

グレブナー基底とあるひとつの応用

岡山大学大学院 自然科学研究科 飯間 圭一郎

この報告の内容は、岡山大学の吉野雄二先生との共同研究に基づくものである。

1 概略

自然数 n に対して、 n を n 以下の正の整数の和として表わしたものを分割と呼ぶ。すなわち、 $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ が n の分割であるとは、 $n \geq \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r \geq 1$ かつ $\lambda_1 + \lambda_2 + \dots + \lambda_r = n$ が成り立つときをいい、 $\lambda \vdash n$ と表わす。但し、 0 の分割は唯一つだけであり $()$ と表わす。

次に以下の3種類の部分集合を考える。

$$A(n) = \{\lambda \vdash n \mid \lambda_i \equiv \pm 1 \pmod{6}\},$$

$$B(n) = \{\lambda \vdash n \mid \lambda_i \equiv \pm 1 \pmod{3}, \lambda_1 > \dots > \lambda_r\},$$

$$C(n) = \{\lambda \vdash n \mid \lambda_i \equiv 1 \pmod{2}, \{\lambda_i\} \text{ の中に同じ数は、高々2個しか登場しない}\}.$$

すべての自然数 n に対して $A(n), B(n)$ および $C(n)$ の濃度が等しいことは、有名なシューアの関数等式として知られている。さらに整数の2-進展開または3-進展開といった組合せ論的な方法で、これらの3つの集合の間に一対一対応が構成できることも知られている。

この報告ではグレブナー基底の理論を用いてこれらの間の一対一対応を再構成することを目指とする。そのためにはグレブナー基底の理論を無限変数多項式環の場合に拡張する必要がある。

2 グレブナー基底

この報告を通して、 k を任意の体とし $S = k[x_1, x_2, \dots]$ を無限変数多項式環とする。ここで無限変数多項式環とは、自然な包含関係による帰納系 $k \subset k[x_1] \subset \dots \subset k[x_1, x_2, \dots, x_n] \subset \dots$ の極限として定義される。すなわち、 $S = \bigcup_{n=0}^{\infty} k[x_1, x_2, \dots, x_n]$ である。非負整数の列 $a = (a_1, a_2, \dots)$ で有限個の i を除いて $a_i = 0$ をみたすもの全体を $\mathbb{Z}_{\geq 0}^{(\infty)}$ と表わし、 S の単項式全体を $\text{Mon}(S)$ と表わす。自然な対応で $\mathbb{Z}_{\geq 0}^{(\infty)}$ と $\text{Mon}(S)$ を同一視する。(i.e. $a \mapsto x^a$). さらに、各自然数 i について $\deg(x_i) = i$ と次数づけることにより S を次数つき k -代数とみなし、その上で自然数 n の分割 λ を自然な対応で n 次の単項式と同一視する。(i.e. $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r) \mapsto x^\lambda = x_{\lambda_r} \cdots x_{\lambda_2} x_{\lambda_1}$).

定義 1 $\text{Mon}(S)$ 上の全順序 $>$ が単項式順序であるとは, $(\text{Mon}(S), >)$ が整列集合であり, 全ての $x^a, x^b, x^c \in \text{Mon}(S)$ に対して, $x^a > x^b$ ならば $x^c x^a > x^c x^b$ が成り立つときをいう.

例 2 $a = (a_1, a_2, \dots), b = (b_1, b_2, \dots) \in \mathbb{Z}_{\geq 0}^{(\infty)}$ とする.

[1] 純辞書式順序; $a_n \neq b_n$ を充たす最後の n に対して, $a_n > b_n$ が成り立つとき, $x^a >_{pl} x^b$ と定める.

[2] 次数辞書式順序; $\deg(x^a) > \deg(x^b)$ を充たしている, もしくはそうでないとき $a_n \neq b_n$ を充たす最後の n に対して, $a_n > b_n$ が成り立つとき, $x^a >_{dl} x^b$ と定める.

[2]' 次数反辞書式順序; $\deg(x^a) > \deg(x^b)$ を充たしている, もしくはそうでないとき $a_n \neq b_n$ を充たす最初の n に対して, $a_n > b_n$ が成り立つとき, $x^a >_{dal} x^b$ と定める.

[3] 次数逆辞書式順序; $\deg(x^a) > \deg(x^b)$ を充たしている, もしくはそうでないとき $a_n \neq b_n$ を充たす最初の n に対して, $a_n < b_n$ が成り立つとき, $x^a >_{rl} x^b$ と定める.

[3]' 次数反逆辞書式順序; $\deg(x^a) > \deg(x^b)$ を充たしている, もしくはそうでないとき $a_n \neq b_n$ を充たす最後の n に対して, $a_n < b_n$ が成り立つとき, $x^a >_{arl} x^b$ と定める.

$$x_1^3 >_{dl} x_2, x_2 >_{pl} x_1^3.$$

$$x_4 >_{dl} x_1 x_3 >_{dl} x_2^2 >_{dl} x_1^2 x_2 >_{dl} x_1^4,$$

$$x_1^4 >_{dal} x_1^2 x_2 >_{dal} x_1 x_3 >_{dal} x_2^2 >_{dal} x_4,$$

$$x_4 >_{rl} x_2^2 >_{rl} x_1 x_3 >_{rl} x_1^2 x_2 >_{rl} x_1^4,$$

$$x_1^4 >_{arl} x_1^2 x_2 >_{arl} x_2^2 >_{arl} x_1 x_3 >_{arl} x_4.$$

以上により, これらの順序はそれぞれ異なる順序である.

ここで $\text{Mon}(S)$ 上の単項式順序 $>$ を 1 つ固定すると, 0 でない全ての多項式 $f \in S$ は次のように表わせる. $f = \alpha_1 x^{a_1} + \alpha_2 x^{a_2} + \dots + \alpha_r x^{a_r}$, 但し, $\alpha_i \neq 0 \in k$ かつ $x^{a_1} > x^{a_2} > \dots > x^{a_r}$. このとき f の先頭項, 先頭単項式および先頭係数をそれぞれ $lt(f) = \alpha_1 x^{a_1}$, $lm(f) = x^{a_1}$, $lc(f) = \alpha_1$ と表わす. イデアル $I (\neq (0)) \subset S$ に対して, 0 でない全ての多項式 $f \in I$ の先頭項 $lt(f)$ が生成するイデアルを I のイニシャルイデアルと呼び $in(I)$ と表わす. I のグレブナー基底は従来の場合と同様に定義できる.

定義 3 イデアル I の部分集合 \mathcal{G} が I のグレブナー基底であるとは, $\{lt(g) | g \in \mathcal{G}\}$ が I のイニシャルイデアル $in(I)$ を生成するときをいう.

補助定理 4 S のイデアルを I , その部分集合を \mathcal{G} とおく. このとき, 全ての自然数 n に対して, $\mathcal{G} \cap k[x_1, x_2, \dots, x_n]$ が $I \cap k[x_1, x_2, \dots, x_n]$ のグレブナー基底であるとき, \mathcal{G} は I のグレブナー基底である.

定理 5 (割り算アルゴリズム). S のある部分集合を \mathcal{G} とおく. このとき 0 でない全ての多項式 $f \in S$ は, 次のように表わせる.

$$f = f_1g_1 + f_2g_2 + \cdots + f_sg_s + f',$$

但し, $g_i \in \mathcal{G}$ かつ $f', f_i \in S$ は, 以下の条件を充たす:

(1) $f' = \sum_{i=1}^t \alpha_i x^{a_i}$ 但し $\alpha_i \neq 0 \in k$ と書いたとき, 各 $i = 1, 2, \dots, t$ について $x^{a_i} \notin (\text{lm}(g) | g \in \mathcal{G})S$ が成り立つ.

(2) $f_i g_i \neq 0$ ならば $\text{lm}(f_i g_i) \leq \text{lm}(f)$ を充たす.

このようにして得られる f' を \mathcal{G} に関する f の剰余と呼ぶ. 一般には剰余が一意的に定まるとは限らないが, \mathcal{G} が $I = \mathcal{G}S$ のグレブナー基底であるとき, \mathcal{G} に関する f の剰余は一意的に定まる.

3 あるひとつの応用

\mathbb{N} の部分集合 W で, ある自然数 $p \geq 2$ に対して $pW \subset W$ を充たすものを考え, S の部分環を $R = k[x_i | i \in W]$ とおく. ここで全ての自然数 n に対して, 以下の 2 種類の部分集合を考える.

$$X(n) = \{\lambda \vdash n | \lambda_i \in W \setminus pW\},$$

$$Y(n) = \{\lambda \vdash n | \lambda_i \in W, \{\lambda_i\} \text{ の中に同じ数は, 高々 } p-1 \text{ 個しか登場しない}\}.$$

ここで, $W = \{n \in \mathbb{N} | n \equiv \pm 1 \pmod{3}\}$, $p = 2$ とするとき, $X(n) = A(n)$, $Y(n) = B(n)$ となり, $W = \{n \in \mathbb{N} | n \equiv \pm 1 \pmod{2}\}$, $p = 3$ とするとき, $X(n) = A(n)$, $Y(n) = C(n)$ となることに注意しておく.

定理 6 上の状況の下で, R の部分集合 $\mathcal{G} = \{x_i^p - x_{pi} | i \in W\}$ を考える. R の単項式全体の単項式順序として次数反逆辞書式順序を採用するとき, \mathcal{G} はイデアル $\mathcal{G}S$ の被約グレブナー基底である.

さらに, 任意の $\lambda \in X(n)$ に対して $x^{\varphi(\lambda)}$ が x^λ の \mathcal{G} に関する剰余となるように写像 $\varphi: X(n) \rightarrow Y(n)$ を定めるとき, φ は $X(n)$ と $Y(n)$ の間の一対一対応を与えている.

(証明) $I = \mathcal{G}S$ とおき, $>$ を次数反逆辞書式順序とする. このとき, 補助定理 4 により \mathcal{G} は I のグレブナー基底である. \mathcal{G} の被約性質は明らかである. \mathcal{G} の各元が二項式であること, \mathcal{G} がグレブナー基底であることから定理 5 により φ は well-defined な写像をなす.

同様に, $>$ ' を次数辞書式順序とすると, 補助定理 4 により $\mathcal{G}' = \{x_{pi} - x_i^p \mid i \in W\}$ は I のグレブナー基底である. よって, 任意の $\rho \in Y(n)$ に対して $x^{\psi(\rho)}$ が x^ρ の \mathcal{G}' に関する剰余となるように well-defined な写像 $\psi : Y(n) \rightarrow X(n)$ を定めることができる.

さらに, 任意の $\lambda \in X(n)$ に対して, $x^\lambda = \sum_{j=1}^t f_j(x_{i_j}^p - x_{pi_j}) + x^\rho$, ($f_1, \dots, f_t \in R$) と表わすとき, $x^\rho = \sum_{j=1}^t f_j(x_{pi_j} - x_{i_j}^p) + x^\lambda$ により, $\psi \circ \varphi = 1_{X(n)}$ が成り立つ. 同様にして, $\varphi \circ \psi = 1_{Y(n)}$ も成り立つので, φ は $X(n)$ と $Y(n)$ の間の一対一対応を与えている. [証明終]

以上により, すべての自然数 n に対して $A(n), B(n)$ および $C(n)$ の間に一対一対応を再構成することができた.

参考文献

- [1] D.EISENBUD, Commutative algebra with a view toward algebraic geometry. Graduate Texts in Mathematics 150. *Springer*, 1995.
- [2] K.IIMA, Y.YOSHINO, Gröbner bases for the polynomial rings with infinitely many variables and applications, in preparation, 2008.