

- 1 アイゼンシュタインの既約性判定を用いて以下の多項式  $f(x) \in \mathbb{Z}[x]$  が  $\mathbb{Q}[x]$  において既約元であることを示せ.

(1)  $f(x) = x^5 - 5x + 10$

(2)  $f(x) = x^4 + 6x^3 + 9x^2 + 3x + 3$

(解答)

- (1) 素数  $p = 5$  を考えると, 最高次係数  $1$  は  $p$  で割り切れず, 定数項  $10$  は  $p$  で割り切れ  $p^2$  で割り切れず, すべての中間項の係数 ( $0$  または  $-5$ ) は  $p$  で割り切れるため, アイゼンシュタインの判定法により  $\mathbb{Q}[x]$  で既約である.
- (2) 素数  $p = 3$  を考えると, 最高次係数  $1$  は  $p$  で割り切れず, 定数項  $3$  は  $p$  で割り切れ  $p^2$  で割り切れず, すべての中間項の係数  $6, 9, 3$  は  $p$  で割り切れるため, アイゼンシュタインの判定法により  $\mathbb{Q}[x]$  で既約である.

- 2 次の多項式  $f(x) \in \mathbb{Z}[x]$  が  $\mathbb{Q}[x]$  において既約元かどうか判定せよ (ヒント:  $f(x+2)$  を計算せよ).

$$f(x) = x^3 - 6x^2 + 12x - 1$$

(解答) ヒントに従い  $f(x+2)$  を求めると,

$$\begin{aligned} f(x+2) &= (x+2)^3 - 6(x+2)^2 + 12(x+2) - 1 \\ &= x^3 + 7 \end{aligned}$$

$f(x+2)$  が既約なことから,  $f(x)$  が既約なことは同値であるため,  $f(x+2)$  にアイゼンシュタインの判定法を適用する.

素数  $p = 7$  を考えると, 最高次係数  $1$  は  $p$  で割り切れず, 定数項  $7$  は  $p$  で割り切れ  $p^2$  で割り切れず, すべての中間項の係数  $0$  は  $p$  で割り切れるため, アイゼンシュタインの判定法により  $f(x+2)$  は, したがって  $f(x)$  は  $\mathbb{Q}[x]$  で既約である.

3  $p$  を素数とする.  $f(x) \in \mathbb{Z}[x]$  が  $\mathbb{Q}[x]$  において既約元であることを示せ.

(1)  $f(x) = x^p - p$

(2)  $f(x) = x^p + p^2x + p$

(解答)

- (1) 最高次係数は1で  $p$  で割り切れず, 定数項  $-p$  は  $p$  で割り切れ  $p^2$  で割り切れず, すべての中間項の係数0は  $p$  で割り切れるため, アイゼンシュタインの判定法により  $\mathbb{Q}[x]$  で既約である.
- (2) 最高次係数は1で  $p$  で割り切れず, 定数項  $p$  は  $p$  で割り切れ  $p^2$  で割り切れず, すべての中間項の係数(0または  $p^2$ )は  $p$  で割り切れるため, アイゼンシュタインの判定法により  $\mathbb{Q}[x]$  で既約である.

4 有理整数環  $\mathbb{Z}$  上の  $n$  変数多項式環  $\mathbb{Z}[x_1, \dots, x_n]$  が一意分解整域であることを示せ. ただし以下のガウスの定理を用いても良い.

—— 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)  $\mathbb{Z}$  は単項イデアル整域 (PID) である. 単項イデアル整域は一意分解整域 (UFD) であるため,  $\mathbb{Z}$  は UFD である. ガウスの定理より,  $\mathbb{Z}[x_1]$  は UFD となる.

$$\mathbb{Z}[x_1, \dots, x_n] \simeq (\mathbb{Z}[x_1, \dots, x_{n-1}])[x_n]$$

より, ガウスの定理を帰納的に用いれば,

$$\mathbb{Z}[x_1]: \text{UFD} \implies \mathbb{Z}[x_1, x_2]: \text{UFD} \implies \dots \implies \mathbb{Z}[x_1, \dots, x_n]: \text{UFD}$$

が従う.