

演習問題 (12/16 配布)

問1.  $K$  を体とし、その代数閉包  $\bar{K}$  を1つ取って固定する。 $f(X) \in K[X]$  を  $K$  上の既約多項式とし、その一つの根を  $\alpha \in \bar{K}$  とする。

- (1) (準備) 体上有限次元な整域は体である。
- (2)  $K$  上の環準同型  $\varphi: K[X] \rightarrow \bar{K}; X \mapsto \alpha$  について、 $\text{Im}\varphi = K(\alpha)$  である。
- (3)  $\text{Ker}\varphi = (f)$  である。これより、 $K[X]/(f) \simeq K(\alpha)$  となる。
- (4)  $\iota: K(\alpha) \hookrightarrow \bar{K}$  を  $K$  上の埋込とする。 $\iota(\alpha)$  も  $f$  の根である。
- (5) 逆に  $f$  の根  $\beta \in \bar{K}$  に対し、 $\iota(\alpha) = \beta$  となる  $K$  上の埋込  $\iota: K(\alpha) \hookrightarrow \bar{K}$  が一意に存在する。
- (6) 以上により、 $K(\alpha)$  の  $\bar{K}$  への  $K$  の埋込全体と、 $f$  の根全体とは、一対一に対応する。

問2.  $f(X) \in K[X]$  を  $K$  上の  $n$  次 monic 多項式とし、その根を (重複度を込めて)  $w_1, \dots, w_n$  とする。根の差積の平方

$$D(f) := \prod_{1 \leq i < j \leq n} (w_i - w_j)^2$$

を  $f$  の判別式 (discriminant) という。

- (1)  $f(X) = X^3 + pX + q$  の3根を  $x_1, x_2, x_3$  とする。 $x_1, x_2, x_3$  の基本対称式と  $p, q$  との関係を用いて、判別式  $D(f) = \prod_{1 \leq i < j \leq 3} (x_i - x_j)^2 = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$  を  $p, q$  で表せ。
- (2)  $f$  の微分  $f'$  の根を  $v_1, \dots, v_{n-1}$  (重根は重複度込みで考える) とするとき、

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(w_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n-1} f(v_j).$$

- (3)  $f(X) = X^n - aX - b$  について判別式  $D(f)$  を求めよ。(ヒント:  $f, f'$  について互除法を用いて計算せよ。)

問3.  $f(X) = X^4 + pX^2 + qX + r$  の4根を  $x_i$  ( $i = 1, \dots, 4$ ) とする。

- (1)  $x_i$  の基本対称式と  $p, q, r$  との関係は?
- (2)  $x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3$  を3根とする3次多項式を求めよ (係数を  $p, q, r$  で表せ)。
- (3)  $(x_1 + x_2)(x_3 + x_4), (x_1 + x_3)(x_2 + x_4), (x_1 + x_4)(x_2 + x_3)$  を3根とする3次多項式を求めよ (係数を  $p, q, r$  で表せ)。

問4.  $K$  を標数  $p > 0$  の体とすると、 $a, b \in K$  に対し、 $(a+b)^p = a^p + b^p, (ab)^p = a^p b^p$  となることを示せ。(ヒント: 二項展開して、素数  $p$  と  $1 \leq k \leq p-1$  とに対し  $p \mid \binom{p}{k}$  となることを用いる。) 即ち、 $\varphi: K \rightarrow K; a \mapsto a^p$ : (中への) 体同型。特に、 $K$  が有限体ならば、 $\varphi$  は  $K$  の体自己同型。

問5. 素数  $p$  と自然数  $r$  との組  $(p, r)$  で  $q := p^r \leq 10$  なるもの  $(p, r) = (2, 2), (2, 3), (3, 2)$  (即ち  $q = 4, 8, 9$ ) に対し、

- (1) 素体  $F_p = \mathbb{Z}/p\mathbb{Z}$  上  $r$  次の既約多項式  $f(X) \in F_p[X]$  を、とにかく見付けよ。
- (2)  $f(X)$  が  $F_p$  上既約であることを、とにかく示せ。
- (3)  $K := F_p[X]/(f)$  により  $q$  元体  $K$  を構成し、その乗積表を書け。
- (4) Frobenius 同型  $\varphi: K \rightarrow K; a \mapsto a^p$  の関数表 ( $a$  と  $\varphi(a)$  との対応表) を作れ。
- (5)  $\varphi^n = \text{id}_K$  となる最小の正整数  $n$  は何か。

問6. 体  $K$  の乗法群  $K^\times$  の有限部分群  $G$  は巡回群。(ヒント: 有限アーベル群の構造定理と、体では  $x^n = 1$  となる  $x$  が高々  $n$  個であることを用いよ。) 特に、 $K = F_q$ : 有限体に対し、 $F_q^\times$  は巡回群。

問7. 前問により、素数  $p$  に対し、 $(\mathbb{Z}/p\mathbb{Z})^\times$  は巡回群である。その生成元を、法  $p$  に関する原始根 (primitive root) という。幾つかの素数  $p$  に対し、原始根をとにかく求めよ。

問 8. (Fermat の小定理)  $p$  を素数とすると、 $a \in \mathbb{Z}$  に対し  $a^p \equiv a \pmod{p}$  となる。これを二通りで証明しよう。

- (1) (乗法的)  $a \not\equiv 0 \pmod{p}$  ならば  $a^{p-1} \equiv 1 \pmod{p}$  であることを示すことにより証明せよ。
- (2) (加法的) 二項係数の性質から  $(a+b)^p \equiv a^p + b^p \pmod{p}$  を導き、 $a$  に関する帰納法を用いて証明せよ。(Fermat による原証明はこちらだったと言われている。)

問 9.  $\mathbb{Z}$  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、

- (1) (Gauss の補題)  $f$  が  $\mathbb{Q}$  上可約ならば、 $\mathbb{Z}$  上でも可約である。従って (対偶を取ると)、 $f$  が  $\mathbb{Z}$  上既約ならば、 $\mathbb{Q}$  上でも既約である。
- (2) 特に、 $f$  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。

問 10. 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)  $f(X) = X^3 + X - 6$
- (3)  $f(X) = X^4 - 10X^2 + 1$  (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 11. 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 12. 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  $\text{mod } p$  での分解 ( $\bar{f}(X) \in \mathbb{F}_p[x]$  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 13. 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 14.  $K$  を体、 $n$  を 1 以上の自然数とする。

- (1)  $K$  の代数閉包  $\bar{K}$  内に 1 の原始  $n$  乗根が存在するための必要十分条件は、「 $\text{ch } K = 0$  または ( $p := \text{ch } K > 0$  かつ  $p \nmid n$ )」である。
- (2) 上の条件を満たすとき、 $\bar{K}$  内の 1 の原始  $n$  乗根の一つを  $\zeta_n$  とする (一つ取って固定)。 $K(\zeta_n)$  は  $K$  上 Galois 拡大。
- (3)  $G := \text{Gal}(K(\zeta_n)/K)$  とする。 $\sigma \in G$  に対し、 $\sigma(\zeta_n) = \zeta_n^a$  となる  $a$  を取ることににより、 $G \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$  が定まる。これは  $\zeta_n$  の選び方に依らない。

問 15.  $p$  を奇素数、 $\zeta_p$  を 1 の原始  $p$  乗根の一つとし、 $K := \mathbb{Q}(\zeta_p)$  とおく。

- (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。(従って、 $\Phi_p(X) = \text{Irr}(\zeta_p/\mathbb{Q})(X)$  である。)
- (4)  $\prod_{\zeta \in \mu_p^*} (1 - \zeta) = p$  を示せ。また、判別式  $D(\Phi_p) = ?$
- (5) 前問の対応により  $G := \text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$  となる。 $\bar{a} = a \text{ mod } p \in (\mathbb{Z}/p\mathbb{Z})^\times$  に対し、 $\sigma_a \in G$  を  $\sigma_a(\zeta_p) = \zeta_p^{\bar{a}}$  で定める。
- (6)  $(p-1)$  次巡回群  $(\mathbb{Z}/p\mathbb{Z})^\times$  の生成元 (法  $p$  に関する原始根) を一つ取って  $\bar{g} = g \text{ mod } p$  とする;  $(\mathbb{Z}/p\mathbb{Z})^\times = \langle \bar{g} \rangle$ 。  $(\mathbb{Z}/p\mathbb{Z})^\times$  の指数 2 の部分群  $H$  を  $\bar{g}$  で表せ。
- (7)  $\xi_i := \sum_{j=0}^{(p-1)/2-1} \zeta_p^{g^{2j+i}}$  ( $i = 0, 1$ ) とする。 $\xi_i \in K^H$  を示し、 $\sigma_g(\xi_0), \sigma_g(\xi_1)$  を求めよ。

(8)  $\xi_0 + \xi_1, \xi_0 \xi_1 \in K^G = \mathbb{Q}$  を示し、その値を求めよ。

(9)  $\xi_0 - \xi_1 = \sum_{i=0}^{p-2} (-1)^i \zeta_p^{g^i}$  は Gauss 和 (次問参照) である。 $(\xi_0 - \xi_1)^2 = ?$

(10)  $\mathbb{Q}$  の 2 次拡大  $K^H$  を求めよ。

(11)  $p-1$  の各約数  $d$  に対し、 $K/\mathbb{Q}$  の  $d$  次中間体が唯一つ存在する。その典型的な生成元を見付けよ。

問 16.  $p$  を奇素数、 $\left(\frac{\cdot}{p}\right)$  を平方剰余記号 (Lagrange 記号)、 $\zeta_p$  を 1 の原始  $p$  乗根 (一

つ取って固定) とする。 $G(p) := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$  を Gauss 和 (Gaussian sum) と言う。

(1)  $(k, p) = 1$  のとき、 $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (\zeta_p^k)^a = \left(\frac{k}{p}\right) G(p)$

(2)  $G(p)^2 = \left(\frac{-1}{p}\right) p (=: p^*)$

(3)  $l$ : 奇素数に対し、平方剰余の相互律  $\left(\frac{l}{p}\right) = \left(\frac{p^*}{l}\right)$  を示せ。

(4)  $\zeta_p = \exp\left(\frac{2\pi i}{p}\right) \in \mathbb{C}$  に取るとき、 $G(p)$  の符号 (偏角) を決定せよ。

問 17.  $m, n$  を互いに素な自然数とする。

(1) (中国剰余定理) 自然に  $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  (環同型)、および  $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$  (群同型)。

(2)  $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$  である。

(3) 上記 2 つを円分体の Galois 対応の下で結び付けよ。

(4)  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$  である。

問 18. (例えば  $n = 5, 7, 8, 9, 12, 15$  など) 幾つかの  $n$  に対し、 $(\mathbb{Z}/n\mathbb{Z})^\times$  の群構造を決定し、部分群を列挙すると共に、対応する  $\mathbb{Q}(\zeta_n)$  の部分体とその適切な生成元の最小多項式を求めよ。

問 19. 次の値を求めよ。

(1)  $\cos 20^\circ \cos 40^\circ \cos 80^\circ$

(2)  $\cos \frac{2\pi}{7} \cos \frac{4\pi}{7} \cos \frac{8\pi}{7}$

(特に、“綺麗な” 値になる理由を Galois 理論から説明せよ。)

問 20. 次の  $\mathbb{Q}$  上の多項式  $f \in \mathbb{Q}[X]$  について、 $\mathbb{Q}$  上の最小分解体  $K := \text{Spl}(f/\mathbb{Q})$  を求めよ。(簡単な生成元 (複数次可) を添加する形で表示せよ。) その  $\mathbb{Q}$  上の拡大次数  $[K:\mathbb{Q}]$  は? また、 $K/\mathbb{Q}$  上の Galois 群  $G = \text{Gal}(K/\mathbb{Q})$  の群構造を決定した上で、 $K/\mathbb{Q}$  の全ての部分体を、 $G$  の部分群との Galois 対応を明らかにして求めよ。

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

(2)  $f(X) = X^5 - 2$

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

(4)  $f(X) = X^4 - 10X^2 + 1$

(5)  $f(X) = X^4 - 20X^2 + 32$

(6)  $f(X) = X^4 - 10X^2 + 5$

問 21.  $K = \mathbb{C}(t)$  を  $\mathbb{C}$  上の一変数有理関数体 ( $t$  は  $\mathbb{C}$  上超越的な元) とする。

(1)  $K$  の  $\mathbb{C}$  上の自己同型  $\sigma$  を  $\sigma(t) := \zeta_n t$  で定めると、 $\sigma$  は位数  $n$  で、 $G := \langle \sigma \rangle$  は位数  $n$  の巡回群。このとき  $K$  の  $G$  による固定体  $K^G$  は?

(2)  $K$  の  $\mathbb{C}$  上の自己同型  $\tau$  を  $\sigma(t) := \frac{1}{t}$  で定めると、 $\tau$  は位数 2 で、 $H := \langle \tau \rangle$  は位数 2 の巡回群。このとき  $K$  の  $H$  による固定体  $K^H$  は?