有限体の存在の証明

黒木 玄

2008 年 4 月 24 日 (木)

目 次

0 はじめに

p は素数であるとし, n は正の整数であるとする. $\mathbb{F}_p = \mathbb{Z}/(p)$ と置くと $\mathbb{F}_p$ は位数 p の有限体である. 位数 p^n の有限体の存在は複数の方法で証明可能である. このノートでは以下の 2 つの方法を紹介することにする:

1. 多項式の完全分解体の存在を使う方法,
2. 有限体上の既約多項式の存在定理を使う方法.

このノートは後者がメインであり, 副産物として有限体 $\mathbb{F}_q$ 係数のモニックな n 次既約多項式の個数の公式と $\mathbb{F}_q[X]$ に関する Riemann 予想の類似の結果が得られる.

1 多項式の完全分解体の存在を使う方法

$\mathbb{F}_p$ 係数の多項式 $f(X) = X^{p^n} - X$ の完全分解体の一つを Ω と表わし, Ω における $f(X)$ の根全体の集合を F と定めると, F が Ω の位数 p^n の有限部分体であることを容易に示せる.

2 有限体上の既約多項式の存在定理を使う方法

μ は Möbius 函数であるとする. すなわち, 正の整数 m について, m が平方因子を持つとき $\mu(m) = 0$ であり, m が互いに異なる r 個の素数の積で表わされるとき $\mu(m) = (-1)^r$ であるとする.

次の定理を示せば位数 p^n の有限体の存在の証明も得られる.

定理 2.1 位数 q の有限体 $\mathbb{F}_q$ 係数のモニックな n 次既約多項式の個数 a_n は次のように表わされる:

$$a_n = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d, \qquad d \text{ は } n \text{ の約数全体を走る.} \quad \square$$

この定理より, 任意の正の整数 n に対して $a_n \neq 0$ であることが容易に確かめられる. 特に $\mathbb{F}_p$ 係数のモニックな n 次既約多項式 f が存在し, $F = \mathbb{F}_p[X]/(f(X))$ によって位数 p^n の有限体 F を構成可能である.

補題 2.2 (Möbius の反転公式) $\displaystyle\sum_{d|n} x_d = y_n$ ならば $\displaystyle x_n = \sum_{d|n}\mu\left(\frac{n}{d}\right)y_d$.

略証. $\zeta(s) = \sum_{m=1}^{\infty} m^{-s}$, $X(s) = \sum_{d=1}^{\infty} x_d d^{-s}$, $Y(s) = \sum_{n=1}^{\infty} y_n n^{-s}$ と置く. このとき $\sum_{d|n} x_d = y_n$ は $\zeta(s)X(s) = Y(s)$ と同値である. Euler 積表示 $\zeta(s) = \prod_{p\text{ は素数}}(1-p^{-s})^{-1}$ を用いて $\zeta(s)^{-1}$ を計算すると $\zeta(s)^{-1} = \sum_{m=1}^{\infty}\mu(m)m^{-s}$ となることがわかる. よって $X(s) = \zeta(s)^{-1}Y(s)$ から $x_n = \sum_{d|n}\mu\left(\frac{n}{d}\right)y_d$ が導かれる. $\square$

Möbius の反転公式は純代数的にも比較的容易に証明される.

定理 2.1 の証明. 函数 $Z(u)$ を次の Euler 積によって定める:

$$Z(u) = \prod_P \frac{1}{1-u^{\deg P}} = \prod_{d=1}^{\infty}\left(\frac{1}{1-u^d}\right)^{a_d}.$$

ここで P は $\mathbb{F}_q$ 係数のモニック既約多項式全体を走る. a_d は $\mathbb{F}_q$ 係数のモニックで次数 d の既約多項式全体の個数と定義されたのであった.

$\mathbb{F}_q[X]$ は UFD なので $\mathbb{F}_q$ 係数のモニック多項式は $\mathbb{F}_q$ 係数のモニックな既約多項式の積で表示され, その表示は積の順序を除けば一意的である. よって u のべき級数としての $Z(u)$ の u^k の係数は $\mathbb{F}_q$ 係数のモニックな k 次多項式全体の個数 q^k に等しい. すなわち

$$Z(u) = \sum_{k=0}^{\infty} q^k u^k = \frac{1}{1-qu}.$$

$Z(u)$ の二つの表示の対数を取ることによって, $-\sum_{d=1}^{\infty} a_d \log(1-u^d) = -\log(1-qu)$ が成立することがわかる. さらに Taylor 展開 $-\log(1-x) = \sum_{n=1}^{\infty} x^n/n$ を適用し, 両辺における u^n/n の係数を比較すれば次が成立することがわかる:

$$\sum_{d|n} d a_d = q^n.$$

したがって Möbius の反転公式より定理 2.1 の結果が得られる. $\square$

以上の証明はゼータ函数や Euler 積の威力がよくわかる点が面白いと思う.

注意 2.3 $\sum_{d|n} d a_d = q^n$ の右辺の q^n は $\mathbb{F}_{q^n}$ の元の個数に等しく, 左辺の $d a_d$ は $\mathbb{F}_{q^n}$ の元でその $\mathbb{F}_q$ 係数の最小多項式の次数が d であるものの個数に等しい. $\square$

3 $\mathbb{F}_q[X]$ に関する Riemann 予想の類似の結果

Euler-Riemann のゼータ函数は次のように定義される:

$$\zeta(s) = \prod_{p\ \text{は素数}} \frac{1}{1-p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^{-s}}$$

ここで二つ目の等号は整数の素因数分解の一意性から得られる. 右辺の定義式は $\operatorname{Re} s > 1$ で収束している. Euler-Riemann のゼータ函数は複素平面全体上の有理型函数に解析接続される. (元来の) Riemann 予想 (Riemann Hypothesis) とは「Euler-Riemann のゼータ函数の $0 \leqq \operatorname{Re} s \leqq 1$ におけるすべての零点は直線 $\operatorname{Re} s = 1/2$ の上にある」という予想 (conjecture) のことである. Riemann 予想は x 以下の素数の個数 $\pi(x)$ に関する次の評価と同値であることが知られている: ある定数 $C > 0$ が存在して

$$|\pi(x) - \mathrm{li}_e(x)| \leqq Cx^{1/2}\log x, \qquad \mathrm{li}_e(x) := \int_e^\infty \frac{dt}{\log t} = \int_1^{\log x} \frac{e^u}{u}du.$$

前節の結果を用いてこの評価の $\mathbb{F}_q[X]$ での類似を証明しよう.

Euler-Riemann のゼータ函数の $\mathbb{F}_q[X]$ での類似物は前節の定理の証明で定義した $Z(u)$ に $u = q^{-s}$ を代入したものである. $Z(q^{-s}) = 1/(1-q^{1-s})$ の零点は存在しない.

x 以下の素数の個数 $\pi(x)$ の $\mathbb{F}_q[X]$ での類似物は $\log_q x$ 次以下のモニックな既約多項式の個数 $\pi_q(x)$ である. 次の定理は $\mathbb{F}_q[X]$ に関する Riemann 予想の類似物である.

定理 3.1 ある定数 $C > 0$ が存在して

$$|\pi_q(x) - \mathrm{li}_q(x)| \leqq Cx^{1/2}\log_q x, \qquad \mathrm{li}_q(x) := \sum_{1 \leqq n \leqq \log_q x} \frac{q^n}{n}.$$

証明. 前節の定理の結果より,

$$\pi_q(x) = \sum_{1 \leqq n \leqq \log_q x} a_n = \sum_{1 \leqq n \leqq \log_q x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

$\mathrm{li}_q(x)$ は右辺を $d = n$ に制限した部分和に等しい. よって

$$|\pi_q(x) - \mathrm{li}_q(x)| = \left| \sum_{1 \leqq n \leqq \log_q x} \frac{1}{n} \sum_{d|n,\, d<n} \mu\left(\frac{n}{d}\right) q^d \right|.$$

n の約数で n より小さいものは $n/2$ 以下になり, Möbius 函数は $0, \pm 1$ に値を取るので,

$$\left| \sum_{d|n,\, d<n} \mu\left(\frac{n}{d}\right) q^d \right| \leqq \sum_{1 \leqq d \leqq n/2} q^d \leqq \frac{n}{2} q^{n/2}.$$

よって

$$|\pi_q(x) - \mathrm{li}_q(x)| \leqq \frac{1}{2} \sum_{1 \leqq n \leqq \log_q x} q^{n/2} \leqq \frac{1}{2} \sum_{1 \leqq n \leqq \log_q x} x^{1/2} \leqq \frac{1}{2} x^{1/2} \log_q x. \quad \square$$