0.1 2001 数学専門

$\boxed{1}$ $A \in GL_2(\mathbb{F}_2)$ について $\det A \in \mathbb{F}^\times = 1$ であるから $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$ である．

$GL_2(\mathbb{F}_2) = \mathrm{Aut}(\mathbb{F}_2^2)$ である．$\varphi \in \mathrm{Hom}(\mathbb{F}_2^2)$ は基底 $(1,0),(0,1)$ で定まる．$\mathbb{F}_2^2$ の元 v で生成される部分空間 $\mathrm{Span}(v) = \{0, v\}$ であるから,非零なベクトルは各対ごとに 1 次独立．よって $(0,0) \neq \varphi(0,1) \neq \varphi(1,0) \neq (0,0)$ なら $\varphi \in \mathrm{Aut}(\mathbb{F}_2^2)$ である．したがって φ は $\mathbb{F}_2^2 \setminus \{0,0\}$ の置換である．集合 X の置換群を $\mathfrak{S}(X)$ で表すと，$f\colon \mathrm{Aut}(\mathbb{F}_2^2) \to \mathfrak{S}(\mathbb{F}_2^2 \setminus \{0,0\})$ が定まり，これが全単射準同型であることは明らか．したがって $SL_2(\mathbb{F}_2) \cong \mathfrak{S}_3$ である．

$\boxed{2}$ A は $x(x-1)$ を 0 でないべき零元としてもつ．

(a) 中国剰余定理から $\mathbb{R}[x]/(x(x-1)) \cong \mathbb{R}[x]/(x) \times \mathbb{R}[x]/(x-1) \cong \mathbb{R}^2$ より零でないべき零元をもたない．よって同型でない．

(b)$x^2(-x^2+2) + (x-1)^2(x+1)^2 = 1$ であるから $(x^2) + ((x-1)^2) = \mathbb{R}[x]$ である．$\varphi\colon \mathbb{R}[x]/(x^2(x-1)^2) \to \mathbb{R}[x]/(x^2) \times \mathbb{R}[x]/((x-1)^2); f + (x^2(x-1)^2) \mapsto (f + (x^2), f + (x-1)^2)$ と定める．φ が well-defined であるのは明らか．$\varphi(f + (x^2(x-1)^2)) = 0$ とすると，$f \in (x^2), f \in (x-1)^2$ である．$f = f \cdot (x^2(-x^2+2) + (x-1)^2(x+1)^2) = (-x^2+2)f \cdot x^2 + (x+1)^2 f \cdot (x-1)^2 \in (x^2(x-1)^2)$ である．よって φ は単射．$g + (x^2), h + (x-1)^2$ に対して $f = g \cdot (x-1)^2(x+1)^2 + h \cdot (-x^2+2)x^2$ とすれば $f + (x^2) = g + (h-g) \cdot (-x^2+2)x^2 + (x^2) = g + (x^2), f + ((x-1)^2) = h + (g-h) \cdot (x-1)^2(x+1)^2 = h + (x-1)^2$ である．よって φ は全射．よって φ は同型写像.

(c)$\mathbb{R}[x]/(x(x-1)) \times \mathbb{R}[x]/(x(x-1)) \cong \mathbb{R}^4$ より零でないべき零元をもたない．よって同型でない．

$\boxed{4}$ (1)$\{1, \zeta, \cdots, \zeta^5\}$ が基底となる．一次独立であることは $\sum_{i=0}^{5} c_i \zeta_i = 0$ であるについて $c_i \neq 0$ なら ζ の最小多項式が 4 次以下であるとわかる．ζ は 1 の原始 7 乗根であるから $x^7 - 1 = (x-1)(x^6 + x^5 + \cdots + 1)$ より $p(x) = x^6 + x^5 + \cdots + 1$ が ζ を根にもつ．$p(x+1) = \frac{(x+1)^7 - 1}{x}$ であり 7 は素数であるから $(x+1)^7$ の x^2 から x^6 までの係数は全て 7 の倍数である．よって $p(x+1)$ も最高次の係数は 1 でそれ以外は 7 の倍数であるからアイゼンシュタインの既約判定法から $\mathbb{Z}[x]$ 上既約である．$p(x)$ はモニックであるから $\mathbb{Q}[x]$ 上既約であるため，$p(x)$ も $\mathbb{Q}[x]$ 上既約．よって $p(x)$ が ζ の最小多項式である．$\deg p = 6$ 矛盾．よって一次独立．

$\mathbb{Q}(\zeta)$ は $\mathbb{Q}[\zeta]$ の商体であるが，$\mathbb{Q}[\zeta] \cong \mathbb{Q}[x]/(p(x))$ で $p(x)$ は既約であり，$\mathbb{Q}[x]$ は PID であるから $(p(x))$ は極大イデアル．よって $\mathbb{Q}[\zeta]$ は体であるから $\mathbb{Q}[\zeta] = \mathbb{Q}(\zeta)$ である．$\mathbb{Q}[\zeta]$ の任意の元が $\{1, \zeta, \cdots, \zeta^5\}$ で生成されることは明らか．よって基底.

(2)$p(x)$ の根は $\zeta^i \quad (i = 1, \cdots, 6)$ である．よって $p(x)$ は $\mathbb{Q}(\zeta)$ で分解するから Galois 拡大.

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ を $\sigma(\zeta) = \zeta^3$ とすれば $\sigma^i(\zeta) = \zeta^{3^i}$ であり，$3^i \equiv 1 \mod (7)$ なる最小の i は 6 であるから σ の位数は 6 である．$|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ より $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ である．

(3)$\mathbb{Z}/6\mathbb{Z}$ の真部分群は $3\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z}$ である．対応する中間体は σ^3 で固定される体と σ^2 で固定される体である．$\sigma^3(\zeta + \zeta^6) = \zeta + \zeta^6 = 2\cos\frac{2\pi}{7}$ であるから，$\mathbb{Q}(\cos\frac{2\pi}{7})$ である．

$\sigma^2(\zeta + \zeta^2 + \zeta^4) = \zeta^2 + \zeta^4 + \zeta$ であるから $\mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$ である．

よって求める中間体は $\mathbb{Q}, \mathbb{Q}(\zeta + \zeta^2 + \zeta^4), \mathbb{Q}(\zeta + \zeta^6), \mathbb{Q}(\zeta)$ である．