代数系の基礎要綱 #8

2002–7–11　　河野

今まで小さい有限体について具体的に見てきたが，ここで少し理論的反省をしてみよう。問題は 2 つある。

(1) 有限体は存在するのか?
(2)q を 1 つ与えたとき有限体は同型を除いて一意に決まるのか?

まず存在の問題。有限体 F_q は $q = p^n$ (ただし p は素数，n は自然数) のでなければ存在しない。しかし $q = p^n$ のとき存在するのかという問題である。q が素数の場合は $F_q = \boldsymbol{Z}_q$ なのでこれは確かに存在する。一般の $q = p^n$ を見る前に 4 元体の場合を思い出して見よう。$F_4 - F_2$ から元 α を取り出してきた。そのときこの α は $X^2 + X + 1 = 0$ の解であった。この議論は最初から F_4 が存在する事を前提に進められている。F_4 の存在を前提にしない場合は次の様に議論できるかもしれない：F_2 の既約多項式 $X^2 + X + 1 = 0$ の解を α とすると，$F_2(\alpha)$ が 4 元体になる。この議論は既約多項式の解が必ず存在する事を前提にしているが，この前提を示す事で (1) の証明を与える事ができるかもしれない。

2 つめの問題は $q = p^n$ が与えられたとき有限体が存在するとして，同型 (きちんとした定義は後で与える) でないものが 2 つ以上存在する事はないのかという問題である。今まで F_q という書き方をしてきたが，これは q から体が一意的に決定されるという事を前提にした表示法であった。以下この 2 つの問題の解決を目指そう。

最初に体 K とその上の既約多項式 $f(X)$ が与えられたときに，$f(X) = 0$ の解が「存在」するかという問題を考える。$K = \boldsymbol{Q}$ の場合は $\boldsymbol{C}$ という $\boldsymbol{Q}$ の拡大体が存在して，解はその中に存在した。一般の体 K の場合も $\boldsymbol{C}$ に対応する体が存在する。その証明は課題にする事にして，ここでは次の定理を述べるにとどめる。

定理 6.4 体 K と K 上の既約多項式 $f(X)$ に対し次を満たす体 L と L の元 α が存在する。
(1) $L = K(\alpha)$
(2) $f(\alpha) = 0$

略証　T を不定元として，$L = \left\{ a_0 + a_1T + \cdots + a_{n-1}T^{n-1} \,\middle|\, a_i \in K \right\}$ とする。$g(T) = a_0 + a_1T + \cdots + a_{n-1}T^{n-1} \in L$ に対し $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ なる $K[X]$ の多項式を $g(X)$ とする (形式的に T の場所に X を代入したとも考えられる)。同じく $h(T) = b_0 + b_1T + \cdots + b_{n-1}T^{n-1} \in L$ に対し $b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$ なる $K[X]$ の多項式を $h(X)$ とする。L の和は $g(X) + h(X) = k(X)$ となる多項式 $k(X)$ に対し $g(T) + h(T) = k(T)$ と定義する ($k(T)$ は $k(X)$ の X に T を代入したもの)。積は $g(X)h(X)$ を $f(X)$ で割った余りの多項式を $r(X)$ とするとき $g(T) \cdot h(T) = r(T)$ と定義する。このとき次を示せば証明は終わる。
(1) この演算で L は体になる。
(2) $\alpha = T$ とおくと，$L = K(\alpha)$
(3) $f(\alpha) = 0$
これらの証明は演習問題にまわす。 ∎

演習問題 *6.2　　上の (1)–(3) を示せ。

定義 6.5 体 K とその拡大体 L_1, L_2 に対し L_1 から L_2 への演算を保つ上への 1 対 1 写像 T が K の元を不変にするとき T を L_1 から L_2 への K 上の**同型写像** (*isomorphism*) といい，L_1 と L_2 は K 上同型であるという。条件を箇条的に書くと T は次を満たす写像である。
(1) $T : L_1 \to L_2$ は上への写像
(2) T は 1 対 1 写像
(3) L_1 の任意の元 a, b に対し $T(a+b) = T(a) + T(b)$
(4) L_1 の任意の元 a, b に対し $T(ab) = T(a)T(b)$
(5) K の任意の元 k に対し $T(k) = k$

命題 6.6 定理 6.4 の様な L は K 上の同型を除いて一意的である。即ち，L を定理 6.4 の体とし L_1 を定理 6.4 の条件を満たす別の体とする。このとき L から L_1 への K 上の同型写像 T が存在する。

略証　定理 4.9 より L_1 は $f(X) = 0$ の解である元 β が存在して $L_1 = K(\beta)$ と書ける。L の任意の元 a はある多項式 $g(X) \in K[X]$ を用いて $a = g(\alpha)$ と書ける。このとき $T(a) = g(\beta)$ と定義すると，これが条件を満たす。 ∎

定理 4.9 から有限体の存在を示すためには次の事が証明されればよい：p を素数とする。任意の自然数 n に対し $F_p[X]$ の規約多項式で次数が n のものが存在する。
この事実は直接示すには組合せ的な議論が少々面倒臭い。そこで方向を変えて分解体というものを考える事により示す。

定義 6.7 K を体とし，$f(X)$ を $K[X]$ の元とする。K の拡大体 L が次の 2 つの条件をみたすとき，$f(X)$ の分解体という。
(1) $f(X)$ は $L[X]$ においては 1 次式の積に分解される。即ち $\alpha_1, \ldots, \alpha_n \in L$ が存在して $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$
(2) $L = K(\alpha_1, \ldots, \alpha_n) (= K(\alpha_1) \cdots (\alpha_n))$

分解体の例を見よう。$K = \boldsymbol{Q}$, $f(X) = X^2 - 2$ とおく。$\alpha = \sqrt{2}$ とおくと，$f(\alpha) = 0$ である。$L = \boldsymbol{Q}(\alpha)$ とおくと，$L[X]$ では $f(X)$ は $f(X) = (X - \alpha)(X + \alpha)$ と分解される。L は $f(X)$ の分解体である。勿論 $L = \boldsymbol{Q}(\alpha, -\alpha)$ が成立しているが，ここでは 1 個付け加えただけで分解体が得られている。
$K = \boldsymbol{Q}$, $f(X) = X^3 - 2$ とする。$\alpha = \sqrt[3]{2}$ とおくと，$f(\alpha) = 0$ である。$L_1 = \boldsymbol{Q}(\alpha)$ とおく。L_1 では $f(X)$ は $f(X) = (X - \alpha)(X^2 + \alpha X + \alpha^2)$ と分解されるが，1 次式の積にはなっていない。$\beta = \dfrac{-1 + i\sqrt{3}}{2}$ とおく。$L = L_1(\beta) = \boldsymbol{Q}(\alpha, \beta)$ では $f(X) = (X - \alpha)(X - \alpha\beta)(\alpha\overline{\beta})$ と分解される。ここで $L = \boldsymbol{Q}(\alpha, \alpha\beta, \alpha\overline{\beta})$ が成立している。

定理 6.8 体 K と多項式 $f(X) \in K[X]$ に対し $f(X)$ の分解体は存在する。2 つの分解体は K 上同型である。

演習問題 *******6.3**　　定理 6.8 を証明せよ。

さて有限体に話を戻そう。

定義 6.9 K を体とする。$K[X]$ の元 $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ に対し $(f(X))' = f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$ とおく。

補題 6.10 $a \in K$, $f, g \in K[X]$ とすると次が成立する。
(1) $(af)' = af'$
(2) $(f+g)' = f' + g'$
(3) $(fg)' = f'g + fg'$
(4) $f(X) = (X-a)^n$ のとき $f'(X) = n(X-a)^{n-1}$

証明　(1),(2) は省略。(3) を示すために最初に f に対し g_1, g_2 が (3) を満たしているとき，g_1+g_2 も満たす事を言う：$(f(g_1+g_2))' = (fg_1+fg_2)' = (fg_1)' + (fg_2)' = f'g_1 fg_1' + f'g_2 + fg_2' = f'(g_1+g_2) + f(g_1'+g_2') = f'(g_1+g_2) + f(g_1+g_2)'$ 。よって g が単項式 X^m の場合に示せばよい。f に関しても同様の議論で f も単項式 X^n としてよい。n についての帰納法で示す。$n=0$ のとき，f は定数なので，$f=0$ である。$(fg)' = fg' = 0g + fg' = f'g + fg'$ で成立している。$n=1$ のときは $(fg)' = (XX^m)' = (X^{m+1})' = (m+1)X^m = 1X^m + XmX^{m-1} = f'g + fg'$ で成立している。n のとき成立を仮定する。$n+1$ のときは $(fg)' = (X^{n+1}g)' = (XX^ng)' = X'(X^ng) + X(X^ng)' = X^ng + X(nX^{n-1}g + X^ng') = (n+1)X^ng + X^{n+1}g' = f'g + fg'$ で成立している。

(4) も n に関する帰納法で示す。$n=1$ のときは成立している：$(X-a)' = 1 = 1(X-a)^0$ 。n のとき成立を仮定すると $((X-a)^{n+1})' = ((X-a)(X-a)^n)' = (X-a)'(X-a)^n + (X-a)((X-a)^n)' = (X-a)^n + (X-a)n(X-a)^{n-1} = (n+1)X^n = (n+1)X^{n+1-1}$ で成立している。

補題 6.11 $f(X) \in K[X]$ が重解を持つ事と $f(X)$ と $f'(X)$ が共通解を持つ事は同値である。

証明　高校時代の実数・複素数の場合の証明と同様である。$f(X)$ が重解 a を持つとき因数定理より $f(X) = (X-a)^2 g(x)$ と書ける。このとき $f'(X) = 2(X-a)g(X) + (X-a)^2 g'(X)$ なので $f'(a) = 0$ で共通解 a を持つ。

逆に共通解 a を持つとき，$f(X)$ を $(X-a)^2$ で割ると余りは 1 次式なので $f(X) = (X-a)^2 g(X) + b(X-a) + c$ と書ける。$f(a) = 0$ より $c = 0$ が分かる。このとき $f'(X) = 2(X-a)g(X) + (X-a)^2 g'(X) + b$ なので $f'(a) = 0$ より $b = 0$ が従い，$f(X)$ が重解 a を持つことが分かる。

命題 6.12 任意の素数 p と，任意の自然数 n に対し $q = p^n$ とおく。このとき有限体 F_q は同型を除いて一意的に存在する。

証明　(**存在**)　F_p を考え，$F_p[X]$ の多項式 $f(X) = X^q - X$ の分解体 F を考える。このとき $\#(F) = q$ となる事を示す。体 F の標数は p である。$\underbrace{1 + \cdots + 1}_{k} = k$ と書く事にすると，2 項係数 ${}_pC_k$ は $k = 1, \ldots, p-1$ のとき p で割り切れるので，F においては ${}_pC_k = 0$ である。よって F の任意の元 $a, b \in F$ に対し $(a+b)^p = a^p + b^p$ が成立する。更にその p 乗を考える事により $(a+b)^{p^2} = ((a+b)^p)^p = (a^p + b^p)^p = (a^p)^p + (b^p)^p = a^{p^2} + b^{p^2}$ が成立する。これを繰り返すと任意の p^m に対し $(a+b)^{p^m} = a^{p^m} + b^{p^m}$ が成立する。特に $(a+b)^q = a^q + b^q$ が成立する。F_p^* の元 a については $a^{p-1} = 1$ が成立しているので，F_p の元 a については $a^p = a$ が成立している。$a^{p^2} = (a^p)^p = a^p = a$ より任意の自然数 m について $a^{p^m} = a$ が成立する。特に $a^q = a$ が成立し,$f(a) = 0$ が成立する。a, b を $f(X) = 0$ の解とすると，$(a+b)^q = a^q + b^q = a + b$ なので $a+b$ も $f(X) = 0$ の解である。また $(ab)^q = a^q b^q = ab$ なので ab も $f(X) = 0$ の解である。F の元は F_p の元と $f(X) = 0$ の解の和・積で書かれので，F の任意の元は $f(X) = 0$ の解である。また $f'(X) = qX^{q-1} - 1 = -1$ なので $f(X) = 0$ と $f'(X) = 0$ に共通解はない。$f(X) = 0$ の解の個数は q 個なので $\#(F) = q$ である。

(**一意性**)　$\#(F) = q$ となる有限体 F が存在したとする。これが $f(X) = X^q - X = 0$ の分解体である事が示されれば一意性が従う。任意の元 $a \in F^*$ に対し $a^{q-1} = 1$ となる。よって任意の元

$a \in F$ に対し $a^q = a$ が成立する。つまり F の任意の元は方程式 $f(X) = X^q - X = 0$ の解になっている。F は $f(X) = 0$ の q 個の解をすべて含んでいるので分解体である。