幾何的視点から観たLucas数列～3階の場合

中央大学大学院 理工学研究科 数学専攻
齊藤暢 (Mitsuru Saitoh)

序

本稿は２０１９年の８月に九州大学で開催された第１３回福岡整数論研究集会で発表した「幾何的視点から観たLucas数列～3階の場合」を第１６回数学総合若手研究集会のために再編したものである．福岡整数論研究集会での講演は整数論研究者を対象としていたが，数学総合若手研究集会はより広い分野の方々との交流を図るとの趣旨であることから，内容に加除を施した．

本講演ではLucas数列を幾何的視点から考察する方法について，特に3階の場合を取り上げて説明する．線型漸化式

$$w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1} w_{k+1} + P_n w_k \ (P_1, \ldots, P_{n-1}, P_n \in \mathbb{Z},\ w_0, w_1, \ldots, w_{n-1} \in \mathbb{Z})$$

によって定義される数列 $(w_k)_{k\geq 0}$ は様々な観点から，例えば整数論や組み合わせ論において興味深い対象であり，膨大な結果が蓄積されている．特に，$n = 2$, $P_1 = 1$, $P_2 = 1$, $w_0 = 0$, $w_1 = 1$ の場合，$(w_k)_{k\geq 0}$ はFibonacci数列に他ならず，広くその名が知られている．

諏訪はWard [10]，Laxton [3][4]，青木/酒井 [1] で展開された議論を見直し，群スキームの理論を援用してLucas数列を幾何的に観る方法を提示した．2階の場合は [6][7] に詳述されており，一般の場合は [8] に概略が述べられている．

本論の第1節では，Lucas数列を学部1年の線型代数の観点で捉える方法について振り返る．次に，第2節で [8] の概略を3階の場合に限定して，また群スキームの引用は軽くして紹介する．最後に第3節ではLucas数列以外の線型漸化式を幾何的視点から観る方法について述べる．最後の小節で福岡整数論研究集会以降に得た結果を追加した．

本稿の題目「幾何的視点から観たLucas数列～3階の場合」は第１３回福岡整数論研究集会での講演題目そのままであるが，内容も重複している．第１３回福岡整数論研究集会報告集に論説「幾何的視点から観たLucas数列～3階の場合」が掲載される予定であるので，興味を持たれた方はそちらも参照していただきたい．

数学総合若手研究集会で講演する機会を与えてくださった世話人の方々にこの場を借りてお礼申し上げます．

1 Introduction

定義 1.1. $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1} t - P_n \in \mathbb{Z}[t]$ に伴うLucas数列とは，線型漸化式 $w_{k+n} = P_1 w_{k+n-1} + \cdots + P_{n-1} w_{k+1} + P_n w_k$ と初項 $L_0 = \ldots = L_{n-2} = 0$, $L_{n-1} = 1$ によって定義される数列 $(L_k)_{k\geq 0}$ のことをいう．

特に，$n = 2$ の場合は $P(t) = t^2 - Pt + Q$ と書き，(P, Q) に伴うLucas数列と呼ぶ．2階のLucas数列の一般項は次に示すBinetの公式としてよく知られている．

命題 1.2.（Binet の公式） α, β を二次方程式 $t^2 - Pt + Q = 0$ の根とする．$\alpha \neq \beta$ ならば，各 $k \geq 0$ に対して

$$L_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$$

が成り立つ．

本論の視点をはっきりさせるために，線型代数の講義でしばしば取り上げられる証明について振り返っておく．

$$A = \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}$$

とおくと，各 $k \geq 0$ に対して

$$\begin{pmatrix} L_k & L_{k+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} A^k$$

が成立する．ここで，$\begin{pmatrix} 1 & \alpha \end{pmatrix}, \begin{pmatrix} 1 & \beta \end{pmatrix}$ はそれぞれ α, β を固有値とする A の固有ベクトルなので，

$$A = \begin{pmatrix} 1 & \alpha \\ 1 & \beta \end{pmatrix}^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 1 & \beta \end{pmatrix}$$

これから，

$$A^k = \frac{1}{\alpha - \beta} \begin{pmatrix} -\alpha^k\beta + \alpha\beta^k & -\alpha^{k+1}\beta + \alpha\beta^{k+1} \\ \alpha^k - \beta^k & \alpha^{k+1} - \beta^{k+1} \end{pmatrix}$$

を，さらに $L_k = \dfrac{\alpha^k - \beta^k}{\alpha - \beta}$ を得る．

補足 1.2.1. $\alpha = \beta$ のときは，A の Jordan 分解

$$A = \begin{pmatrix} 0 & -\alpha^2 \\ 1 & 2\alpha \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} -\alpha & -\alpha^2 \\ 1 & \alpha \end{pmatrix}$$

を考えて，

$$A^k = \begin{pmatrix} (1-k)\alpha^k & -k\alpha^{k+1} \\ k\alpha^{k-1} & (1+k)\alpha^k \end{pmatrix}$$

を，さらに $L_k = k\alpha^{k-1}$ を得る．

Lucas 数列には多くの先行研究が残されている．特に可除性は大きな研究対象になっている．

定義 1.3. $(L_k)_{k\geq 0}$ を $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$ に伴う Lucas 数列とする．Lucas 数列 $(L_k)_{k\geq 0} \mod m$ の rank (あるいは，period) を，$L_k \equiv 0 \mod m, \ldots, L_{k+n-2} \equiv 0 \mod m$ (あるいは，$L_k \equiv 0 \mod m, \ldots, L_{k+n-2} \equiv 0 \mod m, L_{k+n-1} \equiv 1 \mod m$) を満たす正の整数 k が存在するとき，その最小値として定義する．また，Lucas 数列 $(L_k)_{k\geq 0} \mod m$ の rank (あるいは，period) を $r(m)$ (あるいは，$k(m)$) と書く．

$n = 2$ の場合には Lucas [5] がこの分野の出発点である次の結果を示した．

定理 1.4. (**Lucas の lois de l'apparition et la répétition**) P, Q を 0 でない整数，$(L_k)_{k\geq 0}$ を (P, Q) に伴う Lucas 数列とし，p を素数 > 2 とする．このとき，$p \nmid Q$ なら $(L_k)_{k\geq 0}$ の p を法とする rank $r(p)$ が存在する．さらに，$L_k \equiv 0 \mod p \Leftrightarrow r(p)|k$．また，$D = P^2 - 4Q$ とおけば，

(1) $\left(\dfrac{D}{p}\right) = 1$ なら，$r(p)|(p-1)$.

(2) $\left(\dfrac{D}{p}\right) = -1$ なら，$r(p)|(p+1)$.

rank と period の別の視点について考察する．$A = \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix} \in M(2, \mathbb{Z})$ とおく．

観察 1.5. P, Q を 0 でない整数，$(L_k)_{k\geq 0}$ を (P, Q) に伴う Lucas 数列とし，p を素数 > 2 とする．また，$(p, Q) = 1$ とし，$\mathbb{F}_p$ における二次方程式 $t^2 - Pt + Q = 0$ の根を α, β とする．
(1) $\alpha \neq \beta$ の場合，$\mathbb{F}_p$ において $L_k = (\alpha^k - \beta^k)/(\alpha - \beta)$ なので，$L_k \equiv 0 \mod p \Leftrightarrow \alpha^k \equiv \beta^k \mod p$. ここで，

$$A^k = \frac{1}{\alpha - \beta} \begin{pmatrix} -\alpha^k\beta + \alpha\beta^k & -\alpha^{k+1}\beta + \alpha\beta^{k+1} \\ \alpha^k - \beta^k & \alpha^{k+1} - \beta^{k+1} \end{pmatrix}$$

なので，$\alpha^k \equiv \beta^k$ を代入すると，$GL(2, \mathbb{F}_p)$ において $A = \alpha^k I$ を，さらに $PGL(2, \mathbb{F}_p)$ において $A = I$ を得る．
(2) $\alpha = \beta$ 場合．$\mathbb{F}_p$ において $L_k = k\alpha^{k-1}$ なので，$L_k \equiv 0 \mod p \Leftrightarrow k \equiv 0 \mod p$. ここで，

$$A^k = \begin{pmatrix} (1-k)\alpha^k & -k\alpha^{k+1} \\ k\alpha^{k-1} & (k+1)\alpha^k \end{pmatrix}$$

なので，$k \equiv 0 \mod p$ を代入すると，$GL(2, \mathbb{F}_p)$ において $A = \alpha^k I$ を，さらに $PGL(2, \mathbb{F}_p)$ において $A = I$ を得る．

観察 1.5 における k を最小にとることによって Lucas の lois de l'apparition et la répétition を得る．また．観察 1.5 は次のように定式化できる．

定理 1.6. P, Q を 0 でない整数，p を素数 > 2 とする．また，$(p, Q) = 1$ とし，$A = \begin{pmatrix} 0 & -Q \\ 1 & P \end{pmatrix}$ とおく．このとき，次が成立する．
(1) $k(p)$ は $GL(2, \mathbb{F}_p)$ における A の位数と等しい．
(2) $r(p)$ は $PGL(2, \mathbb{F}_p)$ における A の位数と等しい．

このように，Lucas 数列の rank，period に関する議論は有限体を成分にもつ行列の位数に関する議論に移し替えることができるが，行列の固有値を用いているので，適用できる係数の環は体に限定される．しかし，一般の $r(m), k(m)$ や $r(p^n), k(p^n)$ を考察するには必ずしも体でない $\mathbb{Z}/m\mathbb{Z}$ や $\mathbb{Z}/p^n\mathbb{Z}$ の上で議論を展開しなくてはならない．また，3 階以上の線型漸化式を扱う場合には行列による議論だけでは見通しが悪い．次節では，一般の Lucas 数列を体でない場合も含めて rank と period を記述する方法について述べる．

2 Lucas sequence

一般の n 階の Lucas 数列の場合に議論できるが，これ以降は，簡単のために 3 階の Lucas 数列を扱う．

記号 2.1. R を環，$P(t)=t^3-P_1t^2-P_2t-P_3\in R[t]$ とする．また，$R^{\mathbb{N}}$ の部分集合 $\mathcal{L}(P,R)$ を

$$\mathcal{L}(P,R)=\{(w_k)_{k\geq 0}\in R^{\mathbb{N}}\ ;\ \text{各 } k \text{ に対して } w_{k+3}=P_1w_{k+2}+P_2w_{k+1}+P_3w_k\}$$

によって定義すれば，$\mathcal{L}(P,R)$ は $R^{\mathbb{N}}$ の部分 R 加群．$\mathcal{L}(P,R)$ の元は多項式 $P(t)$ を特性多項式にもつ線型漸化式に他ならない．さらに，$(w_k)_{k\geq 0}\mapsto(w_0,w_1,w_2)$ によって R 同型 $\mathcal{L}(P,R)\xrightarrow{\sim}R^3$ が与えられる．

定義 2.2. $\tilde{R}=R[t]/(P(t))$ とし，$\tilde{R}=R[t]/(P(t))$ において $\theta\equiv t \mod P(t)$ とおく．また，D を多項式 $P(t)$ の判別式とする．このとき，$\{1,\theta,\theta^2\}$ は $\tilde{R}$ の R 上の基底をなす．したがって，$\tilde{R}$ は R の上に有限 flat．さらに D が R において巾零でなければ，$\tilde{R}\otimes_R R[1/D]$ は $R[1/D]$ の上に有限 étale である．

$\rho:\tilde{R}\to M(3,R)$ を R 上の基底 $\{1,\theta,\theta^2\}$ に関する R 代数 $\tilde{R}$ の正則表現とする．$\eta\in\tilde{R}$ のノルム $\mathrm{Nr}\,\eta$ を $\mathrm{Nr}\,\eta=\det\rho(\eta)$ によって定義する．このとき，「η が $\tilde{R}$ において可逆 $\Leftrightarrow$ $\mathrm{Nr}\,\eta$ が R において可逆」が成り立つ．

R 準同型 $\omega:\tilde{R}\to R$ を

$$\omega(a_0+a_1\theta+a_2\theta^2)=a_2$$

によって定義する．さらに，R 準同型 $\tilde{\omega}:\tilde{R}\to R^{\mathbb{N}}$ を

$$\tilde{\omega}(\eta)=(\omega(\theta^k\eta))_{k\geq 0}$$

によって定義する．

R の元の列 $(w_k)_{k\geq 0}=(\omega(\theta^k\eta))_{k\geq 0}$ は線型漸化式 $w_{k+3}=P_1w_{k+2}+P_2w_{k+1}+P_3w_k$ を満たすが，次の命題によって R 加群 $\mathcal{L}(P,R)$ と剰余環 $\tilde{R}=R[t]/(P(t))$ とが完全に関係付けられる．

命題 2.3. R 準同型 $\tilde{\omega}:\tilde{R}\to R^{\mathbb{N}}$ は R 同型 $\tilde{\omega}:\tilde{R}\to\mathcal{L}(P,R)$ を誘導する．$\tilde{\omega}:\tilde{R}\to\mathcal{L}(P,R)$ の逆写像は

$$(w_0,w_1,w_2,\ldots)\mapsto w_0\theta^2+(w_1-P_1w_0)\theta+(w_2-P_1w_1-P_2w_0)$$

によって与えられる．

系 2.4. I を R のイデアルとし，$\eta,\eta'\in\tilde{R}$ とする．このとき，$\eta\equiv\eta' \mod I \Leftrightarrow \mathcal{L}(P,R)$ において $\tilde{\omega}(\eta)\equiv\tilde{\omega}(\eta') \mod I$．

R 加群の同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,R)$ によって Binet の公式に縛られずに線型漸化式を扱うことができる．

例 2.5. $(L_k)_{k\geq 0}=\tilde{\omega}(1)\in\mathcal{L}(P,R)$ を $P(t)$ に伴う Lucas 数列と呼ぶことにする．言い換えれば，$(L_k)_{k\geq 0}$ は，線型漸化式 $w_{k+3}=P_1w_{k+2}+P_2w_{k+1}+P_3w_k$ と初項 $L_0=L_1=0$, $L_2=1$ によって定義される R の元の列である．

観察 2.6. R 加群の同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,R)$ によって $\mathcal{L}(P,R)$ に R 代数の構造を定義する．このとき，Lucas 数列 $(L_k)_{k\geq 0}=\tilde{\omega}(1)$ は環 $\mathcal{L}(P,R)$ の単位元である．さらに，R 同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,R)$ は $\tilde{R}$ での θ による乗法を $\mathcal{L}(P,R)$ における項をずらす操作 $(w_k)_{k\geq 0}\mapsto(w_{k+1})_{k\geq 0}$ に移す．

$\eta\in\tilde{R}$ とし，$\boldsymbol{w}=\tilde{\omega}(\eta)\in\mathcal{L}(P,R)$ とおく．さらに $\Delta(\boldsymbol{w})$ を $\Delta(\boldsymbol{w})=\mathrm{Nr}\,\eta$ と定義する．このとき，「$\boldsymbol{w}$ が $\mathcal{L}(P,R)$ において可逆 $\Leftrightarrow$ $\Delta(\boldsymbol{w})$ が R において可逆」が成り立つ．

以上の議論を $R=\mathbb{Z}$ の場合に適用して，Lucas 数列の可除性に関する幾つかの結果を捉え直せる．同型 $\tilde{\omega}:\tilde{R}\xrightarrow{\sim}\mathcal{L}(P,\mathbb{Z})$ によって $\theta^n\in\tilde{R}=\mathbb{Z}[t]/(P(t))$ は数列 $(L_{n+k})_{k\geq 0}$ に移される．したがって，系 2.4 を $R=\mathbb{Z}$, $I=m\mathbb{Z}$ に適用することによって次の定理を得る．

定理 2.7. m を整数 ≥ 2 とし，$(m, P_3) = 1$ と仮定する．このとき，次が成立する．
(1) $k(m)$ は $\mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}[t]/(m, P(t)))^\times$ における θ の位数と等しい．
(2) $r(m)$ は $\mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})^\times/(\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}[t]/(m, P(t)))^\times/(\mathbb{Z}/m\mathbb{Z})^\times$ における θ の位数と等しい．

定理 2.7 は一般の n についても成り立つ．(3 を n に読み替えればよい）定理 2.7 の 2 階の場合の系として，Lucas の lois de l'apparition et la répétition（定理 1.4）が得られる．

最後に，2 階の場合に定理 1.6 と定理 2.7 の関係について述べる．

観察 2.8. 対応 $a + b\theta \mapsto aI + bA$ によって埋め込み $\rho : \mathbb{F}_p[t]/(P(t)) \to M(2, \mathbb{F}_p)$ が与えられる．これはまさに観察 2.2 で見た正則表現に他ならない．

定理 2.7 は定理 1.6 の言い換えになっている．$\rho : \mathbb{F}_p[t]/(P(t)) \to M(2, \mathbb{F}_p)$ により θ は A に対応する．したがって，定理 2.7 は rank，period は $PGL(2, \mathbb{F}_p)$, $GL(2, \mathbb{F}_p)$ においてではなく，その元となる $(\mathbb{F}_p[t]/(P(t))^\times$，$(\mathbb{F}_p[t]/(P(t))^\times/(\mathbb{F}_p)^\times$ において考えれば十分であることを意味している．

定理 1.6 と大きく異なる点は，m は必ずしも素数ではないことである．定理 2.7 では $\mathbb{Z}/m\mathbb{Z}$ が体でない環である場合にも rank，period を群の元の位数としてとらえることができる．

3 Geometric aspects

最後に，Lucas 数列の rank と period を群の作用の観点から捉え直す方法について述べる．ここでは，$G_P(R) = (R[t]/(P(t)))^\times$, $G_{(P)}(R) = (R[t]/(P(t)))^\times/R^\times$ と記すことにする．

記号 3.1. R を環，$P(t) = t^3 - P_1t^2 - P_2t - P_3 \in R[t]$ とする．また，P_3 は R において可逆と仮定する．このとき，

$$\Theta = [\theta\text{によって生成される } G_P(R) \text{ の部分群}]$$

と定義する．

Laxton [3][4] は $G_{(P)}(\mathbb{Q})$, $G_{(P)}(\mathbb{Z}_{(p)})$, $G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ における Θ 軌道分解について考察していると解釈できる．青木-酒井 [1] は $G_P(\mathbb{Z}_{(p)})$ に属さない線型漸化式に対しても Laxton の議論を適用する方法を提示した．以上の先行研究の群スキームの理論を援用した定式化については，2 階の場合は諏訪が [7][8] において徹底して議論していて，さらに [9] で一般の階数の場合に定式化が進めている．以下，その概略を 3 階の場合に説明する．

観察 3.2. $G_P(R)$ の部分群 Θ は群の同型 $\tilde{\omega} : G_P(R) \xrightarrow{\sim} \mathcal{L}(P, R)^\times$ を通して乗法によって $\mathcal{L}(P, R)$ の上に左から作用する．このとき，観察 2.6 で見たように，$(w_k)_{k\geq 0} \in \mathcal{L}(P, R)$ の Θ 軌道は $\{(w_{k+l})_{k\geq 0}\ ;\ l \in \mathbb{Z}\}$ によって与えられる．

また，$\mathcal{L}(P, R)$ の上への Θ の左作用は $\mathcal{L}(P, R)/R^\times$ の上への Θ の左作用を誘導する．$[(w_k)_{k\geq 0}] \in \mathcal{L}(P, R)/R^\times$ の Θ 軌道は $\{[(w_{k+l})_{k\geq 0}]\ ;\ l \in \mathbb{Z}\}$ によって与えられる．

観察 3.3. $\operatorname{Pic} R = 0$ と仮定する．$\mathcal{L}(P, R)^\circ = \{(w_k)_{k\geq 0} \in \mathcal{L}(P, R)\ ;\ (w_0, w_1, w_2) = R\}$ とおく．このとき，$\mathcal{L}(P, R)^\circ$ は $G_P(R) = \mathcal{L}(P, R)^\times$ の $\mathcal{L}(P, R)$ の上への作用に対して安定．したがって，乗法群 $R^\times \subset G_P(R)$ の $\mathcal{L}(P, R)$ の上への作用に対しても安定．$\operatorname{Pic} R = 0$ なので，$\mathbb{P}^2(R) = \mathcal{L}(P, R)^\circ/R^\times$ を得る．このとき，$G_P(R)$ の $\mathcal{L}(P, R)^\circ$ の上への作用は $G_{(P)}(R) = G_P(R)/R^\times$ の $\mathcal{L}(P, R)^\circ/R^\times = \mathbb{P}^2(R)$ の上への作用を誘導する．

$\boldsymbol{w} = (w_k)_{k\geq 0}$ の $\mathcal{L}(P, R)^\circ/R^\times = \mathbb{P}^2(R)$ における類を $[\boldsymbol{w}] = (w_0 : w_1 : w_2)$ で表わす．$(w_0 : w_1 : w_2) \in \mathbb{P}^{n-1}(R) = \mathcal{L}(P, R)^\circ/R^\times$ の Θ 軌道は $\{(w_l : w_{l+1} : w_{l+2})\ ;\ l \in \mathbb{Z}\}$ によって与えられる．

例 3.4. $P(t)=t^3-P_1t^2-P_2t-P_3\in\mathbb{Z}[t]$，$(L_k)_{k\geq 0}$ を $P(t)$ に伴う Lucas 数列とする．また，m を整数 ≥ 2 とし，$(m,P_3)=1$ と仮定する．このとき，$\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})$ における $\tilde{\omega}(1)$ の Θ 軌道は乗法群

$$G_P(\mathbb{Z}/m\mathbb{Z})=\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})^\times\subset\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})$$

の θ によって生成される部分群に他ならない．したがって，$\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})$ における $\tilde{\omega}(1)$ の Θ 軌道の長さは Lucas 数列 $(L_k)_{k\geq 0}$ の period mod m に一致する．また，$\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})^\times$ における $\tilde{\omega}(1)$ の Θ 軌道は

$$G_{(P)}(\mathbb{Z}/m\mathbb{Z})=\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})^\times/(\mathbb{Z}/m\mathbb{Z})^\times\subset\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})^\times$$

の θ によって生成される部分群に他ならない．したがって，$\mathcal{L}(P,\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z})^\times$ における $\tilde{\omega}(1)$ の Θ 軌道の長さは Lucas 数列 $(L_k)_{k\geq 0}$ の rank mod m に一致する．

観察 1.5 では素数 p に対して Lucas 数列の rank　mod p をは射影線型群 $PGL(2,\mathbb{F}_p)$ によって解釈したが，上記の議論によって一般の整数 m に対しても観察 1.5 における議論が定式化された．

観察 3.3 より $\mathrm{Pic}R=0$ のとき，同型写像 $\tilde{\omega}$ によって $G_{(P)}(R)\subset\mathbb{P}^2(R)$ と見ることができる．ここで，$R[t]/(P(t))$ が体でなければ $G_{(P)}(R)\subsetneq\mathbb{P}^2(R)$ となり 2 つの集合の元の個数に差が現れる．特に $R=\mathbb{F}_p$ (p は奇素数) において得られた結果を次に示す．

観察 3.5. p は素数 >2 とする．$G_P(\mathbb{F}_p)=(\mathbb{F}_p[t]/(P(t)))^\times$ および $G_{(P)}(\mathbb{F}_p)=(\mathbb{F}_p[t]/(P(t)))^\times/\mathbb{F}_p^\times$ の構造は $\mathbb{F}_p[t]$ における $P(t)$ の既約分解によって決定される．したがって，$\mathbb{P}^2(\mathbb{F}_p)$ と $G_{(P)}(\mathbb{F}_p)$ との元の個数の差は $\mathbb{F}_p[t]$ における $P(t)$ の既約分解によって現れる．ここで $\#\mathbb{P}^2(\mathbb{F}_p)=p^2+p+1$ である．

(1) $P(t)$ が $\mathbb{F}_p[t]$ において既約のとき $\mathbb{F}_p[t]/(P(t))$ は体となり，同型 $G_{(P)}(\mathbb{F}_p)\xrightarrow{\sim}\mathbb{P}^2(\mathbb{F}_p)$ がいえる．したがって，$\mathbb{P}^2(\mathbb{F}_p)$ と $G_{(P)}(\mathbb{F}_p)$ との元の個数の差はない．

(2) $P(t)$ が $\mathbb{F}_p[t]$ において $(t-\alpha)Q(t)$ ($\alpha\in\mathbb{F}_p$, $Q(t)$ は $\mathbb{F}_p[t]$ において既約) と因数分解されるとき，$G_{(P)}(\mathbb{F}_p)\simeq\mathbb{F}_{p^2}^\times$ となる．したがって，$\#\mathbb{P}^2(\mathbb{F}_p)-\#G_{(P)}(\mathbb{F}_p)=(p^2+p+1)-(p^2-1)=p+2$ より $p+2$ 個の差がある．
この差は次の数列によって現れる．$\mathbb{F}_{p^2}[t]$ において $Q(t)=(t-\beta)(t-\bar{\beta})$ ($\beta\in\mathbb{F}_{p^2}\setminus\mathbb{F}_p$) と因数分解すると

(a) $\boldsymbol{w}=(\alpha^k)_{k\geq 0}$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは 1.

(b) $\boldsymbol{w}=(\lambda\beta^k+\bar{\lambda}\bar{\beta}^k:\lambda\beta^{k+1}+\bar{\lambda}\bar{\beta}^{k+1}:\lambda\beta^{k+2}+\bar{\lambda}\bar{\beta}^{k+2}))_{k\geq 0}$ ($\lambda\in\mathbb{F}_{p^2}$) の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは $p+1$ の約数．ここで，$\#(\mathbb{F}_{p^2}/\mathbb{F}_p^\times)=p+1$ である．

(3) $P(t)$ が $\mathbb{F}_p[t]$ において $(t-\alpha)(t-\beta)(t-\gamma)$ (α, β, γ は $\mathbb{F}_p$ の相異なる元) と因数分解されるとき，$G_{(P)}(\mathbb{F}_p)\simeq\mathbb{F}_p\times\mathbb{F}_p$ となる．したがって，$\#\mathbb{P}^2(\mathbb{F}_p)-\#G_{(P)}(\mathbb{F}_p)=(p^2+p+1)-(p-1)^2=3p$ より $3p$ 個の差がある．
この差は次の数列によって現れる．

(a) $\boldsymbol{w}=(\alpha^k)_{k\geq 0},(\beta^k)_{k\geq 0},(\gamma^k)_{k\geq 0}$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは 1.

(b) $\boldsymbol{w}=(\alpha^k+c\beta^k)_{k\geq 0},(\alpha^k+c\gamma^k)_{k\geq 0},(\beta^k+c\gamma^k)_{k\geq 0}$ ($c\in\mathbb{F}_p^\times$) の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは $p-1$ の約数．ここで，$3\times\#\mathbb{F}_p^\times=3(p-1)$ である．

(4) $P(t)$ が $\mathbb{F}_p[t]$ において $(t-\alpha)^2(t-\beta)$ (α, β, は $\mathbb{F}_p$ の相異なる元) と因数分解されるとき，$G_{(P)}(\mathbb{F}_p)\simeq\mathbb{F}_p\times\mathbb{F}_p^\times$ となる．したがって，$\#\mathbb{P}^2(\mathbb{F}_p)-\#G_{(P)}(\mathbb{F}_p)=(p^2+p+1)-p(p-1)=2p+1$ より $2p+1$ 個の差がある．この差は次の数列によって現れる．

(a) $\boldsymbol{w} = (\alpha^k)_{k\geq 0}, (\beta_k)_{k\geq 0}$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは 1.

(b) $\boldsymbol{w} = (\alpha^k + c\beta^k)_{k\geq 0}$ $(c \in \mathbb{F}_p^\times)$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは $p-1$ の約数．ここで，$\#\mathbb{F}_p^\times = p-1$ である．

(c) $\boldsymbol{w} = (k\alpha^{k-1} + c\alpha^k)_{k\geq 0}$ $(c \in \mathbb{F}_p)$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは p．ここで，$\#\mathbb{F}_p = p$ である．

(5) $P(t)$ が $\mathbb{F}_p[t]$ において $(t-\alpha)^3$ と因数分解されるとき，$G_{(P)}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ となる．したがって，$\#\mathbb{P}^2(\mathbb{F}_p) - \#G_{(P)}(\mathbb{F}_p) = (p^2+p+1) - p^2 = p+1$ より $p+1$ 個の差がある．
この差は次の数列によって現れる．

(a) $\boldsymbol{w} = (\alpha^k)_{k\geq 0}$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは 1.

(b) $\boldsymbol{w} = (k\alpha^{k-1} + c\alpha^k)_{k\geq 0}$ $(c \in \mathbb{F}_p)$ の $\mathbb{P}^2(\mathbb{F}_p)$ における $[\boldsymbol{w}]$ の Θ 軌道の長さは p．ここで，$\#\mathbb{F}_p = p$ である．

参考文献

[1] M. Aoki and Y. Sakai, Mod p equivalence classes of linear recurrence sequences of degree 2, Rocky Mountain J. Math. **47** (2017), 2513–2533.

[2] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15** (1913/14), 30–48.

[3] R. R. Laxton, On groups of linear recurrences. I, Duke Math. J. **36** (1969), 721–736.

[4] R. R. Laxton, On groups of linear recurrences. II, Elements of finite order, Pacific J. Math. **32** (1970), 173–179.

[5] E. Lucas, Théorie des fonctions numériques simplement périodiques, Amer. J. Math. **1** (1878), 184–196.

[6] 齊藤暢, 幾何的視点から観た Lucas 数列〜3 階の場合, 第 1 3 回福岡整数論研究集会報告集に掲載予定

[7] N. Suwa, Geometric aspects of Lucas sequences. I, Preprint series No.122, Chuo Universtiy, 2018.

[8] N. Suwa, Geometric aspects of Lucas sequences. II, Preprint series No.125, Chuo Universtiy, 2018.

[9] N. Suwa, Geometric aspects of Lucas sequences. A survey, Preprint series No.127, Chuo University, 2019.

[10] M. Ward, The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. **35** (1933), 600–628.

[11] M. Ward, The linear p-adic recurrences of order two, Illinois J. Math. **6** (1962), 40–52.