代数学 III 要約 NO.7

今日のテーマ: $\boxed{\text{体の同型を数える。}}$

体 K 上の分離代数的な元 $\alpha_1, \alpha_2, \ldots, \alpha_s$ に対して、$L = K(\alpha_1, \ldots, \alpha_s)$ の元 γ が存在して、$L = K(\gamma)$ とできるのであった。この γ は K 上分離的に取れる。

体 K の拡大体 M と Ω とがあるとき、 M から Ω への K-同型の数を数えることにより、M の性質がある程度分かる。本日はそんな話。

定義 7.1. M から Ω への K-同型の全体の集合を

$$\mathrm{Hom}_K^{\mathrm{algebra}}(M, \Omega)$$

と書く。

まず M が K の単純拡大のときから考えてみよう。

補題 7.2. 体 K 上の代数的数 α の最小多項式を $m(X)$ とおく。K の拡大体 Ω にたいして、Ω 内の m の根を、重複を許さずに (つまり重複を取り除いて) ならべたものを $\gamma_1, \ldots, \gamma_s$ とすると、$K(\alpha)$ から Ω への K-同型はちょうど s 個存在する。とくに、$s \leq [K(\alpha) : K]$ で、等号は次の二つの条件がともに成り立つとき、そしてそのときに限りなりたつ。

(1) α は K 上分離的である。
(2) Ω は m の分解体である。

上の補題は、Ω が十分大きいときには $\mathrm{Hom}_K^{\mathrm{algebra}}(M, \Omega)$ の元の数が分離性の判定に使えることを示唆している。上の補題を何度も用いることにより、次のことが証明できる。

命題 7.3. K 上代数的な元 $\alpha_1, \alpha_2, \ldots, \alpha_t$ と K の拡大体 Ω について、$M = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$ と書くと、

$$\mathrm{Hom}_K^{\mathrm{algebra}}(M, \Omega) \leq [M : K].$$

$\alpha_1, \alpha_2, \ldots, \alpha_t$ がすべて K 上分離的で、Ω が それらの最小多項式すべての分解体ならば、等号が成り立つ。

ちょっとトリッキーだが、次のことにも注意しておこう。

補題 7.4. K の拡大体 M のどれかひとつの元 α が K 上非分離的であるならば、

$$\mathrm{Hom}_K^{\mathrm{algebra}}(M, \Omega) < [M : K].$$

証明は $K(\alpha)$ で一旦途中下車することにより得られる。次の系は分離性の判定が生成元だけで済むことを示しており、大切である。

系 7.5. K 上代数的な元 $\alpha_1, \alpha_2, \ldots, \alpha_t$ が K 上分離的ならば $M = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$ の元はすべて分離的である。

「大きな体」Ω に頼ってばかりいると面倒である。これを排除するために (もちろん他の理由もあるが次のようなものを考える。

定義 7.6. K 上の代数拡大体 L が K 上**正規拡大**であるとは、L の任意の元の任意の共役が L に属するときにいう。言い換えると、これは L の各元の K 上の最小多項式が必ず L 上で一次式の積に分解されるということである。

定義 7.7. 体 K の分離的でかつ正規な代数拡大を**ガロア拡大**と呼ぶ。

体 K のガロア拡大 M が与えられたとすると、上で Ω として使っていたものの代わりに M 自身を使えることがわかる。

問題 7.1. $\mathbb{Q}(\sqrt{7})$ は $\mathbb{Q}$ の正規拡大であることを定義に従って確認しなさい。