体論要約 NO.5

今日のテーマ: **既約性の判定**

今回は少しガロア理論の本筋からは外れる。これまで、個々の例の多項式の既約性について証明なしに議論してきたが、だんだん不自由になってきたのでここでまとめておくことにする。

代数についてよく学びたい人のための注: 今回の議論は $\mathbb{Z}$ とその商体 $\mathbb{Q}$ に関してのべるが、一般の UFD R とその商体 $K = Q(R)$ に関しても同様なことが成り立つ。

次の命題は多項式の既約性判定の際に整数係数と有理係数の差をうまく処理してくれる:

命題 5.1. $\mathbb{Z}$ 上の多項式 $f(X) \in \mathbb{Z}[X]$ が $\mathbb{Q}$ 上で可約ならば、$\mathbb{Z}$ 上でも可約である。

証明には「ガウスの補題」を用いる。その説明のためにひとつ言葉を用意しておこう。

定義 5.2. $\mathbb{Z}$ 上の多項式 $f(X) \in \mathbb{Z}[X]$ が**原始的**であるとは f の係数のすべてを割るような整数が ± 1 しかないときにいう。言い換えると、原始的多項式とは係数の gcd が 1 の多項式である。

補題 5.3 (ガウス)**.** 原始多項式 $f, g \in \mathbb{Z}[X]$ の積 fg はまた原始的である。

命題 5.4. 多項式 $h \in \mathbb{Z}[X]$ が多項式 $f, g \in \mathbb{Z}[X]$ の積の時、

(1) h の定数項は f の定数項と g の定数項の積である。
(2) h の最高次の係数は f の最高次の係数と g の最高次の係数との積である。

とくに、モニックな $\mathbb{Z}[X]$ の多項式がもし可約ならばそれはモニックな因数を持つ。

命題 5.5. 体 K 上の 3 次もしくは 2 次の多項式 $f \in K[X]$ について、f が K の中に根を持たなければ f は K 上既約である。

定理 5.6 (アイゼンシュタイン)**.** $\mathbb{Z}$ を係数にもつモニックな

$$f(X) = X^k + a_{k-1}X^{k-1} + a_{k-2}X^{k-2} + \cdots + a_0$$

が、ある素数 p に対して、次の二つの性質をもつとする。

(1) $f(X) \equiv X^k \pmod{p}$
(2) $f(X)$ の定数項は p^2 で割り切れない。

このとき、f は $\mathbb{Q}$ 上既約である。

次のこともよく用いる。

定理 5.7. 任意の $f \in k[X]$ と任意の定数 $c \in k$ に対して、
$f(X)$ が既約 $\Leftrightarrow$ $f(X + c)$ が既約.

定理 5.8. モニックな整係数多項式 $f(X) \in \mathbb{Z}[X]$ が与えられているとする。ある素数 p に対して f が $\mathbb{Z}/p\mathbb{Z}$ 係数の多項式として既約なら、f は $\mathbb{Q}[X]$ の元として既約である。

問題 5.1. $X^2 - 6$ は $\mathbb{Q}$ 上既約であることを示しなさい。(今回はもちろん $\sqrt{6}$ が無理数であることを使ってはならない。)

問題 5.2. $X^3 - X - 1$ は $\mathbb{Q}$ 上既約であることを示しなさい。

[根と解] 体 一変数多項式 $f(X)$ を

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_d)$$

と因数分解したとき、$\alpha_1, \dots, \alpha_d$ のことを f **の根**と呼ぶ。

- $\alpha_1, \dots, \alpha_d$ 自身は K の元でなくても、K の適当な拡大体 (分かりやすいのは、$K \subset \mathbb{C}$ のときの $\mathbb{C}$ や、K の代数的閉包 (後述) $\bar{K}$) の元でよい。
- 重複はその分も込めて考える。

$f(c) = 0$ を満たす $c \in K$ を $f(X) = 0$ の (K 上の) 解と呼ぶ。