代数学 IB 要約 NO.15

UFD R を係数とする多項式の因数分解には、R の商体 $Q(R)$ での因数分解を考えれば十分であることがガウスの補題により分かるのでした。

今日のテーマ: 既約性の判定

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。

次の命題はガウスの補題の系である。

命題 15.1. $\mathbb{Z}$ 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。

命題 15.2. 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。

系 15.3. $n \in \mathbb{Z}$ が平方数でなければ、$X^2 - n$ は $\mathbb{Q}[X]$ の既約元である。よって、このとき、$\sqrt{n}$ は無理数である。

命題 15.4. 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 15.5 (アイゼンシュタイン)**.** $\mathbb{Z}$ を係数にもつモニックな多項式

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

が、ある素数 p に対して、次の二つの性質をもつとする。

(1) $f(X) = X^k \pmod{p}$

(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 15.6. 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 15.7. 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 15.1. $X^2 - 6$ 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 15.2. $X^3 - X - 1$ は $\mathbb{Q}$ 上既約であることを示しなさい。