有限体上の多項式と形式的冪級数

高校 2 年　黒木 亮汰

1　はじめに

p : 素数, $\mathbb{F}_p$: 位数 p の体. $f(x) \in \mathbb{F}_p[[x]]$: 形式的冪級数とみなした, 定数項が 1 の d 次多項式.

$$f(x) = \sum_{l=0}^{d} c_l x^l$$

と表す. $c_0 = 1 \in \mathbb{F}_p$ は単元なので $f(x) \in \mathbb{F}_p[[x]]$ も単元. $f(x) \in \mathbb{F}_p[[x]]$ の逆元を

$$(f(x))^{-1} = \sum_{k \geq 0} s_k x^k$$

と表す.

主定理 1. 相異なる $r_1, \ldots, r_d \in \mathbb{F}_p^{\times}$ によって

$$f(x) = \prod_{m=1}^{d} (1 - r_m x)$$

と表せるならば $s_{p-1} = 1$.

主定理 2. $d \geq 2$, $r \in \mathbb{F}_p^{\times}$ によって $f(x) = (1 - rx)^d$ と分解できる時, $s_{p-1} = 0$.

主定理 3. $p \neq 2$, $d = 2$ として,

(i) 相異なる $r_1, r_2 \in \mathbb{F}_p^{\times}$ によって $f(x) = (1 - r_1 x)(1 - r_2 x)$ と表せる $\iff$ $s_{p-1} = 1$
(ii) $r \in \mathbb{F}_p^{\times}$ によって $f(x) = (1 - rx)^2$ と表せる $\iff$ $s_{p-1} = 0$
(iii) $f(x) \in \mathbb{F}_p[x]$ が既約 $\iff$ $s_{p-1} = -1$

2　主定理 1 の証明

相異なる $r_1, \ldots, r_d \in \mathbb{F}_p^{\times}$ によって

$$f(x) = \prod_{m=1}^{d} (1 - r_m x)$$

と表せるとする. 整数 $k > -d$ について,

$$g_k(x) := \sum_{m=1}^{d} \left(r_m^{k-1+d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{x - r_j}{r_m - r_j} \right)$$

とおく.

命題 2.1. 整数 $1 \leq M \leq d$ について,

$$g_k(r_M) = r_M^{k-1+d}$$

証明. g_k の総和の $m \neq M$ 部分は 0 であり, $m = M$ 部分は r_M^{k-1+d} である. □

$$t_k := \sum_{m=1}^{d} \left(r_m^{k-1+d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right)$$

とおく.

補題 2.2.

$$t_K = \begin{cases} -c_d^{-1} & (K = -d) \\ 0 & (-d < K < 0) \\ 1 & (K = 0) \end{cases} \qquad \sum_{l=0}^{d} c_l t_{k-l} = 0.$$

証明. $g_k(x)$ は高々 $d-1$ 次なので, $1-d < k < 1$ ならば 2.1 と多項式の一致の定理より

$$\sum_{m=1}^{d} \left(r_m^{k-1+d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{x - r_j}{r_m - r_j} \right) = x^{k-1+d}.$$

$x = 0$ を代入し,

$$\sum_{m=1}^{d} \left(r_m^{k-1+d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{-r_j}{r_m - r_j} \right) = 0.$$

$$\left(-\prod_{j=1}^{d} (-r_j) \right) \sum_{m=1}^{d} \left(r_m^{k-2+d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right) = 0.$$

$$t_{k-1} = \sum_{m=1}^{d} \left(r_m^{k-2+d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right) = 0.$$

ここで $k-1$ を K と置きなおせばよい. $k = 1-d$ ならば同様に

$$-\sum_{m=1}^{d} \left(r_m^{0} \prod_{1 \leq j \leq d,\ j \neq m} \frac{-r_j}{r_m - r_j} \right) = -1.$$

$$\left(\prod_{j=1}^{d} (-r_j) \right) \sum_{m=1}^{d} \left(r_m^{-1} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right) = -1.$$

$$t_{-d} = \sum_{m=1}^{d} \left(r_m^{-1} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right) = -c_d^{-1}.$$

$k = 1$ ならば同様に

$$-\sum_{m=1}^{d} \left(r_m^{d} \prod_{1 \leq j \leq d,\ j \neq m} \frac{x - r_j}{r_m - r_j} \right) = \prod_{j=1}^{d} (x - r_j) - x^d.$$

$$\left(\prod_{j=1}^{d} (-r_j) \right) \sum_{m=1}^{d} \left(r_m^{d-1} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right) = \prod_{j=1}^{d} (-r_j).$$

$$t_0 = \sum_{m=1}^{d} \left(r_m^{d-1} \prod_{1 \leq j \leq d,\ j \neq m} \frac{1}{r_m - r_j} \right) = 1.$$

前半が示せた. 後半を示す.

$$\begin{aligned}\sum_{l=0}^{d} c_l t_{k-l} &= \sum_{l=0}^{d}\left(c_l \sum_{m=1}^{d}\left(r_m^{k-l-1+d} \prod_{1\le j\le d,\ j\neq m} \frac{1}{r_m - r_j}\right)\right)\\ &= \sum_{m=1}^{d}\left(r^{k-1+d}\left(\prod_{1\le j\le d,\ j\neq m} \frac{1}{r_m - r_j}\right)\sum_{l=0}^{d} c_l r_m^{-l}\right)\\ &= \sum_{m=1}^{d}\left(r^{k-1+d}\left(\prod_{1\le j\le d,\ j\neq m} \frac{1}{r_m - r_j}\right) f(r_m^{-1})\right)\\ &= 0.\end{aligned}$$

□

系 2.3.

$$\sum_{k=0}^{\infty} t_k x^k = (f(x))^{-1}.$$

証明. 2.2 より

$$\begin{aligned}f(x)\left(\sum_{k=0}^{\infty} t_k x^k\right) &= \left(\sum_{l=0}^{d} c_l x^l\right)\left(\sum_{k=0}^{\infty} t_k x^k\right)\\ &= \left(\sum_{k=0}^{\infty}\left(\left(\sum_{l=0}^{d} c_l t_{k-l}\right)x^k\right)\right) - c_d t_{-d} x^0\\ &= 1.\end{aligned}$$

□

主定理 1.

$$f(x) = \prod_{m=1}^{d}(1 - r_m x) \quad (r_1, \ldots, r_d \in \mathbb{F}_p^{\times} \text{ は相異なる})$$

と表せるならば $s_{p-1} = 1$.

証明. 2.3, フェルマーの小定理より

$$s_{p-1} = t_{p-1} = \sum_{m=1}^{d}\left(r_m^{p-2+d} \prod_{1\le j\le d,\ j\neq m} \frac{1}{r_m - r_j}\right) = \sum_{m=1}^{d}\left(r_m^{d-1} \prod_{1\le j\le d,\ j\neq m} \frac{1}{r_m - r_j}\right) = t_0 = 1.$$

□

3 主定理 2 の証明

主定理 2. $f(x) = (1 - rx)^d \quad (d \ge 2, r \in \mathbb{F}_p^{\times})$ と分解できる時, $s_{p-1} = 0$.

証明.

$$(f(x))^{-1} = (1 - rx)^{-d} = (\sum_{k=0}^{\infty} r^k x^k)^d = \sum_{k=0}^{\infty}\left(\binom{k-1+d}{k} r^k x^k\right).$$

$d \ge 2$ に注意して

$$s_{p-1} = \binom{p-2+d}{p-1} r^{p-1} = 0.$$

□

4　主定理 3 の証明 ($d = 2$ の場合)

この節では $d = 2$ とする. $d = 2$ の時は計算が単純になり, 強い結果が得られる. 主定理 3 の (i),. . . ,(iii) について左から右が従う事を言えば, $f(x)$ としてあり得るすべての多項式について s_{p-1} が求まるので右から左も言える (この時 $p = 2$ だと $1 = -1$ なので右から左をいう事は出来ない). (iii) の左から右は主定理 2 から従う. (i) の左から右は主定理 1 の結果に含まれるが, 別証を書く.

主定理 3. 相異なる $r_1, r_2 \in \mathbb{F}_p^\times$ によって $f(x) = (1 - r_1x)(1 - r_2x)$ と表せるならば, $s_{p-1} = 1$.

証明.

$$\begin{aligned} f(x)^{-1} &= (1 - r_1x)^{-1}(1 - r_2x)^{-1} \\ &= \left(\sum_{k=0}^{\infty} r_1^k x^k\right)\left(\sum_{k=0}^{\infty} r_2^k x^k\right) \\ &= \sum_{k=0}^{\infty}\left(\left(\sum_{j=0}^{k} r_1^{k-j} r_2^j\right) x^k\right) \\ &= \sum_{k=0}^{\infty}\left(\left(\frac{r_1^{k+1} - r_2^{k+1}}{r_1 - r_2}\right) x^k\right) \end{aligned}$$

なので, フェルマーの小定理より

$$s_{p-1} = \frac{r_1^p - r_2^p}{r_1 - r_2} = 1.$$

□

次に, $f(x) \in \mathbb{F}_p[x]$ が既約なときについて考える. 有限体に関する命題が必要なので, 次章に必要な命題の証明を書き, この章では次章の結果を使う.

$L := \mathbb{F}_p[x]/(f(x))$. $\mathbb{F}_p \to \mathbb{F}_p[x] \to L$ により, $\mathbb{F}_p, \mathbb{F}_p[x]$ の元を L の元と同一視する.

命題 4.1. $f(X) = (1 - x^{-1}X)(1 - x^{-p}X)$, $x^{p^2} = x$.

証明. $f(X) \in L[X]$ とみなすと $f(X)$ は $X = x$ を根に持つので, 5.5 より $X = x, x^p, x^{p^2}$ も根に持つ. $f(x) \in \mathbb{F}_p[x]$ は既約なので, $f(x)$ は $\mathbb{F}_p$ に根を持たない. つまり $\mathbb{F}_p$ の元を L の元とみる時, x, x^p, x^{p^2} は $\mathbb{F}_p$ の元ではない. よって, 5.4 より L において $x \neq x^p$, $x^p \neq x^{p^2}$. $f(X) \in L[X]$ は 2 次なので,

$$f(X) = (1 - x^{-1}X)(1 - x^{-p}X).$$

$f(x^{p^2}) = 0$ なので, 5.2 より $(1 - x^{-1}x^{p^2} = 0)$ 又は $(1 - x^{-p}x^{p^2} = 0)$. ここで, $x^p \neq x^{p^2}$ なので $(1 - x^{-p}x^{p^2} \neq 0)$ で $(1 - x^{-1}x^{p^2} = 0)$. よって $x^{p^2} = x$. □

$f(X)$ を形式的冪級数とみなし, $L[[X]]$ の元とみなす.

主定理 3. f が既約ならば, $s_{p-1} = -1$

証明. $L[[X]]$ において,

$$\begin{aligned} f(X)^{-1} &= (1 - x^{-1}X)^{-1}(1 - x^{-p}X)^{-1} \\ &= \sum_{k=0}^{\infty}\left(\left(\frac{(x^{-1})^{k+1} - (x^{-p})^{k+1}}{x^{-1} - x^{-p}}\right) X^k\right) \end{aligned}$$

より

$$s_{p-1} = \frac{(x^{-1})^p - (x^{-p})^p}{x^{-1} - x^{-p}} = \frac{x^{-p} - x^{-1}}{x^{-1} - x^{-p}} = -1$$

□

以上で主定理の証明が完了した. 例としてフィボナッチ数列を載せる.

例 4.2 (フィボナッチ数列)**.**

$$(a_0, a_1) = (1, 1),\ a_n = a_{n-1} + a_{n-2}$$

で数列 $\{a_n\}$ を定めると,

$$\sum_{k=0}^{\infty} a_k x^k = (1 - x - x^2)^{-1}$$

なので, 主定理 3 より奇素数 p を法として

$$\begin{aligned} &1 - x - x^2 \in \mathbb{F}_p[x] \text{ が可約で重根を持たない} &&\iff a_{p-1} \equiv 1 \\ &1 - x - x^2 \in \mathbb{F}_p[x] \text{ が重根を持つ} &&\iff a_{p-1} \equiv 0 \\ &1 - x - x^2 \in \mathbb{F}_p[x] \text{ が既約} &&\iff a_{p-1} \equiv -1 \end{aligned}$$

また, $p \neq 2$ の時

$$1 - x - x^2 = 0 \iff (2x + 1)^2 = 5$$

より, 平方剰余の議論をすると, p を法として

$$\begin{aligned} p \equiv \pm 1 \,(\mathrm{mod} 5) &\iff \left(\frac{5}{p}\right) = 1 \quad \iff a_{p-1} \equiv 1 \\ p = 5 &\iff \left(\frac{5}{p}\right) = 0 \quad \iff a_{p-1} \equiv 0 \\ p \equiv \pm 2 \,(\mathrm{mod} 5) &\iff \left(\frac{5}{p}\right) = -1 \iff a_{p-1} \equiv -1 \end{aligned}$$

例えば $11 \equiv 1 \,(\mathrm{mod} 5)$ であり, $a_{10} = 89 \equiv 1 \,(\mathrm{mod} 11)$ である. □

5 有限体に関する事

[1] を参考にした. $f(x) \in \mathbb{F}_p[x]$: 既約, $L := \mathbb{F}_p[x]/(f(x))$. $\mathbb{F}_p, \mathbb{F}_p[x]$ の元を L の元とみなす.

命題 5.1. $\mathbb{F}_p[x]$ は PID.

証明. $\{0\} = (0)$ は $\mathbb{F}_p[x]$ の単項イデアル. $I \neq \{0\}$ を $\mathbb{F}_p[x]$ のイデアルとすると, $I \backslash \{0\}$ の中で次数が極小の多項式 $f \neq 0$ が取れる. $\mathbb{F}_p$ は体なので, 任意の $g \in I$ を f で (ユークリッドの意味で) 割ることができる. 割り算の余りは I の元であり, f の次数の極小性から余りは 0 だから $f|g$. よって $I = (f)$. $\mathbb{F}_p$ は体なので $\mathbb{F}_p[x]$ は整域. 示せた. □

命題 5.2. L は有限体.

証明. $\mathbb{F}_p[x]$ は PID だから, $I \supset (f(x))$ を $\mathbb{F}_p[x]$ のイデアルとすると, $I = (h)$ となる $h \in \mathbb{F}_p[x]$ があって, $h|f(x)$. $f(x)$ が既約なので, (h は単元) 又は (h と $f(x)$ は互いに同伴) で, $I = (h) = (\mathbb{F}_p[x]$ 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 $\mathbb{F}_p$ 係数多項式の個数以下なので有限性が示せる. □

命題 5.3. $\Phi : a \mapsto a^p$ は $\mathbb{F}_p$ の恒等写像.

証明. $a = 0$ なら明らか. それ以外はフェルマーの小定理. □

系 5.4. Φ は L の自己同型. $a \in L$ について, $\Phi(a) = a \iff a \in \mathbb{F}_p$.

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. $\mathbb{F}_p$ の元は $x^p - x = 0$ の根なので, 因数定理より $\mathbb{F}_p[x]$ において

$$x^p - x = \prod_{k \in \mathbb{F}_p} (x - k).$$

よって $L[X]$ において

$$X^p - X = \prod_{k \in \mathbb{F}_p} (X - k).$$

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

系 5.5. $f(x) \in \mathbb{F}_p[x]$ について, $f(x) \in L[x]$ とみなすと, $a \in L$ について $f(a) = 0$ ならば $f(a^p) = 0$

証明. L は標数 p なので, $f(x)^p$ を展開して計算すると $f(x)^p = f(x^p)$ が成立. よって

$$f(a^p) = f(a)^p = 0.$$

□

6 終わりに

多項式の $\mathbb{F}_p$ におけるふるまいが, フィボナッチ数列のような整数列に現れていることが感じられた. $d \geq 3$ の場合の結果をより精密にしたい.

参考文献

[1] Proofs about Frobenius :
https://www-users.math.umn.edu/~garrett/coding/Overheads/23_proofs.pdf