0.1 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 $y\neq0$ 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．