

代数拡大と内容の表計算表示

玉木正一

Algebraic extension and expressions of contents of polynomial by the Excel.

by MASAKAZU Tamaki

1) 代数体について

代数体と言うのは、有理数体 Q に最小多項式と呼ばれる代数方程式

$$f(x) = \sum_{i=0}^n a_i x^{n-i} = 0$$

の根を付け加えた体、及びその代数的な拡大体を言う。

例 $x^2+1=0$ の根を付け加えると

$$Q(\sqrt{-1})$$

有理数体に虚数単位を付け加えた体となる。

2) 代数体の整数

一変数整数係数代数方程式の最高次の項の係数が1の時、これをモニックと言うが、モニックな代数方程式の根となっている時、代数的整数と言う。

上記例の様に、最小多項式の根が、そのまま代数的整数になっている事もある。

例 $x^2+1=0$ の根 $\theta = \pm i$

$$x^2+x+1=0 \text{ の根}$$

$$\theta = \frac{-1 \pm \sqrt{3}i}{2}$$

代数体 k に含まれる整数全体を O_k で表す。 n 次の代数体の整数 ω は n 個の整数 $\omega_1, \dots, \omega_n$ を底として有理整数係数を用いて

$$x = x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$$

と表される。

([1] p13 2.1 定理)

例 整数の積は文字式のように計算して最小多項式でリダクションを行う。

例 最小多項式が $x^2+x+1=0$ の時

$$(1+3\theta+2\theta^2)(2-2\theta+\theta^2)$$

$$= (1+3\theta+2(-1-\theta))(2-2\theta+(-1-\theta))$$

$$= -3\theta^2+4\theta-1$$

$$= -3(-1-\theta)+4\theta-1 = 2+7\theta$$

2次体に対しては上の例のように容易にリダクションができるが、3次体以上では底の決定も難しい。

3) 環のイデアル

上の整数全体を整数環という。 k に於ける整数の集合 I_k が次の2つの条件を満たすとき、「イデアル」という。

$$(1) \alpha \in I_k, \beta \in I_k \text{ ならば } \alpha \pm \beta \in I_k$$

$$(2) \alpha \in I_k \text{ で } \lambda \text{ は任意の整数なるとき、}$$

$$\lambda \alpha \in I_k$$

従って $\alpha_1, \alpha_2, \dots, \alpha_r$ が I_k に属するとき

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_r\alpha_r$$

は I_k に属する。

([1] p16 2.2 「イデアル」)

それを、 $\alpha_1, \alpha_2, \dots, \alpha_r$ から生ずるイデアルといい、 $(\alpha_1, \alpha_2, \dots, \alpha_r)$ と表す。

I_k は O_k の Z 部分加群になるので底を有する。

それを $I_k = [\alpha_1, \alpha_2, \dots, \alpha_r]$ と書く。

4) イデアルの加法、乗法

イデアル $A_k = (\alpha_1, \alpha_2, \dots, \alpha_r)$ 、

$$B_k = (\beta_1, \beta_2, \dots, \beta_r)$$

の和は

$$A_k + B_k = (\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_r)$$

積は

$$A_k \cdot B_k = \Sigma \alpha_i \beta_i$$

と書ける。

5) 整数環の基底

2次体 $Q(\sqrt{D})$ の整数環の基底はよく知られているように、

$D \equiv 2, 3 \pmod{4}$ の場合は

全ての整数は $a + b\sqrt{D}$ の形に表されるので、基底は

$$\left[1, \sqrt{D}\right] \quad \text{となる。}$$

$D \equiv 1 \pmod{4}$ の場合は

全ての整数は $a + b\frac{1+\sqrt{D}}{2}$ の形に表されるので、基底は

$$\left[1, \frac{1+\sqrt{D}}{2}\right] \quad \text{となる。}$$

([2] p51 標準的な底)

3次体の時は容易ではなく、判別式の計算も複雑になる。

6) 代数体の判別式

k を n 次の代数体とする。 k の元 α の Q に関する n 個の共約を、 $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$ とする。

k の n 個の組 $(\alpha_1, \alpha_2, \dots, \alpha_n)$ に対して

$$\Delta[\alpha_1, \alpha_2, \dots, \alpha_n] = \begin{vmatrix} \alpha_1^{(1)} & \dots & \alpha_n^{(1)} \\ \alpha_1^{(2)} & \dots & \alpha_n^{(2)} \\ \dots & \dots & \dots \\ \alpha_1^{(n)} & \dots & \alpha_n^{(n)} \end{vmatrix}$$

$$d[\alpha_1, \alpha_2, \dots, \alpha_n] = \Delta[\alpha_1, \alpha_2, \dots, \alpha_n]^2$$

$$\text{特に } [\alpha_1, \alpha_2, \dots, \alpha_n] = [\omega_1, \omega_2, \dots, \omega_n]$$

の時 体の判別式 $d(k)$ と書く

$$\text{又、} [\alpha_1, \alpha_2, \dots, \alpha_n] = [1, \theta, \theta^2, \dots, \theta^{n-1}]$$

の時 方程式の判別式 $d(f)$ と書く

([3] p119-121 定義)

最小多項式が $x^3 - A$ の時

$k = Q[\sqrt[3]{A}]$ を純3次体と言う。

$A = mn^2$ ($m, n = 1$ とすると

$$1 \quad \theta = \sqrt[3]{mn^2} \quad \tilde{\theta} = \sqrt[3]{m^2n}$$

任意の整数は

$$\alpha = a + b\theta + c\tilde{\theta} \quad a, b, c \in Q$$

の形に表される。

7) 純3次体の基底と判別式 ([3] p119-121)

([3] p115 例1. 4)

m, n が平方因子を持たないとする。 $3 \nmid mn$ なら整数の基底として

$$1, \theta = \sqrt[3]{mn^2}, \tilde{\theta} = \sqrt[3]{m^2n}$$

をとる事が出来る。

例 $m=15 \quad n=1$ の時 整数の積のリダクションは表計算を用いて行える。

	$m=$	$n=$	$mn=$
	15	1	15
	1	θ	$\tilde{\theta}$
α	2	3	1
β	5	2	2
$\alpha\beta$	130	49	15

例 $m=3 \quad n=2$ の時 整数の積のリダクションについても表計算を用いて行える。

	$m=$	$n=$	$mn=$
	3	2	6
	1	θ	$\tilde{\theta}$
α	1	2	1
β	-1	2	2
$\alpha\beta$	35	6	9

8) 一般の3次体の判別式と基底

(6) で定義した最小方程式の判別式は

$$f(x) = ax^3 + bx^2 + cx + d = 0$$

に対して

$$d(f) =$$

$$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

となる。ところが

$$d(f) = m(\theta)^2 d(k)$$

平方数なる仮因子を持つ場合がある。

仮因子を持つときには

$$1, \theta, \theta^2$$

なる形の基底を持てない。

その時には別の方法で基底を作らなければならない。

例 デデキントの例

$$f(x) = x^3 + x^2 - 2x + 8 = 0$$

$$d(f) = -2^2 \cdot 503$$

$$1 \text{ つの根を } \alpha, \beta = \frac{4}{\alpha}$$

とすると $1, \alpha, \beta$

を基底に持ち相互関係は

$$\begin{cases} \alpha^2 = 2 - \alpha - 2\beta \\ \beta^2 = -2 - 2\alpha + \beta \\ \alpha\beta = 4 \end{cases}$$

例 整数の積のリダクションは次のように表計算出来る。

	1	α	β
ζ	1	1	3
η	2	3	1
$\zeta\eta$	42	-4	4

仮因子を持たない場合も必ずしも

$$1, \theta, \theta^2$$

なる形の基底を持つとは限らないが、次の例のばあい

は、上の形の基底を持つ。

例 $f(x) = x^3 + ax + 1$ なる形の時

判別式は

$$d(k) = d(f) = -(4a^3 + 27)$$

となる。

$a = 1, 2, 4, 5, 7, 10$ に対して

$$d(f) = -31, -59, -283, -527 = -17 \times 31$$

$$-1329, -4027$$

となり、

基底は $1, \theta, \theta^2$ となる。

例 $a = 2$ の時 整数の積のリダクションは次のように表計算される。

	1	θ	θ^2
α	2	1	3
β	5	-2	2
$\alpha\beta$	14	3	5

([4] p121 例 3. 2)

9) アイゼンシュタイン型の 3 次体

k を n 次代数体とする。

$$d[\alpha_1, \alpha_2, \dots, \alpha_n] = d(f) \text{ の時}$$

$[\alpha_1, \alpha_2, \dots, \alpha_n]$ は基底となる。

この公式を用いてアイゼンシュタイン型の最小方程式を持つ 3 次体の整数環の基底を求めてみよう。

有理整係数多項式

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$$

の係数に、ある素数 p について

$$p \mid a_i \quad p^2 \nmid a_n \quad a_i \in \mathbb{Z}$$

を満たすとき $f(x)$

は既約でアイゼンシュタイン型既約方程式という。

例 次の例では全て

$1, \theta, \theta^2$ の基底を持つ

$$\begin{aligned}x^3-2x+2 &= 0 & d &= -76 = -2^2 \times 19 \\x^3+4x+2 &= 0 & d &= -364 = -2^2 \times 7 \times 13 \\x^3-4x+2 &= 0 & d &= 148 = 2^2 \times 37\end{aligned}$$

これらは カルダーノの解法に近い形をしている。

更に

$$\begin{aligned}x^3-8x+2 &= 0 & d &= 1940 = 2^2 \times 5 \times 97 \\x^3+3x+3 &= 0 & d &= -351 = -3^3 \times 13 \\x^3-3x+3 &= 0 & d &= -135 = -3^3 \times 59 \\x^3+6x+3 &= 0 & d &= -1107 = -3^3 \times 41 \\x^3-6x+3 &= 0 & d &= 621 = 3^3 \times 23 \\x^3+9x+3 &= 0 & d &= -3159 = -3^2 \times 17 \times 23 \\x^3-9x+3 &= 0 & d &= 2673 = 3^5 \times 11 \\x^3+5x+5 &= 0 & d &= -1175 = -5^2 \times 47 \\x^3-5x+5 &= 0 & d &= -175 = -5^2 \times 7 \\x^3+7x+7 &= 0 & d &= -2695 = -7^2 \times 5 \times 11 \\x^3-7x+7 &= 0 & d &= 49 = 7^2 \\x^3+2x+6 &= 0 & d &= -1004 = -2^2 \times 251 \\x^3-2x+6 &= 0 & d &= -940 = -2^2 \times 5 \times 47 \\x^3+4x+6 &= 0 & d &= -1228 = -2^2 \times 307 \\x^3-4x+6 &= 0 & d &= -716 = -2^2 \times 179 \\x^3+6x+6 &= 0 & d &= -1836 = -2^2 \times 3^3 \times 17 \\x^3-6x+6 &= 0 & d &= -108 = -2^2 \times 3^3 \\x^3+9x+6 &= 0 & d &= -243 = -3^5\end{aligned}$$

等で $1, \theta, \theta^2$ の基底を持つ。

例として $x^3-3x+3=0$ の整数の積のリダクションを求めてみよう。

	1	θ	θ^2
α	2	1	3
β	5	-2	2
$\alpha\beta$	22	-29	35

1 0) 2 次体のイデアルの積

2つのイデアル

$$A = [\alpha_1, \alpha_2, \dots, \alpha_n] \quad B = [\beta_1, \beta_2, \dots, \beta_n]$$

の積 AB は $\alpha_i \beta_j$

の全ての組み合わせからなるイデアルである。

([5] p109 定義 4)

例

$$\begin{aligned}&(2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) \\&= (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5}) \\&= (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}) \\&= (1+\sqrt{-5})\end{aligned}$$

1 1) 内容 (Inhalt) の定義

k が代数体 $f(x), g(x), h(x)$ が m 個の変数 $x_1, x_2, \dots, x_m$ なる k 係数の多項式で、同類項は整頓されている。このとき $f(x), g(x), h(x)$ の係数で生成される k のイデアルが A, B, C であるとする。

$f(x) \times g(x) = h(x)$ ならば

$AB = C$ である。

1 0) の例

$$\begin{aligned}&\{2x + (1+\sqrt{-5})\} \{3x + (1+\sqrt{-5})\} \\&= 5x\sqrt{-5} + 2\sqrt{-5} + 6x^2 + 5x - 4 \\&= 6x^2 + 5(1+\sqrt{-5}), -4+2\sqrt{-5} \\&\text{より } (6, 5(1+\sqrt{-5}), -4+2\sqrt{-5}) \\&= (6, 5(1+\sqrt{-5}), 2+2\sqrt{-5}) \\&= (6, 1+\sqrt{-5}) = (1+\sqrt{-5})\end{aligned}$$

1 2) 内容によるイデアルの分解

逆に言えばイデアルが因数分解される時は、既にそれを内容とするある多項式が、因数分解されている。内容が一致する多項式を見つければ良い事になる。

定理 k を n 次代数体、 θ を $k = Q(\theta)$ となる整数。

$f(x) \in Z\{x\}$ を θ の Q に関する最小多項式とする。

d を k の判別式 $d(f)$ を θ の判別式とし

$d(f) = m(\theta)^2 d$ $m(\theta) \in Z\{x\}$ とする。

$m(\theta)$ は仮因子で p を $m(\theta)$ と素である有理素数とする時、多項式 $f(x)$ の $\text{mod } p$ に関する規約多項式の

分解が

$$f(x) \equiv p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_g(x)^{e_g} \pmod{p}$$

ならば p の k に於ける素因数分解は

$$(p) = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g} \quad p_i^{e_i} = (p, p(\theta))$$

となる。 $p_i^{e_i}$ の次数は多項式 $p_i(x)$ の次数に等しい。

例 純3次体 $Q(\sqrt[3]{7})$ に於いて $1, \theta, \theta^2$ は整数基底になる。

素数 $p = 2, 3, 5, 7$ について (p) の因数分解は

$$f(x) = x^3 - 7 \text{ の } \pmod{p} \text{ での分解から}$$

$$x^3 - 7 \equiv x^3 - 1 = (x-1)(x^2+x+1) \pmod{2}$$

$$(2) = p_1 p_2 \quad p_1 = (2, \theta - 1)$$

$$p_2 = (2, \theta^2 + \theta + 1)$$

$$x^3 - 7 \equiv (x+2)^3 \pmod{3}$$

$$(3) = p_1 p_2^2 \quad p_1 = (3, \theta - 1)$$

$$Np_2 = 3$$

$$x^3 - 7 \equiv (x+2)(x^2 - 2x - 1) \pmod{5}$$

$$= x^3 - 5x - 2 \pmod{5}$$

$$(5) = p_1 p_2 \quad p_1 = (5, \theta + 2)$$

$$p_2 = (5, \theta^2 - 2\theta - 1)$$

$$(7) = p_1^3 \quad Np_1 = 7$$

例 カルダーノ型3次体最小多項式が

$$f(x) = x^3 - 2x + 5 = 0$$

$Q(\theta)$ に於いて $1, \theta, \theta^2$ は整数基底になる。

$d(f) = -643$ で素数となっている。

素数 $p = 2, 3, 5$ について

(p) の因数分解は $f(x) = x^3 - 2x + 5$ の $\pmod{p}$ での

分解から

$$x^3 - 2x + 5 \equiv (x-1)(x^2+x+1) \pmod{2}$$

$$(2) = p_1 p_2 \quad p_1 = (2, \theta - 1)$$

$$p_2 = (2, \theta^2 + \theta + 1)$$

$$x^3 - 2x + 5 \equiv (x+1)(x^2 - x + 2) \pmod{3}$$

$$(3) = p_1 p_2 \quad p_1 = (3, \theta + 1)$$

$$p_2 = (3, \theta^2 - \theta + 2)$$

$$x^3 - 2x + 5 \equiv x(x^2 - 2) \pmod{5}$$

$$(5) = p_1 p_2 \quad p_1 = (5, \theta)$$

$$p_2 = (5, \theta^2 - 2)$$

1 3) 結論

イデアルの計算は煩雑であるが表計算を用いるとリダクションがこなせるようになる。マクロ等でソフトを組めば、より実現性の高い物となることであろう。

1 4) 参考文献

- [1] 高木貞治 代数的整数論
- [2] 武隈良一 2次体の整数論
- [3] ファン・デル・ヴェルデン 現代代数学1
- [4] 藤崎源二郎 代数的整数論入門上
- [5] 藤崎源二郎 代数的整数論入門下
- [6] 久保田富雄 整数論入門

(受理年月日 1997年9月30日)