

があったとき、ある正整数 N があって、

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

と途中からすべて同じになる。

Proof. I_n の帰納極限 I_∞ はイデアル I_n を含むイデアルである。I の GB$\{g_1, \ldots, g_s\}$ は I_N に $(N \gg 0)$ 含まれるが、その先は安定する。 □

§9 ブッフベルガーの判定条件

以下でもしばらく $R = K[x_1, \ldots, x_n]$ と置く。

(9.1) 定義 (S 多項式) (1) 2 つの単項式 x^α, x^β の**最小公倍元**とは、$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$ のとき、$\gamma = (\gamma_1, \ldots, \gamma_n)$ を $\gamma_i = \max\{\alpha_i, \beta_i\}$ で定めたときの x^γ のことである。

(2) $f, g \in R$ の **S 多項式** $S(f, g)$ を、x^γ を $\mathrm{LM}(f)$ と $\mathrm{LM}(g)$ の最小公倍元としたとき、

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$

で定義する。

例えば、$x > y$ なる辞書式順序を考えるとき、

$$S(x^2 + y^2, xy) = y(x^2 + y^2) - x \cdot xy = y^3$$

である。

(9.2) 補題 $f_1, \ldots, f_s \in R$ が、すべて同じ多重次数 $\delta \in (\mathbb{Z}_{\geq 0})^n$ を持つとする。このとき次が成立する。

(1) $S(f_j, f_k)$ の多重次数は δ より真に小さい。
(2) ある $c_i \in K$ に対して、$c_1 f_1 + \cdots + c_s f_s$ の多重次数が δ より真に小さいならば、$c_1 f_1 + \cdots + c_s f_s$ は、$S(f_j, f_k)$ $(1 \le j, k \le s)$ の K 係数の 1 次結合である。

Proof. (1) $p_j := f_j \ / \mathrm{LC}(f_j)$ とおく。$S(f_j, f_k) = p_j - p_k$ は x^δ の項がない。
(2) $b_i := c_i \, \mathrm{LC}\ (f_i)$. $\sum_i b_i$ は条件より 0. $\sum_i c_i f_i = \sum_i b_i p_i = b_1(p_1 - p_2) + \cdots + (b_1 + \cdots + b_{s-1})(p_{s-2} - p_{s-1}) + (b_1 + \cdots + b_s) p_s$. この最後の項は 0 だから OK. □

(9.3) 補題 $f, g \in R$ であり、$\mathrm{multideg}\, f = \alpha$, $\mathrm{multideg}\, g = \beta$ とする。x^γ を x^α と x^β の最小公倍元とする。x^δ が x^γ で割り切れるとき、

$$S(x^{\delta-\alpha} f, x^{\delta-\beta} g) = x^{\delta-\gamma} S(f, g)$$

である。

Proof. S 多項式の定義通りに計算すればよい。 □

(9.4) 定理（ブッフベルガーの判定条件） R 上の項順序を固定し、$I = \langle g_1, \ldots, g_s \rangle$ を R の 0 ではないイデアルとする。$G = \{g_1, \ldots, g_s\}$ とおくとき、G が I のグレブナ基底であるための必要十分条件は、任意の異なる i, j に対して $S(g_i, g_j)$ を G で割った余りが 0 であることである。

Proof. [十分性] G がグレブナ基底とする。$S(g_i, g_j) \in I$ だから、(7.6) より、$S(g_i, g_j)$ を G で割った余りは 0 である。

[必要性] 任意の $S(g_i, g_j)$ を G で割った余りが 0 であるとする。$0 \neq f \in I$ をとり、$\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$ を示せばよい。$f \in \langle g_1, \dots, g_s \rangle$ だから、$f = \sum_i h_i g_i$ $(h_i \in R)$ と書けるが、$\mathrm{multideg}(f) \leq \max_i \{\mathrm{multideg}(h_i g_i)\}$ である。もし等号が成立するならば、ある i に対して $\mathrm{LM}(f) = \mathrm{LM}(h_i g_i)$ となるので、$\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$ が言える。等号が不成立と仮定して以下で矛盾を導く。

$f = \sum_i h_i g_i$ の書き方は一意ではないが、項順序が整列順序であるので、そのような書き方のうちから多重次数 $\max_i \{\mathrm{multideg}(h_i g_i)\}$ が最小になるように書き方をとっておく。この最小にとった多重次数をを δ とおく。

$$
\begin{aligned}
f &= \sum_i h_i g_i \\
&= \sum_{\mathrm{multideg}\, h_i g_i = \delta} \mathrm{LT}(h_i) g_i + \sum_{=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{<\delta} h_i g_i. \qquad (*)
\end{aligned}
$$

この第 1 項は、多重指数が δ より小さいので次のように計算できる。

$$
\begin{aligned}
(\text{第 1 項}) &\overset{(9.2)(2)}{=} \sum_{j,k} c_{jk} S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k) \qquad (c_{jk} \in K) \\
&\overset{(9.3)}{=} \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) \qquad (x^{\gamma_{jk}} = LCM(\mathrm{LM}(g_j), \mathrm{LM}(g_k))) \\
&\overset{\text{仮定}}{=} \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} \sum_i a_{ijk} g_i \\
&= \sum_i \left(\sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} a_{ijk} \right) g_i.
\end{aligned}
$$

ここで、(4.7) より、$\mathrm{multideg}\, a_{ijk} g_i \leq \mathrm{multideg}\, S(g_j, g_k)$ だから、S 多項式の定義よりわかる $\mathrm{multideg}\, S(g_j, g_k) < \gamma_{jk}$ と合わせると、上の最後の式のかっこの中は多重次数が δ より小さい項しか現れない。これを (*) に代入すると、$f = \sum_i (\delta \text{ より低次の式}) g_i$ となり、δ のとり方に矛盾する。 □

(9.5) **例** 辞書式順序を考える。
(1) $g_1 = x + y$, $g_2 = x^2 + y^2$ とし、$I = \langle g_1, g_2 \rangle \subset K[x, y]$ とする。$S(g_1, g_2) = xy - y^2$ であり、これを g_1, g_2 で割ると余りは $-2y^2$ になる。$-2y^2$ は g_1, g_2 で割り切れないから、(9.4) より g_1, g_2 はグレブナ基底ではない。

(2) $h_1 = x + y$, $h_2 = y^2$ とすると、$\langle h_1, h_2 \rangle = \langle x + y, x^2 + y^2 \rangle$ である。$S(h_1, h_2) = y^3$ は h_1, h_2 で割り切れるから、(9.4) より h_1, h_2 はグレブナ基底である。

(9.6) **問題** 辞書式順序を考える。$g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$, $g_3 = x - yz^4$ はグレブナ基底ではないことを示せ。

§10 ブッフベルガーのアルゴリズム

(10.1) **定理 (ブッフベルガーのアルゴリズム)** R 上の項順序を固定し、$I = \langle f_1, \ldots, f_s \rangle$ を R の 0 ではないイデアルとする。次の手順が終了したときに得られる G は I のグレブナ基底である。

> $G := \{f_1, \ldots, f_s\}$
> REPEAT
>> 異なる $p, q \in G$ の組すべてに対して、$S(p, q)$ を G で割った余りが 0 でないならば、その余りを G に追加する。
>
> UNTIL G に何も追加されなかった (ならば終了)

Proof. アルゴリズムの最初に $\langle G \rangle = I$ であり、さらに、繰り返しの各段階

で G に追加される元は、その時点での $\langle G\rangle$ の元だから、常に $\langle G\rangle = I$ である。また、アルゴリズムが停止したならば、(9.4) より G はグレブナ基底である。

あとは、アルゴリズムが停止することを言えばよい。繰り返しのある段階で、G に属さない元 r が G に追加されたとすると、割り算の性質より、$\mathrm{LT}(r)$ は $\mathrm{LT}(G)$ のどの元でも割り切れない。よって、$\langle \mathrm{LT}(G)\rangle \subsetneq \langle \mathrm{LT}(G \cup \{r\})\rangle$ である。よって、アルゴリズムが動いているうちは、$\langle \mathrm{LT}(G)\rangle$ たちがイデアルの真の上昇列をなすため、昇鎖条件 (8.2) よりアルゴリズムは停止する。 $\square$

(10.2) **問題** 辞書式順序を考え、イデアルのグレブナ基底を (1 つ) 求めよ。

(1) $I = \langle x + y, x^2 + y^2\rangle$ (2) $I = \langle xy, x^2 + y^2\rangle$

(10.3) **定義 (極小グレブナ基底)** 次の 2 条件を満たすグレブナ基底を、**極小グレブナ基底**と呼ぶ。

(i) すべての $p \in G$ の先頭係数は 1 である。
(ii) すべての $p \in G$ に対して、$\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$ である。

あるグレブナ基底が (ii) の条件を満たさないならば、その p を取り去っても依然としてグレブナ基底である。こうして取り去っていくと、最後には極小グレブナ基底にたどりつくから、極小グレブナ基底は存在する。

しかし、一般には極小グレブナ基底は一意ではない。

(10.4) **問題** 辞書式順序を考え、次の問に答えよ。

(1) $I = \langle x+y, x^2+y^2 \rangle$ の極小グレブナ基底を (1 つ) 求めよ。また、x^2y は I に属するか答えよ。

(2) $I = \langle xy, x^2+y^2 \rangle$ の極小グレブナ基底を (1 つ) 求めよ。また、y^3 は I に属するか答えよ。

§11 簡約グレブナ基底

(11.1) **定義 (簡約グレブナ基底)** 次の 2 条件を満たすグレブナ基底を、**簡約グレブナ基底**と呼ぶ。

(i) すべての $p \in G$ の先頭係数は 1 である。

(ii) すべての $p \in G$ に対して、p のどの単項式も $\langle \mathrm{LT}(G - \{p\}) \rangle$ に属さない。

特に、簡約グレブナ基底は極小グレブナ基底である。

(11.2) **例** 辞書式順序を考える。$\langle x+y, x^2+y^2, y^2 \rangle$ は極小グレブナ基底ではなく、従って簡約グレブナ基底でもないが、$\langle x+y, y^2 \rangle$ は簡約グレブナ基底である。

(11.3) **命題** 項順序を固定する。R の 0 ではないイデアルは、一意的な簡約グレブナ基底を持つ。

Proof. [存在] 極小な $G = \{g_1, .., g_s\}$ をとる。$g_1' = \overline{g_1}^{G-\{g_1\}}$, $G_1 = \{g_1', g_2, .., g_s\}$, $g_2' = \overline{g_2}^{G_1-\{g_2\}}$, $G_2 = \{g_1', g_2', .., g_s\}$, と G_s まで定める。極小性より $\mathrm{LT}(g_1) = \mathrm{LT}(g_1')$ であり、その後も、$\mathrm{LT}(g_i) = \mathrm{LT}(g_i')$ であるか

ら、G_i はすべて極小グレブナ基底である。$\mathrm{LT}(G_i) = \mathrm{LT}(G_s)$ と g_i' が余りなことより G_s は簡約グレブナ基底の条件 (ii) を満たす。

[一意性] G も G' も極小の時、単項式イデアルの極小生成系と同様に、$\mathrm{LT}(G) = \mathrm{LT}(G')$ である。$\mathrm{LT}(g) = \mathrm{LT}(g')$ とすると、$\overline{g - g'}^G = 0$ である。g と g' の先頭項は相殺するが、他の項は $\mathrm{LT}(G) = \mathrm{LT}(G')$ で割れないから $\overline{g - g'}^G = g - g'$ である。よって、$g = g'$. □

(11.4) **例題** 次数付き辞書式順序を用いて、次のイデアルの簡約グレブナ基底を求めよ。

(1) $I = \langle y^3 + x^2, y^3 + xy \rangle$

(2) $I = \langle y^2 + xy, x^3 + xy \rangle$

§12 消去定理

(12.1) **イデアルと連立方程式** 連立方程式

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

を考える。$(x, y, z) = (a, b, c)$ がこの連立方程式の解だとすると、$f_1(a, b, c) = f_2(a, b, c) = f_3(a, b, c) = 0$ である。したがって、イデアル $\langle f_1, f_2, f_3 \rangle$ の元 g も $g(a, b, c) = 0$ を満たすから、$g = 0$ を連立方程式に追加しても、連立方程式の解は変わらない。逆に、加減法[*1]を行って新たな式を得たとき、その式はイデアル $\langle f_1, f_2, f_3 \rangle$ に属する。つまり、連立方程式を加減法で解くことは、イデアル $\langle f_1, f_2, f_3 \rangle$ に属する簡単な式を探すこと

[*1] いわゆる消去法による解法も、加減法に含めることができる。

に相当し、例えば、1 変数しか含まないような簡単な式が見つかればその 1 変数については、解が確定する。

(12.2) **定義 (消去イデアル)** R のイデアル $I = \langle f_1, f_2, \ldots, f_s \rangle$ に対して、l 次の**消去イデアル**を

$$I_l = I \cap K[x_{l+1}, x_{l+2}, \ldots, x_n]$$

で定める。つまり、I に属する多項式のうち、最初の l 変数を含まないもの全体のなす集合である。これは、$K[x_{l+1}, x_{l+2}, \ldots, x_n]$ のイデアルである。また、$I_0 = I$ である。

(12.3) **定理 (消去定理)** R のイデアル I の辞書式順序に関するグレブナ基底を $G = \{g_1, g_2, \ldots, g_s\}$ とすると、

$$G_l = G \cap K[x_{l+1}, x_{l+2}, \ldots, x_n]$$

は、l 次の消去イデアル I_l のグレブナ基底 (特に生成系) である。

Proof. 証明はまだ書いていない。 □

(12.4) **例** 先の連立方程式

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

を考える。$I = \langle f_1, f_2, f_3 \rangle$ の辞書式順序に関する簡約グレブナ基底は、

$$
\begin{aligned}
G &= \{g_1, g_2, g_3, g_4\}, \\
g_1 &= z^4 - 3z^2 + 2 = (z-1)(z+1)(z^2-2), \\
g_2 &= yz^2 - y = y(z-1)(z+1), \\
g_3 &= y^3 + z^3 - 2z = y^3 + z(z^2-2) \\
g_4 &= x - y^2 z
\end{aligned}
$$

である。従って、消去イデアルは、

$$I_1 = \langle g_1, g_2, g_3 \rangle, \quad I_2 = \langle g_1 \rangle$$

である。

$g_1 = 0$ より、$z = \pm 1, \pm\sqrt{2}$ がわかる。まず、$z = \pm\sqrt{2}$ ならば、$g_3 = 0$ より $y = 0$、さらに $g_4 = 0$ より $x = 0$ となり、解 $(x, y, z) = (0, 0, \pm\sqrt{2})$ を得る。次に、$z = \pm 1$ ならば、$g_3 = 0$ より、$y^3 = \pm 1$ となり a を複素数の範囲での 1 の 3 乗根 (3 つある) とすると $y = \pm a$ となり、$g_4 = 0$ より、$x = -a^2$ となるから、解 $(x, y, z) = (\pm a^2, \pm a, \pm 1)$ を得る。

§13 拡張定理

(13.1) **定義 (部分解)** 上の例にように方程式を解く過程での、$z = \pm 1, \pm\sqrt{2}$ だとか、$(y, z) = (\pm 1, \pm 1)$ のような、消去イデアルに対応する連立方程式の解、つまり、後ろからいくつか変数のみで与えられる解を**部分解**と呼ぶ。

上の例では、どの部分解も、すべての変数で与えられる解に拡張できたが、一般にはそうではない。

(13.2) **定理 (拡張定理)** この定理では $K = \mathbb{C}$ とする。$R = \mathbb{C}[x_1, x_2, \ldots, x_n]$ のイデアル $I = \langle f_1, f_2, \ldots, f_s \rangle$ の 1 次の消去イデアルを I_1 とする。各 f_i を x_1 の降冪の順で整理して、

$$f_i = g_i(x_2, \ldots, x_n)x_1^{m_i} + (x_1 \text{ に関して } m_i \text{ 次未満の項})$$

と書く。ただし、$g_i \in \mathbb{C}[x_2, \ldots, x_n]$ は 0 ではない多項式とする。部分解 $(x_2, \ldots, x_n) = (a_2, \ldots, a_n)$ があるとき、ある g_i に対して、$g(a_2, \ldots, a_n) \neq 0$ ならば、この部分解は、解 $(x_1, x_2, \ldots, x_n) = (a_1, a_2, \ldots, a_n)$ に拡張できる。

(13.3) **例** 消去イデアルを用いて連立方程式を解くときに、部分解が拡張できない例を見る。連立方程式

$$\begin{cases} f = xy - yz + 1 = 0 \\ g = xz = 0 \end{cases}$$

を考えると、イデアル $I = \langle f, g \rangle$ の辞書式順序でのグレブナ基底は、

$$G = \{f, g, h\}, \qquad h = yz^2 - z = z(yz - 1)$$

であるから、消去イデアルは、

$$I_1 = \langle h \rangle, \qquad I_2 = \langle 0 \rangle$$

である。方程式 $h = 0$ より、部分解 $(y, z) = (t, 0), (u, u^{-1})$ ($t \in \mathbb{C}$, $u \in \mathbb{C}$, $u \neq 0$) を得る。拡張定理より、$(y, z) = (0, 0)$ 以外の部分解は、元の連立方程式の解に拡張できることがわかる。

実際、$t \neq 0$ ならば、部分解 $(y, z) = (t, 0)$ より、解 $(x, y, z) = (-t^{-1}, t, 0)$ を得るし、部分解 $(y, z) = (u, u^{-1})$ より、解 $(x, y, z) = (0, u, u^{-1})$ を得る。*2

*2 もちろん、この程度の連立方程式ならば手で解いた方がずっと速い。

§14 計算機への応用

(14.1) **幾何ソフトウェアへの応用** GC, GRAPES, Cinderella, GeoGebra に代表される幾何ソフトウェアでは、直線や曲線を描画したり、交点を求めたりできる。交点の座標は連立方程式で求められるが、計算機内部では、有効数字 16 桁程度の、つまり誤差を含むような数値で近似的に方程式を解くのがかつては普通であった。最近では、場合によっては有理数を用いて誤差なく計算することもある。

GeoGebra などでは、描画によって生じたある点が直線の上にあるかどうかを判定する機能もある。例えば、三角形の中線を 2 つ描画し、その交点 G、つまり重心を描画したとする。このとき、残る 3 つ目の中線 m を描画して、その上に点 G があるかどうかを判定することができる。誤差のない計算ならば、どんな三角形を描いたとしても、m 上に G があると判定される。

さらに、上にあげたような幾何ソフトウェアでは、三角形の頂点を自由に動かすことができる。例えば GeoGebra では、頂点を自由に動かしても、直線上に点が載っているかどうかまで判定してくれることがある。つまり、三角形は 1 つしか描画していないが、それを一般の三角形とみた時も、

常に、点 G は線分 m 上にある

というような判定をしてくれる。

この機能にグレブナ基底が活用されているが、それを以下で見てみる。多変数多項式環のイデアルに、ある多項式が属するかどうかは、グレブナ基底が発見されるまでは計算機で計算することは簡単ではなかったが、グレブナ基底を用いることで効率的に計算が可能になったことが背景にある。

(14.2) 幾何ソフトウェアとグレブナ基底 グレブナ基底を用いて、3 中線が 1 点で交わることの判定の原理を説明する。三角形の 3 頂点 A(x_1, y_1), B(x_2, y_2), C(x_3, y_3) があったとする。M を B と C の中点とすると、直線 AM の方程式は、

$$(2y_1 - y_2 - y_3)x - (2x_1 - x_2 - x_3)y - y_1(x_2 + x_3) + x_1(y_2 + y_3) = 0$$

同様に残り 2 つの中線は、

$$(2y_2 - y_3 - y_1)x - (2x_2 - x_3 - x_1)y - y_2(x_3 + x_1) + x_2(y_3 + y_1) = 0$$
$$(2y_3 - y_1 - y_2)x - (2x_3 - x_1 - x_2)y - y_3(x_1 + x_1) + x_3(y_1 + y_2) = 0$$

これらの左辺を順に f_1, f_2, f_3 とする。

まず、$I = \langle f_1, f_2 \rangle$ と定める。図形としては、2 つの中線の交点の座標を表す。そして、f_3 が I に所属するかどうかをグレブナ基底を用いて判定し、所属していれば、3 点 A, B, C の座標によらず 3 中線は 1 点で交わるということが言える。