判別式と終結式

増田佳代・宮西正宜

1 変数の多項式を 1 次式の積に分解したり，また，その逆の操作をすることは高校で繰り返し学習したことである．このような操作は方程式の解を求めるのに必要であるが，また，代数学においてさまざまな定理と結びついている．まず，判別式について解説しよう．

1　判別式

1.1　2 次式の判別式

実数全体の集合を $\mathbb{R}$, 複素数全体の集合を $\mathbb{C}$ で表す．これらは加減乗除が定義された集合であり，それぞれ，**実数体**，**複素数体**とよぶ．一般に，加減乗除の四則演算で閉じた集合を**体**というが，その定義については章末の説明を参照されたい．

K を体として，K に係数をもつ変数 x の多項式

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \quad \forall a_i \in K$$

について，$a_0 \neq 0$ ならば，$f(x)$ は**次数** n の多項式といい，簡単に，n **次式**という．$n = \deg f(x)$ と書く．このとき，a_0 は**最高次の係数**という．K-係数の多項式全体の集合を $K[x]$ で表す．2 つの多項式 $f(x)$ と $g(x)$ を加えたり，積を取ったりすることができる．ただし，2 つの多項式 $f(x)$ と $g(x)$ が与えられたとき，$g(x) \neq 0$ としても，一般に $f(x)$ を $g(x)$ で割り切ることはできないから，除法は定義されない．

さて，2 次式

$$f(x) = ax^2 + bx + c, \quad a \neq 0 \tag{1}$$

を考えよう．方程式 $f(x) = 0$ が解 α をもてば，$f(\alpha) = 0$ であるから，除法の定理によって，

$$f(x) = a(x - \alpha)(x - \beta)$$

とかけて，もう 1 つの解 β もみつかる．さらに，解と係数の間には

$$\alpha + \beta = -\frac{b}{a}, \quad \alpha\beta = \frac{c}{a}$$

という関係がある．ここで，2 つの解 α と β が一致する条件を考えてみよう．高校では，(1) の判別式を

$$D = b^2 - 4ac$$

と定義するとき，$\alpha = \beta$ **となる必要十分条件は** $D = 0$ **である**，という判定条件を学習している．

しかし，直感的には重解をもつ必要十分条件は $\alpha - \beta = 0$ となることである．ここで，$\Delta = \alpha - \beta$ とおいて $f(x)$ の**差積**または**等差式**という．しかし，Δ は α と β を入れ替えると，$-\Delta$ となって，符合は一定ではない．そこで Δ^2 を考えると，その符号は α と β の入れ替えで変わらない．

さて，

$$\begin{aligned} \Delta^2 = (\alpha - \beta)^2 &= (\alpha + \beta)^2 - 4\alpha\beta \\ &= \frac{b^2}{a^2} - \frac{4ac}{a^2} = \frac{1}{a^2}\left(b^2 - 4ac\right) \end{aligned}$$

となるから，$a^2\Delta^2 = D$ という関係がある．

$f(x) = 0$ が重解をもつとき，$f(x) = a(x - \alpha)^2$ とかけて，その導関数は $f'(x) = 2a(x - \alpha)$ となる．すなわち，$f(x) = 0$ と $f'(x) = 0$ は共通解 $x = \alpha$ をもつ．もとの方程式に戻ると，

$$f(x) = ax^2 + bx + c \quad と \quad f'(x) = 2ax + b$$

が共通因子を持つことである．$f'(x) = 0$ を解くと，$x = -\dfrac{b}{2a}$ となり，この解を $f(x)$ に代入すると

$$\begin{aligned} f\left(-\frac{b}{2a}\right) &= \frac{b^2}{4a} - \frac{b^2}{2a} + c = -\frac{b^2}{4a} + c \\ &= -\left(\frac{b^2 - 4ac}{4a}\right) = -\frac{D}{4a} \end{aligned}$$

となる．よって，$f(x) = 0$ が重解をもつ条件が $D = 0$ である，ことが示された．

また，後に終結式のところで述べることがらであるが，次の $f(x)$ と $f'(x)$ の係数を並べた行列式の値も D に関係している．

$$\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = 4a^2c - ab^2 = -a(b^2 - 4ac) = -aD$$

ここで，上式の左辺は 3 次式 $f(x)$ とその導関数 $f'(x)$ の x に関する**終結式 (resultant)** と呼ばれるもので，$\mathrm{Res}_x(f(x), f'(x))$ と表す．その定義と結果は次の節で詳しく説明する．

1.2 3 次式と 4 次式の判別式

以上のような関係が，3 次式の場合にどうなるかを考えてみよう．3 次式を

$$f(x) = ax^3 + bx^2 + cx + d, \quad a \neq 0 \tag{3}$$

と置いて，

$$f(x) = a(x - \alpha)(x - \beta)(x - \gamma)$$

と分解したとしよう．ただし，

$$\alpha+\beta+\gamma=-\frac{b}{a},\quad \alpha\beta+\beta\gamma+\gamma\alpha=\frac{a}{c},\quad \alpha\beta\gamma=-\frac{d}{a}$$

である．このような分解は，K が複素数体であれば，存在することが知られている．$f(x)$ の差積を

$$\Delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$$

とおく．さらに，判別式を $D=\Delta^2$ で定義して，D を $f(x)$ の係数で表してみよう．

実は，D は α,β,γ の順番を入れ替えても変わらない式であり，そのような式は，$\alpha+\beta+\gamma, \alpha\beta+\beta\gamma+\gamma\alpha, \alpha\beta\gamma$ の式として表されることが知られている．計算は複雑で手計算ではあきらめてしまいそうになる．そこで Maple を使って計算を実行すると次のようになる．

$$\begin{aligned}
D &:= -2\alpha^4\beta\gamma+2\alpha^2\gamma^3\beta+2\alpha\beta^2\gamma^3-2\beta^4\alpha\gamma+2\alpha^2\beta^3\gamma+2\alpha^3\gamma\beta^2+2\alpha\beta^3\gamma^2\\
&\quad +2\alpha^3\gamma^2\beta-6\alpha^2\gamma^2\beta^2-2\alpha\beta\gamma^4+\alpha^4\beta^2+\alpha^4\gamma^2-2\alpha^3\gamma^3+\alpha^2\gamma^4-2\alpha^3\beta^3+\beta^4\alpha^2\\
&\quad +\beta^4\gamma^2-2\beta^3\gamma^3+\beta^2\gamma^4\\
&= (\alpha+\beta+\gamma)^2(\alpha\beta+\beta\gamma+\alpha\gamma)^2-4(\alpha+\beta+\gamma)^3\alpha\beta\gamma-4(\alpha\beta+\beta\gamma+\alpha\gamma)^3\\
&\quad +18(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\alpha\gamma)\alpha\beta\gamma-27\alpha^2\beta^2\gamma^2\\
&= \frac{1}{a^4}(b^2c^2-4b^3d-4ac^3+18abcd-27a^2d^2) \qquad (4)
\end{aligned}$$

1.2.1 Maple の計算についての注意

上の計算で最初の等式は $D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ を Maple で展開させて得られる．しかし，2 番目の等式を Maple で得るのは難しい．そこで，(2) 式を拡張した次の式が成り立つと仮定する．

$$-aD=\begin{vmatrix} a & b & c & d & 0\\ 0 & a & b & c & d\\ 3a & 2b & c & 0 & 0\\ 0 & 3a & 2b & c & 0\\ 0 & 0 & 3a & 2b & c \end{vmatrix} \qquad (5)$$

$a=1$ の場合に，上の行列式の値を求めて

$$D=b^2c^2-4b^3d-4c^3+18bcd-27d^2$$

を導く．$a=1$ ならば，$b=-(\alpha+\beta+\gamma), c=\alpha\beta+\beta\gamma+\gamma\alpha, d=-\alpha\beta\gamma$ が成立するから，上式に代入して，

$$\begin{aligned}
D &= (\alpha+\beta+\gamma)^2(\alpha\beta+\beta\gamma+\alpha\gamma)^2-4(\alpha+\beta+\gamma)^3\alpha\beta\gamma-4(\alpha\beta+\beta\gamma+\alpha\gamma)^3\\
&\quad +18(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\alpha\gamma)\alpha\beta\gamma-27\alpha^2\beta^2\gamma^2
\end{aligned}$$

と推量したのである．この展開が $(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ に等しいかどうかは Maple で確かめればよい．

1.2.2　4 次式の判別式

1.2.1 で述べた方針で，次の 4 次式の判別式を求めてみよ．

$$f(x) = ax^4 + bx^3 + cx^2 + dx + e = a(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$$

ただし，解と係数の間には次の関係式がある．

$$\alpha+\beta+\gamma+\delta = -\frac{b}{a}, \quad \alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta = \frac{c}{a}$$
$$\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta = -\frac{d}{a}, \quad \alpha\beta\gamma\delta = \frac{e}{a}$$

判別式は

$$D = (\alpha-\beta)^2(\alpha-\gamma)^2(\alpha-\delta)^2(\beta-\gamma)^2(\beta-\delta)^2(\gamma-\delta)^2$$

で定義するが，この式を展開して次の式が成立することを確かめよ．

$$\begin{aligned}
&(\alpha-\beta)^2(\alpha-\gamma)^2(\alpha-\delta)^2(\beta-\gamma)^2(\beta-\delta)^2(\gamma-\delta)^2 = \\
&\quad 27(\alpha+\beta+\gamma+\delta)^4(\alpha\beta\gamma\delta)^2 + 4(\alpha+\beta+\gamma+\delta)^3(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^3 \\
&\quad -18(\alpha+\beta+\gamma+\delta)^3(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)(\alpha\beta\gamma\delta) \\
&\quad +6(\alpha+\beta+\gamma+\delta)^2(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^2\alpha\beta\gamma\delta \\
&\quad -144(\alpha+\beta+\gamma+\delta)^2(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)(\alpha\beta\gamma\delta)^2 \\
&\quad -(\alpha+\beta+\gamma+\delta)^2(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)^2(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^2 \\
&\quad +4(\alpha+\beta+\gamma+\delta)^2(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)^3(\alpha\beta\gamma\delta) \\
&\quad +80(\alpha+\beta+\gamma+\delta)(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)^2(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)\alpha\beta\gamma\delta \\
&\quad -18(\alpha+\beta+\gamma+\delta)(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^3 \\
&\quad +192(\alpha+\beta+\gamma+\delta)(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)(\alpha\beta\gamma\delta)^2 \\
&\quad -16(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)^4\alpha\beta\gamma\delta \\
&\quad +4(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)^3(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^2 \\
&\quad -144(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^2\alpha\beta\gamma\delta \\
&\quad +128(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta)^2(\alpha\beta\gamma\delta)^2 \\
&\quad +27(\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta)^4 - 256(\alpha\beta\gamma\delta)^3
\end{aligned}$$

したがって，$a=1$ のときは，

$$\begin{aligned}
D = {} & 27b^4e^2 + 4b^3d^3 - 18b^3cde + 6b^2d^2e - 144b^2ce^2 - b^2c^2d^2 + 4b^2c^3e \\
& +80bc^2de - 18bcd^3 + 192bde^2 - 16c^4e + 4c^3d^2 - 144cd^2e + 128c^2e^2 + 27d^4 - 256e^3
\end{aligned}$$

が得られる．このような計算は手計算では推量することも実行することも無理である．この計算の背後には

$$D = -\mathrm{Res}_x(f, f') = -\begin{vmatrix} 1 & b & c & d & e & 0 & 0 \\ 0 & 1 & b & c & d & e & 0 \\ 0 & 0 & 1 & b & c & d & e \\ 4 & 3b & 2c & d & 0 & 0 & 0 \\ 0 & 4 & 3b & 2c & d & 0 & 0 \\ 0 & 0 & 4 & 3b & 2c & d & 0 \\ 0 & 0 & 0 & 4 & 3b & 2c & d \end{vmatrix}$$

という等式がある．

1.2.3 チルンハウゼン変換

3 次式，4 次式の判別式は複雑で見難い形をしている．そこで，方程式の一般性を失わないで，少なくとも解は元の方程式と同じになるように，方程式を変換することを考えよう．

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0, \quad a_0 \neq 0$$

という方程式が与えられれば，$f(x)$ の代わりに $\dfrac{1}{a_0}f(x)$ を考えて，始めから $a_0 = 1$ と仮定しても差し支えない．このことは，断りなしに上の議論でも使っている．すなわち，

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \tag{6}$$

という多項式から出発する．次いで，変数 x を $x' = x + \dfrac{a_1}{n}$ で置き換えてみよう．$x = x' - \dfrac{a_1}{n}$ を (6) 式に代入すると，

$$\begin{aligned} f(x) &= \left(x' - \frac{a_1}{n}\right)^n + a_1\left(x' - \frac{a_1}{n}\right)^{n-1} + \cdots + a_n \\ &= \left\{x'^n - a_1x'^{n-1} + \frac{(n-1)a_1^2}{2n}x'^{n-2} + \cdots + (-1)^n\left(\frac{a_1}{n}\right)^n\right\} \\ &\quad + a_1\left\{x'^{n-1} - \frac{(n-1)a_1}{n}x'^{n-2} + \cdots\right\} + \cdots + a_n \\ &= x'^n - \frac{(n-1)a_1^2}{2n}x'^{n-2} + (x' \text{ の低次の項}) \end{aligned}$$

となって，$f(x)$ は x' の多項式として x'^{n-1} の項をもたない．よって，この変換を許せば，(6) 式は次の形をしていると仮定しても一般性を失わない．

$$f(x) = x^n + a_2x^{n-2} + a_3x^3 + \cdots + a_n \tag{7}$$

この変換を多項式 $f(x)$ の**チルンハウゼン (Tschirnhausen) 変換**という．$n = 2$ ならば，$f(x) = x^2 + bx + c$ を

$$f(x) = \left(x + \frac{b}{2}\right)^2 + \left(c - \frac{b^2}{4}\right)$$

と変換することだから，これは 2 次式の完全平方化に他ならない．

(7) 式の形の場合には，判別式は大幅に簡略化される．例えば，3 次式

$$f(x) = x^3 + ax + b \tag{8}$$

の判別式は, (4) 式に $a = 1, b = 0$ を代入して $D = -(4c^3 + 27d^2)$ を得るから，

$$D = -(4a^3 + 27b^2) \tag{9}$$

となる．また，4 次式

$$f(x) = x^4 + ax^2 + bx + c \tag{10}$$

の場合には, 同様にして，

$$D = -16a^4c + 4a^3b^2 - 144ab^2c + 128a^2c^2 + 27b^4 - 256c^3 \tag{11}$$

が得られる．

ここで，特別な 4 次式を選んで判別式を考えてみよう．

I. $f(x) = x^4 + ax^2 + b$ の場合には，(11) 式から

$$D = -(16a^4b - 128a^2b^2 + 256b^3) = -16b(a^2 - 4b)^2$$

となる．これは，$f(x) = (x^2)^2 + a(x^2) + b$ とかけば，$f(x)$ は x^2 に関する 2 次式となる．その解を α, β とすれば，$x = \pm\sqrt{\alpha}, \pm\sqrt{\beta}$ と定まるから，$b \neq 0$ のときには重解をもつ必要十分条件が $a^2 - 4b = 0$ で与えられることを示している．

II. $f(x) = x(x^3 + bx^2 + cx + d)$ の場合には，

$$D = -d^2(b^2c^2 - 4b^3d + 18bcd - 4c^3 - 27d^2)$$

となって，括弧の中には 3 次式 $g(x) = x^3 + bx^2 + cx + d$ の判別式が現れる．

1.3 対称式

$x_1, x_2, \ldots, x_n$ を n 個の独立変数とする．1 変数多項式の拡張として $x_1, x_2, \ldots, x_n$ の多項式

$$f(x_1, \ldots, x_n) = \sum_{\alpha_1,\ldots,\alpha_n} a_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

を考えることができる．ここで，$\sum_{\alpha_1,\ldots,\alpha_n}$ という記号は，$\alpha_1, \ldots, \alpha_n$ が独立に $0, 1, \ldots$ と負でない整数の値を取ることを意味する．また，$a_{\alpha_1,\ldots,\alpha_n}$ は係数で体 K の元から取ってくるものとする．このような n 変数の多項式の間で加減法と乗法が定義される．それらの全体を $K[x_1, x_2, \ldots, x_n]$ という記号で表す．

ここで，n 文字の置換について復習しよう．n 文字にラベルをつけて，その集合を簡単に $\{1,2,\ldots,n\}$ と表しておく．n 文字の置換とは，集合 $\{1,2,\ldots,n\}$ から自分自身 $\{1,2,\ldots,n\}$ 上への $1:1$ 写像である．その 1 つを σ とすれば，σ は次のように表してもよい．

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

簡単に言えば，列 $\sigma(1),\sigma(2),\ldots,\sigma(n)$ は列 $1,2,\ldots,n$ を並べ替えたに過ぎない．したがって，n 文字の置換は全部で $n!$ 個ある．それら全部の集合を S_n で表すことにする．$\sigma \in S_n$ が与えられると，上の多項式 $f(x_1,\ldots,x_n)$ から多項式

$$\sigma(f)(x_1,\ldots,x_n) := \sum_{\alpha_1,\ldots,\alpha_n} a_{\alpha_1,\ldots,\alpha_n} x_{\sigma(1)}^{\alpha_1} \cdots x_{\sigma(n)}^{\alpha_n}$$

を作ることができる．例えば，

$$n=3, \quad f(x_1,x_2,x_3) = x_1^2 + x_2^3 + x_3^4, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

ならば，$\sigma(f)(x_1,x_2,x_3) = x_3^2 + x_1^3 + x_2^4$ となる．

n 変数多項式 $f(x_1,\ldots,x_n)$ は，S_n のすべての元 σ に対して $\sigma(f) = f$ となるとき，**対称式**であるという．

例 1.1 $1 \le k \le n$ に対して，k 次の多項式 $s_k(x_1,\ldots,x_n)$ を

$$s_k(x_1,\ldots,x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

と定義する．ここで，$\sum_{1 \le i_1 < i_2 < \cdots < i_k \le n}$ は 1 から n までの間にある k 個の数字の列 $i_1, i_2, \ldots, i_k$ を条件 $i_1 < i_2 < \cdots < i_k$ を満たすようにすべて取ることを意味する．

例えば，$n=3$ ならば，$s_1 = x_1+x_2+x_3, s_2 = x_1x_2 + x_1x_3 + x_2x_3, s_3 = x_1x_2x_3$ である．

一般に，次のことが言える．

補題 1.2 T を変数とすると，次の恒等式が存在する．

$$\begin{aligned}&(T-x_1)(T-x_2)\cdots(T-x_n) = \\ &\quad T^n - s_1T^{n-1} + s_2T^{n-2} + \cdots + (-1)^k s_k T^{n-k} + \cdots + (-1)^n s_n\end{aligned}$$

定理 1.3 $f(x_1,\ldots,x_n)$ が K-係数の n 変数の対称式ならば，$f(x_1,\ldots,x_n)$ は $s_1,s_2,\ldots,s_n$ に関する K-係数の多項式として表される．

1.4　方程式の多重解

3 次方程式

$$f(x) = x^3 + ax + b = 0 \tag{8}$$

が重解をもつ必要十分条件は

$$D = -(4a^3 + 27b^2) = 0 \tag{9}$$

であった．条件 (9) のもとでは次の 3 つの条件は同値である．

(1) $a = 0$.

(2) $a = b = 0$.

(3) (8) 式は 3 重解 $x = 0$ をもつ．

ここで，$a \neq 0$ として $t = \dfrac{3b}{2a}$ とおけば，$\left(\dfrac{3b}{2a}\right)^2 = -\dfrac{a}{3}$ だから，$a = -3t^2, b = -2t^3$ と表されて，(8) 式は

$$f(x) = (x + t)^2(x - 2t)$$

と因数分解される．t が値 0 に近づくと，a と b も 0 に近づき，(8) の 3 次式の解は 3 重解 $x = 0$ に近づく．

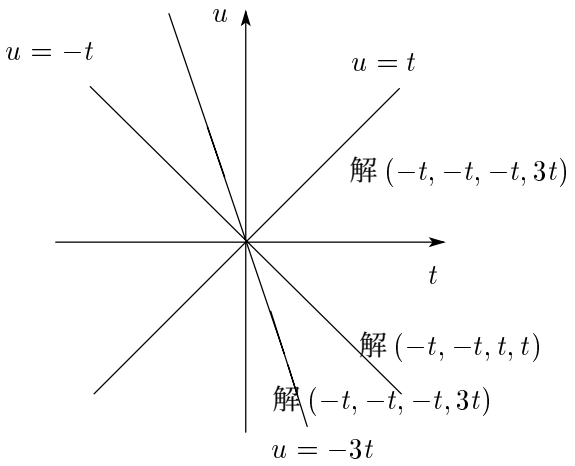
4 次方程式

$$f(x) = x^4 + ax^2 + bx + c \tag{10}$$

についても同様にして考えてみよう．$f(x) = 0$ が重解を持つとして，その重解を $x = -t$ と置く．他の 2 解を $x = -u, x = v$ とすれば $f(x) = (x + t)^2(x + u)(x - v)$ と表されるが，$f(x)$ の 3 次の項の係数は 0 としているので，$v = 2t + u$ となる．すなわち，(10) 式は次のように表される．

$$f(x) = (x + t)^2(x + u)(x - 2t - u) \tag{10 - 1}$$

(10-1) 式は $u = -t$ のとき，$f(x) = (x + t)^2(x - t)^2$ となって，重解 $x = t$ と $x = -t$ をもつ．このとき，$f(x) = 0$ は解 $(-t, -t, t, t)$ をもつということにする．同様にして，$u = t$ のときは解 $(-t, -t, -t, 3t)$ をもち，$u = -3t$ のときは解 $(-t, -t, -t, -3t)$ をもつ．さらに，$t = 0$ のときは 4 重解 $x = 0$ をもつ．これを (t, u) 平面上で図示すると次のようになる．



1.4.1 再び判別式へ

式 (10-1) の右辺を展開して (10) 式と係数を比較すると，次の関係が得られる．

$$a=-u^2-2tu-3t^2,\quad b=-2tu^2-4t^2u-2t^3,\quad c=-t^2u^2-2t^3u$$

これら 3 つの式から t と u を消去すると，a,b,c の関係式が得られる．それは次節で述べる終結式を用いて，次のように計算される．そのために，次の記号を導入する．

$$G=u^2+2tu+3t^2+a,\quad H=2tu^2+4t^2u+2t^3+b,\quad K=t^2u^2+2t^3u+c$$

ここで，G と H を u の多項式と見て，$G=0, H=0$ が共通解をもつ条件は $GH:=\mathrm{Res}_u(G,H)=0$ である．同様に，$H=0$ と $K=0$ が共通解をもつ条件は $HK:=\mathrm{Res}_u(H,K)=0$ である．実際に Maple を使って計算すると，

$$GH=(4t^3+2at-b)^2,\quad HK=t^2(2t^4+bt-2c)^2$$

となる．そこで GH と HK を t の多項式と見て，$GH=0$ と $HK=0$ が t の共通解をもつ条件を求めると，$GHK=\mathrm{Res}_t(GH,HK)=0$ となる．実際に計算すると，

$$GHK=\left\{8b(-16a^4c+4a^3b^2-144ab^2c+128a^2c^2+27b^4-256c^3)\right\}^4$$

となって，(11) 式の判別式が本質的に得られていることが分る．

2　終結式

2.1　定義と定理

前節の説明では肝心なところは終結式と呼ばれるものの計算に帰着されることが分った．本節では，変数 x に関する 2 つの式

$$\begin{aligned} f(x) &= a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m \quad (a_0 \neq 0) \\ g(x) &= b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n \quad (b_0 \neq 0) \end{aligned}$$

の終結式を定義し，その意味付けをしよう．

まず，$f(x)$ と $g(x)$ の係数を，$f(x)$ の係数をずらせながら n 回，$g(x)$ の係数をずらせながら m 回，並べて作った $n+m$ 次の行列式

$$\begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ 0 & 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & \cdots & 0 \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m \\ b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & 0 & \cdots & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & \cdots & 0 \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n \end{vmatrix}$$

を $f(x)$ と $g(x)$ の**終結式**といい，$\mathrm{Res}(f,g)$ または $\mathrm{Res}_x(f,g)$ とかく．

終結式のもつ意味は次の定理に帰着される．

定理 2.1 方程式 $f(x)=0$ と $g(x)=0$ が共通解をもつための必要十分条件は $\mathrm{Res}(f,g)=0$ である．

2.2 条件の必要性

$X_1, X_2, \ldots, X_{m+n}$ を $m+n$ 個の変数として，次の行列表示をもつ連立方程式を考えてみよう．

$$\begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ 0 & 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & \cdots & 0 \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m \\ b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & 0 & \cdots & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & \cdots & 0 \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n \end{pmatrix} \begin{pmatrix} X_{m+n} \\ X_{m+n-1} \\ X_{m+n-2} \\ \vdots \\ X_{m+1} \\ X_m \\ X_{m-1} \\ X_{m-2} \\ \vdots \\ X_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

さて，$f(x)=0$ と $g(x)=0$ が共通解 $x=\lambda$ をもったとしよう．すると，

$$(X_{m+n}, X_{m+n-1}, \ldots, X_2, X_1) = (\lambda^{m+n-1}, \lambda^{m+n-2}, \ldots, \lambda, 1)$$

は容易に確かめられるように，上の連立方程式の自明でない解である．したがって，線形代数学の定理から，係数行列の行列式 $\mathrm{Res}(f,g)=0$ である．実際，係数行列を C とおけば，$\det C = \mathrm{Res}(f,g) \neq 0$ ならば，C の逆行列 C^{-1} が存在して，連立方程式の解は一意的に $C^{-1t}(0,0,\ldots,0)$ と定まる．よって，自明でない解は存在しないことになる．

2.3 1 変数多項式の性質

次に，$\mathrm{Res}(f,g)=0$ ならば，$f(x)=0$ と $g(x)=0$ は共通解をもつことを示したいのであるが，次の分節で述べる証明には 1 変数多項式の性質をいろいろと用いる．証明を読まずに結果だけを眺めて，次の分節に進むのも一つの方法である．

ここでは，体 K 上の 1 変数多項式の集合 $K[x]$ を考える．多項式 $f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$ の最高次の係数 $a_0 \neq 0$ ならば，$f(x)$ を $a_0^{-1}f(x)$ に代えて，最高次の係数を 1 の多項式に変形できる．

次の結果は高校で学習した多項式の**剰余の定理**を一般化したものである．

補題 2.2 $h(x), k(x) \in K[x]$ について，$k(x) \neq 0$ ならば，多項式 $q(x), r(x) \in K[x]$ が存在して，

$$h(x) = q(x)k(x) + r(x), \quad r(x)=0 \text{ または } 0 \leq \deg r(x) < \deg k(x) \ .$$

このような多項式 $q(x), r(x)$ はただ一通りに定まる．

証明. $\deg h(x)$ に関する帰納法で，$q(x)$ と $r(x)$ が存在することを証明する．$\deg h(x) < \deg k(x)$ の場合には，$q(x)=0, r(x)=h(x)$ と置けばよい．$\deg h(x) \geq \deg k(x)$ の場合には，$n=\deg h(x), m=$

$\deg k(x)$ として，$h_1(x) = h(x) - \frac{c_0}{d_0}x^{n-m}k(x)$ と置く．ただし，c_0, d_0 はそれぞれ $h(x), k(x)$ の最高次の係数である．このとき，$\deg h_1(x) < \deg h(x)$ となるから，帰納法の仮定によって，多項式 $q_1(x), r_1(x)$ が存在して，$h_1(x) = q_1(x)k(x) + r_1(x),\ r_1(x) = 0$ または $0 \leq \deg r_1(x) < \deg k(x)$ となる．そこで，$q(x) = \frac{c_0}{d_0}x^{n-m} + q_1(x),\ r(x) = r_1(x)$ と置けばよい．

$q(x)$ と $r(x)$ が一意的に定まることを示そう．$q(x), r(x)$ と $q'(x), r'(x)$ がそれぞれ上の条件を満たせば，

$$(q(x) - q'(x))k(x) = r'(x) - r(x), \quad r'(x) - r(x) = 0 \text{ または } 0 \leq \deg(r'(x) - r(x)) < \deg k(x)$$

となる．しかるに，$\deg(q(x) - q'(x))k(x) = \deg(q(x) - q'(x)) + \deg k(x) \geq \deg k(x)$ だから，不等式 $0 \leq \deg(r'(x) - r(x)) < \deg k(x)$ が成立することはない．よって，$r'(x) = r(x)$．すると，$(q(x) - q'(x))k(x) = 0$ だから，$q'(x) = q(x)$ となる． 証明終

$q(x)$ を**商**といい，$r(x)$ を**剰余**という．この結果から，次の**ユークリッドの互除法**が導かれる．

補題 2.3 $h(x), k(x) \in K[x]$ に対して，多項式 $q_1(x), q_2(x), \ldots, q_n(x), k_2(x), \ldots, k_n(x)$ が一意的に存在して，次の条件を満たす．

$$\begin{array}{lcll}
h(x) & = & q_1(x)k(x) + k_2(x), & \deg k_2(x) < \deg k(x) \\
k(x) & = & q_2(x)k_2(x) + k_3(x), & \deg k_3(x) < \deg k_2(x) \\
\cdots & & \cdots & \cdots \\
k_{n-2}(x) & = & q_{n-1}(x)k_{n-1}(x) + k_n(x), & \deg k_n(x) < \deg k_{n-1}(x) \\
k_{n-1}(x) & = & q_n(x)k_n(x) & k_n(x) \neq 0
\end{array}$$

証明． 最初の 1 行は剰余の定理を書き換えたものである．2 行目も，$k(x)$ と $k_2(x)$ に対して剰余の定理を適用する．順次，この定理を適用していくと，

$$\deg k(x) > \deg k_2(x) > \deg k_3(x) > \cdots$$

と剰余の次数が下がっていくので，このステップは無限回は続かない． 証明終

補題の中で，$k_0(x) = h(x), k_1(x) = k(x)$ とすると，添え字の番号と重ねるステップの回数が合ってくる．

2 つの多項式 $h(x), k(x)$ に付いて，$h(x) = q(x)k(x)$ となる多項式 $q(x)$ がある場合，$k(x)$ は $h(x)$ の**約数**といい，$k(x) \mid h(x)$ と書く．$h(x)$ は $k(x)$ の**倍数**ともいう．多項式 $d(x)$ が $d(x) \mid h(x), d(x) \mid k(x)$ を満たすとき，$d(x)$ は $h(x), k(x)$ の**公約数**という．ある多項式 $\widetilde{d}(x)$ は，

(1) $\widetilde{d}(x) \mid h(x),\ \widetilde{d}(x) \mid k(x)$,

(2) $d(x) \mid h(x),\ d(x) \mid k(x)$ ならば，$d(x) \mid \widetilde{d}(x)$

の 2 条件を満たすとき，$h(x)$ と $k(x)$ の**最大公約数**という．$\widetilde{d}(x)$ が $h(x)$ と $k(x)$ の最大公約数ならば，他の最大公約数は $\widetilde{d}(x)$ の定数倍，すなわち，$\widetilde{d}(x)$ に K の 0 でない元をかけたもの，である．

補題 2.4 ユークリッド互除法に関する前補題の記号を使うと，$k_n(x)$ は $h(x)$ と $k(x)$ の最大公約数である．このとき，多項式 $a(x), b(x)$ が存在して

$$a(x)h(x) + b(x)k(x) = k_n(x)$$

とできる．

証明. ユークリッドの互除法を逆にたどると，$k_n(x) \mid k_{n-1}(x), k_n(x) \mid k_{n-2}(x), \ldots, k_n(x) \mid k(x), k_n(x) \mid h(x)$ が分かるので，$k_n(x)$ は $h(x)$ と $k(x)$ の公約数である．逆に，$d(x)$ を $h(x)$ と $k(x)$ の公約数とする．ユークリッドの互除法の最初のステップにより，$d(x) \mid k_2(x)$ が分かる．$d(x) \mid k(x), d(x) \mid k_2(x)$ だから，第 2 のステップにより，$d(x) \mid k_3(x)$ が分かる．順次，この議論を進めると，$d(x) \mid k_{i-1}(x), d(x) \mid k_i(x)$ から，$d(x) \mid k_{i+1}(x)$ が分かる．最後に，$d(x) \mid k_n(x)$ となる．よって，$k_n(x)$ は $h(x)$ と $k(x)$ の最大公約数である．

$k_n(x)$ を $a(x)h(x) + b(x)k(x)$ という形で表そう．$k_n(x) = k_{n-2}(x) - q_{n-1}(x)k_{n-1}(x)$ であるから，$k_2(x), k_3(x), \ldots, k_{n-1}(x)$ が，やはり，適当な多項式 $a(x), b(x)$ を見つけて $a(x)h(x)+b(x)k(x)$ の形に表されることをいえばよい．$k_2(x) = h(x) - q_1(x)k(x)$ だから，$k_2(x)$ については成立する．

i に関する帰納法で，$k_{i-1}(x) = a_{i-1}(x)h(x) + b_{i-1}(x)k(x), k_i(x) = a_i(x)h(x) + b_i(x)k(x)$ と表されたとすると，$k_{i+1}(x) = k_{i-1}(x) - q_i(x)k_i(x)$ だから，

$$\begin{aligned} k_{i+1}(x) &= a_{i-1}(x)h(x) + b_{i-1}(x)k(x) - q_i(x)\{a_i(x)h(x) + b_i(x)k(x)\} \\ &= \{a_{i-1}(x) - q_i(x)a_i(x)\}h(x) + \{b_{i-1}(x) - q_i(x)b_i(x)\}k(x) \end{aligned}$$

となって，$k_{i+1}(x)$ についてもよい．したがって，補題の後半部分が証明された． 証明終

$h(x)$ と $k(x)$ の最大公約数を $\gcd(h(x), k(x))$ と書く．最大公約数が 1 の定数倍になるとき，$h(x)$ と $k(x)$ は**互いに素**であるという．したがって，$h(x)$ と $k(x)$ が互いに素である必要十分条件は多項式 $a(x), b(x)$ が存在して $a(x)h(x) + b(x)k(x) = 1$ となることである．

多項式 $p(x)$ は，$p(x) = h_1(x)h_2(x)$ と 2 つの多項式の積に表すとき $h_1(x)$ か $h_2(x)$ のどちらかは必ず定数であるとき，**既約**な多項式であるという．この条件は $p(x)$ の係数が属する体 K に依存した概念である．例えば，$p(x) = x^2 + 1$ は $K = \mathbb{R}$（実数体）のときは既約な多項式であるが，$K = \mathbb{C}$（複素数体）のときは，$p(x) = (x + \sqrt{-1})(x - \sqrt{-1})$ と分解するから，既約な多項式ではない．与えられた多項式を既約な多項式の積に分解することに関して，次の結果がある．2 つの多項式 $h(x), g(x) \in K[x]$ は，ある定数 $c \in K$ が存在して $g(x) = ch(x)$ となるとき，**同伴**であるといい，$h(x) \sim k(x)$ と書くことにする．

定理 2.5 体 K が与えられたとき，$K[x]$ に属する多項式について，次の結果が成立する．

(1) 任意の多項式 $h(x)$ は既約な多項式の積 $h(x) = p_1(x)p_2(x)\cdots p_m(x)$ として表される．この分解を $h(x)$ の**既約分解**という．

(2) $h(x)$ の 2 つの既約分解

$$p_1(x)p_2(x)\cdots p_m(x) = q_1(x)q_2(x)\cdots q_n(x)$$

が与えられると，$m = n$ であり，添え字の並べ替え $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ が存在して，$p_i(x) \sim q_{\sigma(i)}(x)$ $(i = 1, 2, \ldots, n)$ とできる．

証明．(1) $h(x)$ の次数に関する帰納法で証明する．$\deg h(x) = 1$ ならば，$h(x)$ は既約な多項式である．また，もし $h(x)$ が既約多項式であるならば定理は成立している．$h(x)$ は既約多項式でない（**可約多項式**という．）ならば，$h(x) = h_1(x)h_2(x)$ という分解で，$\deg h_1(x) < \deg h(x), \deg h_2(x) < \deg h(x)$ となるものが存在する．帰納法の仮定により，既約分解

$$h_1(x) = p_1(x)p_2(x)\cdots p_r(x), \quad h_2(x) = p_{r+1}(x)p_{r+2}(x)\cdots p_m(x)$$

が存在する．このとき，$h(x) = p_1(x)\cdots p_r(x)p_{r+1}(x)\cdots p_m(x)$ は $h(x)$ の既約分解である．

(2) $p(x)$ を既約多項式とし，$p(x) \mid h_1(x)h_2(x)$ ならば，$p(x) \mid h_1(x)$ または $p(x) \mid h_2(x)$ となることを示そう．$d(x) = \gcd(p(x), h_1(x))$ とすると，$d(x) \mid p(x)$ である．$p(x)$ は既約多項式だから，$d(x) \sim 1$ または $d(x) \sim p(x)$ である．$d(x) \sim p(x)$ ならば，$p(x) \mid h_1(x)$ である．$d(x) \sim 1$ と仮定しよう．このとき，$p(x)$ と $h_1(x)$ は互いに素な多項式である．よって，多項式 $a(x), b(x)$ が存在して，$a(x)p(x) + b(x)h_1(x) = 1$ とできる．すると，

$$h_2(x) = h_2(x)\left(a(x)p(x) + b(x)h_1(x)\right) = p(x)\left\{a(x)h_2(x) + b(x)\frac{h_1(x)h_2(x)}{p(x)}\right\}$$

となって，$p(x) \mid h_2(x)$ となる．

さて，$p_1(x)p_2(x)\cdots p_m(x) = q_1(x)q_2(x)\cdots q_n(x)$ を $h(x)$ の 2 つの既約分解とする．$p_1(x) \mid q_1(x)\left(q_2(x)\cdots q_n(x)\right)$ だから，上の注意により，$p_1(x) \mid q_1(x)$ または $p_1(x) \mid q_2(x)\cdots q_n(x)$ となる．$p_1(x) \mid q_1(x)$ ならば，$q_1(x)$ も既約多項式だから，$p_1(x) \sim q_1(x)$. $p_1(x) \mid q_2(x)\cdots q_n(x)$ ならば，同様にして，$p_1(x) \sim q_{i_1}(x)$ となる添字 i_1 が存在することが分る．ここで，定数倍を取ることで係数を調整すれば，

$$p_2(x)\cdots p_m(x) = q_1(x)\cdots q_{i_1-1}(x)q_{i_1+1}(x)\cdots q_n(x) \tag{12}$$

とできる．2 つの既約分解に現れる既約多項式の数 $m + n$ に関する帰納法を使えば，既約分解 (12) に現れる既約多項式の数は $m + n - 2$ である．したがって，$m - 1 = n - 1$ であり，$p_j(x) \sim q_{i_j}(x)$ $(j = 2, \ldots, n)$ とできる．したがって，求める既約分解の一意性が証明できた．　　証明終

2.4　条件の十分性

定理の証明で難しいのは十分性の証明である．その証明のために次の結果を用いる．

補題 2.6　m 次方程式 $f(x) = 0$ と n 次方程式 $g(x) = 0$ が共通解をもつ必要十分条件は，多項式 $\varphi(x)$ と $\psi(x)$ が存在して，次の 2 条件を満たすことである．

(1) $\deg \varphi(x) < n$ かつ $\deg \psi(x) < m$.

(2) $\varphi(x)f(x) = \psi(x)g(x)$.

証明. $f(x) = 0$ と $g(x) = 0$ が共通解 $x = \lambda$ をもったとすれば，**因数定理**から，$f(x) = (x - \lambda)f_1(x), g(x) = (x - \lambda)g_1(x)$ と書ける．そこで，$\varphi(x) = g_1(x), \psi(x) = f_1(x)$ と置けば，

$$\begin{aligned} \deg \varphi(x) &= \deg g_1(x) = n - 1 < n \\ \deg \psi(x) &= \deg f_1(x) = m - 1 < m \\ \varphi(x)f(x) &= (x - \lambda)f_1(x)g_1(x) = \psi(x)g(x) \end{aligned}$$

となって，$\varphi(x), \psi(x)$ は条件を満たす.

逆に，条件 (1) と (2) を満たす多項式 $\varphi(x)$ と $\psi(x)$ が存在したと仮定しよう．多項式 $f(x)$ は既約多項式の積に因数分解される．それを $f(x) = f_1(x) \cdots f_r(x)$ としよう．このとき，$f(x)\varphi(x) = g(x)\psi(x)$ だから，どの $f_i(x)$ も $g(x)\psi(x)$ を割っている．定理 2.5 により，もしどの $f_i(x)$ も $g(x)$ を割らなければ，すべての $f_i(x)$ が $\psi(x)$ を割っている．すると，$f(x)$ が $\psi(x)$ を割ることになって，$\deg \psi(x) < \deg f(x)$ という仮定に反する．したがって，ある $f_i(x)$ は $g(x)$ を割っている．すなわち，$f(x)$ と $g(x)$ は共通因子をもつので，$f(x) = 0$ と $g(x) = 0$ は共通解をもつ. 証明終

ここで，

$$\begin{aligned} \varphi(x) &= \alpha_0 x^{n-1} + \alpha_1 x^{n-2} + \cdots + \alpha_{n-2}x + \alpha_{n-1} \\ \psi(x) &= \beta_0 x^{m-1} + \beta_1 x^{m-2} + \cdots + \beta_{m-2}x + \beta_{m-1} \end{aligned}$$

と置くと，等式 $\varphi(x)f(x) = \psi(x)g(x)$ より，両辺の各単項式の係数を比較して，次の等式が得られる.

$$\begin{aligned} x^{m+n-1} &\cdots & a_0\alpha_0 &= b_0\beta_0 \\ x^{m+n-2} &\cdots & a_0\alpha_1 + a_1\alpha_0 &= b_0\beta_1 + b_1\beta_0 \\ & & & \\ x^{m+n-i} &\cdots & a_0\alpha_{i-1} + a_1\alpha_{i-2} + \cdots + a_{i-1}\alpha_0 &= b_0\beta_{i-1} + b_1\beta_{i-2} + \cdots + b_{i-1}\beta_0 \\ & & & \\ x &\cdots & a_{m-1}\alpha_n + a_m\alpha_{n-1} &= b_{n-1}\beta_m + b_n\beta_{m-1} \end{aligned}$$

これらの関係式は次のように行列表示される．

$$(\alpha_0,\ldots,\alpha_{n-1},-\beta_0,\ldots,-\beta_{m-1})\begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ 0 & 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m & \cdots & 0 \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & \cdots & a_{m-1} & a_m \\ b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & 0 & \cdots & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n & \cdots & 0 \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & b_n \end{pmatrix}$$
$$= (0,\ldots,0,0,\ldots,0)\ .$$

ここで，$(\alpha_0,\ldots,\alpha_{n-1},-\beta_0,\ldots,-\beta_{m-1}) \neq (0,\ldots,0,0,\ldots,0)$ だから，係数行列の行列式 $\mathrm{Res}(f,g)$ は 0 でなければならない．

2.5 パラメータ表示された平面代数曲線

終結式は代数学でいろいろな問題に応用されるが，消去理論はその一つである．まず，平面代数曲線を定義し，そのパラメータ表示を考えてみよう．

これ以降，体 K は有理数体 $\mathbb{Q}$ を含むものとする．すなわち，1 の整数倍 $n\cdot 1$ は 0 でなく，それを n と同一視すると K の中で逆元 $\frac{1}{n}$ を取ることができる．例えば，K として実数体 $\mathbb{R}$ や複素数体 $\mathbb{C}$ を考えておけばよい．集合 K^2 を $K^2=\{(a,b)\mid a,b\in K\}$ と定義する．$\mathbb{R}^2$ で実平面を表すように，K^2 の元 (a,b) は K-平面の点と考える．また，座標 x,y を考えて K-平面 K^2 を xy- 平面といい，a をその x 座標，b をその y 座標という．

x,y を変数とする K 係数の多項式 $F(x,y)$ を考え，K^2 の部分集合

$$C_K(f) := \{(a,b)\in K^2 \mid F(a,b)=0\}$$

を考え，$C_K(F)$ が有限集合でない場合に $C(F)$ を方程式 $F(x,y)=0$ で定義される**平面代数曲線**，簡単に**代数曲線**，という．このとき，$F(x,y)$ を**定義多項式**という．多項式 $F(x,y)$ は，2 つの定数でない多項式の積に表されるとき**可約**であるといい，可約でないとき**既約**であるという．既約な多項式 $F(x,y)$ によって定義される代数曲線を**既約代数曲線**という．

例えば，$F(x,y)=x^2+y^2$ ならば，$C_{\mathbb{R}}(F)=\{(0,0)\}$ だから，$C_{\mathbb{R}}(F)$ は代数曲線ではない．実数体 $\mathbb{R}$ の代わりに複素数体 $\mathbb{C}$ を考えると，$C_{\mathbb{C}}(F)=C_{\mathbb{C}}(x+\sqrt{-1}y)\cup C_{\mathbb{C}}(x-\sqrt{-1}y)$ となって，$C_{\mathbb{C}}(F)$ は可約代数曲線となる．

t を変数として，t の多項式で定義される 2 つの関数を考えよう．

$$(*)\quad \begin{cases} x = f(t) = a_0t^m+a_1t^{m-1}+\cdots+a_{m-1}t+a_m, & a_0\neq 0 \\ y = g(t) = b_0t^n+b_1t^{n-1}+\cdots+b_{n-1}t+b_n, & b_0\neq 0 \end{cases}$$

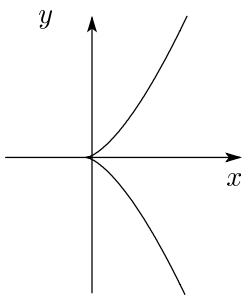
ここで，t が K の元を取りながら変化するとき，点 $(f(t), g(t))$ は平面 K^2 の点集合を構成する．そこで，$F(x, y) = \mathrm{Res}_t(f(t) - x, g(t) - y)$ と定義すると，次のことがらが成立する．

定理 2.7 $C_K(F) = \{(f(\lambda), g(\lambda)) \mid \lambda \in K\}$.

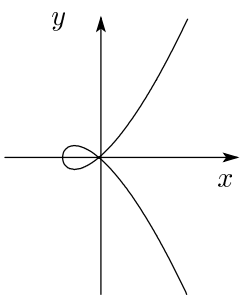
証明. $\lambda \in K$ について，$f(t) - f(\lambda) = 0$ と $g(t) - g(\lambda) = 0$ は共通解 $t = \lambda$ をもつ．よって，定理 2.1 により，$F(f(\lambda), g(\lambda)) = \mathrm{Res}_t(f(t) - f(\lambda), g(t) - g(\lambda)) = 0$. すなわち，$\{(f(\lambda), g(\lambda)) \mid \lambda \in K\} \subseteq C_K(F)$. 逆に，$(\alpha, \beta) \in C_K(F)$ ならば，$F(\alpha, \beta) = \mathrm{Res}_t(f(t) - \alpha, g(t) - \beta) = 0$ だから，定理 2.1 により，ある $\lambda \in K$ が存在して，$f(\lambda) - \alpha = 0, g(\lambda) - \beta = 0$ となる．すなわち，$C_K(F) \subseteq \{(f(\lambda), g(\lambda)) \mid \lambda \in K\}$. 証明終

多項式 $F(x, y)$ は必ずしも既約な多項式ではない．章末で説明する用語を使うと，既約多項式 $G(x, y) \in K[x, y]$ と $c \in K \setminus \{0\}$ が存在して $F(x, y) = cG(x, y)^N$ と書けることが分っている．ただし，N は体の拡大次数 $[K(t) : K(x, y)] = 1$ に等しい．明らかに，$C_K(F) = C_K(G)$ だから，$C_K(F)$ は既約代数曲線である．$(*)$ を $C_K(F)$ の**多項式パラメータ表示**という．例を考えてみよう．ただし，グラフを描くときは体 K を実数体 $\mathbb{R}$ に取ることにする．

例 2.8 $x = f(t) = t^2, y = g(t) = t^3$ ならば，$F(x, y) = y^2 - x^3$. $x = f(t) = t^2 - 1, y = g(t) = t(t^2 - 1)$ ならば，$F(x, y) = y^2 - x^2 - x^3$.



$y^2 = x^3$

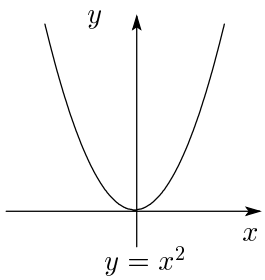


$y^2 = x^2(1 + x)$

Maple で $F(x, y)$ を計算するのは簡単である．Maple がもっている終結式を計算する核関数を使って，例えば次のようにする．

```
f(t) := t^2 - 1;  g(t) := t * (t^2 - 1);
F(x, y) := resultant(f(t) - x, g(t) - y, t);
```

例 2.9 $x = f(t) = t^2, y = g(t) = t^4$ ならば，$F(x, y) = (x^2 - y)^2$. このとき，$G(x, y) = y - x^2$ として，$F(x, y) = G(x, y)^2$ で，$t = \pm\lambda$ に対して，曲線上の同一点 (λ^2, λ^4) が対応している．



$y = x^2$

多項式パラメータ表示をもつ平面代数曲線でも多くの興味深い例が構成できるが**有理式パラメータ表示**をもつ平面代数曲線を定義しよう．K 係数の多項式を分母と分子に置いた式

$$\frac{a(t)}{b(t)} = \frac{a_0t^m + a_1t^{m-1} + \cdots + a_{m-1}t + a_m}{b_0t^n + b_1t^{n-1} + \cdots + b_{n-1}t + b_n}, \quad b(t) \neq 0$$

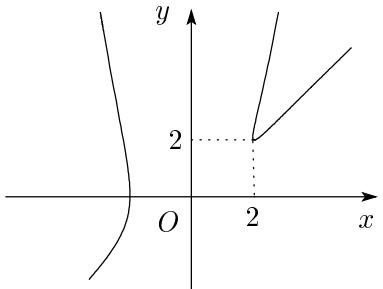
を**有理式**という．有理数の四則演算と同様にして，有理式の間に加法，減法，乗法が定義される．さらに，$a(t) \neq 0$ ならば，有理式 $\dfrac{a(t)}{b(t)}$ は逆元 $\dfrac{b(t)}{a(t)}$ をもつ．すなわち，K 係数の t に関する有理式全体の集合を $K(t)$ で表すと，$K(t)$ は体になる．この体を t に関する K **係数** 1 **変数有理関数体**という．

t の 2 つの有理式を考えよう．

$$(**) \begin{cases} x = \dfrac{a(t)}{b(t)} = \dfrac{a_0t^m + a_1t^{m-1} + \cdots + a_{m-1}t + a_m}{b_0t^n + b_1t^{n-1} + \cdots + b_{n-1}t + b_n}, & a(t) \neq 0,\ b(t) \neq 0 \\ y = \dfrac{c(t)}{d(t)} = \dfrac{c_0t^r + c_1t^{r-1} + \cdots + c_{r-1}t + c_r}{d_0t^s + d_1t^{s-1} + \cdots + d_{s-1}t + d_s}, & c(t) \neq 0,\ d(t) \neq 0 \end{cases}$$

$(**)$ は分母を払えば，係数に x または y を含む 2 つの多項式 $a(t) - xb(t) = 0$ と $c(t) - yd(t) = 0$ に表される．そこで，$F(x, y) = \mathrm{Res}_t(a(t) - xb(t), c(t) - yd(t))$ と定義すれば，$F(x, y) = 0$ はある平面代数曲線の定義方程式となる．

例 2.10 $x = \dfrac{t^2+1}{t}, y = \dfrac{t^3+1}{t^2}$ とすると，$F(x, y) = \mathrm{Res}_t(t^2 - xt + 1, t^3 - yt^2 + 1) = x^3 - yx^2 - (y + 3)x + y^2 + 2y + 2$ となる．曲線 $F(x, y) = 0$ のグラフは次のようになる．



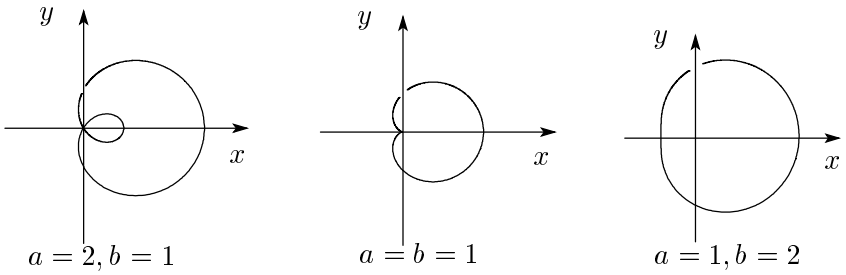
$x^3 - yx^2 - (y + 3)x + y^2 + 2y + 2 = 0$

次の曲線は**リマソン**または**蝸牛線**と呼ばれる代数曲線である．とくに，$a = b$ のときは**心臓形曲線（カルディオイド）**と呼ばれる．

例 2.11 a, b を正の実数として，

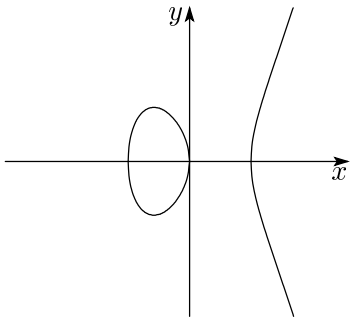
$$x = \frac{-2t(b(t^2+1) - 2at)}{(t^2+1)^2}, \quad y = \frac{(t^2-1)(b(t^2+1) - 2at)}{(t^2+1)^2}$$

とおく．このとき，$F(x, y) = (x^2 + y^2 - ax)^2 - b^2(x^2 + y^2)$ で，そのグラフは次のようになる．



どの平面代数曲線も有理式パラメータ表示ができるわけではない．

例 2.12 $F(x, y) = y^2 - x^3 + 4x = 0$ で定義される平面代数曲線は有理式パラメータ表示をもたない．そのグラフは次のような形をしている．一般に，2 つ以上の連結成分[1]を持つ平面代数曲線は有理式パラメータ表示をもたない．



パラメータ表示 $(x = f(t), y = g(t))$ または $\left(x = \dfrac{a(t)}{b(t)}, y = \dfrac{c(t)}{d(t)}\right)$ をもつ代数曲線の場合，体 K の元 λ に対して曲線上の点

$$(f(\lambda), g(\lambda)) \quad \text{または} \quad \left(\frac{a(\lambda)}{b(\lambda)}, \frac{c(\lambda)}{d(\lambda)}\right)$$

が対応している．また，有理式パラメータ表示の場合には，$b(\lambda) = 0$ または $d(\lambda) = 0$ となるような K の元 λ は避けて考えている．この対応は $1:1$ とは限らないが，次の結果が知られている．

[1] 一筆書きできる閉じた曲線を連結成分という．例 2.10 の場合には，2 つの開いた部分はつながっていないように見えるが，無限遠でつながっている．

定理 2.13 体 K は有理数体 $\mathbb{Q}$ を部分体として含むと仮定する．パラメータ表示 $(x = f(t), y = g(t))$ または $\left(x = \dfrac{a(t)}{b(t)}, y = \dfrac{c(t)}{d(t)}\right)$ をもつ平面代数曲線 C について，次の結果が成立する．

(1) 多項式表示の場合には，t の多項式 $u = h(t)$ と u の多項式 $\varphi(u), \psi(u)$ が存在して，$f(t) = \varphi(h(t)), g(t) = \psi(h(t))$ となり，パラメータ表示

$$\lambda \in K \mapsto (\varphi(\lambda), \psi(\lambda)) \in C$$

は有限個の λ の値を除いて $1:1$ の対応を与える．さらに，

$$F(x,y) = \mathrm{Res}_t(f(t) - x, g(t) - y),\ G(x,y) = \mathrm{Res}_u(\varphi(u) - x, \psi(u) - y),\ N = \deg h(t)$$

とすると，$K \setminus \{0\}$ の元 c が存在して，$F(x,y) = c(G(x,y))^N$ となる．

(2) 有理式表示の場合には，t の有理式 $v = \dfrac{h(t)}{k(t)}$ と v の有理式 $\dfrac{\alpha(v)}{\beta(v)}, \dfrac{\gamma(v)}{\delta(v)}$ が存在して，

$$\frac{a(t)}{b(t)} = \frac{\alpha(h(t)/k(t))}{\beta(h(t)/k(t))}, \quad \frac{c(t)}{d(t)} = \frac{\gamma(h(t)/k(t))}{\delta(h(t)/k(t))}$$

となり，パラメータ表示

$$\lambda \in K \mapsto \left(\frac{\alpha(\lambda)}{\beta(\lambda)}, \frac{\gamma(\lambda)}{\delta(\lambda)}\right)$$

は有限個の λ の値を除いて $1:1$ の対応を与える．さらに，

$$\begin{aligned} F(x,y) &= \mathrm{Res}_t(a(t) - xb(t), c(t) - yd(t)) \\ G(x,y) &= \mathrm{Res}_v(\alpha(v) - x\beta(v), \gamma(v) - y\delta(v)) \\ N &= \max(\deg h(t), \deg k(t)) \end{aligned}$$

とすると，$K \setminus \{0\}$ の元 c が存在して，$F(x,y) = c(G(x,y))^N$ となる．

(3) 多項式パラメータ表示 $(*)$ の場合，$\gcd(m,n) = 1$ ならば，上の対応は $1:1$ である．

証明. (3) のみを体論の基礎知識を使って証明する．その解説については次節を参照されたい．x の有理関数体 $K(x)$ は $K(t)$ の部分体で，拡大 $K(t)/K(x)$ は有限次代数拡大である．また，t の $K(x)$ 上の最小多項式は $f(X) - x$ である．したがって，拡大次数 $[K(t) : K(x)] = m = \deg f(t)$ である．同様にして，$[K(t) : K(y)] = n = \deg g(t)$ である．ここで，

$$[K(t) : K(x)] = [K(t) : K(x,y)][K(x,y) : K(x)],\ [K(t) : K(y)] = [K(t) : K(x,y)][K(x,y) : K(y)]$$

が成立する．よって，$[K(t) : K(x,y)] \mid m$，$[K(t) : K(x,y)] \mid n$．しかるに，$\gcd(m,n) = 1$ だから，$[K(t) : K(x,y)] = 1$．すなわち，$K(t) = K(x,y)$ が成立する．これは，t が K 係数の x, y の有理式 $t = A(x,y)/B(x,y)$ として書けることを意味する．よって，C 上の点 (p,q) を与えるパラメータ t の値は $\lambda = A(p,q)/B(p,q)$ と定まる． 証明終

3　初歩的な体論

体論を体の公理系から始めることも可能であるが，抽象的になりすぎるので，その方面からの入門は大学の教科書に委ねることとしよう．ここでは，加法・減法・乗法・除法の四則演算が定義されている集合と理解しておこう．ただし，体 K で除法が成り立つということは，$a, b \in K$ で $a \neq 0$ のとき，方程式 $ax = b$ が唯一の解をもつということで，その解を $a^{-1}b$ とか b/a と表す．

整数の集合を $\mathbb{Z}$ と書くが，$a, b \in \mathbb{Z}$ で $a \neq 0$ のとき，方程式 $ax = b$ は必ずしも解けない．例えば，$2x = 3$ は $\mathbb{Z}$ に解をもたない．しかし，有理数体 $\mathbb{Q}$ では解 $\frac{2}{3}$ をもつ．別の見方をすれば有理数体は整数係数のどんな方程式 $ax = b$ $(a \neq 0)$ でも解をもつように，$\mathbb{Z}$ にそれらの解の全体を付け加えた集合と考えることもできる．

K 係数の多項式の集合 $K[t]$ は加法・減法・乗法が定義されているが，$\mathbb{Z}$ の場合と同じく，方程式 $a(t)X = b(t)$ $(a(t), b(t) \in K[t], a(t) \neq 0)$ は必ずしも解をもたない．そこで，有理式の全体の集合 $K(t)$ は，$K[t]$ に多項式係数の方程式 $a(t)X = b(t)$ の解を全部付け加えて作ったものと理解することができる．

もう一つの体の作り方は，K を体として K 係数の既約多項式

$$f(t) = a_0 t^m + a_1 t^{m-1} + \cdots + a_{m-1} t + a_m, \quad a_0 \neq 0$$

を考える．方程式 $f(t) = 0$ の解 θ が存在したとして，K に θ を付け加えて K を含む体 $K(\theta)$ を次のように定義する．

$$K(\theta) := \{a(\theta) \mid a(t) \in K[t]\}$$

まず，$K(\theta)$ がもつ性質を考えよう．証明を簡単にするために，$f(t)$ を $a_0^{-1} f(t)$ で置き換えて，$f(t)$ の最高次の係数は 1 と仮定する．このような多項式を**モニック**な多項式という．

補題 3.1　(1) K 係数の多項式 $a(t)$ について，$a(\theta) = 0$ ならば $f(t) \mid a(t)$ である．また，その逆も正しい．

(2) $a(t) \in K[t]$ について，剰余の定理により $a(t) = q(t)f(t) + a'(t),\ a'(t) = 0$ または $0 \leq a'(t) < \deg f(t)$ と表すと，$a(\theta) = a'(\theta)$．このとき，$a'(t) \equiv a(t) \pmod{f(t)}$ と書く．

(3) $a_1(t), a_2(t) \in K[t]$ に対して，$a_3(t), a_4(t)$ を $a_3(t) = a_1(t) + a_2(t), a_4(t) = a_a(t)a_2(t)$ と定義すると，$a_3(\theta) = a_1(\theta) + a_2(\theta), a_4(\theta) = a_1(\theta)a_2(\theta)$．

(4) $a(t) \in K[t]$ について，$a(\theta) \neq 0$ ならば，ある $b(t) \in K[t]$ が存在して $a(\theta)b(\theta) = 1$ となる．

証明.　(1) $h(t) \in K[t]$ をモニックな多項式で $h(\theta) = 0$ となるもののうち次数が最小のものとする．剰余の定理（補題 2.2）によって，$f(t) = q(t)h(t) + r(t),\ r(t) = 0$ または $0 \leq \deg r(t) < \deg f(t)$ とできる．$f(\theta) = 0$ だから，$r(t) \neq 0$ ならば $r(\theta) = 0$ となる．これは $h(t)$ の選び方に反する．よって，$h(t) \mid f(t)$．　しかるに，$f(t)$ はモニックな既約多項式だから，$f(t) = h(t)$ となる．$a(\theta) = 0$ ならば，$a(t) = q'(t)f(t) + r'(t),\ r'(t) = 0$ または $0 \leq \deg r'(t) < \deg f(t)$ とすると，$r'(t) = 0$ でなければならない．すなわち，$f(t) \mid a(t)$．　逆に，$f(t) \mid a(t)$ ならば，$a(t) = f(t)h(t)$ と書くと，$a(\theta) = f(\theta)h(\theta) = 0$.

(2) と (3) は明らかであろう．

(4) $d(t) = \gcd(f(t), a(t))$ とすると，$d(t) \mid f(t)$ かつ $d(t) \mid a(t)$．$f(t)$ は既約多項式だから，$d(t) \sim 1$ または $d(t) = f(t)$ としてもよい．$d(t) = f(t)$ ならば，$a(\theta) = 0$ となって仮定に矛盾する．よって，$d(t) \sim 1$ である．補題 2.4 によって，$b(t), c(t) \in K[t]$ が存在して $a(t)b(t) + f(t)c(t) = 1$ となる．したがって，$a(\theta)b(\theta) = 1$ である． 証明終

補題 3.1 により，$K(\theta)$ は K を含む体になる．別の言葉で言えば，$K(\theta)$ は K の**拡大体**になっている．さらに，$m = \deg f(t)$ に対して，$1, \theta, \theta^2, \ldots, \theta^{m-1}$ は $K(\theta)$ の**基底**である．すなわち，$K(\theta)$ の元 $a(\theta)$ は一意的に

$$a(\theta) = c_0 + c_1\theta + \cdots + c_{m-1}\theta^{m-1}, \quad c_0, c_1, \ldots, c_{m-1} \in K$$

と表される．なぜならば，補題 3.1 の (2) によって，$\deg a(t) < m = \deg f(t)$ と仮定してもよい．もし $b(t) \in K[t], \deg b(t) < \deg f(t)$ に対して，$a(\theta) = b(\theta)$ となれば，補題 3.1 の (1) によって，$f(t) \mid a(t) - b(t)$．$\deg(a(t) - b(t)) < \deg f(t)$ だから，$a(t) = b(t)$ が従う．したがって，上の表示の一意性が分かる．線形代数学の言葉を使えば，$K(\theta)$ は m 次元の K 上のベクトル空間になっている．このとき，$K(\theta)$ は K の**拡大次数** $[K(\theta) : K] = m$ の**有限次代数拡大体**になっているという．

解 θ は K を含む大きな体の中に存在すると仮定して，以上の議論を行った．このような仮定を認めることが煩わしいと思う読者は，次のようにして $K(\theta)$ に相当する K の拡大体 L を作ってもよい．まず，

$$L := \{a(t) \mid \deg a(t) < \deg f(t)\} \cup \{0\}$$

と置く．加法は，$a(t), b(t) \in L$ に対して多項式の和として $a(t)+b(t)$ を対応させる．$a(t)b(t) \equiv c(t) \pmod{f(t)}$, $c(t) \in L$ とするとき，$a(t)$ と $b(t)$ の L における積を $c(t)$ で定義する．このとき，L は上の $K(\theta)$ と加減乗除の四則演算を込めて同じものを考えていることが示される．

補題 3.2 L から $K(\theta)$ への写像を

$$\sigma : L \to K(\theta), \quad \sigma(a(t)) \mapsto a(\theta)$$

で与えると，σ は上への 1 : 1 写像で加法と乗法を保つ．すなわち，σ は次の性質をもつ．

$$\begin{aligned} \sigma(a(t) + b(t)) &= a(\theta) + b(\theta) = \sigma(a(t)) + \sigma(b(t)) \\ \sigma(a(t)b(t)) &= \sigma(c(t)) = c(\theta) = a(\theta)b(\theta) = \sigma(a(t))\sigma(b(t)) \end{aligned}$$

このとき，σ は体の**同型写像**であるという．

証明. σ が上への 1 : 1 写像であることを示そう．$\sigma(a(t)) = \sigma(b(t))$ ならば，$a(\theta) = b(\theta)$．ここで $a(t), b(t) \in L$ だから，$\deg a(t) < \deg f(t)$ かつ $\deg b(t) < \deg f(t)$．よって，$\deg(a(t) - b(t)) < \deg f(t)$．したがって，補題 3.1, (1) により，$a(t) = b(t)$．すなわち，$\sigma$ は 1 : 1 写像である．また，任意の $a(t) \in K[t]$ に対して，補題 3.1, (2) により，$a(t) \equiv a'(t) \pmod{f(t)}$, $a'(t) \in L$ となる．したがって，$a(\theta) = a'(\theta) = \sigma(a'(t))$．すなわち，$\sigma$ は上への写像である．σ が加法と乗法を保つことは容易に示されるので，証明は割愛する． 証明終

この同型写像で $\theta = \sigma(t \pmod{f(t)})$ である．したがって，始めから体 $L = \{a(t) \in K[t] \mid \deg a(t) < \deg f(t)\} \cup \{0\}$ を考えて，θ として $t \pmod{f(t)}$ を取れば，それが方程式 $f(t) = 0$ の一つの解となる．体 L を $K[t]/(f(t))$ と表し，$K[t]$ の $f(t)$ による**剰余体**という．

次の結果を定理 2.13, (3) の証明で使った．

補題 3.3 $K \subset L \subset M$ を体の有限次代数拡大とすると，$[M : K] = [M : L][L : K]$ が成立する．

証明. $m = [L : K]$ として，L の K 上のベクトル空間としての基底を $\{u_1, u_2, \ldots, u_m\}$ とする．また，$n = [M : L]$ として，M の L 上のベクトル空間としての基底を $\{v_1, v_2, \ldots, v_n\}$ とする．このとき，$\{u_i v_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ が K 上のベクトル空間としての M の基底であることを示せばよい．w を M の元とすると，$w = \ell_1 v_1 + \ell_2 v_2 + \cdots + \ell_n v_n$, $\ell_j \in L$ と書ける．また，$\ell_j = k_{j1}u_1 + k_{j2}u_2 + \cdots + k_{jm}u_m$, $k_{ji} \in K$ と書けるから，$w = \sum_{j=1}^{n} \sum_{i=1}^{m} k_{ji} u_i v_j$ と表される．その表し方が一意的であることを示せばよい．$\sum_{j=1}^{n} \sum_{i=1}^{m} k_{ji} u_i v_j = \sum_{j=1}^{n} \sum_{i=1}^{m} k'_{ji} u_i v_j$ とすれば，

$$\begin{aligned} 0 &= \sum_{j=1}^{n} \sum_{i=1}^{m} (k_{ji} - k'_{ji}) u_i v_j \\ &= \left(\sum_{i=1}^{m} (k_{1i} - k'_{1i}) u_i \right) v_1 + \cdots + \left(\sum_{i=1}^{m} (k_{ni} - k'_{ni}) u_i \right) v_n \end{aligned}$$

だから，$1 \leq j \leq n$ について，$\sum_{i=1}^{m} (k_{ji} - k'_{ji}) u_i = 0$. よって，$1 \leq i \leq m$ について，$k_{ji} - k'_{ji} = 0$ となる．よって，$k_{ji} = k'_{ji}$ となる． 証明終