【問題】 体を $K = \mathbb{Q}(\sqrt[4]{2})$ とおくとき，以下の問いに答えよ．

(1) K が $\mathbb{Q}$ の Galois 拡大ではない事を示せ．
(2) K を含む $\mathbb{Q}$ の Galois 拡大 L で最小のものを求めよ．
(3) Galois 群 $Gal(L/\mathbb{Q})$ が位数 8 の二面体群と同型である事を示せ．
(4) L の部分体を全て求めよ．

(H29 千葉大学理学研究科 数学・情報)

【解答】 $i = \sqrt{-1}$ とする．

(1) $f(x) = x^4 - 2$ と置けば Einsenstein の既約性判定法より $f(x)$ は $\mathbb{Q}$ 上既約であり，$f(\sqrt[4]{2}) = 0$ だから $f(x)$ は $\sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式である．$\mathbb{C}$ に於いて $f(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$ と分解されるが，$\pm\sqrt[4]{2}i$ は K に含まれないから $f(x)$ は K で 1 次式の積に分解されない．よって K は $\mathbb{Q}$ の正規拡大ではなく，従って Galois 拡大ではない．
(2) $L = \mathbb{Q}(\sqrt[4]{2}, i)$ とすれば, (1) の計算より L は $\mathbb{Q}$ 上の既約単多項式の $f(x)$ の最小分解体となり，従って L は $\mathbb{Q}$ の Galois 拡大である．
(3) 位数 8 の 2 面体群 D_4 とは基本関係式 $s^2 = t^2 = (st)^4 = e$ を持つ 2 つの生成元 s, t により生成される位数 8 の群である事に注意する．

K と $\mathbb{Q}(x)/f(x)\mathbb{Q}(x)$ と $\mathbb{Q}$ 上同型だから $[K : \mathbb{Q}] = \deg f(x) = 4$． $L = K(i) = K + Ki$ より $[L : K] = 2$． よって $\sharp Gal(L/\mathbb{Q}) = [L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 8$ となる． $Gal(L/\mathbb{Q})$ の元は $\sqrt[4]{2}, i$ の行き先により決定される事に注意し，$\sigma, \tau \in Gal(L/\mathbb{Q})$ をそれぞれ

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad \sigma(i) = i, \qquad \tau(\sqrt[4]{2}) = \sqrt[4]{2}, \quad \sigma(i) = -i$$

によって定義する．このとき

	id	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

だから $Gal(L/\mathbb{Q}) = \{\sigma^i,\ \sigma^i\tau\}_{i=0,1,2,3}$ となる．

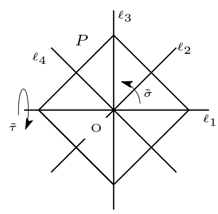
$$(\sigma\tau)^2(\sqrt[4]{2}) = \sigma\tau(i\sqrt[4]{2}) = (-i)\cdot i\sqrt[4]{2} = \sqrt[4]{2}, \qquad (\sigma\tau)^2(i) = \sigma\tau(-i) = i, \qquad \therefore \quad (\sigma\tau)^2 = id,$$

及び $\tau^2 = id$，$(\sigma\tau \cdot \tau)^4 = \sigma^4 = id$ より，$t \mapsto \tau$，$s \mapsto \sigma\tau$ によって D_4 から $Gal(L/\mathbb{Q})$ への群の全射が導かれる．共に位数 8 である事から，これは同型射となる．
(4) 最初に 2 面体群 D_4 の部分群を決定する．D_4 は右図の正方形 P を P に移す変換群であり，各元は次のような変換を表す：

(i) $G_0 = \{id\}$，$G_1 = D_4$ とする．
(ii) 原点 O を中心とする $\pi/2$ 回転を $\tilde{\sigma}$，直線 ℓ_1 に関する折り返しを $\tilde{\tau}$ とする．D_4 は $\tilde{\sigma}, \tilde{\tau}$ により生成され,

$$\tilde{\sigma}^4 = id, \quad \tilde{\tau}^2 = id, \quad (\tilde{\tau}\tilde{\sigma})^2 = id$$

が成立．従って $\tilde{\sigma} \mapsto \sigma$，$\tilde{\tau} \mapsto \tau$ という対応は D_4 から $Gal(L/\mathbb{Q})$ への同型となる．



(iii) $\tilde{\sigma}$ により生成される群 G_2 は位数 4 の部分群となる．
(iii) $\tilde{\sigma}^2$ ($= \pi$ 回転) は位数 2 の元となる．$\tilde{\sigma}^2$ で生成される群 G_3 は位数 2 の部分群となる．
(iv) ℓ_2，ℓ_3，ℓ_4 に関する折り返しはそれぞれ $\tilde{\sigma}\tilde{\tau}$，$\tilde{\sigma}^2\tilde{\tau}$，$\tilde{\sigma}^3\tilde{\tau}$ により与えられる．$\tilde{\tau}$，$\tilde{\sigma}\tilde{\tau}$，$\tilde{\sigma}^2\tilde{\tau}$，$\tilde{\sigma}^3\tilde{\tau}$ で生成される部分群をそれぞれ $G_4, \cdots, G_7$ とすれば各 G_i は位数 2 の部分群となる．
(v) 直線 ℓ_1, ℓ_3 に関する折り返しにより生成される部分群を $G_8 = \{id, \tilde{\tau}, \tilde{\sigma}^2\tilde{\tau}, \tilde{\sigma}^2\}$ とする．
(vi) 直線 ℓ_2, ℓ_4 に関する折り返しにより生成される部分群を $G_9 = \{id, \tilde{\sigma}\tilde{\tau}, \tilde{\sigma}^3\tilde{\tau}, \tilde{\sigma}^2\}$ とする．

以上より D_4 の部分群は $G_0 \sim G_9$ の計 10 個である．次に G_i に関する L の不変体を L_i を求める．$L_0 = L$，$L_1 = \mathbb{Q}$ となる事は自明．L の $\mathbb{Q}$ 上の基底 $\{\sqrt[4]{2^j}, i\sqrt[4]{2^j}\}_{j=0,1,2,3}$ をとり，任意の $x \in L$ を

$$x = x_0 + x_1\sqrt[4]{2} + x_2\sqrt[4]{2^2} + x_3\sqrt[4]{2^3} + x_4 i + x_5 i\sqrt[4]{2} + x_6 i\sqrt[4]{2^2} + x_7 i\sqrt[4]{2^3}$$

と表す．

(i) $\sigma(x) = x_0 - x_5\sqrt[4]{2} - x_2\sqrt[4]{2^2} + x_7\sqrt[4]{2^3} + x_4 i + x_1 i\sqrt[4]{2} - x_6 i\sqrt[4]{2^2} - x_3 i\sqrt[4]{2^3}$ より

$$\sigma(x) = x \quad \Leftrightarrow \quad x_1 = x_2 = x_3 = x_5 = x_6 = x_7 = 0, \quad \Leftrightarrow \quad x = x_0 + x_4 i \qquad \therefore \quad L_2 = \mathbb{Q}(i)$$

(ii) $\sigma^2(x) = x_0 - x_1\sqrt[4]{2} + x_2\sqrt[4]{2^2} - x_3\sqrt[4]{2^3} + x_4 i - x_5 i\sqrt[4]{2} + x_6 i\sqrt[4]{2^2} - x_7 i\sqrt[4]{2^3}$ より

$$\sigma^2(x) = x \quad\Leftrightarrow\quad x_1 = x_3 = x_5 = x_7 = 0, \quad\Leftrightarrow\quad x = x_0 + x_2\sqrt[4]{2^2} + x_4 i + x_6 i\sqrt[4]{2^2}, \qquad \therefore\quad L_3 = \mathbb{Q}(i, \sqrt{2}).$$

(iii) $\tau(x) = x_0 + x_1\sqrt[4]{2} + x_2\sqrt[4]{2^2} + x_3\sqrt[4]{2^3} - x_4 i - i x_5\sqrt[4]{2} - x_6 i\sqrt[4]{2^2} - i x_7\sqrt[4]{2^3}$ より

$$\tau(x) = x \quad\Leftrightarrow\quad x_4 = x_5 = x_6 = x_7 = 0, \quad\Leftrightarrow\quad x = x_0 + x_1\sqrt[4]{2} + x_2\sqrt[4]{2^2} + x_3\sqrt[4]{2^3}, \qquad \therefore\quad L_4 = \mathbb{Q}(\sqrt[4]{2}) = K.$$

(vi) $\sigma\tau(x) = x_0 + x_5\sqrt[4]{2} - x_2\sqrt[4]{2^2} - x_7\sqrt[4]{2^3} - x_4 i + x_1 i\sqrt[4]{2} + x_6 i\sqrt[4]{2^2} - x_3 i\sqrt[4]{2^3}$ より

$$\begin{aligned}\sigma\tau(x) = x \quad&\Leftrightarrow\quad x_2 = 0,\ x_4 = 0,\ x_5 = x_1,\ x_7 = -x_3 \\ &\Leftrightarrow\quad x = x_0 + x_1\frac{1+i}{\sqrt[4]{2}} + x_2\left(\frac{1+i}{\sqrt[4]{2}}\right)^2 + x_3\left(\frac{1+i}{\sqrt[4]{2}}\right)^3 \qquad \therefore\quad L_5 = \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right).\end{aligned}$$

(v) $\sigma^2\tau(x) = x_0 - x_1\sqrt[4]{2} + x_2\sqrt[4]{2^2} - x_3\sqrt[4]{2^3} - x_4 i + x_5 i\sqrt[4]{2} - x_6 i\sqrt[4]{2^2} + x_7 i\sqrt[4]{2^3}$ より

$$\tau(x) = x \quad\Leftrightarrow\quad x_1 = x_3 = x_4 = x_6 = 0 \quad\Leftrightarrow\quad x = x_0 + x_2\sqrt[4]{2^2} + x_5 i\sqrt[4]{2} + x_7 i\sqrt[4]{2^3}, \qquad \therefore\quad L_6 = \mathbb{Q}(i\sqrt[4]{2}).$$

(vi) $\sigma^3\tau(x) = x_0 - x_5\sqrt[4]{2} - x_2\sqrt[4]{2^2} + x_7\sqrt[4]{2^3} - x_4 i - x_1 i\sqrt[4]{2} + x_6 i\sqrt[4]{2^2} + x_3 i\sqrt[4]{2^3}$ より

$$\begin{aligned}\tau(x) = x \quad&\Leftrightarrow\quad x_2 = 0,\ x_4 = 0,\ x_5 = -x_1,\ x_7 = x_3 \\ &\Leftrightarrow\quad x = x_0 + x_1\frac{1-i}{\sqrt[4]{2}} + x_2\left(\frac{1-i}{\sqrt[4]{2}}\right)^2 + x_3\left(\frac{1-i}{\sqrt[4]{2}}\right)^3 \qquad \therefore\quad L_7 = \mathbb{Q}\left(\frac{1-i}{\sqrt[4]{2}}\right).\end{aligned}$$

(vii) $L_8 = L_4 \cap L_6$ より $L_8 = \mathbb{Q}(\sqrt{2})$.

(viii) $L_9 = L_5 \cap L_7$ より $L_8 = \mathbb{Q}(i\sqrt{2})$.

以上より L の部分体 (= 拡大 $L/\mathbb{Q}$ の中間体) は次の図の通り：

$$\begin{tikzcd}
 & & & & \mathbb{Q}(\sqrt[4]{2}, i) \arrow[dllll, dash] \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] \arrow[drrrr, dash] & & & & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[drr, dash] & & \mathbb{Q}(i\sqrt[4]{2}) \arrow[d, dash] & & \mathbb{Q}(\sqrt{2}, i) \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \mathbb{Q}\left(\frac{1+i}{\sqrt[4]{2}}\right) \arrow[d, dash] & & \mathbb{Q}\left(\frac{1-i}{\sqrt[4]{2}}\right) \arrow[dll, dash] \\
 & & \mathbb{Q}(\sqrt{2}) \arrow[drr, dash] & & \mathbb{Q}(i) \arrow[d, dash] & & \mathbb{Q}(i\sqrt{2}) \arrow[dll, dash] & & \\
 & & & & \mathbb{Q} & & & &
\end{tikzcd}$$

$\square$

【問題】　(1)　環 $\mathbb{Z}[X]/(X^2-1)$ は整域ではなく，環 $\mathbb{Z}[X]/(X^2+1)$ は整域であることを示せ.

(2)　p を奇素数とするとき，環 $\mathbb{Z}[X]$ のイデアルとして

$$(X^{p^2-1}-1) \subset (X^2+1)$$

であることを示せ.

(3)　p を奇素数とし，自然な準同型

$$\mathbb{Z}[X] \to \mathbb{Z}[X]/(p, X^2+1)$$

における $n \in \mathbb{Z}, X$ の像をそれぞれ $\overline{n}, \overline{X}$ と書く．このとき任意の $a, b \in \mathbb{Z}$ に対して

$$(\overline{a}\overline{X}+\overline{b})^p = \overline{a}\overline{X}+\overline{b}$$

が成立するための p の条件を求めよ.

(4)　環 $\mathbb{Z}[X]/(p, X^2+1)$ が整域であるための奇素数 p の条件を求めよ.

(H24 千葉大学理学研究科 数学専攻)

【解答】 (1) $\mathbb{Z}[X]$ から $\mathbb{Z}[X]/(X^2\pm1)$ への標準的射影を $\pi_\pm$ と記す．$\mathbb{Z}[X]/(X^2-1)$ に於いて $\pi_-(X-1)$, $\pi_-(X+1) \neq 0$, かつ $\pi_-(X-1)\pi_-(X+1) = \pi_-(X^2-1) = 0$ となるから $\mathbb{Z}[X]/(X^2-1)$ は整域ではない.

一方，$f(X), g(X) \in \mathbb{Z}[X]$ に対し $f(X)g(X) \in (X^2+1)$，$f(X) \notin (X^2+1)$ だとする．今,

$$f(X) = f_1(X)(X^2+1)+f_2(X), \quad g(X) = g_1(X)(X^2+1)+g_2(X)$$
$$(f_1(X), f_2(X), g_1(X), g_2(X) \in \mathbb{Z}[X],\ f_2(X) = a_0+a_1X, g_2(X) = b_0+b_1X,\ a_0, a_1, b_0, b_1 \in \mathbb{Z})$$

と表す．このとき $f_2(X)g_2(X) \in (X^2+1)$ であり，$f_2(X)g_2(X) = a_1b_1X^2+(a_0b_1+a_1b_0)X+a_0b_0$ だから $a_0b_1+a_1b_0 = 0$, $a_1b_1 = a_0b_0$．特に

$$a_1(a_0b_1+a_1b_0) = (a_0^2+a_1^2)b_0 = 0 \qquad a_0(a_0b_1+a_1b_0) = (a_0^2+a_1^2)b_1 = 0$$

が成立．$f(X) \notin (X^2+1)$ より $f_2(X) \neq 0$，従って $a_0^2+a_1^2 \neq 0$ だから $b_0 = b_1 = 0$，即ち $g(X) \in (X^2+1)$ となる．故に (X^2+1) は素イデアル，よって $\mathbb{Z}[X]/(X^2+1)$ は整域である.

(2) p は奇素数だから，$p = 2\ell+1$ $(\ell \in \mathbb{Z})$ と表される. $m = \frac{\ell(\ell+1)}{2}$ と置くと

$$X^{p^2-1}-1 = X^{4\ell(\ell+1)}-1 = (X^8)^m-1 = (X^8-1)\{(X^8)^{m-1}+(X^8)^{m-2}+\cdots+X^8+1\}$$

となる．$X^8-1 = (X^4+1)(X^4-1)$ だから $(X^{p^2-1}-1) \subset (X^2+1)$ となる.

(3) 一般に任意の $a, b \in \mathbb{Z}$ に対し $(\overline{a}\overline{X}+\overline{b})^p = \overline{a}\overline{X}^p+\overline{b}$ が成立．従って

$$(\overline{a}\overline{X}+\overline{b})^p = \overline{a}\overline{X}+\overline{b} \quad (\forall\, a, b \in \mathbb{Z}) \quad \Leftrightarrow \quad \overline{X}^p-\overline{X} = \overline{0}$$

となる．$p = 2m+1$ $(m \in \mathbb{Z}_{>0})$ と置くとき，左辺の両辺に $\overline{X}$ を掛ければ

$$\overline{X}^{2m+1}-\overline{X} = \overline{0} \quad \Leftrightarrow \quad \overline{X}^{2m}-1 = (-\overline{1})^m-\overline{1} = \overline{0} \quad \Leftrightarrow \quad m \in 2\mathbb{Z}$$

従って等式が成立するための条件は $p \in 4\mathbb{Z}+1$ である.

(4) $A = \mathbb{Z}[X]/(p, X^2+1) = \mathbb{F}_p[X]/\mathbb{F}_p[X](X^2+1)$ $(\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z})$ と置く．このとき A が整域である事と X^2+1 が $\mathbb{F}_p$ 上既約である事は同値である.

X^2+1 が既約でないとすると $X^2+1 = (X-a)(X-b)$ となる $a, b \in \mathbb{F}_p$ が存在する．$(X-a)(X-b) = X^2-(a+b)X+ab$ より $b = -a$，$ab = -a^2 = 1$ だから，$a^2+1 = 0$ を満たす．逆に $a^2+1 = 0$ となる $a \in \mathbb{F}_p$ が存在すれば $X^2+1 = (X+a)(X-a)$ だから，X^2+1 が既約である事と $a^2+1 = 0$ となる $a \in \mathbb{F}_p$ が存在しない事は同値となる.

今，$p-1$ と素な整数を代表とする $r \in \mathbb{F}_p$ を固定するとき，$\mathbb{F}_p^\times = \{r, r^2, \cdots, r^{p-1}\}$ $(r^{p-1} = 1)$ が成立する．$r^m = -1$ ならば $r^{2m} = 1 = r^{p-1}$ だから $r^{\frac{p-1}{2}} = -1$ となる．このとき

$$a^2+1 = 0 \text{ となる } a \in \mathbb{F}_p \text{ が存在} \quad \Leftrightarrow \quad r^{2\ell} = r^{\frac{p-1}{2}} \text{ となる } \ell \text{ が存在}$$

従って X^2+1 が $\mathbb{F}_p$ 上既約である事と $p \notin 4\mathbb{Z}+1$ が同値となる．p は奇素数だから A が整域である為の条件は $p \in 4\mathbb{Z}+3$ である. □

【問題】 k を体，$A=k[X,Y,Z]/(X-Y^2-Z^3)$ とする．

(1) (Y,Z) が A の極大イデアルであることを示せ．
(2) (X) が A の素イデアルであることを示せ．
(3) $(X-Y^2)$ が A の素イデアルではないことを示せ．

(H17 千葉大学理学研究科 数学専攻)

【解答】 $x=X+(X-Y^2-Z^3)$, $y=Y+(X-Y^2-Z^3)$, $z=Z+(X-Y^2-Z^3)$ と置く．$x=X+(X-Y^2-Z^3)=Y^2+Z^3+(X-Y^2-Z^3)=y^2+z^3$ と表されるから，A の任意の元は y,z の多項式として表される．$f(Y,Z)=\sum_{i,j\geq 0}a_{ij}Y^iZ^j$ $(a_{ij}\in k)$ に対し $f(Y,Z)\in(X-Y^2-Z^3)$ だとすると $f(Y,Z)=(X-Y^2-Z^3)g(X,Y,Z)$ $(g(X,Y,Z)\in k[X,Y,Z])$ と表される．$g(X,Y,Z)=\sum_{i=0}^n g_i(Y,Z)X^i$ とするとき

$$f(Y,Z)=g_n(Y,Z)X^{n+1}+\sum_{i=1}^n(g_{i-1}(Y,Z)-(Y^2+Z^3)g_i(Y,Z))X^i-(Y^2+Z^3)g_0(Y,Z)$$

となるから，X^i の係数を比較すれば

$$g_n(Y,Z)=0,\qquad g_{i-1}(Y,Z)=(Y^2+Z^3)g_i(Y,Z)\quad(i=1,\cdots,n),\qquad f(Y,Z)=-(Y^2+Z^3)g_0(Y,Z)$$

より $f(Y,Z)=0$ となる．従って $k[Y,Z]\ni f(Y,Z)\mapsto f(y,z)\in A$ は同型となる．

(1) $\varphi:A\to k$, $\varphi_1(f)=a_{00}$ $(f=\sum_{i,j\geq 0}a_{ij}y^iz^j\in A\ (a_{ij}\in k))$ とすれば φ は全射であり，$yA+zA\subset\operatorname{Ker}\varphi$ が成立．一方，$f\in\operatorname{Ker}\varphi$ だとすると

$$f=y\sum_{i>0}a_{i0}y^{i-1}+z\sum_{i\geq 0,j>0}a_{ij}y^iz^{j-1}\in yA+zA$$

だから $\operatorname{Ker}\varphi\subset yA+zA$．従って $A/(yA+zA)\simeq k$，即ち $yA+zA$ は A の極大 ideal となる．
(2) $y^{2i}+(y^2+z^3)A=(-z^3)^i+(y^2+z^3)A$ より一般の $f(y,z)\in A$ に対し $f(y,z)-f_0(z)-f_1(z)y\in(y^2+z^3)A$ となる $f_0(z),f_1(z)$ が存在する．$f(y,z)\in(y^2+z^3)A$ だとすると A に於いて $f_0(z)+f_1(z)y=(y^2+z^3)g(y,z)$ と表される．$g(y,z)=\sum_{i=0}^n g_i(z)y^i$ とするとき

$$f_0(z)+f_1(z)y=z^3g_0(z)+z^3g_1(z)y+\sum_{i=2}^n(g_{i-2}(z)+z^3g_i)(z)y^i+g_{n-1}(z)y^{n+1}+g_n(z)y^{n+2}$$

より $g_n(z)=g_{n-1}(z)=0$, $g_{i-2}(z)=-z^3g_i$ $(i=2,\cdots,n)$ となり，従って $f_0(z)=z^3g_0(z)=0$, $f_1(z)=z^3g_1(z)=0$ となる．

今，$f(z)=f_0(z)+f_1(z)y$, $g(z)=g_0(z)+g_1(z)y\in A$ に対し

$$\begin{aligned}f(z)g(z)+(y^2+z^3)A&=f_0(z)g_0(z)+f_1(z)g_0(z)y+f_0(z)g_1(z)y+f_1(z)g_1(z)y^2+(y^2+z^3)A\\&=f_0(z)g_0(z)-f_1(z)g_1(z)z^3+(f_1(z)g_0(z)+f_0(z)g_1(z))y+(y^2+z^3)A\end{aligned}$$

より，$f(z)g(z)\in(y^2+z^3)A$ ならば $f_0(z)g_0(z)-f_1(z)g_1(z)z^3=f_1(z)g_0(z)+f_0(z)g_1(z)=0$ となる．

$$\begin{aligned}f_0(z)(f_0(z)g_0(z)-z^3f_1(z)g_1(z))&=f_0(z)^2g_0(z)+z^3f_1(z)^2g_0(z)=(f_0(z)^2+z^3f_1(z)^2)g_0(z)=0\\f_1(z)(f_0(z)g_0(z)-z^3f_1(z)g_1(z))&=-f_0(z)^2g_1(z)-z^3f_1(z)^2g_1(z)=-(f_0(z)^2+z^3f_1(z)^2)g_1(z)=0\end{aligned}$$

より $g(z)\neq 0$ ならば $f_0(z)^2=-z^3f_1(z)^2$ となり，この等式の次数を比較すれば $f_0(z)=f_1(z)=0$ となる．よって $f(z)g(z)\in(y^2+z^3)A$, $g(z)\notin(y^2+z^3)A$ ならば $f(z)\in(y^2+z^3)A$ となるから，$(y^2+z^3)A$ は素イデアルである．

(3) $(x-y^2)A=z^3A$ である事に注意する．一般の $f(y,z)\in A$ に対し $f(y,z)-f_0(y)-f_1(y)z-f_1(y)z^2\in z^3A$ となる $f_0(y),f_1(y),f_2(y)$ が存在する．$f(y,z)\in z^3A$ だとすると A に於いて $f_0(y)+f_1(y)z+f_1(y)z^2=z^3g(y,z)$ と表されるが，両辺の z に関する次数を比較すれば $f_0(z)=f_1(z)=f_2(z)=0$ となる．ここで $f(y,z)=z$, $g(y,z)=z^2$ とすれば $f(y,z),g(y,z)\notin z^3A$ だが，$f(y,z)g(y,z)\in z^3A$ となるから $(x-y^2)A$ は素イデアルではない． $\square$

【問題】 実数体 $\mathbb{R}$ 上の 2 次行列環 $M_2(\mathbb{R})$ の部分集合 A を以下で定める．

$$A = \left\{ \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \middle| \ r, s \in \mathbb{R} \right\}$$

以下の問に答えよ．

(1) A は $M_2(\mathbb{R})$ の部分環であることを証明せよ．
(2) $\mathbb{R}$ 上 1 変数多項式環 $\mathbb{R}[X]$ から A への写像 ϕ を以下で定める．

$$\phi : \mathbb{R}[X] \to A, \qquad r_0 + r_1 X + \cdots + r_n X^n \ \mapsto \ \begin{pmatrix} r_0 & r_1 \\ 0 & r_0 \end{pmatrix}$$

$r_i \in \mathbb{R}$．このとき ϕ は環の準同型かつ全射であることを証明せよ．
(3) (2) での ϕ に対して，$\mathrm{Ker}\ \phi = (X^2)$ であることを証明せよ．
(4) A のイデアルをすべて求めよ．

(H16 千葉大学理学研究科 数学専攻)

【解答】 (1) $B_i = \begin{pmatrix} r_i & s_i \\ 0 & r_i \end{pmatrix} \in A \ \ (i = 1, 2)$ に対し

$$B_1 \pm B_2 = \begin{pmatrix} r_1 \pm r_2 & s_1 \pm s_2 \\ 0 & r_1 \pm r_2 \end{pmatrix}, \qquad B_1 B_2 = \begin{pmatrix} r_1 r_2 & r_1 s_2 + s_1 r_2 \\ 0 & r_1 r_2 \end{pmatrix} \in A$$

であり，さらに $E_2 \in A$ (E_2 は 2 次単位行列) となるから，A は $M_2(\mathbb{R})$ の部分環である．

(2) $f_i = r_{i0} + r_{i1} X + \cdots + r_{in} X^n \in \mathbb{R}[X] \ \ (i = 1, 2)$ とする．加法について

$$\begin{aligned} \phi(f_1 + f_2) &= \phi\left(\sum_{j=0}^{n} (r_{1j} + r_{2j}) X^j \right) = \begin{pmatrix} r_{10} + r_{20} & r_{11} + r_{21} \\ 0 & r_{10} + r_{20} \end{pmatrix} \\ &= \begin{pmatrix} r_{10} & r_{11} \\ 0 & r_{10} \end{pmatrix} + \begin{pmatrix} r_{20} & r_{21} \\ 0 & r_{20} \end{pmatrix} = \phi\left(\sum_{j=0}^{n} r_{1j} X^j \right) + \phi\left(\sum_{j=0}^{n} r_{2j} X^j \right) \end{aligned}$$

より $\phi(f_1 + f_2) = \phi(f_1) + \phi(f_2)$．一方，積について

$$f_1 f_2 = \left(\sum_{j=0}^{n} r_{1j} X^j \right) \left(\sum_{\ell=0}^{n} r_{1\ell} X^\ell \right) = \sum_{j,\ell=0}^{n} (r_{1j} r_{2\ell}) X^{j+\ell} = r_{10} r_{20} + (r_{10} r_{21} + r_{11} r_{20}) X + \sum_{i=2}^{2n} \sum_{j+\ell=i} (r_{1j} r_{2\ell}) X^i$$

だから，

$$\phi(f_1 f_2) = \begin{pmatrix} r_{10} r_{20} & r_{10} r_{21} + r_{11} r_{20} \\ 0 & r_{10} r_{20} \end{pmatrix} = \begin{pmatrix} r_{10} & r_{11} \\ 0 & r_{10} \end{pmatrix} \begin{pmatrix} r_{20} & r_{21} \\ 0 & r_{20} \end{pmatrix} = \phi\left(\sum_{j=0}^{n} r_{1j} X^j \right) \phi\left(\sum_{j=0}^{n} r_{2j} X^j \right)$$

より $\phi(f_1 f_2) = \phi(f_1)\phi(f_2)$ となる．また $\phi(1) = E_2$ である事が容易に分かる．以上より ϕ は $\mathbb{R}[X]$ から A への (単位元を単位元に写す) 環の準同型である事が確かめられた．

(3) $f = r_0 + r_1 X + \cdots + r_n X^n \in \mathbb{R}[X]$ に対し

$$\phi(f) = \begin{pmatrix} r_0 & r_1 \\ 0 & r_0 \end{pmatrix} = O \quad \Leftrightarrow \quad r_0 = r_1 = 0 \quad \Leftrightarrow \quad f \in (X^2)$$

だから，$\mathrm{Ker}\ \phi = (X^2)$．

(4) (2)(3)，及び準同型定理より A は単位的環として $\mathbb{R}[X]/(X^2)$ と同型となる．$\mathbb{R}[X]/(X^2)$ のイデアルは $\mathbb{R}[X]$ の (X^2) を含む (単項) イデアル (f) ($f \in \mathbb{R}[X]$ は単多項式) によって $(f)/(X^2)$ と表される．このとき $f \mid X^2$ より f は $1, X, X^2$，従って $\mathbb{R}[X]/(X^2)$ のイデアルは $\mathbb{R}[X]/(X^2)$, $(X)/(X^2)$, 0 の何れかとなる．この結果を A に還元すれば，A のイデアルは以下の 3 種類である：

$$A, \qquad \left\{ \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} \middle| \ s \in \mathbb{R} \right\}, \qquad O.$$

□

【問題】 R は可換環で L, M は R 加群とし，L から M への R 準同型写像からなる R 加群を $\mathrm{Hom}_R(L, M)$ で表す．$a \in R$ は M 上の非零因子 $(0 \neq x$ ならば $ax \neq 0)$ とする．

(1) a は $\mathrm{Hom}_R(L, M)$ 上の非零因子でもあることを示せ．

(2) さらに $b \in R$ は剰余加群 M/aM 上の非零因子とせよ．但し $aM = \{ax \mid x \in M\}$ である．$N = \mathrm{Hom}_R(L, M)$ とおくと b は N/aN 上の非零因子でもあることを示せ．

(H15 千葉大学理学研究科 数学専攻)

【解答】 (1) $af = 0$ だとする．このとき任意の $x \in L$ に対し $af(x) = 0$ となる．a は M の非零因子だから $f(x) = 0$，従って $f = 0$ となる．故に a は $\mathrm{Hom}_R(L, M)$ の非零因子である．

(2) $f \in N$ に対し $bf \in aN$，即ち $bf = ag$ となる $g \in N$ が存在したとする．このとき任意の $x \in L$ に対し $bf(x) = ag(x) \in aM$ となるから，b が M/aM の非零因子であることより $f(x) \in aM$，即ち，$f(x) = ah(x)$ $(h(x) \in M)$ と表される．a は非零因子だから，$h(x)$ は $f(x)$ に対し一意に決まる．ここで $x, y \in L$，$r, s \in R$ とすると

$$ah(rx + sy) = f(rx + sy) = rf(x) + sf(y) = rah(x) + sah(y) = a(rh(x) + sh(y))$$

より $h(rx + sy) = rh(x) + sh(y)$，従って $h \in N$ となる．これより $bf \in aN$ ならば $f = ah \in aN$ となる事から，b は N/aN 上の非零因子となる． $\square$