代数学 II 要約 NO.4

今日のテーマ:

$\boxed{\text{1 変数多項式環とその剰余環 (2), } \mathbb{F}_p \text{ の単純拡大体}}$

先週、次の定理が残ってしまっていた。

定理 4.1 (定理 3.2 とおなじ)**.** 体 k 上の多項式 $f, g \in k[X] \setminus \{0\}$ に対して、次のような多項式 $a, b, d \in k[X]$ が存在する。

(1) d は f, g の公約数である。(すなわち、$f, g \in dk[X]$)

(2) $af + bg = d$.

次の系は有限体 (等いろいろな体) を作る際の基本である。

系 4.1. $k[X]$ の元 $p(X)$ が既約 (つまり、$p(X)$ の約数は $p(X)$ 自身の定数倍か、定数に限る) ならば、$k[X]/p(X)k[X]$ は体である。

k が有限体 (例えば、$\mathbb{F}_p$) ならば上の補題のようにして作られた体は必然的に有限体になる。

$K = k[X]/p(X)k[X]$ での X のクラスを ξ と書くと、K は k に ξ という一つの元を付け加えた体になっている。このような体を k の単純拡大体と呼ぶ。

$k[X]$ の既約元を発見する方法についてはあとあと述べる予定であるが、取りあえず次のことぐらいはとりあえず知っておくとよいだろう。

補題 4.1. $k[X]$ の元 f の次数が 2 または 3 であり、かつ $f(a) = 0$ となるような $a \in k$ が存在しないならば、f は既約である。

この段階で, 有限体の演算の実際について知っておくのも悪くはなかろう。加、減、乗算についてはそんなに難しくはないと思われるので、ここでは 0 以外の元の逆元の計算法について簡単に触れておく。要はユークリッドの互除法であって、代数学 I ですでに目にしているはずである。まずユークリッドの互除法の簡単な復習から。

例題 4.1 (ユークリッドの互除法)**.** 等式

$$72l + 56m = 8$$

を満たす整数 l, m の組を一組求めよ。

(解答) まず次のような計算を行なう

$72 \div 56 = 1$ 余り 16	$72 = 56 \times 1 + 16$	$\begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 56 \\ 16 \end{pmatrix}$
$56 \div 16 = 3$ 余り 8	$56 = 16 \times 3 + 8$	$\begin{pmatrix} 56 \\ 16 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 16 \\ 8 \end{pmatrix}$
$16 \div 8 = 2$ 余り 0	$16 = 8 \times 2 + 0$	$\begin{pmatrix} 16 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$

各々の行の行列算を組み合わせると、

$$\begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$$

逆であることに注意して、上の式を次のように変形することが出来る。

$$\begin{pmatrix}8\\0\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}3&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}1&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}72\\56\end{pmatrix}$$
$$=\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}72\\56\end{pmatrix}=\begin{pmatrix}-3&4\\7&9\end{pmatrix}\begin{pmatrix}72\\56\end{pmatrix}$$

この式の第一行に着目すると、$8=(-3)\times 72+4\times 56$ を得る。
(答え)　$l=-3, m=4.$

例題 4.2. $\mathbb{F}_{31}$ での 11 の逆元を求めよ。
(解答) 上の例題 4.1 の要領で $31l+11m=1$ なる $l, m\in\mathbb{Z}$ を求めることにより、

$$31\times 5+11\times(-14)=1$$

を得る。この式の両辺を $\mathbb{F}_{31}$ のなかで考えると、

$$[11]_{31}[-14]_{31}=[1]_{31}$$

すなわち、11 の $\mathbb{F}_{31}$ での逆元は $-14(=17)$ である。

問題 4.1. $K=\mathbb{F}_3[X]/(X^3-X-1)\mathbb{F}_3[X]$ での X のクラスを ξ と書き、$a, b\in K$ を $a=\xi^2+\xi+1,\ b=\xi^2-1$ で定義する。このとき、$a+b, a-b, ab, b^{-1}$ をそれぞれ ξ の 2 次以下の式であらわしなさい。

問題 4.2. $K=\mathbb{F}_{37}[X]/(X^3-X+2)\mathbb{F}_{37}[X]$ での X のクラスを ξ と書くとき、K での $12\xi^2+5\xi+1$ の逆元を求めなさい。(なお、この K は実は体であるのだが、そこまでは示さなくてもよい。)