代数学 I 特論要約 NO.6

今日のテーマ

有限体の乗法群は巡回群であること

定義 6.1 (**オイラーの関数**). $1, 2, \ldots, n$ **の中で、**n **と互いに素な数の個数を** $\varphi(n)$ **と書く。**

補題 6.1. 位数 n **の巡回群を** $C_n = \langle a; a^n = e \rangle$ **とかく。このとき、**

(1) $\varphi(n)$ **は、**C_n **の生成元** *(=***位数がちょうど** n **と一致するもの***)* **の個数と等しい。**

(2) **一般に、**C_n **の元のうち位数がちょうど** d **に一致するものの個数は、**

$$\begin{cases} \phi(d) & (d \text{ が } n \text{ の約数のとき}) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

であたえられる。

補題 6.2. 体 K **の乗法群** $K^\times$ **の元で、位数が** n **のものは** $\varphi(n)$ **個以下である。**

命題 6.1. 有限体 K **の乗法群** $K^\times$ **は必ず巡回群である。**

補題 6.3. p **は素数であるとし、**$q = p^n$ *(*n **は正の整数***)* **とする。このとき、**$\mathbb{F}_p$ **の多項式** $f(X) = X^q - X$ **について、**$\mathbb{F}_p$ **の拡大体** K **で、次のような性質をみたすものが存在する。**

(1) f **は** K **上の多項式として一次式の積に分解する。**

(2) K **の元は全て** f **の根である。**

有限体の元の個数は必ず素数の巾だったことを思い出しておこう。逆に、次のことが成り立つ。

定理 6.2. 素数 p **の巾** p^n **が与えられたとき、元の個数が** p^n **の体** K **が存在する。**K **は同型を除いて一意的である。**

系 6.1. 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。**

定義 6.2. 元の個数が $q = p^n$ **の体のことを** $\mathbb{F}_q$ **と書く。**

問題 6.1. 10 **以上の素数** p **と** 2 **以上の整数** d **を各自で決めて、**$\mathbb{F}_p$ **上既約かつモニックな多項式を二つ与え** (f, g)**、**$\mathbb{F}_p[X]/f(X)\mathbb{F}_p[X]$ **での** g **の根を書き下しなさい。**