代数学２，第10回の内容の理解度チェックの解答

2025/7/7　担当：那須

R を一意分解整域 (UFD) とする．R 上の 1 変数多項式環 $R[x]$ の元

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

に対し，係数 $a_0, a_1, \ldots, a_n$ の最大公約元を $c(f)$ と表し，f の**内容** *(content)* という．

$\boxed{1}$ 次の多項式 $f(x) \in \mathbb{Z}[x]$ に対し，$f(x)$ の内容 $c(f)$ の値を求めよ．

(1) $f(x) = 4 - 10x$

(2) $f(x) = 6 - 9x + 18x^2$

(3) $f(x) = 1 - 2x + 4x^2 + \cdots + (-2)^n x^n$

(解答)

(1) $c(f) = \gcd(4, -10) = 2.$

(2) $c(f) = \gcd(6, -9, 18) = 3.$

(3) $c(f) = \gcd(1, -2, 4, \ldots, (-2)^n) = 1.$

$\boxed{2}$ $\mathbb{Z}[x]$ の元 $f(x) = 4 + 6x$ と $g(x) = 3 - 9x + 12x^3$ に対し $f(x)g(x)$ を計算せよ．また $c(fg)$ の値を求めよ．

(解答)

$$f(x)g(x) = (4 + 6x)(3 - 9x + 12x^3) = 72x^4 + 48x^3 - 54x^2 - 18x + 12.$$

$$c(fg) = c(f)c(g) = 2 \cdot 3 = 6.$$

$\boxed{3}$ $f(x) \in \mathbb{Z}[x]$ を

$$f(x) = 72x^4 + 48x^3 - 54x^2 - 18x + 12$$

とする．

(1) $f(x)$ を $\mathbb{Z}[x]$ において，素元の積に分解せよ．

(2) $f(x)$ を $\mathbb{Q}[x]$ において，素元の積に分解せよ．

(解答)

(1) $f(x) = 2 \cdot 3 \cdot (x + 1)(2x - 1)^2(3x + 2)$　（ただし素元の順序と単元の積をのぞく）

(2) $f(x) = 72(x + 1)(x - \frac{1}{2})^2(x + \frac{2}{3})$　（ただし素元の順序と単元の積をのぞく）

$\boxed{4}$ R を一意分解整域とする. $p \in R$ を素元とすれば, p は $R[x]$ の素元であることを示せ.

(**解答**) $f(x), g(x) \in R[x]$ に対し, $p \mid f(x)g(x)$ とする. このとき $h(x) \in R[x]$ が存在し, $ph(x) = f(x)g(x)$ を満たす. 両辺の内容を取ると, $pc(h) = c(f)c(g) \in R$ となる. つまり $p \mid c(fg) = c(f)c(g)$ となるため, p が素元であることから $p \mid c(f)$ または $p \mid c(g)$ が従う. したがって $p \mid f(x)$ または $p \mid g(x)$ を得る.

$\boxed{5}$ R を一意分解整域とし, k を R の商体とする. $R[x]$ の素元は, k の単元かまたは $k[x]$ の素元であることを示せ. (ただし, もし必要であれば, 以下のガウスの定理を用いてもよい.)

ガウスの定理

整域 R に対し, R が一意分解整域であるための必要十分条件は, R 上の 1 変数多項式環 $R[x]$ が一意分解整域となることである.

(**解答**) $f(x) \in R[x]$ を $R[x]$ の素元とする. ガウスの定理より, $R[x]$ は一意分解整域であり, 一意分解整域において素元と既約元は一致するため, $f(x)$ は $R[x]$ の既約元である.

f の内容を $c(f) = c \in R$ とすれば,

$$f(x) = cf_0(x)$$

を満たす原始的な元 $f_0 \in R[x]$ が存在する.

$f(x)$ は $R[x]$ の既約元であるため, $c \sim 1$ または $f_0(x) \sim 1$ が成り立つ.

前者が成り立つとき, $f(x) \sim f_0(x)$ を意味し, $f(x)$ は $R[x]$ の既約元であるため $f_0(x)$ も $R[x]$ の既約元である. f_0 は原始的なので, $k[x]$ における素元である.

後者が成り立てば, $R[x]$ において $f(x) \sim c$ となり, $k[x]$ において $f(x) \sim 1$ となるため, R の商体 k では単元となる.

[3]※この講義に関する情報はホームページを参照. https://hirokazunasu.github.io/2025/alg2.html