$\mathbb{F}_q$ 上 n 次既約多項式の個数

高校 2 年 2 組 35 番　中山裕大

1　はじめに

本日は灘校文化祭及び数学研究部にお越しいただき誠にありがとうございます.

この記事では,$\mathbb{F}_q$ 上 n 次既約多項式の個数について書いていきます.

2　準備

以下必要な知識を証明抜きに書く.

$a := b$ とは a を b(に等しいもの) として定義するということを意味する. 整数 a, b に対し,a, b の最大公約数を $\gcd(a, b)$ とかき,a が b を割り切るとき $a|b$ とかく.$\mathbb{Z}^+, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ はそれぞれ正の整数, 非負整数, 整数, 有理数, 実数, 複素数の集合とする.$n \in \mathbb{N}_0$, 数列 $\{a_1, a_2, \ldots\}$, 集合 $A, B, A_1, A_2, \ldots$ に対し

$$\sum_{k=1}^{n} a_k := \begin{cases} a_1 + a_2 + \ldots + a_n & (n > 0) \\ 0 & (n = 0) \end{cases}$$

$$\bigcup_{k=1}^{n} A_k := \begin{cases} A_1 \cup A_2 \cup \ldots \cup A_n & (n > 0) \\ \emptyset & (n = 0) \end{cases}$$

等とし,$\bigcap_{k=1}^{n} A_k$ 等も同様とする. また $A \times B := \{(a, b)|, a \in A, b \in B\}$, $A^n := \{(a_1, a_2, \cdots, a_n)|a_1, a_2, \cdots, a_n \in A\}(n > 0)$, $A \backslash B := \{x \in A|x \notin B\}$ とし,A が B の真部分集合のとき $A \subsetneqq B$ と書く. また $\sharp A$ で A の元の個数を表す (ただし元が無限個のときは $\sharp A := \infty$).

定義 1（体） 集合 K が体であるとは,K に 2 種類の演算 $+$(加法), $\cdot$ (乗法. 以後表記しない) があり,

1. $\forall a, b, c \in K, ((a + b) + c = a + (b + c)$ かつ $(ab)c = a(bc)$ かつ $a(b + c) = ab + ac)$
2. $\forall a, b \in K, (a + b = b + a$ かつ $ab = ba)$
3. $\exists 0 \in K, \forall a \in K, \exists -a \in K, (a + 0 = a$ かつ $a + (-a) = 0)$
4. $\exists 1 \in K \backslash \{0\}, \forall a \in K \backslash 0, \exists a^{-1} \in K, (a1 = a$ かつ $aa^{-1} = 1)$

が成り立つことをいう.

体 L とその部分集合 K に対し,K は L と同じ演算 で体になるとき,L は K の拡大体, K は L の部分体という.またこのとき, $K, a \in L$ を含む最小の体を $K(a)$ と書く.

体 $K, a \in K, n \in \mathbb{Z}^+$ に対し,na で a を n 回足したものを表す.$\{n \in \mathbb{Z}^+|n1 = 0\}$ が空でないとき $char(K) := \min\{n \in \mathbb{Z}^+|n1 = 0\}$, 空の時 $char(K) := 0$ とし,K の標数という. 体の標数は 0 か素数である

ことが知られている.

例 （体） 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は標数 0 の体, $\mathbb{Z}$ は体でない.

2. 素数 p をとり,$\mathbb{F}_p := \{0, 1, 2, \ldots, p-1\}$ において $a + +b :=$ ($a+b$ を p で割った余り), $a \cdot \cdot b :=$ (ab を p で割った余り) とすれば,$\mathbb{F}_p$ は $++, \cdot\cdot$ をそれぞれ加法, 乗法とする標数 p の体となる（証明は略す）.
3. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$

定義 2（体上の多項式） 体 K に対し,K の元を係数にもつ多項式を K 上多項式といい (K の元も K 上多項式とみなす),$K[x]$ を K 上多項式全体の集合とする.$f(x) \in K[x]$ の次数 を $\deg f(x)$ とかく.$\deg 0 := -\infty$ とする.$K[x]$ において定数とは K の元のこととする.$f(x), g(x) \in K(x)$ に対し, ある $h(x) \in K[x]$ が存在して $g(x) = f(x)h(x)$ となるとき $f(x)|_K g(x)$ とかく.$f(x) \in K[x] \backslash K$ が既約多項式とは任意の $g(x), h(x) \in K[x]$ に対し, $f(x) = g(x)h(x)$ ならば $g(x), h(x)$ のうち少なくとも一方は K の元 となることをいう.

体 L が体 K の拡大体で $a \in L$ のとき $K[a] := \{f(a) \in L | f(x) \in K[x]\}$ とおく.

例 （体上の多項式） 1. $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ はそれぞれ有理係数多項式, 実係数多項式, 複素係数多項式の集合.

2. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$
3. 体 L は体 K の拡大体のとき, $a \in L$ に対し $K(a) = \{\frac{g(a)}{f(a)} \in L | f(x), g(x) \in K[x], f(a) \neq 0\}$ である.

定義 3（微分） K を体とするとき,$f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_0 \in K[x]$ ($n > 0 \Rightarrow \alpha_n \neq 0$) に対し, $f'(x) := n\alpha_n x^{n-1} + (n-1)\alpha_{n-1} x^{n-2} + \ldots + \alpha_1$ とし,$f(x)$ の微分という.

和の微分の公式, 定数倍の微分の公式, 積の微分の公式は実解析と同様に成立することがわかる.

定義 4（代数閉体） 体 K が代数閉体であるとは,$\forall f(x) \in K[x] \backslash K, \exists a \in K, f(a) = 0$ となることである.

例 （代数閉体） $\mathbb{Q}, \mathbb{R}$ は代数閉体ではない (上の記号で $f(x) := x^2 + 1$ とすればよい).$\mathbb{C}$ は代数閉体であることが知られている (代数学の基本定理).

定理 5 p は 0 または素数とするとき標数 p の代数閉体が存在する.

代数閉体上の n 次 ($n \in \mathbb{Z}^+$) 多項式 $f(x)$ は重複度をこめてちょうど n 個の根 $a_1, a_2, \ldots, a_n \in F$ を持ち, $f(x) = \alpha(x - a_1)(x - a_2)\ldots(x - a_n)$ ($\alpha \neq 0$) と書けることが知られている.

以下 p は素数, q は p の正の整数乗とする.標数 p の代数閉体を 1 つとり F と書く. 以下の議論は F の取り方によらないことが知られている.

補題 6 $\forall a, b \in F, \forall m \in \mathbb{Z}^+, (a+b)^{p^m} = a^{p^m} + b^{p^m}$

証明

$$\begin{aligned} \forall a, b \in F, (a+b)^p &= \sum_{k=0}^{p} \left({}_pC_k a^k b^{p-k}\right) \\ &= a^p + b^p \end{aligned}$$

$$\left(\because 1 \leqq \forall k \leqq p-1, k_pC_k = p_{p-1}C_{k-1} \left(= \tfrac{p!}{(k-1)!(p-k)!}\right) \Rightarrow p|_pC_k\right)$$

$$\begin{aligned}\therefore \forall a,b\in F,\forall m\in\mathbb{Z}^+,(a+b)^{p^m} &= (a^p+b^p)^{p^{m-1}}\\ &= \dots\\ &= a^{p^m}+b^{p^m}\end{aligned}$$

■

定義 7　$m\in\mathbb{Z}^+$に対し $\mathbb{F}_{p^m}:=\{x\in F|x^{p^m}=x\}$ とおく.$\mathbb{F}_{p^m}$は p^m個の元を持つ唯一の F の部分体であることが知られている (体であることの証明には補題 6 を用いる).

補題 8　$m_1,m_2\in\mathbb{Z}^+$に対し

1. $\mathbb{F}_{p^{m_1}}\cap\mathbb{F}_{p^{m_2}}=\mathbb{F}_{p^{\gcd(m_1,m_2)}}$
2. $m_1|m_2\Rightarrow\mathbb{F}_{p^{m_1}}\subsetneqq\mathbb{F}_{p^{m_2}}$

証明　1. まず $\mathbb{F}_{p^{m_1}}\cap\mathbb{F}_{p^{m_2}}\subsetneqq\mathbb{F}_{p^{\gcd(m_1,m_2)}}$ を示す.$a\in\mathbb{F}_{p^{m_1}}\cap\mathbb{F}_{p^{m_2}}$ のとき,$a=0$ なら自明に $a\in\mathbb{F}_{p^{\gcd(m_1,m_2)}}$.$a\neq0$ のとき $a^{p^{m_1}-1}=a^{p^{m_2}-1}=1$ が成立. 対称性より $m_1\leqq m_2$ としてよい. すると,

$$\begin{aligned}&a^{(p^{m_1}-1)-(p^{m_2}-1)}=1\\ \Leftrightarrow\ &a^{(p^{m_1-m_2}-1)p^{m_2}}+(-1)^{p^{m_2}}=0\ (\because p>2\text{ ならよい.}p=2\text{ のとき }-1=1\text{ よりよい.})\\ \Leftrightarrow\ &(a^{p^{m_1-m_2}-1}-1)^{p_2^m}=0\ (\because\text{補題 6})\\ \Leftrightarrow\ &a^{p^{m_1-m_2}-1}-1=0\Leftrightarrow a^{p^{m_1-m_2}-1}=1\end{aligned}$$

同様に (ユークリッドの互除法のように) 繰り返すことにより $a^{p^{\gcd(m_1,m_2)}-1}=1\therefore a\in\mathbb{F}_{p^{\gcd(m_1,m_2)}}$
次に $\mathbb{F}_{p^{m_1}}\cap\mathbb{F}_{p^{m_2}}\supsetneqq\mathbb{F}_{p^{\gcd(m_1,m_2)}}$ を示す.$a\in\mathbb{F}_{p^{\gcd(m_1,m_2)}}$のとき

$$\begin{aligned}a^{p^{\gcd(m_1,m_2)}} &= a\\ \therefore a^{p^{m_1}} &= a^{(p^{\gcd(m_1,m_2)})^{\frac{m_1}{\gcd(m_1,m_2)}}}\\ &= a^{(p^{\gcd(m_1,m_2)})^{\frac{m_1}{\gcd(m_1,m_2)}-1}}\\ &= \dots\\ &= a\\ \therefore a&\in\mathbb{F}_{p^{m_1}}\end{aligned}$$

同様に $a\in\mathbb{F}_{p^{m_2}}$ より $a\in\mathbb{F}_{p^{m_1}}\cap\mathbb{F}_{p^{m_2}}$. よって示された.

2. 1. より

$$\mathbb{F}_{p^{m_1}}\cap\mathbb{F}_{p^{m_2}}=\mathbb{F}_{p^{\gcd(m_1,m_2)}}=\mathbb{F}_{q^{m_1}}\therefore\mathbb{F}_{p^{m_1}}\subsetneqq\mathbb{F}_{p^{m_2}}$$

■

定義 9（ベクトル空間）　集合 V が体 K 上ベクトル空間 であるとは,V 上の演算 $+$(加法) があり,$k\in K,\boldsymbol{a}\in V$ に対し $k\boldsymbol{a}$(スカラー倍) が一意に定まり,

1. $\forall\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in V,(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$
2. $\forall\boldsymbol{a},\boldsymbol{b}\in V,\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a}$
3. $\exists\boldsymbol{0}\in V,\forall\boldsymbol{a}\in V,\exists-\boldsymbol{a}\in V,(\boldsymbol{a}+\boldsymbol{0}=\boldsymbol{a}\text{ かつ }\boldsymbol{a}+(-\boldsymbol{a})=\boldsymbol{0})$
4. $\forall k,l\in K,\forall\boldsymbol{a}\in V,(k+l)\boldsymbol{a}=k\boldsymbol{a}+l\boldsymbol{a}$
5. $\forall k\in K,\forall\boldsymbol{a},\boldsymbol{b}\in V,k(\boldsymbol{a}+\boldsymbol{b})=k\boldsymbol{a}+k\boldsymbol{b}$

6. $\forall k,l \in K, \forall \boldsymbol{a} \in V, (kl)\boldsymbol{a} = k(l\boldsymbol{a})$
7. $\forall \boldsymbol{a} \in V, 1\boldsymbol{a} = \boldsymbol{a}$

が成り立つことをいう.

体 K 上のベクトル空間 V の部分集合 U が

1. $\forall n \in \mathbb{Z}^+, \forall k_1, k_2, \ldots, k_n \in K, \forall \boldsymbol{u_1}, \boldsymbol{u_2}, \ldots, \boldsymbol{u_n} \in U, (k_1\boldsymbol{u_1} + k_2\boldsymbol{u_2} + \ldots + k_n\boldsymbol{u_n} = \boldsymbol{0} \Rightarrow k_1 = k_2 = \ldots = k_n = 0)$ を満たすとき,U は一次独立であるという. そうでないとき U は一次従属という.
2. $\forall \boldsymbol{v} \in V, \exists n \in \mathbb{Z}^+, \exists k_1, k_2, \ldots, k_n \in K, \exists \boldsymbol{u_1}, \boldsymbol{u_2}, \ldots, \boldsymbol{u_n} \in U, k_1\boldsymbol{u_1} + k_2\boldsymbol{u_2} + \ldots + k_n\boldsymbol{u_n} = \boldsymbol{v}$ を満たすとき,U は生成系であるという.

K 上 ベクトル空間 V には空でない一次独立な生成系 U が存在することが知られており, そのような U を V の基底 という. ベクトル空間の基底の個数は基底の取り方によらず一定であることが知られており, それを (K 上) ベクトル空間 V の次元といい,$\dim_K V$ で表す.$\dim_K V$ が有限のとき,$V, K^{\dim_K V}$ の間には「ベクトル空間の構造を保存」する全単射があり, また集合 $U \subsetneqq V$ に対し $\sharp U > \dim_K V$ のとき U は一次従属である ことが知られている.

体 K 上のベクトル空間 V とその部分集合 U に対し,U は V と同じ加法, スカラー倍でベクトル空間になるとき,U は V の部分ベクトル空間という.このとき $\dim_K U \leqq \dim_K V$ が知られている.

例 （ベクトル空間）　1. K が体で $n \in \mathbb{Z}^+$のとき, K^nにおいて $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n, k \in K$ のとき

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) := (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$$
$$k(a_1, a_2, \cdots, a_n) := (ka_1, ka_2, \cdots, ka_n)$$

として加法, スカラー倍を定義すれば K^nは K 上ベクトル空間となる.

2. 体 L は体 K の拡大体のとき,L は K 上ベクトル空間. このとき,$[L : K] := \dim_K L$ とする.
3. 体 K に対し $K[x]$ は K 上無限次元ベクトル空間. 基底は $\{1, x, x^2, x^3, \ldots\}$

3　最小多項式

定理 10　K は体, L は K の拡大体とする.$a \in L$ に対し,$f(a) = 0$ なる $f(x) \in K[x]\backslash K$ が存在するとき ,$g(a) = 0$ かつ $\forall f(x) \in K[x], f(a) = 0 \Rightarrow g(x)|_K f(x)$ なる最高次の項の係数が 1 の $g(x) \in K[x]\backslash K$ は一意に定まる.このとき $g(x)$ は既約で,$K(a) = K[a]$ かつ $\deg g(x) = [K(a) : K]$.この $g(x)$ を a の K 上最小多項式という.

証明　まず, 条件を満たす $g(x)$ は一意に存在することを示す.

(存在)

条件より $f(a) = 0$ なる $f(x) \in K[x]\backslash K$ であって次数が最小なもの $g_0(x)$ がとれる.$g_0(x)$ の最高次の項の係数を $\alpha(\neq 0)$ とし,$g(x) := \alpha^{-1}g_0(x)$ とおくと, この $g(x)$ が条件を満たすことを示す.

まず $g(a) = \alpha g_0(a) = \alpha 0 = 0$.

次に,$f(x) \in K[x]\backslash K$ が $f(a) = 0$ を満たすとき,$f(x)$ を $g(x)$ で割った商, 余りをそれぞれ $q(x), r(x)(\in K[x])$ とおくとき $r(a) = f(a) - g(a)q(a) = 0 - 0q(a) = 0$. すると,$r(x) \neq 0$ と仮定すると,$\deg r(x) <$

$\deg g(x) = \deg g_0(x)$ より $g_0(x)$ の次数の最小性に矛盾. よって $r(x) = 0 \Leftrightarrow g(x)|_K f(x)$.

また,$g(x) = \alpha^{-1} g(x)$ の最高次の項の係数は $\alpha^{-1}\alpha = 1$.

よって,$g(x)$ は条件を満たす.

(一意性)

$g_1(x), g_2(x) \in K[x]\backslash K$ が条件を満たすとき,$g_1(x) = g_2(x)$ を示せばよい. 条件より $g_1(x)|_K g_2(x)$. 同様に $g_2(x)|_K g_1(x)$. すると,$g_1(x)$ は $g_2(x)$ の 0 でない定数倍. 最高次の項の係数の比較により $g_1(x) = g_2(x)$.

あとはこの $g(x)$ が既約で $K(a) = K[a]$ かつ $\deg g(x) = [K(a) : K]$ であることを示せばよい.

$g(x)$ が既約でないと仮定すると,$g(x) = h_1(x)h_2(x)$ $(h_1(x), h_2(x) \in K[x]\backslash K)$ とおけ, このとき $0 = g(a) = h_1(a)h_2(a) \therefore (h_1(a) = 0$ または $h_2(a) = 0)$. 対称性より $h_1(a) = 0$ としてよい. 今 $1 \leqq \deg h_1(x) = \deg g(x) - \deg h_2(x) \leqq \deg g(x) - 1 = \deg g_0(x) - 1$ なので $g_0(x)$ の次数の最小性に矛盾. よって $g(x)$ は既約.

次に $K(a) = K[a]$ を示す.$K(a) \supseteqq K[a]$ は自明.$K(a) \subseteqq K[a]$ を示す.$K(a)$ の各元は $\frac{p(a)}{q(a)}$ $(p(x), q(x) \in K[x], p(a) \neq 0)$ と書ける.$p(a) \neq 0$ なので $g(x) \nmid p(x)$. これと $g(x)$ は既約より $p(x), g(x)$ は互いに素. すると,

$$\begin{aligned} &\exists s(x), t(x) \in K[x] \ , \ s(x)p(x) + t(x)g(x) = 1 \ (\because \text{ユークリッドの互除法のようにすればよい}) \\ &\Rightarrow s(a)p(a) = s(a)p(a) + t(a)0 = s(a)p(a) + t(a)g(a) = 1 \\ &\Rightarrow \frac{q(a)}{p(a)} = q(a)s(a) \in K[a] \end{aligned}$$

よって $K(a) \subseteqq K[a]$. よって示された.

最後に $\deg g(x) = [K(a) : K]$ を示す.$1, a, a^2 \ldots, a^{\deg g(x)-1}$ が基底となることを示せばよい. まず,$k_1 1 + k_2 a + k_3 a^2 + \ldots + k_{\deg g(x)} a^{\deg g(x)-1} = 0$ $(k_1, k_2, k_3, \ldots, k_{\deg g(x)-1} \in K)$ のとき,$k_1 = k_2 = k_3 = \ldots = k_{\deg g(x)-1} = 0$ でなければ,$g(x)$ より次数が小さく a を代入すると 0 になる多項式 $k_1 1 + k_2 a + k_3 a^2 + \ldots + k_{\deg g(x)} a^{\deg g(x)-1}$ がとれ,$g_0(x)(g(x))$ の次数の最小性に矛盾. よって $k_1 = k_2 = k_3 = \ldots = k_{\deg g(x)-1} = 0$. 次に,$K(a)(= K[a])$ の各元は $f(a)$ $(f(x) \in K[x])$ と表されるが,$f(x)$ を $g(x)$ で割った商, 余りをそれぞれ $q(x), r(x) \in K[x]$ $(\deg r(x) < \deg g(x))$ とおくと

$$\begin{aligned} f(x) &= g(x)q(x) + r(x) \\ \therefore f(a) &= g(a)q(a) + r(a) = 0q(a) + r(a) = r(a) \end{aligned}$$

ここで,$\deg r(x) < \deg g(x)$ より $r(a) = k_1 1 + k_2 a + k_3 a^2 + \ldots + k_{\deg g(x)} a^{\deg g(x)-1} = 0$ $(k_1, k_2, k_3, \ldots, k_{\deg g(x)-1} \in K)$ と表せる. よって,$\{1, a, a^2 \ldots, a^{\deg g(x)-1}\}$ は ベクトル空間 $K(a)$ の K 上 基底であり, 示された.

■

例　$\sqrt{-1}$ の $\mathbb{Q}$ 上最小多項式,$\mathbb{R}$ 上最小多項式はともに $x^2 + 1$

4　完全性

以下,$f(x) \in \mathbb{F}_q[x]$ に対し,$f(x)$ の根とは $f(a) = 0$ なる $a \in F$ のこととする. 定理 12 をこの節の目標とする.

補題 11　$f(x) \in \mathbb{F}_q[x]$ が重根を持つには, $f(a) = 0$ かつ $f'(a) = 0$ なる $a \in F$ が存在する.

証明　($\Rightarrow$)

$f(x)$ は重根 a を持つとすると $f(x)=(x-a)^2g(x)$ $(g(x)\in F[x])$ とおける. このとき $f'(x)=2(x-a)g(x)+(x-a)^2g'(x)$ より $f(a)=f'(a)=0$.

($\Leftarrow$)

$f(a)=f'(a)=0, a\in F$ のとき,$f(a)=(x-a)g(x), g(x)\in F[x]$ とおけ, このとき $f'(x)=g(x)+(x-a)g'(x)$ $\therefore 0=f'(a)=g(a)$ より $g(x)=(x-a)h(x)$ とおける. すると $f(x)=(x-a)g(x)=(x-a)^2h(x)$ より $f(x)$ は重根 a をもつ.

■

定理 12　任意の $\mathbb{F}_q$ 上既約多項式 $f(x)$ は重根をもたない[*1].

証明　$f(x)$ は重根 a をもつと仮定する.$f(a)=0$ より a の $\mathbb{F}_q$ 上最小多項式 $f_0(x)$ をとれる.$f(a)=0$ より $f_0(x)|_{\mathbb{F}_q}f(x)$ で,$f(x)$ は既約より $f(x)$ は $f_0(x)$ の 0 でない定数倍.

すると,$\deg f_0(x)=\deg f(x)>\deg f'(x)$. これと $f_0(x)|_{\mathbb{F}_q}f'(x)$($\because$ 補題 11 より $f'(a)=0$) より $f'(x)=0$.$f(x)=:\alpha_nx^n+\alpha_{n-1}x^{n-1}+\ldots+\alpha_0$ $(n>0,\alpha_n\neq 0)$ とおくと

$$\begin{aligned}0=f'(x)&=n\alpha_nx^{n-1}+(n-1)\alpha_{n-1}x^{n-2}+\ldots+\alpha_1\\ \therefore 1\leqq\forall i\leqq n,\alpha_i\neq 0&\Rightarrow p|i\end{aligned}$$

より $g_k(x^{p^k})=f(x)$ なる $k\in\mathbb{Z}^+, g_k(x)\in\mathbb{F}_q[x]$ がとれ, そのような最大の k を m とおく.$g_m(x)=:\beta_{n'}x^{n'}+\beta_{n'-1}x^{n'-1}+\ldots+\beta_0$ $(n'=\frac{n}{p^m},\beta_{n'}=\alpha_n\neq 0)$ とおくと

$$\begin{aligned}&\left(\beta_{n'}^{\frac{q^m}{p^m}}x^{n'}+\beta_{n'-1}^{\frac{q^m}{p^m}}x^{n'-1}+\ldots+\beta_0^{\frac{q^m}{p^m}}\right)^{p^m}\\ &=\beta_{n'}^{q^m}x^{n'p^m}+\beta_{n'-1}^{q^m}x^{(n'-1)p^m}+\ldots+\beta_0^{q^m}\ (\because\text{補題 6})\\ &=\beta_{n'}^{q^{m-1}}x^{n'p^m}+\beta_{n'-1}^{q^{m-1}}x^{(n'-1)p^m}+\ldots+\beta_0^{q^{m-1}}\ (\because\mathbb{F}_q\text{の定義})\\ &=\ldots\\ &=\beta_{n'}x^{n'p^m}+\beta_{n'-1}x^{(n'-1)p^m}+\ldots+\beta_0\ (\because\mathbb{F}_q\text{の定義})\\ &=g_m(x^{p^m})=f(x)\end{aligned}$$

より $f(x)$ は既約でないので矛盾. よって $f(x)$ は重根を持たない.

■

5　既約多項式の個数

定理 13　$n\in\mathbb{Z}^+$に対し $\mathbb{F}_q$ 上 n 次既約多項式の個数は

$$\frac{q-1}{n}\sum_{d|n,d\in\mathbb{Z}^+}\left(\mu\left(\frac{n}{d}\right)q^d\right)$$

[*1] このことを体 $\mathbb{F}_q$ は完全体であるという.

ここで,

$$\begin{array}{rccc} \mu: & \mathbb{Z}^+ & \longrightarrow & \mathbb{Z} \\ & \cup & & \cup \\ & n & \longmapsto & \begin{cases} 1 & (n=1 \text{ のとき}) \\ (-1)^k & (\text{相異なる素数 } p_1,p_2,\ldots,p_k \text{を用いて } n=p_1p_2\ldots p_k \text{と書けるとき}) \\ 0 & (\text{その他のとき}) \end{cases} \end{array}$$

証明　$\mathbb{F}_q$ 上 n 次既約多項式の個数を N とおく.n の素因数の集合を P(ただし $n=1$ なら $P=\emptyset$) とおく.$a\in F$ に対し

$\exists f(x)\in\mathbb{F}_q[x], f(x)$ は n 次で既約かつ $f(a)=0$

$\Leftrightarrow f(x)$ は n 次で既約かつ $f(a)=0$[*2]かつ a の $\mathbb{F}_q$上最小多項式 $f_0(x)$ に対し $f_0(x)|_{\mathbb{F}_q}f(x)$

$\Leftrightarrow f(a)=0$ かつ $f(x)$ は n 次で a の $\mathbb{F}_q$上最小多項式 $f_0(x)$ の 0 でない定数倍

$\Leftrightarrow \exists f_0(x)\in\mathbb{F}_q[x], f_0(a)=0$ かつ $f_0(x)$ は a の $\mathbb{F}_q$上最小多項式で $\deg f_0(x)=n$

$\Leftrightarrow [\mathbb{F}_q(a):\mathbb{F}_q]=n$ ($\because(\Rightarrow)$ 定理 10

($\Leftarrow$)$\{1,a,a^2,\ldots,a^n\}$ は定義 9 の議論より一次従属 $\therefore g(a)=0$ なる $g(x)\in K[x]\backslash K$ がとれる.

あとは定理 10 を用いる.)

$\Leftrightarrow a\in\mathbb{F}_{q^k}$なる最小の k は n

($\because(\Rightarrow)$ 定義 9 の議論より$\sharp\mathbb{F}_q(a)=q^n$ $\therefore$ 定義 7 の議論より $\mathbb{F}_q(a)=\mathbb{F}_{q^n}$.すると

$a\in\mathbb{F}_{q^n}$は自明に成立.$k<n$ に対し $a\in\mathbb{F}_{q^k}$のとき$\sharp\mathbb{F}_{q^k}=q^k<q^n=\sharp\mathbb{F}_{q^n}$なので補題 8 より

$\mathbb{F}_q\subsetneqq\mathbb{F}_{q^k}$ $\therefore \mathbb{F}_q(a)\subsetneqq\mathbb{F}_q\cup\mathbb{F}_{q^k}=\mathbb{F}_{q^k}\subsetneqq\mathbb{F}_{q^n}$となり矛盾.

($\Leftarrow$) 補題 8 より $\mathbb{F}_q\subsetneqq\mathbb{F}_{q^n}$ $\therefore \mathbb{F}_q(a)\subsetneqq\mathbb{F}_q\cup\mathbb{F}_{q^n}=\mathbb{F}_{q^n}$ $\therefore$ 定義 9 の議論より $[\mathbb{F}_q(a):\mathbb{F}_q]\leqq[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$.

また定義 9 の議論より$\sharp\mathbb{F}_q(a)=q^{[\mathbb{F}_q(a):\mathbb{F}_q]}$ $\therefore$ 定義 7 の議論より $\mathbb{F}_q(a)=\mathbb{F}_{q^{[\mathbb{F}_q(a):\mathbb{F}_q]}}$.

すると $[\mathbb{F}_q(a):\mathbb{F}_q]<n$ と仮定すると n の最小性に矛盾. $\therefore [\mathbb{F}_q(a):\mathbb{F}_q]=n$.)

$$\begin{aligned} \Leftrightarrow a &\in \mathbb{F}_{q^n}\backslash\bigcup_{k=1}^{n-1}\mathbb{F}_{q^k} \\ &= \mathbb{F}_{q^n}\backslash\bigcup_{k=1}^{n-1}(\mathbb{F}_{q^k}\cap\mathbb{F}_{q^n}) \\ &= \mathbb{F}_{q^n}\backslash\bigcup_{k=1}^{n-1}\mathbb{F}_{q^{\gcd(k,n)}} \ (\because \text{補題 8}) \\ &= \mathbb{F}_{q^n}\backslash\bigcup_{i\in P}\mathbb{F}_{q^{\frac{n}{i}}} \ (\because \text{補題 8 より } 1\leqq\forall k\leqq n-1,\exists i\in P,\gcd(k,n)|\frac{n}{i}\Rightarrow\mathbb{F}_{q^{\gcd(k,n)}}\subseteqq\mathbb{F}_{q^{\frac{n}{i}}}) \end{aligned}$$

定理 12 より各 $\mathbb{F}_q$ 上 n 次既約多項式に対し, 代入して多項式の値が 0 になる F の元は n 個. またある $\mathbb{F}_q$ 上 n 次既約多項式 $f_0(x)$ に代入して多項式の値が 0 に なるような各々の $a\in F$ に対し,a の $\mathbb{F}_q$上最小多項式を $g(x)$ とおくと,$f(x)\in\mathbb{F}_q[x]\backslash\mathbb{F}_q$ に対し

$(\deg f(x)=n$ かつ $f(x)$ は既約かつ $f(a)=0)\Leftrightarrow f(x)$ は $g(x)$ の 0 でない定数倍

($\because(\Rightarrow)f(a)=0$ より $g(x)|_{\mathbb{F}_q}f(x).f(x)$ は既約より $f(x)$ は $g(x)$ の 0 でない定数倍.

($\Leftarrow$)$f_0(a)=0$ より $g(x)|_{\mathbb{F}_q}f_0(x).f_0(x)$ は既約より $f_0(x)$ は $g(x)$ の 0 でない定数倍.

$\therefore \deg g(x)=\deg f_0(x)=n$.あとは自明.)

[*2] a の $\mathbb{F}_q$上 最小多項式 $f_0(x)$ の存在を保証する為にこのような条件は残しておく.

より,$\deg f(x)=n$ かつ $f(x)$ は既約かつ $f(a)=0$ なる $f(x)\in\mathbb{F}_q[x]\backslash\mathbb{F}_q$ は $\sharp(\mathbb{F}_q\backslash\{0\})=q-1$ 個. よって

$$nN=(q-1)\sharp\left(\mathbb{F}_{q^n}\setminus\bigcup_{i\in P}\mathbb{F}_{q^{\frac{n}{i}}}\right)\left(=\sharp\{(f(x),a)\in\mathbb{F}_q[x]\times F|\deg f(x)=n,f(x)\text{ は既約},f(a)=0\}\right)$$

$$\begin{aligned}\therefore N&=\frac{q-1}{n}\sharp\left(\mathbb{F}_{q^n}\setminus\bigcup_{i\in P}\mathbb{F}_{q^{\frac{n}{i}}}\right)\\&=\frac{q-1}{n}\sharp\left(\mathbb{F}_{q^n}+\sum_{j=1}^{\sharp P}(-1)^j\sum_{i_1<i_2<\ldots<i_j,i_1,i_2,\ldots i_j\in P}\sharp\left(\bigcap_{k=1}^{j}\mathbb{F}_{q^{\frac{n}{i_k}}}\right)\right)\ (\because\text{包除の原理})\\&=\frac{q-1}{n}\left(q^n+\sum_{j=1}^{\sharp P}(-1)^j\sum_{i_1<i_2<\ldots<i_j,i_1,i_2,\ldots i_j\in P}\mathbb{F}_{q^{\gcd(\frac{n}{i_1},\frac{n}{i_2},\ldots,\frac{n}{i_j})}}\right)\ (\because\text{補題 8})\\&=\frac{q-1}{n}\left(q^n+\sum_{j=1}^{\sharp P}\sum_{i_1<i_2<\ldots<i_j,i_1,i_2,\ldots i_j\in P}(-1)^jq^{\gcd(\frac{n}{i_1},\frac{n}{i_2},\ldots,\frac{n}{i_j})}\right)\\&=\frac{q-1}{n}\left(\mu\left(\frac{n}{n}\right)q^n+\sum_{1\leqq j\leqq\sharp P,i_1<i_2<\ldots<i_j,i_1,i_2,\ldots i_j\in P}\mu\left(\frac{n}{\frac{n}{i_1i_2\ldots i_j}}\right)q^{\frac{n}{i_1i_2\ldots i_j}}\right)\\&=\frac{q-1}{n}\sum_{d|n,d\in\mathbb{Z}^+}\left(\mu\left(\frac{n}{d}\right)q^d\right)\ (\because\mu\text{の定義})\end{aligned}$$

■

6　終わりに

いかがでしたか. この記事は,JMO 夏季セミナーというイベントにおいて証明なしで紹介されていたものを示そうと思って書いたものです. 実際に書いてみると予備知識が重きを占める記事となってしまったので, あまり載せるのに適した内容ではないかと思われましたが, 実力のなさと準備期間の短さの為にこの記事を載せることとなってしまいました. 本当に申し訳ございません. 来年はもう少し精進したいと思います. それでも, 最初は訳がわからなかった式の意味が明確に見えたのは嬉しかったです.

今後の展望としては, 多変数の $\mathbb{F}_q$ 上 n 次既約多項式を数え上げることが考えられます (が, その場合はそれなりに大きな方針転換が必要な気がします). 文化祭後も考えていきたいと思います.

この記事にも必ず誤植があるでしょうが, 大したことがなければお許し下さい.

最後になりますが, ここまで拙い記事をお読みいただき有り難うございました. 他の記事も是非お読みになって下さい.

7　参考文献

2014 年度の JMO 夏季セミナーでいただいた資料を参考にさせていただきました.