

今日のテーマ 《多項式環は素元分解環である》

**定理 14.1.**  $R$  が素元分解環ならば  $R[X]$  も素元分解環である。

上の定理の系として直ちにわかる次のことは大変基本的で、重要である。

**系 14.2.** 素元分解環  $R$  上の  $n$  変数多項式環  $R[X_1, X_2, \dots, X_n]$  はまた素元分解環である。

**補題 14.1.** 整域  $R$  が与えられているとき、集合

$$S_R = R \times (R \setminus \{0\}) = \{(a, b); a \in R, b \in R, b \neq 0\}$$

に同値関係を

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

で定義する。 $(a, b) \in S_R$  のこの同値関係によるクラスを  $a/b$  と書く。 $Q(R) = S_R / \sim$  に和、積を

$$a/b + c/d = (ad + bc)/bd$$

$$a/b \cdot c/d = (ac)/(bd)$$

で定義すると、これらうまく定義されて、 $Q(R)$  は体になる。

**定義 14.1.** 整域  $R$  にたいして上のように作られる環  $Q(R)$  を  $R$  の商体と呼ぶ。

定理 14.1 の証明には、 $Q(R)[X]$  の素因数分解を利用して  $R[X]$  の素因数分解をすることを考える。そのために次の概念を用いよう。

**定義 14.2.** 素元分解環  $R$  上の一変数多項式  $f$  が原始的であるとは、 $f$  の係数を全て集めたものの最大公約数が 1 であるときにいう。

多項式の係数の「共通因数」をくり出すことにより、次のことが言える。

**補題 14.2.** 任意の  $f \in R[X]$  は

$$f = af_1 \quad (a \in R, f_1 \in R[X] \text{ は原始的})$$

と書くことができる。 $a$  は同伴を除いて一意的である。

**補題 14.3** (ガウス). 素元分解環  $R$  が与えられているとし、 $K = Q(R)$  とおく。このとき

(1)  $R[X]$  の元  $f, g$  と  $R$  の素元  $p$  とにたいして、

$$fg \in pR[X] \Leftrightarrow (f \in pR[X] \text{ or } g \in pR[X])$$

(2)  $R[X]$  の原始的な元の積は必ず原始的である。

(3)  $R[X]$  の原始的な元  $f$  について、次のことは同値である。

- (a)  $f$  は  $R[X]$  の素元である。
- (b)  $f$  は  $R[X]$  の既約元である。
- (c)  $f$  は  $K[X]$  の既約元である。
- (d)  $f$  は  $K[X]$  の素元である。

**証明.** (1)  $R[X]/pR[X] \cong (R/p)[X]$  であり (問題 14.2)、 $(R/p)$  は整域だから、 $(R/p)[X]$  も整域。ゆえに  $pR[X]$  は  $R[X]$  の素イデアルである。

(2) は (1) からすぐに従う。

(3): (a)  $\implies$  (b) は補題 10.3 の (1) から従う。 $K[X]$  はユークリッド整域であるから、一意分解環。ゆえに、(c)  $\Leftrightarrow$  (d) である。

(b)  $\implies$  (c):  $f$  は  $R[X]$  の原始的既約元であるとする。 $f$  がもし  $K[X]$  で既約でなければ、

$$c_1f = c_2g_1h_1$$

$(c_1, c_2 \in R \setminus \{0\}, g_1, h_1 \in R[X])$  は原始的かつ 1 次以上) なる  $c_1, c_2, g_1, h_1$  が存在することが分かる。 $g_1 h_1$  は (2) により原始的であるから。 $c_1$  と  $c_2$  は同伴。そのことから、

$$f = u g_1 h_1 (\exists u \in R^\times)$$

がわかる。これは  $f$  が  $R[X]$  の既約元であることに反する。

(d)  $\implies$  (a):  $f$  は  $R[X]$  の原始的な元で、 $K[X]$  の素元であるとする。 $gh \in fR[X]$  なる  $g, h \in R[X]$  があるとすると、 $K[X]$  のなかで考えることにより

$$g \in fK[X] \text{ or } h \in fK[X]$$

がわかる。どちらでもおなじことであるから  $g \in fK[X]$  としよう。一般性を失うことなく、 $g$  は原始的であると仮定してよい。 $g \in K[X]$  から

$$b_0 g = b_1 f m$$

なる  $b_0, b_1 \in R \setminus \{0\}$  と、原始的な元  $m \in R[X]$  の存在が分かる。再び (2) のより、 $b_0$  と  $b_1$  とは同伴であることを知る。したがって、 $g \in fR[X]$ .  $\square$

**問題 14.1.** 整域  $R$  にたいして、 $Q(R)$  の和がうまく定義されることを実際に証明せよ。

**問題 14.2.** 可換環  $R$  が与えられているとする。このとき、任意の  $p \in R$  にたいして環としての同型

$$R[X]/pR[X] \cong (R/pR)[X]$$

が存在することを示しなさい。