代数学 I 特論要約 NO.8

今日のテーマ

有限体のガロア理論

補題 8.1. 体 K から 体 L への環準同型写像は必ず単射である。もしそのような準同型写像が存在すれば、K と L の標数は等しい。

定義 8.1. 体 K の拡大体 L にたいし、L から L への環自己同型で、K 上恒等写像に等しいものを L の K 上の自己同型という。L の K 上の自己同型の全体を $\mathrm{Aut}_K(L)$ で書きあらわす。

補題 8.2. $\mathbb{F}_{p^r}$ から $\mathbb{F}_{p^s}$ への環準同型写像が存在するための必要十分条件は、 r が s の約数であることである。さらに、そのとき $\mathbb{F}_{p^r}$ から $\mathbb{F}_{p^s}$ への環準同型写像の像は一意的である。

上の補題により、正の整数 s, t にたいして、$\mathbb{F}_{p^s}$ は $\mathbb{F}_{p^{st}}$ の部分体と見るのが普通であるので、以下そのようにする。

命題 8.1.

$$\mathrm{Aut}_{\mathbb{F}_{p^s}}(\mathbb{F}_{p^{st}}) \cong C_t$$

ここで、左辺の生成元としては

$$\phi^s(x) = x^{p^s}$$

(ϕ は前回出て来たフロベニウス写像。ϕ^s は$\mathbb{F}_{p^s}$ に関するフロベニウス準同型と呼ばれる) を採ることができる。

定理 8.2. $\mathbb{F}_{p^s}$ と $\mathbb{F}_{p^{st}}$ のあいだの中間体と、C_t の部分群とは一対一に対応する。

問題 8.1. $\mathbb{F}_3$ 上の多項式 $f(X) = X^6 + X - 1$ について、

(1) **f は $\mathbb{F}_3$ 上一次の因数をもたないことを示しなさい。**
(2) **f は $\mathbb{F}_3$ 上二次の因数をもたないことを示しなさい。(ヒント: f と $X^{3^2} - X$ との GCD を考えよ。)**
(3) **f は $\mathbb{F}_3$ 上三次の因数をもたないことを示しなさい。**
(4) **f は既約であることを示しなさい。(これを直接示すような解答を得た場合には上の (1)-(3) は省略しても構わない。)**
(5) **$K = \mathbb{F}_3$ と $L = \mathbb{F}_3[X]/f(X)\mathbb{F}_3[X]$ の中間体を全て求めよ。**