代数学 I 特論要約 NO.7

今日のテーマ

フロベニウス準同型

標数 p の体や、それを含む環には、面白い自己準同型が存在する。

命題 7.1. R は (単位元をもつ可換) 環で、$p_R = 0_R$ であるとする。(これは R が $\mathbb{F}_p$ を含むと言っても同じ。)

このとき、$\phi : R \to R$ を

$$\phi(x) = x^p$$

で定めると、ϕ は R から R への環準同型になる。(ϕ のことをフロベニウス準同型と呼ぶ。)

この命題を用いて先週やり残した部分を証明しておこう。

補題 7.1. p は素数であるとし、$q = p^n$ (n は正の整数) とする。標数 p の任意の体 K に対して、

$$\{x \in K; x^q = x\}$$

は K の (有限) 部分体をなす。

さらに次のことの証明が残っていた。

- 元の数が p^n の体は同型を除いて唯一つである。
- 任意の素数 p と任意の正の整数 d に対して、$\mathbb{F}_p$ 上の既約 d 次式が少なくとも一つ存在する。

ついでに多項式の性質の落ち穂拾いもしておこう。

- 体上の一変数 d 次多項式の根は d 個以下である。
- 体 K 上の一変数多項式 $f(X)$ にたいして、その微分 $f'(X)$ が定義される。微分は

$$(af + bg)' = af' + bg' \quad (fg)' = f'g + fg' \quad (f, g \in K[X], a, b \in K)$$

なる公式を満足する。

- 体上の一変数多項式 f が重根をもつ必要十分条件は、f と f' が共通因数をもつことである。

命題 7.2. 有限体上の既約な一変数多項式は重根をもたない。

問題 7.1.

(1) 素数 $p > 10$ を選んで $\mathbb{F}_p$ 上の 3 次既約多項式 $f(X) \in \mathbb{F}_p[X]$ の例を一つ挙げなさい。

(2) 上の p, f に対して、$L = \mathbb{F}_p[X]/(f(X)\mathbb{F}_p[X])$ とおく。L での X のクラスを a と書いたとき、a, a^p, a^{p^2} を求めなさい。

(3) f の L での根を a を用いてあらわし、L 上で f を因数分解しなさい。