(1) $A, B \in \mathrm{GL}_2(\mathbb{F}_p)$ を相異なる対角行列とする．A と B が共役なのは, それぞれ対角成分を入れ替えたものに等しいことと同値であることに注意する．したがって, 対角行列 H_C, H_D をそれぞれ定数行列と定数でない対角行列の集合とすれば, 対角行列と共役なものの個数は

$$\sum_{A \in H_C} \left|\{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_p)\}\right| + \frac{1}{2} \sum_{A \in H_D} \left|\{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_p)\}\right|$$

である．また, $A \in H_C$ に対しては

$$\left|\{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_p)\}\right| = 1$$

である．さらに, $A \in H_D$ に対して, $P \mapsto PAP^{-1}$ という共役による群作用を考えれば, その安定化群の位数を計算すれば, $(p-1)^2$ となることと, $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$ であることから,

$$\left|\{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_p)\}\right| = \frac{p(p-1)^2(p+1)}{(p-1)^2} = p(p+1)$$

となる．したがって, $|H_C| = p-1$, $|H_D| = (p-1)(p-2)$ であることに注意すれば,

$$\sum_{A \in H_C} \left|\{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_p)\}\right| + \frac{1}{2} \sum_{A \in H_D} \left|\{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_p)\}\right| = p - 1 + \frac{p(p+1)(p-1)(p-2)}{2}$$

となるので, 対角行列と共役でないものの個数は

$$p(p^2-1)(p-1) - (p-1) - \frac{p(p+1)(p-1)(p-2)}{2} = \frac{(p-1)^2(p^2+2^+2)}{2}$$

である．

(2) 仮定より, 最小多項式が一致するので, それを m とする．さらに, X, Y それぞれの固有多項式を p_X, p_Y とする．Cayley-Hamilton の定理より, 最小多項式は固有多項式を割り切るので, $\deg m \leq 2$ である．

(a) $\deg m = 1$ のとき, ある $a \in \mathbb{F}_p$ が存在して, $m(t) = t - a$ となる．$m(X) = m(Y) = 0$ より,

$$X = aI_2 = Y$$

となるので, 特に共役である．

(b) $\deg m = 2$ のとき, 固有多項式は monic であって, 最小多項式が一意であることから, $m = p_X = p_Y$ となる．つまり, X, Y は同じ固有多項式をもち, さらに固有多項式と最小多項式は等しくなる．このとき, 補題より, それぞれ固有多項式の同伴行列と共役なので, X, Y は共役になる．

以上より, X, Y は共役である．

(3) (2) について, 逆も成り立つことに注意する．$\mathbb{F}_p[t]$ の元であって, $\mathrm{GL}_2(\mathbb{F}_p)$ の元の最小多項式となるものの個数を求めればよい．

(a) $a \neq 0$ として, $t - a \in \mathbb{F}_p[t]$ なるものは, $aI_2 \in \mathrm{GL}_2(\mathbb{F}_p)$ の最小多項式なので, $p-1$ 個．逆に, 定数行列の最小多項式はすべて $t-a$ という形をしている．ゆえに, 最小多項式が一次式となるような $\mathrm{GL}_2(\mathbb{F}_p)$ の元の共役類は $p-1$ 個である．

(b) 最小多項式が二次式となるような $\mathrm{GL}_2(\mathbb{F}_p)$ の元について, その固有多項式は最小多項式と一致するので, 補題より, 固有多項式の同伴行列と共役である．逆に, 同伴行列の最小多項式は二次式になるので, 最小多項式が二次式となるような $\mathrm{GL}_2(\mathbb{F}_p)$ の元の個数は $\mathrm{GL}_2(\mathbb{F}_p)$ に属する同伴行列の個数に等しい．同伴行列が $\mathrm{GL}_2(\mathbb{F}_p)$ に属する必要十分条件はその固有多項式の定数項が零でないことなので, $\mathrm{GL}_2(\mathbb{F}_p)$ に属する同伴行列の個数は $p(p-1)$

以上より, $\mathrm{GL}_2(\mathbb{F}_p)$ の元の最小多項式は $(p-1)(p+1)$ 個ある.
さらに, (1) で計算していることから, 対角行列を含む $\mathrm{GL}_2(\mathbb{F}_p)$ の共役類の個数は $(p-1)+(p-1)(p-2)/2$ なので, 対角行列を含まない $\mathrm{GL}_2(\mathbb{F}_p)$ の共役類の個数は

$$(p-1)(p+1)-(p-1)-\frac{(p-1)(p-2)}{2}=\frac{(p+2)(p-1)}{2}$$

である.

Lemma 1. 体 K 上の n 次正方行列 A について, 次は同値である.

(1) A はその固有多項式の同伴行列と共役.
(2) A の固有多項式は最小多項式と一致する.
(3) ある $x \in K^n$ が存在して, $\{A^0x, A^1x, \dots, A^{n-1}x\}$ は K^n の基底.

Proof. A の固有多項式を p_A, 最小多項式を m_A とする.

(1) ⇒ (2) 同伴行列を C とする. $\det(tI-A)=\det(tI-C)$ なので, A の固有多項式は C のそれに等しい. ゆえに, 同伴行列の最小多項式の次数が n であることを示せば十分である. $\deg m_C \le n-1$ と仮定する. $0 \le k \le n-1$ に対して, $C^k e_1 = e_{k+1}$ なので, $m_C(C)e_1$ は $e_1, \dots, e_n$ の線形和となる. しかし, $m_C(C)=0$ なので $m_C(0)=0$ となって, 矛盾. したがって, $\deg m_C = n$.

(2) ⇒ (3) $x \in K^n \setminus \{0\}$ を任意にとる. $\{A^0x, A^1x, \dots, A^kx\}$ が K 上線形独立になるような最大の k を m として, $W_x = \mathrm{span}_K\{A^0x, A^1x, \dots, A^mx\}$ とおく. $A^{m+1}x \in W_x$ なので, ある $a_i \in K$ が存在して,

$$A^{m+1}x = \sum_{i=0}^{m} a_i A^i x$$

が成り立つ. このとき, 元の対応に注目すれば, $A|_{W_x}$ は

$$m_{A|_{W_x}}(t) = t^m - a_1 t^{m-1} - \cdots - a_{m-1}t - a_m \in K[t]$$

の同伴行列となる. しかし, $m_{A|_{W_x}}(A)=0$ より, $m_{A|_{W_x}}$ は m_A で割り切れることと, (1) ⇒ (2) で示したことから, $m_{A|_{W_x}}$ が最小多項式なので特に既約である. ゆえに, $m_A = m_{A|_{W_x}}$ が成り立つ. したがって, $m=n$ である. 以上より, W_x は K^n の部分線形空間であって, $\dim W_x = n$ なので, $W_x = K^n$ が成り立つ.

(3) ⇒ (1) $P=(A^0x, \cdots, A^{n-1}x)$ として, $A=P^{-1}CP$ が成り立てば十分である. ただし, C は p_A の同伴行列である. また, $A^0x, \cdots, A^{n-1}x$ は K^n の基底であることから, $A(A^ix)=P^{-1}CP^{-1}(A^ix)$ が成り立てば十分であり, これは計算によってすぐに従う.

□