代数学 II 要約 NO.7

今日のテーマ:

$\boxed{\text{有限体の乗法群の構造と、有限体の存在 II}}$

前回、いくつかの定理と補題の証明が残ってしまっていた。

定理 7.1 (定理 6.1 と同じ). 素数 p と正の整数 n にたいして、 元の数が $q = p^n$ の体は存在する。もっと詳しくいうと、$X^q - X \in F_p[X]$ が一次式の積に分解するような体 L (前の補題によって存在する) をとり、L のなかの $X^q - X$ の根の全体を K とおくと、K は体で、その元の数は q になる。

この定理のうち、 K が体で、その元の数が q 以下であることは前回証明した。K の元の数がちょうど q 個であることを示すには、多項式の微分の概念を知っておいた方が便利である。

補題 7.1. 体 k 上の多項式 $p(X) = \sum_{k=0}^{n} a_k X^k$ に対して、その微分を

$$p'(X) = \frac{d}{dX} p(X) = \sum_{k=0}^{n} k a_k X^{k-1}$$

で定義する。この時、

(1) 微分は p の係数体をどう選ぶかに関係しない。
(2) 微分は k-線型である。
(3) $(pq)' = p'q + pq'$.

補題 7.2 (補題 6.2 とおなじ). 有限体 K に対して、

$$a_n = \#\{x; x \text{ の位数は } n\}$$

と定義すると、

(1) $a_n \neq 0$ であるのは n が $q-1$ の約数の時に限る。
(2) $a_n \leq \varphi(n) = (1$ から n までの整数で, n と互いに素なものの数$)$

定理 7.2 (定理 6.2 とおなじ). 有限体 K にたいして、位数が $\#(K) - 1$ であるような K の元 x が存在する。言い換えると、K の乗法群 $K^\times$ は巡回群である。

系 7.1. 素数 p と正の整数 n に対して、$\mathbb{F}_p$ 上の既約多項式 $f(X)$ で、その次数が n のものが存在する。

注意: 次の問題は (いつもの例に反して)難易度の順に並んでいない. 解きやすいものをとくこと。また、これらは本質的に違う問題というわけではないので、今回は 一問のみ を選んで解くこと。

問題 7.1. 元の数が 16 の体 K を $\mathbb{F}_2[X]/f(X)\mathbb{F}_2(X)$ の形でつくり、その K に対して $K^\times$ の生成元を一つ求めなさい。

問題 7.2. 元の数が 27 の体 K を $\mathbb{F}_3[X]/f(X)\mathbb{F}_3(X)$ の形でつくり、その K に対して $K^\times$ の生成元を一つ求めなさい。

問題 7.3. 元の数が 25 の体 K を $\mathbb{F}_5[X]/f(X)\mathbb{F}_5(X)$ の形でつくり、その K に対して $K^\times$ の生成元を一つ求めなさい。