体論要約 NO.7

今日のテーマ:**正規拡大、分離拡大、ガロア拡大**

定義 7.1. 体 K の拡大体 L の各元が K 上代数的のとき、L のことを K 上の**代数拡大体**という。

以下、代数拡大体の性質を見ることが話題の中心になる。

既存の体 K にたいして、その上の代数的な元 α を付け加えて新しい体 $K(\alpha)$ をつくることができるのであった．それは α の K 上の最小多項式 $m(X)$ を用いて作られる

$$K[X]/m(X)K[X]$$

という剰余環と同型である。特にその同型類は m だけに依存している。

一般に、与えられた多項式 f に対して、f の根を次々に K に加えることにより、f の分解体を作ることができ、なかんづく最小分解体は f によって同型を除いて一意に決まるのであった。

定義 7.2. 体 K 上の代数的な元 α が**分離的**であるとは、α の K 上の最小多項式が重根を持たないときにいう。

分離性は代数学を進んで学びたい者にとっては大事な概念であるが、その重要性や取り扱い方は一旦ガロア理論に習熟してからのほうがよく分かるように思える。したがってこの講義では定義と、「標数 0 のとき」についての注意をしておくに止めよう。(体 K において、1 を何回か足すと 0 になる場合がある。そのような「回数」を K の標数とよぶ。もっとカッコヨク言えば次のようになる。)

定義 7.3. 体 K に対して、一意に定まる環準同型

$$\mathbb{Z} \to K$$

の核は 0 か、$p\mathbb{Z}$ (p はある素数) と等しいかのいずれかである。前者の時、K の標数は 0 であるといい、後者の時、K の標数は p であるという。K の標数を $\mathrm{char}(K)$ と書く。

例えば素数 p を与えたとき、 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は 標数 p である。

命題 7.4. K の標数が 0 ならば、K 上のすべての代数的な元は K 上分離的である。

証明には、つぎのような (形式的) 微分を用いると良い。

定義 7.5. 体 (もしくは、もっと一般に、可換環) K にたいして、K-線形写像

$$\frac{d}{dX} : K[X] \to K[X]$$

を

$$\frac{d}{dX}(\sum_{j=0}^{t} a_j X^j) = (\sum_{j=0}^{t} j a_j X^{j-1})$$

で定義する。

命題 7.6. 体 (もしくは、可換環)K に対して、次のことが成り立つ。

(1) $\frac{d}{dX}$ は K-線形写像である。
(2) $\frac{d}{dX}(X^j) = jX^{j-1} \qquad (j = 0, 1, 2, \dots)$
(3) $\frac{d}{dX}$ は上の二つを満たす $K[X]$ から $K[X]$ への唯一の写像である。
(4) $\frac{d}{dX}(f \cdot g) = \frac{d}{dX}(f) \cdot g + f \cdot \frac{d}{dX}(g) \qquad (\forall f, \forall g \in K[X])$.

定義 7.7. 体 K の代数拡大体 L について、L のどの元も K 上分離的であるとき、L は K 上**分離的**であるという。

上の命題により、$\mathrm{char}\, K = 0$ ならば K の代数拡大体は必ず K 上分離的である

定義 7.8. 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 7.9. 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。

分離性を意識するといろいろな話がラクにすすむ。例えば:

補題 7.10. K は無限個の元を持つ体とする。K 上の代数的な元 α, β が、ともに K 上分離的ならば

$$K(\alpha, \beta) = K(\alpha + c\beta)$$

をみたす $c \in K$ が少なくともひとつ存在する。

α, β の最小多項式をそれぞれ f, g とし、f の根を $\alpha_1, \alpha_2, \ldots, \alpha_s$ g の根を $\beta_1, \beta_2, \ldots, \beta_t$ とおく。必要ならば番号を付け替えて $\beta = \beta_1, \alpha = \alpha_1$ としてよい。c として避けるべきなのは

$$(*) \qquad -\frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \qquad (i \neq 1)$$

である。β の分離性により分母の $\beta_j - \beta_1$ は 0 でないことに注意。([蛇足ながら分離性の仮定はそこだけに必要というわけではない。) そもそもこれら (*) のうちそもそも K に入ることすらない元もあるのだが、ともかく避けるべきものは有限個なので補題の言うような c は存在する。

系 7.11. K は無限個の元を持つ体とする。体 K 上の有限個の分離的な元 $\alpha_1, \alpha_2, \ldots, \alpha_s$ で生成される体

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_s)$$

は実際にはある一つの元 γ をうまく選べば

$$L = K(\gamma)$$

とそれひとつだけで生成される。

問題 7.1.

$$\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

であることを証明せよ。

問題 7.2. $\alpha = \sqrt{3} + \sqrt{5}, \beta = -\sqrt{5} + \sqrt{7}$ とする。

$$\sqrt{5} \in \mathbb{Q}(\alpha, \beta)$$

かつ

$$\sqrt{5} \notin \mathbb{Q}(\alpha + \beta)$$

であることを示しなさい.

問題 7.3. $\mathbb{Q}$ 上の代数的数 α, β で $\mathbb{Q}(\alpha + \beta) \neq \mathbb{Q}(\alpha, \beta)$ が成り立つ (できるだけ簡単な) 例をあげよ。(原理がわかれば前問より易しい。)

問題 7.4. (この問題に完答するにはもう少し先の知識まで必要であるが、参考のために掲げておく。) $\alpha = \sqrt{2} + 2\sqrt{3} + 4\sqrt{5}, \beta = 3\sqrt{2} + 3\sqrt{3} - \sqrt{5} + \sqrt{7}$ とする。このとき、

$$\mathbb{Q}(\alpha, \beta) \neq \mathbb{Q}(\alpha + c\beta)$$

をみたすような $c \in \mathbb{Q}$ を全て求めなさい。