【問題】 $M_2(\mathbb{Q})$ を成分が有理数の 2 次正方行列全体からなる集合とする．$A \in M_2(\mathbb{Q})$ に対し

$$L_A = \{aE + bA \mid a, b \in \mathbb{Q}\}$$

と置く (ただし E は単位行列とする)．このとき次の問いに答えよ．

(1) L_A は行列の和と積に関して可換環になる事を示せ．

(2) A が有理数でない固有値を持つとき，L_A は体になる事を示せ．

(3) $A = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix}$ のとき，体 L_A は体 $\mathbb{Q}(\sqrt{5})$ に同型である事を示せ．

(H21 首都大学東京理工学研究科 数学専攻)

【解答】 (1) Cayley-Hamilton の定理より $A^2 = (\mathrm{tr}\ A)A - (\det A)E$ だから，$aE + bA,\ a'E + b'A \in L_A$ に対し

$$\begin{aligned}
&(aE + bA) \pm (a'E + b'A) = (a \pm a')E + (b \pm b')A \in L_A, \\
&(aE + bA)(a'E + b'A) = (aa' - bb'(\det A))E + (ab' + ba' + bb'(\mathrm{tr}\ A))A \in L_A, \\
&(a'E + b'A)(aE + bA) = (aa' - bb'(\det A))E + (ab' + ba' + bb'(\mathrm{tr}\ A))A = (aE + bA)(a'E + b'A)
\end{aligned}$$

が成立．これらと $I = 1 \cdot I + 0 \cdot A \in L_A$ より L_A は可換環となる．

(2) $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ とする．$aE + bA$ $((a, b) \neq (0, 0))$ について，$b = 0$ ならば $|aE| \neq 0$．$b \neq 0$ のとき $|aE + bA| = b^2|(-a/b)E - A|$ より $|aE + bA| = 0$ だとすると $-a/b$ は A の固有値となるが，これは A の固有値が有理数ではないという仮定に反する．従ってこの場合も $|aE + bA| \neq 0$ となり，$(a, b) \neq (0, 0)$ となる a, b に対し $aE + bA$ は逆元を持つ．よってこの場合，L_A は体となる．

(3) $\varphi : L_A \to \mathbb{Q}(\sqrt{5})$ を $\varphi(aI + bA) = a + b\sqrt{5}$ により定義する．このとき $\varphi(E) = 1$ 及び

$$\begin{aligned}
\varphi((aE + bA) + (a'E + b'A)) &= \varphi((a + a')E + (b + b')A) = a + a' + (b + b')\sqrt{5} \\
&= a + b\sqrt{5} + a' + b'\sqrt{5} = \varphi(aE + bA) + \varphi(a'E + b'A)
\end{aligned}$$

$$\begin{aligned}
\varphi((aE + bA)(a'E + b'A)) &= \varphi((aa' + 5bb')E + (ab' + a'b)A) = (aa' + 5bb') + (ab' + a'b)\sqrt{5} \\
&= (a + b\sqrt{5})(a' + b'\sqrt{5}) = \varphi(aE + bA)\varphi(a'E + b'A)
\end{aligned}$$

より φ は環準同型射であり，

- $\varphi(aE + bA) = a + b\sqrt{5} = 0$ ならば $a = b = 0$，従って $aE + bA = O$.
- $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ に対し $\varphi(aE + bA) = a + b\sqrt{5}$.

より この φ は同型射となる． □

【問題】 $\mathbb{Z}$ 上の 1 変数多項式環 $\mathbb{Z}[X]$ の元 $f(X)$ に対し，写像

$$\Phi_{f(X)} : \mathbb{Z}[X] \to \mathbb{Z}[X]\ ; \quad h(X) \mapsto h(f(X))$$

を考える．但し $h(f(X))$ は $h(X)$ の変数 X に $f(X)$ を代入する事により得られる $\mathbb{Z}[X]$ の元とする．また本問では環準同型写像は常に単位元を単位元に写すものとする．このとき次の問いに答えよ．

(1) 任意の環準同型写像 $\Phi : \mathbb{Z}[X] \to \mathbb{Z}[X]$ に対し，$\Phi = \Phi_{f(X)}$ を満たす $f(X) \in \mathbb{Z}[X]$ が存在する事を示せ．
(2) $\mathbb{Z}[X]$ の元 $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ $(a_0, \cdots, a_n \in \mathbb{Z})$ に対し，$\Phi_{f(X)}$ が全射になるための必要十分条件は $n = 1$ かつ $a_1 \in \{1, -1\}$ であることを示せ．
(3) 集合 $\mathrm{Aut}\ \mathbb{Z}[X] = \{\Phi : \mathbb{Z}[X] \to \mathbb{Z}[X] \mid \Phi$ は全射環準同型写像 $\}$ は写像の合成に関して群をなす事を示せ．
(4) $\mathrm{Aut}\ \mathbb{Z}[X]$ は可換群ではない事を示せ．

(H21 首都大学東京理工学研究科 数学専攻)

【解答】 (1) $f(X) = \Phi(X)$ とする．Φ は環準同型だから，任意の $h(X)$ に対し $\Phi(h(X)) = h(\Phi(X)) = h(f(X)) = \Phi_{f(X)}(h(X))$，従って $\Phi = \Phi_{f(X)}$ となる．
(2) $n = 1$ かつ $a_1 \in \{\pm 1\}$ だとする．このとき任意の $h(X) = \sum_{i=0}^{m} b_i X^i$ $(b_m \neq 0)$ に対し

$$h(X) = \sum_{i=0}^{m} b_i a_1^i (a_1 X)^i = \sum_{i=0}^{m} b_i a_1^i (a_1 X + a_0 - a_0)^i = \Phi_{f(X)} \left(\sum_{i=0}^{m} b_i a_1^i (X - a_0)^i \right)$$

より $\Phi_{f(X)}$ は全射である．逆に $\Phi_{f(X)}$ は全射だとする．このとき $\Phi_{f(X)}(h(X)) = X$ となる $h(X)$ が存在．$h(X) = \sum_{i=0}^{m} b_i X^i$ $(b_m \neq 0)$ だとすると $\Phi_{f(X)}(h(X))$ の最高次は mn だから，$\Phi_{f(X)}(h(X)) = X$ となる為には $mn = 1$，従って $n = m = 1$ でなければならない．更に

$$\Phi_{f(X)}(h(X)) = b_1(a_1 X + a_0) + b_0 = a_1 b_1 X + a_0 b_1 + b_0 = X$$

の 1 次の係数を比較すれば $a_1 b_1 = 1$．$\mathbb{Z}$ の単元は ± 1 のみだから $a_1 \in \{\pm 1\}$ でなければならない．
(3) $f_i(X) = a_{i1} X + a_{i0}$ $(i = 0, 1,\ a_{i1} \in \{\pm 1\})$ に対し

$$\Phi_{f_2(X)}(\Phi_{f_1(X)}(h(X))) = h(f_1(f_2(X))) = \Phi_{f_1(f_2(X))}(h(X)),$$
$$f_1(f_2(X)) = a_{11}a_{21}X + a_{11}a_{20} + a_{10}, \quad a_{11}a_{21} \in \{\pm 1\}$$

より $\Phi_{f_2(X)} \cdot \Phi_{f_1(X)} \in \mathrm{Aut}\,\mathbb{Z}[X]$ である．写像の合成に関する結合律より $\mathrm{Aut}\,\mathbb{Z}[X]$ は合成に関し結合律を満たす事は明らか．$f(X) = X$ とすれば $\Phi_{f(X)} = id$ ($\mathbb{Z}[X]$ 上の恒等写像) より id は $\mathrm{Aut}\,\mathbb{Z}[X]$ の元であり，特に単位元である事は明らか．$f(X) = a_1 X + a_0$ に対し $g(X) = a_1(X - a_0)$ とすると

$$f(g(X)) = a_1(a_1(X - a_0)) + a_0 = X, \qquad g(f(X)) = a_1((a_1 X + a_0)) - a_0) = X$$

より $\Phi_{g(X)} \cdot \Phi_{f(X)} = \Phi_{f(X)} \cdot \Phi_{g(X)} = id$．従って $\Phi_{g(X)}$ は $\Phi_{f(X)}$ の逆元になる．以上より $\mathrm{Aut}\,\mathbb{Z}[X]$ は群である事が確められた．
(4) $f_1(X) = X - 1$, $f_2(X) = -X + 1$ に対し

$$\Phi_{f_1(X)} \cdot \Phi_{f_2(X)}(X) = \Phi_{f_1(X)}(-X + 1) = -(X - 1) + 1 = -X + 2,$$
$$\Phi_{f_2(X)} \cdot \Phi_{f_1(X)}(X) = \Phi_{f_2(X)}(X - 1) = -X$$

より $\Phi_{f_2(X)} \cdot \Phi_{f_1(X)} \neq \Phi_{f_1(X)} \cdot \Phi_{f_2(X)}$．この例より $\mathrm{Aut}\,\mathbb{Z}[X]$ は非可換である事が分かる． □

【問題】 $R=\mathbb{Z}+\mathbb{Z}\sqrt{5}$ とする.

(1) $I=(5)$ は素イデアルではない事を示せ.
(2) $J=(\sqrt{5})$ は極大イデアルである事を示せ.
(3) ±1 以外の R の単元の一つを求めよ. それを α とするとき, $\alpha+J$ の群 $(R/J)^\times$ での位数を求めよ.

(H21 首都大学東京理工学研究科 数学専攻)

【解答】 (1) $\sqrt{5}\notin I$ かつ $\sqrt{5}\sqrt{5}\in I$ より I は素イデアルではない.

(2) $J=5\mathbb{Z}+\mathbb{Z}\sqrt{5}$ より $a+b\sqrt{5}\in R-J$ をとるとき, $a=5a'+r$ $(a',r\in\mathbb{Z},\,0<r<5)$ と表せば $a+b\sqrt{5}+J=r+J$ が成立.

$$r=1,\ 2,\ 3,\ 4 \quad\Rightarrow\quad r^4=1,\ 16,\ 81,\ 256 \quad\Rightarrow\quad r^4-1\in 5\mathbb{Z}$$

に注意すれば $(a+b\sqrt{5}+J)^4=1+J$. 従って R/J は体, 即ち J は極大イデアルである.

(3) $a+b\sqrt{5},\ x+y\sqrt{5}\in R$ とする.

$$(a+b\sqrt{5})(x+y\sqrt{5})=1 \quad\Rightarrow\quad ax+5by=1 \text{ かつ } ay=-bx.$$

$ax+5by=1$ より $a\neq0$ であり, $\mathbb{Q}$ に於いて後者より $y=-(b/a)x$. これを前者に代入して整理すれば $x=a/(a^2-5b^2)$ だから, $a^2-5b^2=\pm1$ ならば $a+b\sqrt{5}$ は R の単元となる. これに注意すれば ±1 以外の単元として例えば $\alpha=2+\sqrt{5}$ をとる事ができる.

次にこの α について

$$\alpha+J=2+J,\qquad \alpha^2+J=4+J,\quad \alpha^3+J=3+J,\quad \alpha^4+J=1+J$$

より $\alpha+J$ の $(R/J)^\times$ に於ける位数は 4 となる. □

【問題】 R を $0 \neq 1$ となる可換環，K を体，L を K の拡大体とする．以下，任意の環準同型射は全て単位的だとする．

(1) R が真のイデアルを持たなければ R は体である事を示せ．
(2) 環準同型射 $f : K \to R$ は単射である事を示せ．
(3) 拡大次数 $[L : K]$ の定義を述べよ．
(4) $[L : K] < \infty$ ならば $f\big|_K = 1_K$ となる環準同型射 $f : L \to L$ は全射である事を示せ．

(H21 首都大学東京理工学研究科 数学専攻)

【解答】 (1) $x \neq 0$ となる $x \in R$ をとる．仮定より $Rx = R$ であるから $rx = 1$ となる $r \in R$ が存在し，故に x は単元となる．従って R は体である．

(2) K は真のイデアルしか持たないので，K のイデアル $\operatorname{Ker} f$ は $\{\boldsymbol{o}\}$ か K．$f(1) = 1$ より $f \neq 0$ だから $\operatorname{Ker} f = \{\boldsymbol{o}\}$，従って f は単射である．

(3) L を K 上の線型空間と考えたときの L の K 上の次元を体の拡大 L/K の拡大次数といい，これを $[L : K]$ $(= \dim_K L)$ と記す．

(4) f は L 上の K 線型変換と考える事が出来る．L は体だから (2) より f は単射．また有限次元線型空間間の線型写像に関する次元公式より

$$\operatorname{rank} f = \operatorname{rank} f + 0 = \operatorname{rank} f + \dim \operatorname{Ker} f = \dim_K L,$$

従って $\operatorname{Im} f = L$ となり，従って f は全射である．□

【問題】 代数的閉体 K 上の多項式環 $K[X]$ の商体を $K(X)$ とし，任意の $a \in K$ に対し

$$K[X]_{(a)} = \left\{ \frac{f(X)}{g(X)} : f(X), g(X) \in K[X],\ g(a) \neq 0 \right\},$$
$$P_a = \left\{ \frac{f(X)}{g(X)} : f(X), g(X) \in K[X],\ f(a) = 0,\ g(a) \neq 0 \right\}$$

と置くとき，以下の問いに答えよ．

(1) P_a は $K[X]_{(a)}$ の素イデアルである事を証明せよ．
(2) $K[X]_{(a)}/P_a$ は環として K と同型である事を証明せよ．
(3) $K(X)$ に於いて $\bigcap_{a \in K} K[X]_{(a)} = K[X]$ である事を証明せよ．

(H21 首都大学東京理工学研究科 数学専攻)

【解答】 $f(X),\ g(X),\ f_i(X),\ g_i(X) \in K[X]\ (i = 1, 2),\ h(X),\ h_i(X) = f_i(X)/g_i(X) \in K(X)$ とする．

(1) $h(X) = f(X)/g(X) \in K[X]_{(a)},\ h_i(X) = f_i(X)/g_i(X) \in P_a\ \ (f(X),\ g(X),\ f_i(X),\ g_i(X) \in K[X]\ (i = 1, 2))$ だとする．

$$h_1(X) + h_2(X) = (g_2(X)f_1(X) + g_1(X)f_2(X))/g_1(X)g_2(X), \quad g_2(a)f_1(a) + g_1(a)f_2(a) = 0$$
$$h_1(X)h_2(X) = f_1(X)f_2(X)/g_1(X)g_2(X), \qquad\qquad f_1(a)f_2(a) = 0$$

より P_a は $K[X]_{(a)}$ のイデアルである．次に $h_1(X)h_2(X) \in P_a$ だとすると $f_1(a)f_2(a) = 0$，従って $f_1(a) = 0$ または $f_2(a) = 0$ となり，これより $h_1(X) \in P_a$ または $h_2(X) \in P_a$ となる．故に P_a は素イデアルである．

(2) $\phi_a : K[X]_{(a)} \to K,\ \phi_a(h(X)) = h(a)$ とすると ϕ_a は単位的環準同型射であり，任意の $\alpha \in K$ に対し $\alpha/1 \in K[X]_{(a)}$ かつ $\phi_a(\alpha/1) = \alpha$ だから ϕ_a は全射．定義より $P_a = \mathrm{Ker}\,\phi_a$ となるから，準同型定理より $K[X]_{(a)}/P_a \simeq K$ となる．

(3) $K[X] \subset \bigcap_{a \in K} K[X]_{(a)}$ は自明．$h(X) = f(X)/g(X) \in \bigcap_{a \in K} K[X]_{(a)}\ \ (f(X), g(X)$ は互いに素$)$ に対し $g(X)$ は定数ではないとする．K は代数的閉体だから $g(a) = 0$ となる $a \in K$ が存在する．一方，$h(X) = f_a(X)/g_a(X) \in K[X]_{(a)}$ $(f_a(X), g_a(X) \in K[X],\ g_a(a) \neq 0)$ と表され，$g_a(X)f(X) = f_a(X)g(X)$ より $g_a(a)f(a) = 0,\ f(a) = 0$ となる．剰余の定理より $f(X), g(X)$ は共に $X - a$ で割り切れるが，これは $f(X), g(X)$ が互いに素である事に反する．故に $g(X)$ は定数，即ち $h(X) \in K[X]$ である． □

【問題】 A を単位元を持つ環，M を左 A 加群，N_1, N_2 を M の部分 A 加群とする．

$$N_1 + N_2 = \{x \in M : x = y_1 + y_2 \text{ を満たす } y_1 \in N_1,\ y_2 \in N_2 \text{ がある } \}$$

と置く．以下を証明せよ．

(1) $N_1 + N_2$ は M の部分 A 加群である．
(2) $N_1 \subset N_1 + N_2$，$N_2 \subset N_1 + N_2$ が成り立つ．
(3) L を M の部分 A 加群とする．もし $N_1 \subset L$，$N_2 \subset L$ ならば $N_1 + N_2 \subset L$ が成り立つ．

(H21 首都大学東京理工学研究科 数学専攻)

【解答】 (1) $\boldsymbol{o} = \boldsymbol{o} + \boldsymbol{o}$ $(\boldsymbol{o} \in N_1,\ \boldsymbol{o} \in N_2)$ より $\boldsymbol{o} \in N_1 + N_2$．$x_i = y_{i1} + y_{i2} \in N_1 + N_2$ $(i = 1, 2)$，$a_1, a_2 \in A$ のとき

$$a_1x_1 + a_2x_2 = (a_1y_{11} + a_2y_{21}) + (a_1y12 + a_2y22) \in N_1 + N_2.$$

従って $N_1 + N_2$ は M の部分 A 加群である．

(2) 任意の $x_1 \in N_1$ に対し $x_1 = x_1 + \boldsymbol{o}$ $(\boldsymbol{o} \in N_2)$ より $x_1 \in N_1 + N_2$，$N_1 \subset N_1 + N_2$ である．$N_2 \subset N_1 + N_2$ も同様．

(3) 任意の $x = x_1 + x_2 \in N_1 + N_2$ $(x_i \in N_i)$ に対し $x_i \in L$ と L が部分 A 加群である事から $x_1 + x_2 \in L$．従って $N_1 + N_2 \subset L$ となる． □

【問題】　$\beta = 1 - \sqrt{3} + \sqrt{5}$ について次の問に答えよ．

(1)　β は $\mathbb{Q}(\sqrt{3})$ 上の最小多項式を求めよ．
(2)　β は $\mathbb{Q}$ 上の最小多項式を求めよ．
(3)　$\mathbb{Q}(\beta)$ を $\mathbb{Q}$ の Galois 拡大である事を示し，Galois 群 $Gal(\mathbb{Q}(\beta)/\mathbb{Q})$ の構造を求めよ．
(4)　$\mathbb{Q}(\beta)$ に含まれる $\mathbb{Q}$ の 2 次拡大体を全て求めよ．

(H20 首都大学東京理工学研究科 数学専攻)

【解答】　(1)　$(\beta + \sqrt{3} - 1)^2 = 5$, $\beta^2 + 2(\sqrt{3} - 1)\beta - 2\sqrt{3} - 1 = 0$ より $m_1(t) = t^2 + 2(\sqrt{3} - 1)t - 2\sqrt{3} - 1$ とすれば $m_1(\beta) = 0$．$\beta \notin \mathbb{Q}(\beta)$ より $m_1(t)$ の次数は 2 以上だから，$m_1(t)$ が $\mathbb{Q}(\sqrt{3})$ 上の最小多項式となる．

(2)　$\beta^2 - 2\beta - 1 = 2\sqrt{3}(\beta + 1)$, $(\beta^2 - 2\beta - 1)^2 = 12(\beta + 1)^2$, $\beta^4 - 4\beta^3 - 10\beta^2 + 28\beta - 11 = 0$ となる．ここで $m_2(t) = t^4 - 4t^3 - 10t^2 + 28t - 11$ とすれば $m_2(\beta) = 0$．$m_3(t) = m_2(t + 1) = t^4 - 16t^2 + 4$ と置くとき，$\mathbb{R}[t]$ に於いて

$$m_3(t) = (t^2 - 2\sqrt{3}t - 2)(t^2 + 2\sqrt{3}t - 2) = (t + \sqrt{3} - \sqrt{5})(t + \sqrt{3} + \sqrt{5})(t - \sqrt{3} + \sqrt{5})(t - \sqrt{3} - \sqrt{5})$$

従って

$$m_2(t) = (t - 1 + \sqrt{3} - \sqrt{5})(t - 1 + \sqrt{3} + \sqrt{5})(t - 1 - \sqrt{3} + \sqrt{5})(t - 1 - \sqrt{3} - \sqrt{5})$$

となるから $m_2(t)$ は $\mathbb{Q}$ 上既約となる．これより $m_2(t)$ は β の $\mathbb{Q}$ 上の最小多項式である．

(3)　$\gamma = \beta - 1$ とすれば $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta)$ であり，(2) の計算より $m_3(t)$ が γ の $\mathbb{Q}$ 上の最小多項式となる．$m_3(t)$ の根は $\pm\sqrt{3} \pm \sqrt{5}$ であり

$$-\gamma = \sqrt{3} - \sqrt{5}, \qquad \frac{2}{\gamma} = \sqrt{3} + \sqrt{5}, \qquad -\frac{2}{\gamma} = -\sqrt{3} - \sqrt{5}$$

となるから $m_3(t)$ の根は全て $\mathbb{Q}(\gamma)$ に属す．従って $\mathbb{Q}(\gamma)$ は既約多項式 $m_3(t)$ の $\mathbb{Q}$ 上の最小分解体となり，よって $\mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$ は $\mathbb{Q}$ の Galois 拡大体である．次に単位的 $\mathbb{Q}$ 代数射 $\sigma, \tau : \mathbb{Q}(\gamma) \to \mathbb{Q}(\gamma)$ を $\sigma(\gamma) = -\gamma$, $\tau(\gamma) = 2/\gamma$ により定義すると

$$\sigma^2 = \tau^2 = 1, \qquad \sigma \cdot \tau = \tau \cdot \sigma$$

となる事が容易に確められ，これより $Gal(\mathbb{Q}(\beta)/\mathbb{Q}) = Gal(\mathbb{Q}(\gamma)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる事が分かる．

(4)　(3) の記号を用いれば，$Gal(\mathbb{Q}(\beta)/\mathbb{Q})$ の位数 2 の部分群は $H_1 = \{id, \sigma\}$, $H_2 = \{id, \tau\}$, $H_3 = \{id, \sigma\tau\}$ の 3 種．$\mathbb{Q}(\gamma)$ の元 x を $\mathbb{Q}$ 上の基底 $\{1, \gamma, \gamma^2, \gamma^3\}$ を用いて $x = x_0 + x_1\gamma + x_2\gamma^2 + x_3\gamma^3$ と表す．

(i)　$\sigma(x) = x_0 - x_1\gamma + x_2\gamma^2 - x_3\gamma^3$ より $\sigma(x) = x \Leftrightarrow x_1 = x_3 = 0$．従って $\mathbb{Q}(\gamma)^{H_1} = \mathbb{Q}(\gamma^2)$．$\gamma^2 = 8 - 2\sqrt{15}$ より $\mathbb{Q}(\gamma^2) = \mathbb{Q}(\sqrt{15})$ となる．

(ii)　$\gamma^4 - 16\gamma^2 + 4 = 0$ より

$$\begin{aligned}\tau(x) &= x_0 + \frac{2x_1}{\gamma} + \frac{4x_2}{\gamma^2} + \frac{8x_3}{\gamma^3} = x_0 + x_1(-\frac{1}{2}\gamma^3 + 8\gamma) + x_2(16 - \gamma^2) + x_3(126\gamma - 8\gamma^3) \\ &= x_0 + 16x_2 + (8x_1 + 126x_3)\gamma - x_2\gamma^2 + \left(-\frac{x_1}{2} - 8x_3\right)\gamma^3.\end{aligned}$$

これより $\tau(x) = x \Leftrightarrow x_2 = 0$, $x_1 = -18x_3$，従って $x = x_0 + x_3(-18\gamma + \gamma^3) = x_0 + x_3\left(-2\gamma - \frac{4}{\gamma}\right) = x_0 - 4x_3\sqrt{5}$ となり，$\mathbb{Q}(\gamma)^{H_2} = \mathbb{Q}(\sqrt{5})$ となる．

(iii)　(ii) より $\sigma\tau(x) = x_0 + 16x_2 - (8x_1 + 126x_3)\gamma - x_2\gamma^2 - \left(-\frac{x_1}{2} - 8x_3\right)\gamma^3$．これより $\tau(x) = x \Leftrightarrow x_2 = 0$, $x_1 = -14x_3$，従って $x = x_0 + x_3(-14\gamma + \gamma^3) = x_0 + x_3\left(2\gamma - \frac{4}{\gamma}\right) = x_0 - 4x_3\sqrt{3}$ となり，$\mathbb{Q}(\gamma)^{H_3} = \mathbb{Q}(\sqrt{3})$ となる．

以上より $\mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$ に含まれる $\mathbb{Q}$ の 2 次拡大体は $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{3})$ の 3 個である．　□

【問題】 自然数 n に対し，$\zeta^n = 1$ かつ $\zeta^m \neq 1$ (ただし m は $1 \leq m < n$ となる全ての自然数) となるような複素数 ζ を 1 の原始 n 乗根と呼び，それら全ての集合を W_n と書く．さらに

$$\Phi_n(X) = \prod_{\zeta \in W_n} (X - \zeta)$$

とおく．このとき以下の問いに答えよ．

(1) 1 の原始 12 乗根を全て求め，それぞれ $a + bi$ (ただし a, b は実数，$i = \sqrt{-1}$) の形で表せ．
(2) $\Phi_5(X)$ と $\Phi_9(X)$ を具体的に多項式の形で表せ．
(3) 奇素数 p に対し $\Phi_p(X+1) = \sum_{j=0}^{N} a_j X^j$ ($N = |W_p|$) とおいたとき，各 a_j を求めよ．
(4) 奇素数 p に対し $\Phi_p(X)$ が $\mathbb{Q}$ 上既約であることを証明せよ．

(H19 首都大理工学研究科 数学専攻)

【解答】 (1) $\zeta = e^{i\theta}$ と置く．このとき $\zeta^{12} = e^{i12\theta} = 1$ より $12\theta \in 2\pi\mathbb{Z}$，したがって $\theta = i\frac{k}{6}\pi$ ($k \in \mathbb{Z}$, $0 \leq k < 12$) と表される．この k に対し

$$1 \leq \exists m < 12 \ \text{ s.t. } \ \frac{mk}{6}\pi \in 2\pi\mathbb{Z} \quad \Leftrightarrow \quad k \in \{2, 3, 4, 6, 8, 9, 10\}$$

だから，ζ が原始 12 乗根である事と k と 12 は互いに素である事が同値になる．故に原始 12 乗根の全体 W_{12} は次の 4 つからなる：

$$e^{i\frac{\pi}{6}} = \frac{\sqrt{3}}{2} + \frac{1}{2}i, \quad e^{i\frac{5\pi}{6}} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i, \quad e^{i\frac{7\pi}{6}} = -\frac{\sqrt{3}}{2} - \frac{1}{2}i, \quad e^{i\frac{11\pi}{6}} = \frac{\sqrt{3}}{2} - \frac{1}{2}i$$

(2) $e^{i\frac{2k\pi}{5}}$ ($0 < k < 5$) が原始 5 乗根の全体だから

$$\begin{aligned}
\Phi_5(X) &= (X - e^{i\frac{2\pi}{5}})(X - e^{i\frac{4\pi}{5}})(X - e^{i\frac{6\pi}{5}})(X - e^{i\frac{8\pi}{5}}) \\
&= (X^2 + 1 - (e^{i\frac{2\pi}{5}} + e^{i\frac{8\pi}{5}})X)(X^2 + 1 - (e^{i\frac{4\pi}{5}} + e^{i\frac{6\pi}{5}})X) \\
&= (X^2+1)^2 - (e^{i\frac{2\pi}{5}} + e^{i\frac{8\pi}{5}} + e^{i\frac{4\pi}{5}} + e^{i\frac{6\pi}{5}})X(X^2+1) + (e^{i\frac{2\pi}{5}} + e^{i\frac{4\pi}{5}} + e^{i\frac{6\pi}{5}} + e^{i\frac{8\pi}{5}})X^2
\end{aligned}$$

($\because$ $(e^{i\frac{2\pi}{5}} + e^{i\frac{8\pi}{5}})(e^{i\frac{4\pi}{5}} + e^{i\frac{6\pi}{5}}) = e^{i\frac{6\pi}{5}} + e^{i\frac{8\pi}{5}} + e^{i\frac{12\pi}{5}} + e^{i\frac{14\pi}{5}} = e^{i\frac{6\pi}{5}} + e^{i\frac{8\pi}{5}} + e^{i\frac{2\pi}{5}} + e^{i\frac{4\pi}{5}}$). ここで $\zeta = e^{i\frac{2\pi}{5}}$ ($\neq 1$) と置けば $(\zeta - 1)(\zeta + \zeta^2 + \zeta^3 + \zeta^4) = \zeta^5 - \zeta = 1 - \zeta$ だから $\zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$.

$$\therefore \quad \Phi_5(X) = (X^2+1)^2 + (X^2+1)X - X^2 = \underline{X^4 + X^3 + X^2 + X + 1}$$

一方，$k = 3, 6$ 以外の $0 < k < 9$ に対する $e^{i\frac{2k\pi}{9}}$ が原始 9 乗根となるから

$$\begin{aligned}
\Phi_9(X) &= (X - e^{i\frac{2\pi}{9}})(X - e^{i\frac{4\pi}{9}})(X - e^{i\frac{8\pi}{9}})(X - e^{i\frac{10\pi}{9}})(X - e^{i\frac{14\pi}{9}})(X - e^{i\frac{16\pi}{9}}) \\
&= (X - e^{i\frac{2\pi}{9}})(X - e^{i\frac{16\pi}{9}}) \times (X - e^{i\frac{4\pi}{9}})(X - e^{i\frac{14\pi}{9}}) \times (X - e^{i\frac{8\pi}{9}})(X - e^{i\frac{10\pi}{9}}) \\
&= \{X^2 + 1 - (e^{i\frac{2\pi}{9}} + e^{i\frac{16\pi}{9}})X\}\{X^2 + 1 - (e^{i\frac{4\pi}{9}} + e^{i\frac{14\pi}{9}})X\}\{X^2 + 1 - (e^{i\frac{8\pi}{9}} + e^{i\frac{10\pi}{9}})X\}
\end{aligned}$$

ここで $\zeta = e^{i\frac{2\pi}{9}}$ ($\neq 1$) と置くと

$$1 + \zeta^3 + \zeta^6 = 1 + e^{i\frac{2\pi}{3}} + e^{i\frac{4\pi}{3}} = 1 + \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) + \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = 0$$

となる事から

$$(\zeta - 1)(\zeta + \zeta^2 + \zeta^4 + \zeta^5 + \zeta^7 + \zeta^8) = \zeta(\zeta^2 - 1)(1 + \zeta^3 + \zeta^6) = 0,$$

従って $\zeta + \zeta^2 + \zeta^4 + \zeta^5 + \zeta^7 + \zeta^8 = 0$ となる．さらに

$$\begin{aligned}
&(\zeta + \zeta^8)(\zeta^2 + \zeta^7) + (\zeta^2 + \zeta^7)(\zeta^4 + \zeta^5) + (\zeta^4 + \zeta^5)(\zeta + \zeta^8) \\
=&\zeta + \zeta^4 + \zeta^7 + \zeta^2 + \zeta^5 + \zeta^8 + 3\zeta^3 + 3\zeta^6 \\
=&\zeta(1 + \zeta^3 + \zeta^6) + \zeta^2(1 + \zeta^3 + \zeta^6) + 3(1 + \zeta^3 + \zeta^6) - 3 = -3
\end{aligned}$$

$$\begin{aligned}
&(\zeta + \zeta^8)(\zeta^2 + \zeta^7)(\zeta^4 + \zeta^5) = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 - 1 \\
=&(1 + \zeta^3 + \zeta^6) + (\zeta + \zeta^4 + \zeta^7) + (\zeta^2 + \zeta^5 + \zeta^8) - 1 = (1 + \zeta + \zeta^2)(1 + \zeta^3 + \zeta^6) - 1 = -1
\end{aligned}$$

従って

$$\begin{aligned}\Phi_9(X) &= (X^2+1)^3 - \{(\zeta+\zeta^8)+(\zeta^2+\zeta^7)+(\zeta^4+\zeta^5)\}(X^2+1)^2X \\ &\quad + \{(\zeta+\zeta^8)(\zeta^2+\zeta^7)+(\zeta^2+\zeta^7)(\zeta^4+\zeta^5)+(\zeta^4+\zeta^5)(\zeta+\zeta^8)\}(X^2+1)X^2 \\ &\quad - \{(\zeta+\zeta^8)(\zeta^2+\zeta^7)(\zeta^4+\zeta^5)\}X^3 \\ &= (X^2+1)^3 - 0\cdot(X^2+1)^2X + (-3)(X^2+1)X^2 - (-1)X^3 \\ &= X^6+3X^4+3X^2+1-3X^3-3X^2+X^3 = \underline{X^6+X^3+1}\end{aligned}$$

(3) $\zeta = e^{\frac{2\pi i}{p}}$ と置けば $W_p = \{\zeta^k : k = 1, \cdots, p-1\}$. W_p の元は $X^p-1=0$ の解であり, $X^p-1=(X-1)(X^{p-1}+\cdots+X+1)$ 及び $\zeta^k \neq 1$ $(1 \leq k \leq p-1)$ より $\Phi_p(X) = X^{p-1}+\cdots+X+1$. 従って

$$\Phi_p(X+1) = \sum_{k=0}^{p-1}(X+1)^k = \sum_{k=0}^{p-1}\sum_{j=0}^{k} {}_kC_jX^j = \sum_{j=0}^{p-1}\sum_{k=j}^{p-1} {}_kC_jX^j \qquad \therefore \quad a_j = \underline{\sum_{k=j}^{p-1} {}_kC_j} \quad (0 \leq j \leq p-1).$$

(4) p 個の元から成る有限体を $\mathbb{F}_p$ と記す. 等式 $X^p-1=(X-1)\Phi_p(X)$ の X を $X+1$ に置き換え, これを $\mathbb{F}_p[X]$ で考えると

$$\sum_{j=0}^{p-1} a_jX^{j+1} = X\Phi_p(X+1) = (X+1)^p - 1 = X^p+1-1 = X^p$$

だから $\mathbb{F}_p$ に於いて $a_j = 0$, 従って $p \mid a_j$ $(0 \leq j < p-1)$. 特に $a_0 = \sum_{k=0}^{p-1} {}_kC_0 = p$ だから $p^2 \nmid a_0$. Eisenstein の既約性判定法より $\Phi_p(X+1)$, 従って $\Phi_d(X)$ は $\mathbb{Z}$ 上既約. 故に $\Phi_d(X)$ は $\mathbb{Q}$ 上でも既約となる. □

【問題】 R は可換環，I, J を R の相異なるイデアルとする．次の命題が正しければ証明を与え，間違っていれば反例を与えよ．

(1) $I \cup J$ はイデアルである．

(2) $I \cap J$ はイデアルである．

(3) もし $I \cap J$ が素イデアルであれば $I \subset J$ または $J \subset I$ が成り立つ．

(H17 東京都立大学理学研究科 数学専攻)

【解答】 (1) 間違っている．

(反例) $\mathbb{C}[X, Y]$ を複素係数 2 変数多項式環とし，$I = (X), J = (Y)$ とする．このとき $X \in I \subset I \cup J$，$Y \in J \subset I \cup J$ であるが，$X + Y \notin I$ かつ $X + Y \notin J$ より $X + Y \notin I \cup J$．したがって $I \cup J$ はイデアルではない． ■

(2) 正しい．

(証明) $x, y \in I \cup J$ のとき $x + y \in I$ かつ $x + y \in J$ より $x + y \in I \cap J$．次に $x \in I$，$y \in R$ に対し $yx \in I$ かつ $yx \in J$ より $yx \in I \cap J$．従って $I \cap J$ はイデアルである． ■

(3) 正しい．

(証明) $I \not\subset J$ だとし，$x \in I \setminus I \cap J$ を取る．このとき任意の $y \in J$ に対し $yx \in I \cap J$ であり，$I \cap J$ が素イデアルである事，及び $x \notin I \cap J$ より $y \in I \cap J \subset I$ となる．即ち $J \subset I$ となる． □

【問題】 A を可換環，$A[X]$ を A 上一変数の多項式環，

$$f = a_nX^n + \cdots + a_1X + a_0 \in A[X]$$

とする．次を証明せよ．

(1) f が $A[X]$ の単元 $\Leftrightarrow$ a_0 が A の単元で $a_1, \ldots, a_n$ は A のべき零元．
(2) f が $A[X]$ のべき零元 $\Leftrightarrow$ $a_0, \ldots, a_n$ は A のべき零元．
(3) f が $A[X]$ の零因子 $\Leftrightarrow$ ある $b \in A$ $(b \neq 0)$ があって $bf = 0$．

(H17 東京都立大学理学研究科 数学専攻)

【解答】 $a_n \neq 0$ とする．

(1) n に関する帰納法により証明する．$n = 0$ のときは自明だから $n > 0$ とする．$fg = 1$ $(g = b_0 + b_1X + \cdots + b_mX^m \in A[X])$ のとき，両辺の 0 次の項を比較すれば $a_0b_0 = 1$ となる事が分かる．一方，降べキに並べると $fg = a_nb_mX^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)X^{m+n-1} + \cdots$ より

$$\begin{aligned}
a_nb_m &= 0 & & \\
a_{n-1}b_m + a_nb_{m-1} &= 0 & a_n^2b_{m-1} &= 0, \\
a_{n-2}b_m + a_{n-1}b_{m-1} + a_nb_{m-2} &= 0 & a_n^3b_{m-2} &= 0, \\
a_{n-3}b_m + a_{n-2}b_{m-1} + a_{n-1}b_{m-2} + a_nb_{m-3} &= 0 & a_n^4b_{m-3} &= 0, \\
& \cdots & & \\
\cdots + a_{n-2}b_2 + a_{n-1}b_1 + a_nb_0 &= 0 & a_n^{m+1}b_0 &= 0.
\end{aligned}$$

b_0 は単元だから $a_n^{m+1} = 0$ となり a_n はベキ零となる．更に

$$1 = f^{m+1}g^{m+1} = (f^{m+1} - a_n^{m+1}X^{n(m+1)})g^{m+1} = (f - a_nX^n)(f^m + f^{m-1}a_nX^n + \cdots + a_n^mX^{nm})g^{m+1}$$

より $f - a_nX^n$ は $A[X]$ の単元であり，帰納法の仮定より $a_0 \in A^\times$ かつ $a_1, a_2, \cdots, a_{n-1}$ はベキ零となる．逆に $a_0 \in A^\times$ かつ $a_1, \cdots, a_n$ はベキ零だとする．帰納法の仮定より $(f - a_nX^n)g = 1$ となる $g \in A[X]$ が存在する．$a_n^m = 0$ だとすると $(fg - 1)^m = a_n^mX^{mn}g^m = 0$，従って

$$f(f^{m-1}g^m + {}_mC_1f^{m-2}g^{m-1} + \cdots + {}_mC_{m-2}fg^2 + {}_mC_{m-1}g) = 1$$

となり $f \in A[X]^\times$ となる．

(2) n に関する帰納法により証明する．$n = 0$ のときは自明だから $n > 0$ とする．$f^m = 0$ だとすると f^m の最高次 mn の係数は $a_n^m = 0$ となる．

$$(f - a_nX^n)^{2m} = f^m\sum_{i=0}^{m} {}_{2m}C_if^{m-i}(a_nX^n)^i + a_n^mX^{nm}\sum_{i=1}^{m} {}_{2m}C_{m+i}f^{m-i}(a_nX^n)^i = 0$$

より $f - a_nX^n$ は再びベキ零．帰納法の仮定より $a_0, \cdots, a_{n-1}$ もベキ零である．逆に $a_0, \cdots, a_n$ がベキ零だとする．$a_n^m = 0$ だとする．帰納法の仮定より $(f - a_nX^n)^l = 0$ となる l が存在する．このとき

$$f^{lm} = (f^m)^l = (f^m - a_n^mX^{nm})^l = (f - a_nX^n)^l(f^{m-1} + f^{m-2}a_nX^n + \cdots + a_n^{m-1}X^{n(m-1)})^l = 0$$

だから f もベキ零となる．

(3) $\Leftarrow$ は自明．逆に f は零因子だとする．g を $fg = 0$ となる零ではない，次数が最小の $A[X]$ の元とする．$g = b_mX^m + \cdots + b_1X + b_0$ $(b_m \neq 0)$ だとする．仮に $b_mf \neq 0$ だとすると $a_ib_m \neq 0$ となる i が存在し $a_ig \neq 0$ となる．$a_ig \neq 0$ となる $0 \leq i \leq n$ の中で最大なものを改めて i とすると

$$0 = fg = a_ngX^n + a_{n-1}gX^{n-1} + \cdots + a_igX^i + \cdots + a_0g = (a_iX^i + \cdots + a_0)g$$

が成立．fg の最高次の係数 a_ib_m は 0 となるから，a_ig は g よりも低い次数を持ち，更に $f \cdot a_ig = 0$ となるが，これは g の取り方，特に次数の最小性と矛盾する．故に $b_mf = 0$ である． □

【問題】　$p(X)=X^3+X^2+c$　($c\in\mathbb{R}$) に対し $D(c)=-c(27c+4)$ と置く.

(1)　$p(X)$ が重根を持つ　$\Leftrightarrow$　$D(c)=0$ を示せ.
(2)　$D(c)\neq 0$ とし, $p(X)$ の 1 つの根を θ とする. このとき

$$D(c)=p'(\theta)^2(\theta+1)(1-3\theta)$$

である事を示せ. また $p(X)$ の θ 以外の根を θ を用いて表せ.
(3)　$p(X)$ が相異なる 3 実根を持つ為の必要十分条件は $D(c)>0$ である事を示せ.
(4)　$c\in\mathbb{Q}$, $D(c)\neq 0$ とし, $p(X)$ は $\mathbb{Q}$ 上既約とする. また θ を $p(X)$ の根とする. このとき $\mathbb{Q}(\theta)/\mathbb{Q}$ は Galois 拡大　$\Leftrightarrow$　$D(c)$ は $\mathbb{Q}$ 内の平方根　を示せ.

(H16 東京都立大学理学研究科 数学専攻)

【解答】　(1)　$p(X)$ の (分解体に於ける)3 根を $\theta_1,\theta_2,\theta_3$ とする. 解と係数の関係より

$$\theta_1+\theta_2+\theta_3=-1,\qquad \theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1=0,\qquad \theta_1\theta_2\theta_3=-c,$$

が成立. ここで $\Delta=(\theta_1-\theta_2)^2(\theta_2-\theta_3)^2(\theta_3-\theta_1)^2$ と置く.

$$\begin{aligned}(\theta_1-\theta_2)(\theta_1-\theta_3)&=\theta_1^2-(\theta_2+\theta_3)\theta_1+\theta_2\theta_3=\theta_1^2-(\theta_2+\theta_3)\theta_1-(\theta_2+\theta_3)\theta_1\\&=\theta_1^2+2(1+\theta_1)\theta_1=3\theta_1^2+2\theta_1.\end{aligned}$$

同様に $(\theta_2-\theta_1)(\theta_2-\theta_3)=3\theta_2^2+2\theta_2$, $(\theta_3-\theta_1)(\theta_3-\theta_2)=3\theta_3^2+2\theta_3$ を得る.

$$\begin{aligned}\Delta&=-(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_2-\theta_1)(\theta_2-\theta_3)(\theta_3-\theta_1)(\theta_3-\theta_2)\\&=-(3\theta_1^2+2\theta_1)(3\theta_2^2+2\theta_2)(3\theta_3^2+2\theta_3)=-\theta_1\theta_2\theta_3(3\theta_1+2)(3\theta_2+2)(3\theta_3+2)\\&=-\theta_1\theta_2\theta_3\{27\theta_1\theta_2\theta_3+18(\theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1)+12(\theta_1+\theta_2+\theta_3)+8\}=c(-27c-4)=D(c).\end{aligned}$$

Δ の定義より $p(X)$ が重根を持つ事と $D(c)=0$ となる事は同値となる.

(2)　$\theta^3+\theta^2+c=0$ より

$$p'(\theta)^2(\theta+1)(1-3\theta)=(3\theta^2+2\theta)^2(\theta+1)(1-3\theta)=-\theta^2(\theta+1)(27\theta^3+27\theta^2-4)=-c(27c+4)=D(c).$$

また $p(X)=(X-\theta)(X^2+(\theta+1)X+\theta^2+\theta)$ と分解でき, θ 以外の根は $X^2+(\theta+1)X+\theta^2+\theta$ の根, 即ち

$$\frac{-(\theta+1)\pm\sqrt{(\theta+1)(1-3\theta)}}{2}$$

により与えられる.

(3)　$p(X)$ は 3 次式だから少なくとも 1 つの実根 θ を持つ. $p(X)$ が相異なる 3 実根を持つとする. (1) より $D(c)\neq 0$ であり, $p'(\theta)\neq 0$, 従って $p'(\theta)^2>0$ となる. 更に $X^2+(\theta+1)X+\theta^2+\theta$ が相異なる 2 実根を持つ事から $(\theta+1)(1-3\theta)>0$. 従って $D(c)>0$ となる. 逆に $D(c)>0$ だとすると $p'(\theta)\neq 0$ より θ は単根であり, $(\theta+1)(1-3\theta)>0$ より $X^2+(\theta+1)X+\theta^2+\theta$ は相異なる 2 実根を持ち, これらより $p(X)$ は相異なる 3 実根を持つ事が分かる.

(4)　$\theta_1=\theta,\theta_2,\theta_3$ を $p(X)$ の $\mathbb{C}$ に於ける相異なる 3 根とし, $K=\mathbb{Q}(\theta_1,\theta_2,\theta_3)$ と置く. K は $p(X)$ の $\mathbb{Q}$ 上の最小分解体だから $K/\mathbb{Q}$ は Galois 拡大であり, $\mathbb{Q}(\theta)$ は $K/\mathbb{Q}$ の中間体となる. 任意の $\sigma\in Gal(K/\mathbb{Q})$ は根の集合 $\{\theta_1,\theta_2,\theta_3\}$ の置換を定めるから, $\sigma(\theta_i)=\theta_{\sigma(i)}$ により群の準同型射

$$\varphi:Gal(K/\mathbb{Q})\to\mathfrak{S}_3\qquad \varphi(\sigma)=\begin{pmatrix}1&2&3\\ \sigma(1)&\sigma(2)&\sigma(3)\end{pmatrix}$$

($\mathfrak{S}_3$ は 3 次対称群) が定まる. φ は単射だから

$$3=[\mathbb{Q}(\theta):\mathbb{Q}]\leq[K:\mathbb{Q}]=\sharp Gal(K/\mathbb{Q})\leq\sharp\mathfrak{S}_3=6$$

となる. 更に $\sqrt{D(c)}=\pm(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_3-\theta_1)\in K$, かつ $\sigma(\sqrt{D(c)})=\mathrm{sgn}(\varphi(\sigma))\sqrt{D(c)}$　($\sigma\in Gal(K/\mathbb{Q})$) となる事に注意する.

$\sqrt{D(c)}\in\mathbb{Q}$ のとき, $K^{Gal(K/\mathbb{Q})}=\mathbb{Q}$ より任意の $\sigma\in Gal(K/\mathbb{Q})$ に対し $\sigma(\sqrt{D(c)})=\sqrt{D(c)}$, 従って $\mathrm{sgn}(\varphi(\sigma))=1$ となるから $\varphi(\sigma)$ は $\mathfrak{A}_3$　(3 次交代群 =3 次巡回群) に含まれる. $3=[\mathbb{Q}(\theta):\mathbb{Q}]\leq[K:\mathbb{Q}]\leq\sharp\mathfrak{A}_3=3$, 従って $K=\mathbb{Q}(\theta)$ となる.

逆に $\mathbb{Q}(\theta)/\mathbb{Q}$ が Galois 拡大だとすると $K=\mathbb{Q}(\theta)$ となり, これより $\varphi(Gal(K/\mathbb{Q}))$ は $\mathfrak{S}_3$ の位数 3 の部分群, 即ち $Gal(K/\mathbb{Q})$ は $\mathfrak{A}_3$ と同型となる. 従って $\varphi(\sigma)$ は偶置換となり, $\sigma(\sqrt{D(c)})=\sqrt{D(c)}$, よって $\sqrt{D(c)}\in K^{Gal(K/\mathbb{Q})}=\mathbb{Q}$ となる.　□