代数学 II 要約 NO.13

今日のテーマ:

平方剰余の相互法則 II

前回、平方剰余の相互法則の証明が残ってしまっていた。ガウスの和の定義の復習から書いておこう。

定義 13.1. 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。

ついでにこの定義の意味についてもう少しだけ述べておこう。まず、上の λ は次のようにしてとることができる。$\mathbb{F}_{p^{\ell-1}}^{\times}$ は位数 $p^{\ell-1}-1$ の巡回群で、その生成元を ξ とおく。フェルマーの小定理により $p^{\ell-1}-1$ は ℓ で割り切れるから、$\xi^{(p^{\ell-1}-1)/\ell}$ を考えることができる。この元の位数はちょうど ℓ であるから、これを λ とすればいい。なお、λ の取り方は一意的ではなく、1 の ℓ 乗根は λ^a $a = 0, 1, 2, \ldots, p-1$ の p 個ある。これらに対応して τ_a ができる。下の補題の (1) はそれらが符号の差を除いて等しいことを述べている。ただし、$a = 0$ のときだけは特別で、$\tau_0 = 0$ がなりたつ。

補題 13.1. 次の等式が成り立つ。

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

定理 13.1 (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 $\ell^* = (-1)^{(\ell-1)/2}\ell$)

問題 13.1. $p = 31$, $\ell = 5$ にたいして、$\mathbb{F}_p$ の 1 の原始 ℓ-乗根を一つ見つけ、ガウスの和 τ を求めて、τ^2 を実際に計算してみなさい。

問題 13.2. 奇素数 ℓ と、体 K が与えられていて、1 の原始 ℓ 乗根 λ が K のなかに存在するとする。(とくに、K の標数は ℓ ではない。) $\mathbb{F}_\ell$ 上の K-値関数の全体 V は (各点ごとの加法、スカラー倍により) K 上のベクトル空間になり、V 上に内積が

$$\langle f, g \rangle = \sum_{a=0}^{\ell-1} f(a)g(-a)$$

で定まる。(証明不要)

(1) V の K 上の次元を求めよ。(答のみでよい。)

$$\chi_a(x) = \lambda^{ax}$$

で定義するとき、内積 $\langle \chi_a, \chi_b \rangle$ を求めよ。

(3) $\{\chi_a\}_{a=0}^{\ell-1}$ は V の基底であることを示しなさい。さらに、V の元 f を

$$f = \sum_{a=0}^{\ell-1} c_a \chi_a$$

と書くためには、 $c_a \in K$ をどのように求めればよいか、述べなさい。

問題 13.3. 前問と同じ仮定の下で、フーリエ変換 $\mathcal{F} : V \to V$ を、

$$\mathcal{F}[f](a) = \langle f, \chi_a \rangle$$

で定義する。このとき、

(1) $\langle \mathcal{F}[f], \chi_a \rangle = \ell f(-a)$ がなりたつことを示しなさい。

(2) $\mathcal{F}[\mathcal{F}[f]]$ を計算し、$\mathcal{F}$ の逆変換を求めなさい。

(3) 任意の $f, g \in V$ に対して、$\langle \mathcal{F}[f], g \rangle = \langle f, \mathcal{F}[g] \rangle$ が成り立つことを示しなさい。

(4) $f_L \in V$ を

$$f_L(a\ 1_{\mathbb{F}_\ell}) = \left(\frac{a}{\ell}\right) 1_K \qquad (a \in \mathbb{Z})$$

で定義する。f_L は $\mathcal{F}$ の固有ベクトルであることを示し、それが属する固有値を求めなさい。