代数学 II 要約 NO.12

今日のテーマ:

1 変数の方程式のゼータ関数 II, 平方剰余の相互法則

前回、次の補題が残ってしまっていた。

補題 12.1. *(補題 11.6 と同じ)* $\mathbb{F}_q$ 上の既約な *1* 変数 n 次多項式 $f(X)$ が与えられているとする。このとき、

(1) $f(X)$ が $\mathbb{F}_{q^r}$ のなかに根をもつのは r が n の倍数のときに限る。
(2) r が n の倍数ならば、$\mathbb{F}_{q^r}$ のなかの $f(X)$ の根はちょうど n 個ある。

命題 12.1. *(命題 11.1 と同じ)* $\mathbb{F}_q$ 上の既約な *1* 変数多項式 n 次多項式 $f(X)$ に対して、$V(f)$ の合同ゼータ関数は

$$Z(V(f),t) = 1/(1-t^n)$$

で与えられる。

一般に、ゼータ関数が p によってどのように変わるかは複雑である。例えば X^2-5 は各素数 p に対して $\mathbb{F}_p$ 上の多項式と見られるが、それが既約かどうかは p によって異なる。どのような p に対して既約であるかを判定するのに便利なのが、平方剰余記号とその相互法則である。相互法則の証明はいろいろ知られているが、この講義の話の応用として有限体上のガウス和を用いた証明を紹介する。

定義 12.1. 奇素数 p と、p で割れない整数 a に対して、平方剰余記号 (Legendre 記号) を

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (X^2-a \text{ が } \mathbb{F}_p \text{ 上可約のとき}) \\ -1 & (X^2-a \text{ が } \mathbb{F}_p \text{ 上既約のとき}) \end{cases}$$

により定義する。a が p の倍数の時には、$\left(\frac{a}{p}\right)=0$ と定義する。

補題 12.2. 奇素数 p に対して、次の式が成り立つ。

(1)
$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$$

(2)
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

とくに $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ にも注意しておく。

定義 12.2. p, ℓ は相異なる奇素数であるとし、$\mathbb{F}_p$ の拡大体の 1 の原始 ℓ-乗根 λ を取る。整数 a に対して、有限体のガウス和 τ_a を

$$\tau_a = \sum_{t=1}^{\ell-1} \left(\frac{t}{\ell}\right)\lambda^{at}$$

で定義する。τ_1 のことを単に τ とかく。

(1) $\tau_a = \left(\frac{a}{\ell}\right)\tau$.
(2) $\sum_{a=0}^{l-1} \tau_a \tau_{-a} = \ell(\ell-1)$.
(3) $\tau^2 = (-1)^{(\ell-1)/2}\ell$ $(= \ell^*$ と書く$)$.
(4) $\tau^{p-1} = (\ell^*)^{(p-1)/2}$.
(5) $\tau^p = \tau_p$.

(なぜ、上の補題のような計算をしたくなるのか、その一つのヒントはフーリエ級数論にある。)

上の補題を使うと次の定理を証明できる。但し (3) の証明は問題に譲る。

定理 12.2 (平方剰余の相互法則). 奇素数 ℓ に対して次の等式が成り立つ。

(1) $\left(\frac{p}{\ell}\right) = \left(\frac{\ell^*}{p}\right)$ (但し $\ell^* = (-1)^{(\ell-1)/2}\ell$)
(2) $\left(\frac{-1}{\ell}\right) = (-1)^{(\ell-1)/2}$
(3) $\left(\frac{2}{\ell}\right) = (-1)^{(\ell^2-1)/8}$

問題 12.1. $\mathbb{F}_{359}$ 上の多項式 $X^2 - 113$ は既約かどうか判定しなさい。ヒントをつけると簡単すぎるのでノーヒント。

問題 12.2. p は奇素数であるとする。$\mathbb{F}_p$ 上の多項式 $f(X) = X^2 - 5$ に対して、その定める方程式 (系) $V(f)$ のゼータ関数 $Z(V(f), t)$ を求めよ。

問題 12.3. 奇素数 p に対して、
$X^4 + 1 \in \mathbb{F}_p[X]$ の根を ζ とするとき、

(1) $x = \zeta + \zeta^{-1}$ の二乗 x^2 をもとめなさい。
(2) $p = \pm 1 \mod 8$ のとき、$x^p - x$ を求めなさい。
(3) $p = \pm 3 \mod 8$ のとき、$x^p + x$ を求めなさい。
(4) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ を示しなさい。