$GL_2(\mathbb{F}_p)$ の Sylow 部分群の構造

青山学院大学　理工学部　物理・数理学科
学籍番号:15114035　片柳 創
指導教員 西山 享

平成 30 年 2 月 20 日

目 次

1　序論

1.1　研究の背景

私が本研究に至った動機は，2, 3 年次に群，環，体と代数学の基礎的な概念を学び，内容に興味を持ったからである．群論を学ぶ中で様々な部分群を考える必要があるが，部分群にはかなり強い制約が課せられている．本論文中にも紹介するが，Lagrange の定理によると有限群の部分群の位数は，その有限群の位数の約数であるということが知られている．そこで，その逆である,「有限群の位数の約数を位数とする部分群は必ず存在するか」という問いが自然に生まれる．しかし，一般にはその答えは否定的である．ところが，特別な約数の場合にはそのような位数を持つ部分群の存在が示され，部分群の分類など役立つ．そのようなものの一つが Sylow 部分群である．特殊な部分群ではあるが，基本的な部分群の構造に役立つ Sylow 部分群に興味を持ったのが本研究を始めた動機である．

1.2　研究の主結果

p を素数とする．このとき，

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \quad : \text{有限体}$$

とする．また，$\mathbb{F}_p$ の元を成分に持つ 2×2 の正則行列全体がなす群を $GL_2(\mathbb{F}_p)$ と表す．

有限群 G の位数を n とする．また，素数 q に対して n を割り切る q の冪で最大のものを q^e $(e \geq 0)$ とする．このとき，G の部分群で位数が q^e に等しいものを G の q-Sylow 部分群という．

G の一つの例として，$GL_2(\mathbb{F}_p)$ を本論文では考える．本研究の主結果とは以下の 2 つである．$G = GL_2(\mathbb{F}_p)$ とする．

(1) $p = 2,\ 3,\ 5,$ のとき，$GL_2(\mathbb{F}_p)$ の q-Sylow 部分群を全て決定した．

$p = 2$，$G = GL_2(\mathbb{F}_2)$ (定理 17)

q	2	3
q-Sylow 部分群の個数	3	1
位数 q^e の元の固有方程式 $\Phi(x)$	$x^2 + 1$	$x^2 + x + 1$

$p = 3$，$G = GL_2(\mathbb{F}_3)$ (定理 18)

q	2	3
q-Sylow 部分群の個数	3	4
位数 q^e の元の固有方程式 $\Phi(x)$	存在しない	$x^2 - 2x + 1$

$p=5$，$G=GL_2(\mathbb{F}_5)$ (定理 19)

q	2	3	5
q-Sylow 部分群の個数	15	10	6
位数 q^e の元の固有方程式 $\Phi(x)$	存在しない	x^2+x+1	x^2-2x+1

となった．Sylow 部分群と固有方程式は密接に関係していることが観察できた．しかし，時間不足のため，それを正確に表すのは現時点では難しい．

(2) $q=p$ のときには $G=GL_2(\mathbb{F}_p)$ の p-Sylow 部分群を決定できた．G の p-Sylow 部分群は

$$U=\left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\in GL_2(\mathbb{F}_p)\mid k=0,1,\ldots,p-1\right\}$$

のような部分群 U の共役部分群となっている．また，p-Sylow 部分群の個数は $p+1$ である．(定理 20)

q-Sylow 部分群 $(q\neq p)$ は，位数 q^e が $e=1$ であれば巡回群となるが，個数の性質は時間不足でわからなかった．また，$e>1$ の場合は $\mathbb{F}_p$ を一般にすると難しそうだった．

1.3 本論文の構成

2 章では，群とはどういったものであるか，という定義から始まり，剰余類，作用，軌道と群にどのような概念を加えることで群論の至る幅を広げているのかを紹介する，3 章で Sylow の定理を紹介・証明する．4 章では $GL_2(\mathbb{F}_p)$ の p-Sylow 部分群を $p=2,\ 3,\ 5$ において全て決定する．また，一般の p においての p-Sylow 部分群の構造を考察する．

1.4 参考

同研究室の菅亮輔氏が Sylow 部分群と正多面体の対称性の関係について研究しているので，そちらの卒業論文 [5] も参照していただきたい．

2　群の基本的な性質

この節では群の定義を与えたあと，本論文で考察する群の紹介をする．また，Sylow の定理の証明に使用する，作用や軌道といった概念を紹介する．

定義 1 (群). 集合 G と G 上の 2 項演算 $*$ が性質 (1)–(3) を満たすとき、G は**群**であるという．$*$ を集合 G 上の 2 項演算とし，$\sigma, \tau, \rho \in G$ とする．

(1) (結合律) $\forall\sigma, \tau, \rho$ に対し，$\sigma * (\tau * \rho) = (\sigma * \tau) * \rho$ が成り立つ．

(2) (単位元の存在) $\exists\varepsilon \in G$ が存在して，$\forall\sigma$ に対し，$\varepsilon * \sigma = \sigma * \varepsilon = \sigma$ が成り立つ．

(3) (逆元の存在) $\forall\sigma$ に対し，$\exists\xi \in G$ が存在して $\sigma * \xi = \xi * \sigma = \varepsilon$ が成り立つ．

$*$ は以下省略して，$a * b = ab$ のように書くことが多い．

G が群のとき，G の元の個数 (集合 G の濃度) を，群 G の**位数**と呼び，$|G|$ と表す．位数が有限の群を**有限群**といい，位数が無限の群を**無限群**という．

以下 G と書けば有限群を表し，特に断らなければ群は全て有限群とする．

2.1　群の例

後に紹介する作用・軌道の概念から任意の有限群は (ある次数の) 対称群の部分群に同型であることがわかる．このように有限群の代表といえる対称群の定義をまず与える．また，本論文で考察する $GL_2(\mathbb{F}_p)$ を紹介し，位数を計算する．

定義 2 (n 次対称群 $\mathfrak{S}_n$). $X_n = \{1, 2, \cdots, n\}$ を n 元集合とする．X_n からそれ自身への全単射 (置換) の全体を n **次対称群**と呼び，$\mathfrak{S}_n$ と表す．すなわち，

$$\mathfrak{S}_n := \{\sigma : X_n \to X_n \mid \sigma\text{は全単射}\}$$

である．

定義 3 (一般線形群，p-元体). K を体として，$M_n(K)$ を K 上の n 次正方行列全体とする．$M_n(K)$ に属する正則行列全体は通常の行列の積に関して群をなす．この群を K 上の $\boldsymbol{n}$ **次一般線形群**と呼び，$GL_n(K)$ と表す．すなわち，

$$GL_n(K) := \{A \in M_n(K) \mid \det(A) \neq 0\}$$

である．また，p を素数とするとき，$\mathbb{Z}/p\mathbb{Z}$ は体である．この体を $\boldsymbol{p}$ **-元体**と呼び，$\mathbb{F}_p$ と表す．すなわち，

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

である．

補題 4 ($GL_n(\mathbb{F}_p)$ の位数). $GL_n(\mathbb{F}_p)$ の位数は,

$$\left|GL_n(\mathbb{F}_p)\right| = p^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}(p^k-1) \tag{2.1}$$

である.

[証明]. 正則行列であるということは基底を並べたものになっている. よって, n 個の線形独立な $\mathbb{F}_p$ の元からなる n 次ベクトルの取り方を考えれば良い. 1 列目の取り方が p^n-1 通り, 2 列目は 1 列目と線形独立なので, p^n-p 通りとなる. すなわち,

$$\begin{aligned}\left|GL_n(\mathbb{F}_p)\right| &= (p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}) \\ &= p^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}(p^k-1)\end{aligned}$$

となる. (詳しくは [3, p. 41] の Proposition 2 を参照されたい) □

2.2 部分群から派生する群

群 G の空でない部分集合 H が G 上の演算に関して閉じていて, 且つ H の任意の元の逆元を H に含むとき H を G の**部分群**という. 後に紹介する Sylow の定理において Sylow 部分群の個数を決定するために正規化群というものを考える. このように, 部分群から派生するような群をここでは紹介する.

定義 5 (共役部分群, 正規部分群, 正規化群). H を群 G の部分群, $\sigma \in G$ とする.

(1) $\sigma H\sigma^{-1}$ もまた G の部分群になり, これを H の**共役部分群**という. 位数は H と同じで,

$$|\sigma H\sigma^{-1}| = |H|$$

が成り立つ.

(2) H と H の任意の共役部分群が一致するとき, すなわち,

$$\forall\sigma \in G, \quad \sigma H\sigma^{-1} = H$$

となるとき, H を**正規部分群**といい, $H \lhd G$ と表す. また, 可換群の部分群は全て正規部分群となる.

(3) $H \subset M \subset G$ となる部分群 M に対して, H が M の正規部分群であるような最大の部分群 M を H の**正規化群**といい $N_G(H)$ と表す. すなわち,

$$N_G(H) := \{\sigma \mid H = \sigma H\sigma^{-1}\}$$

である.

例 6 (部分群の例)**.** 群 G を $\mathfrak{S}_3$ として，互換を (i,j) のように表す．$H=\{\varepsilon,\ (1,2)\}$ のとき，$\sigma=(1,3)$ とすると，H の共役部分群は，

$$\sigma H\sigma^{-1}=\{\varepsilon,\ (2,3)\}$$

となる．また，H の正規化群 $N_G(H)$ は，

$$N_G(H)=\{\varepsilon,\ (1,2)\}=H$$

となる．また，$\mathfrak{S}_3$ の正規部分群は $\mathfrak{S}_3$ の偶置換全体がなす群 A_3 となる．すなわち，

$$A_3=\{\varepsilon,\ (1,2,3),\ (1,3,2)\},\quad A_3\lhd\mathfrak{S}_3$$

である．

2.3 剰余類

この節では群をその部分群に関して剰余類分解する，ということを定義していく．特に，Lagrange の定理に関しては Sylow 部分群の構造を把握する上で大いに役に立つ定理である．

定義 7 (剰余類、剰余類分解)**.** $\sigma\in G$ に対して，σ に右から H の元を掛けて得られる元全体の集合を σH と書き，σ の H に関する**右剰余類**と呼ぶ．すなわち，

$$\sigma H:=\{\sigma\xi\mid\xi\in H\}$$

である．また，G は相異なる H の右剰余類の共通部分の無い和集合として表すことができる．すなわち，

$$G:=\coprod_{j\in J}\tau_jH$$

であり，これを (H に関する G の) **右剰余類分解**と呼ぶ．また，相異なる右剰余類全体を集めた集合を考え，それを G/H と表す．すなわち，

$$G/H:=\{\tau_jH\mid j\in J\}$$

である．この $\{t_j\ (j\in J)\}$ を G/H の代表系と呼ぶ．

ここで，群 G の，部分群 H の正規化群 $N_G(H)$ の右剰余類を考える．すると，$G/N_G(H)$ の元と H の共役部分群は一対一に対応している．すなわち，

$$\begin{cases}G/N_G(H)\longleftrightarrow\{\sigma H\sigma^{-1}\mid\sigma\in G\}\\ \sigma N_G(H)\longleftrightarrow\sigma H\sigma^{-1}\end{cases}$$

と対応している．

定義 8 (両側分解)．$H,\ K$ を群 G の部分群とする．$a,\ b \in G$ の分類を，

$$a \sim b \iff \exists h \in H,\ \exists k \in K\ s.t.\ b = hak$$

のようにして決めると，剰余類分解と同じように G の分割が得られ，

$$G = \coprod_{\lambda \in \Lambda} H a_\lambda K$$

となる．これを $H,\ K$ による G の**両側分解**と呼び，$H \backslash G / K$ と表す．

定義 9 (指数)．G/H の元の個数を G における H の**指数**と呼び，$|G : H|$ と表す．すなわち，

$$|G : H| = |G/H|$$

である．

定理 10 (Lagrange の定理)．H を群 G の部分群とする．$|H|$ は $|G|$ の約数であって，

$$|G| = |G : H||H|$$

が成り立つ．

証明は [1, p. 216] の定理 3.34 を参照されたい．

定理 10 の逆，すなわち,「有限群の位数の約数を位数とする部分群は必ず存在する」という命題は成り立たない．反例の一つとしては，4 次交代群 A_4 は位数 6 の部分群をもたないことがわかっている．([1, p. 245] の例題 3.7 参照)

また，Lagrange の定理より位数が素数の群 G を考えると，部分群は $\{\varepsilon\}$ か G しかないことがわかる．したがって，$\sigma\ (\neq \varepsilon)\ \in G$ としたとき，σ で生成された部分群 $\langle \sigma \rangle$ は G に一致する．よって，G は σ を生成元とする巡回群となる．すなわち，

$$G = \langle \sigma \rangle$$

である．

2.4 群の作用・軌道

定義 11 (作用)．X を集合とする．$\forall \sigma \in G,\ \forall x \in X$ に対し、$\sigma \cdot x \in X$ が定まっている．すなわち，

$$f : G \times X \to X, \quad (\sigma, x) \longmapsto \sigma \cdot x \quad ((\sigma, x) \in G \times X)$$

となるような写像 f が定まっているとする．この f が (1)(2) を満たすとき，G **は** X **へ作用する**といい，$G \curvearrowright X$ と表す．

(1) $\forall\sigma, \tau \in G, \forall x \in X$ に対し，$\sigma \cdot (\tau \cdot x) = (\sigma * \tau) \cdot x$ が成り立つ．

(2) $\forall x \in X$ に対し，$\varepsilon \cdot x = x$ が成り立つ．

定義 12 (軌道、固定群)**.** 群 G が集合 X に作用しているとし，$x \in X$ とする．σ が G の元すべてを動くとき，$\sigma \cdot x$ 全体の集合を，(G の作用に関する) x の**軌道**と呼び、$\mathcal{O}(x)$ と表す．すなわち，

$$\mathcal{O}(x) := \{\sigma\cdot \mid \sigma \in G\} \subset X$$

である．x を $\mathcal{O}(x)$ の代表元と呼ぶ．また，x を動かさない G の元全体を (G の作用に関する) x の**固定群**と呼び，G_x と表す．すなわち，

$$G_x := \{\sigma \in G \mid \sigma \cdot x = x\}$$

である．

定義 13 (軌道分解)**.** x_j を軌道 $\mathcal{O}(x_j)$ の代表元とする．X を軌道の共通部分の無い和として表すことができる．すなわち，

$$X = \coprod_{j \in J} \mathcal{O}(x_j)$$

であり，こうして得られる分割を，(G の作用に関する)X の**軌道分解**と呼ぶ.

3 Sylow の定理

本論文では主に Sylow 部分群の性質を研究する．Sylow 部分群は Sylow の定理により存在が保証されているが，まず，これを証明する．

定理 14 (Sylow の定理 I(存在))**.** G を有限群とし，$n = |G|$ を位数とする．p を素数とする．p^e を n を割り切る p のベキで最大のもの ($e \geq 0$) とすると，G の部分群で位数が p^e に等しいものが (少なくとも 1 つ) 存在する．これを G の ***p*-Sylow 部分群**と呼ぶ.

このように群 G の位数の約数のうち特殊な約数 p^e に関して，位数が p^e となる G の部分群が必ず存在する，というのが Sylow の定理である．Lagrange の定理の際にも紹介したように，$|G|$ の一般の約数 m に対して，位数 m の部分群が存在するとは限らない．

[証明]. (Sylow の定理 I(存在)) G の部分集合で元の個数が p^e に等しいもの全体の集合を $\mathcal{X}$ とする．すなわち，

$$\mathcal{X} = \{A \mid A \subset G,\ |A| = p^e\}$$

である．また，$\sigma \in G$，$A \in \mathcal{X}$ に対して，

$$\sigma \cdot A = \{\sigma * \rho \mid \rho \in A\}$$

と定めれば，$\sigma \cdot A \in \mathcal{X}$ である．また，対応 $(\sigma, A) \to \sigma \cdot A$ によって，G の $\mathcal{X}$ への作用が定まる．この作用の軌道分解を，

$$\mathcal{X} = \coprod_{j=1}^{t} \mathcal{O}(A_j) \quad (A_j \in \mathcal{X}) \tag{3.1}$$

とする．また，軌道の代表元 A_j の固定群を G_j で表す．すなわち，

$$G_j = \{\sigma \in G \mid \sigma \cdot A_j = A_j\} \quad (j = 1,\ \cdots,\ t)$$

である．

補題 15. 以上の記号の下に，次の (1) – (3) が成り立つ．

(1) $|\mathcal{X}| \not\equiv 0 \pmod{p}$ が成り立つ．

(2) $|G_j| \leq p^e \quad (j = 1,\ \cdots,\ t)$ が成り立つ．

(3) $\exists j'\ (1 \leq j' \leq t)$ が存在して，$(G : G_{j'}) \not\equiv 0 \pmod{p}$ が成り立つ．

[証明]. (1) $\mathcal{X}$ の定義より，

$$|\mathcal{X}| = \binom{n}{p^e} = \binom{p^e m}{p^e} \text{ (二項係数)}$$

(ただし，m を $\gcd(p,\ m) = 1$ を満たす自然数とする．) となる．$\mathbb{F}_p$ 上の多項式環 $\mathbb{F}_p(T)$ の中で考える．$(1+T)^n \in \mathbb{F}_p(T)$ の T^{p^e} の係数を α とする $(\alpha \in \mathbb{F}_p)$．まず，$a = 1,\ b = T$ とすると，二項定理より，

$$\alpha = \binom{n}{p^e} = \binom{p^e m}{p^e} \quad (\in \mathbb{F}_p)$$

となる．ここで，$\mathrm{Frob}_p : \mathbb{F}_p \to \mathbb{F}_p$(Frobenius 写像) を考えると，

$$(1+T)^p = \mathrm{Frob}_p(1+T) = \mathrm{Frob}_p(1) + \mathrm{Frob}_p(T) = 1 + T^p$$

が得られる．これを繰り返すと，

$$(1+T)^{p^e} = 1 + T^{p^e} \quad (\mathbb{F}_p(T) \text{ の元として等しい}) \tag{3.2}$$

となる．式 (3.2) の両辺を m 乗して，T^{p^e} の係数を比較する．式 (3.2) の左辺の m 乗は $(1+T)^n$ に等しいので，T^{p^e} の係数は α である．また，式 (3.2) の右辺を m 乗した式の T^{p^e} の係数は m に等しい．したがって，$\alpha = m$ である．このことと式 (3.2) より，

$$\binom{p^e m}{p^e} = m\ (= \alpha)$$

である．この等式を整数の合同式として表すと，

$$\binom{p^e m}{p^e} \equiv m \pmod p$$

いま，$m \neq 0$ となるため，

$$|\mathcal{X}| = \binom{p^e m}{p^e} \not\equiv 0 \pmod p$$

が成り立つ．(詳しくは [1][p. 148] 例題 2.6 参照を参照されたい)
(2) $\rho_0 \in A_j$ に対し，写像 $f : G_j \to A_j$ を，

$$f(\sigma) = \sigma * \rho_0 \quad (\sigma \in G_j)$$

として定める．すると，$\sigma,\ \sigma^{'}$ について，

$$\sigma * \rho_0 = \sigma^{'} * \rho_0 \implies \sigma = \sigma^{'}$$

が成り立つので，f は単射である．したがって $|G_j| \leq |A_j| = p^e$ が成り立つ．
(3) 式 (3.1) の両辺の元の個数を考えると，

$$|\mathcal{X}| = \sum_{j=1}^{t} |\mathcal{O}(A_j)|$$

が成り立つ．この等式と補題 15(1) から，$|\mathcal{O}(A_j)| \not\equiv 0 \pmod{p}$ をみたす $j^{'}$ が (少なくとも 1 つ) 存在することがわかる $(1 \leq j^{'} \leq t)$．また，$|\mathcal{O}(A_{j'})| = |G : G_{j'}|$ であることから補題 15(3) が成り立つ． □

(証明 (Sylow の定理 I(存在)) の続き)
補題 15(3) の条件をみたす G の部分群 $G_{j'}$ を 1 つとり，それを H とおく $(H = G_{j'})$．すると，

$$(G : H) = \frac{|G|}{|H|} \not\equiv 0 \pmod p$$

であり，$|H|$ は p^e の倍数である．一方，補題 15(2) より，

$$|H| \leq p^e$$

が成り立っている．したがって $|H| = p^e$ となる．この H が求めていた部分群 (の 1 つ) である． □

3.1 p-Sylow 部分群

Sylow の定理によって存在が示された位数 p^e の部分群の一つを S_p と書く．すなわち，

$$|S_p| = p^e$$

である．このような p-Sylow 部分群 S_p の構造を考察するのが本節の主題である．ここでは主に [2] を参考にした．

3.2 p-Sylow 部分群の個数

まず，Sylow 部分群 S_p の共役性や個数に関する性質を述べる．

定理 16 (Sylow の定理 II(共役性))．

(1) p-Sylow 部分群はすべて互いに共役である．

(2) p-Sylow 部分群の個数を n_p とすると，

$$\begin{cases} n_p = |G : N_G(S_p)| \\ n_p \equiv 1 \pmod{p} \end{cases}$$

が成り立つ．

[証明]．(Sylow の定理 II(共役性))
(1) S_p, S_p' を G の p-Sylow 部分群とする．S_p, S_p' による G の両側分解 $S_p \backslash G / S_p'$ を，

$$G = \coprod_{i=1}^{r} S_p \sigma_i S_p'$$

とする．$S_p \sigma_i S_p'$ に含まれる S_p の左剰余類の個数は，

$$p^{e_i} = |S_p' : \sigma_i^{-1} S_p \sigma_i \cap S_p'| \quad (e_i \geq 0)$$

に等しいから，S_p の左剰余類全部の個数，すなわち，$|G : S_p|$ は，

$$|G : S_p| = p^{e_1} + p^{e_2} + \cdots + p^{e_r}$$

と表される．この左辺は p と素であるから，$p^{e_i} = 1$ となる i が存在する．このとき，

$$|S_p' : \sigma_i^{-1} S_p \sigma_i \cap S_p'| = 1, \quad S_p' = \sigma_i^{-1} S_p \sigma_i \cap S_p'$$

が成り立つ．また，$|S_p'| = |\sigma_i^{-1} S_p \sigma_i| = p^e$ であることから，

$$S_p' = \sigma_i^{-1} S_p \sigma_i$$

が成り立つ．

(2) $N_G(S_p)$ に関する G の右剰余類分解を，

$$G/N_G(S_p) = \coprod_{\lambda\in\Lambda} \sigma_\lambda N_G(S_p), \quad \{\sigma_\lambda\} \text{ は代表系}$$

とすると，$n \in N_G(S_p)$ に対して，

$$\begin{aligned}(\sigma_\lambda n)S_p(\sigma_\lambda n)^{-1} &= \sigma_\lambda(nS_pn^{-1})\sigma_\lambda^{-1}\\ &= \sigma_\lambda S_p\sigma_\lambda^{-1}\end{aligned}$$

が成り立つ．また，(1) により，S_p, S_p' は共役なので，相異なる S_p の個数は，$N_G(S_p)$ に関する (G の) 相異なる右剰余類の個数に等しい．すなわち，

$$n_p = |G : N_G(S_p)|$$

である．また，$N_G(S_p)$, S_p による G の両側分解 $N_G(S_p)\backslash G/S_p$ を，

$$G = \coprod_{i=1}^{r} N_G(S_p)\sigma_i S_p \quad (\sigma_1 = \varepsilon \in G \text{ とする.})$$

とし，$1 \leq i \leq r$ に対して，

$$p^{e_i} = (S_p : \sigma_i^{-1}S_p\sigma_i \cap S_p), \quad (\text{ただし，} p^{e_1} = 1 \text{ とする.})$$

とおく．いま，$p^{e_i} = 1$ $(i > 1)$ となる i が存在すると仮定すると，

$$S_p \subset \sigma_i^{-1}N_G(S_p)\sigma_i \implies \sigma_i S_p \sigma_i^{-1} \subset N_G(S_p)$$

となり，S_p, $\sigma_i S_p \sigma_i^{-1}$ はともに $N_G(S_p)$ の $p-$Sylow 部分群である．しかし，S_p は $N_G(S_p)$ の正規部分群であるから，

$$S_p = \sigma_i S_p \sigma_i^{-1}, \quad (\sigma_i \in N_G(S_p)) \implies N_G(S_p)\sigma_i S_p = N_G(S_p)\sigma_1 S_p$$

となり，これは $i > 1$ に矛盾する．したがって，

$$|G : N_G(S_p)| = 1 + \sum_{i=2}^{r} p^{e_i} \quad (e_i \geq 1) \ \equiv 1 \pmod{\mathrm{p}}$$

□

4　$GL_2(\mathbb{F}_p)$ の Sylow 部分群

以下，上記で示したような p-Sylow 部分群が実際にどのような構造をしているのか，有限群として $GL_2(\mathbb{F}_p)$ を例に考察する．構造を考察する上で，まず，p-Sylow 部分群の位数が素数であるか否か (すなわち，$e = 1$ か $e > 1$) で分類し考える．具体的には，

- $e = 1$ のとき
  定理 1(Lagrange の定理) より p-Sylow 部分群は巡回群となる．よって PC を用いて位数 p の元を探し，正規化群を計算することで全て算出されているかを確認した．実際には自ら C 言語でプログラミングをしたのだが結果に明らかな誤りが生じることもあった為，正規化群を必ず計算した．

- $e > 1$ のとき
  p^e の約数を位数とする元を PC を用いて求め，その元を生成元とする巡回群の正規化群のうち位数が p^e となるものを探索した．

といった方法で p-Sylow 部分群の探索と構造の考察をおこなった．また，元の位数を確認するにあたり，同じ固有多項式を持つ行列は同じ位数になるという予想がたったため，それも確認する．

4.1　$G = GL_2(\mathbb{F}_2)$ $(p = 2)$ の Sylow 部分群

まず，もっとも簡単な例として $GL_2(\mathbb{F}_2)$ で計算をおこなった．式 (2.1) より位数は，

$$|GL_2(\mathbb{F}_2)| = 2 \cdot 3$$

である．また，簡単な乗積表を考えれば $GL_2(\mathbb{F}_2) \cong \mathfrak{S}_3$ である．6 個しか元がないため具体的に書き表すと，

$$GL_2(\mathbb{F}_2) = \left\{ E_2, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

である．ここで E_2 は単位行列 ($GL_2(\mathbb{F}_2)$ の単位元) を表す．この中から位数 2 の部分群と位数 3 の部分群を探索する．位数が素数のため巡回群となるため実際に計算し，位数 2, 3 の元を探した．結果としては以下のようになった．

定理 17 ($GL_2(\mathbb{F}_2)$ の Sylow 部分群)**.** $GL_2(\mathbb{F}_2)$ の Sylow 部分群は次のようになる．

- 2-Sylow 部分群

$$\left\{ E_2, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}, \left\{ E_2, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}, \left\{ E_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

また，位数 2 の元の固有多項式 $\Phi_A(x)$ は，

$$\Phi_A(x) = x^2 + 1$$

となる．

- 3-Sylow 部分群

$$\left\{ E_2,\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

また，位数 3 の元の固有多項式 $\Phi_A(x)$ は，

$$\Phi_A(x) = x^2 + x + 1$$

となる．

[証明].

- 2-Sylow 部分群 $|S_2| = 2$
個数が少ないので，網羅的に計算して，位数 2 の元からなる巡回群を探すと，

$$\left\{ E_2,\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\},\ \left\{ E_2,\ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\},\ \left\{ E_2,\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

となった．また，一般的には定理 18 のように計算するのが良い．定理 16 より，

$$n_2 \equiv 1 \pmod p$$

となる．また，定理 10 より，$n_2 = 1,\ 3$ のため，上記で全てであることがわかる．実際の計算としては，

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \equiv E_2 \pmod 2$$

のようにして元の位数が 2 であることがわかる．

- 3-Sylow 部分群 $|S_3| = 3$
同様に，位数 3 の元からなる巡回群を探すと，

$$\left\{ E_2,\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

となった．定理 16 より，

$$n_3 \equiv 1 \pmod p$$

となる．また，定理 10 より，$n_3 = 1$ のため，上記で全てであることがわかる． □

4.2　$G = GL_2(\mathbb{F}_3)$ $(p=3)$ の Sylow 部分群

式 (2.1) より位数は，

$$|GL_2(\mathbb{F}_3)| = 2^4 \cdot 3$$

である．

定理 18 ($GL_2(\mathbb{F}_3)$ の Sylow 部分群)**.** $GL_2(\mathbb{F}_3)$ の Sylow 部分群は次のようになる．

- 2-Sylow 部分群

$$N_G\left(\left\langle\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\right\rangle\right)$$

- 3-Sylow 部分群

$$\left\langle\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}2 & 1\\ 2 & 0\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0 & 1\\ 2 & 2\end{pmatrix}\right\rangle$$

また，位数 3 の元の固有多項式 $\Phi_A(x)$ は，

$$\Phi(x) = x^2 - 2x + 1$$

となる．

[証明].

- 2-Sylow 部分群 $|S_2| = 2^4$
PC 上の計算では位数 2^4 の元は存在しなかった (2-Sylow 部分群の構造は巡回群ではない)．2^4 の約数を位数に持つ元としては，位数 2, 4, 8 の元があったため，位数 8 の巡回群の正規化群から考える．そこで，

$$A = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\quad T = \langle A\rangle : \text{位数 } 8 \text{ の巡回群}$$

を例にとって計算をしていく．正規化群の計算の簡易化のために A の対角化を考える．そのため A の固有多項式 $\Phi_A(x)$ の根を考えると，

$$\Phi_A(x) = x^2 - x - 1$$

$$\Phi_A(0) = 2,\ \Phi_A(1) = 2,\ \Phi_A(2) = 1$$

となり，$\mathbb{F}_3$ 上では因数分解不可能であることがわかる．したがって，$\Phi_A(x)$ の根の1つを α とすると，

$$\begin{array}{ll} \alpha & \alpha^5 = 2\alpha \\ \alpha^2 = \alpha + 1 & \alpha^6 = 2\alpha + 2 \\ \alpha^3 = 2\alpha + 1 & \alpha^7 = \alpha + 2 \\ \alpha^4 = 2 & \alpha^8 = 1 \end{array}$$

となり，またもう1つの根を β とすると，

$$\begin{cases} \alpha + \beta = 1 \\ \alpha\beta = 2 \end{cases} \implies \beta = \frac{2}{\alpha} = 2\alpha + 1 = \alpha^3$$

となる．したがって，$\Phi_A(x)$ の根は $\alpha,\ \alpha^3$ となる．よって，$\mathbb{F}_3$ に α を添加した拡大体 $\mathbb{F}_3(\alpha)$ 上では $\Phi_A(x)$ は根を持ち，$GL_2(\mathbb{F}_3(\alpha))$ 上では対角化が可能である．また，上記に示した様に $\alpha^n(n \geq 2)$ は α の一次式で表せるため，$\mathbb{F}_3(\alpha)$ は α の一次式で表せる．すなわち，

$$\mathbb{F}_3(\alpha) = \{a\alpha + b \mid a, b \in \mathbb{F}_3\}, \quad |\mathbb{F}_3(\alpha)| = 9$$

となる．$\widetilde{G} = GL_2(\mathbb{F}_3(\alpha))$ とすると，対角化行列 $P \in \widetilde{G}$ は,

$$P = \begin{pmatrix} \alpha & \alpha^3 \\ 1 & 1 \end{pmatrix}, \quad P^{-1}AP = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^3 \end{pmatrix} = \gamma$$

となる．また，$S = \langle\gamma\rangle$ とし，

$$\begin{cases} N_G(T) = \{g \in G \mid gTg^{-1} = T\} \\ N_{\widetilde{G}}(S) = \{\sigma \in \widetilde{G} \mid \sigma S\sigma^{-1} = S\} \\ \widetilde{N} = \{B \in N_{\widetilde{G}}(S) \mid PBP^{-1} \in GL_n(\mathbb{F}_3)\} \end{cases}$$

とすると，

$$\begin{aligned} \sigma\gamma &= PgP^{-1} \cdot PAP^{-1} \\ &= PgAP^{-1} \\ &= PAgP^{-1} \\ &= PAP^{-1} \cdot PgP^{-1} \\ &= \gamma\sigma \end{aligned}$$

であることから，$|N_G(T)| = |\widetilde{N}|$ となる．よって $|\widetilde{N}|$ を計算する．したがって，

$$\begin{cases} \sigma\gamma\sigma^{-1} = \gamma^k \ (\exists k) \\ \det\sigma \neq 0 \end{cases}$$

をみたす σ を計算すると，

$$\sigma = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ or } \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \quad a, b \in \mathbb{F}_3(\alpha)$$

となる．このうちで $P\sigma P^{-1} \in GL_2(\mathbb{F}_3)$ をみたすものを計算すると，

$$|\widetilde{N}| = 16$$

となる．$|N_G(T)| = |\widetilde{N}| = 16$ より，$N_G(T)$ は $GL_2(\mathbb{F}_3)$ の 2-Sylow 部分群であることがわかった．相異なる位数 8 の巡回群は 3 個存在するため，共役であるが相異なる $N_G(T)$ も 3 個存在する．また，定理 16 より，

$$n_2 \equiv 1 \pmod{p}$$

となる．定理 10 より，$n_2 = 1,\ 3$ のため，上記で全てである．

- 3-Sylow 部分群 $|S_3| = 3$
  PC を用いて位数 3 の元を算出し，巡回群の形にまとめると，

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} \right\rangle$$

となる．以下，正規化群を求め，n_3 を計算する．

$$U = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_3) \mid k = 0, 1, 2 \right\}$$

とすると，

$$N_G(U) = \{A \in GL_2(\mathbb{F}_3) \mid AU = UA\}$$

であるため，条件をみたす A を計算すると，

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

または，

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

となる．また，$ad - bc \neq 0$ に注意すると，

$$N_G(U) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F}_3,\ ac \not\equiv 0 \pmod{3} \right\}$$

である．したがって $|N_G(U)| = 12$ となり，定理 16 より，

$$n_3 = \frac{48}{12} = 4$$

となり，上記で全てであることがわかる． □

4.3 $G = GL_2(\mathbb{F}_5)$ $(p=5)$ の Sylow 部分群

式 (2.1) より位数は,

$$|GL_2(\mathbb{F}_5)| = 2^5 \cdot 3 \cdot 5$$

である.

定理 19 ($GL_2(\mathbb{F}_5)$ の Sylow 部分群). $GL_2(\mathbb{F}_5)$ の Sylow 部分群は次のようになる.

- 2-Sylow 部分群 (以下の 15 個存在する.)

$$N_G\left(\left\langle\begin{pmatrix}0&2\\2&0\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}0&1\\4&0\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}1&1\\3&4\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}1&3\\1&4\end{pmatrix}\right\rangle\right)$$

$$N_G\left(\left\langle\begin{pmatrix}3&0\\0&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}3&0\\1&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}3&0\\2&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}3&0\\3&2\end{pmatrix}\right\rangle\right)$$

$$N_G\left(\left\langle\begin{pmatrix}3&0\\4&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}3&1\\0&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}3&2\\0&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}3&3\\0&2\end{pmatrix}\right\rangle\right)$$

$$N_G\left(\left\langle\begin{pmatrix}3&4\\0&2\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}4&1\\3&1\end{pmatrix}\right\rangle\right),\ N_G\left(\left\langle\begin{pmatrix}4&3\\1&1\end{pmatrix}\right\rangle\right)$$

- 3-Sylow 部分群 (以下の 10 個存在する.)

$$\left\langle\begin{pmatrix}0&1\\4&4\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0&2\\2&4\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0&3\\3&4\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0&4\\1&4\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}1&1\\2&3\end{pmatrix}\right\rangle$$

$$\left\langle\begin{pmatrix}1&2\\1&3\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}1&3\\4&3\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}1&4\\3&3\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}2&1\\3&2\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}2&2\\4&2\end{pmatrix}\right\rangle$$

- 5-Sylow 部分群 (以下の 6 個存在する.)

$$\left\langle\begin{pmatrix}0&1\\4&2\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0&2\\2&2\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0&3\\3&2\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}0&4\\1&2\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}1&0\\1&1\end{pmatrix}\right\rangle,\ \left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$$

[証明].

- 2-Sylow 部分群 $|S_2| = 2^5$
  PC 上の計算では位数 2^5 の元は存在しなかった (2-Sylow 部分群の構造は巡回群ではない). よって, $GL_2(\mathbb{F}_3)$ の $2-$Sylow 部分群と同様に 2^5 の約数を位数に持つ元を探

索したところ，位数 2, 4, 8, の元が存在した．したがって，位数 8 から考察する．そこで，

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}, \quad T = \langle A \rangle : \text{位数 } 8 \text{ の巡回群}$$

を例にとって計算すると，

$$N_G(T) = \{g \in G \mid gTg^{-1} = T\}, \quad |N_G(T)| = 48$$

となり，不適であった．次に位数 4 を考察する．

$$B = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \quad S = \langle B \rangle : \text{位数 } 4 \text{ の巡回群}$$

を例にとって計算すると，

$$N_G(S) = \{\sigma \in G \mid \sigma S \sigma^{-1} = S\}, \quad |N_G(S)| = 32$$

となった．したがって，位数 4 の巡回群の正規化群が 2-Sylow 部分群であることがわかった．また，B と同じ固有方程式 $\Phi(x)$ を持つ位数 4 の元は 30 個 (15 組) 存在する．よって，同じ $\Phi(x)$ を持つ元を生成元とする相異なる位数 4 の巡回群は 15 個存在する．したがって，共役であるが相異なる $N_G(T)$ も 15 個存在することがわかった．また，定理 16 より，

$$n_2 \equiv 1 \pmod{p}$$

となる．定理 10 より，$n_2 = 1,\ 3,\ 5,\ 15$ のため，上記で全てである．

- 3-Sylow 部分群 $|S_3| = 3$
  PC を用いて位数 3 の元を算出し，巡回群の形にまとめると，

$$\left\langle \begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 2 \\ 2 & 4 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 3 \\ 3 & 4 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \right\rangle$$

$$\left\langle \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 4 \\ 3 & 3 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 2 \\ 4 & 2 \end{pmatrix} \right\rangle$$

となる．正規化群の位数を計算し，個数を算出するために，

$$T = \left\langle \begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix} \right\rangle = \left\{ E_2,\ A = \begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix},\ B = \begin{pmatrix} 4 & 4 \\ 1 & 0 \end{pmatrix} \right\}$$

を例にとって計算すると，

$$N_G(T) = \{g \in G \mid gAg^{-1} = A \text{ or } B\}, \quad |N_G(T)| = 48$$

となる．定理 16 より，

$$n_3 = \frac{480}{48} = 10$$

となり，上記で全てであるとわかる．

- 5-Sylow 部分群 $|S_5| = 5$
  3-Sylow 部分群と同様にして計算すると，

$$\left\langle \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0 & 4 \\ 1 & 2 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$T = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{F}_5 \right\}, \quad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$N_G(T) = \{g \in G \mid gAg^{-1} = A^k \ (\exists k)\}, \quad |N_G(T)| = 80$$

となる．よって，

$$n_5 = \frac{480}{80} = 6$$

となり，上記で全てであるとわかる． □

4.4 一般の素数 p の場合に関する考察

$GL_2(\mathbb{F}_p)$ の Sylow 部分群の構造は大きく二つに分類される．それは，

- (Type I) Sylow 部分群の位数が素数の場合
- (Type II) Sylow 部分群の位数が素数の 2 次以上の冪の場合

の 2 つである．上の場合に関しては定理 10(Lagrange の定理) から巡回群であることがわかっている．また，$GL_2(\mathbb{F}_p)$ の p-Sylow 部分群に関しては，次の定理が成り立つ．

定理 20. $GL_2(\mathbb{F}_p)$ の p-Sylow 部分群は，

$$U = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_p) \mid k = 0, 1, \ldots, p-1 \right\}$$

のような部分群 U の共役部分群となり，$p+1$ 個存在する．

[証明]. $GL_2(\mathbb{F}_p)$ の p-Sylow 部分群は，

$$|GL_2(\mathbb{F}_p)| = p(p-1)(p^2-1)$$

$$(p-1)(p^2-1) \equiv 1 \pmod p$$

より，位数が p である．また，

$$U = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_p) \mid k = 0, 1, \ldots, p-1 \right\}$$

のような対角成分が全て 1 の上半三角行列全体は常に位数 p の巡回群になっている．また，$N_G(U)$ は,

$$A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} A, \quad \det\ A \neq 0, \quad (k = 1,\ \cdots,\ p-1)$$

を満たすような A を考えると，

$$N_G(U) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in GL_2(\mathbb{F}_p) \mid a \equiv ck \pmod{p},\ k = 1,\ \cdots,\ p-1 \right\}$$

となり，位数を考えると，

$$|N_G(U)| = p(p-1)^2$$

となる．($N_G(U)$ は $GL_2(\mathbb{F}_p)$ のボレル部分群である．) また，定理 16 より，

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

となる． □

(Type I) の場合は他にも $p+1$ の素因数の場合が考えられる．また，(Type Ⅱ) の場合に関しては，2-Sylow 部分群の場合は，$p = 3,\ 5$ では 2^e の約数を位数とする巡回群の正規化群となっていることが観察された．しかし，$p = 3,\ 5$ では p と異なるのは 2-Sylow 部分群しか存在しないので，参考にならなかった．そのような理由で，奇素数の冪 (Type Ⅱ) の場合に関しては時間不足のため研究できていない．

5 結論

本研究では $GL_2(\mathbb{F}_p)$ の p-Sylow 部分群の構造を把握することを目的として考察を重ねた．何をもってその構造を把握したと言えるのか，というのは難しい問いであると思うが，私は一つの目標として「生成元と関係式による表示を与えること」を目指していた．結果としては，$GL_2(\mathbb{F}_p)$ の p-Sylow 部分群は位数が素数であれば巡回群である．また，素数でなければ $p = 2,\ 3,\ 5$ では，巡回群の正規化群になっているということが観察された．今後の課題は，$p \geq 7$ のときに Sylow 部分群の一般的な性質について考えることであるが，特に，

- 位数が素数の 2 次以上の冪の場合の Sylow 部分群の構造
- 行列の次数を上げた際の (つまり $G = GL_n(\mathbb{F}_p)$)Sylow 部分群の構造
- 生成元と関係式による表示の考察

が今後の課題として挙げられる．また，生成元と関係式による表示を考察する場合，$SL_n(\mathbb{F}_p)$ の p-Sylow 部分群に関しても考える必要があり ([4] 参照)，そちらの構造の考察に関しても今後研究したいと思う．

6 謝辞

本研究を行うにあたって，西山享教授には，セミナーや論文の添削など，丁寧かつ熱心なご指導を頂きました．ここに，深甚なる謝意を表します．また，中間発表や卒業研究発表の場でご助言頂いた，中山教授，古川教授，増田准教授にも深謝いたします．最後に，多くの有意義な意見を与えてくださった同研究室所属の院生並びに学部生の皆様にも，感謝致します．

参考文献

[1] 中島匠一，代数と数論の基礎，共立出版，2000．

[2] 浅野啓三・永尾汎，群論，岩波全書，1965．

[3] J.L. Alperin and Rowen B. Bell，*Groups and representations*，GTM162，Springer-Verlag New York，1995．

[4] 佐藤隆夫，群の表示，近代科学社，2017．

[5] 菅亮輔，正多面体に内接する図形と p-Sylow 部分群，青山学院大学理工学部物理・数理学科卒業論文 (2017 年度)