$x^{(q^n-1)/(q-1)} - c \in \mathbb{F}_q[x]$ の因数分解

高校 2 年　黒木 亮汰

$x^{(q^n-1)/(q-1)} - c \in \mathbb{F}_q[x]$ を因数分解します. 有限体に関する命題は
https://www-users.math.umn.edu/~garrett/coding/Overheads/23_proofs.pdf
を参考にしました.
$q(=p^N)$: 素数の冪, $\mathbb{F}_q$: 位数 q の体, n : 正整数, $f(x) \in \mathbb{F}_q[x]$: n 次モニック既約多項式, $L := \mathbb{F}_q[x]/(f(x))$.
自然な埋め込みと射影の合成 $\mathbb{F}_q \to \mathbb{F}_q[x] \to L$ により, $\mathbb{F}_q, \mathbb{F}_q[x]$ の元を L の元と同一視する.

命題 1. $\mathbb{F}_q[x]$ は PID.

証明. $\{0\} = (0)$ は $\mathbb{F}_q[x]$ の単項イデアル. $I \neq \{0\}$ を $\mathbb{F}_q[x]$ のイデアルとすると, I の中で次数が極小の多項式 $f \neq 0$ が取れる. $\mathbb{F}_q$ は体なので, 任意の $g \in I$ を f で割ることができる. 割り算の余りは I の元であり, f の取り方から余りは 0 だから $f|g$. よって $I = (f)$. $\mathbb{F}_q$ は体なので $\mathbb{F}_q[x]$ は整域. 示せた. □

命題 2. L は有限体.

証明. $\mathbb{F}_q[x]$ は PID だから, $I \supset (f(x))$ を $\mathbb{F}_q[x]$ のイデアルとすると, $I = (a)$ となる $a \in \mathbb{F}_q[x]$ があって, $a|f(x)$. $f(x)$ が既約なので, a は単元又は a と $f(x)$ は互いに同伴で, $I = (a) = (\mathbb{F}_q[x]$ 又は $(f(x)))$. よって $(f(x))$ は極大なので, L は体. L の位数は n 次未満の $\mathbb{F}_q$ 係数多項式の個数なので有限性が示せる. □

命題 3. $\Phi : a \mapsto a^q$ は $\mathbb{F}_q$ の恒等写像.

証明. $\mathbb{F}_q^\times$ は位数 $q-1$ の群なので, $a \in \mathbb{F}_q^\times$ の位数は $q-1$ の約数. よって $a^q = a$. これは $a = 0$ でも成り立つ. □

命題 4. Φ は L の自己同型. $a \in L$ について, $\Phi(a) = a \Rightarrow a \in \mathbb{F}_q$.

証明. L は標数 p だから自己準同型であることが分かり, 有限体だから自己同型であることがわかる. $\mathbb{F}_q$ の元は $x^q - x = 0$ の根なので, 因数定理より

$$x^q - x = \prod_{k \in \mathbb{F}_q} (x - k)$$

L は体なので $\Phi(a) = a \Rightarrow a \in \mathbb{F}_q$. □

補題 5. $f(X) \in L[X]$ とみなすと

$$f(X) = \prod_{0 \leq k < n} (X - x^{q^k})$$

よって, L において

$$f(0) = \prod_{0 \leq k < n} (-x^{q^k}) = (-1)^n x^{(q^n-1)/(q-1)}$$

証明. $x \in L$ は $f(X) \in L[X]$ の根なので, 任意の $k \geq 0$ について, $\Phi^k(x)$ は $f(X)$ の根. L は体なので, $f(X)$ の根は高々 n 個. よって, $\Phi^i(x) = \Phi^j(x)$ となる $0 \leq i < j \leq n$ がある. Φ は L の自己同型なので $\Phi^{j-i}(x) = x$. よって, $\Phi^h(x) = x$ となる最小の $h > 0$ があって, $h \leq n$.

$$g(X) := \prod_{0 \leq k < h} (X - \Phi^k(x)) \in L[X]$$

の係数は $\Phi^0(x)(= x), \Phi^1(x), \Phi^2(x), ..., \Phi^{h-1}(x)$ の対称式だから, h の定義より係数は Φ で不変で $g(X) \in \mathbb{F}_q[X]$. $g(X)$ の定義より $g(X)$ は重根を持たないので, $f(X)$ は $g(X)$ を因数に含む. $g(X) \in \mathbb{F}_q[X]$ は 1 次以上のモニック多

項式で, $f(X) \in \mathbb{F}_q[X]$ はモニック既約なので, $f(X) = g(X)$. よって, $g(X)$ は n 次で, $h = n$. よって,

$$f(0) = g(0) = \prod_{0 \le k < n} (-\Phi^k(x)) = (-1)^n x^{(q^n-1)/(q-1)}$$

□

補題 6. m が n の正の倍数ならば, つまり $m = an$ となる $a \in \mathbb{Z}^+$ があるとき,
$x^{(q^m-1)/(q-1)} - (-1)^{n(q^m-1)/(q^n-1)} f(0)^a$ は $f(x)$ を因数に持つ.

証明. $m = an$ となる $a \in \mathbb{Z}$ があるとき, $\mathbb{F}_q$ の元が q 乗で不変であることから, L において

$$f(0)^a = f(0)^{(q^{an}-1)/(q^n-1)} = (-1)^{n(q^m-1)/(q^n-1)} x^{(q^n-1)(q^m-1)/(q-1)(q^n-1)} = (-1)^{n(q^m-1)/(q^n-1)} x^{(q^m-1)/(q-1)}$$

よって $x^{(q^m-1)/(q-1)} - (-1)^{n(q^m-1)/(q^n-1)} f(0)^a$ は $f(x)$ を因数に持つ. □

$\mathbb{F}_q$の元 $c \neq 0$ をとる.

補題 7. $h(x) := x^{(q^n-1)/(q-1)} - c \in \mathbb{F}_q[x]$ は重根を持たない.

証明. $h'(x) = (q^n - 1)x^{(q^n-q)/(q-1)}/(q-1)$ と $h(x)$ は互いに素なので示せた. □

命題 8. m が n の倍数でないとき, $x^{q^m} - x \in \mathbb{F}_q[x]$ は $f(x)$ を因数に持たない.

証明. $L[X]$ において

$$f(X) = \prod_{0 \le k \le n} (X - x^{q^k})$$

であり, L において $\Phi^h(x) = x$ となる最小の $h > 0$ は n なので, $x \neq x^{q^m}$. よって x は $X^{q^m} - X \in L[X]$ の根ではないので, $X^{q^m} - X \in L[X]$ は $f(X)$ を因数に持たない. よって, $x^{q^m} - x \in \mathbb{F}_q[x]$ は $f(x)$ を因数に持たない. □

定理 9. $\mathbb{F}_q[x]$ において

$$x^{(q^n-1)/(q-1)} - c = \prod_{m|n,\ m>0} \left(\prod_{f(x) \text{ は } m \text{ 次モニック既約で } (-1)^{m(q^n-1)/(q^m-1)} f(0)^{n/m} = c} f(x) \right)$$

証明.

$$x \prod_{c \in \mathbb{F}_q^\times} (x^{(q^n-1)/(q-1)} - c) = x(x^{(q-1)(q^n-1)/(q-1)} - 1) = x^{q^n} - x$$

なので, 補題 $6, 7, 8$ から従う. □

系 10. $\mathbb{F}_q[x]$ において

$$x^{q^n} - x = \prod_{m|n,\ m>0} \left(\prod_{f(x) \text{ は } m \text{ 次モニック既約}} f(x) \right)$$

証明. 定理 9 とその証明から従う. □

例 11. (n が素数, q が奇数, $a^{(q^n-1)/(q-1)} = c$ となる $a \in \mathbb{F}_q$がない) $\Rightarrow$ ($n|(q^n-1)/(q-1)$ かつ $-c = (-1)^n c^{(q^n-1)/(n(q-1))}$

証明. $a^{(q^n-1)/(q-1)} = c$ となる $a \in \mathbb{F}_q$ がないならば, 定理 9 の右辺に 1 次の因数はなく, n が素数なので, 右辺には n 次の因数しかない. 左辺が $(q^n-1)/(q-1)$ 次なので $n|(q^n-1)/(q-1)$. $x = 0$ を代入して, $-c = (-1)^n c^{(q^n-1)/(n(q-1))}$. 示せた. □