

## 2011年度 前期 代数学特論 III

更新日時 2011-08-07 16:38:26 担当 和地 輝仁

### 目次

1 シラバス抜粋	1
2 授業のノート	2
§1 多項式環	2
§2 項順序と割り算アルゴリズム	3
§3 ディクソンの補題	6
§4 グレブナ基底	7
§5 ヒルベルトの基底定理	8
§6 ブッフベルガーのアルゴリズム	8
§7 消去理論	10
イデアルメンバシップの問題追加、連立方程式の話を追加	

## 1 シラバス抜粋

### 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. 1変数多項式環   | 9. ヒルベルトの基底定理      |
| 2. 多項式の除算    | 10. ブッフベルガーのアルゴリズム |
| 3. 多変数多項式環   | 11. イデアル所属問題       |
| 4. イデアル      | 12. 消去法            |
| 5. 項順序       | 13. 連立方程式          |
| 6. イニシャルイデアル | 14. 計算機への応用        |
| 7. ディクソンの補題  | 15. 期末試験           |
| 8. グレブナ基底    |                    |

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)  $\{a + b\sqrt{2}; a, b \text{ は整数}\}$  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

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

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  $\deg f$  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  $R[X_1, X_2, \dots, X_n]$  も定める。

(1.5) 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。

- (1)  $0 \in I$
- (2)  $f, g \in I$  ならば  $f + g \in I$
- (3)  $a \in R, f \in I$  ならば  $af \in I$

以下しばらく  $R$  を環とする。

(1.6) 例 イデアルの例をいくつかあげる。

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

(1.7) 補題 (単項イデアル)  $f \in R$  のとき、

$$(f) = Rf = \{af \mid a \in R\}$$

と定めると、 $(f)$  は  $R$  のイデアルになる。 $(f)$  を  $f$  で生成される単項イデアルと呼び、 $f$  を  $(f)$  の生成元と呼ぶ。

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

$$I + J = \{f + g \mid f \in I, g \in J\},$$

$$IJ = \left\{ \sum_{\text{有限和}} f_i g_i \mid f_i \in I, g_i \in J \right\}$$

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

(1.9) 補題  $f_1, \dots, f_s \in R$  のとき、

$$(f_1, \dots, f_s) = \{a_1 f_1 + \dots + a_s f_s \mid a_j \in R\}$$

と定めると  $(f_1, \dots, f_s)$  は  $R$  のイデアルである。これを、 $f_1, \dots, f_s$  で生成されるイデアルと呼び、 $f_1, \dots, f_s$  を  $(f_1, \dots, f_s)$  の生成元 (生成系) と呼ぶ。

(1.10) 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。

(1.11) 例  $(x^2 - 1, x^2 - x) \subset K[x]$  に  $x^3 + 1$  が属するかどうか調べよ。

(解)  $I = (x^2 - 1, x^2 - x)$  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、 $(x - 1) \subset I$  である。次に、 $x^2 - 1 = x(x - 1)$  かつ  $x^2 - x = x(x - 1)$  だから  $x^2 - 1, x^2 - x \in (x - 1)$  である。よって、 $I \subset (x - 1)$  なので  $I = (x - 1)$  である。すると  $x^3 + 1$  は ( $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$  いずれでも)  $x - 1$  の倍数ではないので、 $x^3 + 1$  は  $I$  に属さない。

(1.12) 命題  $f_1, \dots, f_s \in K[x]$  のとき、 $f_1, \dots, f_s$  の最大公約元を  $f$  とすると、 $(f_1, \dots, f_s) = (f)$  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。

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

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

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

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

(1.14) 今後の目的 (1)  $R$  の任意のイデアルの「よい」生成元を求められるか ( $n = 1$  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 ( $n = 1$  なら yes)。

(3)  $f_1, \dots, f_s \in R$  のとき、連立方程式  $f_1 = 0, \dots, f_s = 0$  が解けるか ( $n = 1$  なら 4 次まで yes)。

(1.15) 例  $K[x, y]$  のイデアル  $I = (x + y, x^2 + y^2)$  に  $y^3$  は属するか。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。

## §2 項順序と割り算アルゴリズム

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

(2.1) 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  $x^\alpha$  ( $\alpha = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$ ) と表す。 $\alpha \in (\mathbb{Z}_{\geq 0})^n$  を多重指数と呼ぶ。

(2.2) 項順序  $n$  変数多項式環  $R$  の単項式の単項式  $x^\alpha$  ( $\alpha \in (\mathbb{Z}_{\geq 0})^n$ ) 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。

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

(2.4) 例 (辞書式順序)  $(\mathbb{Z}_{\geq 0})^n$  上の項順序  $>_{\text{lex}}$  を次で定める:  $\alpha, \beta \in (\mathbb{Z}_{\geq 0})^n$  に対して、 $\alpha >_{\text{lex}} \beta$  であるとは、 $\alpha$  と  $\beta$  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  $\alpha >_{\text{lex}} \beta$  と定めると言ってもよい。

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

(2.6) 例 (次数付き逆辞書式順序)  $(\mathbb{Z}_{\geq 0})^n$  上の項順序  $>_{\text{revlex}}$  を次で定める:  $\alpha, \beta \in (\mathbb{Z}_{\geq 0})^n$  に対して、 $\alpha >_{\text{revlex}} \beta$  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、 $x_1 > x_2 > \dots > x_n$  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。

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

(2.7) 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  $\alpha$  のうち  $>$  に関して最大のものを  $\text{multideg}(f) \in (\mathbb{Z}_{\geq 0})^n$  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  $\beta$  と置く。

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

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

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

(2.8) 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。

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

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

- (2)  $LT(f)$  が  $LT(g)$  で割り切れないならば、 $LT(f)$  は余りに加算し、 $f$  から  $LT(f)$  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。

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

$$\begin{array}{r} xy + y^3 \ ) \ \begin{array}{r} xy^2 \quad -y^4 \\ x^2y^3 + x^2 \\ \hline x^2y^3 + xy^5 \\ -xy^5 + x^2 \quad \rightarrow x^2 \\ \hline -xy^5 \\ -xy^5 - y^7 \\ \hline y^7 \quad \rightarrow y^7 \\ \hline 0 \end{array} \end{array}$$

以上より、商が  $xy^2 - y^4$  で、余りが  $x^2 + y^7$  である。

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

(2.12) 例 (2.10) 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。

$$\begin{array}{r} xy + y^3 \ ) \ \begin{array}{r} x^2 \\ x^2y^3 + x^2 \\ \hline x^2y^3 + x^3y \\ -x^3y + x^2 \quad \rightarrow -x^3y + x^2 \\ \hline 0 \end{array} \end{array}$$

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

- (1)  $LT(f)$  が  $LT(g_1), \dots, LT(g_s)$  で割り切れるか順に試し、最初に割り切れたものを  $LT(g_i)$  とすると、商として  $LT(f)/LT(g_i)$  を立てて割り算を 1 段階実行し、 $f - g_i LT(f)/LT(g_i)$  を新たな  $f$  として割り算を続行する。  
 (2)  $LT(f)$  がどの  $LT(g_i)$  で割り切れないならば、 $LT(f)$  は余りに加算し、 $f$  から  $LT(f)$  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。

(2.14) 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。

$$\begin{array}{r} \begin{array}{l} 1: y^3 \\ 2: \quad 1 \end{array} \ ) \ \begin{array}{r} x^2 + y \\ xy^2 + y \\ \hline x^2y^3 + xy^2 \\ y^4 + x^2y^3 \\ \hline xy^2 - y^4 \\ xy^2 + y \\ \hline -y^4 - y \quad \rightarrow -y^4 - y \\ \hline 0 \end{array} \end{array}$$

$$\begin{array}{r} \begin{array}{l} 1: xy \\ 2: \end{array} \ ) \ \begin{array}{r} xy^2 + y \\ x^2 + y \\ \hline x^2y^3 + xy^2 \\ xy^2 + x^2y^3 \\ \hline 0 \end{array} \end{array}$$

(2.15) 割り算の恒等式  $f \in R$  を  $g_1, \dots, g_s \in R$  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。

$$f = a_1g_1 + \dots + a_sg_s + r$$

$$\text{multideg}(f) \geq \text{multideg}(a_i g_i) \quad (1 \leq i \leq s)$$

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

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

(2.17) 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)  $f = x^2y^2 + x^4y^3, g_1 = x^3 + y, g_2 = x^2y^2 + y$
- (2)  $f = x^3y^3 + x^4y^2, g_1 = x^2 + x^4y, g_2 = x^3y + x^2y^2$
- (3)  $f = x^2y^2z + x^2z^2, g_1 = xz + y^2, g_2 = z^2 - x$
- (4)  $f = x^2y^2z - y^5, g_1 = xyz - y^3, g_2 = xy - z^3$

### §3 ディクソンの補題

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

(3.1) 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。

(3.2) 補題  $A$  を多重指数の集合とし、 $I = (x^\alpha \mid \alpha \in A)$  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  $x^\alpha$  が  $x^\beta$  を割り切れることは同値である。

(3.3) 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。

(3.4) 定理 (ディクソンの補題)  $A$  を多重指数の集合とし、 $I = (x^\alpha \mid \alpha \in A)$  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  $x^\alpha$  ( $\alpha \in A'$ ) で生成される。

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

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

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:

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

このとき  $I$  は次の  $I$  に属する単項式

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

で生成される。なぜなら、 $I$  の単項式  $x^\alpha y^p$  があつたとき、 $p \geq M$  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  $x^{\alpha_k(i)}y^q$  ( $q \leq p$ ) 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。

(3.5) 命題  $(\mathbb{Z}_{\geq 0})^n$  上の順序  $>$  が、(2.2) の (T1) と (T2) を満たすとすると、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。

(3.6) 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」

(3.7) 問題  $R$  の単項式イデアル  $I = (x^\alpha \mid \alpha \in A)$  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。

(3.8) 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  $x^\alpha, x^\beta$  の間にも割り切る関係がないことを言う。

## §4 グレブナ基底

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

(4.1) 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、単項式の集合  $\text{LT}(I)$  と単項式イデアル  $(\text{LT}(I))$  を

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

で定める。 $(\text{LT}(I))$  を  $I$  の先頭項イデアルと呼ぶ。

(4.2) 注意  $I = (f_1, \dots, f_s)$  のとき、常に  $(\text{LT}(I)) \supset (\text{LT}(f_1), \dots, \text{LT}(f_s))$  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、 $I = (x+y, x^2+y^2) \subset K[x, y]$  の各生成元先頭項で生成されるイデアルは、 $(x, x^2) = (x)$  である。ところが、(1.15)により  $y^3 \in I$  であったから、 $(\text{LT}(I)) \supsetneq (x)$  である。

(4.3) 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  $G = \{g_1, \dots, g_s\}$

が  $I$  のグレブナ基底であるとは、 $(\text{LT}(I)) = (\text{LT}(g_1), \dots, \text{LT}(g_s))$  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。

(4.4) 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。

(4.5) 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。

(4.6) 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。

(4.7) 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、 $G = \{g_1, \dots, g_s\}$  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  $\text{LT}(g_i)$  ( $i = 1, \dots, s$ ) 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。

(4.8) 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。

## §5 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、(4.5) と (4.6) から明らかである。

(5.1) 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。

(5.2) 命題 (昇鎖条件)  $R$  中のイデアルの列

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

があったとき、ある正整数  $N$  があって、

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

と途中からすべて同じになる。

## §6 ブッフベルガーのアルゴリズム

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

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

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

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

で定義する。

例えば、 $x > y$  なる辞書式順序を考えると、

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

である。

(6.2) 補題  $f_1, \dots, f_s \in R$  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  $\delta$  より真に小さい。

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

(6.3) 補題  $f, g \in R$  であり、 $\text{multideg } f = \alpha, \text{multideg } g = \beta$  とする。 $x^\gamma$  を  $x^\alpha$  と  $x^\beta$  の最小公倍元とする。 $x^\delta$  が  $x^\gamma$  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。

(6.4) 定理 (ブッフベルガーの判定条件)  $R$  上の項順序を固定し、 $I = (g_1, \dots, g_s)$  を  $R$  の 0 ではないイデアルとする。 $G = \{g_1, \dots, g_s\}$  とおくと、 $G$  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、(4.8) 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、 $\text{LT}(f) \in (\text{LT}(G))$  を示せばよい。 $f \in (g_1, \dots, g_s)$  だから、 $f = \sum_i h_i g_i$  ( $h_i \in R$ ) と書けるが、 $\text{multideg}(f) \leq \max_i \{\text{multideg}(h_i g_i)\}$  である。もし等号が成立するならば、ある  $i$  に対して  $\text{LM}(f) = \text{LM}(h_i g_i)$  となるので、 $\text{LT}(f) \in (\text{LT}(G))$  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  $\max_i \{\text{multideg}(h_i g_i)\}$  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  $\delta$  とおく。

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

この第1項は、多重指数が  $\delta$  より小さいので次のように計算できる。

$$\begin{aligned} (\text{第1項}) &\stackrel{(6.2)(2)}{=} \sum_{j,k} c_{jk} S(\text{LT}(h_j) g_j, \text{LT}(h_k) g_k) \quad (c_{jk} \in K) \\ &\stackrel{(6.3)}{=} \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) \quad (x^{\gamma_{jk}} = \text{LCM}(\text{LM}(g_j), \text{LM}(g_k))) \\ &\stackrel{\text{仮定}}{=} \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} \sum_i a_{ijk} g_i \\ &= \sum_i \left( \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} a_{ijk} \right) g_i. \end{aligned}$$

ここで、(2.15) より、 $\text{multideg } a_{ijk} \leq \text{multideg } S(g_j, g_k)$  だから、 $S$  多項式の定義よりわかる  $\text{multideg } S(g_j, g_k) < \gamma_{jk}$  と合わせると、上の最後の式のかっこの中は多重次数が  $\delta$  より小さい項しか現れない。これを (\*) に代入すると、 $f = \sum_i (\delta$  より低次の式)  $g_i$  となり、 $\delta$  のとり方に矛盾する。  $\square$

(6.5) 例 辞書式順序を考える。

(1)  $g_1 = x + y$ ,  $g_2 = x^2 + y^2$  とし、 $I = (g_1, g_2) \subset K[x, y]$  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、(6.4) 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、 $(h_1, h_2) = (x + y, x^2 + y^2)$  である。 $S(h_1, h_2) = y^3$  は  $h_1, h_2$  で割り切れるから、(6.4) より  $h_1, h_2$  はグレブナ基底である。

(6.6) 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。

(6.7) 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、 $I = (f_1, \dots, f_s)$  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。

$G := \{f_1, \dots, f_s\}$   
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  $(G) = I$  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  $(G)$  の元だから、常に  $(G) = I$  である。また、アルゴリズムが停止したならば、(6.4) 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、 $\text{LT}(r)$  は  $\text{LT}(G)$  のどの元でも割り切れない。よって、 $(\text{LT}(G)) \subsetneq (\text{LT}(G \cup \{r\}))$  である。よって、アルゴリズムが動いているうちは、 $(\text{LT}(G))$  たちがイデアルの真の上昇列をなすため、昇鎖条件 (5.2) よりアルゴリズムは停止する。  $\square$

(6.8) 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。

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

(6.9) 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、 $\text{LT}(p) \notin (\text{LT}(G - \{p\}))$  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。

(6.10) 問題 辞書式順序を考え、次の問に答えよ。

- (1)  $I = (x + y, x^2 + y^2)$  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)  $I = (xy, x^2 + y^2)$  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。

(6.11) 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  $(\text{LT}(G - \{p\}))$  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。

(6.12) 例 辞書式順序を考える。 $(x + y, x^2 + y^2, y^2)$  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、 $(x + y, y^2)$  は簡約グレブナ基底である。

(6.13) 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  $G = \{g_1, \dots, g_s\}$  をとる。 $g'_1 = \overline{g_1}^{G - \{g_1\}}$ ,  $G_1 = \{g'_1, g_2, \dots, g_s\}$ ,  $g'_2 = \overline{g_2}^{G_1 - \{g_2\}}$ ,  $G_2 = \{g'_1, g'_2, \dots, g_s\}$ , と  $G_s$  まで定める。極小性より  $\text{LT}(g_1) = \text{LT}(g'_1)$  であり、その後も、 $\text{LT}(g_i) = \text{LT}(g'_i)$  であるから、 $G_i$  はすべて極小グレブナ基底である。 $\text{LT}(G_i) = \text{LT}(G_s)$  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、 $\text{LT}(G) = \text{LT}(G')$  である。 $\text{LT}(g) = \text{LT}(g')$  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  $\text{LT}(G) = \text{LT}(G')$  で割れないから  $\overline{g - g'}^G = g - g'$  である。よって、 $g = g'$ 。□

## §7 消去理論

(7.1) 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  $(f_1, f_2, f_3)$  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<sup>1</sup>を行って新たな式を得たとき、その式はイデアル  $(f_1, f_2, f_3)$  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  $(f_1, f_2, f_3)$  に属する簡単な式を探すことに相当し、例えば、1 変数しか含まないような簡単な式が見つければその 1 変数については、解が確定する。

(7.2) 定義 (消去イデアル)  $R$  のイデアル  $I = (f_1, f_2, \dots, f_s)$  に対して、 $l$  次の消去イデアルを

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

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、 $K[x_{l+1}, x_{l+2}, \dots, x_n]$  のイデアルである。また、 $I_0 = I$  である。

(7.3) 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  $G = \{g_1, g_2, \dots, g_s\}$  とすると、

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

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。□

<sup>1</sup>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。

(7.4) 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 = (f\_1, f\_2, f\_3)\$ の辞書式順序に関する簡約グレブナ基底は、

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

である。従って、消去イデアルは、

$$I_1 = (g_1, g_2, g_3), \quad I_2 = (g_1)$$

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\_2 = 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。

(7.5) 定義 (部分解) 上の例の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。

(7.6) 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, \dots, x\_n]\$ のイデアル \$I = (f\_1, f\_2, \dots, f\_s)\$ の 1 次の消去イデアルを \$I\_1\$ とする。各 \$f\_i\$ を \$x\_1\$ の降幂の順で整理して、

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

と書く。ただし、\$g\_i \in \mathbb{C}[x\_2, \dots, x\_n]\$ は 0 ではない多項式とする。部分解 \$(x\_2, \dots, x\_n) = (a\_2, \dots, a\_n)\$ があるとき、ある \$g\_i\$ に対して、\$g(a\_2, \dots, a\_n) \neq 0\$ ならば、この部分解は、解 \$(x\_1, x\_2, \dots, x\_n) = (a\_1, a\_2, \dots, a\_n)\$ に拡張できる。

(7.7) 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 = (f, g)\$ の辞書式順序でのグレブナ基底は、

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

であるから、消去イデアルは、

$$I_1 = (h), \quad I_2 = (0)$$

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。<sup>2</sup>

<sup>2</sup> 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。