目次

0.1 H6 数学選択

[3] (1)E_1 上で $0 < f(x) < 1$ であるから，$f(x)^n > f(x)^{n+1}$ である．よって $f(x)^{\frac{1}{n+1}} > f(x)^{\frac{1}{n}}$ となるから $\{f(x)^{\frac{1}{n}}\}_{n=1}^{\infty}$ は単調増加．また $\lim_{n\to\infty} f(x)^{\frac{1}{n}} = 1$ である．よって単調収束定理から $\lim_{n\to\infty}\int_{E_1} f(x)^{\frac{1}{n}}dx = \int_{E_1}\lim_{n\to\infty} f(x)^{\frac{1}{n}}dx = \int_{E_1} 1dx = \mu(E_1)$ となる．

(2)E_2 上で $1 \leq f(x)$ であるから, $f(x) \leq f(x)^n$ より $f(x)^{\frac{1}{n}} \leq f(x)$ となる．また $\lim_{n\to\infty} f(x)^{\frac{1}{n}} = 1$ である．$f(x)$ は E_2 上可積分であるから, ルベーグの収束定理より $\lim_{n\to\infty}\int_{E_2} f(x)^{\frac{1}{n}}dx = \int_{E_2}\lim_{n\to\infty} f(x)^{\frac{1}{n}}dx = \int_{E_2} 1dx = \mu(E_2)$ となる．

(3)$\mathbb{R}$ 上可積分であるから，E_2 上可積分である．また $E_1 \cap E_2 = \emptyset$ であるから，$\mu(E_1 \cup E_2) = \mu(E_1) + \mu(E_2) = \lim_{n\to\infty}\int_{E_1\cup E_2} f(x)^{\frac{1}{n}}dx = \lim_{n\to\infty}\int_{\mathbb{R}} f(x)^{\frac{1}{n}}dx$ となる．

[4] (1)0 が M の内点でないことを示す．内点ならば ε 近傍 $B(0,\varepsilon)$ がとれる．X の基底の各ベクトル v について $\varepsilon\frac{v}{2\|v\|}$ とすることで，$B(0,\varepsilon)$ の部分集合で X の基底となるものが存在すると分かる．これは $M \neq X$ に矛盾．よって 0 は内点でない.

任意の $v \in M$ について v が内点ならば，v の ε 近傍 $B(v,\varepsilon)$ が存在する．$B(v,\varepsilon) - v = \varepsilon B(0,\varepsilon) \subset M$ となり，0 も内点である．これは矛盾.

(2)X を $L^1([0,1])$ とする．これは Banach 空間である．

$L^\infty([0,1])$ は $L^1([0,1])$ の無限次元の部分空間である．$\frac{1}{x} \in L^1([0,1])$ であるが，$\frac{1}{x} \notin L^\infty([0,1])$ である．したがって真部分空間である．また完備であるから閉集合である．これが (i) の例.

$C^0([0,1])$ を $[0,1]$ 上の連続関数全体とすればこれは，無限次元の部分空間である．$\{x^n\}$ は X の収束列であり，$C^0([0,1])$ の数列であるが，極限は $f(x) = \begin{cases} 0 & (0 \leq x < 1) \\ 1 & (x = 1) \end{cases}$ であり，$C^0([0,1])$ には属さない．これが (ii) の例.

(3) すべての F_n が内点をもたないとする．$x_1 \in X \setminus F_1$ を任意にとる．このとき開集合であるから

$\mathrm{Cl}(B(x_1,\delta_1)) \subset X\backslash F_1$ となる δ_1 をとれる．(Cl で閉包をあらわす．)$x_1 \in F_a$ となる a が存在する．$a=2$ としても一般性を失わない．$x_1 \in F_2$ であるが，F_2 は内点をもたないため，$B(x_1,\delta_1)\cap X\setminus F_2 \neq \emptyset$ である．よって $x_2 \in B(x_1,\delta_1)\cap X\setminus F_2$ となる x_2 がとれる．$0<\delta_2<\frac{\delta_1-d(x_1,x_2)}{2}$ をみたし，$\mathrm{Cl}(B(x_2,\delta_2)) \subset X\setminus F_2$ となる δ_2 がとれる．δ_2 の定め方から，$B(x_2,\delta_2)\subset B(x_1,\delta_1)$ である．これを繰り返して点列 $\{x_n\}$ と数列 $\{\delta_n\}$ を得る．$n\geq m$ に対して $\|x_n-x_m\|\leq \delta_m \leq \frac{\delta_1}{2^m}\to 0 \quad (m,n\to\infty)$ であるから $\{x_n\}$ は Cauchy 列である．X は完備であるから $\{x_n\}$ は収束する．$x_*=\lim_{n\to\infty} x_n$ とする．$x_*\in F_N$ なる N が存在する．$\mathrm{Cl}(B(x_N,\delta_N))\subset X\setminus F_N$ であり，$\{x_n\}_{n=N}^{\infty}$ は閉集合 $\mathrm{Cl}(B(x_N,\delta_N))$ の収束点列であるから，$x_*\in \mathrm{Cl}(B(x_N,\delta_N))\subset X\setminus F_N$ となる．これは矛盾．

6 (1) 斉次式であることから可約であれば，$x^2+xy+y^2=(x-ay)(x-by) \quad (a,b\in F)$ とできる．$x^2+xy+y^2=x^2-(a+b)xy+abx^2$ となるから，$a+b=-1, ab=1$ より $a^2+a+1=0$ をみたす．また $b=a^2$ である．よって可約であれば $x^2+xy+y^2=(x-\varepsilon y)(x-\varepsilon^2 y)$ となる ε が存在して $\varepsilon^2+\varepsilon+1=0$ を満たす．

逆に $\varepsilon^2+\varepsilon+1=0$ をみたす $\varepsilon\in F$ が存在すれば，可約である．

$\mathrm{ch}F\neq 3$ のとき．$\varepsilon\neq 1$ である．$\varphi\colon F^2\to F^2;(x,y)\mapsto(x-\varepsilon y, x-\varepsilon^2 y)$ とする．φ は加法群として準同型である．$x-\varepsilon y=0=x-\varepsilon^2 y$ となるとき，$\varepsilon\neq 1$ より $y=0, x=0$ となる．よって φ は単射であるから，全単射である．任意の $a\in F^\times$ に対して $uv=a$ なら $u=av^{-1}$ である．したがって $uv=a$ となる (u,v) の組は $|F|-1$ 個である．$a=0$ なら $u=0$ または $v=0$ であるから $2|F|-1$ 個である．φ が全単射であるから，これが求める解の個数．

$\mathrm{ch}F=3$ のとき．$\varepsilon=1$ より $x^2+xy+y^2=(x-y)^2=a$ である．よって $a=0$ なら解は $\{(x,x)\in F^2 \mid x\in F\}$ より $|F|$ 個である．$a\neq 0$ なら二乗して a になる数が存在するとき，$\mathrm{ch}F\neq 2$ より解は 2 個あるから $2|F|$ 個である．存在しないなら 0 個である．

(2)F の位数を q とする．既約であるから $\mathrm{ch}F\neq 3$ である．すなわち $3\nmid q$ である．また $3\mid q-1$ なら乗法群は巡回群であるから，位数 3 の元 ε が存在する．このとき $\varepsilon^3-1=0$ であり，$\varepsilon\neq 1$ であるから $\varepsilon^2+\varepsilon+1=0$ である．これは既約性に矛盾．よって $3\nmid q-1$ である．

$a=0$ のとき．解 $(x,y)\neq(0,0)$ を持つと仮定する．対称性から $y\neq 0$ としてよい．$x=\varepsilon y$ を満たす $\varepsilon\in F$ が存在する．このとき $\varepsilon^2+\varepsilon+1=0$ となり，既約性に矛盾．したがって解は 1 個である．

$a\neq 0$ のとき，$\varepsilon^2+\varepsilon+1$ をみたす ε を F に添加した拡大体 $K:=F(\varepsilon)$ を考える．$\varepsilon^q=\varepsilon^2$ である．K は F 上の 2 次元ベクトル空間であるから，任意の $z\in K$ は $z=\alpha-\varepsilon\beta \quad (\alpha,\beta\in F)$ と一意にあらわせる．$z^{q+1}=zz^q=(\alpha-\varepsilon\beta)(\alpha-\varepsilon^2\beta)=\alpha^2+\alpha\beta+\beta^2$ である．したがって $\phi\colon K^\times\to F^\times; z\mapsto z^{q+1}$ は群準同型である．$K^\times=\langle g\rangle$ となる g が存在する．$z\in ker\phi$ について $g^k=z$ なる k が存在する．$(g^k)^{q+1}=1$ より $(q^2-1)\mid k(q+1)$ である．これをみたす $0\leq k<q^2-1$ は $0, q-1, 2(q-1), \cdots, q(q-1)$ の $q+1$ 個である．したがって $|ker\phi|=q+1$ である．よって $|\mathrm{Im}\,\phi|=|q^2-1|/|\ker\phi|=q-1=|F^\times|$ である．よって ϕ は全射である．以上より $0\neq a\in F$ に対して $\phi^{-1}(a)\ni z=\alpha+\beta\varepsilon$ とすれば，$\alpha^2+\alpha\beta+\beta^2=a$ であり，$K^\times$ の元は $F^2\setminus\{(0,0)\}$ と一対一対応するから，解の個数は $q+1$ である．

(3) 単射にならない a を考える．$f(x)=f(y)$ かつ $x\neq y$ とする．$x^3+ax=y^3+ay$ より $(x-y)(x^2+xy+y^2)=-a(x-y)$ であるから $x^2+xy+y^2=-a$ である．

$3\mid(q+1)$ のとき，すなわち x^2+xy+y^2 が既約なとき，$a\neq 0$ なら $x^2+xy+y^2=-a$ を満たす (x,y) は $q+1$ 個あるから，$x\neq y$ となる解も存在する．よって単射でない．$a=0$ なら解は $(0,0)$ のみであるから単射．

$3\mid q$ のとき，(1) から $a=0$ あるいは二乗して $-a$ になる数が存在しないときに単射，それ以外は単射でない．

$3\mid(q-1)$ のとき，$a=0$ なら単射でない．$a\neq 0$ で単射な a が存在すると仮定する．解の個数が $q-1$ であり，$(0,0)$ は解でないから解は $(x,x) \quad (x\in F^\times)$ である．すなわち $x^2+x^2+x^2=-a$ より $x^2=-3^{-1}a \quad (x\in F^\times)$ である．二次方程式であるから解は重複を含めて 2 個．よって $q-1=|F^\times|\leq 2$ であ

る．$3 \mid (q-1)$ よりこれを満たす $q \geq 2$ は存在しない．したがって $a \neq 0$ なら単射でない．

7 帰納法でとく．$n=1$ は明らか．$n-1$ 以下で成立すると仮定する．H_{n-1} を $n-1$ 次正方行列ですべての主小行列式が非零な行列な行列とする．下三角行列 P_{n-1} と上三角行列 Q_{n-1} を用いて $H_{n-1} = P_{n-1}Q_{n-1}$ とできる．$0 \neq \det H_{n-1} = \det P_{n-1} \det Q_{n-1}$ であるから，$\det P_{n-1} \neq 0, \det Q_{n-1} \neq 0$ である．

$$H_n = \begin{pmatrix} H_{n-1} & a \\ b^T & c \end{pmatrix} = \begin{pmatrix} P_{n-1} & 0 \\ b^T Q_{n-1}^{-1} & 1 \end{pmatrix} \begin{pmatrix} Q_{n-1} & P_{n-1}^{-1}a \\ 0 & c - b^T Q_{n-1}^{-1} P_{n-1}^{-1} a \end{pmatrix} = P_n Q_n$$

とすれば，P_n は下三角行列であり，Q_n は上三角行列である．

0.2 H7 数学選択

4 (1) 距離空間においてコンパクト性と点列コンパクト性は同値である．点列 $\{\alpha_{n,k}\}_{k=1}^{\infty}; \alpha_{n,k} := \delta_{n,k}$ は $\{\alpha_{n,k}\}_{k=1}^{\infty} \in B$ である．B の点列 $\{\alpha_n\}_{n=1}^{\infty}$ を $\alpha_n := \{\alpha_{n,k}\}_{k=1}^{\infty}$ とすると，$\{\alpha_n\}_{n=1}^{\infty}$ は収束部分列を持たない．(任意の異なる二項の差が 1 以上であるためコーシー列にならない．) よって B は点列コンパクトでない．

(2)$1 - \|x\|$ の連続性は明らか．$(\sum \frac{\zeta_k}{k})^2 \leq \sum \zeta_k^2 \sum \frac{1}{k^2}$(コーシーシュワルツ) より収束性と連続性がわかる．よって f は連続で $f(\alpha_n) = \frac{1}{n}$ より $\inf_{x \in B} f(x) = 0$ である．

$\min_{x \in B} f(x)$ が存在すれば，$\|x\| = 1, \sum \frac{\zeta_k}{k} = 0$ だがこれを満たす x は存在しない．

6 (1)$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ より galois 群の非自明な部分群はただ一つ．よって非自明な中間体もただ一つである．

(2)$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{id}, \sigma, \sigma^2, \sigma^3$ とする．$\sigma^2((\sqrt{\alpha})^2) = \sigma^2(\alpha) = \alpha$ より $\sigma^2(\sqrt{\alpha}) = -\sqrt{\alpha}$ である．同様に $\sigma^2(\sqrt{\beta}) = -\sqrt{\beta}$ である．よって $\sigma^2(\sqrt{\alpha\beta}) = (-\sqrt{\alpha})(-\sqrt{\beta}) = \sqrt{\alpha\beta}$ である．すなわち $\sqrt{\alpha\beta} \in F$ であるから $\alpha\beta$ は F の平方数.

(3)K/F は二次拡大であるから $K = F(\sqrt{x + y\sqrt{a}})$ $(x, y \in \mathbb{Q})$ と書ける．$K/\mathbb{Q}$ が galois 拡大であることから，$\sqrt{x + y\sqrt{a}}$ の $\mathbb{Q}$ 上の共役 $\sqrt{(x - y\sqrt{a})} \in K$ である．また $K = F(\sqrt{x - y\sqrt{a}})$ であるから (2) より $x^2 - y^2 a = (c + d\sqrt{a})^2$ となる $c, d \in \mathbb{Q}$ が存在する．$x^2 - y^2 a = c^2 + d^2 a + 2cd\sqrt{a}$ より $cd = 0$ である．$\sqrt{x + y\sqrt{a}}$ の $\mathbb{Q}$ 上の共役は $\pm\sqrt{x \pm y\sqrt{a}}$ である．$\sigma(\sqrt{x + y\sqrt{a}}) = -\sqrt{x + y\sqrt{a}}$ なら $\sqrt{x + y\sqrt{a}} \in F$ となるから，$\sigma(\sqrt{x + y\sqrt{a}}) = \sqrt{x - y\sqrt{a}}$ としてよい．(σ と σ^3 の対称性) このとき，$-\sqrt{x + y\sqrt{a}} = \sigma^2(\sqrt{x + y\sqrt{a}}) = \sigma(\sqrt{x - y\sqrt{a}}) = \sigma(\frac{\sqrt{x^2 - y^2 a}}{\sqrt{x + y\sqrt{a}}})$ より $\sigma(\sqrt{x^2 - y^2 a}) = -\sqrt{x + y\sqrt{a}}\sigma(\sqrt{x + y\sqrt{a}}) = -\sqrt{x^2 - y^2 a}$ となるから $\sqrt{x^2 - y^2 a} \notin \mathbb{Q}$ である．

よって $c = 0$ であるから $x^2 - y^2 a = d^2 a$ である．よって $a = \left(\frac{xd}{d^2 + y^2}\right)^2 + \left(\frac{xy}{d^2 + y^2}\right)^2$ である．

7 (1)

> $x^2 + y^2 - 1$ の既約性を示せばよいが，やや面倒．そこで UFD 上の原始多項式の既約性はその商体上の既約性と同値であることを使う．

$x^2 + y^2 - 1$ が $K(y)[x]$ 上で既約であれば，$K[x, y]$ 上でも既約である．$x^2 + y^2 - 1$ が $K(y)[x]$ 可約なら $K(y)$ に根 $f(y)/g(y)$ $(f(y), g(y) \in K[y])$ をもつ．また $\mathrm{ch}K \neq 2$ より $y - 1 \neq y + 1$ である．このとき $f(y)^2 = (1 - y^2)g(y)^2$ であるが，$K[y]$ の等式とみたときに素元 $1 - y$ の個数が右辺と左辺で異なるため矛盾．よって可約でないから既約である．よって $K[x, y]$ は UFD だから $x^2 + y^2 - 1$ は素元であり $(x^2 + y^2 - 1)$ は素イデアル，よって $R = K[x, y]/(x^2 + y^2 - 1)$ は整域.

(2)x が既約であるが素元でないことを示す．x が素元 $\Leftrightarrow R/(x)$ は整域．ここで $R/(x) \cong K[y][x]/(x, x^2 + y^2 - 1) \cong K[y]/(y^2 - 1)$ である．$y^2 - 1 = (y - 1)(y + 1)$ より $y^2 - 1$ は既約でないから $R/(x)$ は整域でない．よって x は素元でない．

$f(x,y)+I \in R$ について，$f(x,y) = (x^2+y^2-1)h(x,y)+ya(x)+b(x)$ となる $a(x),b(x) \in K[x]$ が存在する．$f(x,y)+I = g(x,y)+I$ なら $g(x,y)-f(x,y) = (x^2+y^2-1)p(x)$ となる $p(x) \in K[x]$ が存在して，$g(x,y) = (x^2+y^2-1)(h(x,y)+p(x))+ya(x)+b(x)$ となる．よって $a(x),b(x)$ は R の各元に対して一意に定まる．ノルム $N\colon R \to K[x]$ を $N(a(x)+b(x)y+I) = a(x)^2-b(x)^2(1-x^2)$ とする．

$$N((a(x)+b(x)y+I)(c(x)+d(x)y+I)) = N(ac(x)+bd(x)(1-x^2)+(ad+bc)(x)y+I)$$
$$=(ac(x)+bd(x)(1-x^2))^2-(ad+bc)^2(1-x^2) = (a(x)^2-b(x)^2(1-x^2))(c(x)^2-d(x)^2(1-x^2)) = N(a(x)+b(x)y+I)N(c($$

よって $N((f(x,y)+I)(g(x,y)+I)) = N(f(x,y)+I)N(g(x,y)+I)$ である．

有限次拡大 E/F に対して $m_a\colon E \to E$ が m 倍写像として定まる．E の F 上基底 S を一つ固定して S に関する表現行列の行列式が a のノルムである．(青雪江 4.12 節)
整域 R に対してその商体 P を考えれば α を添加した環 $R(\alpha)$ のノルムを $P(\alpha)/P$ のノルムの制限として考えられる．
上の観察から R は $K[x]$ に y を添加した環だと思える．($\mathbb{Z}$ に $\sqrt{2}$ を添加するのと同じノリ)
そこで R 上のノルムは $K[x]$ の商体 $K(x)$ 上のノルムを考えればよい．R の $K(x)$ 上の基底は $\{1,y\}$ であるから f 倍写像では $m_f(1) = a+by, m_f(y) = (1-x^2)b+ay$ である．行列式は $\begin{vmatrix} a & (1-x^2)b \\ b & a \end{vmatrix} = a^2-b^2(1-x^2)$ である．これがノルム．
以上を認めれば $N(fg) = N(f)N(g)$ が成り立つことは明らか．

$x+I = (a(x)+b(x)y+I)(c(x)+d(x)y+I)$ とする．$N(x+I) = x^2$ より，次の 2 つ場合がある．

(i)$N(a(x)+b(x)y+I) = a(x)^2-b(x)^2(1-x^2) = \pm x, N(c(x)+d(x)y+I) = c(x)^2-d(x)^2(1-x^2) = \pm x$(複号同順)

(ii)$N(a(x)+b(x)y+I) = a(x)^2-b(x)^2(1-x^2) = \pm 1, N(c(x)+d(x)y+I) = c(x)^2-d(x)^2(1-x^2) = \pm x^2$(複号同順)

(i) のとき，x の次数が左辺は偶数で右辺は奇数だから矛盾．(ii) のとき，$(a(x)+b(x)y+I)(a(x)-b(y)+I) = a(x)^2-b(x)^2(1-x^2)+I = \pm 1+I$ より $a(x)+b(x)y+I$ は単元．よって x は既約元である．

よって R は UFD でない．

(3) 全射環準同型 $\varphi\colon K[x,y] \to K[u,v]/(uv-1); x \mapsto \frac{u+v}{2}, y \mapsto \frac{u-v}{2\sqrt{-1}}$ を考える．$\ker\varphi = ((x+\sqrt{-1}y)(x-\sqrt{-1}y)-1) = (x^2+y^2-1)$ である．よって $R \cong K[u,v]/(uv-1)$ である．$uv-1 = 0 \in K[u,v]/(uv-1)$ より $uv = 1$ すなわち，$v = u^{-1}$ である．よって $R \cong K[u,u^{-1}]$ である．$K[u,u^{-1}]$ は $K[u]$ の $\{u^n \mid n = 0,1,2,\dots\}$ による局所化である．$K[u]$ は UFD であるからその局所化もまた UFD である．よって R は UFD である．

0.3 H8 数学選択

6

群 G と $N \triangleleft G, H \leq G$ について $NH = G, H \cap N = \{e\}$ ならば半直積 $N \rtimes H \cong G$ である．

$$N = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}, H = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^2 \right\} \text{とする．}$$

$\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & n\\ 0 & 1\end{pmatrix}$ より $NH=G$ でありまた $H\cap N=\{e\}$ である．よって $N\rtimes H\cong G$ である．

$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ は位数無限であり，$\begin{pmatrix}-1 & b\\ 0 & 1\end{pmatrix}$ は位数 2 である．

$\varphi\in \mathrm{Aut}(G)$ を任意にとる．$\varphi\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$ は位数が無限であるから $\varphi\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ となる．

同様に $\varphi\left(\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}-1 & b\\ 0 & 1\end{pmatrix}$ となる．$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^n=\begin{pmatrix}1 & an\\ 0 & 1\end{pmatrix}$ である．よって φ の全射性から $a=\pm1$ である．逆に $a=\pm1, b\in\mathbb{Z}$ が定まれば同型写像 φ が一意に定まる．半直積 $\mathbb{Z}\rtimes_f \mathbb{Z}/2\mathbb{Z}$ を $f(i)=(n\mapsto(-1)^i n)$ で定める．このとき $\mathrm{Aut}(G)\to\mathbb{Z}\rtimes_f\mathbb{Z}/2\mathbb{Z}; \varphi\mapsto(b,a)$ は全単射である．$\phi\mapsto(d,c)$ に対して $\varphi\circ\phi\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)=\varphi\left(\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & ac\\ 0 & 1\end{pmatrix}, \varphi\circ\phi\left(\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\right)=\varphi\left(\begin{pmatrix}-1 & d\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}-1 & b+ad\\ 0 & 1\end{pmatrix}$ より $\varphi\circ\phi\mapsto(b+ad,ac)=(b+(-1)^a d,ac)=(b,a)\cdot(d,c)$ となるから $\mathrm{Aut}(G)\to\mathbb{Z}\rtimes_f\mathbb{Z}/2\mathbb{Z}$ は同型射．

7 (1)$f(x^2)=f(x)g(x)$ なる $g(x)\in\mathbb{Q}[x]$ が存在する．f の根 α に対して $f(\alpha^2)=f(\alpha)g(\alpha)=0$ より α^2 も f の根である．f が n 次多項式であるから，異なる根は高々 n 個である．よって $\alpha^{2^m}=\alpha^{2^k}$ となる $m>k$ が存在する．このとき $\alpha^{2^m-2^k}=1$ となるから α は 1 の冪根である．

α が偶数位数の根であるとする．すなわち $\alpha^{2m}=1$ となる最小の正の整数 m が存在する．このとき $\alpha^m=-1$ となる．また $x^m-1=0$ は α^2 を根にもつ．f は α^2 の最小多項式であるから $x^m-1=f(x)h(x)$ となる $h(x)\in\mathbb{Q}[x]$ が存在する．α を代入すると $-2=\alpha^m-1=f(\alpha)h(\alpha)=0$ となり矛盾する．よって α は奇数位数の根である．

(2)f の根 α,β の位数を $s>t$ とする．$f(x)|(x^t-1)$ であるから $\alpha^t=1$ である．これは $s>t$ であることに矛盾する．よって f の根は全て位数が等しい．

f の根 α の位数が m であるとする．$f(-\alpha)=0$ なら $(-\alpha)^m=(-1)^m\alpha^m=(-1)^m=1$ となり m は偶数である．これは矛盾．

$f((-\alpha)^2)=f(\alpha^2)=f(\alpha)g(\alpha)=0$ であり，$f((-\alpha)^2)=f(-\alpha)g(-\alpha)=0$ であるから $g(-\alpha)=0$ である．g の次数は f と等しいから最高時の係数に注意すれば $g(x)=(-1)^n f(-x)$ である．

(3)f が奇数位数の冪根の最小多項式であるから f は円分多項式である．オイラーのトーシュエント関数を φ とすると，位数 m の 1 の冪根を解に持つ円分多項式の次数は $\varphi(m)$ である．

$\varphi(m)\le 6$ となる奇数 m を考える．$1,2,4,8,16,m-1,32$ は m と互いに素である．したがって $m\ge 34$ なら $\varphi(m)>6$ である．また $33\ge m\ge 18$ で $3,5,7$ のいずれも素因数にもつ数は存在しない．よって $m\ge 18$ なら $\varphi(m)>6$ である．$m=1,3,5,7,9$ なら $\varphi(m)\le 6$ であり，$m=11,13,15,17$ なら $\varphi(m)>6$ である．$m=1,3,5,7$ に対応する円分多項式は $x-1, x^2+x+1, x^4+x^3+x^2+x+1, x^6+x^5+x^4+x^3+x^2+x+1$ である．$m=9$ なら $(x^9-1)/(x^3-1)=x^6+x^3+1$ である．

この 5 つが求める $f(x)$ である．

0.4 H9 数学選択

6 (1)$p(t)=t^3-x^3\in L[t]$ が x の最小多項式であることを示す．$p(t)=(t-x)(t-e^{2\pi i/3}x)(t-e^{4\pi i/3}x)$ である．したがって $p(t)$ は L 上で既約なモニック多項式．

(2)$L(x)\ni x^{-1}(xy)=y$ より $K=L(x)$ である．$p(t)$ の根をすべて K は含むから K/L は正規拡大．よって K/L はガロア拡大で拡大次数は 3．すなわち $\mathrm{Gal}(K/L)\cong\mathbb{Z}/3\mathbb{Z}$.

(3)$M(x)\cdot M(y)=M(x,y)=K$ であり，$M(x)\cap M(y)=L$ である．$M(x)/M, M(y)/M$ は galois 拡大で

$\mathrm{Gal}(M(x)/M) \cong \mathrm{Gal}(M(y)/M) \cong \mathbb{Z}/3\mathbb{Z}$ である．galois 拡大の推進定理より $\mathrm{Gal}(K/M) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ である．

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ の非自明な部分群は $\langle(1,0)\rangle, \langle(1,1)\rangle, \langle(1,2)\rangle, \langle(0,1)\rangle$ である．$\sigma \in \mathrm{Gal}(M(x)/M)$ を $\sigma(x) = e^{2\pi i/3}x$ とし，$\tau \in \mathrm{Gal}(M(y)/M)$ を $\tau(y) = e^{2\pi i/3}y$ とする．(σ, id) で不変な K の元は y であるから $\langle(1,0)\rangle$ に対応する中間体は $M(y)$ である．同様にしてそれぞれ $M(xy^2), M(xy), M(x)$ が対応する．

以上より中間体は $M, M(x), M(y), M(xy), M(xy^2), K$ である．

8 (1) 位相空間 X が連結であるとは，X の空でない開集合 U, V で $U \cap V = \emptyset, U \cup V = X$ を満たすものが存在しないことである．

位相空間 X が弧状連結であるとは，X の任意の 2 点 x, y に対して連続写像 $\gamma : [0,1] \to X$ で $\gamma(0) = x, \gamma(1) = y$ を満たすものが存在することである．

(2)X を局所弧状連結であり連結である位相空間とする．連結性から $X \neq \emptyset$ である．$x, y \in X$ に対して, 連続写像 $\gamma : [0,1] \to X$ で $\gamma(0) = x, \gamma(1) = y$ を満たすものが存在するとき $x \sim y$ とかく．

$U = \{y \in X \mid x \sim y\}$ とする．$y \in U$ に対して弧状連結な開近傍 U_y が存在する．任意の $z \in U_y$ に対して $z \sim y \sim x$ であるから $z \in U$ である．よって $U_y \subset U$ である．すなわち U は開集合である．

$z \in X \setminus U$ とする．z に対して弧状連結な開近傍 U_z が存在する．$U_z \cap U \neq \emptyset$ であるとすると $y \in U_z \cap U$ が存在する．このとき $x \sim y \sim z$ であるから $z \in X \setminus U$ に矛盾する．よって $U_z \cap U = \emptyset$ である．z は任意であるから $X \setminus U$ は開集合である．よって U は開かつ閉である．X は連結であるから $U = X$ である．すなわち X は弧状連結である．

(3)M を連結な多様体とする．(2) より局所弧状連結であることを示せばよい．M の点 x に対して x を含む開集合 U と同相写像 $\varphi : U \to V \subset \mathbb{R}^n$ が存在する．$\varphi(x) \subset B(\varphi(x), \varepsilon) \subset V$ となる ε 開球が存在する．$x \in \varphi^{-1}(B(\varphi(x), \varepsilon))$ は x を含む弧状連結な開集合である．よって局所弧状連結.

0.5 H10 数学選択

6 L/K を有限次 galois 拡大とする．$L[x]$ で $f(x) = g_1(x) \dots g_n(x)$ と既約元分解されるとする．$f(x)$ の最小分解体を F で表す．$i \neq j$ として g_i の根 α,g_j の根 β を任意にとって固定する．既約であるから g_j は β の最小多項式と同伴である．$f(x)$ は K 上で既約であるから，$\sigma \in \mathrm{Gal}(F/K)$ で $\sigma(\alpha) = \beta$ となるものが存在する．$\sigma(g_i)(\beta) = \sigma(g_i(\alpha)) = 0$ であるから $\sigma(g_i)$ は β を根にもつ．L/K が正規拡大であるから $\sigma|_L$ は L 上の K-自己同型である．よって $\sigma(g_i)$ は $L[x]$ の既約多項式である．よって $\sigma(g_i)$ も β の最小多項式と同伴である．すなわち $\deg g_i = \deg \sigma(g_i) = \deg g_j$ である．

7 (1)(p, x^2+1) が $\mathbb{Z}[x]$ 上素イデアル $\Leftrightarrow \mathbb{Z}[x]/(p, x^2+1)$ が整域．$\Leftrightarrow (\mathbb{Z}[x]/(p))/((p, x^2+1)/(p))$ が整域．$\Leftrightarrow \mathbb{F}_p[x]/(x^2+1)$ が整域．$\Leftrightarrow x^2+1$ が $\mathbb{F}_p[x]$ 上既約．$\Leftrightarrow -1$ が $\mathbb{F}_p$ 上平方非剰余.

次が成り立つことを示す．-1 が $\mathbb{F}_p$ 上平方剰余 $\Leftrightarrow 4 \mid (p-1)$.

$\Rightarrow$ ある $x \in \mathbb{F}_p^\times$ が存在して $x^2 = -1$ となる．$x^4 = 1$ であるから x は位数 4 の元．よって $4 \mid (p-1)$.

$\Leftarrow 4 \mid |\mathbb{F}_p^\times|$ であるから sylow の定理より位数 4 以上の $2-$sylow 部分群が存在する．$x^2 = 1$ をみたす $x \in \mathbb{F}_p^\times$ は $x = \pm 1$ のみであるから $x^2 = -1$ をみたす x が存在する．

以上より (p, x^2+1) が $\mathbb{Z}[x]$ 上素イデアル $\Leftrightarrow 4 \nmid p-1$ である．

-1 が平方剰余でないについては平方剰余の相互法則の第一補充法則 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ から $\frac{p-1}{2}$ が奇数であることと同値である．これは $p-1$ が 4 の倍数でないことと同値である．

0.6 H11 数学選択

7 Galois 群が推移的なとき．$f(x)$ が可約であると仮定する．$f(x)=g_1(x)g_2(x)\dots g_n(x)$ と $K[x]$ 上で既約分解される．g_1 の根 α と g_2 の根 β を任意にとって固定する．$f(x)$ の最小分解体を F で表す．推移的であるから $\sigma\in \mathrm{Gal}(F/K)$ で $\sigma(\alpha)=\beta$ となるものが存在する．このとき $\sigma(g_1)(\beta)=\sigma(g_1(\alpha))=0$ であるから $\sigma(g_1)$ は β を根にもつ．よって $\sigma(g_1)$ と g_2 は共に β の最小多項式と同伴である．$g_1\in K[x]$ より $\sigma(g_1)=g_1$ であるから g_1 と g_2 は同伴である．このとき α は g_1,g_2 のどちらの根でもあるがこれは f の分離性に矛盾.

$f(x)$ が $K[x]$ 上で既約であるとき．$f(x)$ の 2 根 α,β をとって固定する．$\mathrm{Gal}(F/K)\alpha=\{\alpha_1,\dots,\alpha_n\}$ とする．$g(x)=\prod_{i=1}^n(x-\alpha_i)$ とする．このとき $\mathrm{Gal}(F/K)g(x)=g(x)$ より $g(x)\in K[x]$ である．$g(x)$ の根は α の共役であるから $g(x)\mid f(x)$ である．既約性から $cg(x)=f(x)\quad(c\in K)$ とできる．これは $\mathrm{Gal}(F/K)$ が推移的であることを意味する.

8 $(1)f(x,y)=\sum a_{ij}x^iy^j$ とできる．$f(tx,ty)=\sum a_{ij}t^{i+j}x^iy^j=t^nf(x,y)=\sum a_{ij}t^nx^iy^j$ である．$K(x,y)[t]$ における等式とみれば $\sum_{i+j=k}a_{ij}t^kx^iy^j=0,\quad(k\neq n)$ である．したがって $a_{ij}=0\quad(i+j\neq n)$ である．よって $f(x)=\sum_{i+j=n}a_{ij}x^iy^j$ である.

$x\frac{\partial f}{\partial x}+y\frac{\partial f}{\partial y}=x\sum_{i+j=n}a_{ij}ix^{i-1}y^j+y\sum_{i+j=n}a_{ij}jx^iy^{j-1}=\sum_{i+j=n}a_{ij}(i+j)x^iy^j=nf(x,y)$ である.

$(2)f(tx,ty)=(tx)^2+(tx)(ty)+(ty)^2=t^2(x^2+xy+y^2)=t^2f(x,y)$ である．したがって (1) より $2f=x\frac{\partial f}{\partial x}+y\frac{\partial f}{\partial y}$ である.

よって $J_f=(f,\frac{\partial f}{\partial x},\frac{\partial f}{\partial y})=(\frac{\partial f}{\partial x},\frac{\partial f}{\partial y})$ である.

$\frac{\partial f}{\partial x}=2ax+2by,\frac{\partial f}{\partial y}=2bx+2cy$ であるから $J_f=(2ax+2by,2bx+2cy)$ である.

$a=b=0$ のとき．$J_f=(y)$ より $\mathbb{C}[x,y]/J_f\cong\mathbb{C}[x]$ である．これは無限次元．$b=c=0$ のときも同様.

$a=c=0,b\neq0$ のとき．$J_f=(x,y)$ である．$\mathbb{C}[x,y]/J_f\cong\mathbb{C}$ である．これは有限次元.

$a=0,b\neq0\neq c$ のとき．$J_f=(2by,2bx+2cy)=(x,y)$ である．$\mathbb{C}[x,y]/J_f\cong\mathbb{C}$ である．これは有限次元.

$c=0,a\neq0\neq b$ のときも同様.

$b=0,a\neq0\neq c$ のとき．$J_f=(2ax,2cy)=(x,y)$ である．よって有限次元.

$a\neq0,b\neq0,c\neq0$ のとき．$J_f=(\frac{a}{b}x+y,x+\frac{c}{b}y)$ である．$(\frac{a}{b}x+y)-\frac{a}{b}(x+\frac{c}{b}y)=(1-\frac{ac}{b^2})y$ より $J_f=(ax+by,(1-\frac{ac}{b^2})y)$ である.

ここで $1-\frac{ac}{b^2}=0$ ならば $J_f=(ax+by)$ より $\mathbb{C}[x,y]/J_f\cong\mathbb{C}[y]$ である．これは無限次元.

$1-\frac{ac}{b^2}\neq0$ ならば $J_f=(x,y)$ より有限次元.

以上より f が有限次元である条件は $ac\neq b^2$ である.

0.7 H12 数学選択

8 (1) $\pi(ab)=(ab)^2=a^2b^2=\pi(a)\pi(b)$ である．よって準同型.

$(2)\pi(a)=b\in\mathrm{Im}\,\pi$ に対して，$\pi(x)=b$ なら x は $x^2-b=0$ の根である．したがって $\pi(x)=b$ となる x は $a,-a$ のみ.

$a=-a$ なら $a=0\vee2=0\in\mathbb{F}_p^\times$ である．$a\in\mathbb{F}_p^\times$ より $a\neq0$ で p は奇素数であるから $2\neq0$ である．よって $a\neq-a$ である.

したがって位数は $\frac{p-1}{2}$ である.

$(3)\ker\pi^2=\left\{x\;\middle|\;x^4=1\right\}$ である．$x^2=1$ となる x は $1,-1$ のみ．$x\in\ker\pi^2$ で $x\neq\pm1$ なら $x^2=-1$ である.

したがって $p-1$ が 4 の倍数ならば -1 は平方剰余であるから $\ker\pi^2$ は位数 4 の群 $\{-1,1,a,-a\}\quad(a^2=-1)$

となる．

$p-1$ が 4 の倍数でないならば -1 は平方非剰余であるから $\ker \pi^2$ は位数 2 の群 $\{-1,1\}$ となる．

(4)$1^2=1,2^2=4,3^2=9,4^2=5,5^2=3$ であるから，$\mathbb{F}_{11}^{\times}$ は x^2-2 の根を持たない．よって x^2-2 は既約である．

$x^4-2=(x^2+4x+8)(x^2+7x+8)$ であるから既約でない．

9 (1)G による不変体を L^G とする．$G=\{\sigma,\tau,\sigma\circ\tau\}$ である．$\sigma(x^2+y^2)=y^2+x^2,\sigma(xy)=yx,\tau(x^2+y^2)=x^2+y^2,\tau(xy)=xy$ であるから $K\subset L^G$ である．$[L:L^G]=|\operatorname{Gal}(L/L^G)|=|G|=4$ である．

$L=K(x)$ である．$(t-x)(t+x)(t-y)(t+y)=t^4-(x^2+y^2)t^2+x^2y^2$ であるから $[L:K]\leq 4$ である．したがって $K=L^G$ である．よって L/K は Galois 拡大で galois 群は G である．

(2)G の非自明な部分群は $\langle\sigma\rangle,\langle\tau\rangle,\langle\sigma\circ\tau\rangle$ である．$\sigma(x+y)=y+x,\tau(x^2-y^2)=x^2-y^2,\sigma\circ\tau(x-y)=x-y$ であり，また $\tau(x+y)=-x-y,\sigma(x^2-y^2)=y^2-x^2,\tau(x-y)=-x+y$ である．よって $K(x+y),K(x^2-y^2),K(x-y)$ がそれぞれに対応する中間体である．これに L,K を加えたものが全ての中間体である．

0.8 H13 数学選択

N (1)$t^4-zt^2+1=(t-x)(t+x)(t-\frac{1}{x})(t+\frac{1}{x})$ であるから $K(x)/K(z)$ は正規拡大．$\mathrm{ch}K\neq 2$ より $x\neq\frac{1}{x}$ より t^4-zt^2+1 は分離多項式．よって x が $K(z)$ 上分離的であるから $K(z)/K(x)$ が Galois 拡大．

(2)t^2-ty+1 は $K(y)$ 上の x の最小多項式であり，根は $x,\frac{1}{x}$ である．よって $K(y)/K(x)$ は Galois 拡大であるから $\mathrm{Aut}(K(y)/K(x))=\mathrm{Gal}(K(y)/K(x))$ である．よって位数は 2 である．

$\mathrm{ch}K\neq 2$ なら $K(x)/K(z)$ は Galois 拡大であった．$K(y)$ が非自明な中間体となるから $[K(x):K(z)]=4$ である．よって $\mathrm{Aut}(K(x)/K(z))$ の位数は 4 である．

$\mathrm{ch}K=2$ なら $K(x)/K(z)$ は正規拡大であるが分離拡大でない．したがって $\sigma(x)=\frac{1}{x}$ と id の 2 個が $\mathrm{Aut}(K(x)/K(z))$ の元である．位数は 2.

O (1)$m_{(a,b)}\subsetneq J$ なるイデアル J が存在すると仮定する．$f(x,y)\in J\setminus m_{(a,b)}$ となる $f(x,y)\in\mathbb{C}[x,y]$ をとる．$f(x,y)=g(x,y)(x-a)+h(y)(y-b)+r$ となる $g(x,y)\in\mathbb{C}[x,y],h(y)\in\mathbb{C}[y],r\in\mathbb{C}$ が存在する．このとき $r\in J$ より $J=\mathbb{C}[x,y]$ である．よって $m_{(a,b)}$ は極大イデアルである．

(2)$\phi(x^3-y^2)=0$ より $\ker\phi\supset(x^3-y^2)$ である．$f(x,y)\in\ker\psi$ に対して $f(x,y)=g(x,y)(x^3-y^2)+h_1(x)y+h_2(x)$ となる $g(x,y)\in\mathbb{C}[x,y],h_1(x),h_2(x)\in\mathbb{C}[x]$ が存在する．

$0=f(t^3,t^2)=h_1(t^2)t^3+h_2(t^2)$ であるから $-h_1(t^2)t^3=h_2(t^2)$ である．右辺の t の次数は偶数であるから，$h_1=0$ である．よって $h_2=0$ より $f(x,y)\in(x^3-y^2)$ である．すなわち $\ker\psi=(x^3-y^2)$ である．

(3)$\psi(m_{(a,b)})=(t^3-a,t^2-b)$ である．

$b=0$ のとき．$(t^3-a,t^2-b)=(t^3-a,t^2)=(a,t^2)=\begin{cases}(t^2) & a=0\\ (1) & a\neq 0\end{cases}$ である．

$b\neq 0$ のとき．$(t^3-a,t^2-b)=(-a-bt,t^2-b)=(\frac{a}{b}+t,t^2-b)=(\frac{a}{b}+t,\frac{a^2}{b^2}-b)=\begin{cases}(\frac{a}{b}+t) & a^2=b^3\\ (1) & a^2\neq b^3\end{cases}$ である．

0.9 H14 数学選択

D (1)$f(t)=\sum a_it^i,g(t)=\sum b_jt^j$ とする．$\deg f>\deg g$ なら $f(t)^2+g(t)^2$ の次数は $2\deg f>0$ となる．$\deg f=\deg g$ なら $f(t)^2+g(t)^2$ なら最高次の係数は $a_n^2+b_n^2>0$ より定数でない．

(2) 同型写像 $\phi:\mathbb{R}[x,y]/(x^2+y^2-1)\to\mathbb{R}[t]$ があると仮定する．$x^2+y^2=1\in\mathbb{R}[x,y]/(x^2+y^2-1)$ より

$\phi(x)^2+\phi(y)^2=1\in\mathbb{R}[t]$ である．

ψ は $\mathbb{R}$ 上の同型写像であるから $\phi(x),\phi(y)\notin\mathbb{R}$ である．これは (1) に矛盾.

(3)(x^2+y^2-1) が素イデアルであることを示せばよく，そのためには $\mathbb{R}[x,y]$ は UFD であるから x^2+y^2-1 が既約であることを示せばよい.

$\mathbb{R}[x]$ は UFD であるから，$\mathbb{R}[x][y]$ 上の既約性は $\mathbb{R}(x)[y]$ 上の既約性と同値である.

可約なら $x^2+\frac{f(x)^2}{g(x)^2}=1$ となる $f(x),g(x)\in\mathbb{R}[x]$ が存在する．このとき $x^2g(x)^2+f(x)^2=g(x)^2$ である．x の次数は $\max(2+2\deg g,2\deg f)>2\deg g$ となり矛盾．したがって x^2+y^2-1 は既約である.

0.10 H15 数学選択

D (1)$(p)=\mathcal{P}\subset J\subsetneq R$ なる R のイデアル J を任意にとる．PID であるから $J=(d)$ とかける．$R\neq(d)$ より d は単元ではない．$p=dk$ なる $k\in R$ が存在する．p は既約元であるから d,k のいずれかは単元である，よって k は単元．このとき $(d)=(p)$ となるから $\mathcal{P}$ は極大イデアル.

(2) (a)$\mathbb{Z}$ は Euclid 整域であるから PID

$I\subset\mathbb{Z}$ について d を I に属す最小の正整数とする．$a\in I$ について $a=qd+r\quad(0\leq r<d)$ となる q,r が存在する．$a-qd\in I$ より $r\in I$．d の最小性から $r=0$ である．よって $a\in(d)$ より $I=(d)$ である.

(b)$\mathbb{F}_p$ は体であるから，$\mathbb{F}_p[x]$ は体上の 1 変数多項式環だから PID

$I\subset\mathbb{F}_p[x]$ について $f(x)$ を I に属す次数最小の多項式のうちの一つとする．$g(x)\in I$ について $g(x)=f(x)q(x)+r(x)\quad(0\leq\deg r(x)<\deg f(x))$ とできる．$g(x)-f(x)q(x)=r(x)$ より $r(x)\in I$ であるから $r(x)=0$ である．よって $I=(f(x))$ である.

(c)$\mathbb{Z}$ は体でないから $\mathbb{Z}[x]$ は PID でない.

$I=(2,x)$ を考えると $2f(x)+xg(x)=1$ なら $2f(0)=1$ となり矛盾．よって $I\neq\mathbb{Z}[x]$ である．$I=(a(x))$ とすると $x=a(x)f(x)$ とできるが x は既約元であるから $f(x)$ は単元である．よって $f(x)=\pm1$ であるがこのとき $a(x)=\pm x$ となり $2\notin(a(x))$ となるから矛盾．よって PID でない.
一般に $K[x]$ が PID $\Leftrightarrow$K が体.

E (1)1 列目のベクトルの選び方が p^2-1 通り，正則になるためには 2 列目が 1 列目の定数倍でなければよいから p^2-p 通り．よって $|G|=(p^2-1)(p^2-p)$ 通り.

(2)$(x-\alpha)(x-\beta)$ と書ける多項式の数を考える．異なる α,β を選ぶ場合は $p(p-1)/2$ 通り．$\alpha=\beta$ を選ぶ場合は p 通り．よって $p(p-1)/2+p=p(p+1)/2$ 通り．モニックな多項式の総数は p^2 通りであるから既約なモニック多項式の総数は $p^2-p(p+1)/2=p(p-1)/2$ 通り.

(3)$A=\begin{pmatrix}0&1\\-b&a\end{pmatrix}$ とすれば固有多項式は $\det(xI-A)=x^2+ax+b$ である．$B=\begin{pmatrix}x&y\\z&w\end{pmatrix}$ とする．$BA=\begin{pmatrix}-by&x+ay\\-bw&z+aw\end{pmatrix}=\begin{pmatrix}z&w\\-bx+az&-by+aw\end{pmatrix}=AB$ なら $z=-by,w=x+ay$ である．逆に $z=-by,w=x+ay$ なら $BA=AB$ である．B は正則であるから $\begin{pmatrix}x\\z\end{pmatrix}=k\begin{pmatrix}y\\w\end{pmatrix}$ となる $k\in\mathbb{F}_p$ が存在しな

い．存在するとき，$-by = z = kw = kky + kay$ より $y(k^2 + ak + b) = 0$ となる．$x^2 + ax + b$ が既約であるから $k^2 + ak + b = 0$ となる k は存在しない．よって $y = 0$ である．

以上より $y \neq 0$ 以外の (x, y) 毎に $AB = BA$ を満たす B が存在する．したがって $|C(A)| = p^2 - 1$ である．

一般に次が成り立つ．K を体として $A \in M_n(K)$ とする．A の最小多項式が n 次なら $C_{M_n(K)}(A) = K[A]$ である．さらに A が既約なら $K[A]$ は体である．
前半の主張は単因子論を用いて $\{v, Av, \cdots, A^{n-1}v\}$ が K^n の基底となる事を示して，$Bv = f \cdot v$ とすれば $Bu = f(A)u \quad (u \in K^n)$ となることを示す．後半の主張は $\varphi\colon K[x] \to M_n(K); f(x) \mapsto f(A)$ とすれば $K[x]/(p(x)) \cong K[A]$ となり $p(x)$ が既約なら $K[x]/(p(x))$ は体であるから $K[A]$ も体である．($p(x)$ は最小多項式)
つまり (3) の答えは $|K[A]^\times| = p^2 - 1$ である．

(4) $A \in GL_2(\mathbb{F}_p)$ の固有多項式が既約な x^2+ax+b だとする．A は固有ベクトルを持たないから $0 \neq v \in \mathbb{F}_p^2$ について $\{v, Av\}$ は基底となる．この基底に関して A の表現行列は $\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$ である．よって固有多項式が $x^2 + ax + b$ であるような行列は全て共役である．よって既約な固有方程式を持つ行列が含まれる共役類は既約な方程式の数に等しい．すなわち $p(p-1)/2$ 通り．

可約な場合はジョルダン標準形と共役である．ジョルダン標準形の形は $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ のいずれかである．これらの異なる共役類の数は $(p-1) + (p-1) + ((p-1)^2 - (p-1))/2 = (p+2)(p-1)/2$ である．

以上より共役類の数は $p(p-1)/2 + (p+2)(p-1)/2 = p^2 - 1$ である．

0.11 H16 数学選択

A $(1)x^4 - 14x^2 + 9 = 0$ とする．$x^2 = y$ とおけば $y^2 - 14y + 9 = 0$ より $y = 7 \pm 2\sqrt{10}$ となる．よって $x = \pm\sqrt{7 \pm 2\sqrt{10}}$ が根である．

$\sqrt{7+2\sqrt{10}}\sqrt{7-2\sqrt{10}} = 3$ より $\mathbb{Q}(\sqrt{7+2\sqrt{10}})/\mathbb{Q}$ は 4 次 Galois 拡大である．

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{7+2\sqrt{10}})/\mathbb{Q})$ は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$ のいずれかである．

$\sigma(\sqrt{7+2\sqrt{10}}) = \sqrt{7-2\sqrt{10}}$ とする．$\sigma^2(\sqrt{7+2\sqrt{10}}) = \sigma(\sqrt{7-2\sqrt{10}}) = \sigma(3/\sqrt{7+2\sqrt{10}}) = 3/\sqrt{7-2\sqrt{10}} = \sqrt{7+2\sqrt{10}}$ より $\sigma^2 = \mathrm{id}$ である．

$\sigma(\sqrt{7+2\sqrt{10}}) = -\sqrt{7+2\sqrt{10}}$ とする．これも $\sigma^2 = \mathrm{id}$ である．

位数が 2 の元を 2 つ以上もつから $\mathrm{Gal}(\mathbb{Q}(\sqrt{7+2\sqrt{10}})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．

$(2)x^4 - 20x^2 + 98 = 0$ とする．$x^2 = y$ とおけば $y^2 - 20y + 98 = 0$ より $y = 10 \pm \sqrt{2}$ となる．よって $x = \pm\sqrt{10 \pm \sqrt{2}}$ が根である．

$\sqrt{10+\sqrt{2}}\sqrt{10-\sqrt{2}} = 7\sqrt{2}$ であり $(\sqrt{10+\sqrt{2}})^2 = 10 + \sqrt{2} \in \mathbb{Q}(\sqrt{10+\sqrt{2}})$ であるから $\mathbb{Q}(\sqrt{10+\sqrt{2}})/\mathbb{Q}$ は 4 次 Galois 拡大である．

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{10+\sqrt{2}})/\mathbb{Q})$ として $\sigma(\sqrt{10+\sqrt{2}}) = \sqrt{10-\sqrt{2}}$ とする．$10 + \sigma(\sqrt{2}) = \sigma((\sqrt{10+\sqrt{2}})^2) = (\sqrt{10-\sqrt{2}})^2 = 10 - \sqrt{2}$ より $\sigma(\sqrt{2}) = -\sqrt{2}$ である．$\sigma^2(\sqrt{10+\sqrt{2}}) = \sigma(\sqrt{10-\sqrt{2}}) = \sigma(7\sqrt{2}/\sqrt{10+\sqrt{2}}) = -7\sqrt{2}/\sqrt{10-\sqrt{2}} = -\sqrt{10+\sqrt{2}}$ より $\sigma^2 \neq \mathrm{id}$ である．

位数が 2 でない元が属すから $\mathrm{Gal}(\mathbb{Q}(\sqrt{10+\sqrt{2}})/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ である．

B $(1)k$ 上 1 次元ベクトル空間は k と同型である．よって $\rho\colon \mathbb{Z}/3\mathbb{Z} \to GL(k)$ としてよい．

$f \in GL(k)$ の元は $a \in k$ に対して $f(a) = f(a \cdot 1_k) = af(1_k)$ であるから $f(1_k)$ で定まる．$i \in \mathbb{Z}/3\mathbb{Z}$ に対し

て $\rho(i)(1_k)=\alpha\in k$ とする．$\rho(i+i+i)=\rho(0)=\mathrm{id}$ より $\rho^3(1_k)=\alpha^3=1_k$ である．k の標数は 3 であるから $x^3-1_k=(x-1_k)^3$ より $\alpha=1_k$ である．よって $\rho(i)=\mathrm{id}$ である．すなわち $\rho(G)=\{\mathrm{id}\}$ である．

(2) 略

(3)$V=W_1\oplus W_2$ が存在するとする．$\rho(1+3\mathbb{Z})$ の V 上の最小多項式は W_1,W_2 上の最小多項式の最小公倍数である．$\rho(1+3\mathbb{Z})v=\lambda v\quad(\lambda\in k)$ とすると，$v=\rho(0+3\mathbb{Z})v=\rho(1+3\mathbb{Z})^3v=\lambda^3v$ より $1_k=\lambda^3$ である．よって $\lambda=1_k$ である．最小多項式は固有値以外を根に持たないから W_1 上の最小多項式は $(t-1_k)$ の因数，W_2 上の最小多項式は $(t-1_k)^2$ の因数である．すなわち V 上の最小多項式は W_2 上の最小多項式と一致して 2 次以下である．

V の基底 $\{v_1,v_2,v_3\}$ による $\rho(1+3\mathbb{Z})$ の表現行列は $A=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$ であり $(A-E_3)^2\neq0$ であるから最小多項式は 3 次である．これは矛盾．

(4)$W_1=\langle v_1+v_2+v_3\rangle, W_2=\langle -v_2+v_3, v_1-v_3\rangle$ とする．$\begin{vmatrix}1&0&1\\1&-1&0\\1&1&-1\end{vmatrix}=3\neq0$ より $V=W_1\oplus W_2$ である．

$\rho(1+3\mathbb{Z})(v_1+v_2+v_3)=v_1+v_2+v_3$ より $\rho(G)W_1\subset W_1$ である．$\rho(1+3\mathbb{Z})(-v_2+v_3)=v_1-v_3\in W_2, \rho(1+3\mathbb{Z})(v_1-v_3)=-v_1+v_2=-(-v_2+v_3)-(v_1-v_3)\in W_2$ より $\rho(G)W_2\subset W_2$ である．

0.12 H17 数学選択

L (1) 二次方程式は $x^2, x^2+1, x^2+x, x^2+x+1$ の 4 つである．このうち既約なものは根を $\mathbb{F}_2$ に持たないもの，すなわち x^2+x+1 である．

(2) 二次のモニック多項式は p^2 個ある．可約なモニック多項式は $(x-\alpha)(x-\beta)$ の形である．$\alpha\neq\beta$ に対して $(x-\alpha)(x-\beta)=(x-\beta)(x-\alpha)$ であることを踏まえると可約なモニック多項式の個数は $(p^2-p)/2+p=(p^2+p)/2$ である．

よって既約なモニック多項式の個数は $p^2-(p^2+p)/2=(p^2-p)/2$ である．

(3)$x^2+1\in\mathbb{F}_p[x]$ が既約 $\Leftrightarrow -1$ が平方剰余

-1 が平方剰余なら $^\exists x\in\mathbb{F}_p^\times$ が $x^4=1$ である．すなわち $\mathbb{F}_p$ は位数 4 の部分群を持つから $4|(p-1)$ である．

逆に $4|(p-1)$ なら sylow の定理から位数が 4 以上の 2-sylow 部分群 H が存在する．$x^2=1$ となる x は ±1 のみであるから，位数が 4 以上であることより $^\exists x\in H$ が $x^2=-1$ である．よって -1 は平方剰余である．

すなわち x^2+1 が既約 $\Leftrightarrow p\equiv1 \mod 4$ である．

M (1)$f^2=\mathrm{id}$ より f は対角化可能であり F 上ベクトル空間として $V=W_1\oplus W_{-1}$ と分解できる．ここで W_i は固有値 i の固有空間である．

$\varphi\colon V\to V_f; v\mapsto v+f(v)$ とすれば $\ker\varphi=W_{-1}$ である．全射でもあるから $\dim_F V_f=\dim_F V-\dim_F W_{-1}$ である．$W=W_1$ であるから $\dim_F W=\dim_F V-\dim_F W_{-1}$ である．よって $\dim_F V_f=\dim_F W$ である．

$f(v+f(v))=f(v)+f^2(v)=f(v)+v$ より $V_f\subset W$ である．よって $V_f=W$ である．

K/F は二次拡大であるから $\sigma(\alpha)=-\alpha$ なる $\alpha\in K$ が存在する．W の F 上の基底 $\{v_1,v_2,\dots,v_m\}$ をとる．

$\{\alpha v_1,\alpha v_2,\dots,\alpha v_m\}$ は W_{-1} の基底となる．$v\in W_{-1}$ に対して $\alpha v\in W$ より $\alpha v=\sum_{i=1}^m a_iv_i$ より $\alpha^2v=\sum_{i=1}^m a_i\alpha v_i, \alpha^2\in F$ より W_{-1} を生成する．また $\sum c_i\alpha v_i=0\quad(c_i\in F)$ なら $\sum c_iv_i=0$ であるから $c_i=0$ である．よって $\{\alpha v_1,\alpha v_2,\dots,\alpha v_m\}$ は W_{-1} の基底となる．

$u\in V$ に対して $u=u_1+u_{-1}\quad(u_1\in W_1,u_{-1}\in W_{-1})$ と一意にあらわせる．$u_1\in W$ より $u_1=\sum_{i=1}^m a_iv_i$ と表せる．また $u_{-1}=\sum_{i=1}^m b_i\alpha v_i$ と表せる．よって $u=\sum_{i=1}^m(a_i+b_i\alpha)v_i$ と表せる．すなわち $\{v_1,v_2,\dots,v_m\}$ は K 上で V を生成する．

$\sum(a_i+b_i\alpha)v_i=0\quad(a_i,b_i\in F)$ とする．$\sum a_iv_i=0\in W, \sum b_i\alpha v_i=0\in W_{-1}$ である．よって $a_i=b_i=0$ で

ある．すなわち $\{v_1, v_2, \ldots, v_m\}$ は K 上で V の基底となる．

よって $m = n$ である．すなわち $\dim_F W = n$ である．

0.13 H18 数学選択

1 (1)F/K が 2 次拡大であれば $\alpha \in F \setminus K$ の最小多項式の根は $a + b\sqrt{\beta}$ の形で表せる．この $\sqrt{\beta}$ を添加した体は F となる．

2 次の中間体の一つを $M = K(\sqrt{\beta})$ $(\beta \in K)$ とする．L/M は 2 次拡大であるから，$L = M(\sqrt{\gamma})$ $(a, b \in K, \gamma = a + b\sqrt{\beta})$ と表せる．

$b \neq 0$ のとき．$(\gamma^2 - a)^2 = b^2\beta$ より $x^4 - 2ax^2 + (a^2 - b^2\beta) = 0$ の根は $\pm\sqrt{a \pm b\sqrt{\beta}}$ である．この多項式が可約なら $K(\sqrt{a + b\sqrt{\beta}})/K$ は 2 次拡大である．$(\sqrt{a + b\sqrt{\beta}})^2 = a + b\sqrt{\beta}$ より $K(\sqrt{a + b\sqrt{\beta}}) = K(\sqrt{\beta}) = M$ となる．これは矛盾．よって多項式は既約である．

$b = 0$ のとき $\delta = \sqrt{\beta} + \sqrt{\gamma}$ とすると $(\delta - \sqrt{\beta})^2 = \gamma = a^2$ より $\delta^2 + \beta - a^2 = 2\sqrt{\beta}\delta$．よって $\delta^4 + 2(\beta - a^2)\delta^2 + (\beta - a^2)^2 = 4\beta\delta^2$ より $x^4 - 2(a^2 + \beta)x^2 + (\beta - a^2)^2 = 0$ の根は $\pm\sqrt{\beta} \pm \sqrt{\gamma}$ である．標数が 2 でないから $K(\sqrt{\beta}, \sqrt{\gamma})/K$ は Galois 拡大である．Galois 群は $\{\mathrm{id}, \sigma, \tau, \tau \circ \sigma\}$ $(\sigma(\sqrt{\beta}) = \sqrt{\beta}, \sigma(\sqrt{\gamma}) = \sqrt{\gamma}, \tau(\sqrt{\beta}) = -\sqrt{\beta}, \tau(\sqrt{\gamma}) = \sqrt{\gamma})$ である．

このとき任意の $f \in \mathrm{Gal}(K(\sqrt{\beta}, \sqrt{\gamma})/K)$ に対して $f(\delta) \neq \delta$ であるから，$K(\delta)/K$ は 4 次拡大である．すなわち $x^4 - 2(a^2 + \beta)x^2 + (\beta - a^2)^2$ は既約である．

(2)$b \neq 0$ のとき，$a^2 - b^2\beta = c^2$ $(c \in K)$ である．$\sqrt{a + b\sqrt{\beta}}\sqrt{a - b\sqrt{\beta}} = \sqrt{a^2 - b^2\beta} = c \in K$ より $K(\sqrt{a + b\sqrt{\beta}}) \ni \sqrt{a - b\sqrt{\beta}}$ である．よって L/K は Galois 拡大である．

$\sigma \in \mathrm{Gal}(L/K)$ について $\sigma(\sqrt{a + b\sqrt{\beta}}) = \sqrt{a - b\sqrt{\beta}}$ とする．このとき $\sigma^2(\sqrt{a + b\sqrt{\beta}}) = \sigma(\sqrt{a - b\sqrt{\beta}}) = \sigma(c/\sqrt{a + b\sqrt{\beta}}) = c/\sqrt{a - b\sqrt{\beta}} = \sqrt{a + b\sqrt{\beta}}$ より $\sigma^2 = \mathrm{id}$ である．すなわち $\mathrm{Gal}(L/K)$ は位数 2 の元を二つもつ．

$\mathrm{Gal}(L/K)$ は位数 4 の群であるから，$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ のいずれかである．位数 2 の元を二つもつ群は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であるから，$\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．

よって中間体の数は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ の部分群の数であるから 5 である．非自明な中間体は 3 個ある．

0.14 H19 数学選択

7 (1)ch$F \neq 2$ より $\alpha \neq -\alpha$ である．したがって $F(\alpha)/F$ は Galois 拡大である．$\mathrm{id} \neq \sigma \in \mathrm{Gal}(F(\alpha)/F)$ をとる．$\sigma(\alpha) = -\alpha$ である．$F(\beta) = F(\alpha)$ より $\sigma(\beta) = -\beta$ である．よって $F(\alpha\beta) = \alpha\beta$ より $\alpha\beta \in F$ である．すなわち $ab = (\alpha\beta)^2$ となり F の平方数.

(2)(a)$\mathrm{Gal}(L/F) \cong \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ であるから，唯一の真部分群 $\{\bar{0}, \bar{2}\}$ に対応する中間体 K が唯一の非自明な中間体である．

(b)F 上 2 次の元とすると $F(\xi)/F$ は 2 次拡大であるから $F(\xi) = K = F(\gamma)$ である．このとき $L = K(\xi) = F(\xi)$ となり矛盾する．したがって 4 次の元である．

(c)ξ の F 上の最小多項式は $(x^2 - p)^2 = q^2c$ である．この方程式の解は $\pm\sqrt{p \pm q\gamma}$ である．L/K は Galois 拡大であるから，$L = K(\sqrt{p + q\gamma}) = K(\sqrt{p - q\gamma})$ である．したがって $(p + q\gamma)(p - q\gamma) = p^2 - q^2\gamma^2 = (a + b\gamma)^2$ なる $a, b \in F$ が存在する．$p^2 - q^2c - a^2 - b^2c = 2ab\gamma$ より $ab = 0$ である．

$a = 0$ のとき，$p^2 - q^2c = b^2c$ より $p^2 = (b^2 + q^2)c$ である．よって $c = (\frac{pb}{b^2+q^2})^2 + (\frac{pq}{b^2+q^2})^2$ とできる．

$b = 0$ なら $\sqrt{p^2 - q^2c} = a \in F$ である．$\sigma(\sqrt{p + q\gamma}) = \sqrt{p - q\gamma}$ に対して $\sigma(\sqrt{p - q\gamma}) = \sigma(a/\sqrt{p + q\gamma}) = \frac{a}{\sqrt{p-q\gamma}} = \sqrt{p + q\gamma}$ である．したがって $\sigma^2 = \mathrm{id}$ である．$\tau(\sqrt{p + q\gamma}) = -\sqrt{p + q\gamma}$ とすると $\tau^2 = \mathrm{id}$ である．これは $\mathrm{Gal}(L/K)$ が巡回拡大であることに矛盾.