RIMS Kôkyûroku Bessatsu
B86 (2021), 149–176

Geometric aspects of Lucas sequences, a survey

By

Noriyuki Suwa[*]

Abstract

This article is a concise survey on the divisibility problem for Lucas sequences, including the Fibonacci sequence. We present a method of viewing Lucas sequences in the framework of group scheme theory, starting with the sights of milestones in the history of researches, especially showing respect for the works achieved by Edouard Lucas au temps des cerises in the 19th century.

Introduction

The Lucas sequences, including the Fibonacci sequence, have been studied widely for a long time, and there is left an enormous accumulation of research. Particularly the divisibility problem is a main subject in the study on Lucas sequences.

More explicitly, let P and Q be non-zero integers, and let $(w_k)_{k\geq 0}$ be the sequence defined by the linear recurrence relation $w_{k+2} = Pw_{k+1} - Qw_k$ with the initial terms $w_0, w_1 \in \mathbb{Z}$. If $w_0 = 0$ and $w_1 = 1$, then $(w_k)_{k\geq 0}$ is nothing but the Lucas sequences $(L_k)_{k\geq 0}$ associated to (P, Q). The divisibility problem asks to describe the set $\{k \in \mathbb{N} \,;\, w_k \equiv 0 \mod m\}$ for a positive integer m. The first step was certainly taken forward by Edouard Lucas [11], who established *les lois de l'apparition et de la répétition* in the case where m is a prime number and $(w_k)_{k\geq 0}$ is the Lucas sequence. More precisely, he proved the following:

Les lois de l'apparition et de la répétition. *Assume that P and Q are relatively prime to each other, and let p be a prime with $(p, Q) = 1$. Then there exists a positive integer k such that $L_k \equiv 0 \mod p$. Furthermore, take r as the least positive integer such that $L_r \equiv 0 \mod p$. Then $L_k \equiv 0 \mod p$ if and only if k is divisible by r.*

Received March 31, 2019. Revised February 1, 2020.
2020 Mathematics Subject Classification(s): 13B05, 14L15, 12G05.
Key Words: *Lucas sequence, group scheme*
Partially supported by Grant-in-Aid for Scientific Research No.19K03408

[*] Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan.
e-mail: suwa@math.chuo-u.ac.jp

After his study there have been piled up various kinds of results. Lucas also defined an important invariant, called the rank of the Lucas sequence $(L_k)_{k\geq 0} \mod m$ and denoted by $r(m)$ usually, as the least positive integer k such that $L_k \equiv 0 \mod m$ if exists. The notion of rank is a key to describe the laws of apparition and repetition.

In this article we give a survey on study of the divisibility problem for Lucas sequences from a geometric viewpoint, translating several descriptions on Lucas sequences into the language of affine group schemes.

First we explain briefly a main idea of the argument developed in the article. Recall the Fermat-Euler Theorem, which is very important in the elementary number theory:

Theorem of Fermat-Euler. *Let m be a positive integer, and a be an integer with $(a, m) = 1$. Then we have $a^{\varphi(m)} \equiv 1 \mod m$. Here φ denotes the Euler totient function.*

Nowadays the Fermat-Euler Theorem is recognized as a corollary of the Lagrange Theorem, which is very important in the elementary group theory:

Theorem of Lagrange. *Let G be a finite group and $g \in G$. Then the order of g divides the order of G.*

Applying the Lagrange Theorem to the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$, we obtain immediately the Fermat-Euler Theorem. Now we interpret the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ as the group of $\mathbb{Z}/m\mathbb{Z}$-valued points of the multiplicative group scheme $\mathbb{G}_{m,\mathbb{Z}}$. In this article we reinterpret the notion of rank mod m for Lucas sequences as the order of an element in the group of $\mathbb{Z}/m\mathbb{Z}$-valued points of the affine group scheme $G_{(P)}$, which is defined in the section 2. This enables us to prove the laws of apparition and repetition as a corollary of the Lagrange Theorem.

Next we explain the organization of the article. The Section 1 is a short review about history of study on the divisibility problem for Lucas sequences. As milestones of researches, we select works of Lucas [11], Carmichael [5], Ward [16], Laxton [9] and Aoki-Sakai [2]. In the Section 2, we introduce the affine group schemes denoted by G_P, U_P and $G_{(P)}$, giving explanation on the groups of $\mathbb{Z}_p$-valued points. In the Section 3, we reformulate the algebra of linear recurrence sequences, which ascends to Ward [15] and Hall [7], and relate Lucas sequences with the group schemes G_P and $G_{(P)}$. In the Section 4, we present an interpretation on the notion of rank and period for Lucas sequences in our context. In the Section 5, we reformulate and generalize remarkable results of Laxton and of Aoki-Sakai, which suggest a way to treat Lucas sequences geometrically. The argument developed in the Sections 2–5 is almost a paraphrase of the method explained precisely in [13] and [14]. We give only short verifications, omitting detailed account.

Acknowlegdement. The author would like to express his hearty thanks to Masato

Kurihara and Akira Masuoka for their advices and encouragement. He highly appreciates it that the referee read the manuscript very carefully and gave several valuable comments and references, which helped him to improve the description of the article.

Notation. For a ring R, $R^\times$ denotes the multiplicative group of invertible elements of R.

$\tilde{R} = \mathbb{Z}[t]/(P(t))$ defined in 2.1

$\mathcal{L}(P, R)$ defined in 1.7 and in 3.1

$\mathbb{G}_{m,\mathbb{Z}}$ the multiplicative group scheme

$G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$ the Weil restriction of $\mathbb{G}_m$ with respect to $\tilde{R}/R$, defined in 2.1

$U_P = \mathrm{Ker}[\mathrm{Nr} : \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}]$ defined in 2.1

$G_{(P)} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}/\mathbb{G}_{m,R}$ defined in 2.1

$\beta : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to G_{(P)} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}/\mathbb{G}_{m,R}$ the canonical surjection

$\Theta \subset G_P(R)$ defined in 5.1

$\Theta \subset G_{(P)}(R)$ defined in 5.1

1. History

In the section, we fix *non-zero integers* P, Q with $P^2 - 4Q \neq 0$ and put $D = P^2 - 4Q$.

Notation 1.1. Let α, β denote the roots of the quadratic equation $t^2 - Pt + Q = 0$. We define sequences $(L_k)_{k \geq 0}$ and $(S_k)_{k \geq 0}$ by

$$L_k = L_k(P, Q) = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \; S_k = S_k(P, Q) = \alpha^k + \beta^k.$$

The sequences $(L_k)_{k \geq 0}$ and $(S_k)_{k \geq 0}$ are called *the Lucas sequence* and *the companion Lucas sequence* associated to (P, Q), respectively.

The following assertions are verified immediately from the definition.

(1) $L_0 = 0$, $L_1 = 1$, $L_{n+2} - PL_{n+1} + QL_n = 0$, $S_0 = 2$, $S_1 = P$, $S_{n+2} - PS_{n+1} + QS_n = 0$.

(2) $S_n^2 - DL_n^2 = 4Q^n$.

(3) $2S_{n+m} = S_n S_m + DL_n L_m$, $2L_{n+m} = L_n S_m + S_n L_m$.

In particular,

(4) $S_{2n} = \frac{1}{2}(S_n^2 + DL_n^2) = S_n^2 - 2Q^n = DL_n^2 + 2Q^n$, $L_{2n} = L_nS_n$.

Hereafter, we assume that P and Q are *relatively prime* to each other.

1.2. The following facts were established Lucas [11] and Carmichael [5].

(1) $(L_n, S_n) = 1$ or 2 for any $n \geq 1$. Furthermore,

(a) If Q is even, then we have $L_n \equiv 1 \mod 2$ and $S_n \equiv 1 \mod 2$ for any $n \geq 1$.

(b) If Q is odd, then we have $L_n \equiv n \mod 2$ and $S_n \equiv 0 \mod 2$ for any $n \geq 1$.

(c) Assume that both Q and P are odd. If n is divisible by 3, then we have $L_n \equiv 0 \mod 2$ and $S_n \equiv 0 \mod 2$. On the other hand, if n is not divisible by 3, then we have $L_n \equiv 1 \mod 2$ and $S_n \equiv 1 \mod 2$.

(2) Let m and n be positive integers, and put $d = (m, n)$. Then we have:

(a) $(L_m, L_n) = L_d$.

(b) $(S_m, S_n) = S_d$ if m/d and n/d are odd.

(3) Let m and n be positive integers, and let p be a prime number. Put $\nu = \mathrm{ord}_p L_m$.

(a) If $p > 2$, $\nu \geq 1$ or if $p = 2$, $\nu \geq 2$, then we have $\mathrm{ord}_p L_{mn} = \nu + \mathrm{ord}_p n$.

(b) Assume that $p = 2$ and $\nu = 1$. If n is odd, then we have $\mathrm{ord}_2 L_{mn} = 1$. On the other hand, if n is even, then we have $\mathrm{ord}_p L_{mn} \geq 1 + \mathrm{ord}_2 n$.

(4) Let m and n be positive integers, and let p be a prime number > 2. Put $\nu = \mathrm{ord}_p S_m$, and assume $\nu \geq 1$.

(a) If n is odd, then we have $\mathrm{ord}_p L_{mn} = 0$ and $\mathrm{ord}_p S_{mn} = \nu + \mathrm{ord}_p n$.

(b) If n is even, then we have $\mathrm{ord}_p L_{mn} = \nu + \mathrm{ord}_p n$ and $\mathrm{ord}_p S_{mn} = 0$.

(5) Let p be a prime number > 2 with $(p, Q) = 1$. Then:

(a) If $\left(\frac{D}{p}\right) = 1$, then L_{p-1} is divisible by p.

(b) If $\left(\frac{D}{p}\right) = -1$, then L_{p+1} is divisible by p.

(c) If D is divisible by p, then L_p is divisible by p.

Concerning the divisibility of the Lucas sequence $(L_k)_{k\geq 0}$, Lucas introduced an important notion:

Definition 1.3. Let m be an integer ≥ 2. The rank of the Lucas sequence $(L_k)_{k\geq 0}$ mod m is defined as the least positive integer k such that $L_k \equiv 0 \mod m$, if exists. We shall denote by $r(m)$ the rank of the Lucas sequence $(L_k)_{k\geq 0} \mod m$.

Combining the assertions mentioned in 1.2, we obtain the following results:

Theorem 1.4. (Lucas-Carmichael) *Assume that P and Q are relatively prime to each other, and let m be an integer with $m \geq 2$ and $(m, Q) = 1$. Then*:

(1) *There exists a positive integer k such that $L_k \equiv 0 \mod m$. Furthermore, $L_k \equiv 0 \mod m$ if and only if k is divisible by $r(m)$.*

(2) *Let p be an odd prime and N a positive integer, and put $\nu = \mathrm{ord}_p L_{r(p)}$. Then we have*

$$r(p^N) = \begin{cases} r(p) & (N \le \nu) \\ p^{N-\nu} r(p) & (N > \nu) \end{cases}.$$

(3) *Let N be a positive integer, and put $\nu = \mathrm{ord}_p L_{r(4)}$. Then we have $r(2^N) = 2^{N-\nu} r(4)$ for $N > \nu$.*

(4) *Let p be an odd prime. Then:*

(a) *If $\left(\dfrac{D}{p}\right) = 1$, then $r(p)$ divides $p-1$.*

(b) *If $\left(\dfrac{D}{p}\right) = -1$, then $r(p)$ divides $p+1$.*

(c) *If D is divisible by p, then $r(p) = p$.*

(5) *Let p be an odd prime. There exists a positive integer k such that $S_k \equiv 0 \mod p$ if and only if $r(p) \equiv 0 \mod 2$. In this case, the least positive integer k such that $S_k \equiv 0 \mod p$ is given by $k = r(p)/2$.*

Remark 1.5. Lucas called $r(p)$ *le rang d'arrivée* or *d'apparition* of the prime number in the sequence $(L_k)_{k\ge 0}$. Lucas called the first assertion of Theorem 1.4 *les lois de l'apparition et de la répétition.*

Lucas proved his results, basing his argument mainly on the formula

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \ S_n = \alpha^n + \beta^n$$

and keeping in mind the analogy of the sequences $(L_k)_{k\ge 0}$ and $(S_k)_{k\ge 0}$ to the trigonometric functions:

$$\sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}, \ \cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}.$$

Carmichael simplified and sharpened the argument, introducing polynomials

$$\Phi_n(X,Y) = \prod_{\substack{0<k\le n \\ (k,n)=1}} (X - e^{2ki\pi/n}Y)$$

(homogenization of the cyclotomic polynomials) and establishing formulas

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_{\substack{d|n \\ d\ne 1}} \Phi_d(\alpha,\beta)$$

and

$$S_n = \alpha^n + \beta^n = \frac{L_{2n}}{L_n} = \prod_{\substack{d|2n \\ d\nmid n,\ d\neq 1}} \Phi_d(\alpha,\beta).$$

1.6. Ward [16] enlarged and clarified the argument on divisibility problem for Lucas sequences, considering linear recurrence sequences of p-adic integers and employing the p-adic exponential and the p-adic logarithmic functions. He generalized the laws of apparition and repetition for linear recurrence sequences of order 2 and established remarkable results. Now we recall a part of his work.

Definition 1.6.1. Let P and Q be p-adic integers, and put $D = P^2 - 4Q$. Let $\boldsymbol{w} = (w_k)_{k\geq 0}$ denote the sequence defined by the linear recurrence relation $w_{k+2} = Pw_{k+1} - Qw_k$ with the initial terms $w_0, w_1 \in \mathbb{Z}_p$. Assume that w_0 or w_1 is a p-adic unit.

(1) p is said to be *a divisor of* $\boldsymbol{w}$ if there exists k such that $w_k \equiv 0 \mod p$;

(2) p is said to be *an unbounded divisor of* $\boldsymbol{w}$ if, for any $N > 0$, there exists k such that $w_k \equiv 0 \mod p^N$;

(3) p is said to be *a bounded divisor of* $\boldsymbol{w}$ if p is a divisor of $\boldsymbol{w}$ but not unbounded.

Theorem 1.6.2. (Ward [16]) *Let P and Q be p-adic integers, and let $\boldsymbol{w} = (w_k)_{k\geq 0}$ denote the sequence defined by the linear recurrence relation $w_{k+2} = Pw_{k+1} - Qw_k$ with the initial terms $w_0, w_1 \in \mathbb{Z}_p$. Put $D = P^2 - 4Q$ and $\Delta = w_1^2 - Pw_0w_1 + Qw_0^2$. Assume that Q is a p-adic unit and that w_0 or w_1 is a p-adic unit.*

(1) *Assume that both w_0 and w_1 are p-adic units. If Δ is divisible by p, then p is not a divisor of $\boldsymbol{w}$* ([Theorem 8.1]);

(2) *Assume that both D and Δ are p-adic units. Put $P' = 2w_1 - Pw_0$ and $Q' = \Delta$, and let $(L'_k)_{k\geq 0}$ denote the Lucas sequence associated to (P', Q'). Then, p is a divisor of $\boldsymbol{w}$ if and only if $r(p)$ is divisible by $r'(p)$. Here $r(p)$ and $r'(p)$ denote the ranks mod p of $(L_k)_{k\geq 0}$ and $(L'_k)_{k\geq 0}$, respectively* ([Theorem 9.2]);

(3) *Assume that both D and Δ are p-adic units and that w_0 is divisible by p. Then, p is a bounded divisor of $\boldsymbol{w}$ if and only if* $\mathrm{ord}_p w_0 < \mathrm{ord}_p L_{r(p)}$ ([Theorem 9.3]).

Remark 1.6.3. Ward established a beautiful formula for the p-adic orders of $(w_k)_{k\geq 0}$ ([16, Theorem 10.1]). The second assertion of [16, Theorem 11.1] is false if $p = 3$ and $D \equiv -3 \mod 9$. We refer to [13, Remark 3.16 and Remark 4.4] for a corrected statement.

1.7. Put $f(t) = t^2 - Pt + Q$. Assume that P and Q are relatively prime to each other and $P^2 - 4Q \neq 0$. Laxton [9, 10] reformulated the argument developed by Ward [16], defining a group $G(f)$ constructed on the linear recurrence sequences with characteristic polynomial $f(t)$. Now we recall the definition of the group $G(f)$, modifying descriptions and notations.

Definition 1.7.1. Put

$$\mathcal{L}(f,\mathbb{Z}) = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathbb{Z}^{\mathbb{N}}\ ;\ w_{k+2} = Pw_{k+1} - Qw_k \text{ for each } k \geq 0\}$$

and

$$\mathcal{L}(f,\mathbb{Z})^{\diamond} = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})\ ;\ w_1^2 - Pw_0w_1 + Qw_0^2 \neq 0\}.$$

We define an equivalence relation $\sim_L$ on $\mathcal{L}(f,\mathbb{Z})^{\diamond}$ as the relation generated by the following two equivalence relations:

(1) for $\boldsymbol{v}, \boldsymbol{w} \in \mathcal{L}(f,\mathbb{Z})^{\diamond}$, we have $\boldsymbol{v} \sim_L' \boldsymbol{w}$ if there exist non-zero integers k and l such that $k\boldsymbol{v} = l\boldsymbol{w}$;

(2) for $\boldsymbol{v} = (v_k)_{k\geq 0}, \boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})^{\diamond}$, we have $\boldsymbol{v} \sim_L'' \boldsymbol{w}$ if there exists a positive integer n such that $v_{k+n} = w_k$ for all $k \geq 0$ or $v_k = w_{k+n}$ for all $k \geq 0$.

We put $G(f) = \mathcal{L}(f,\mathbb{Z})^{\diamond}/\sim_L$. We shall denote by $[\boldsymbol{w}]$ the equivalence class of $\boldsymbol{w} \in \mathcal{L}(f,\mathbb{Z})^{\diamond}$ in $G(f)$.

Furthermore, for $\boldsymbol{v} = (v_k)_{k\geq 0}, \boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})^{\diamond}$, the product $\boldsymbol{vw} \in \mathcal{L}(f,\mathbb{Z})^{\diamond}$ is defined by

$$\boldsymbol{vw} = (v_0w_1 + v_1w_0 - Pv_0w_0, v_1w_1 - Qv_0w_0, \ldots).$$

Then $\mathcal{L}(f,\mathbb{Z})^{\diamond}/\sim_L$ is a commutative group ([9, Proposition 2.1]). We shall call $G(f)$ the Laxton group associated to the quadratic polynomial $f(t) = t^2 - Pt + Q$.

Fix now a prime p. Put

$$G(f,p^N) = \left\{ [\boldsymbol{w}] \in G(f)\ ;\ \begin{array}{c} \text{there exists } (w_k)_{k\geq 0} \in [\boldsymbol{w}] \text{ such that} \\ (w_0,w_1) = 1 \text{ and } w_k \equiv 0 \mod p^N \text{ for some } k \end{array} \right\}.$$

for each positive integer N. Then $G(f,p^N)$ is a subgroup $G(f)$ ([5, Proposition 3.1]). Furthermore, put

$$K(f,p) = \left\{ [\boldsymbol{w}] \in G(f)\ ;\ \begin{array}{c} \text{there exists } (w_k)_{k\geq 0} \in [\boldsymbol{w}] \text{ such that} \\ (w_0,w_1) = 1 \text{ and } (w_1^2 - Pw_0w_1 + Qw_0^2, p) = 1 \end{array} \right\}$$

and

$$H(f,p) = \text{the inverse image in } G(f) \text{ of the torsions in } G(f)/K(f,p)\}.$$

Then $K(f,p)$ and $H(f,p)$ are subgroups $G(f)$.

Summing up, we have gotten a descending chain of subgroups

$$G(f) \supset H(f,p) \supset K(f,p) \supset G(f,p) \supset G(f,p^2) \supset \cdots \supset G(f,p^N) \supset \cdots.$$

Definition 1.8. We put

$$\mathcal{R}(f,\mathbb{Z}) = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(f,\mathbb{Z})\ ;\ (w_0,w_1) = 1 \text{ and } w_0 > 0 \text{ or } w_0 = 0,\ w_1 = 1\}$$

Let p be a prime, and let $\boldsymbol{w} \in \mathcal{R}(f, \mathbb{Z})$.

(1) p is said to be *a divisor of* $\boldsymbol{w}$ if there exists $\boldsymbol{w}' = (w'_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z})$ such that $\boldsymbol{w}' \sim \boldsymbol{w}$ and $w'_0 \equiv 0 \mod p$;

(2) p is said to be *an unbounded divisor of* $\boldsymbol{w}$ if, for any $N > 0$, there exists $\boldsymbol{w}' = (w'_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z})$ such that $\boldsymbol{w}' \sim \boldsymbol{w}$ and $w'_0 \equiv 0 \mod p^N$;

(3) p is said to be *a bounded divisor of* $\boldsymbol{w}$ if p is a divisor of $\boldsymbol{w}$ but not unbounded.

Proposition 1.9. (Laxton [9]) *Let p be an odd prime p and $\boldsymbol{w} \in \mathcal{R}(f, \mathbb{Z})$. Assume that $w_1^2 - Pw_0w_1 + Qw_0^2 \neq 0$ and $(p, Q) = 1$. Then*:

(1) *p is a divisor of $\boldsymbol{w}$ if and only if $[\boldsymbol{w}] \in G(f, p)$.*

(2) *Put $\nu = \mathrm{ord}_p L_{r(p)}$. Then p is a unbounded divisor of $\boldsymbol{w}$ if and only if $[\boldsymbol{w}] \in G(f, p^\nu)$.*

Remark 1.10. We adopt here the definition given by Laxton [9], which is a modification of the definition given by Ward [16] in the context of Laxton group theory.

The original definition in Ward [16] is more straightforward, as is recalled in 1.6.1. Let $\boldsymbol{w} = (w_k)_{k \geq 0} \in \mathcal{L}(f, \mathbb{Z})$.

(1) p is said to be a divisor of $\boldsymbol{w}$ if there exists $k \geq 0$ such that $w_k \equiv 0 \mod p$;

(2) p is said to be an unbounded divisor of $\boldsymbol{w}$ if, for any $N > 0$, there exists $k \geq 0$ such that $w_k \equiv 0 \mod p^N$.

This definition is equivalent to ours if $\boldsymbol{w} \in \mathcal{R}(f, \mathbb{Z})$ and $(p, 2Q) = 1$. We refer to [13, Remark 4.16] for detailed accounts on the difference of the two definitions. On the other hand, we refer to [13, Remark 4.15] for a verification of Proposition 1.9.

1.11. Laxton's work is pioneering, but seems unfortunately ignored and forgotten none the less for its importance though there have appeared remarkable works referring to Laxton's article, for example, Lagarias [8] and Ballot [3, 4]. A main reason may be that Laxton did not give an explicit description of $G(f)$. It is a main theme of [13] and [14] to interpret the Laxton group in the framework of group scheme theory.

After half a century, Aoki-Sakai [2] recovered Laxton's work, establishing the following remarkable assertions:

Theorem 1.12. *Assume $Q = \pm 1$, and let p be an odd prime. Then we have*

$$\#\left\{ (w_0 : w_1) \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}) \ ; \ \begin{array}{c} (w_k)_{k \geq 0} \in \mathcal{R}(f, \mathbb{Z}) \\ \text{and } w_k \not\equiv 0 \mod p \text{ for any } k \end{array} \right\} = (p+1) - r(p).$$

Furthermore, assume that $w_1^2 - Pw_0w_1 + Qw_0^2 \not\equiv 0 \mod p$. Then, $(w_k : w_{k+1}) = (w_0 : w_1)$ in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ if and only if k is divisible by $r(p)$.

Remark 1.12.1. The second assertion is just a geometric expression of the laws of apparition and repetition. Here we modify the statement in [1], adopting the notation $\mathbb{P}^1$, the projective line.

2. Group schemes G_P, U_P and $G_{(P)}$

We refer to [6] or [17] on formalisms of affine group schemes, Hopf algebras and the cohomology with coefficients in group schemes.

Definition 2.1. Let R be a ring and $P(t) = t^n - P_1t^{n-1} - \dots - P_{n-1}t - P_n \in R[t]$. Let D denote the discriminant of the polynomial $P(t)$. Put $\tilde{R} = R[t]/(P(t))$, and let θ denote the image of t in $\tilde{R}$. Then $\{1, \theta, \dots, \theta^{n-1}\}$ is an R-basis of $\tilde{R}$. This implies that $\tilde{R}$ is finite and flat over R. If D is not nilpotent in R, then $\tilde{R} \otimes_R R[1/D]$ is finite and étale over $R[1/D]$.

Let $\rho : \tilde{R} \to M(n, R)$ denote the regular representation of the R-algebra $\tilde{R}$ with respect to the R-basis $\{1, \theta, \dots, \theta^{n-1}\}$. Then, for $\eta \in \tilde{R}$, the norm $\mathrm{Nr}\,\eta = \mathrm{Nr}_{\tilde{R}/R}\eta$ is given by $\mathrm{Nr}\,\eta = \det \rho(\eta)$. It is readily seen that η is invertible in $\tilde{R}$ if and only if $\mathrm{Nr}\,\eta$ is invertible in R.

Put $G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$ (the Weil restriction of the multiplicative group scheme $\mathbb{G}_{m,\tilde{R}}$ with respect to the ring extension $\tilde{R}/R$). Then, for an R-algebra S, we have $G_P(S) = (\tilde{R} \otimes_R S)^\times$.

The canonical injection $R^\times \to \tilde{R}^\times$ is represented by the homomorphism of group schemes

$$i : \mathbb{G}_{m,R} \to G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}.$$

On the other hand, the norm map $\mathrm{Nr} : \tilde{R}^\times \to R^\times$ is represented by the homomorphism of group schemes

$$\mathrm{Nr} : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}$$

It is verified without difficulty that

(1) $G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}$ is smooth over R;

(2) $i : \mathbb{G}_{m,R} \to G_P$ is a closed immersion;

(3) $\mathrm{Nr} : G_P \to \mathbb{G}_{m,R}$ is faithfully flat;

(4) $\mathrm{Nr} \circ i : \mathbb{G}_{m,R} \to \mathbb{G}_{m,R}$ is the n-th power map.

We put

$$U_P = \mathrm{Ker}[\mathrm{Nr} : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to \mathbb{G}_{m,R}]$$

and

$$G_{(P)} = \mathrm{Coker}[i : \mathbb{G}_{m,R} \to G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}].$$

Then $G_{(P)}$ is smooth over R. Furthermore, if D is not nilpotent in R, then $G_P \otimes_R R[1/D]$, $U_P \otimes_R R[1/D]$ and $G_{(P)} \otimes_R R[1/D]$ are tori over $R[1/D]$. We denote by

$$\beta : G_P = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}} \to G_{(P)} = \prod_{\tilde{R}/R} \mathbb{G}_{m,\tilde{R}}/\mathbb{G}_{m,R}$$

the canonical surjection.

Reamrk 2.2. The regular representation $\rho_R : G_P(R) = \tilde{R}^\times \to GL(n,R)$ is represented by a homomorphism of group schemes $\rho : G_P \to GL_{n,R}$. It is readily seen that $\rho : G_P \to GL_{n,R}$ is a closed immersion.

By the definition, we have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[d, equal] & G_P \arrow[r, "\beta"] \arrow[d, "\rho"] & G_{(P)} \arrow[r] \arrow[d, "\rho"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & GL_{n,R} \arrow[r] & PGL_{n,R} \arrow[r] & 0
\end{tikzcd} .$$

The induced homomorphism $\rho : G_{(P)} \to PGL_{n,R}$ is a closed immersion, and $G_{(P)}$ acts on $\mathbb{P}^{n-1}_R$ through the homomorphism $\rho : G_{(P)} \to PGL_{n,R}$. We refer [12, Section 2] for detailed accounts in the case of $n = 2$.

Remark 2.3. Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$, and let p be a prime.

(1) The exact sequence of group schemes

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \xrightarrow{i} G_P \xrightarrow{\beta} G_{(P)} \longrightarrow 0$$

yields a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Q}^\times \arrow[r, "i"] & G_P(\mathbb{Q}) \arrow[r, "\beta"] & G_{(P)}(\mathbb{Q}) \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z}_{(p)}^\times \arrow[r, "i"] \arrow[u] \arrow[d] & G_P(\mathbb{Z}_{(p)}) \arrow[r, "\beta"] \arrow[u] \arrow[d] & G_{(P)}(\mathbb{Z}_{(p)}) \arrow[r] \arrow[u] \arrow[d] & 0 \\
0 \arrow[r] & (\mathbb{Z}/p^N\mathbb{Z})^\times \arrow[r, "i"] & G_P(\mathbb{Z}/p^N\mathbb{Z}) \arrow[r, "\beta"] & G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) \arrow[r] & 0
\end{tikzcd}$$

(2) The reduction maps $G_P(\mathbb{Z}_{(p)}) \to G_P(\mathbb{Z}/p^N\mathbb{Z})$ and $G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ are surjective.

Indeed, let R be a ring. Then the exact sequence of group schemes

$$0 \longrightarrow \mathbb{G}_{m,\mathbb{Z}} \xrightarrow{i} G_P \xrightarrow{\beta} G_{(P)} \longrightarrow 0$$

yields an exact sequence

$$0 \longrightarrow R^\times \xrightarrow{i} G_P(R) \xrightarrow{\beta} G_{(P)}(R) \longrightarrow H^1(R, \mathbb{G}_{m,R}),$$

and therefore, an exact sequence

$$0 \longrightarrow R^\times \xrightarrow{i} G_P(R) \xrightarrow{\beta} G_{(P)}(R) \longrightarrow 0$$

if $H^1(R, \mathbb{G}_{m,R}) = \mathrm{Pic}(R) = 0$. This is the case when $R = \mathbb{Q}$, $\mathbb{Z}_{(p)}$ or $\mathbb{Z}/p^N\mathbb{Z}$.

Furthermore, $\eta \in \mathbb{Z}[\theta]$ is invertible if and only if $\mathrm{Nr}\,\eta \not\equiv 0 \mod p$. Therefore the reduction maps $G_P(\mathbb{Z}_{(p)}) \to G_P(\mathbb{Z}/p^N\mathbb{Z})$ and $G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ are surjective.

Notation 2.4. Let p be a prime number, and let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}_p[t]$. Let $|\ |_p$ denote the p-adic absolute value normalized by $|p|_p = 1/p$. We define a real-valued function $\|\ \|_p$ on the $\mathbb{Q}_p$-linear space $\tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathbb{Q}_p.1 + \mathbb{Q}_p.\theta + \cdots + \mathbb{Q}_p.\theta^{n-1}$ by

$$\|a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}\|_p = \max(|a_0|_p, |a_1|_p, \ldots, |a_{n-1}|_p)$$

(the sup-norm). It is readily seen that

(a) $\|\eta\|_p = 0$ if and and if $\eta = 0$;

(b) $\|c\eta\|_p = |c|_p \|\eta\|_p$ for $c \in \mathbb{Q}_p$ and $\eta \in \tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

(c) $\|\eta + \xi\|_p \le \max(\|\eta\|_p, \|\xi\|_p)$ for $\eta, \xi \in \tilde{R} \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

(d) $\|\eta\xi\|_p \le \|\eta\|_p \|\xi\|_p$ for $\eta, \xi \in \tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

The $\mathbb{Q}_p$-linear space $\tilde{R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is complete with respect to the norm $\|\ \|_p$.

Definition 2.5. Let p be a prime. Let $\eta \in \tilde{R}$. Then the series

$$\exp \eta = \sum_{k=0}^{\infty} \frac{\eta^k}{k!}$$

converges in $\tilde{R}$ if $p > 2$ and $\eta \in p\tilde{R}$ or if $p = 2$ and $\eta \in 4\tilde{R}$. The map $\exp : p^N\tilde{R} \to \tilde{R}$ induces an isomorphism of the additive group $p^N\tilde{R}$ to the multiplicative group $1 + p^N\tilde{R}$ if $p > 2$ and $N \ge 1$ or if $p = 2$ and $N \ge 2$. The inverse of $\exp : p^N\tilde{R} \xrightarrow{\sim} 1 + p^N\tilde{R}$ is given by

$$1 + \eta \mapsto \log(1 + \eta) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \eta^k.$$

Hereafter we *assume that* $p > 2$ *and* $N \ge 1$ *or that* $p = 2$ *and* $N \ge 2$. Then we obtain the assertions mentioned below, paraphrasing the arguments developed in [13, Section2] and omitting detailed proofs.

Proposition 2.6. *The map* $\exp : p^N\tilde{R} \to G_P(\mathbb{Z}_p)$ *gives rise to an isomorphism*

$$\exp : p^N\tilde{R} \xrightarrow{\sim} \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z})].$$

Therefore, $\mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z})]$ *is a free* $\mathbb{Z}_p$*-module of rank* n*. Moreover, we obtain an exact sequence*

$$0 \longrightarrow p^N\tilde{R} \xrightarrow{\exp} G_P(\mathbb{Z}_p) \longrightarrow G_P(\mathbb{Z}/p^N\mathbb{Z}) \longrightarrow 0.$$

Corollary 2.7. *Let* $\eta \in G_P(\mathbb{Z}_p)$*, and assume that*

$$\eta \in \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^N\mathbb{Z})],\ \eta \notin \mathrm{Ker}[G_D(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+1}\mathbb{Z})].$$

Then we have

$$\eta^p \in \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+1}\mathbb{Z})],\ \eta^p \notin \mathrm{Ker}[G_P(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+2}\mathbb{Z})].$$

Remark 2.7.1. We can verify the assertion much more simply, using the well-known congruence relation

$$(1 + p^N\xi)^p \equiv 1 + p^{N+1}\xi \mod p^{N+2}$$

under the assumption that $p > 2$, $N \geq 1$, or $p = 2$, $N \geq 2$. However, we adopt here an argument applicable also to $G_{(P)}(\mathbb{Z}_p)$, as is done in Corollary 2.10.

Corollary 2.8. *If* $p > 2$*, then we have an exact sequence*

$$0 \longrightarrow (\mathbb{Z}/p^{N-1}\mathbb{Z})^n \longrightarrow G_P(\mathbb{Z}/p^N\mathbb{Z}) \longrightarrow G_P(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0.$$

On the other hand, if $p = 2$*, then we have an exact sequence*

$$0 \longrightarrow (\mathbb{Z}/2^{N-2}\mathbb{Z})^n \longrightarrow G_P(\mathbb{Z}/2^N\mathbb{Z}) \longrightarrow G_P(\mathbb{Z}/4\mathbb{Z}) \longrightarrow 0.$$

Corollary 2.9. *The reduction map* $G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ *is surjective. Furthermore,* $\mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})]$ *is a free* $\mathbb{Z}_p$*-module of rank* $n-1$*.*

Proof. Consider a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & p^N\mathbb{Z}_p \arrow[r, "i"] \arrow[d, "\exp"] & p^N\tilde{R} \arrow[d, "\exp"] & & \\
0 \arrow[r] & \mathbb{G}_m(\mathbb{Z}_p) \arrow[r] \arrow[d] & G_P(\mathbb{Z}_p) \arrow[r] \arrow[d] & G_{(P)}(\mathbb{Z}_p) \arrow[r] \arrow[d] & 0 \cdot \\
0 \arrow[r] & \mathbb{G}_m(\mathbb{Z}/p^N\mathbb{Z}) \arrow[r] \arrow[d] & G_P(\mathbb{Z}/p^N\mathbb{Z}) \arrow[r] \arrow[d] & G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}$$

Here $i : p^N\mathbb{Z}_p \to p^N\tilde{R}$ denotes the canonical injection. We obtain the result, applying the snake lemma to the above diagram and noting that $\mathrm{Coker}[i : p^N\mathbb{Z}_p \to p^N\tilde{R}]$ is a free $\mathbb{Z}_p$-module of rank $n-1$.

Corollary 2.10. *Let $\eta \in G_{(P)}(\mathbb{Z}_p)$, and assume that*

$$\eta \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})],\ \eta \notin \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^{N+1}\mathbb{Z})].$$

Then we have

$$\eta^p \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_P(\mathbb{Z}/p^{N+1}\mathbb{Z})],\ \eta^p \notin \mathrm{Ker}[G_{(P)}(\mathbb{Z}_p) \to G_{(P)}(\mathbb{Z}/p^{N+2}\mathbb{Z})].$$

Corollary 2.11. *If $p > 2$, then we have an exact sequence*

$$0 \longrightarrow (\mathbb{Z}/p^{N-1}\mathbb{Z})^{n-1} \longrightarrow G_{(P)}(\mathbb{Z}/p^N\mathbb{Z}) \longrightarrow G_{(P)}(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0.$$

On the other hand, if $p = 2$, then we have an exact sequence

$$0 \longrightarrow (\mathbb{Z}/2^{N-2}\mathbb{Z})^{n-1} \longrightarrow G_{(P)}(\mathbb{Z}/2^N\mathbb{Z}) \longrightarrow G_{(P)}(\mathbb{Z}/4\mathbb{Z}) \longrightarrow 0.$$

3. Lucas sequences

Notation 3.1. Let R be a ring and $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in R[t]$. We put

$$\mathcal{L}(P,R) = \{(w_k)_{k\geq 0} \in R^{\mathbb{N}}\ ;\ w_{k+n} = P_1w_{k+n-1} + \cdots + P_{n-1}w_{k+1} + P_nw_k \text{ for each } k \geq 0\}.$$

The elements of $\mathcal{L}(P,R)$ are nothing but the linear recurrence sequences with the characteristic polynomial $P(t)$. The map $(w_k)_{k\geq 0} \mapsto (w_0, w_1, \dots, w_{n-1})$ gives rise to an R-isomorphism $\mathcal{L}(P,R) \xrightarrow{\sim} R^n$.

Definition 3.2. Put $\tilde{R} = R[t]/(P(t))$ and $\theta = t \mod P(t)$. Then $\{1, \theta, \dots, \theta^{n-1}\}$ is an R-basis of $\tilde{R}$. We define an R-homomorphism $\omega : \tilde{R} \to R$ by

$$\omega(a_0 + a_1\theta + \cdots + a_{n-2}\theta^{n-2} + a_{n-1}\theta^{n-1}) = a_{n-1}.$$

Moreover, we define an R-homomorphism $\tilde{\omega} : \tilde{R} \to R^{\mathbb{N}}$ by

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

Proposition 3.3. *The R-homomorphism $\tilde{\omega} : \tilde{R} \to R^{\mathbb{N}}$ induces an R-isomorphism $\tilde{\omega} : \tilde{R} \to \mathcal{L}(P,R)$.*

Proof. Put $w_k = \omega(\theta^k \eta)$ for each $k \geq 0$. Then $\tilde{\omega}(\eta) = (w_k)_{k \geq 0} \in \mathcal{L}(P, R)$ since

$$\begin{aligned}
&w_{k+n} - P_1 w_{k+n-1} - \cdots - P_{n-1} w_{k+1} - P_n w_k \\
&= \omega(\theta^{k+n}\eta) - P_1\omega(\theta^{k+n-1}\eta) - \cdots - P_{n-1}\omega(\theta^{k+1}\eta) - P_n\omega(\theta^k\eta) \\
&= \omega((\theta^n - P_1\theta^{n-1} - \cdots - P_{n-1}\theta - P_n)\theta^k\eta) = 0.
\end{aligned}$$

Moreover, the inverse of $\tilde{\omega} : \tilde{R} \to \mathcal{L}(P, R)$ is given by

$$\begin{aligned}
&(w_0, w_1, \ldots, w_{n-1}, \ldots) \mapsto \\
&\quad w_0\theta^{n-1} + (w_1 - P_1 w_0)\theta^{n-2} + \cdots + (w_{n-1} - P_1 w_{n-2} - \cdots - P_{n-2} w_1 - P_{n-1} w_0).
\end{aligned}$$

Corollary 3.4. *Let I be an ideal of R, and let $\eta, \eta' \in \tilde{R}$. Then $\eta \equiv \eta' \mod I$ if and only if $\tilde{\omega}(\eta) \equiv \tilde{\omega}(\eta') \mod I$ in $\mathcal{L}(P, R)$.*

Example 3.5. We shall call $(L_k)_{k \geq 0} = \tilde{\omega}(1) \in \mathcal{L}(P, R)$ the *Lucas sequence* associated to $P(t)$. That is to say, the sequence $(L_k)_{k \geq 0}$ is the linear recurrence sequence with the characteristic polynomial $P(t)$ and with initial terms $L_0 = \ldots = L_{n-2} = 0$ and $L_{n-1} = 1$.

Example 3.6. Assume $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1} t - P_n \in \mathbb{Z}[t]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ denote the roots of the equation $P(t) = 0$, and put

$$S_0 = n \text{ and } S_k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k \text{ for } k \geq 1.$$

Then $(S_k)_{k \geq 0} \in \mathcal{L}(P, \mathbb{Z})$, and we have $\tilde{\omega}(P'(\theta)) = (S_k)_{k \geq 0}$.

Indeed, derivating

$$\log P(t) = \sum_{j=1}^{n} \log(t - \alpha_j),$$

we obtain

$$\frac{P'(t)}{P(t)} = \sum_{k=0}^{\infty} S_k t^{-k-1}$$

and therefore

$$t^l P'(t) = P(t)(S_0 t^{l-1} + \cdots + S_{l-2} t + S_{l-1}) + P(t) \sum_{k=0}^{\infty} S_{k+l} t^{-k-1}$$

for $l \geq 1$. Put now

$$R_l(t) = P(t) \sum_{k=0}^{\infty} S_{k+l} t^{-k-1}$$

for $l \geq 0$. Then it is readily seen that $R_l(t) \in \mathbb{Z}[t]$, deg $R_l(t) \leq n - 1$ and the coefficient of t^{n-1} in $R_l(t)$ is given by S_l. Hence we obtain

$$\omega(\theta^l P'(\theta)) = \omega(R_l(\theta)) = S_l.$$

3.7. We define an R-algebra structure of $\mathcal{L}(P,R)$ through the R-isomorphism $\tilde{\omega} : \tilde{R} \xrightarrow{\sim} \mathcal{L}(P,R)$. Then the Lucas sequence $(L_k)_{k\geq 0} = \tilde{\omega}(1)$ is the unit of the ring $\mathcal{L}(f,R)$. It is readily seen that the multiplication by θ on $\tilde{R}$ induces the shift operation $(w_k)_{k\geq 0} \mapsto (w_{k+1})_{k\geq 0}$ on $\mathcal{L}(P,R)$ through the isomorphism $\tilde{\omega} : \tilde{R} \xrightarrow{\sim} \mathcal{L}(P,R)$.

Now let $\eta \in \tilde{R}$ and $\boldsymbol{w} = \tilde{\omega}(\eta) \in \mathcal{L}(P,R)$. We define $\Delta(\boldsymbol{w}) \in R$ by $\Delta(\boldsymbol{w}) = \mathrm{Nr}\,\eta$. Then $\boldsymbol{w}$ is invertible in $\mathcal{L}(P,R)$ if and only if $\Delta(\boldsymbol{w})$ is invertible in R.

Remark 3.8. Let $\rho : \tilde{R} \to M(n,R)$ denote the regular representation with respect to the R-basis $\{1, \theta, \dots, \theta^{n-1}\}$. Then the square matrix $\rho(\eta)$ is defined by

$$(\eta\ \eta\theta\ \dots\ \eta\theta^{n-1}) = (1\ \theta\ \dots\ \theta^{n-1})\rho(\eta).$$

Define now square matrices L and W by

$$L = \begin{pmatrix} L_0 & L_1 \dots & L_{n-1} \\ L_1 & L_2 \dots & L_n \\ \vdots & \vdots \ddots & \vdots \\ L_{n-1} & L_n \dots & L_{2n-2} \end{pmatrix}$$

and

$$W = \begin{pmatrix} w_0 & w_1 \dots & w_{n-1} \\ w_1 & w_2 \dots & w_n \\ \vdots & \vdots \ddots & \vdots \\ w_{n-1} & w_n \dots & w_{2n-2} \end{pmatrix}.$$

Then we have an equality

$$W = L\rho(\eta),$$

which implies

$$\det W = (-1)^{n(n-1)/2}\mathrm{Nr}\,\eta.$$

since $L_0 = \cdots = L_{n-2} = 0$ and $L_{n-1} = 1$. The determinant $\det W$ is often called the *invariant* of the linear recurrence sequence $(w_k)_{k\geq 0}$.

Remark 3.9. Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$, and let D denote the discriminant of the polynomial $P(t)$. Then we have $P'(\theta)^2 = D$ in $\tilde{R} = \mathbb{Z}[t]/(P(t))$. Define now $(S_k)_{k\geq 0} \in \mathcal{L}(P,\mathbb{Z})$ as in 3.6 by

$$S_0 = n \text{ and } S_k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k \text{ for } k \geq 1,$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the roots of the equation $P(t) = 0$. Then the square of $(S_k)_{k\geq 0}$ coincides with the sequence $(DL_k)_{k\geq 0}$ in the ring $\mathcal{L}(P,\mathbb{Z})$.

Remark 3.10. Ward [15] introduced the residue ring $\tilde{R} = R[t]/(P(t))$ to examine periodicities of linear recurrence sequences, where $R = \mathbb{Z}/m\mathbb{Z}$. We may feel an atmosphere of the period in his sentence [15, p.602]:

The method employed are elementary in the sense that no use is made either of the theory of ideals or the fundamental theorem of algebra. Instead free use is made of polynomial congruences to single and double moduli in the spirit of Kronecker's theory of algebraic fields.

Analyzing the residue ring $\tilde{R} = R[t]/(P(t))$ in details, Hall [7] also obtained remarkable results on periodicities of linear recurrence sequences. Applying the theory of group schemes to the method employed by Ward and Hall, we have naturally gotten formulations presented in [13], [14] and this survey.

4. Rank and period of Lucas sequences

Definition 4.1. Let $(L_k)_{k\geq 0}$ denote the Lucas sequence associated to $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$. The rank (resp. the period) of the Lucas sequence $(L_k)_{k\geq 0} \mod m$ is defined as the least positive integer k such that $L_k \equiv 0 \mod m, \ldots, L_{k+n-2} \equiv 0 \mod m$ (resp. $L_k \equiv 0 \mod m, \ldots, L_{k+n-2} \equiv 0 \mod m$ and $L_{k+n-1} \equiv 1 \mod m$), if exists. We shall denote by $r(m)$ (resp. $k(m)$) the rank (resp. the period) of the Lucas sequence $(L_k)_{k\geq 0} \mod m$.

Theorem 4.2. *Let m be an integer with $m \geq 2$ and $(m, P_n) = 1$. Then we have*:

(1) *$k(m)$ is equal to the order of θ in $G_P(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}[t]/(m, P(t)))^\times$.*

(2) *$r(m)$ is equal to the order of $\beta(\theta)$ in $G_{(P)}(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}[t]/(m, P(t)))^\times/(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. The first assertion follows immediately from Corollary 3.4. Consider now the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & (\mathbb{Z}/m\mathbb{Z})^\times \arrow[r] \arrow[d, equal] & G_P(\mathbb{Z}/m\mathbb{Z}) \arrow[r] \arrow[d, "\wr\ \tilde{\omega}"] & G_{(P)}(\mathbb{Z}/m\mathbb{Z}) \arrow[r] \arrow[d, "\wr\ \tilde{\omega}"] & 0 \\
0 \arrow[r] & (\mathbb{Z}/m\mathbb{Z})^\times \arrow[r] & \mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})^\times \arrow[r] & \mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})^\times/(\mathbb{Z}/m\mathbb{Z})^\times \arrow[r] & 0
\end{tikzcd}$$

Let $\eta \in G_P(\mathbb{Z}/m\mathbb{Z})$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then $\tilde{\omega}(\eta) = (\underbrace{0, \ldots, 0}_{n-1}, a, \ldots)$ in $\mathcal{L}(P, \mathbb{Z}/m\mathbb{Z})$ if and only if $\eta = a$ in $G_P(\mathbb{Z}/m\mathbb{Z})$, which means $\beta(\eta) = 1$ in $G_{(P)}(\mathbb{Z}/m\mathbb{Z})$. Hence we obtain the second assertion.

Corollary 4.3. *Let m be an integer with $m \geq 2$ and $(m, P_n) = 1$. Then*:

(1) *We have $L_k, \ldots, L_{k+n-2} \equiv 0 \mod m$ if and only if k is divisible by $r(m)$.*

(2) *We have $L_k, \ldots, L_{k+n-2} \equiv 0 \mod m$ and $L_{k+n-1} \equiv 1 \mod m$ if and only if k is divisible by $k(m)$.*

(3) *The rank $r(m)$ divides the order of $G_{(P)}(\mathbb{Z}/m\mathbb{Z})$.*

(4) *The period $k(m)$ divides the order of $G_P(\mathbb{Z}/m\mathbb{Z})$.*

(5) *The rank $r(m)$ divides the period $k(m)$.*

Corollary 4.4. *Let p be an odd prime. Then $k(p)/r(p)$ divides $p-1$.*

Example 4.5. Let p be a prime with $(p, P_n) = 1$.

(a) Assume that $P(t)$ is factorized by distinct linear polynomials in $\mathbb{F}_p[t]$. Then $G_P(\mathbb{F}_p)$ and $G_{(P)}(\mathbb{F}_p)$ is isomorphic to the multiplicative groups $\mathbb{G}_m^n(\mathbb{F}_p) = (\mathbb{F}_p^\times)^n$ and $\mathbb{G}_m^{n-1}(\mathbb{F}_p) = (\mathbb{F}_p^\times)^{n-1}$, respectively. Then both $r(p)$ and $k(p)$ divide $p-1$.

(b) Assume that $P(t)$ remains irreducible in $\mathbb{F}_p[t]$. Then $G_P(\mathbb{F}_p)$ isomorphic to the multiplicative groups $\mathbb{F}_{p^n}^\times$, which is cyclic of order $p^n - 1$. Therefore, $k(p)$ divides $p^n - 1$. Furthermore, $G_{(P)}(\mathbb{F}_p)$ is cyclic of order $(p^n-1)/(p-1)$. Therefore, $r(p)$ divides $(p^n-1)/(p-1)$.

In particular, if $P(t)$ is a quadratic polynomial, we recover the results of Lucas and Carmichael mentioned in 1.2:

(1) If $\left(\dfrac{D}{p}\right) = 1$, then we have $k(p)|(p-1)$ and $r(p)|(p-1)$;

(2) $\left(\dfrac{D}{p}\right) = -1$, then we have $k(p)|(p^2-1)$ and $r(p)|(p+1)$;

(3) If $p|D$, then we have $k(p)|p(p-1)$ and $r(p) = p$.

Proposition 4.6 generalizes the results of Lucas and Carmichael mentioned as (2) and (3) in 1.2:

Proposition 4.6. *Let $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$, and let p be a prime with $(p, P_n) = 1$. Put*

$$\nu = \begin{cases} \max\{N \ ; \ \beta(\theta)^{r(p)} \in \operatorname{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})] & \text{if } p > 2 \\ \max\{N \ ; \ \beta(\theta)^{r(4)} \in \operatorname{Ker}[G_{(P)}(\mathbb{Z}_{(2)}) \to G_{(P)}(\mathbb{Z}/2^N\mathbb{Z})] & \text{if } p = 2 \end{cases}$$

and

$$\nu' = \begin{cases} \max\{N \ ; \ \theta^{k(p)} \in \operatorname{Ker}[G_P(\mathbb{Z}_{(p)}) \to G_P(\mathbb{Z}/p^N\mathbb{Z})] & \text{if } p > 2 \\ \max\{N \ ; \ \theta^{k(4)} \in \operatorname{Ker}[G_P(\mathbb{Z}_{(2)}) \to G_P(\mathbb{Z}/2^N\mathbb{Z})] & \text{if } p = 2 \end{cases}.$$

Then we have, for $N > \nu$,

$$r(p^N) = \begin{cases} p^{N-\nu} r(p) & \text{if } p > 2 \\ 2^{N-\nu} r(4) & \text{if } p = 2 \end{cases}$$

and, for $N > \nu'$,

$$k(p^N) = \begin{cases} p^{N-\nu'} k(p) & \text{if } p > 2 \\ 2^{N-\nu'} k(4) & \text{if } p = 2 \end{cases}.$$

Proof. First we prove the assertion (1). Assume that $N > \nu$. By the definition of ν, we have

$$\beta(\theta)^{r(p)} \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^{\nu}\mathbb{Z})]$$

and

$$\beta(\theta)^{r(p)} \notin \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^{\nu+1}\mathbb{Z})].$$

Therefore, by Corollary 2.10, we obtain inductively

$$\beta(\theta)^{p^{N-\nu}r(p)} \in \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^{N}\mathbb{Z})]$$

and

$$\beta(\theta)^{p^{N-\nu-1}r(p)} \notin \mathrm{Ker}[G_{(P)}(\mathbb{Z}_{(p)}) \to G_{(P)}(\mathbb{Z}/p^{N}\mathbb{Z})].$$

These imply that $r(p^N) = p^{N-\nu}r(p)$.

We can prove the assertion (2) similarly, using here Corollary 2.7.

It is more subtle to examine the relation between $r(p^N)$ and $k(p^N)$ even in the case of $n = 2$, as is indicated by Propositions 4.7.1–4.7.5. In the following statements, P and Q are integers and $P(t) = t^2 - Pt + Q$. We refer to [14, Section 3] for verification.

Proposition 4.7.1. *Assume that* $P \equiv 0 \mod 2$, $Q \equiv 1 \mod 2$ *and* $P \neq 0$, *and put* $\nu = \mathrm{ord}_2 P$. *Then*:

(1) *We have*

$$r(2^N) = \begin{cases} 2 & \text{if } N \leq \nu \\ 2^{N-\nu+1} & \text{if } N \geq \nu + 1 \end{cases}.$$

(2) *If* $\nu = 1$, *then we have* $k(2^N) = 2^N$ *for* $N \geq 1$.

(3) *If* $\nu \geq 2$, *then we have*

$$k(2^n) = \begin{cases} 2^{N-\nu+1} & \begin{array}{l}\text{if } N \geq \nu + 1 \text{ and} \\ (\text{the order of } -Q \bmod 2^N) \leq 2^{N-\nu}\end{array} \\ 2 \times (\text{the order of } -Q \bmod 2^N) & \text{otherwise} \end{cases}.$$

Proposition 4.7.2. *Assume that* $P \equiv 1 \mod 2$, $Q \equiv -1 \mod 4$ *and* $(P^2 - Q)(P^2 - 3Q) \neq 0$.

(1) *Put* $\nu = \mathrm{ord}_2(P^2 - Q)(P^2 - 3Q)$. *Then we have* $\nu \geq 3$ *and*

$$r(2^N) = \begin{cases} 3 & \text{if } N = 1 \\ 6 & \text{if } 2 \leq N \leq \nu \\ 6 \times 2^{N-\nu} & \text{if } N \geq \nu + 1 \end{cases}.$$

(2) *We have* $k(2^N) = 3 \times 2^{N-1}$ *for* $N \geq 1$.

Proposition 4.7.3. *Assume that* $P \equiv 1 \mod 2$, $Q \equiv 1 \mod 4$ *and* $P^2 - Q \neq 0$, *and put* $\nu = \mathrm{ord}_2(P^2 - Q)$. *Then we have* $\nu \geq 2$ *and*

$$r(2^N) = \begin{cases} 3 & \text{if } N \leq \nu \\ 3 \times 2^{N-\nu} & \text{if } N \geq \nu + 1 \end{cases}.$$

Proposition 4.7.4. *Assume that* $Q \equiv 1 \mod 4$. *Then*:

(1) *If* $P \equiv 5 \mod 8$, *then we have*

$$k(2^N) = \begin{cases} 3 & \text{if } N = 1 \\ 6 & \text{if } N = 2 \\ 3 \times 2^{N-2} & \text{if } N \geq 3 \end{cases}.$$

(2) *If* $P \equiv 5 \mod 8$, *then we have*

$$k(2^N) = \begin{cases} 3 & \text{if } N = 1, 2 \\ 3 \times 2^{N-2} & \text{if } N \geq 3 \end{cases}.$$

Proposition 4.7.5. *Assume that* $P \equiv \pm 1 \mod 8$, $Q \equiv 1 \mod 4$ *and* $P^2 - Q \neq 0$. *Then there exists* $r \in \mathbb{Z}_2$ *such that* $r^2 = -D/3$ *and* $r \equiv 1 \mod 4$.

(1) *Assume* $P \equiv 1 \mod 8$, *and put* $\mu = \min[\mathrm{ord}_2(P + r - 2) - 1, \mathrm{ord}_2(r - 1)]$. *Then we have* $\mu \geq 2$ *and*

$$k(2^N) = \begin{cases} 3 & \text{if } N = 1 \\ 6 & \text{if } 2 \leq N \leq \mu + 1 \\ 6 \times 2^{N-\mu-1} & \text{if } N \geq \mu + 2 \end{cases}.$$

(2) *Assume* $P \equiv -1 \mod 8$, *and put* $\mu = \min[\mathrm{ord}_2(P + r), \mathrm{ord}_2(r - 1)]$. *Then we have* $\mu \geq 2$ *and*

$$k(2^N) = \begin{cases} 3 & \text{if } 1 \leq N \leq \mu \\ 3 \times 2^{N-\mu} & \text{if } N \geq \mu + 1 \end{cases}.$$

5. The action of Θ on Lucas sequences

Notation 5.1. Let R be a ring and $P(t) = t^n - P_1 t^{n-1} - \cdots - P_{n-1} t - P_n \in R[t]$. Then the isomorphism of rings $\tilde{\omega} : \tilde{R} = R/(P(t)) \xrightarrow{\sim} \mathcal{L}(P, R)$ gives rise to an isomorphism of the multiplicative group $\tilde{\omega} : G_P(R) = \tilde{R}^\times \xrightarrow{\sim} \mathcal{L}(P, R)^\times$, and $G_P(R)$ acts on $\mathcal{L}(P, R)$ by the multiplication.

We define a subset $\mathcal{L}(P,R)^\circ$ of $\mathcal{L}(P,R)$ by

$$\mathcal{L}(P,R)^\circ = \{\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P,R)\ ;\ w_0R + w_1R + \cdots + w_{n-1}R = R\}.$$

Then $\mathcal{L}(P,R)^\circ$ is stable by the action of $G_P(R)$ on $\mathcal{L}(P,R)$.

The action of $G_P(R)$ on $\mathcal{L}(P,R)^\times \subset \mathcal{L}(P,R)^\circ \subset \mathcal{L}(P,R)$ induces actions of $G_P(R)/R^\times$ on $\mathcal{L}(P,R)^\times/R^\times \subset \mathcal{L}(P,R)^\circ/R^\times \subset \mathcal{L}(P,R)/R^\times$. If $\mathrm{Pic}(R) = 0$, then the canonical homomorphism $G_P(R)/R^\times \to G_{(P)}(R)$ is bijective, and $\mathcal{L}(P,R)^\circ/R^\times$ is identified to the projective space $\mathbb{P}^{n-1}(R)$ by $[\boldsymbol{w}] \mapsto (w_0 : w_1 : \ldots : w_{n-1})$.

Assume now that P_n is invertible in R. Then θ is invertible in $\tilde{R}$. We denote by Θ the subgroup of $G_P(R) = \tilde{R}^\times$ generated by θ. By abuse of notation, we denote by Θ also the subgroup of $G_{(P)}(R)$ generated by θ.

Hereafter we assume $P(t) = t^n - P_1t^{n-1} - \cdots - P_{n-1}t - P_n \in \mathbb{Z}[t]$.

5.2. Let m be an integer ≥ 2 with $(m, P_n) = 1$. Let $\eta \in \tilde{R}$, and put $\boldsymbol{w} = \tilde{\omega}(\eta) \in \mathcal{L}(P,\mathbb{Z})$. Put

$$\Theta\eta = \{\theta^k\eta\ ;\ k \geq 0\} \subset \tilde{R} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}[t]/(m, P(t)).$$

Then we have

$$\begin{aligned} |\Theta\eta| &= \text{the least positive integer } l \text{ such that } \theta^l\eta \equiv \eta \mod m \\ &= \text{the least positive integer } l \text{ such that } w_{l+j} \equiv w_j \mod m \text{ for } 0 \leq j < n. \end{aligned}$$

That is to say, $|\Theta\eta|$ is nothing but the period mod m of the linear recurrence sequences $\boldsymbol{w} = (w_k)_{k\geq 0}$.

Furthermore, assume that $(w_0, w_1, \ldots, w_{n-1}, m) = 1$. Let $[\eta]$ denote the image of η in $\mathbb{Z}[t]/(m, P(t))/(\mathbb{Z}/m\mathbb{Z})^\times$. Put

$$\Theta[\eta] = \{\theta^k[\eta]\ ;\ k \geq 0\} \subset (\mathbb{Z}[t]/(m, P(t)))/(\mathbb{Z}/m\mathbb{Z})^\times = \mathbb{P}^{n-1}(\mathbb{Z}/m\mathbb{Z}).$$

Then we have

$$\begin{aligned} |\Theta\eta| = \ &\text{the least positive integer } l \text{ such that} \\ &(w_l : w_{l+1} : \ldots : w_{l+n-1}) = (w_0 : w_1 : \ldots : w_{n-1}) \text{ in } \mathbb{P}^{n-1}(\mathbb{Z}/m\mathbb{Z}). \end{aligned}$$

Remark 5.3. Assume that $P_n \neq 0$. Then θ is invertible in $\tilde{R}\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}/(P(t))$. We may call the quotient group $G_{(P)}(\mathbb{Q})/\Theta$ the Laxton group associated to the polynomial $P(t) \in \mathbb{Z}[t]$. Indeed, if P and Q are relatively prime non-zero integers with $P^2 - 4Q \neq 0$ and $P(t) = t^2 - Pt + Q$, then the isomorphism of rings $\tilde{\omega} : \tilde{R}\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}[t]/(t^2 - Pt + Q) \xrightarrow{\sim} \mathcal{L}(P,\mathbb{Q})$ induces an isomorphism of groups $G_{(P)}(\mathbb{Q})/\Theta \xrightarrow{\sim} G(P)$ as is established as [13, Theorem 4.2] and [14, Theorem 4.2].

Remark 5.3.1. We refer to [13, Remark 4.4] for correction of some statements in [5].

Remark 5.3.2. The assertion of [13, Theorem 4.2] and [14, Theorem 4.2] is established by Aoki and Kida [1] independently with a different terminology.

5.4. Let $\eta \in \tilde{R} = \mathbb{Z}[t]/(P(t))$ and $\boldsymbol{w} = \tilde{\omega}(\eta) \in \mathcal{L}(P, \mathbb{Z})$. Denote by $k(\boldsymbol{w}, m)$ the period mod m of $\boldsymbol{w}$. It would be interesting to compare $k(\boldsymbol{w}, m)$ with $k(m)$, the period of the Lucas sequence $(L_k)_{k\geq 0}$ associated to $P(t)$. If m is prime to P_n, then $k(\boldsymbol{w}, m)$ is given as the Θ-orbit length of η in $\tilde{R} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}[t]/(m, P(t))$, and therefore, $k(\boldsymbol{w}, m)$ divides $k(m)$. In particular, if η is invertible in $\mathbb{Z}[t]/(m, P(t))$, then we obtain $k(\boldsymbol{w}, m) = k(m)$.

Moreover, assume that $(w_0, w_1, \ldots, w_{n-1}, m) = 1$ and $(P_{n-1}, m) = 1$. Denote by $r(\boldsymbol{w}, m)$ the period of the ratio $(w_k : w_{k+1} : \ldots : w_{k+n-1}) \in \mathbb{P}^{n-1}(\mathbb{Z}/m\mathbb{Z})$. It would be interesting also to compare $r(\boldsymbol{w}, m)$ with $r(m)$, the rank of the Lucas sequence $(L_k)_{k\geq 0}$ associated to $P(t)$. In fact, $r(\boldsymbol{w}, m)$ is given as the Θ-orbit length of $[\eta]$ in $(\mathbb{Z}[t]/(m, P(t)))/(\mathbb{Z}/m\mathbb{Z})^{\times}$, and therefore, $r(\boldsymbol{w}, m)$ divides $r(m)$. In particular, if η is invertible in $\mathbb{Z}[t]/(m, P(t))$, then we obtain $r(\boldsymbol{w}, m) = r(m)$.

In the case of $P(t) = t^2 - Pt + Q \in \mathbb{Z}[t]$, we have gotten following assertions, which generalize results established by Aoki-Sakai [2] and mentioned as Theorem 1.12:

Proposition 5.5. ([13, Proposition 3.22] and [14, Proposition 3.26]) *Let p be a prime, N a positive integer and $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$. Assume that neither Q nor (w_0, w_1) is divisible by p. Then, there exists $k \geq 0$ such that $w_k \equiv 0 \mod p^N$ if and only if $(w_0 : w_1)$ is contained in the Θ-orbit of $(0 : 1)$ in $\mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z})$. Therefore we have*

$$\#\left\{(w_0 : w_1) \in \mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z}) \; ; \; \begin{matrix} (w_k)_{k\geq 0} \in \mathcal{L}(f, \mathbb{Z}/p^N\mathbb{Z}) \\ \text{and } w_k \neq 0 \text{ for any } k \end{matrix}\right\} = (p+1)p^{N-1} - r(p^N).$$

Theorem 5.6. ([13, Theorem 3.24] and [14, Theorem 3.27]) *Let p be a prime with $(p, Q) = 1$ and N a positive integer. Let $\boldsymbol{w} = (w_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z}_{(p)})$, and put $\mu = \mathrm{ord}_p \mathit{\Delta}(\boldsymbol{w})$. Assume that $(w_0, w_1) = \mathbb{Z}_{(p)}$. Then we have*

$$\text{the length of the orbit } (w_0 : w_1)\Theta \text{ in } \mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z}) = \begin{cases} 1 & (N \leq \mu) \\ r(p^{N-\mu}) & (n \geq \mu + 1) \end{cases}.$$

Example 5.7. Let $P(t) \in \mathbb{Z}[t]$, and put $\eta = P'(\theta) \in \tilde{R} = \mathbb{Z}[t]/(P(t))$ and $\tilde{\omega}(\eta) = (S_k)_{k\geq 0} \in \mathcal{L}(P, \mathbb{Z})$. Let D denote the discriminant of the polynomial $P(t)$. Then we have $\eta^2 = D$ in $\tilde{R}$. Therefore, if $D \neq 0$, then η is invertible in $\tilde{R}$ and $\beta(\eta)$ is of order 2 in $G_{(P)}(\mathbb{Q})$.

In the case of $n = 2$, we recover a result obtained by Lucas and Carmichael, which is mentioned as 1.4 (5):

— *Let $P(t) = t^2 - Pt + Q \in \mathbb{Z}[t]$ and p an odd prime with $(p, Q) = 1$. Then, there exists $k \geq 0$ such that $S_k \equiv 0 \mod p^N$ if and only if $r(p)$ is even. Furthermore, put $\mu = \mathrm{ord}_p D$. Then we have*

$$\text{the length of the orbit } (S_0 : S_1)\Theta \text{ in } \mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z}) = \begin{cases} 1 & (N \leq \mu) \\ r(p^{N-\mu}) & (n \geq \mu + 1) \end{cases}.$$

Indeed, assume that there exists $k \geq 0$ such that $S_k \equiv 0 \mod p^N$. Then, by Proposition 5.5, we obtain $\beta(\eta) \in \Theta \subset G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$. Hence $r(p^N) = |\Theta|$ is even since $\beta(\eta)$ is of order 2, and therefore $r(p)$ is also even. Conversely, assume that $r(p)$ is even. Then $r(p^N)$ is also even. Hence $\Theta \subset G_{(P)}(\mathbb{Z}/p^N\mathbb{Z})$ contains an element of order 2. We can conclude $\beta(\eta) = -1 \in \Theta$, noting that -1 is a unique element of order 2 of $G_{(P)}(\mathbb{Q})$.

The second assertion follows immediately from Theorem 5.6.

The problem is rather complicated for $k(m)$. We conclude the article, by giving two numerical examples. Example 5.8 is concerning the Fibonacci sequence, and Example 5.9 is concerning the Tribonacci sequence. Here we modify the method of Hall [7], employing terminologies of p-adic numbers.

Example 5.8. Put $P(t) = t^2 - t - 1$. Let θ denote the image of t in $\mathbb{Z}[t]/(t^2 - t - 1)$. Then we have $\mathrm{Nr}\,\theta = -1$ and $\mathrm{Disc}(P) = 5$.

Notation 5.8.1. The residue ring $\mathbb{Z}_2[\theta] = \mathbb{Z}_2[t]/(t^2 - t - 1)$ is a complete discrete valuation ring, and 2 is a uniformizer of $\mathbb{Z}_2[\theta]$. The order of θ in the multiplicative group $G_P(\mathbb{Z}/2^j\mathbb{Z}) = (\mathbb{Z}[\theta]/(2^j))^\times$ is given by $k(2^j) = 3 \cdot 2^{j-1}$ for $j \geq 1$.

Put

$$X_{N,j} = \begin{cases} \{0\} & (j = 0) \\ \{\eta \in \mathbb{Z}_2[\theta]/(2^N) \ ; \ \mathrm{ord}_2\eta = N - j\} & (1 \leq j \leq N) \end{cases}.$$

Then we obtain a decomposition

$$\mathbb{Z}[\theta]/(2^N) = X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,N-1} \cup X_{N,N}.$$

Proposition 5.8.2. *Under the notations above, we have*:

(1) $X_{N,j} = \{\eta \in \mathbb{Z}[\theta]/(2^N) \ ; \ |\Theta\eta| = k(2^j) = 3 \cdot 2^{j-1}\}$ *for* $1 \leq j \leq N$. *Therefore, the isomorphism* $\tilde{\omega} : \mathbb{Z}[\theta]/(2^N) \xrightarrow{\sim} \mathcal{L}(P, \mathbb{Z}/2^N\mathbb{Z})$ *gives rise to bijections*

$$X_{N,j} \xrightarrow{\sim} \{\boldsymbol{w} \in \mathcal{L}(P, \mathbb{Z}/2^N\mathbb{Z}) \ ; \ \boldsymbol{w} \text{ is of period } k(2^j) = 3 \cdot 2^{j-1}\}$$

for $1 \leq j \leq N$.

(2) $|X_{N,j}| = \begin{cases} 1 & (j=0) \\ 3 \cdot 4^{j-1} & (1 \leq j \leq N) \end{cases}.$

(3) $|\Theta \backslash X_{N,j}| = \begin{cases} 1 & (j=0) \\ 2^{j-1} & (1 \leq j \leq N) \end{cases}.$

Proof. (1) Let $\eta \in \mathbb{Z}[\theta]/(2^N)$ with $0 \leq \mathrm{ord}_2\eta < N$. Put $N - j = \mathrm{ord}_2\eta$. Then we have

$$\begin{aligned} |\Theta\eta| &= \text{the least positive integer } l \text{ such that } \theta^l\eta \equiv \eta \mod 2^N \\ &= \text{the least positive integer } l \text{ such that } \theta^l \equiv 1 \mod 2^j, \end{aligned}$$

which implies $|\Theta\eta| = k(2^j)$.

(2) For $0 \leq j \leq N-1$, we have

$$X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,j} = \mathrm{Ker}[\mathbb{Z}[\theta]/(2^N) \to \mathbb{Z}[\theta]/(2^{N-j})],$$

which implies $|X_{N,j}| = 4^j - 4^{j-1} = 3 \cdot 4^{j-1}$ for $1 \leq j \leq N$.

(3) It follows from (1) and (2) that $|\Theta \backslash X_{N,j}| = (3 \cdot 4^{j-1})/(3 \cdot 2^{j-1}) = 2^{j-1}$ for $1 \leq j \leq N$.

Notation 5.8.3. The residue ring $\mathbb{Z}_5[\theta] = \mathbb{Z}_5[t]/(t^2 - t - 1)$ is a complete discrete valuation ring, and $\sqrt{5} = 2\theta - 1$ is a uniformizer of $\mathbb{Z}_5[\theta]$. Recall that the order of θ in the multiplicative group $G_P(\mathbb{Z}/5^j\mathbb{Z}) = (\mathbb{Z}[\theta]/(5^j))^\times$ is given by $k(5^j) = 4 \cdot 5^j$ for $j \geq 1$.

Put

$$X_{N,j} = \begin{cases} \{0\} & (j=-1) \\ \{\eta \in \mathbb{Z}[\theta]/(5^N) \ ; \ \mathrm{ord}_5\eta = N - 1/2\} & (j=0) \\ \{\eta \in \mathbb{Z}[\theta]/(5^N) \ ; \ \mathrm{ord}_5\eta = N-j, N-j-1/2\} & (1 \leq j \leq N-1) \\ \{\eta \in \mathbb{Z}[\theta]/(5^N) \ ; \ \mathrm{ord}_5\eta = 0\} & (j=N) \end{cases}.$$

Then we obtain a decomposition

$$\mathbb{Z}[\theta]/(5^N) = X_{N,-1} \cup X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,N-1} \cup X_{N,N}.$$

Note that $\mathrm{ord}_5\eta = j \Leftrightarrow \mathrm{ord}_5\mathrm{Nr}\,\eta = 2j$.

Lemma 5.8.4. *Let j be an integer ≥ 1. Then we have* $\mathrm{ord}_5(\theta^{4\cdot 5^j} - 1) = j + 1/2$ *and* $\mathrm{ord}_5(\theta^k - 1) \leq j - 1/2$ *for $k < 4 \cdot 5^j$.*

Proposition 5.8.5. *Under the notations above, we have*:

(1) $X_{N,j} = \{\eta \in \mathbb{Z}[\theta]/(5^N) \ ; \ |\Theta\eta| = 4 \cdot 5^j\}$ *for $0 \leq j \leq N$. Therefore, the isomorphism $\tilde{\omega} : \mathbb{Z}[\theta]/(5^N) \xrightarrow{\sim} \mathcal{L}(P, \mathbb{Z}/5^N\mathbb{Z})$ gives rise to bijections*

$$X_{N,j} \xrightarrow{\sim} \{\boldsymbol{w} \in \mathcal{L}(P, \mathbb{Z}/5^N\mathbb{Z}) \ ; \ \boldsymbol{w} \text{ is of period } 4 \cdot 5^j\}$$

for $0 \leq j \leq N$.

(2) $$|X_{N,j}| = \begin{cases} 1 & (j=-1) \\ 4 & (j=0) \\ 24 \cdot 5^{2j-1} & (1 \leq j \leq N-1) \\ 4 \cdot 5^{2N-1} & (j=N) \end{cases}.$$

(3) $$|\Theta \backslash X_{N,j}| = \begin{cases} 1 & (j=-1,0) \\ 6 \cdot 5^{j-1} & (1 \leq j \leq N-1) \\ 5^{N-1} & (j=N) \end{cases}.$$

Proof. (1) Let $\eta \in \mathbb{Z}_5[\theta]/(5^N)$ with $0 \leq \mathrm{ord}_5 \eta < N$. Put $s = \mathrm{ord}_5 \eta$. Then we have

$$\begin{aligned} |\Theta\eta| &= \text{the least positive integer } l \text{ such that } \theta^l \eta \equiv \eta \mod 5^N \\ &= \text{the least positive integer } l \text{ such that } \theta^l \equiv 1 \mod 5^{N-s}. \end{aligned}$$

By Lemma, we have

$$l = \begin{cases} 4 & (\text{if } s = N-1/2) \\ 4 \cdot 5^j & (\text{if } s = N-j \text{ or } N-j-1/2) \\ 4 \cdot 5^N & (\text{if } s = 0) \end{cases}.$$

(2) For $0 \leq j \leq N-1$, we have

$$X_{N,-1} \cup X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,j} = \mathrm{Ker}[\mathbb{Z}[\theta]/(5^N) \to \mathbb{Z}[\theta]/(5^{N-j-1/2})],$$

which implies $|X_{N,j}| = 5^{2j+1} - 5^{2j-1} = 24 \cdot 5^{2j-1}$ for $1 \leq j \leq N$. On the other hand, we have $|X_{N,N}| = 5^{2N} - 5^{2N-1} = 4 \cdot 5^{2N-1}$ and $|X_{N,0}| = 5 - 1 = 4$.

(3) It follows from (1) and (2) that $|\Theta\backslash X_{N,j}| = (24 \cdot 5^{2j-1})/(4 \cdot 5^j) = 6 \cdot 5^{j-1}$ for $1 \leq j \leq N-1$, and $|\Theta \backslash X_{N,N}| = (4 \cdot 5^{2N-1})/(4 \cdot 5^N) = 5^{N-1}$.

Example 5.9. Put $P(t) = t^3 - t^2 - t - 1$. Let θ denote the image of t in $\mathbb{Z}[t]/(t^3 - t^2 - t - 1)$. Then we have $\mathrm{Nr}\,\theta = 1$ and $\mathrm{Disc}(P) = -44$.

Notation 5.9.1. The residue ring $\mathbb{Z}_5[\theta] = \mathbb{Z}_5[t]/(t^3 - t^2 - t - 1)$ is a complete discrete valuation ring, and 5 is a uniformizer of $\mathbb{Z}_5[\theta]$. Note that the order of θ in the multiplicative group $G_P(\mathbb{Z}/5^j\mathbb{Z}) = (\mathbb{Z}[\theta]/(5^j))^\times$ is given by $k(5^j) = 31 \cdot 5^{j-1}$ for $j \geq 1$.

Put

$$X_{N,j} = \begin{cases} \{0\} & (j=0) \\ \{\eta \in \mathbb{Z}[\theta]/(5^j)\ ;\ \mathrm{ord}_2 \eta = N-j\} & (1 \leq j \leq N) \end{cases}.$$

Then we obtain a decomposition

$$\mathbb{Z}[\theta]/(5^N) = X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,N-1} \cup X_{N,N}.$$

Proposition 5.9.2. *Under the notations above, we have*:

(1) $X_{N,j} = \{\eta \in \mathbb{Z}[\theta]/(5^N)\ ;\ |\Theta\eta| = k(5^j) = 31 \cdot 5^{j-1}\}$ *for* $1 \leq j \leq N$. *Therefore, the isomorphism* $\tilde{\omega} : \mathbb{Z}[\theta]/(5^N) \overset{\sim}{\to} \mathcal{L}(P, \mathbb{Z}/5^N\mathbb{Z})$ *gives rise to bijections*

$$X_{N,j} \overset{\sim}{\to} \{\boldsymbol{w} \in \mathcal{L}(P, \mathbb{Z}/5^N\mathbb{Z})\ ;\ \boldsymbol{w} \text{ is of period } k(5^j) = 31 \cdot 5^{3(j-1)}\}$$

for $1 \leq j \leq N$.

(2) $|X_{N,j}| = \begin{cases} 1 & (j = 0) \\ 124 \cdot 5^{3(j-1)} & (1 \leq j \leq N) \end{cases}.$

(3) $|\Theta \backslash X_{N,j}| = \begin{cases} 1 & (j = 0) \\ 4 \cdot 5^{2(j-1)} & (1 \leq j \leq N) \end{cases}.$

Proof. (1) Let $\eta \in \mathbb{Z}_5[\theta]/(5^N)$ with $0 \leq \mathrm{ord}_5\eta < N$. Put $N - j = \mathrm{ord}_5\eta$. Then we have

$$\begin{aligned} |\Theta\eta| &= \text{the least positive integer } l \text{ such that } \theta^l\eta \equiv \eta \mod 5^N \\ &= \text{the least positive integer } l \text{ such that } \theta^l \equiv 1 \mod 5^j, \end{aligned}$$

which implies $|\Theta\eta| = k(5^j)$.

(2) For $0 \leq j \leq N-1$, we have

$$X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,j} = \mathrm{Ker}[\mathbb{Z}[\theta]/(5^N) \to \mathbb{Z}[\theta]/(5^{N-j})],$$

which implies $|X_{N,j}| = 5^{3j} - 5^{3(j-1)} = 124 \cdot 5^{3(j-1)}$ for $1 \leq j \leq N$.

(3) It follows from (1) and (2) that $|\Theta \backslash X_{N,j}| = (124 \cdot 5^{3(j-1)})/(31 \cdot 5^{j-1}) = 4 \cdot 5^{2(j-1)}$ for $1 \leq j \leq N$.

Notation 5.9.3. The residue ring $\mathbb{Z}_2[\theta] = \mathbb{Z}_2[t]/(t^3 - t^2 - t - 1)$ is a complete discrete valuation ring, and $\pi = \theta - 1$ is a uniformizer of $\mathbb{Z}_2[\theta]$ and $\mathrm{ord}_2\pi = 1/3$.

Put

$$\begin{aligned} X_{N,-1} &= \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ \eta = 0 \text{ or } \mathrm{ord}_2\eta = N - 1/3\}\ (N \geq 1), \\ X_{N,0} &= \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ \mathrm{ord}_2\eta = N - 2/3\}\ (N \geq 1), \\ X_{N,1} &= \begin{cases} \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ \mathrm{ord}_2\eta = 0\} & (N = 1) \\ \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ \mathrm{ord}_2\eta = N-1, N-4/3\} & (N \geq 2) \end{cases}, \\ X_{N,N} &= \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ \mathrm{ord}_2\eta = 1/3, 0\}\ (N \geq 2), \\ X_{N,j} &= \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ \mathrm{ord}_2\eta = N - j + 1/3, N - j, N - j - 1/3\} \\ &\qquad\qquad\qquad\qquad\qquad\qquad (N \geq 3,\ 2 \leq j \leq N-1) \end{aligned}$$

Then we obtain a decomposition

$$\mathbb{Z}[\theta]/(2^N) = X_{N,-1} \cup X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,N-1} \cup X_{N,N}.$$

Note that $\mathrm{ord}_2\eta = j \Leftrightarrow \mathrm{ord}_2\mathrm{Nr}\,\eta = 3j$.

Lemma 5.9.4. *Let j be an integer ≥ 1. Then we have*:
(1) *for $j = 1, 2$, $\mathrm{ord}_2(\theta^{2^j} - 1) = 2^j/3$ and $\mathrm{ord}_2(\theta^k - 1) \leq 2^{j-1}/3$ for $k < j$;*
(2) *for $j \geq 3$, $\mathrm{ord}_2(\theta^{2^j} - 1) = j - 2/3$ and $\mathrm{ord}_2(\theta^k - 1) \leq j - 5/3$ for $k < j$.*

Proposition 5.9.5. *Under the notations above, we have*:

(1) *$X_{N,j} = \{\eta \in \mathbb{Z}[\theta]/(2^N)\ ;\ |\Theta\eta| = 2^{j+1}\}$ for $-1 \leq j \leq N$. Therefore, the isomorphism $\tilde{\omega} : \mathbb{Z}[\theta]/(2^N) \xrightarrow{\sim} \mathcal{L}(P, \mathbb{Z}/2^N\mathbb{Z})$ gives rise to bijections*

$$X_{N,j} \xrightarrow{\sim} \{\boldsymbol{w} \in \mathcal{L}(f, \mathbb{Z}/2^N\mathbb{Z})\ ;\ \boldsymbol{w} \text{ is of period } 2^{j+1}\}$$

for $0 \leq j \leq N$.

(2)

$$\begin{aligned}
|X_{N,-1}| &= 2\ (N \geq 1), \\
|X_{N,0}| &= 2\ (N \geq 1), \\
|X_{N,1}| &= \begin{cases} 4 & (N = 1) \\ 12 & (N \geq 2) \end{cases}, \\
|X_{N,N}| &= 3 \cdot 2^{3N-2}\ (N \geq 2), \\
|X_{N,j}| &= 7 \cdot 2^{3j-2}\ (N \geq 3,\ 2 \leq j \leq N-1)
\end{aligned}$$

(3)

$$\begin{aligned}
|\Theta\backslash X_{N,-1}| &= 2\ (N \geq 1), \\
|\Theta\backslash X_{N,0}| &= 1\ (N \geq 1), \\
|\Theta\backslash X_{N,1}| &= \begin{cases} 1 & (N = 1) \\ 3 & (N \geq 2) \end{cases}, \\
|\Theta\backslash X_{N,N}| &= 3 \cdot 2^{2N-3}\ (N \geq 2), \\
|\Theta\backslash X_{N,j}| &= 7 \cdot 2^{2j-3}\ (N \geq 3,\ 2 \leq j \leq N-1)
\end{aligned}$$

Proof. (1) Let $\eta \in \mathbb{Z}_2[\theta]/(2^N)$ with $0 \leq \mathrm{ord}_2\eta < N$. Put $s = \mathrm{ord}_5\eta$. Then we have

$$\begin{aligned}
|\Theta\eta| &= \text{the least positive integer } l \text{ such that } \theta^l\eta \equiv \eta \mod 2^N \\
&= \text{the least positive integer } l \text{ such that } \theta^l \equiv 1 \mod 2^{N-s}.
\end{aligned}$$

By Lemma 5.9.4, we have

$$l = \begin{cases} 1 & \text{if } s = N - 1/3 \\ 2 & \text{if } s = N - 2/3 \\ 4 & \text{if } n = 1,\ s = 0, \text{ or } N \geq 2,\ s = N-1, N-4/3 \\ 2^{j+1} & \text{if } N \geq 3,\ 2 \leq j \leq N-1 \text{ and } s = N-j+1/3, N-j, N-j-1/3 \\ 2^{N+1} & \text{if } N \geq 2 \text{ and } s = 1/3, 0 \end{cases} .$$

(2) For $N \geq 2$ and $1 \leq j \leq N-1$, we have

$$X_{N,-1} \cup X_{N,0} \cup X_{N,1} \cup \cdots \cup X_{N,j} = \mathrm{Ker}[\mathbb{Z}[\theta]/(2^N) \to \mathbb{Z}[\theta]/(2^{N-j-1/3})],$$

which implies $|X_{N,j}| = 2^{3j+1} - 2^{3j-2} = 7 \cdot 2^{3j-2}$. Moreover, $|X_{N,N}| = 2^{3N} - 2^{3N-2} = 3 \cdot 2^{3N-2}$ and $|X_{N,1}| = 4 - 1 = 2$.

(3) It follows from (1) and (2) that $|\Theta \backslash X_{N,j}| = (7 \cdot 2^{3j-2})/2^{j+1} = 7 \cdot 2^{2j-3}$ for $1 \leq j \leq N-1$, and $|\Theta \backslash X_{N,N}| = (3 \cdot 2^{3N-2})/2^{N+1} = 3 \cdot 2^{2N-3}$.

References

[1] Aoki, M. and Kida, M., On the Laxton group, *Res. Number Theory*, **5** (2019), Art. 13, 22pp.

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

[3] Ballot, C., Density of prime divisors of linear recurrences, *Memoir of the A. M. S.,* vol. 115, Amer. Math. Soc., Providence, RI, 1995.

[4] Ballot, M., Group structure and maximal division for cubic recursions with a double root, *Pacific J. Math.*, **173** (1996), 337–355.

[5] Carmichael, R. D., On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.*, **15** (1913), 30–70.

[6] Demazure, M. and Gabriel, P., *Groupes algébriques, I*, Masson/North-Holland, 1970.

[7] Hall, M., An isomorphism between linear recurring sequences and algebraic rings, *Trans. Amer. Math. Soc.*, **44** (1938), 196–218.

[8] Lagarias, J. C., The set of primes dividing the Lucas numbers has density 2/3, *Pacific J. Math.*, **118** (1985), 449–461.

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

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

[11] Lucas, E., Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.*, **1** (1878), 184–240.

[12] Suwa, N., Twisted Kummer and Kummer-Artin-Schreier theories, *Tôhoku Math. J.*, **60** (2008), 183–218.

[13] Suwa, N., Geometric aspects of Lucas sequences. I, To appear in Tokyo J. Math.

[14] Suwa, N., Geometric aspects of Lucas sequences. II, Preprint series No.125, Department of Mathematics, Chuo University (2018)

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

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

[17] Waterhouse, W. C., Introduction to affine group schemes, Springer, 1979.