【問題】 $\mathbb{F}_2$ を二つの元 $\{0,1\}$ からなる体とする．行列の各成分が $\mathbb{F}_2$ の元であり，行列式が $1 \in \mathbb{F}_2$ となる 2 次正方行列全体を $SL(2,\mathbb{F}_2)$ と表す．すなわち

$$SL(2,\mathbb{F}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{F}_2,\ ad-bc=1 \right\}.$$

$SL(2,\mathbb{F}_2)$ は行列の積に関して群となる．

(1) $SL(2,\mathbb{F}_2)$ の元の位数を列挙せよ．

(2) $SL(2,\mathbb{F}_2)$ と 3 次対称群は同型であることを示せ．

(H24 東工大情報理工学研究科 数理・計算科学専攻)

【解答】 (1) $SL(2,\mathbb{F}_2)$ の元は以下の 6 個である：

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\quad ST = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\quad TS = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\quad STS = TST = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

直接計算する事により位数はそれぞれ $\underline{1,2,2,3,3,2}$ である事が分かる．

(2) $SL_2(\mathbb{F}_2)$ の (E 以外の)，及び 3 次対称群の単位元 e 以外の演算表は以下のようになる．但し $s,t,\cdots$ はそれぞれ対称群の元

$$s=(1,2),\quad t=(2,3),\quad st = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\quad ts = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\quad sts = tst = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

を表し，表の i 行 j 列は (i 行)·(j 列) を表す．

	S	T	ST	TS	STS
S	E	ST	T	STS	TS
T	TS	E	TST	S	ST
ST	STS	S	TS	E	T
TS	T	TST	E	ST	S
STS	ST	TS	S	T	E

$SL(2,\mathbb{F}_2)$ の演算表

	s	t	st	ts	sts
s	e	st	t	sts	ts
t	ts	t	tst	s	st
st	sts	s	ts	e	t
ts	t	tst	e	st	s
sts	st	ts	s	t	e

3 次対称群の演算表

これらの表より $SL(2,\mathbb{F}_2)$ から 3 次対称群への写像 f を

$$f(E)=e,\quad f(S)=s,\quad f(T)=t,\quad f(ST)=st,\quad f(TS)=ts,\quad f(STS)=sts$$

により定めれば，f が群としての同型写像となる事が分かる． □

〔雑感〕 元の個数が少ない場合は上のような泥臭い計算で十分賄える．ただし対称群については (隣接互換で生成されるとか，基本関係式等の) 知識を必要とする．

【問題】 G を有限群とし，p を G の位数を割る最小の素数とする．このとき G の，指数 p の部分群は正規部分群であることを示せ．

(H10 東工大理学研究科 数学)

【解答】 e を G の単位元とし，H を指数 p の部分群とする．H に関する右剰余類集合を

$$G/H = \{k_1H, k_2H, \cdots, k_pH\} \qquad (k_1 = e,\ k_iH \cap k_jH = \varnothing \quad (i \neq j))$$

とし，G/H の置換の全体を $\mathfrak{S}(G/H)$ と記す．左移動が誘導する G/H 上の G の作用を π とし，その核を $K := \mathrm{Ker}\ \pi$ とする．

(i) 任意の $k \in K$ に $kH = \pi_k(H) = H$ だから，K は H に含まれる G の部分群である．$[G:K] = [G:H][H:K] = p[H:K]$ より $p \mid [G:K]$ が成り立つ．

(ii) $\mathfrak{S}(G/H)$ は p 次対称群 $\mathfrak{S}_p$ と同一視でき，群の完全系列

$$e \longrightarrow K \longrightarrow G \xrightarrow{\pi} \mathfrak{S}(G/H) \simeq \mathfrak{S}_p$$

より $\mathrm{Im}\ \pi$ は $\mathfrak{S}_p$ の部分群と同一視できるから，$[G:K] = \sharp G/\sharp K = \sharp \mathrm{Im}\ \pi$ は $p!$ の約数となる．

(i) (ii) より $[H:K]$ は $(p-1)!$ の約数となるが，p に対する仮定より $[H:K] = 1$，特に $H = K$ が成り立つ．K は π の核，従って G の正規部分群だから H は正規部分群である． □

〈雑感〉 ずっと “指数” を “位数” と勘違いし，3 週間近く止まっていた．実は演習問題程度だった (-_-;) .

【問題】 素数 p に対し

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{Z}/p\mathbb{Z} \right\}$$

は

$$SL(2, \mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z}/p\mathbb{Z}, \ ad - bc = 1 \right\}$$

のシロー部分群になっていることを示せ.

(H10 東工大理学研究科 数学)

【解答】 $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ の逆元は $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$ である事が容易に確かめれらる. また

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \in U$$

より U は $SL(2, \mathbb{Z}/p\mathbb{Z})$ の部分群であり, $\sharp U = p$ となる.

次に $\sharp SL(2, \mathbb{Z}/p\mathbb{Z})$ について考える. その為に最初に $\sharp GL(2, \mathbb{Z}/p\mathbb{Z})$ を計算する. $GL(2, \mathbb{Z}/p\mathbb{Z})$ の元は $\mathbb{Z}/p\mathbb{Z}$ 上の 2 次元線形空間 $V = (\mathbb{Z}/p\mathbb{Z})^2$ の基底と 1 対 1 に対応する. 最初に零ベクトルと異なる V のベクトルの選び方は $p^2 - 1$ 通り. 零ベクトルと異なるベクトル $\boldsymbol{v}_1$ を選んだとき, これと一次独立なベクトル (即ち $\boldsymbol{v}_1$ の生成する部分空間以外のベクトル) の選び方は $p^2 - p$ 通り. 従って

$$\sharp GL(2, \mathbb{Z}/p\mathbb{Z}) = \ V \text{ の基底の個数} = (p^2 - 1)(p^2 - p)$$

となる. $GL(2, \mathbb{Z}/p\mathbb{Z})$, $SL(2, \mathbb{Z}/p\mathbb{Z})$, および乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ に対し

$$e \ \to \ SL(2, \mathbb{Z}/p\mathbb{Z}) \ \hookrightarrow \ GL(2, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p\mathbb{Z})^\times \ \to \ e$$

という群の完全系列があり, これと準同型定理より

$$\sharp GL(2, \mathbb{Z}/p\mathbb{Z}) / \sharp SL(2, \mathbb{Z}/p\mathbb{Z}) = \sharp (GL(2, \mathbb{Z}/p\mathbb{Z}) / SL(2, \mathbb{Z}/p\mathbb{Z})) = \sharp (\mathbb{Z}/p\mathbb{Z})^\times = p - 1$$

従って $\sharp SL(2, \mathbb{Z}/p\mathbb{Z}) = \sharp GL(2, \mathbb{Z}/p\mathbb{Z}) / (p-1) = p(p^2 - 1)$ となる. この事から U は $SL(2, \mathbb{Z}/p\mathbb{Z})$ の Sylow p 部分群である事が分かる. □

※ H6 京都大学理学研究科の群論の問題参照.