代数学 III 要約 NO.5

今日のテーマ: $\boxed{\text{分解体}}$

体 K 上の一変数既約多項式 $f(X)$ が与えられているとする。K に f の根 α を付け加えてできたような体 $L_1 = K(\alpha)$ をつくることができるのであった。もちろん、f は L_1 上一次の因数 $X - \alpha$ をもつ。しかし、f がこれ以上因数分解できるかどうかは場合による。

定義 5.1. 体 K とその上の (既約とは限らない) 一変数多項式 $f \in K[X]$ が与えられているとする。このとき、K の拡大体 L が f の**分解体**であるとは、f が L 上の多項式として 1 次式の積に分解できるときにいう。

もっと一般に、 体 K 上の有限個の一変数多項式 $f_1, f_2, \ldots, f_s$ が与えられたとき、L がその分解体であるとは、各 f_j が L で一次式の積に分解できるようなときにいう。(これは実際には積 $f_1 f_2 \ldots f_s$ の分解体ということと同じである。)

与えられた一変数多項式 f にたいして、その分解体は一意とは限らない。じっさい、L_1 が f の分解体なら、L_1 の拡大体はどれも f の分解体である。

命題 5.2. K 上の任意の一変数多項式 f は分解体をもつ。すなわち、ある体 L で、f が L 上一次式の積に分解できるようなものが存在する。

上の命題を用いると、L が f の分解体であるとは、L を十分大きい体 Ω に埋め込んだ時に f の Ω における K 上の共役がすべて L に含まれているということと同値であるということがわかる。

定理 5.3. 体 K の拡大体 L_0 と、その拡大体 $L_1 = K(\theta_1, \theta_2, \ldots, \theta_t)$ が与えられているとする。$\theta_1, \theta_2, \ldots, \theta_t$ の K 上の最小多項式を $f_1, f_2, \ldots, f_t$ と置こう。このときもし L が $f_1, f_2, \ldots, f_t$ の分解体ならば次のことが成り立つ。

中への K-同型 $\sigma_0 : L_0 \to L$ が任意に与えられたとき、σ_0 の延長であるような中への同型 $\sigma : L_1 \to L$ が存在する。

上の定理の条件は 「(L の十分大きな拡大体 Ω の中で,) $\theta_1, \theta_2, \ldots, \theta_t$ のすべての K 上の (Ω 内での) 共役が L に属する」ということと同値である。

定義 5.4 (間に合わせ的)**.** 体 K とその上の一変数多項式 f が与えられたとき、f の分解体 Ω が存在するのであった。Ω の中での f の根を $\alpha_1, \alpha_2, \ldots, \alpha_s$ とおくとき、$K(\alpha_1, \alpha_2, \ldots, \alpha_s)$ は明らかに K の拡大体で f の分解体のうち極小なものである。これを f の**極小分解体** (minimal splitting field) と呼ぼう。

上で「間に合わせ的」と書いたのは次のように「最小...」と呼ぶことが普通だからである。(英語なら the が付くか否かの違いに過ぎない。)

命題 5.5. 体 K とその上の一変数多項式 f が与えられたとき、f の極小分解体はすべて互いに K-同型である。したがってそれらをいちいち区別せずに**最小分解体** (the minimal splitting field) と呼ぶ。

今回のまとめ:

一変数多項式はそれがどんなものであれ体を拡大すれば一次式の積に分解できるということ、そのために必要な体はどれも同型であることを学んだ。このことは今後の議論に重要な基礎を与える。

問題 5.1. $f(X) = X^4 + X^3 + X^2 + X + 1 (\in \mathbb{Q}[X])$ とおく。このとき、

(1) f は $X^5 - 1$ の因数であることを示しなさい。
(2) f のひとつの根を α と置くと、$\alpha^2, \alpha^3, \alpha^4$ も f の根であることを示しなさい。
(3) $\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ 上の f の最小分解体であることを示しなさい。

問題 5.2. 前問の f は $\mathbb{Q}[X]$ の元として既約であることを示しなさい。(ヒント: f が既約でなかったとして、 $f = gh$ と因数分解されたとする。g, h はともにモニックとして良い。前問の結果をもちいて、g, h の定数項がまた f の根であることを示せ。その結果 f が $\mathbb{Q}$ 上に解を持つことにするが、これは f の複素数体上の素因数分解の結果に反する。(f は実数の根をもたない)。