代数学 II 要約 NO.11

今日のテーマ:

$\boxed{\text{フロベニウス写像・1変数の方程式のゼータ関数}}$

補題 11.1. R は環で、ある素数 p があって、$p_R = \overbrace{1_R + 1_R + \cdots + 1_R}^{p\text{ 個}} = 0_R$ が成り立っているとする。このとき、$\Phi : R \to R$ を $\Phi(x) = x^p$ で定義すれば、Φ は R からそれ自身への準同型 *(*自己準同型*)* を与える。

Φ を k 回繰り返した写像 $(\Phi)^k$ は

$$(\Phi)^k(x) = x^{p^k}$$

で与えられることにも注意しておく。

定義 11.1. 素数 p のベキ $q = p^s$ にたいして、$\mathbb{F}_q$ の拡大体 $\mathbb{F}_{q^r}$ の自己同型

$$\Phi_q : x \mapsto x^q$$

を $\mathbb{F}_{q^r}$ の $\mathbb{F}_q$ 上のフロベニウス自己同型と呼ぶ。

補題 11.2. $f(X)$ は $\mathbb{F}_q$ 上の n 次の既約多項式だとする。このとき、f の根の一つを α とすると、

(1) $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ はそれぞれ f の根である。
(2) f の根は上で挙げたもので尽きている。

補題 11.3. $\mathbb{F}_{q^r}$ の $\mathbb{F}_q$ 上の自己同型 *(*$\mathbb{F}_{q^r}$ から $\mathbb{F}_{q^r}$ への自己同型写像で $\mathbb{F}_q$ に制限すると恒等写像になるもの*)* の全体は、 Φ_q によって生成される位数 r の巡回群である。

次の補題は補題 11.2 の (1) の拡張にあたる。

補題 11.4. n 変数の多項式 $f_1, f_2, \ldots, f_m \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ の決める方程式系 $V_1 = V(f_1, f_2, \ldots, f_m)$ に対して、「フロベニウス写像」$\Phi_q : V_1(F_{q^r}) \ni x \mapsto \Phi_q(x) \in V_1(F_{q^r})$ を次のようにして定義できる。

$$\Phi_q(x_1, x_2, \ldots, x_n) = (\Phi_q(x_1), \Phi_q(x_2), \ldots, \Phi_q(x_n))$$

x が Φ_q の不動点 *(*$\Phi_q(x) = x$*)* であることと、$x \in V_1(F_q)$ であることとは同値である。

本講義では触れないが、上の補題は合同ゼータ関数の性質を調べる最初のヒントになる。

1変数方程式のゼータ関数を決定しておこう。まず既約性についての簡単な補題から

補題 11.5. $\mathbb{F}_q$ 上の *1*変数 n 次多項式 $f(X)$ に対して、

(1) f の既約因子 q は f と $X^{q^k} - X \quad (k = \deg(q))$ との共通因子である。
(2) f が既約であるための必要十分条件は、$k = 1, 2, \ldots, n-1$ の各々に対し、$f(X)$ と $X^{q^k} - X$ とが共通因子をもたないことである。

例えば、$\mathbb{F}_q$ 上の *4*次または *5*次の *1*変数多項式 $f(X)$ は、$X^{q^2} - X$ と共通因子をもたなければ既約である。

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 11.1. $\mathbb{F}_q$ 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。

今回の話をもちいると、次の２問はかなり解きやすくなる。

問題 8.1 次のような (1)-(3) の例を ((4) が解きやすいように) 作り,(4) を 求めなさい。

(1) 素数 $p > 2$
(2) 正の整数 $n > 2$
(3) $\mathbb{F}_p$ 上の相異なる n 次既約多項式 $f, g \in \mathbb{F}_p[X]$
(4) $\mathbb{F}_p[X]/f(X)\mathbb{F}_p[X]$ での g の一次式への分解

問題 9.1 $p = 5$ とする。 $\mathbb{F}_p$ 上のモニックな 4 次既約多項式 f の例を挙げ、 f の一つの根を α とした時、 f の他の根を α であらわしなさい。 (つまり、 f を $\mathbb{F}_p[\alpha]$ 上で一次式の積に分解しなさい。)

問題 11.1. $\mathbb{F}_3$ 上の多項式 $f(X) = X^4 + 1$ に対して、

(1) f を $\mathbb{F}_3$ 上の既約な多項式の積に分解しなさい。
(2) $V(f)$ の合同ゼータ関数 $Z(V(f),t)$ を求めよ。

(ヒント: f は $\mathbb{F}_3$ 上既約ではないので、命題 11.1 はそのままでは使えない。)

問題 11.2. 4 で割ると 3 余るような素数 p に対しては、$a \in \mathbb{Z}/p\mathbb{Z}$ をどのように選んでも、 $X^4 - a$ は $\mathbb{Z}/p\mathbb{Z}$ 上既約にならないことを示しなさい。

問題 11.3. 4 で割ると 1 余るような素数 p に対して、$(\mathbb{Z}/p\mathbb{Z})^\times$ の生成元 r をとる。このとき、

(1) $r^{(p^2-1)/4} = -1$ であることを示しなさい。
(2) $X^4 - r$ は $\mathbb{Z}/p\mathbb{Z}$ 上既約であることを示しなさい。

(ヒント:任意の素数 $p > 2$ と $(\mathbb{Z}/p\mathbb{Z})^\times$ の生成元 r とに対して、$r^{(p-1)/2}$ は $(\mathbb{Z}/p\mathbb{Z})^\times$ の位数 2 の元である。(なぜか？))

問題 11.4. $\mathbb{F}_p$ の元 a で、どんな $b \in \mathbb{F}_p$ をとってきても $b^2 \neq a$ を満たすものが与えられたとする。$f(X) = X^2 - a$ とし、$R = \mathbb{F}_p[X]/f(X)\mathbb{F}_p[X]$ を $\mathbb{F}_p$ 上の 2 次元ベクトル空間と見たとき、$R \ni r \mapsto r^2 \in R$ を表示するような 2 次行列 A をもとめ、$\mathrm{tr}(A^k)$ を計算しなさい。$V(X^2 - a)$ の合同ゼータ関数とこの結果の関係について、わかることを (思い付く限り) 述べよ。

($\mathrm{tr}(A^k)$ は $\mathbb{F}_p$ の元であるから、「個数」という量 ($\mathbb{Z}$ の元) と比べると少し情報量が落ちる。この問題で、$X^2 - a$ を任意の既約多項式に置き換えても同様のことができるのだが、それは少し難しすぎるので、ここでは問題としては課さない。)