**補足と演習問題 (12/22 配布)**

**問 1.** $K$ を体とし、その代数閉包 $\overline{K}$ 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 $\alpha \in \overline{K}$ 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 $\varphi : K[X] \to \overline{K}; X \mapsto \alpha$ について、$\mathrm{Im}\varphi = K(\alpha)$ である。
(3) $\mathrm{Ker}\varphi = (f)$ である。これより、$K[X]/(f) \simeq K(\alpha)$ となる。
(4) $\iota : K(\alpha) \hookrightarrow \overline{K}$ を $K$ 上の埋込とする。$\iota(\alpha)$ も $f$ の根である。
(5) 逆に $f$ の根 $\beta \in \overline{K}$ に対し、$\iota(\alpha) = \beta$ となる $K$ 上の埋込 $\iota : K(\alpha) \hookrightarrow \overline{K}$ が一意に存在する。
(6) 以上により、$K(\alpha)$ の $\overline{K}$ 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) $w_1, \ldots, w_n$ とする。根の差積の平方

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

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 $D(f) = \prod_{1 \le i < j \le 3} (x_i - x_j)^2 = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ を $p, q$ で表せ。
(2) $f$ の微分 $f'$ の根を $v_1, \ldots, v_{n-1}$ (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 $x_i$ $(i = 1, \ldots, 4)$ 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 $p > 0$ の体とするとき、$a, b \in K$ 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 $1 \le k \le p-1$ とに対し $p \mid \binom{p}{k}$ となることを用いる。) 即ち、$\varphi : K \to K; a \mapsto a^p$ : (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 $q := p^r \le 10$ なるもの $(p, r) = (2, 2), (2, 3), (3, 2)$ (即ち $q = 4, 8, 9$) に対し、

(1) 素体 $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ 上 $r$ 次の既約多項式 $f(X) \in \boldsymbol{F}_p[X]$ を、とにかく見付けよ。
(2) $f(X)$ が $\boldsymbol{F}_p$ 上既約であることを、とにかく示せ。
(3) $K := \boldsymbol{F}_p[X]/(f)$ により $q$ 元体 $K$ を構成し、その乗積表を書け。
(4) Frobenius 同型 $\varphi : K \to K; a \mapsto a^p$ の関数表 ($a$ と $\varphi(a)$ との対応表) を作れ。
(5) $\varphi^n = \mathrm{id}_K$ 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、$K = \boldsymbol{F}_q$ : 有限体に対し、$\boldsymbol{F}_q^\times$ は巡回群。

**問 7.** 前問により、素数 $p$ に対し、$(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ 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) $p$ を素数とするとき、$a \in \boldsymbol{Z}$ 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) $a \not\equiv p$ 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.** 次の体拡大 $L/K$ が Galois 拡大でないことを簡潔に説明せよ。また、$L$ を含む拡大体 $\widetilde{L}$ で、$\widetilde{L}/K$ が Galois 拡大となるようなものが存在するか。存在するならその最小なもの ($L/K$ の Galois 閉包という) は何か。

(1) $L = \boldsymbol{Q}(\sqrt[3]{2}), K = \boldsymbol{Q}$
(2) $L = \boldsymbol{F}_p(T), K = \boldsymbol{F}_p(T^p)$ (ここに、$T$ は $\boldsymbol{F}_p$ 上超越的)

**問 10.** $\boldsymbol{Z}$ 上の monic な多項式 $f(X) = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$ $(a_n = 1)$ に対し、

(1) (Gauss の補題) $f$ が $\boldsymbol{Q}$ 上可約ならば、$\boldsymbol{Z}$ 上でも可約である。従って (対偶を取ると)、$f$ が $\boldsymbol{Z}$ 上既約ならば、$\boldsymbol{Q}$ 上でも既約である。
(2) 特に、$f$ が有理数の根 $x \in \boldsymbol{Q}$ を持つならば、$x \in \boldsymbol{Z}$ かつ $x | a_0$ である。

**問 11.** 上問を用いて、次の多項式が $\boldsymbol{Z}$ 上 (従って $\boldsymbol{Q}$ 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 12.** 素数 $p$ に対し、自然な射影 $\boldsymbol{Z} \to \boldsymbol{Z}/p\boldsymbol{Z} = \boldsymbol{F}_p$ から定まる環準同型 $\boldsymbol{Z}[X] \to \boldsymbol{F}_p[X]$ による $f(X) \in \boldsymbol{Z}[X]$ の像を $\overline{f}(X) \in \boldsymbol{F}_p[x]$ と書くことにする。$f(X) \in \boldsymbol{Z}[X]$ に対し、或る素数 $p$ について $\overline{f}(X) \in \boldsymbol{F}_p[x]$ が既約なら、$f$ は $\boldsymbol{Z}$ 上 (従って $\boldsymbol{Q}$ 上) 既約。

**問 13.** 次の多項式 $f(X) \in \boldsymbol{Z}[X]$ の既約性を、幾つかの素数 $p$ に対する $\bmod p$ での分解 ($\overline{f}(X) \in \boldsymbol{F}_p[x]$ 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 14.** 第 8 円分多項式 $\Phi_8(X) \in \boldsymbol{Z}[X]$ について、

(1) $\Phi_8(X)$ を求め、その $\boldsymbol{Z}$ 上での既約性を直接判定せよ。
(2) $\Phi_8(X)$ が $\bmod p$ 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: $\boldsymbol{F}_p^\times$ 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 $\bmod p$ で可約 (若干の初等整数論の知識が要る)。

**問 15.** $K$ を体、$n$ を 1 以上の自然数とする。

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

**問 16.** $p$ を奇素数、$\zeta_p$ を 1 の原始 $p$ 乗根の一つとし、$K := \boldsymbol{Q}(\zeta_p)$ とおく。

(1) 第 $p$ 円分多項式 $\Phi_p(X) \in \boldsymbol{Z}[X]$ を求めよ。
(2) $g(Y) := \Phi_p(Y+1) \in \boldsymbol{Z}[X]$ とおくと、$g$ は $\boldsymbol{Z}$ 上 (従って $\boldsymbol{Q}$ 上) 既約。(ヒント: Eisenstein の既約性判定法が使える。)
(3) $\Phi_p$ : $\boldsymbol{Z}$ 上 (従って $\boldsymbol{Q}$ 上) 既約。(従って、$\Phi_p(X) = \mathrm{Irr}(\zeta_p/\boldsymbol{Q})(X)$ 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 $\mathrm{Gal}(K/\boldsymbol{Q}) \simeq (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ で、$\mathrm{Gal}(K/\boldsymbol{Q})$ は $(p-1)$ 次巡回群。

**問 17.** 前問の状況で、$G := \mathrm{Gal}(K/\boldsymbol{Q})$ とおき、$\overline{a} = a \bmod p \in (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ に対し、$\sigma_a \in G$ を $\sigma_a(\zeta_p) = \zeta_p^a$ で定める。

(1) $(p-1)$ 次巡回群 $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ の生成元 (法 $p$ に関する原始根) を一つ取って $\overline{g} = g \bmod p$ とする; $(\boldsymbol{Z}/p\boldsymbol{Z})^\times = \langle\overline{g}\rangle$。$(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ の指数 2 の部分群 $H$ を $\overline{g}$ で表せ。

(2) $\xi_i := \displaystyle\sum_{j=0}^{(p-1)/2-1} \zeta_p^{g^{2j+i}}$ $(i = 0, 1)$ とする。$\xi_i \in K^H$ を示し、$\sigma_g(\xi_0), \sigma_g(\xi_1)$ を求めよ。

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

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

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

**問 18.** $p$ を奇素数、$\left(\dfrac{\cdot}{p}\right)$ 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。$G(p) := \displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a$ を **Gauss 和 (Gaussian sum)** と言う。

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

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

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

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

**問 19.** $p$ を奇素数、$\zeta_p$ を 1 の原始 $p$ 乗根の一つとし、$K := \boldsymbol{Q}(\zeta_p)$ とおく。$p-1$ の各約数 $d$ に対し、$K/\boldsymbol{Q}$ 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 20.** $m, n$ を互いに素な自然数とする。

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

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

**問 21.** (例えば $n = 5, 7, 8, 9, 12, 15$ など) 色々な $n$ に対し、$(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ の群構造を決定し、部分群を列挙すると共に、対応する $\boldsymbol{Q}(\zeta_n)$ の部分体とその適切な生成元の最小多項式を求めよ。

**問 22.** 次の値を求めよ。(特に、"綺麗な" 値になる理由を Galois 理論から説明せよ。)

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

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

**問 23.** 次の $\boldsymbol{Q}$ 上の多項式 $f \in \boldsymbol{Q}[X]$ について、$\boldsymbol{Q}$ 上の最小分解体 $K := \mathrm{Spl}(f/\boldsymbol{Q})$ を求めよ。(簡単な生成元 (複数可) を添加する形で表示せよ。) その $\boldsymbol{Q}$ 上の拡大次数 $[K : \boldsymbol{Q}]$ は ? また、$K/\boldsymbol{Q}$ 上の Galois 群 $G = \mathrm{Gal}(K/\boldsymbol{Q})$ の群構造を決定した上で、$K/\boldsymbol{Q}$ 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 24.** $f(X) \in \boldsymbol{Q}[X]$ を $\boldsymbol{Q}$ 上の既約 monic 多項式、$\alpha$ をその根の一つとして、根体 $K := \boldsymbol{Q}(\alpha)$ を考える。$K$ の元は或る $g(X) \in \boldsymbol{Q}[X]$ を用いて $g(\alpha)$ の形で表せるが、$g(\alpha) \neq 0$ のとき、この逆元 $g(\alpha)^{-1} \in K$ を計算して具体的に表す方法を述べよ。(即ち、$g(\alpha)^{-1} = h(\alpha)$ となる $h(X) \in \boldsymbol{Q}[X]$ を計算する具体的な方法を与えよ。)

**問 25.** $n$ 次対称群 $\mathfrak{S}_n$ について、$\alpha = (1\ 2\ \cdots\ n), \beta = (1\ 2) \in \mathfrak{S}_n$ とするとき、$\mathfrak{S}_n = \langle \alpha, \beta \rangle$ となることを示せ。また、$n$ 次交代群 $\mathfrak{A}_n$ について、これと似たような生成系で表すことを考えよ。

**問 26.** $p$ を素数とする。$H$ を $p$ 次対称群 $\mathfrak{S}_p$ の可移部分群とする。

(1) $H$ は $p$ 次巡換を含むことを示せ。

(2) $H$ が互換を 1 つでも含めば、$H = \mathfrak{S}_p$ であることを示せ。

**問 27.** 上問を踏まえて、

(1) $f(X) = X^5 - 20X + 5 \in \boldsymbol{Q}[X]$ について、$\mathrm{Gal}(f/\boldsymbol{Q}) \simeq \mathfrak{S}_5$ であることを示せ。

(2) $\mathrm{Gal}(f/\boldsymbol{Q}) \simeq \mathfrak{S}_7$ となる 7 次式 $f(X) \in \boldsymbol{Q}[X]$ の例を作れ。

**問 28.** $K = \boldsymbol{C}(t)$ を $C$ 上の一変数有理関数体 ($t$ は $\boldsymbol{C}$ 上超越的な元) とする。

(1) $K$ の $\boldsymbol{C}$ 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 $\boldsymbol{C}$ 上の自己同型 $\tau$ を $\sigma(t) := t^{-1}$ 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？

**問 29.** $K = \boldsymbol{C}(x, y)$ を $C$ 上の 2 変数有理関数体 ($x, y$ は $\boldsymbol{C}$ 上代数的独立な元) とする。

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

(2) $K$ の $\boldsymbol{C}$ 上の自己同型 $\tau$ を $\sigma(x) := x^{-1}, \sigma(y) := y^{-1}$ 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？