# 代数学 II 要約 NO.5

今日のテーマ:

$\boxed{\text{有限体上の線型代数について}}$

諸君は線型代数と言うと $\mathbb{R}$ や $\mathbb{C}$ の上のそれしか知らないかも知れないが、一般の体についても線型代数学の知識はほとんどそのまま使える。例えば、行列, 行列式, 逆行列 (ガウスの掃き出し法など), 線型空間とその基底、線型写像、などは体が違ってもほとんど扱いは変わらない。例えば問題 5.1 を解いて感じをつかんで頂きたい。

但し、行列の固有値などについて固有方程式を解く必要があるので、その根の取り扱いについて知るまで待たなければならない。また、ノルムの正値性などを使う部分 (二次形式の理論など) は修正する必要があったり、問題によっては体の差が大きく効いてくる場合もある。臨機応変に対応して頂きたい。

**定義 5.1.** 体 $K$ の部分集合 $k$ が $0, 1$ を含み、$K$ の演算をそのまま流用して体になっている時、$k$ は $K$ の部分体である ($K$ は $k$ の拡大体である) と言う。$K$ が $k$ の拡大体ならば、$K$ は $k$ 上の線型空間でもある。$K$ の $k$ 上の線型空間としての次元 $\dim_k K$ を $[K : k]$ で書き表し、$K$ の $k$ 上の拡大次数と呼ぶ。($[K : k]$ は有限でない時もある。) $[K : k]$ が有限である時、すなわち $K$ が $k$ 上の線型空間として有限次元である時、 $K$ は $k$ の有限次拡大であると言う。

**補題 5.1.** $p$ は $k[X]$ の既約元であるとする。このとき、$k[X]/(p(X)k[X])$ の $k$ 上の拡大次数は $\deg(p)$ と等しい。

**補題 5.2.** $k$ の拡大体 $M$, $M$ の拡大体 $L$ が与えられている時、

$$[L : M][M : k] = [L : k]$$

がなりたつ。

**補題 5.3.** 有限体 $k$ の拡大体 $L$ の $k$ 上の拡大次数が $d$ ならば、

$$(\#L) = (\#k)^d$$

がなりたつ。とくに、$k$ の標数を $p$ と書くと、$(\#k)$ の元の個数は必ず $p^N$ *($N$ は正の整数)* の形をしている。

(#? は ? の元の数をあらわす記号である。)

**問題 5.1.** $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ の元を成分に持つ行列

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 1 \end{pmatrix}$$

の行列式と逆行列とを求めなさい。