代数学 II 要約 NO.9

今日のテーマ:

有限体は元の数で完全に決まること II

前回は復習止まりで、次の定理や命題を残してしまったので、今回はその証明をする。

定理 9.1 (定理 8.1 と同じ). 素数 p と正の整数 n に対して、元の個数が $q = p^n$ であるような有限体 K が存在する *(*定理 *6.2)*。この K にたいして、次のことが成り立つ。

(1) $K^\times$ の *(*群としての*)* 生成元 a の $\mathbb{F}_p$ 上の最小多項式の次数は n である。

(2) $\mathbb{F}_p$ 上の n 次の既約多項式は必ず K で一次式の積に分解される。

命題 9.2 (命題 8.3 と同じ). 体 k の拡大体 K, L があって、K のほうは k 上一つの元 α で生成される k の有限次拡大体であるとする。さらに、α の k 上の最小多項式を m とおく。このとき、もし、L の元 β で、$m(\beta) = 0$ を満たすものがあれば、K から L への中への同型写像 φ で、$\varphi(\alpha) = \beta$ をみたすものが存在する。

定理 9.3 (定理 8.4 と同じ). 体 K_1, K_2 の元の数がともに有限で、同じ q であるなら、K_1 と K_2 とは同型である *(*すなわち、K_1 から K_2 への上への同型写像 φ が存在する。

$K^\times$ の構造を知ると、次のような問題も片付けられる。(とは言ってもこれは Fermat の定理 (あるいは群論の Lagrange の定理) の範疇である。)

問題 2.3 一般に、素数 p に対して、 10 進法で書いた整数を p で割った余りを「一定の桁数毎に区切って」 求める方法はいつでも存在するだろうか？ (但しもちろん $p = 2$ と $p = 5$ の場合は例外とする。)

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。)

(解説) 諸君のレポートを見ると、$\mathbb{F}_{37}[X]/(X^3 - X + 2)\mathbb{F}_{37}[X]$ のようなものの扱いについて理解できている人と、できてない人の差がはっきり分かれてきているのがわかる。

$\mathbb{F}_{37}$ についてはわかっているようだし、$\mathbb{F}_{37}[X]$ も大丈夫だろう。あとは それを $(X^3 - X + 2)\mathbb{F}_{37}[X]$ で割った剰余環の理解が欠けているのだろう。

問題の K で、X のクラスを (X とそのまま表記しても良いし、$\overline{X}$ あるいは $[X]$ のような記号でもよいのだが、ここでは字画を減らすために) ξ と書くと、K とは、$\mathbb{F}_{37}$ に、$\xi^3 - \xi + 2 = 0$ という関係式をもった元 ξ を付け加えてできる環である。$\xi^3 - \xi + 2 = 0$ という関係式から、

$3(\xi^3 - \xi + 2) = 0$, $\xi(\xi^3 - \xi + 2) = 0$, $(\xi^2 + 30\xi + 23)(\xi^3 - \xi + 2) = 0$ 等々の関係式が得られるはずである。また、

$\xi^3 = \xi - 2$, $\xi^4 = \xi^2 - 2\xi$

などの関係式も得られる。このような環をそもそも作れるかどうか、ということも大事なことなのだが、これが多項式の全体 $\mathbb{F}_{37}[X]$ を $X^3 -$

まり、関係式 $\xi^3-\xi+2=0$ をもつような ξ を $\mathbb{F}_{37}$ に付け加えるというだけでは、(全く何の知識もない初歩の段階では) それがうまくできるかどうかがわからないが、$\mathbb{F}_{37}$-係数の多項式の全体 $\mathbb{F}_{37}[X]$ を (X^3-X+2) の倍数を法としてクラス分けする

$$f \sim g \Leftrightarrow f-g \in (X^3-X+2)\mathbb{F}_{37}[X]$$

ということはできるはずであるし、そのクラス分けをしたクラスの全体 $K=\mathbb{F}_{37}[X]/(X^3-X+2)\mathbb{F}_{37}[X]$ が環の構造をもつこと、さらには X の K でのクラスが上述の関係式を満たすことも確かめられるというわけである。

ちょうど、$\mathbb{Z}/9\mathbb{Z}$ では $9=0$ が成り立つことや、$\mathbb{Z}/11\mathbb{Z}$ では $11=0$ が成り立つことと同様である。

問題 9.1. $p=5$ とする。$\mathbb{F}_p$ 上のモニックな 4 次既約多項式 f の例を挙げ、f の一つの根を α とした時、f の他の根を α であらわしなさい。(つまり、f を $\mathbb{F}_p[\alpha]$ 上で一次式の積に分解しなさい。)

上の問題は少し難しすぎたかも知れないので、次の問題を追加しておく。こちらは少し簡単である。

問題 9.2. 上の問題で $p=3$ のときはどうか。

両方の問題とも、f の既約性まで論じることが望ましい。