2010 年度 前期 代数学特論 III

更新日時 2010-08-06 12:53:24　担当 和地 輝仁

目 次

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

授業で用いる演習問題や基本事項を記す。

§1　群

(1.1)　**演算**　集合 S 上の**演算**とは、写像 $S \times S \to S$ $((x,y) \mapsto xy)$ のことを言う。

(1.2)　**群**　集合 G が**群**であるとは、G 上に演算があり (**積**と呼ぶ)、次の条件を満たすときを言う。

(G1) 積が結合法則を満たす
(G2) ある $e \in G$ が存在して、任意の $x \in G$ に対して $ex = xe = x$ を満たす (e を G の**単位元**と呼ぶ)。
(G3) 任意の $x \in G$ に対して、 $xy = yx = e$ を満たす $y \in G$ が存在する (y を x の**逆元**と呼び $\boldsymbol{x^{-1}}$ と書く)。

(1.3)　**アーベル群 (可換群)**　群 G が**アーベル群** (**可換群**) であるとは、G が次の条件を満たすときを言う。

(G4) 積が交換法則を満たす

このとき演算を加法的に $x+y$ を表し、**加法群**と呼ぶこともある。

(1.4)　**例**　次の集合と演算の組は群をなす。
(1) $(\mathbb{Z}, +)$
(2) $(\mathbb{Q}^\times, \times)$. ただし、$\mathbb{Q}^\times = \mathbb{Q} - \{0\}$.
(3) $(\mathbb{Q}_{>0}, \times)$. ただし、$\mathbb{Q}_{>0} = \{x \in \mathbb{Q} \mid x > 0\}$.
(4) $(\{\pm 1\}, \times)$
(5) $(\mathrm{Mat}_n(\mathbb{R}), +)$. ただし、$\mathrm{Mat}_n(\mathbb{R})$ は n 次正方行列全体。
(6) $(GL_n(\mathbb{R}), 積)$. ただし、$GL_n(\mathbb{R})$ は n 次正則行列全体。
(7) $(\mathrm{Aut}(X), \circ)$. ただし、$\mathrm{Aut}(X)$ は集合 X から X への全単射全体で、$\circ$ は写像の合成。
(8) $(S_n, \circ)$. ただし、S_n は n 次対称群で、$\circ$ は写像の合成。

また、これらのうち (1), (2), (3), (4) はアーベル群であり、(5), (6), (7), (8) はアーベル群ではない。

(1.5)　**部分群**　群 G の部分集合 H が G の**部分群**であるとは、H が G と同じ演算で群をなすことを言う。つまり、積で閉じていて、逆元でも閉じている空ではない部分集合のことである。

(1.6)　**例**　次の部分集合は部分群である。
(1) $\mathbb{Z}$ の部分集合 $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$.
(2) $(\mathrm{Mat}_n(\mathbb{R}), +)$ の対角行列全体がなす部分集合。
(3) $(GL_n(\mathbb{R}), +)$ の対角行列全体がなす部分集合。
(4) n 次対称群 S_n の、偶置換全体のなす部分集合 A_n.

(1.7)　**関係**　$\sim$ が集合 S 上の**関係**であるとは、$x, y \in S$ に対して $x \sim y$ であるかそうでないかが確定する場合を言う。

また、S 上の関係 $\sim$ が**同値関係**であるとは、$\sim$ が次の 3 条件を満たすことを言う。

(E1) 任意の $x \in S$ に対して $x \sim x$ (**反射律**)。
(E2) $x \sim y$ ならば $y \sim x$ (**対称律**)。
(E3) $x \sim y$ かつ $y \sim z$ ならば $x \sim z$ (**推移律**)。

(1.8)　**例**　次は同値関係の例である。
(1) あるクラスの学生の集合において、X さんの血液型が Y さんの血液型と同じならば X∼Y と定める。
(2) 47 都道府県の県庁所在地の集合において、都市 A から都市 B へ陸続きで (つまり、トンネルや橋や船で海を越えずに) 行けるならば A∼B と定める。
(3) 写像 $f : X \to Y$ があるとき、$x_1, x_2 \in X$ に対して、$f(x_1) = f(x_2)$ のとき $x_1 \sim x_2$ と定める。

(1.9)　**同値類**　集合 S 上に同値関係 $\sim$ があるとする。$x \in S$ に対して、

$$[x] = \{y \in S \mid x \sim y\}$$

と定め、$\sim$ に関する x の**同値類**と呼び、x を $[x]$ の**代表元**と呼ぶ。

$x \sim y$ ならば $[x] = [y]$ であるから、ある同値類に属する元はどれも代表元になりうる。つまり、代表元のとり方は一意ではない。

(1.10)　**同値類別**　集合 S 上に同値関係 $\sim$ があるとする。$\sim$ に関する同値類 S_1 と S_2 があったとき、$S_1 \neq S_2$ ならば共通部分は空である。したがって S を同値類に分割することができる:

$$S = \coprod_{S_i:\ \text{同値類}} S_i \qquad \text{(共通部分のない集合たちによる和集合)}.$$

これを S の $\sim$ に関する**同値類別**と呼ぶ。

同値類全体の集合を

$$S/\sim = \{S_i \mid S_i \text{ は同値類 }\}$$

と定め、S の $\sim$ に関する**商集合**と呼ぶ。

自然な全射 $\pi : S \to S/\sim\ (x \mapsto [x])$ を考えたとき、S の部分集合 X であって、π により $S \sim$ と 1 対 1 に対応するものを、$S/\sim$ の**完全代表系**と呼ぶ。素朴には、各同値類から 1 つずつ代表元を集めて作った S の部分集合である。完全代表系は一意ではない。

(1.11)　**例**

(1) (1.8) の (1) において、同値類は同じ血液型の学生全体のなす集合であり、商集合は $\{S_A, S_B, S_O, S_{AB}\}$ である。ただし、S_T は、血液型が T 型の学生全体のなす集合である。また、例えば、AB 型の学生が 1 人もいなければ、商集合は $\{S_A, S_B, S_O\}$ のように同値類の数が減る。

(2)　(1.8) の (2) において、同値類は、{ 北海道 }, { 本州の都道府県庁所在地全体 }, { 四国の都道府県庁所在地全体 }, { 九州の都道府県庁所在地全体 }, { 沖縄 } であり、商集合は、これらを 5 つの元とする集合である。

(3) (1.8) の (3) において、同値類は、$[x] = \{x' \in X \mid f(x') = f(x)\}$ $(x \in X)$ であり、商集合は、$\{[x] \mid x \in X\}$ である。

(4) 平面 $\mathbb{R}^2$ を点の集合と見たとき、$\mathrm{P}, \mathrm{Q} \in \mathbb{R}^2$ に対して、P と Q が等しいか、または、直線 PQ の傾きが 1 のときに、$\mathrm{P} \sim \mathrm{Q}$ と定めると同値関係になる。P の同値類 [P] は、P を通る傾き 1 の直線である。

(1.12)　**剰余集合**　群 G とその部分群 H に対して、$x^{-1}y \in H$ のとき $x \sim y$ と定める $(x, y \in G)$ と、同値関係になる (証明せよ)。この同値関係による $x \in G$ の同値類は、

$$[x] = xH := \{xh \mid h \in H\}$$

となる (等号を証明してみよ)。$[x] = xH$ を H による**左剰余類**と呼び、商集合 $G/\sim$ を G/H と書き、H による**左剰余集合** (H で**右から割った集合**) と呼ぶ (左、左、右の用語に注意)。

最初の同値関係を $x \sim y \ \Leftrightarrow\ xy^{-1} \in H$ で定めると、同様にして $[x] = Hx = \{hx \mid h \in H\}$ となり、これを H による**右剰余類**と呼び、商集合 $G/\sim$ を $H\backslash G$ と書き、H による**右剰余集合** (H で**左から割った集合**) と呼ぶ。

(1.13)　**命題**　(1) H を群 G の部分群とすると $\#(G/H) = \#(H\backslash G)$ であり、G が有限群ならばこれらは $\#G/\#H$ に等しい。

(2) H と K を群 G の部分群とし、$H \supset K$ とする。このとき、$\#(G/K) = \#(G/H) \times \#(H/K)$ である (無限集合の時は、濃度の積を直積集合の濃度で定める)。

(1.14)　**正規部分群**　群 G の部分群 H が**正規部分群**であるとは、任意の $x \in G$ に対して $xHx^{-1} \subset H$ となるときを言う。

(1.15)　**補題**　群 G の部分群 H が正規部分群であるための必要十分条件は、$G/H = H\backslash G$ となることである。

(1.16) **命題** H を群 G の正規部分群とすると、G/H に自然に群の構造が入る。これを G の H による**剰余群**と呼ぶ。

(1.17) **準同型写像**

(1.18) **核**

(1.19) **準同型定理**

(1.20) **直積群**

§2 多項式環

(2.1) **多項式環のイデアル** 体 K を $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ のいずれかとする。$K[x_1, \ldots, x_n]$ を K 上の n **変数多項式環**と呼ぶ。

$R = K[x_1, \ldots, x_n]$ 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 $R = K[x_1, \ldots, x_n]$ とする。

(2.2) **補題** $f \in R$ 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。

(2.3) **補題** $I, J \subset R$ 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。

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

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

と定めると $(f_1, \ldots, f_s)$ 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 $(f_1, \ldots, f_s)$ の**生成元** (**生成系**) と呼ぶ。

(2.5) **補題** 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。

(2.6) **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。

(2.7) **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、$(f_1, \ldots, f_s) = (f)$ 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。

(2.8) **問題** (1) イデアル $(x^2 - 1, x^3 - 1) \subset K[x]$ に $x^3 + 1$ は属するかどうか言え。
(2) イデアル $(x^2 - 1, x^2 + 1) \subset K[x]$ に $x^3 + 1$ は属するかどうか言え。

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

(2.10)　**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。

§3　項順序と割り算アルゴリズム

以下しばらく $R = K[x_1, \ldots, x_n]$ と置く。

(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。

(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) $x^2 + xyz + x^2z + y^3 + xy^2$

(3.9) 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) $\mathrm{LT}(f)$ 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。

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

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

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

(3.11) 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。

(3.12) 例 (3.10) 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。

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

(3.13) 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。

(3.14) **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。

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

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

(3.15) **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。

$$f = a_1g_1 + \cdots + a_sg_s + r$$
$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_ig_i) \qquad (1 \leq i \leq s)$$

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

(3.16) **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。

(3.17) **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) $f = x^2y^2z - y^5$, $g_1 = xyz - y^3$, $g_2 = xy - z^3$

§4　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。

(4.1) **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。

(4.2) **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^α が x^β を割り切ることは同値である。

(4.3) **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。

(4.4) **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^α $(\alpha \in A')$ 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

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

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 $x^{\alpha_p(i)}y^p$ 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。

(4.5) **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。

(4.6) **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」

(4.7) **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。

(4.8) **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。

§5 グレブナ基底

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

(5.1) **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 $(\mathrm{LT}(I))$ を

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

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

(5.2) **注意** $I = (f_1, \dots, f_s)$ のとき、常に $(\mathrm{LT}(I)) \supset (\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s))$ 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、$I = (x+y, x^2+y^2) \subset K[x, y]$ の各生成元の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、(2.10) により $y^3 \in I$ であったから、$(\mathrm{LT}(I)) \supsetneq (x)$ である。

(5.3) **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、$(\mathrm{LT}(I)) = (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s))$ 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。

(5.4)　**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。

(5.5)　**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。

(5.6)　**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。

(5.7)　**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、$G = \{g_1, \ldots, g_s\}$ 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。

(5.8)　**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。

§6　ヒルベルトの基底定理

以下でもしばらく $R = K[x_1, \ldots, x_n]$ と置く。次の定理は、(5.5) と (5.6) から明らかである。

(6.1)　**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。

(6.2)　**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。

§7　ブッフベルガーのアルゴリズム

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

(7.1)　**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。

(7.2)　**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、$S(f_j, f_k)$ $(1 \leq j, k \leq s)$ の K 係数の 1 次結合である。

(7.3) **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。

(7.4) **定理** R 上の項順序を固定し、$I = (g_1, \ldots, g_s)$ 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、(5.8) 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、$\mathrm{LT}(f) \in (\mathrm{LT}(G))$ を示せばよい。$f \in (g_1, \ldots, g_s)$ 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、$\mathrm{LT}(f) \in (\mathrm{LT}(G))$ 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 $\max_i\{\mathrm{multideg}(h_i g_i)\}$ 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。

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

$$\begin{aligned} (\text{第 1 項}) &\overset{(7.2)}{=} \sum_{j,k} c_{jk} S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k) \qquad (c_{jk} \in K) \\ &\overset{(7.3)}{=} \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) \qquad (x^{\gamma_{jk}} = LCM(\mathrm{LM}(g_j), \mathrm{LM}(g_k))) \\ &\overset{\text{仮定}}{=} \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} \sum_i a_{ijk} g_i \\ &= \sum_i \left(\sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} a_{ijk} \right) g_i. \end{aligned}$$

ここで、(3.15) より、$\mathrm{multideg}\, a_{ijk} \leq \mathrm{multideg}\, S(g_j, g_k)$ 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、$f = \sum_i (\delta$ より低次の式$) g_i$ となり、δ のとり方に矛盾する。 □

(7.5) **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、(7.4) 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、(7.4) より h_1, h_2 はグレブナ基底である。

(7.6) **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。

(7.7) **定理** R 上の項順序を固定し、$I = (f_1, \ldots, f_s)$ 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。

$G := \{f_1, \ldots, f_s\}$
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)

(7.8) **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、$\mathrm{LT}(p) \notin (\mathrm{LT}(G - \{p\}))$ 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。

(7.9) **問題** 辞書式順序を考える。$I = (x+y, x^2+y^2)$ の極小グレブナ基底を (1 つ) 求めよ。また、xy^2 は I に属するか答えよ。

(7.10) **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 $(\mathrm{LT}(G - \{p\}))$ 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。

(7.11) **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。

(7.12) **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、$g = g'$. □