十六夜環の既約元について

染谷　匠

高木　俊一

1. **目的**

2, 3元体を係数体Fとする多項式環において

$R = F[X]$ ：十五夜環

$R_0 = F[X^2, X^3]$ ：十六夜環

十五夜環では既約元分解は一意的。

十六夜環では一意的でない。

例

$$X^6 = (X^2)^3 = (X^3)^2$$

　このように分解が二通り以上あるものが存在する。
よって十六夜環においては素元でない既約元が存在する。

十六夜環において既約元への分解が何通り出てくるか調べた。

ただし、今回は6次以下。

2. **定義**

整域Rにおいて

①**単元**uとは、あるvがあり　$uv = 1$　となること。

②**可約元**とは、0でなく単元でないα, βの積として表せる元。

③0でなく単元でなく、しかも可約でない元を**既約元**という。

④xが**素元**であるとは、

$\alpha\beta \in (x)$なら$\alpha \in (x)$または$\beta \in (x)$

即ち、$\alpha\beta = x\gamma$なら$\alpha = x\delta$または$\beta = x\delta'$となる。

3. **方法**

3.1. Prolog**を使う**. 多項式をリストによって次のように表現する。

多項式：$a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n$ を
リスト：$[a_0, a_1, \cdots, a_{n-1}, a_n]$ で表す。

多項式の四則演算に対応したリストの四則演算のプログラムを作製。

3.2. **十五夜環での既約元.** 四則演算をつかい、最小約元がもとの元と同じとき既約元である。

Table 1

2元体	全ての元(個)	既約元(個)
1次	2	2
2次	4	1
3次	8	2
4次	16	3
5次	32	6
6次	64	9
合計	126	23

Table 2

3元体	全ての元(個)	既約元(個)
1次	3	3
2次	9	3
3次	27	8
4次	81	18
5次	243	48
6次	729	116
合計	1092	196

3.3. **十六夜環での既約元**. 十六夜環では割り算が一般にはできないので、可約元をまずつくり、その残りのうち0でも定数でもない元が既約元である。

Table 3

2元体	全ての元(個)	既約元(個)
2次	2	2
3次	4	4
4次	8	5
5次	16	8
6次	32	13
合計	62	32

Table 4

3元体	全ての元(個)	既約元(個)
2次	3	3
3次	9	9
4次	27	21
5次	81	54
6次	243	139
合計	363	226

3.4. **十六夜環での既約元分解**. 6次の元で二通りの分解ができるものは次の通り

2元体では5個

Table 5

X^6	$= (X^2)^3$	$= (X^3)^2$
$X^6 + 1$	$= (X^2 + 1)(X^4 + X^2 + 1)$	$= (X^3 + 1)^2$
$X^6 + X^4$	$= (X^2)^2(X^2 + 1)$	$= (X^3 + X^2)^2$
$X^6 + X^5$	$= X^2(X^4 + X^3)$	$= X^3(X^3 + X^2)$
$X^6 + X^5 + X^3 + X^2$	$= (X^2 + 1)(X^4 + X^3 + X^2)$	$= (X^3 + 1)(X^3 + X^2)$

3元体では14個

Table 6

X^6	=	$(X^2)(X^2)(X^2)$	=	$(X^3)(X^3)$
$X^6 + 2$	=	$(X^2 + 2)(X^2 + 2)(X^2 + 2)$	=	$(X^3 + 1)(X^3 + 2)$
$X^6 + 2X^4$	=	$(X^2)(X^2)(X^2 + 2)$	=	$(X^3 + X^2)(X^3 + 2X^2)$
$X^6 + 2X^4 + X^2 + 2$	=	$(X^2 + 2)(X^4 + 1)$	=	$(X^3 + X^2 + 1)(X^3 + 2X^2 + 2)$
$X^6 + X^5$	=	$(X^2)(X^4 + X^3)$	=	$(X^3)(X^3 + X^2)$
$X^6 + X^5 + 2X^3 + X^2 + 1$	=	$(X^2 + 2)(X^4 + X^3 + X^2 + 2)$	=	$(X^3 + 1)(X^3 + X^2 + 1)$
$X^6 + X^5 + 2X^3 + 2X^2$	=	$(X^2 + 2)(X^4 + X^3 + X^2)$	=	$(X^3 + 2)(X^3 + X^2)$
$X^6 + X^5 + X^4$	=	$(X^2)(X^4 + X^3 + X^2)$	=	$(X^3 + 2X^2)(X^3 + 2X^2)$
$X^6 + X^5 + X^4 + 2X^3 + X^2$	=	$(X^2 + 2)(X^4 + X^3 + 2X^2)$	=	$(X^3 + 2X^2)(X^3 + 2X^2 + 2)$
$X^6 + 2X^5$	=	$(X^2)(X^4 + 2X^3)$	=	$(X^3)(X^3 + 2X^2)$
$X^6 + 2X^5 + X^3 + X^2 + 1$	=	$(X^2 + 2)(X^4 + 2X^3 + X^2 + 2)$	=	$(X^3 + 2)(X^3 + 2X^2 + 2)$
$X^6 + 2X^5 + X^3 + 2X^2$	=	$(X^2 + 2)(X^4 + 2X^3 + X^2)$	=	$(X^3 + 1)(X^3 + 2X^2)$
$X^6 + 2X^5 + X^4$	=	$(X^2)(X^4 + 2X^3 + X^2)$	=	$(X^3 + X^2)(X^3 + X^2)$
$X^6 + 2X^5 + X^4 + X^3 + X^2$	=	$(X^2 + 2)(X^4 + 2X^3 + 2X^2)$	=	$(X^3 + X^2)(X^3 + X^2 + 1)$

以上のような分解ができることから、
十六夜環では既約であっても素元ではない元が存在することがわかった。

Lemma

$f \in R_0, f$ は R で素元 $\Rightarrow$ f は R_0 でも素元

Lemmaの証明

$f \in R_0 \subset R$ をとり、f は R で素元とする。
$\alpha, \beta \in R_0$ によって、
$\alpha\beta \in (f)$ とすると、(f) は R で素イデアルだから $\alpha \in (f)$ or $\beta \in (f)$
よって $f = \alpha p$ or $f = \beta q$ $(p, q \in R)$ となる。

次に、$p, q \in R_0$を示す。

実際、

$f = 1 + a_2X^2 + \cdots + a_nX^n$

$\alpha = 1 + b_2X^2 + \cdots + b_nX^n$

$p = 1 + c_1X + \cdots + c_nX^n$

とおくと、$f = \alpha p = 1 + c_1X + (c_2 + b_1)X^2 + \cdots \in R_0$

なので、

$c_1 = 0$となるから$p \in R_0$

よって　R_0において$\alpha \in (f)$　//

以上のことより、十六夜環の既約元は、以下の三種類のように分類ができる。

松：十六夜環で素元かつ十五夜環でも素元
竹：十六夜環では素元だが十五夜環では可約
梅：十六夜環で素元ではない

以前の、分解が二通り以上のものにおいて、一方にしか出ない既約元は梅です。

6次の元の既約性を判断するには、
9次の元まで分解することによって出来ました。

その結果、竹はなく、松か梅でした。

4. **考察**

なぜ竹が出てこないのかを考えてみます。

たとえば、$f = X^4 + X^3 \in R_0$は$X^4 + X^3 = (X + 1)X^3$
と分解できますが、
$X + 1 \notin R_0$なのでR_0ではこれ以上分解できません。
しかしここで$g = X^2 \in R_0$をとってくると、
$fg = (X^4 + X^3)X^2 = ((X + 1)X^3)X^2$
$= ((X + 1)X^2)X^3 = (X^3 + X^2)X^3$
$(X^3 + X^2), X^3 \in R_0$
となります。

よって、fに対して適当な$g \in R_0$をもってくると別の分解ができるようになります。
したがって、

$$f = f_1 f_2$$

とした時に、仮に$f_1 \notin R_0$であっても、
適当なhをとってきて、

$$f_1 h \in R_0$$

となるようなhを常にとってくることができるのではないかと考えました。

5. **証明**

竹が出てこないことの証明

$R_0 = F[X^2, X^3] \subset R = F[X], (F = \text{体})$
☆$f \in R_0$は素元、Rでは可約とする。このとき矛盾することを示す。

まず、定数項が存在する場合において

$f = 1 + a_2X^2 + \cdots$　はRで可約なので分解してよい。

よって、$f = f_1 f_2$とすると、

$$f_1 = 1 + b_1 X + \cdots$$
$$f_2 = 1 + c_1 X + \cdots$$

となり、$c_1 = -b_1 (\neq 0)$　である。

$f(X) = f_1(X) f_2(X)$でXを$-X$に置き換えると

$f(-X) = f_1(-X) f_2(-X)$

そこで　$\overline{f}(X) = f(-X)$　とおくと　$\overline{f} = \overline{f_1}\,\overline{f_2}$

$f\overline{f} = f_1 \overline{f_1} f_2 \overline{f_2}$　とすると　$f_1\overline{f_1}, f_2\overline{f_2} \in R_0$　になる。

fは素元なので、$\varphi \in R_0$があり　$f_1\overline{f_1} = f\varphi$　と書ける。

よって　$f\overline{f} = f\varphi f_2\overline{f_2}$

$\overline{f} = \varphi f_2\overline{f_2}$

また$\overline{f}$も素元である。

よって$\psi \in R_0$により、

①$f_2\overline{f_2} = \overline{f}\psi$　又は　②$\varphi = \overline{f}\psi$　と書ける。

①ならば　$\overline{f} = \varphi\overline{f}\psi$　よって　$\varphi\psi = 1$

これよりφ, ψは単元となるので、

$\varphi = \psi = 1$　としてよい。

よって　$f = f_1\overline{f_1}$　となる。

②ならば　$\bar{f} = \bar{f}\psi f_2 \bar{f_2}$により、$1 = \psi f_2 \bar{f_2}$

f_2は単元になり、定数になる。

よって$f \in R_0$で素元なら　$f_1 \in R$により

$f = f_1 \bar{f_1}$　と書ける。

この時

Lemma

$f_1 \in R$　既約なら　$f_2 \neq f_1, \bar{f_1}$(f_2はRで既約)　があり、

(定数倍の差は許されない)

$g = f_1 f_2 \in R_0$　のようにとれる。

Lemmaの証明

$f_1 \in R$　既約とする。$\varphi = f_1\overline{f_1}$　は素元でないことを証明する。

①$f_1 = 1 - aX$　のとき$(a \neq 0)$

$f_2 = 1 + aX + a^2X^2$　とおく。

$g = f_1f_2 = 1 - a^3X^3 \in R_0$　gは既約

$g\overline{g} = f_1\overline{f_1} \cdot f_2\overline{f_2} = \varphi\varphi_2$

$f_1\overline{f_1} = 1 - a^2X^2, \quad f_2\overline{f_2} = 1 + a^2X^2 + a^4X^4$

$\overline{g}$も既約であり、$f_1\overline{f_1}$も既約である。

また、$f_2\overline{f_2}$はR_0においてgで割れないので、

この分解は一意的でない。

よって、$f_1\overline{f_1}$は素元でない。

② $f_1 = 1 - aX + \cdots$　($a \neq 0$,　2次以上)

$f_2 = 1 + aX$　とおく。

$g = f_1 f_2 \in R_0$

$g\bar{g} = f_1\bar{f_1} \cdot f_2\bar{f_2} \in R_0$

$\varphi = f_1\bar{f_1}$が素元なら、

$g = \varphi p$,　$\bar{g} = \bar{\varphi}\bar{p}$となる。

よって、

$\varphi p\bar{g} = \varphi\varphi_2$,　$\varphi_2 = p\bar{g}$,

$\varphi_2 = f_2\bar{f_2}$,　$\varphi_2 = 1 - a^2X^2$　は2次式

gは3次以上なので矛盾。　//

　すると　$g\overline{g} = f_1\overline{f_1}f_2\overline{f_2}$　と二通りに分けられる。
よって、$f = f_1\overline{f_1} \in R_0$　は素元でない既約元になり、
仮定に反する。

次に、定数項が存在しない場合において
$f = f_1f_2 = X^p(1 + a_1X + a_2X^2 + \cdots)$　$(p = 2, 3)$ とすると、

$$f_1 = X^p$$
$$f_2 = 1 + a_1X + a_2X^2 + \cdots$$

と分解できるので、

$$f\overline{f} = f_1\overline{f_1} \cdot f_2\overline{f_2}$$

とすると、$f_1\overline{f_1}, f_2\overline{f_2} \in R_0$ となり、同様に証明できる。

よって、竹は存在しない。

6. まとめ

- 十六夜環の既約元は松と梅の二種類に分けられる。
- 可約元も分解が二つ以上分けられる場合がある。
  6次においては一つと二つに分けられる。
  そして数は以下のようになる。

Table 7

2元体	2次	3次	4次	5次	6次	計
松	0	1	1	3	4	9
梅	2	3	4	5	9	23
可約元	0	0	3	8	19	30

Table 8

3元体	2次	3次	4次	5次	6次	計
松	1	2	6	16	38	63
梅	2	7	15	38	101	163
可約元	0	0	6	27	104	137

7. これからの展望

・一般にp元体n次で判別できるようにする。

・十六夜環の既約元の個数がわかる公式を求める。

・可約元で分解が一つと二つ以上の分類と、
その理由について。

・梅を紅梅、白梅に分類する。

紅梅：$f = g\bar{g}$　($f \in R_0$で既約,$g \in R$で既約)
で表せるもの

白梅：紅梅以外の梅

例　2元体において

$f = 1 + X^2 = (1 + X)(1 - X)$　よって紅梅

$f = 1 + X^3 = (1 + X)(1 - X + X^2)$　よって白梅