2017 年度 代数学 III 期末試験問題

1 月 22 日（月）13:00-16:00 (180 分)　斎藤 毅

・問題用紙　1 枚，解答用紙　3 枚，計算用紙 1 枚.
・筆記用具，計時機能のみの時計　以外もちこめません.
・なるべく，答案用紙の第 n ページに問題 n を解答してください.

問題 1 $\mathbf{Q}$ を有理数体とし，実数体 $\mathbf{R}$ の部分体 $K \subset L$ を $K = \mathbf{Q}(\sqrt{3}, \sqrt{5}) \subset L = \mathbf{Q}(\sqrt{\sqrt{3}+\sqrt{5}}) \subset \mathbf{R}$ で定める．M を L の $\mathbf{Q}$ 上のガロワ閉包とする.

1. K は $\mathbf{Q}$ のガロワ拡大であることを示せ.
2. 拡大次数 $[K : \mathbf{Q}]$ を求めよ.
3. K の部分体をすべて求め，$K = \mathbf{Q}(\sqrt{3}+\sqrt{5})$ を示せ。
4. $\sqrt{3}+\sqrt{5} \in K$ の $\mathbf{Q}$ 上のトレース，ノルムと最小多項式を求めよ.
5. 拡大次数 $[L : \mathbf{Q}]$ を求めよ.
6. $\sqrt{\sqrt{3}+\sqrt{5}}$ の $\mathbf{Q}$ 上の最小多項式を求めよ.
7. 拡大次数 $[M : \mathbf{Q}]$ を求めよ.

問題 2 $L = \mathbf{C}(T)$ を複素数体上の 1 変数有理関数体とし，$V, S \in L$ を

$$V = T^2, \quad S = V^2 - 4V + 2 = T^4 - 4T^2 + 2$$

で定める．L の部分体 $K \subset L_1$ を $K = \mathbf{C}(S),\ L_1 = \mathbf{C}(V)$ で定める.

$P \in K[X]$ を T の K 上の最小多項式とし，$Q \in L[X]$ を P をわりきる既約多項式で，1 次式ではないものとする．M を L の K 上の Galois 閉包とし，$G = \mathrm{Gal}(M/K)$ を Galois 群とする．$Y \in M$ を $Q(Y) = 0$ をみたす元とする．$W = \dfrac{1}{2}(T - iY)$ とおき，$R \in K[X]$ を W の K 上の最小多項式とする.

1. 拡大次数 $[L : K]$ を求めよ.
2. 最小多項式 $P \in K[X]$ を求めよ．P を $L[X]$ で既約多項式の積に分解せよ.
3. 拡大次数 $[M : L]$ を求めよ.
4. $\dfrac{1}{W}$ を T と Y の式として表し，$M = \mathbf{C}(W)$ であることを示せ.
5. 最小多項式 $R \in K[X]$ を求めよ．R を $M[X]$ で 1 次式の積に分解せよ.
6. 中間体 $K \subset L_2 \subset M$ で M が L_2 の巡回 4 次拡大となるものは，ただ 1 つであることを示し，$L_2 = \mathbf{C}(U)$ をみたす多項式 $U \in \mathbf{C}[W]$ を 1 つ求めよ.
7. Galois 群 $G = \mathrm{Gal}(M/K)$ は $\mathrm{Gal}(M/L)$ と $\mathrm{Gal}(M/L_2)$ の半直積であることを示し，K, L, L_1, L_2, M 以外の中間体をすべて求めよ.

問題 3 p を素数とし，$\mathbf{F}_p$ で有限体 $\mathbf{Z}/p\mathbf{Z}$ を表わす．$X^5 - 1$ の $\mathbf{F}_p$ 上の最小分解体を K で表わす.　（注意：小問 2, 3 の答は p によって変わります.）

1. $X^5 - 1 \in \mathbf{F}_p[X]$ が分離多項式であるための，p についての条件を求めよ.
2. 拡大次数 $[K : \mathbf{F}_p]$ を求めよ.
3. $X^5 - 1 \in \mathbf{F}_p[X]$ を既約多項式の積に分解し，それぞれの既約多項式を $K[X]$ で 1 次式の積に分解せよ.

1 1. K は $\mathbf{Q}$ 上の分離多項式 $(X^2-3)(X^2-5)$ の最小分解体だから，ガロワ拡大.

2. $G \subset \mathrm{Gal}(\mathbf{Q}(\sqrt{3})/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\sqrt{5})/\mathbf{Q}) = \mathbf{F}_2^2$ だから，G は $\mathbf{F}_2$ 線形空間. $\sigma, \tau \in G, \bar{a}, \bar{b} \in A$ に対し，$\sigma\tau(\sqrt{a}) = \sigma(\tau(\sqrt{a})/\sqrt{a} \cdot \sqrt{a}) = \sigma(\sqrt{a})/\sqrt{a} \cdot \tau(\sqrt{a})/\sqrt{a} \cdot \sqrt{a}$, $\sigma(\sqrt{ab})/\sqrt{ab} = \sigma(\sqrt{a})\sqrt{a} \cdot \sigma(\sqrt{b})\sqrt{b}$ だから，$(\ ,\ )$ は双線形. $\sigma(\sqrt{3}) = \sqrt{3}, \sigma(\sqrt{5}) = \sqrt{5}$ なら，$\sigma = 1$. 任意の $\sigma \in G$ に対し $\sigma(\sqrt{a}) = \sqrt{a}$ なら $\sqrt{a} \in \mathbf{Q}$ で，$a \in \mathbf{Q}^{\times 2}$. よって，$(\ ,\ )$ は非退化.

したがって，$[K\colon \mathbf{Q}] = \sharp G = 4$.

3. $K, \mathbf{Q}, \mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{5}), \mathbf{Q}(\sqrt{15})$

$\sqrt{3}+\sqrt{5}$ は $\mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{5}), \mathbf{Q}(\sqrt{15})$ のどれにも含まれないから $\mathbf{Q}(\sqrt{3}+\sqrt{5}) = K$.

4. トレース：$(\sqrt{3}+\sqrt{5}) + (-\sqrt{3}+\sqrt{5}) + (\sqrt{3}-\sqrt{5}) + (-\sqrt{3}-\sqrt{5}) = 0$.

ノルム：$(\sqrt{3}+\sqrt{5})(-\sqrt{3}+\sqrt{5})(\sqrt{3}-\sqrt{5})(-\sqrt{3}-\sqrt{5}) = 4$.

最小多項式：$(X-\sqrt{3}-\sqrt{5})+(X-\sqrt{3}+\sqrt{5})+(X+\sqrt{3}-\sqrt{5})+(X+\sqrt{3}+\sqrt{5})$
$= ((X-\sqrt{3})^2-5)((X+\sqrt{3})^2-5) = (X^2-2)^2-12X^2 = X^4-16X^2+4$.

別解 $(\sqrt{3}+\sqrt{5})^2 = 8+2\sqrt{15}$ だから，$(X^2-8)-60 = X^4-16X^2+4$.

5. $a, b, c, d \in \mathbf{Q}$ とすると $(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15})^2 = a^2+3b^2+5c^2+15d^2+\cdots$ は $\sqrt{3}+\sqrt{5}$ と等しくならないから，$[L:K] = 2$. よって $[L:\mathbf{Q}] = 8$.

6. X^8-16X^4+4.

$(X-\sqrt{\sqrt{3}+\sqrt{5}})(X+\sqrt{\sqrt{3}+\sqrt{5}})(X^2+(\sqrt{3}+\sqrt{5}))(X^2-(\sqrt{3}-\sqrt{5}))(X^2+(\sqrt{3}-\sqrt{5}))$

7. $(\sqrt{5}-\sqrt{3})(\sqrt{5}+\sqrt{3}) = 2$ だから，$M = L(\sqrt{2}, \sqrt{-1}) = \mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5})(\sqrt{\sqrt{3}+\sqrt{5}})$. 2 と同様に $[\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbf{Q}] = 16$.

$\mathbf{Q}(\sqrt{\sqrt{3}+\sqrt{5}})$ は $\mathbf{Q}$ のガロワ拡大でないから，$\mathbf{Q}$ の 2 次拡大の合成体の部分体にはならない．よって $[M:\mathbf{Q}] = 32$.

2 1. $\sigma \in \mathrm{Aut}_{L_1} L$ を $\sigma(T) = -T$ で定め，$\tau \in \mathrm{Aut}_K L_1$ を $\tau(V) = 4-V$ で定める．$2 = \sharp\langle\sigma\rangle \leqq [L:L_1] \leqq 2$, $2 = \sharp\langle\tau\rangle \leqq [L_1:K] \leqq 2$ だから，L は L_1 の，L_1 は K の Galois 拡大であり，$[L:K] = [L:L_1] \cdot [L_1:K] = 2 \cdot 2 = 4$.

2. $T^4-4T+2 = S$ だから，P は X^4-4X^2+2-S をわりきる．P は 4 次式だから $P = X^4-4X^2+2-S$. $P(T) = 0$ だから，$P = P-P(T) = X^4-4X^2-(T^4-4T^2) = (X^2-T^2)(X^2+T^2-4) = (X-T)(X+T)(X^2+T^2-4)$. 2 次式 $Q = X^2+T^2-4 = 0$ は $L = \mathbf{C}(T)$ 内に解をもたないから，既約.

3. M は P の最小分解体だから，$M = L[X]/Q$ で，$[M:L] = \deg Q = 2$.

4. $Y^2+T^2-4 = 0$ だから，$\dfrac{1}{2}(T-iY) \cdot \dfrac{1}{2}(T+iY) = 1$. $W = \dfrac{1}{2}(T-iY)$ より $\dfrac{1}{W} = \dfrac{1}{2}(T+iY)$ であり，$T = W + \dfrac{1}{W}$, $Y = i(W - \dfrac{1}{W})$ である.

$M = \mathbf{C}(T,Y) = \mathbf{C}(W)$. $[M : \mathbf{C}] = \infty$ だから，W は $\mathbf{C}$ 上超越的で，$M = \mathbf{C}(W)$ は 1 変数有理関数体.

5. T^4-4T^2+2 に $T = W + \dfrac{1}{W}$ を代入すれば，$W^4+4W^2+6+4W^{-2}+W^{-4}-4(W^2+2+W^{-2})+2 = W^4+W^{-4}$ だから，$W^4+W^{-4} = S$. よって，R は X^8-SX^4+1 をわりきる．R は 8 次式だから，$R = X^8-SX^4+1$.

$R = (X^4-W^4)(X^4-W^{-4}) = (X-W)(X+W)(X-iW)(X+iW)(X-\dfrac{1}{W})(X+\dfrac{1}{W})(X-\dfrac{i}{W})(X+\dfrac{i}{W})$.

6. $S = W^4 + \dfrac{1}{W^4}$ だから $L_2 = \mathbf{C}(W^4)$ は中間体．$\sigma,\ \tau \in G$ を $\sigma(W) = iW$,

$\tau(W) = 1/W$ で定めると，$G = \langle \sigma, \tau \rangle$. G の位数 4 の元は $\sigma^{\pm 1}$ だけだから，位数 4 の巡回部分群は $\langle \sigma \rangle$ だけ．対応する中間体は $L_2 = \mathbf{C}(W^4)$.

7. $\tau\sigma\tau^{-1}(W) = -iW$ だから $\tau\sigma\tau^{-1} = \sigma^{-1}$. よって，$G = \langle \tau \rangle \ltimes \langle \sigma \rangle$.

K, $L = \mathbf{C}(T) = \mathbf{C}(W + \dfrac{1}{W})$, $L_1 = \mathbf{C}(V) = \mathbf{C}(W^2 + \dfrac{1}{W^2})$, $L_2 = \mathbf{C}(W^4)$, $M = \mathbf{C}(W)$ に対応する G の部分群はそれぞれ $G, \langle \tau \rangle, \langle \sigma^2, \tau \rangle, \langle \sigma \rangle, 1$. これ以外の部分群は $\langle \tau\sigma \rangle, \langle \tau\sigma^2 \rangle, \langle \tau\sigma^3 \rangle, \langle \sigma^2 \rangle, \langle \tau\sigma, \sigma^2 \rangle$. 対応する中間体は，$\mathbf{C}(W + i/W), \mathbf{C}(W - 1/W), \mathbf{C}(W - i/W), \mathbf{C}(W^2), \mathbf{C}(W^2 - 1/W^2)$.

3 1. $(X^5 - 1)' = 5X^4$ は $p \neq 5$ なら $X^5 - 1$ とたがいに素，$p = 5$ なら $X^5 - 1$ でわりきれるから，求める条件は $p \neq 5$.

2. $p = 5$ なら $K = \mathbf{F}_p$ で $[K : \mathbf{F}_p] = 1$.

$p \neq 5$ とする．$\mathrm{Gal}(K/\mathbf{F}_p) = \langle F \rangle = \langle p \rangle \subset (\mathbf{Z}/5\mathbf{Z})^\times$ だから，$p \equiv 1 \bmod 5$ のとき $[K : \mathbf{F}_p] = 1$, $p \equiv 4 \bmod 5$ のとき $[K : \mathbf{F}_p] = 2$, $p \equiv 2, 3 \bmod 5$ のとき $[K : \mathbf{F}_p] = 4$.

3. $p = 5$ のとき，$X^5 - 1 = (X - 1)^5$. $p \equiv 1 \bmod 5$ のとき $X^5 - 1 = (X - 1)(X - \zeta_5)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4)$, $p \equiv 4 \bmod 5$ のとき $X^5 - 1 = (X - 1)P_1P_2$, $P_1 = (X - \zeta_5)(X - \zeta_5^4), P_2 = (X - \zeta_5^2)(X - \zeta_5^3)$, $p \equiv 2, 3 \bmod 5$ のとき $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X^1 + 1)$, $X^4 + X^3 + X^2 + X^1 + 1 = (X - \zeta_5)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4)$.