

18. 演習 (6)

問18-1. \mathbb{Z} 上の monic な多項式 $f(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ ($a_n = 1$) に対し、 f が有理数の根 $x \in \mathbb{Q}$ を持つならば、 $x \in \mathbb{Z}$ かつ $x|a_0$ である。(ヒント: $x = n/d, d, n \in \mathbb{Z}, (d, n) = 1$ と既約分数で書いて、 d の素因子 p について考察せよ。)

問18-2. 上問を用いて、次の多項式が \mathbb{Z} 上 (従って \mathbb{Q} 上) 既約であることを示せ。

(1) $f(X) = X^3 + 2X - 1$

(2) $f(X) = X^3 + X - 6$

問18-3. 素数 p に対し、自然な射影 $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ から定まる環準同型 $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ による $f(X) \in \mathbb{Z}[X]$ の像を $\bar{f}(X) \in \mathbb{F}_p[X]$ と書くことにする。 $f(X) \in \mathbb{Z}[X]$ に対し、或る素数 p について $\bar{f}(X) \in \mathbb{F}_p[X]$ が既約なら、 f は \mathbb{Z} 上 (従って \mathbb{Q} 上) 既約。

問18-4. 次の多項式 $f(X) \in \mathbb{Z}[X]$ の既約性を、幾つかの素数 p に対する $\text{mod } p$ で分解 ($\bar{f}(X) \in \mathbb{F}_p[X]$ の分解) を考えることにより、判定せよ。

(1) $f(X) = X^3 + 3X + 9$

(2) $f(X) = X^3 + 2X + 8$

(3) $f(X) = X^4 + 5X^2 + 2X + 15$

問18-5. $f(X) := X^4 - 10X^2 + 1 : \mathbb{Z}$ 上既約。(ヒント: まづ 1 次因子を持たないこと、次に 2 次式 2 つの積にならないことを確かめよ。)

問18-6. 第 8 円分多項式 $\Phi_8(X) \in \mathbb{Z}[X]$ について、

(1) $\Phi_8(X)$ を求め、その \mathbb{Z} 上での既約性を直接判定せよ。

(2) $\Phi_8(X)$ が $\text{mod } p$ で 1 次式の積に分解するような素数 p の条件を決定せよ。(ヒント: \mathbb{F}_p^\times 内に 1 の原始 8 乗根が存在する条件は?)

(3) 任意の素数 p に対し、 $\Phi_8(X)$ は $\text{mod } p$ で可約 (若干の初等整数論の知識が要る)。

問18-7. 素数 p に対し、

(1) 第 p 円分多項式 $\Phi_p(X) \in \mathbb{Z}[X]$ を求めよ。

(2) $g(Y) := \Phi_p(Y+1) \in \mathbb{Z}[X]$ とおくと、 g は \mathbb{Z} 上 (従って \mathbb{Q} 上) 既約。(ヒント: Eisenstein の既約性判定法が使える。)

(3) $\Phi_p : \mathbb{Z}$ 上 (従って \mathbb{Q} 上) 既約。

(4) $\prod_{\zeta \in \mu_p^*} (1 - \zeta) = p$ を示せ。

(5) 判別式 $D(\Phi_p) = ?$

問18-8. $\zeta_n := e^{\frac{2\pi i}{n}} \in \mathbb{C}$ とおく。 $\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)$ を ζ_n で表せ。

問18-9. 上問で $n = 5$ として、

(1) $\omega_5 := 2 \cos\left(\frac{2\pi}{5}\right)$ の \mathbb{Q} 上の最小多項式を求めよ。その判別式は?

(2) ζ_5 を根号を用いて表せ。

(3) 正五角形を定規とコンパスとを用いて作図せよ。

問18-10. $\omega_7 := 2 \cos\left(\frac{2\pi}{7}\right)$ の \mathbb{Q} 上の最小多項式を求めよ。その判別式は?

問18-11. 正整数 $n \geq 1$ と、相異なる n 個の整数 $a_1, \dots, a_n \in \mathbb{Z}$ に対し、

$f(X) := \prod_{i=1}^n (X - a_i) + 1 \in \mathbb{Z}[X]$ を考える。

(1) n : 奇数 $= 2k + 1$ のとき、 $f : \mathbb{Z}$ 上既約。

(2) n : 偶数 ≥ 4 のとき、 f は \mathbb{Z} 上可約たり得るか。