数理解析研究所講究録
941巻 1996年 7-14

2.

多項式環上の素イデアル分解について

下山武司
野呂正行
横山和弘 (富士通情報研)

2.1 素イデアル分解と代数拡大体上の因数分解

素イデアル分解の流れ

$\mathbf{Q}[x_1, \ldots, x_n]$: 有理数体 $\mathbf{Q}$ 上の多項式環 ($\mathbf{Q}[X]$ と略記)

I : $\mathbf{Q}[X]$ のイデアル.

一般にイデアル I の radical の素イデアル分解 (prime decomposition) は, 次の様な流れで行われる.

$\boxed{\mathbf{Q}[X] \text{ の イデアル } I}$

$\Downarrow$

$\boxed{\text{イデアルの 0-次元化}}$

$\Downarrow$

$\boxed{\text{イデアルの radical 化}}$

$\Downarrow$

$\boxed{\text{0-次元 radical の素イデアル分解}}$

イデアルの 0-次元化

I の Maximally independent set U に対し $I^e = I\mathbf{Q}(U)[X \setminus U]$: 0-次元イデアル は, $\mathbf{Q}(U)[X \setminus U]$

上の 0-次元イデアル. 又 $I^{ec} = I^e \cap \mathbf{Q}[X]$ と置いたときに

$$\sqrt{I} = \sqrt{I^{ec}} \cap \sqrt{Id(I,f)}$$

を満たす多項式 f が求められる.

これ以降, 体 $\mathbf{K}$ を $\mathbf{K} = \mathbf{Q}(U)$ と置いて, イデアルは $\mathbf{K}[x_1, ..., x_r] = \mathbf{K}[X]$ 上 0-次元の物であると考える.

0-次元イデアルの radical 化

$\mathbf{K}[x_1, ..., x_r]$ 上の 0-次元イデアル I に対し, 各 $i = 1, ..., r$ に付いて $I \cap \mathbf{K}[x_i] = Id(f_i)$ となる x_i の一変数多項式 f_i を取る. この時, 次が言える.

$$I \text{ が radical} \Leftrightarrow \text{全ての } f_i \text{ が } \mathbf{K} \text{ 上既約}$$

代数拡大体上の因数分解

$\mathbf{K}$ の successive extension を考える. $\mathcal{K} = \mathbf{K}(\alpha_1, ..., \alpha_r)$ s.t. $p_1(\alpha_1) = 0$, $p_2(\alpha_1, \alpha_2) = 0, ...,$ $p_r(\alpha_1, ..., \alpha_r) = 0$

$\mathcal{K}$ の上で $\mathbf{K}[x]$ の square-free 多項式 $f(x)$ を分解することは剰余環

$$\mathcal{H} = \mathbf{K}[x_1, ..., x_r, x]/Id(p_1(x_1), ..., p_r(x_1, ..., x_r), f(x))$$

を次の様な体 $\mathcal{L}_i$ への直和分解を与えることと同値である.

$$\text{(A)} \qquad \mathcal{H} = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_m$$

ちなみに各体 $\mathcal{L}_i$ が $\mathbf{K}[x_1, ..., x_r, x]/P_i$ (P_i は maximal ideal) で与えられ,

$$\mathbf{K}(x_1, ..., x_r)[x]P_i = Id(f_i)$$

と書けたとき, $\mathbf{K}(x_1, ..., x_r)[x]$ の多項式 f_i は, f の素因子で,

$$f = f_1 \cdots f_m.$$

剰余環の分解 (A) は, 最も素朴には Norm を計算し, 因数分解すればよい.

$$Norm(f(x-\beta), \alpha_1, ..., \alpha_r) = Id(f(x-\beta), p_1, ..., p_r) \cap \mathbf{K}[x]$$

ただし, β は $\mathcal{K}$ の primitive element

0-次元 radical イデアルの素イデアル分解

これ以降, I は $\mathbf{K}[X]$ 上 0-次元 radical イデアルとする.

I の素イデアル分解 $P_1 \cap ... \cap P_r$ を考える. ここで, P_i は, $\mathbf{K}[X]$ の maximal ideal. これは, $\mathbf{K}[X]/I$ の体の分解

$$(B) \qquad \mathbf{K}[X]/I = \mathbf{K}[X]/P_1 \oplus \ldots \oplus \mathbf{K}[X]/P_r$$

を与えることと同値.

式 (A),(B) を見比べる事で, 次が言える.

$\boxed{\text{0-次元 radical ideal の素イデアル分解}}$

⇕ 本質的に同じ

$\boxed{\text{代数拡大体上の因数分解}}$

$\mathbf{K}[x_1,...,x_r]$ イデアル I の primitive element をそのまま求めるのは非常に重い計算.

⇓

変数 $x_1,...,x_r$ を代数的数と見なし successive factorization したほうが計算効率がよい.

Successive Algebraic Factorization の素イデアル分解への応用

$\mathbf{K}[x_1,...,x_r]$ の 0-次元 radical ideal I を successive algebraic factorization を応用して次の様な素イデアル分解 algorithm が考えられる.

(1)$I\cap\mathbf{K}[x_1]$ の生成元 $g(x_1)$ を求める.

(2)$g(x_1)$ を因数分解し $g=g_1\cdots g_m$. とする. これより

$$I=Id(I,g_1(x_1))\cap\cdots\cap Id(I,g_m(x_1)).$$

(3)ここで $Id(I,g_1(x_1))$ を取る.

α_1 を $g_1(\alpha_1)=0$ を定義多項式とする代数的数とすると, 次の同型が成り立つ

$$\mathbf{K}[x_1,...,x_r]/Id(I,g_1(x_1))=\mathbf{K}(\alpha_1)[x_2,...,x_r]/I|_{x_1=\alpha_1}.$$

$I|_{x_1=\alpha_1}$ を I_1 と置き直すと, I_1 は, $\mathbf{K}(\alpha_1)[x_2,...,x_r]$ の 0-次元 radical イデアルである.

(4)続いて, $I_1\cap\mathbf{K}(\alpha_1)[x_2]$ の生成元 $h(x_2)$ を取る. (h は, α_1 を係数に持つ一変数多項式.)

(5)$h(x_2)$ を代数拡大体 $\mathbf{K}(\alpha_1)$ 上で因数分解する.

$h(x_2)$ の素因子 $h_1\in\mathbf{K}(\alpha_1)[x_2]$ に対し, $h_0(\alpha_2)=0$ を定義多項式に持つ代数的数 α_2 を取ると, 上と同様に次の同型が成り立つ.

$$\mathbf{K}[x_1,...,x_r]/Id(I,g_1(x_1),h_1(x_1,x_2))=\mathbf{K}(\alpha_1,\alpha_2)[x_3,...,x_r]/I|_{x_1=\alpha_1,x_2=\alpha_2}.$$

これを $x_3,...,x_r$ と繰り返せば, 次の様な剰余環の体への分解が得られる.

$$\mathbf{K}[X]/I=\bigoplus_{i=1}^{d}\mathbf{K}(\alpha_{i,1},...,\alpha_{i,r})$$

ただし, $d=\dim_{\mathbf{K}}\mathbf{K}[X]/I$ である.

$\{\alpha_{i,1},...,\alpha_{i,r}\}_{i=1,...,d}$ の定義多項式より I の素イデアル分解が計算できた.

参考:

- Successive Algebraic factorization は, Anai, H. , Noro M. , Yokoyama K. (1995) を参照.
- 有理数体上のイデアルの最少多項式は "Linear solving and Hensel Lifting" によって効率的に計算.

(参照:野呂正行「Generalized Shape Lemma の Hensel 構成による計算」1995.11.21 数解研)

- 有理数体上代数拡大体上の GCD 計算は, Chinese Remainder を利用すると効率的

2.2 $Id(P,s)$ で表されるイデアルの素イデアル分解

背景：下山&横山 による準素イデアルアルゴリズム

Theorem R のイデアル I とその *separator* 系 $S_1,\ldots,S_r$ を取る. 各 i に対し, $\overline{Q}_i = IR_{S_i} \cap R$, $s_i = \prod_{s\in S_i} s$, と置き k_i を $(I : s_i^{k_i}) = IR_{s_i} \cap R$ を満たす自然数とする. $I' = Id(I, s_1^{k_1},\ldots,s_r^{k_r})$ と置くと

(C) $$I = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I',$$

が成り立つ. 更に, $I' = R$ あるいは $\dim(I') < \dim(I)$ のいずれかが成り立つ.

Definition 上の分解 *(C)* を pseudo-primary decompsition と呼ぶ. また, 各 $\overline{Q}_i$ を I の pseudo-primary component, I' を *pseudo-primary decomposition* の remaining component と呼ぶ.

Corollary $\sqrt{I'} = \sqrt{Id(P_1,s_1)} \cap \cdots \cap \sqrt{Id(P_r,s_r)}$.

Theorem *pseudo-primary ideal* I に対し, Q を I の唯一の *isolated primary component*, f を *extractor* とする. k を $IR_f \cap R = (I : f^k)$ を満たす自然数, I' をイデアル $Id(I, f^k)$ とすると $Q = IR_f \cap R$ であり, つぎが成り立つ.

(D) $$I = Q \cap I'.$$

更に, $I' = R$ あるいは $\dim(I) > \dim(I')$ が言える.

Definition I を *pseudo-primary ideal*, P をその *radical* とする. 上の *Theorem* の *decomposition (D)* を I から Q の extraction と呼び, I' を *extraction* の remaining component. と呼ぶ.

Corollary $\sqrt{I'} = \sqrt{Id(P,f)}$.

Special Prime Decomposition of Radicals

pseudo-primary decomposition または extraction の入力イデアル V を取る.

radical $\sqrt{V}$ の素イデアル分解は, 一つの素イデアル P に一つの要素 f を加えたもので生成されるイデアル $Id(P,f)$ の素イデアル分解に帰着できる.

$$\Downarrow$$

$\boxed{Id(P,f) \text{ の形の素イデアル分解を利用.}}$

Procedure (E) $PrimaryDecomposition(I, d)$

Input: A positive integer d and an ideal I such that $\dim(I) \leq d$.

Output: A set $\mathcal{PL}$ of isolated prime divisor of I with dimension d.

begin

  $\mathcal{PL} \leftarrow \{\}$, $J \leftarrow I$

  $\mathcal{U} \leftarrow$ the set of all maximal strongly independent sets

    modulo I with d elements

  for all U in $\mathcal{U}$ do

    If U is not a strongly independent set modulo J

      then continue

    $\mathcal{P}^* \leftarrow$ the set of all prime divisor of I computed in $\mathbf{Q}_U$

    $\mathcal{PL} \leftarrow \{P^* \cap R \mid P^* \in \mathcal{P}^*\} \cap \mathcal{PL}$

    $H \leftarrow$ a Gröbner basis of I with respect to a block

      order $U \ll X \setminus U$

    $f \leftarrow lcm\{HC_U(g) \mid g \in H\}$, $J \leftarrow Id(J, f)$

  return $\mathcal{PL}$

end

Mathematical Background of Specail Procedure

Proposition 素イデアル P_0 と P_0 に含まれない R の要素 s に対しイデアル $Id(P_0, s) \neq R$ の isolated prime は全て次元が等しく $\dim(P_0) - 1$ である.

Lemma I を R のイデアルとし, I の *isolated prime* の中で最大の次元を持つものを P とする. すると, 任意の *admissible order* $<$ に付いて, 全ての P に関する *maximal strongly independent set* U は, また I に関する *maximal strongly independent set* にもなる.

Remark 次の事柄は, *Procedure (E)* の効率のよさを示している.

(1) 有理関数体上の *0*-次元イデアルの *prime decomposition* の回数は, I の *isolated prime* の個数で押さえられる.

(2) 有理関数体上の *0*-次元イデアルの *prime decomposition* は, I に対してのみ行われる.

(3) Remaining ideal J は, 変数が *strong independent* かどうかを確かめるのに用いる. そのチェックには, 任意の *order* に対する *Gröbner* 基底が使える.

Implememtation of Prime Decomposition

次の分解式を用いる.

(F) $\sqrt{Id(I,fg)} = \sqrt{Id(I,f)} \cap \sqrt{Id(I,g)}$

(G) $\sqrt{I} = \sqrt{(IR_f \cap R)} \cap \sqrt{Id(I,f)}$

Implementation of the General Procedure

I を R の任意の ideal とする. ($Q_U := \mathbf{Q}(U)[X \setminus U]$.)

(1)分解式 (F) 及び (G) を用いて, 次の様なイデアル J_i を計算する.

(i) $\sqrt{I} = \sqrt{J_1} \cap \cdots \cap \sqrt{J_s}$,

(ii) J_i の Gröbner 基底の全ての要素は R 上の多項式として既約である.

(iii) J_i に関する maximal strongly independent set U_i に対して $J_i\mathbf{Q}_{U_i} \cap R = J_i$

(2)各 J_i に対し, 全ての prime component を次の様にして求める.

(2.1) $\mathbf{Q}_{U_i}$ の 0-次元イデアル $J_i\mathbf{Q}_{U_i}$ に対しその radical J_i' を計算する.

(2.2) J_i' の prime decomposition を計算する.

(2.3) 各 $P_{i,j}'$ に対し, R への contraction $P_{i,j}$ ($P_{i,j} = P_{i,j}' \cap R$) を計算する.

•各 $P_{i,j}$ は, R の素イデアルでかつ$\sqrt{J_i} = P_{i,1} \cap \cdots \cap P_{i,t_i}$.

(3)$P_{i,j}$ の中で余分な component を取り除く. (component $P_{i,j}$ が余分なものかどうかは, $P_{i,j}$ が別の component $P_{i',j'}$ を真に含むかどうかで判定できる.)

Implementation of the Special Procedure

Procedure をより実用的にするために decomposition (F) を組み込む.

Pre-Procedure: 与えられたイデアル I に (F) を適用するために$\sqrt{I} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_s}$ かつ各 I_i の Gröbner 基底の全ての要素は R の多項式として既約となるイデアル I_i を計算する.

Procedure ($PrimeDecomposition(I)$ (special version))

Input: An ideal I such that every isolated prime divisor has the same dimension.

Output: A set $\mathcal{PL}$ of all prime divisors of $\sqrt{I}$.

begin

  $\mathcal{PL} \leftarrow \{\}$, $d \leftarrow \dim(I)$

  $\mathcal{I} \leftarrow$ the set of all ideals obtained by Pre-Procedure.

  for each J in $\mathcal{I}$

    if $\dim(J) \neq d$ then continue

    if J is prime then $\mathcal{PL} \leftarrow \{J\} \cup \mathcal{PL}$

    else $\mathcal{PL} \leftarrow SpecialPrimeDecomposition(d, J) \cup \mathcal{PL}$

  return $\mathcal{PL}$

end

Remark 経験的には, 非常に多くの例で *pre-procedure decomposition* ですでに *prime decomposition* になっている. 事実, *example* に上げた全ての例において, *pre-procedure* で計算されたイデア

ルは 147 個, そのうちの 142 個 *(96.6%)* がすでに素イデアルであった. すなわち, 多くの場合この *procedure* は, 初めの素イデアル判定のところで終了する.

参考文献

[1]Aho, A.V., Hopcroft, J.E., Ullman, J.D. (1974). *The Design and Analysis of Computer Algorithms.* Addison-Wesley, Reading, MA.

[2]Anai, H. , Noro M. , Yokoyama K. (1995). *Computation of the splitting fields and the Galois groups of polynomials.* MEGA '94.

[3]Atiyah, M.F., MacDonald, I.G. (1969). *Introduction to Commutative Algebra.* Addison-Wesley, Reading, MA.

[4]Alonso, M.E., Mora, T., Raimondo, M. (1990). Local decomposition algorithms. AAECC-8, Springer LNCS **508**, 208-221.

[5]Backelin, J., Fröberg, R. (1991). How we prove that there are exactly 924 cyclic 7-roots. Proceedings of ISSAC'91, ACM Press, 103-111.

[6]Becker, T., Weispfenning, V. (1993). *Gröbner Bases.* Springer-Verlag, New York.

[7]Boege, W., Gebauer, R., Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating Gröbner bases. *J. Symb. Comp.* **1**, 83-98.

[8]Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Doctoral Dissertation Math. Inst. University of Innsbruck, Austria.

[9]Buchberger, B. (1985) Gröbner bases: An algorithmic method in polynomial ideal theory. In: Bose, N.K. (ed.), *Multidimensional Systems Theory*, Reidel, Dordrecht, 184-232.

[10]Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Inventiones Mathematicae*, **110**, 207-235.

[11]Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149-167.

[12]Gräbe H.G. (1994). On factorized Gröbner bases. To appear in Proc. Computer Algebra in Science and Engineering.

[13]Gräbe H.G. (1995). CALI – A REDUCE package for constructive commutative algebra, Version 2.2.1. (anonymous ftp from `aix550.informatik.uni-leipzig.de`)

[14]Kalkbrener, M., Sturmfels, B. (1993). Initial complexes of prime ideals. To appear in *Advances in Mathematics.*

[15]Kredel, H. (1987). Primary ideal decomposition. EUROCAL '87, Springer LNCS **378**, 270-281.

[16]Kredel, H., Weispfenning, V. (1988). Computing dimension and independent sets for polynomial ideals. *J. Symb. Comp.* **6**, 231-247.

[17]Lazard, D. (1985). Ideal bases and primary decomposition: Case of two variables. *J. Symb. Comp.* **1**, 261-270.

[18]Nagata, M. (1962). *Local Rings.* Tracts in Mathematics Number 13, Interscience Publishers, New York.

[19]Noro, M., Takeshima, T. (1992). Risa/Asir – a computer algebra system. Proceedings of ISSAC'92, ACM Press, 387-396. (anonymous ftp from `(133.12.50.13)` `ftp.mm.sophia.ac.jp`, directory `/asir`)

[20]Oaku,T. (1994). Computation of the characteristic variety and the singular locus of a system of differential equations with polynomial coefficients. *Japan J. Indust. Appl. Math.* **11**, 485-497.

[21]Rutman, E.W. (1992). Gröbner bases and primary decomposition of modules. *J. Symb. Comp.* **14**, 483-503.

[22]Shimoyama, T., Yokoyama, K. (1994). Localization and primary decomposition of polynomial ideals. FUJITSU ISIS Research Report, ISIS-RR-94-10E.

[23]Wang, D. (1992). Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. *Computer Aided Geometric Design* **9**, 471-484.

[24]Zariski, O., Samuel, P. (1958/60). *Commutative Algebra*, vols. I, II. Van Nostrand, Princeton, NJ. Reprint Springer-Verlag, New York, 1975/79.