数理解析研究所講究録
第1666巻 2009年 6-8

多項式剰余環における逆元の計算と準素イデアル分解

佐藤洋祐
YOSUKE SATO
東京理科大学
TOKYO UNIVERSITY OF SCIENCE*

1 研究の動機

以下は計算機代数の大抵の教科書に載っている基本的な定理である. 以下において K は任意の体、$\bar{X}$ は1つ以上の変数、Y はそれとは異なる変数を表す.

定理1 (Radical membership)
イデアル $I \subseteq K[\bar{X}]$ と多項式 $f \in K[\bar{X}]$ にたいして以下が成り立つ.

$$f \in \sqrt{I} \Longleftrightarrow I + \langle Yf - 1 \rangle = \langle 1 \rangle$$

それでは $I + \langle Yf - 1 \rangle \neq \langle 1 \rangle$ の場合はどうなっているであろうか.

I が0次元の場合、以下を証明するのは容易である.

定理2
$f(\bar{X}) \notin \sqrt{I}$ なら $I + \langle Yf(\bar{X}) - 1 \rangle$ のグレブナー基底 (項順序は $Y > \bar{X}$ なるブロック順序) は必ず $\{Y - h(\bar{X}), g_1(\bar{X}), \ldots, g_l(\bar{X})\}$ の形をしていて、$h(\bar{X})$ は $K[\bar{X}]/\langle g_1(\bar{X}), \ldots, g_l(\bar{X}) \rangle$ における $f(\bar{X})$ の逆元となる. さらに、$\langle g_1(\bar{X}), \ldots, g_l(\bar{X}) \rangle$ は $f(\bar{X})$ が $K[\bar{X}]/J$ で逆元を持つような I を含む $(J \supseteq I)$ イデアル J の中で最小のものになっている. すなわち、そのような J に対して常に $J \supseteq \langle g_1(\bar{X}), \ldots, g_l(\bar{X}) \rangle$ となる.

例 $\frac{1}{\sqrt{3+2\sqrt{2}}+\sqrt{2}+1}$ の分母の有理化

$X_1 = \sqrt{3+2\sqrt{2}}$、$X_2 = \sqrt{2}$ と考え、$I = \langle X_1^2 - (3 + 2X_2), X_2^2 - 2 \rangle$ とおき $\mathbb{Q}[X_1, X_2]/I$ において $f = X_1 + X_2 + 1$ の逆元を求めることに他ならない.
$\langle X_1^2 - (3 + 2X_2), X_2^2 - 2, (X_1 + X_2 + 1)Y - 1 \rangle$ のグレブナー基底は $\{X_2^2 - 2, X_1 - X_2 - 1, Y - \frac{X_2 - 1}{2}\}$ である. これより、$J = \langle X_2^2 - 2, X_1 - X_2 - 1 \rangle$ が $X_1 + X_2 + 1$ が $\mathbb{Q}[\bar{X}]/J$ で逆元を持つような I を含むイデアル J の中で最小のものになっていることがわかる.
これは $X_1 - X_2 - 1 = 0$ すなわち $\sqrt{3+2\sqrt{2}} = \sqrt{2} + 1$ のとき、$\frac{1}{\sqrt{3+2\sqrt{2}}+\sqrt{2}+1} = \frac{\sqrt{2}-1}{2}$ となることを意味している.

*ysato@rs.kagu.tus.ac.jp

本論文では、一般の (高次元) イデアル I の場合に上の定理２を拡張して得られた結果とそれから容易に導かれるイデアルの準素分解にについて成り立つ性質について報告する.

2 主結果

証明した主要な結果は以下の定理である.

定理３

一般のイデアル $I \subseteq K[\bar{X}]$ と多項式 $f(\bar{X}) \in K[\bar{X}]$ に対して、以下は同値である.

(1) $f(\bar{X})$ が $K[\bar{X}]/J$ で逆元を持つような最小の イデアル $J(I \subseteq J)$ が存在する.

(2) $I + \langle Y f(\bar{X}) - 1\rangle$ のグレブナー基底 (項順序は $Y > \bar{X}$ なるブロック順序) は
$\{Y - h(\bar{X}), g_1(\bar{X}), \ldots, g_l(\bar{X})\}$ なる形をしている.

$\langle g_1(\bar{X}), \ldots, g_l(\bar{X})\rangle$ は実際 (1) の最小のイデアルとなり、$h(\bar{X})$ が逆元になる.

定理４

定理３の (1)、(2) が成り立つときは、$J = I : f^{\infty}$ であり、$I : f^{\infty} = I : f^m$ なる最小の m にたいして、$I = (I + \langle f^m\rangle) \cap (I : f^m)$ が成り立ち、

(i) $f \in \sqrt{I + \langle f^m\rangle}$
(ii) f は $K[\bar{X}]/(I : f^m)$ で逆元をもつ

が成り立つが、このような分解はユニークに定まる. すなわち　$f \in \sqrt{I_1}$ かつ f が $K[\bar{X}]/I_2$ で逆元を持つようなイデアル I_1 と I_2 にたいして、$I = I_1 \cap I_2$ となっていれば、$I_1 = I : f^m$、$I_2 = I + \langle f^m\rangle$ でなければならない.

定理４からの帰結として、以下が成り立つ.

定理 ５

定理３の (1)、(2) が成り立つとき、 $I = I + \langle f^m\rangle$ と $I : f^m$ の準素分解をそれぞれ

$$I + \langle f^m\rangle = Q_1 \cap \cdots \cap Q_s \quad I : f^m = Q_{s+1} \cap \cdots \cap Q_t$$

とすると $Q_1 \cap \cdots \cap Q_s \cap Q_{s+1} \cap \cdots \cap Q_t$ は I の準素分解になる.

注意事項

定理3の(1)、(2)が成り立たなくても
$I : f^{\infty} = I : f^{m}$ なる最小の m にたいして、

$I = (I + \langle f^{m} \rangle) \cap (I : f^{m})$ は成り立つ.

この分解が自明でない場合、I の準素分解に使えるが、両者の準素分解を合わせたものが、I の準素分解になっているとはかぎらない.

反例
$I = \langle XY, XZ \rangle$、$f = Z$ にたいして、

$I + \langle f \rangle = \langle XY, Z \rangle = \langle X, Z \rangle \cap \langle Y, Z \rangle$(準素分解)

$I : f^{\infty} = I : f = \langle X \rangle$

$I = \langle X, Z \rangle \cap \langle Y, Z \rangle \cap \langle X \rangle$ において $\langle X, Z \rangle$ は冗長.

3 応用

以下のような応用が考えられる.

1. 準素イデアル分解の Dynamic Evaluation

定理3の条件(2)をみたす $f(\bar{X})$ が何らかの形で得られていれば I の準素イデアル分解がより容易になる.

2. Comprehensive Gröbner Systems の適用

パラメーターを持つ I と f に対して Comprehensive Gröbner Systems の計算が有効.
原理的にはイデアルの準素分解が、Comprehensive Gröbner Systems の計算によって、連立代数方程式の解法に帰着される. この方程式をどこの拡大体で解くかによって、準素分解が決まる.

参 考 文 献

[1] Becker, T and Weispfenning, V. (1993). Gröbner Bases. Graduate Texts in Mathematics 141, Springer-Verlag.

[2] Cox, D., Little, J. and O'Shea, D. (1996). Ideals, Varieties and Algorithms – An Introduction to Computational Algebraic Geometry and Commutative Algebra – Second Edition, Springer.

[3] Sato, Y. and Suzuki, A. (2009). Computation of Inverses in Residue Class Rings of Parametric Polynomial Ideals. International Symposium on Symbolic and Algebraic Computation (ISSAC 2009), Proceedings. to appear